

Counterphish : Phishing Dark Waters, Beyond the Hook.

**Building
Human
Firewalls
Against
Evolving
Digital Fraud**



By : Khawar Nehal and Belal Jahangir

Version 1.0

Date : 30 July 2025

Part 1: Foundations of Digital Deception

Chapter 1: History of Scams → Digital Phishing

- **1.1 Evolution of Social Engineering**
 - 1.1.1 Pre-Internet Cons (Nigerian Prince Scam Origins)
 - 1.1.2 First Recorded Phishing Attacks (1996 AOL Cases)
 - 1.1.3 Web 2.0 Exploitation (MySpace/Facebook Era)
- **1.2 Major Historical Breaches**
 - 1.2.1 Target 2013: HVAC Vendor Compromise
 - 1.2.2 RSA SecurID 2011: Spear-Phishing Timeline
 - 1.2.3 Colonial Pipeline 2021: DarkSide Phishing Lure Analysis
- **1.3 Cybercrime Milestones**
 - 1.3.1 Phishing-for-Ransomware Shift (2015-Present)
 - 1.3.2 Cryptocurrency Scam Waves (2017 ICOs → 2021 DeFi)

Chapter 2: Human Psychology & Cognitive Biases (200p)

- **2.1 Exploitable Cognitive Flaws**
 - 2.1.1 Authority Bias (Fake CEO Requests)
 - 2.1.2 Scarcity Urgency (“24-Hour Account Closure” Tactics)
 - 2.1.3 Herd Mentality (Fake “Trending” Alerts)
 - **2.2 Neuroscientific Triggers**
 - 2.2.1 Dopamine Response to Notification Designs
 - 2.2.2 Stress-Induced Compliance Patterns
-

Part 2: Modern Phishing Techniques

Chapter 3: Advanced Email Threats

- **3.1 Business Email Compromise (BEC)**
 - 3.1.1 Vendor Impersonation Workflows
 - 3.1.2 CEO Fraud Psychological Profiling
 - 3.1.3 Invoice Scam Forensic Signatures
- **3.2 Evasion Techniques**
 - 3.2.1 Homoglyph Domain Algorithms (e.g., “AppIe.com”)
 - 3.2.2 Dynamic HTML Obfuscation
 - 3.2.3 Attachment Sandbox-Breaching Methods

Chapter 4: Multi-Channel Attacks (350p)

- **4.1 QR Phishing (Quishing)**
 - 4.1.1 Physical-Digital Bridge Exploits (Malicious Posters)
 - 4.1.2 QR Code Generation Toolkits
 - **4.2 Collaboration Platform Threats**
 - 4.2.1 Slack/Microsoft Teams Malware Delivery
 - 4.2.2 Fake Meeting Links (Zoom/WebEx)
-

Part 3: Technical Defenses

Chapter 5: Email Security Protocols

- **5.1 DMARC Deep Dive**
 - 5.1.1 Policy Enforcement Hierarchies (p=none → quarantine → reject)
 - 5.1.2 Forensic Reporting Analysis Tools
 - 5.1.3 Subdomain Policy Inheritance Risks
- **5.2 BIML Implementation**
 - 5.2.1 Verified Mark Certificate (VMC) Requirements
 - 5.2.2 Logo Spoofing Countermeasures

Chapter 6: AI-Powered Defense Systems

- **6.1 Natural Language Processing (NLP)**
 - 6.1.1 Linguistic Anomaly Detection Models
 - 6.1.2 Generative Adversarial Network (GAN) Training
 - **6.2 Behavioral AI**
 - 6.2.1 Mouse Movement Biometrics
 - 6.2.2 Session Hijacking Prediction Algorithms
-

Part 4: Human Firewall Development

Chapter 7: Training Program Architecture

- **7.1 Microlearning Modules**
 - 7.1.1 90-Second Threat Recognition Drills
 - 7.1.2 Just-in-Time Mobile Learning (JITML)
- **7.2 Phishing Simulation Science**
 - 7.2.1 Difficulty Scoring Systems (Vishing vs. Smishing)
 - 7.2.2 Ethical Boundaries in Trauma-Inducing Scenarios

Chapter 8: Role-Specific Training

- **8.1 Executive Protection Protocols**
 - 8.1.1 Digital Executive Shielding (DES) Frameworks
 - 8.1.2 Family Office Threat Mitigation
 - **8.2 Finance Team Defense**
 - 8.2.1 Payment Redirection Scenario Drills
 - 8.2.2 Cryptocurrency Wallet Social Engineering
-

Part 5: Industry-Specific Defense

Chapter 9: Healthcare Sector

- **9.1 HIPAA-Compliant Response**
 - 9.1.1 Patient Data Ransomware Negotiation
 - 9.1.2 Medical Device Phishing Vectors (IoT Risks)

- **9.2 Telemedicine Exploits**
 - 9.2.1 Fake Patient Portal Tactics
 - 9.2.2 EHR System Credential Harvesting

Chapter 10: Financial Institutions

- **10.1 SWIFT Network Protections**
 - 10.1.1 Transaction Verification Dual-Control Systems
 - **10.2 Deepfake Vishing**
 - 10.2.1 Voice Cloning Detection Tools
 - 10.2.2 Synthetic Video Countermeasures
-

Part 6: Future Threat Landscape

Chapter 11: AI-Augmented Threats

- **11.1 Generative Phishing**
 - 11.1.1 GPT-Phish Campaign Case Studies
 - 11.1.2 Personalized Lure Generation Engines
 - **11.2 Quantum Computing Risks**
 - 11.2.1 Post-Quantum Cryptography Migration
 - 11.2.2 Q-Day Preparedness Checklists
-

Part 7: Operational Toolkits

Chapter 12: Incident Response Playbooks

- **12.1 Triage Procedures**
 - 12.1.1 Compromised Account Containment Ladders
 - 12.1.2 Threat Actor Communication Protocols
 - **12.2 Forensic Investigation**
 - 12.2.1 Browser Artifact Analysis (IndexedDB, Cache)
 - 12.2.2 Mobile Device SMS Acquisition Techniques
-

Copyright Notice

© 2025 Khawar Nehal. All rights reserved.

This document is protected by copyright law. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the copyright owner, except in the case of brief quotations in critical reviews or articles.

For permission requests, write to the publisher at the address below:

Khawar Nehal

Remote Support LLC

315 E 5TH ST STE 202 WATERLOO IA 50703-4757 USA

Phone : +1 563 231 7041

Email : khawar@remote-support.space

Web : <http://remote-support.space>

Applied Technology Research Center

C-55 Block A KDA Officers, Karachi 75260, Sindh, Pakistan

Phone : +92 343 270 2932

Email : khawar@atrc.net.pk

Web : <http://atrc.net.pk>

[Table of Contents](#)

1.1.1 Pre-Internet Cons (Nigerian Prince Scam Origins)

Long before the age of email and social media, confidence tricksters perfected the **advance-fee scam**, a scheme in which a victim is promised a large reward—but only after paying a small “processing” fee up front. One of the earliest and most enduring variants was the “**Spanish Prisoner**” **letter scam**, which dates back to at least the 19th century:

- **Spanish Prisoner Scam (late 18th–early 20th centuries)**

Con artists would send letters claiming that a wealthy aristocrat was unjustly imprisoned in Spain. They’d promise the recipient a share of a hidden fortune in exchange for funds to secure the prisoner’s release. By the early 1900s, newspapers such as *The Fargo Forum and Daily Republican* were reporting near-falls of victims almost paying out based on these letters ([Prairie Public](#), [WNYC Studios](#)).

- **Mechanics of the Advance-Fee Trick**

1. **Initial Contact:** A personalized letter arrives, often addressed to “Friend” or “Esteemed Colleague,” describing dire circumstances requiring immediate financial help.
2. **Small First Fee:** Victims are asked for a modest sum (e.g., postage or a legal fee) “to secure documents.”
3. **Escalating Demands:** Once the first fee is paid, the con artist invents additional obstacles—more “legal” or “transfer” costs—each time promising imminent payoff.
4. **Vanishing Act:** After collecting enough small payments, the scammer disappears, leaving the victim empty-handed.

The **FBI** defines this type of fraud as an “advance-fee scheme,” noting that scammers promise a valuable reward in exchange for up-front payments that they never deliver ([Wikipedia](#)).

- **Transition to the “Nigerian Prince” (pre-Internet, 1980s–1990s)**

As global postal and fax networks expanded, the classic advance-fee trick migrated into new geographies. By the 1980s, fraudsters operating out of Nigeria began sending letters and faxes claiming to be members of a deposed royal family or high-ranking government officials. The narrative typically ran:

“I am Prince X of [Former Kingdom]. My family’s assets are frozen after a coup. If you advance ₦500,000 for legal fees, I will share ₦50 million...”

- **Why Nigeria?**

Economic and political turmoil in Nigeria during the 1980s and early 1990s—coups, oil price crashes, and widespread corruption—created ripe conditions for such cons. Although the offices of actual Nigerian royalty did not exist, the allure of quick riches combined

with the anonymity of international mail made the scheme remarkably effective ([Science Friday](#), [Wikipedia](#)).

- **“419 Scam” Terminology**

These Nigerian variants became known as **419 scams**—named for Section 419 of the Nigerian Criminal Code that deals with fraud—well before the advent of the Internet. Victims were drawn in by affectionate pen-pal letters, small test-payments, and the gradual escalation of fees, mirroring the structure perfected by the Spanish Prisoner swindle.

This pre-Internet era laid the social-engineering groundwork—leveraging **authority**, **scarcity**, and **reciprocity**—that would later propel the “Nigerian Prince” scam into global infamy in the email age.

1.1.2 First Recorded Phishing Attacks (1996 AOL Cases)

In early 1996, the warez community on America Online (AOL)—initially focused on trading pirated software and “cracking” credit-card generators—pivoted to a new form of deception: stealing genuine user credentials. After AOL successfully blocked algorithmically generated credit-card numbers, hackers turned to posing as AOL staff to trick real subscribers into divulging their login and billing information (phishing.org, [Infosec Institute](http://InfosecInstitute.com)).

- **AOHell Toolkit & Automated Scripts**

The breakthrough tool was **AOHell**, a Windows application released by a teenage hacker in January 1994. By 1996, AOHell had been extended with “phishing” modules that automated message-sending to hundreds of users at once. These scripts generated windows mimicking official AOL billing dialogs and dispatched them via AOL Instant Messenger or chat rooms, prompting unsuspecting users to enter their passwords and credit-card details into fraudulent forms ([Wikipedia](http://Wikipedia.org), [Surfshark](http://Surfshark.com)).

- **Origin of the Term “Phishing”**

On **January 2, 1996**, the term “**phishing**” first appeared in the Usenet newsgroup **alt.online-service.america-online**, describing the tactic of “fishing” for passwords with electronic lures. Early phishers deliberately substituted “ph” for “f” (echoing hacker slang like “phreaking”), giving the scam its enduring name ([History of Information](http://HistoryofInformation.com), [IJRASET](http://IJRASET.com)).

- **Social-Engineering Tactics**

Attackers crafted screen names such as “**AOLBilling**,” “**AccountSupport**,” or “**CustomerService**”, exploiting users’ trust in official-looking handles. Messages were carefully worded to invoke authority and urgency:

“**Dear Subscriber**, due to a billing error, your account will be suspended. Please verify your password and credit-card number by replying to this private message.”

Once users complied, phishers instantly harvested valid credentials and sold or abused the accounts for spam, warez distribution, and further attacks (phishing.org, [Infosec Institute](http://InfosecInstitute.com)).

- **AOL’s Countermeasures**

As losses mounted, AOL implemented on-screen warnings, blocked known phishing scripts, and added two-factor challenges for password changes. Though rudimentary by today’s standards, these measures significantly disrupted the first wave of phishing—proving that even basic technical defenses, combined with user education, can blunt social-engineering attacks ([Control Engineering](http://ControlEngineering.com), [Get Cyber Safe](http://GetCyberSafe.com)).

This 1996 AOL episode represents the first documented use of bulk, scripted social engineering to harvest credentials—a clear progenitor of the global phishing scourge that would explode with the rise of mass email in the late 1990s and early 2000s.

Evolution of Social Engineering

▣ Web 2.0 Exploitation (MySpace/Facebook Era)

Mid-2000s to Early 2010s

🔍 Overview

The rise of **Web 2.0** transformed the internet into a participatory space where users shared real identities, personal details, and social connections. Platforms like **MySpace, Facebook, Orkut, and LinkedIn** became digital playgrounds—not just for users, but also for **social engineers**, who exploited the openness, trust, and interconnectivity of these networks.

🔑 Key Exploitation Techniques

▣▣▣ Fake Profiles & Impersonation

- Attackers created cloned or entirely fictional personas.
- They gained friend connections and trust to spread:
 - Malware links
 - Scam messages
 - Credential-stealing forms

Example: “Hi, it’s me from your school group! Can you do me a quick favor?”

🗡️ Clickjacking & Likejacking

- Users were tricked into clicking hidden buttons or liking malicious posts.
- Often involved sensational content or curiosity bait:
 - “Shocking video! You have to see this!”

Clicking a “play” button actually “liked” or shared a malware link.

▣ Social App Exploitation

- Early Facebook apps (quizzes, games, “who viewed your profile”) collected:
 - Names
 - Emails
 - Friend lists

- Locations
- Data was often sold, stolen, or reused in phishing or fraud campaigns.

“Which superhero are you? Just allow access to your profile to find out!”

▣ Spear Phishing via Personal Info

- Public details like birthdays, employers, locations, and posts allowed attackers to:
 - Craft **tailored phishing messages**
 - Imitate friends or colleagues
 - Deliver more believable scams

“Hey [Name], here are your vacation photos! Just log in to see.”

▣ Why These Attacks Succeeded

- **Oversharing:** Users publicly listed personal data (school, job, etc.)
- **Trust by design:** Friendships = credibility
- **Low awareness:** Few knew about phishing, impersonation, or fake apps
- **Lack of platform controls:** No strong permission systems or verification features early on

▣ Notable Case Study: Koobface Worm

- Spread on Facebook via fake video links (“Is this you?”)
- Redirected users to malware pages
- Turned infected devices into part of a botnet
- Harvested credentials and promoted further attacks

♥ Platform Responses

- Facebook and others eventually introduced:
 - Two-Factor Authentication (2FA)
 - Restricted app permissions
 - Flagging of suspicious content
 - Phishing awareness popups

▣ Legacy of the Era

- Set the stage for **targeted social engineering** and identity-based scams
- Techniques refined during this time later fueled:
 - Business Email Compromise (BEC)

- Romance scams
- Fake recruiter scams
- Deepfake-enhanced deception

Major Historical Breaches

1.2.1 Target 2013: HVAC Vendor Compromise

□ Overview

In **late 2013**, retail giant **Target Corporation** suffered one of the most high-profile data breaches in U.S. history, resulting in the theft of **40 million credit and debit card records** and **70 million personal customer records**. The attack was not only notable for its scale but for how the **attackers gained access—through a third-party HVAC vendor**.

🔑 How the Breach Happened

- Vendor Access as Initial Entry Point

- Attackers **phished credentials** from **Fazio Mechanical Services**, an HVAC contractor working with Target.
- Fazio had access to **Target's vendor portal**, used for billing and contract work.

This minor vendor had **network credentials**, but lacked **multi-factor authentication** or network segmentation.

- Lateral Movement and Malware Deployment

- Once inside the vendor portal, attackers used **privilege escalation and lateral movement** to access Target's **Point-of-Sale (POS) network**.
 - They installed **memory-scraping malware (BlackPOS)** on POS terminals to capture customer payment data.
-

- Data Exfiltration

- Card data was **encrypted, staged**, and **exfiltrated in batches** to attacker-controlled external servers.
 - Attackers used **foreign servers** and tools to avoid detection.
-

📁 What Was Stolen

- **40 million** credit/debit card numbers (track data + CVV)
- **70 million** customer records (names, emails, addresses, phone numbers)

□ Timeline

- **November 15, 2013:** Intrusion begins
 - **November 27, 2013:** Malware deployed to POS systems (Black Friday weekend)
 - **December 15, 2013:** Breach publicly reported
 - **January 2014:** CEO and CIO resign
 - **2017:** Target agrees to an \$18.5 million multistate settlement
-

□ Why It Worked

Weakness	Description
Lack of Vendor Network Segmentation	Vendor had access to critical internal systems
Poor Authentication Controls	No 2FA for external vendors
Insufficient POS Monitoring	Malware went undetected for weeks
Delayed Response	Alarms were triggered but not acted upon quickly

⚖ Impact & Aftermath

- **Financial Cost:** Over **\$200 million** in losses, lawsuits, and settlements
 - **Reputation Damage:** Erosion of customer trust during peak retail season
 - **Security Reform:** Major retailers reevaluated third-party access policies
-

□ Lessons Learned

- **Third-party risk is organizational risk**
- Implement **Zero Trust architecture**: never assume any connection is safe
- **Continuous monitoring** and **segmented networks** are critical
- Visibility into supply chain security is now a **compliance requirement**

Major Historical Breaches

1.2.2 RSA SecurID 2011: Spear-Phishing Timeline

♥ Overview

In **March 2011**, RSA Security (a division of EMC) suffered a **sophisticated cyberattack** that compromised the integrity of its **SecurID two-factor authentication system**—used by **militaries, governments, and Fortune 500 companies**. The breach began with a **spear-phishing email** and eventually undermined global trust in RSA's security products.

“The attack on RSA was not just against a company—it was against the backbone of enterprise authentication systems.”

✉ How the Attack Began: Spear-Phishing Entry

- March 2011: Email with Malicious Excel File

- An email with the **subject line: “2011 Recruitment Plan”** was sent to a **small number of RSA employees**.
- It contained a **malicious Excel spreadsheet** with an embedded **zero-day Flash vulnerability**.
- Once opened, it silently downloaded a **remote access tool (Poison Ivy)**.

Despite being caught by spam filters, the email was manually moved to inboxes by recipients—a classic example of social engineering over technical barriers.

□ Timeline of the Breach

Date	Event
March 2011	Spear-phishing email sent; initial infection via Excel zero-day
Week 1	Attackers escalate privileges and pivot within RSA's internal network
Week 2–3	Secure files related to SecurID algorithm and token operations exfiltrated
April 2011	RSA publicly acknowledges breach in blog post and media statements
June 2011	Lockheed Martin targeted—attack linked to stolen RSA token data

🔓 What Was Stolen

- Sensitive data related to **SecurID's seed values**, token generation, and internal mechanisms
 - Not customer credentials directly, but **enough metadata to weaken the authentication process**
-

🎯 Strategic Targeting

- Believed to be part of a **nation-state operation** (possibly Chinese APT groups)
 - Purpose: To **compromise high-value targets** by breaking SecurID-protected environments
 - Later attacks on **Lockheed Martin, Northrop Grumman, and L-3 Communications** were tied to this breach
-

⚠️ Why It Worked

Vulnerability	Description
Social Engineering	Convincing spear-phishing email bypassed user suspicion
Zero-Day Exploits	Flash vulnerability unknown to security software
Lack of Internal Segmentation	Attackers could move laterally with limited resistance
Metadata Leakage	Attackers didn't need passwords—just token mechanics and seed info

🔚 Aftermath

- RSA issued **72,000 replacement SecurID tokens**
 - Customers were urged to **add additional layers of authentication**
 - RSA's **brand trust** took a significant hit
 - Sparked **industry-wide re-evaluation** of reliance on token-based 2FA
-

📌 Lessons Learned

- **Spear-phishing remains a top-tier threat vector—even for cybersecurity firms**
- Attacks may target **metadata or internal systems**, not just credentials
- **Zero-day defense, endpoint protection, and employee training** must align

- Breaches in trust-based systems can ripple through **entire national infrastructures**

Major Historical Breaches

1.2.3 Colonial Pipeline 2021: DarkSide Phishing Lure Analysis

Overview

In **May 2021**, Colonial Pipeline—the largest refined oil pipeline in the United States—was hit by a **ransomware attack** orchestrated by the **DarkSide cybercriminal group**. The attack led to a **multi-day shutdown** of fuel delivery across the East Coast, sparking fuel shortages, price spikes, and national panic.

This was the **first major cyberattack** to cause **physical disruption of critical infrastructure** at national scale in the U.S.

Initial Access: Phishing Lure & VPN Exploitation

- DarkSide's Entry Strategy

- While the **exact phishing email** has not been publicly disclosed, U.S. federal investigations and forensic analysis confirm that:
 - The attackers **gained VPN credentials** via a compromised employee account.
 - The **account had no multi-factor authentication (MFA)** enabled.
 - It is **believed** that the credentials were obtained through a **prior phishing campaign** or dark web leak.

“They only needed one unlocked door—a single account with no MFA.”

Attack Timeline

Date	Event
April 2021	Compromised VPN credentials obtained (via phishing or credential reuse)
May 6, 2021	Ransomware deployed to Colonial's internal business network
May 7, 2021	Colonial shuts down the pipeline as a precautionary measure
May 8–12, 2021	Fuel shortages and panic buying across Southeastern U.S.

May 13, 2021	Colonial confirms it paid a \$4.4 million ransom in cryptocurrency
June 2021	FBI recovers \$2.3 million of the ransom by tracing crypto wallets

🔧 Technical Execution

- Ransomware payload was custom-built using **DarkSide RaaS (Ransomware-as-a-Service)** platform.
- It **encrypted corporate files**, email servers, and key business operations—but **not the industrial control system (ICS)** directly.
- Colonial shut down pipeline operations **out of caution**, fearing further spread.

📉 Impact

- **5,500 miles of pipeline** shut down
- **12,000 gas stations** out of fuel across the Southeast
- Flight delays and disruptions in airline fuel supplies
- **Presidential emergency declaration** issued
- Colonial Pipeline paid **\$4.4M** in Bitcoin, later partially recovered

🔍 Why It Worked

Weakness	Description
No MFA on VPN Access	Allowed attackers in with a single stolen password
Lack of Segmentation	Business systems connected to operational shutdown triggers
Human Error (Credential Reuse)	Password may have been reused or leaked from another service
Reactive Shutdown	Fear of spread caused voluntary shutdown—even without ICS hit

♥ Security Response & Reforms

- Colonial implemented **MFA and endpoint detection** post-attack
- U.S. government launched **new federal guidelines** for pipeline cybersecurity
- CISA and FBI issued bulletins on **DarkSide TTPs (Tactics, Techniques, Procedures)**
- Sparked the **first major public-private push** toward critical

infrastructure defense

⚖️ Legal & Policy Impact

- U.S. created the **Ransomware Task Force**
 - Encouraged crypto-tracing operations (Chainalysis, FBI wallet monitoring)
 - Elevated ransomware to **national security threat level**
-

📦 Lessons Learned

- **Phishing and credential reuse remain devastatingly effective**
- Even **non-ICS attacks** can paralyze critical infrastructure through indirect disruption
- Ransomware gangs now **operate like businesses**, complete with helpdesks and affiliate programs
- **MFA is not optional** for any system with remote access privileges

Cybercrime Milestones

1.3.1 Phishing-for-Ransomware Shift (2015–Present)

The Convergence of Social Engineering and Crypto-extortion

Overview

Beginning around **2015**, cybercriminals increasingly fused **phishing attacks with ransomware deployment**—using deceptive emails not just to steal credentials, but to gain entry into systems and **encrypt entire networks** for ransom. This strategic shift gave rise to the modern era of **“Big Game Hunting”**, where high-value targets are attacked with customized ransomware through spear-phishing.

“From inbox to lockdown—one click, and the whole company is paralyzed.”

Pre-2015: Classic Phishing Use-Cases

- **Credential harvesting:** Email login pages (Office365, Gmail)
- **Bank fraud:** Impersonating financial institutions
- **Malware delivery:** Keyloggers, adware, basic trojans
- Goal: Steal information **quietly and discreetly**

Post-2015: Ransomware Joins the Payload

- **Phishing emails** became the **main entry vector** for ransomware
- Emails often included:
 - **Booby-trapped attachments** (.doc, .xls with macros)
 - **Links to malware-laced websites**
 - **Socially engineered messages** from fake HR, IT, or CEO accounts

Example Subject Line: “Urgent: Updated Covid-19 Remote Work Policy.docm”

Major Campaigns and Actors

Year	Actor/Group	Target Type	Method
2016	Locky Ransomware	Hospitals, SMBs	Malicious Word attachments
2017	WannaCry	Global (via SMB)	Combined phishing and

		vuln)	exploits
2018	Ryuk (via TrickBot)	Enterprises	Phishing + credential harvesting
2020	Maze	Corporates, Gov	Phishing → lateral movement → ransomware
2021	Conti/DarkSide	Critical infrastructure	Phishing → remote access → lockdown

🔗 Extortion Evolution: Double & Triple Threats

- **Double extortion** (2019–present):
 - Encrypt data **AND** steal it, then threaten to leak
- **Triple extortion** (2021–present):
 - Encrypt + leak + **DDoS attack** to pressure victims

“Pay us, or we’ll leak your files and crash your site too.”

📌 Why It Worked

Factor	Description
Human Error	Phishing relies on emotional triggers and urgency
Poor Email Hygiene	Lack of filtering, no attachment scanning
Weak Endpoint Security	Inadequate detection of script-based ransomware
No Segmentation	One compromised system often led to full network access
Untested Backups	Victims couldn’t recover without paying

♥ Security Shifts Post-2015

- Rapid adoption of:
 - **Email gateways & sandboxing**
 - **MFA everywhere**
 - **Security awareness training**
- Rise of **Zero Trust architectures** and **EDR (Endpoint Detection and Response)** tools
- Governments began **banning ransom payments** and regulating breach disclosures

🌐 Global Impact

- **Cyber insurance premiums skyrocketed**

- Enterprises began **treating ransomware as a disaster scenario**
 - Led to **nation-state mimicry** of ransomware gangs for plausible deniability
 - Cemented **phishing** as the single **most dangerous initial access vector**
-

□ Key Takeaways

- Phishing is no longer just for stealing info—**it is now the front line of extortion**
- Email is the **#1 attack vector** for ransomware groups
- Defense requires a **people-process-technology blend**, not just tools

Cybercrime Milestones

1.3.2 Cryptocurrency Scam Waves (2017 ICOs → 2021 DeFi)

From token hype to decentralized rug pulls

📌 Overview

The rise of cryptocurrency brought unprecedented financial innovation—and a gold rush of **fraud, deception, and social engineering**. Beginning with the **ICO boom of 2017** and evolving into **DeFi and NFT scams by 2021**, cybercriminals exploited hype, anonymity, and lack of regulation to steal **billions of dollars** from retail and institutional investors.

“The blockchain never lies—but scammers don’t need to. They just need you to believe.”

📌 2017–2018: ICO Mania & Fake Token Projects

- What is an ICO (Initial Coin Offering)?

- A blockchain-based method for startups to raise capital by issuing new cryptocurrencies
- Buyers invest in hopes that tokens will rise in value like early Bitcoin or Ethereum

- Common Scams:

- **Fake Teams:** Stolen LinkedIn profiles, fake advisors
- **Pump-and-Dump Tokens:** Hyped up, dumped after launch
- **Whitepaper Clones:** Copied technical documents from legitimate projects
- **Exit Scams:** Developers raised millions and vanished

Example: “BitConnect” promised 1% daily returns. In 2018, it collapsed as a Ponzi scheme after taking in over **\$2 billion**.

📌 2019–2020: NFT and Crypto Wallet Phishing

- Rise of crypto wallets like **MetaMask, Trust Wallet, and Ledger**
- Attackers used:
 - Fake “airdrop” campaigns
 - Imitation websites with wallet-connect popups
 - **Seed phrase phishing** (social media, fake support accounts)

“To claim your NFT, just enter your wallet seed phrase.”

▣ 2020–2021: DeFi Boom and Smart Contract Exploits

- What is DeFi?

- Decentralized Finance: Crypto lending, trading, or yield farming apps with **no central authority**
- Built on smart contracts (often unaudited, exploitable)

- Common DeFi Scams:

- **Rug Pulls:** Developers remove all liquidity and flee
- **Flash Loan Attacks:** Exploit protocols by borrowing huge amounts with no collateral
- **Fake Tokens:** Lookalike coin names, often using known brands like “UniSwap,” “TeslaCoin,” etc.
- **Front-End Spoofing:** Fake DeFi site mimicking real one, designed to steal funds

Example: “Meerkat Finance” (2021) stole \$31M in BNB by draining smart contracts within 24 hours of launch.

▣ Scam Progression Timeline

Year	Wave	Key Scam Types
2017	ICO Boom	Fake coins, Ponzi tokens, exit scams
2018	ICO Bust	Regulatory crackdown, lawsuits
2019	Wallet Phishing	Fake sites, support scams, seed theft
2020	NFT Phishing Begins	“Free drop” bait, Discord hacks
2021	DeFi Rug Pulls	Smart contract exploits, liquidity theft

▣ Why They Worked

Weakness	Exploited Factor
Hype & Greed	Promises of “next Bitcoin” with quick returns
Lack of Regulation	No KYC/AML, no investor protections
Technical Illiteracy	Users didn’t understand wallet security or smart contracts
Anonymous Developers	No accountability, no legal trail
Social Proof Illusions	Fake Discord communities, bots simulating interest

⚖️ Global Impact

- **Over \$14 billion lost to crypto-related scams in 2021 alone** (Chainalysis)
 - Institutional investors also duped via DeFi protocols and fake VC partnerships
 - Fueled **skepticism of blockchain** from traditional finance and regulators
-

♥️ Mitigation Measures

- **Smart contract audits** (e.g., Certik, Trail of Bits)
 - **Wallet safety education:** Seed phrase protection, fake site detection
 - **DApp permission reviews** and revocation tools
 - Governments began:
 - Taxing crypto
 - Cracking down on crypto advertising
 - Enforcing **AML/KYC laws** in centralized exchanges
-

📌 Key Takeaways

- Crypto scams exploit **technical hype, social engineering, and anonymity**
- The same psychological levers used in email phishing are now deployed on-chain
- **Security in crypto = user education + trust minimization + smart contract audits**

Exploitable Cognitive Flaws

2.1.1 Authority Bias (Fake CEO Requests)

“Because the boss said so.”

□ Definition: Authority Bias

Authority bias is a cognitive shortcut in which people are more likely to comply with a request if it appears to come from someone in a position of authority—like a CEO, doctor, or law enforcement officer—even if the request seems unusual or suspicious.

“Humans are wired to follow orders from perceived authority figures—even without question.”

🔊 How It's Exploited in Social Engineering

- Business Email Compromise (BEC)

- Scammers spoof or hack an executive's email (e.g., CEO, CFO)
- Send urgent instructions to subordinates:
 - Wire transfers
 - Gift card purchases
 - Sharing sensitive documents
- Often timed late in the day or during holidays to avoid verification

Subject: *“Need this urgently — please process before end of day.”*

- Voice Spoofing (Fake CEO Phone Calls)

- Attackers use deepfake audio or social engineering to **impersonate a high-ranking executive** over the phone
 - Real-world: A 2019 UK company was scammed into wiring **€220,000** to a Hungarian supplier after a **deepfake voice call** from their “CEO”
-

- Whaling Attacks

- Target high-level executives directly
- Use admiration or intimidation to extract:
 - Login credentials
 - Confidential business documents
 - Executive calendars or passwords

“This is the CEO. I need you to verify your admin credentials so we can resolve a compliance issue immediately.”

⚠ Common Red Flags Overridden by Authority Bias

Signal Normally Suspicious	But Rationalized As...
Unusual request timing	“They must be in a time crunch.”
Generic or odd language	“They’re just stressed or traveling.”
Urgency & secrecy	“They must know more than I do.”
No confirmation allowed	“I’ll get in trouble if I delay asking.”

🧠 Why It Works Psychologically

- People are conditioned from school and work to **obey authority figures**
- Disobedience feels risky—especially in hierarchical organizations
- Attackers exploit workplace norms like “**don’t question leadership**”
- Urgency adds pressure, short-circuiting critical thinking

🌐 Real-World Examples

- **Ubiquiti Networks (2015)**: \$46.7M lost via fraudulent CEO email
- **Pathé Films (2018)**: \$21M transferred after a spoofed email from the CEO demanding secrecy
- **Facebook & Google (2013–2015)**: Combined \$100M+ loss to fake invoice requests impersonating senior executives

♥ Defense Tactics

- **Multi-step verification**: No financial request should be acted on from email alone
- **Verify requests via alternate channels** (phone, Slack, in person)
- **Executive impersonation training** in phishing simulations
- **Create a “safe-to-question” culture**: Staff must feel free to validate even urgent executive messages

📌 Key Takeaways

- Authority bias is **one of the most dangerous psychological vulnerabilities** in social engineering
- Attackers don’t need real access—just a believable impersonation of a

powerful figure

- Combating it requires **policy, verification processes, and cultural rewiring**

Exploitable Cognitive Flaws

2.1.2 Scarcity & Urgency (“24-Hour Account Closure” Tactics)

“Act now—or lose everything.”

⌘ Definition: Scarcity & Urgency Bias

Scarcity bias is a cognitive shortcut where people place **higher value on things perceived as limited**, while urgency creates **pressure to act quickly**, bypassing critical thinking. Together, they are core to many scam strategies.

“You have 24 hours to act, or your account will be permanently disabled.”

□ How It’s Exploited in Social Engineering

- Phishing Emails with Fake Deadlines

- Threaten imminent consequences (account deactivation, service suspension, legal action)
- Appear to be from:
 - Banks (“Verify your identity within 12 hours or we’ll freeze your account”)
 - Cloud services (“Your Google Drive will be deleted in 24 hours”)
 - HR or IT (“Your benefits access is expiring. Click here to renew.”)

- SMS & Vishing Scams

- Texts or calls using:
 - Limited-time offers (e.g., “last chance to claim your reward”)
 - Legal threats (e.g., “your SIM card will be blocked today”)
- Social engineering over the phone with intense emotional language:

“This is urgent—we need to confirm your identity or your card will be canceled.”

- Tech Support Scams

- Fake pop-ups warn of “virus infection” or “illegal activity” with

countdown timers

- Victims told they must call immediately or lose data/access

Example: *“You have 5 minutes to call Microsoft Support before your computer locks.”*

⚠ Common Red Flags Masked by Urgency

Suspicious Detail	Rationalized By Victim As...
Generic greeting (“Dear user”)	“They’re just automating the message.”
Poor grammar	“It must’ve been rushed due to urgency.”
Unusual sender domain	“Maybe it’s a backup email or secondary address.”
External link to login	“They said time is critical—I’ll fix it later.”

🧠 Why It Works Psychologically

- Urgency triggers **fight-or-flight** emotional response
- Scarcity causes **loss aversion**—fear of losing access, money, or opportunity
- The faster the decision must be made, the **less rational** it becomes
- Stress inhibits memory recall and technical awareness (e.g., checking URLs)

🌐 Real-World Examples

- **PayPal Phishing (Recurring):** “Account suspension within 24 hours” email with spoofed login page
- **Netflix Credential Harvesting:** “Payment failed—update info now to avoid service interruption”
- **COVID-19 Vaccine Scams (2021):** Fake portals offering “priority access” to vaccines for a limited time

♥ Defense Tactics

- **Slow down:** Teach users to pause when a message feels urgent
- **Hover-over practice:** Always check URLs before clicking
- **Timeout-resistant policies:** Enforce no urgent requests via email or SMS
- **Security banners:** Highlight external emails with warning labels
- **Simulated urgency phishing drills** to test and train users

□ **Key Takeaways**

- Scarcity and urgency are **core tools in manipulating fast decisions**
- These tactics override logic by creating **emotional pressure**
- Defense requires training people to **trust procedure over panic**

Exploitable Cognitive Flaws

2.1.3 Herd Mentality (Fake “Trending” Alerts)

“Everyone’s doing it—so should you.”

□ Definition: Herd Mentality

Herd mentality (also called **social proof bias**) is the psychological tendency to conform to what others are doing, especially in situations of uncertainty. People assume that if many others believe, buy, or act on something, it must be safe or correct—even if it’s not.

| “This link has gone viral—you need to see it before it’s taken down!”

□ How It’s Exploited in Social Engineering

- Fake Trending Alerts or Viral Posts

- Scammers use buzzwords like:
 - “Trending now”
 - “Most viewed today”
 - “Everyone is talking about this”
- Lures include:
 - Fake celebrity videos
 - Leaked documents
 - Shocking news or deaths
 - “Top 10 investment tips used by millionaires”

| Example: *“Elon Musk just launched a new crypto—join 100,000 others investing now!”*

- Bot-Boosted Social Media Posts

- Attackers inflate engagement with:
 - Fake likes
 - Bot comments (“This worked for me!”)
 - Retweets from cloned accounts
- Users trust the post based on **visible popularity**, not content authenticity

- Malicious “Like & Share” Campaigns

- Fake giveaways (“Share to win an iPhone”)

- Malware links or phishing sites disguised as:
 - Polls
 - Contests
 - Quizzes
 - Designed to go viral rapidly and gain trust through volume
-

▢ Platforms Commonly Abused

- **Facebook:** Viral “shocking video” bait
 - **Twitter/X:** Trending hashtags tied to scams
 - **YouTube:** Live streams with fake crypto giveaways
 - **Telegram/Discord:** Group chats full of bots echoing scam messages
-

▢ Why It Works Psychologically

Trigger	Effect
“Everyone’s doing it”	Reduces fear of being scammed—“so many people can’t be wrong”
FOMO (Fear of Missing Out)	Victims rush to act without verifying
Emotional Amplification	“You’re the last to know”—generates urgency through belonging pressure
Groupthink	Lack of independent thought when surrounded by consensus

▢ Real-World Examples

- **YouTube Crypto Giveaway Scams:** Fake Tesla or SpaceX livestreams offering to double your Bitcoin
 - **Fake Investment Discords:** 10,000-member groups hyping “pump-and-dump” coins
 - **Twitter Hacks (2020):** Verified accounts (Elon Musk, Apple) tweeted fake Bitcoin links
 - **COVID “Cures” and Hoaxes:** Viral misinformation shared by friends and influencers without verification
-

♥ Defense Tactics

- **Train users to question popularity:** High engagement doesn’t mean legitimacy
- **Look beyond engagement metrics:** Check source, domain, and context
- **Limit social sharing of sensitive actions** (e.g., never share login via group links)

- **Report and block** suspicious pages, contests, or “too good to be true” giveaways
 - **Use browser plug-ins** or tools that highlight bot-likes and comment farms
-

□ **Key Takeaways**

- Herd mentality gives attackers **mass trust at scale** without proof
- It's not what's being said, but **how many appear to believe it** that persuades
- The best defense is **critical skepticism—even when everyone else seems convinced**

Neuroscientific Triggers

2.2.1 Dopamine Response to Notification Designs

“The ping that hijacks your brain.”

□ Definition: Dopamine and Behavior

Dopamine is a neurotransmitter associated with **pleasure, reward, motivation, and habit formation**. It spikes when we **anticipate** a reward, not just when we receive it—creating feedback loops of behavior like checking notifications or refreshing apps.

“Every red bubble, buzz, or chime isn’t just information—it’s a hit of neural currency.”

□ How Notifications Hijack Attention

- Color Psychology

- Most alerts use **red**, which is evolutionarily linked to **danger and urgency**.
- The color stimulates **amygdala activation**—triggering a primitive emotional response.

- Variable Reward Systems

- Not every notification is rewarding—but **some are**.
- This creates a **dopamine loop**, similar to slot machines:
 - Randomized rewards = more compulsive checking
 - Intermittent reinforcement = stronger habit formation

Example: *One message is spam, the next is a crush. That unpredictability hooks you.*

□ Design Elements That Maximize Dopamine Response

Feature	Neurological Effect
Red badge icon	Triggers urgency, raises cortisol and dopamine levels
Buzz/vibration	Physical cue associated with anticipation
Sound notifications	Pavlovian association with reward or social validation

In-app alerts (popups)	Immediate interruption enhances salience and craving
Delay in message loading	Builds anticipation → stronger dopamine spike

□ Why It Works

- The **anticipation** of the unknown message stimulates more dopamine than the content itself.
- Dopamine builds **habit strength**—leading users to:
 - Check phones impulsively
 - Prioritize interruption over task
 - Ignore rational skepticism in the moment of alert

That's why phishing texts that mimic real notifications (“📦 Your delivery is on hold”) are so effective—they're riding this neurochemical wave.

□ Exploitation in Social Engineering

- **Phishing alerts** disguised as real app notifications:
 - “⚠ Suspicious login detected. Tap to verify.”
 - “📧 New message from HR. Action required.”
- Attackers exploit the **dopamine trigger** to push:
 - Instant clicks
 - Emotional decision-making
 - Suspended judgment

- Smishing (SMS Phishing) & Push Notification Spoofing

- Short, urgent messages delivered via mobile
- Tied to dopamine-induced **habitual device-checking**

Example: “New voicemail from Bank of America. Tap to listen.” (links to phishing page)

♥ Defense Tactics

- **Awareness training:** Teach users how dopamine is manipulated by design
- **Delay response discipline:** Pause 5 seconds before reacting to notifications
- **Use grayscale mode:** Reduces color-triggered urgency on phones
- **Audit app permissions:** Minimize apps allowed to push alerts
- **Turn off non-essential badges:** Prevent habitual checking without conscious intent

□ Key Takeaways

- Modern UI/UX is **neurologically weaponized** to maximize attention
- Attackers use these same tactics to inject **malicious urgency via familiar alerts**
- Controlling dopamine triggers = **regaining cognitive control and digital hygiene**

Neuroscientific Triggers

2.2.2 Stress-Induced Compliance Patterns

“Fear shuts down logic—just say yes.”

▣ **Definition: Cortisol and the Stress Response**

When we perceive a threat, our brain releases **cortisol**, the body’s primary **stress hormone**. This activates the **fight, flight, or freeze** response, reducing activity in the **prefrontal cortex** (responsible for decision-making and critical thinking) and increasing reliance on **reflexive action**.

▮ *“Under stress, we don’t think. We react.”*

△ **How Attackers Exploit Stress Responses**

- **Threat-Based Messaging**

- Social engineers trigger cortisol spikes using:
 - Legal threats (“You are under investigation.”)
 - Financial panic (“Unauthorized charges detected.”)
 - Professional consequences (“You’ll be reported to HR.”)

▮ *Example: “Your account will be reported for suspicious activity unless verified now.”*

- **Emotional Pressure Tactics**

- Attackers simulate urgency or personal crises to provoke:
 - Guilt (“Why didn’t you help me when I asked?”)
 - Shame (“You allowed a breach!”)
 - Fear (“You’re out of compliance!”)
-

- **Live Voice & Vishing Attacks**

- Real-time stress amplifies compliance
- Callers use:
 - Fast speech
 - Complex instructions
 - Authoritative tones
- Victims comply to **end the interaction quickly**, not because they believe it’s legitimate

“If you hang up, you may be liable for legal obstruction. Stay on the line.”

□ Neurological Impact of Stress on Decision-Making

Brain Function	Effect Under Stress
Prefrontal cortex	Suppressed (↓ logic, ↓ skepticism)
Amygdala (emotion center)	Activated (↑ fear, ↑ obedience)
Hippocampus (memory retrieval)	Impaired (↓ ability to recall protocol)
Dopamine	May be hijacked to reward <i>compliance</i>

□ Real-World Attack Scenarios

- **IRS Tax Scams:** “You owe back taxes. Pay now or be arrested.”
- **Fake IT Support:** “Your machine is infected—install this tool or lose access.”
- **Emergency Family Scams:** “Your son’s been in an accident. Send money for treatment.”
- **Corporate Urgency:** “CEO needs this wire transfer immediately. Don’t delay.”

□ Why It Works

- **Cognitive shutdown:** The brain bypasses rational checks under threat
- **Panic-induced haste:** Victims focus on *escaping stress*, not evaluating accuracy
- **Scripted obedience:** People default to compliance in unfamiliar, high-stress environments
- **Shame suppression:** People avoid embarrassment by silently obeying

♥ Defense Tactics

- **Train employees in stress recognition:** Teach how cortisol affects behavior
- **Use scripts for stressful scenarios:** “Pause. Verify. Escalate.”
- **Simulate stress-based phishing drills**
- **Encourage reporting without blame:** Mistakes made under pressure must be destigmatized
- **Build emotional resilience:** Calm users = resistant users

Business Email Compromise (BEC)

3.1.1 Vendor Impersonation Workflows

“When your supplier gets spoofed—your wallet bleeds.”

□ Definition: Vendor Impersonation in BEC

In **Vendor Impersonation**, attackers pose as **trusted third-party suppliers**, using forged or hijacked email accounts to trick organizations into making **fraudulent payments**—often by swapping out bank account details on legitimate invoices.

“You trust your vendor. The attacker knows that. So they become the vendor.”

□ Typical BEC Vendor Impersonation Workflow

Step 1: Intelligence Gathering

- Attacker identifies a business relationship:
 - Through **LinkedIn**, **email scraping**, or **previous phishing**
 - Looks for recurring invoice-based suppliers (e.g., IT support, construction firms, logistics)
- Collects:
 - Real vendor names, invoice formats, past amounts, and contact style

Step 2: Email Spoofing or Account Takeover

- Options:
 - **Spoofed domain**: @vvendorr.com instead of @vendor.com
 - **Real compromise**: Gains access to the vendor’s actual mailbox (via phishing or credential stuffing)

Example: Attacker sends from “billing@vvendorr.com” with the subject “Updated wire instructions.”

Step 3: Fake Invoice or Bank Details

- Attacker replicates or modifies a **real invoice**, changing:
 - **Bank account details**
 - **Sender email**
 - Sometimes adds urgency or explanation:

“Due to an audit, please remit this month’s payment to our new bank account.”

Step 4: Victim Executes Payment

- Victim (Accounts Payable team) sees:
 - Familiar vendor
 - Expected amount
 - Plausible explanation
- Trusting the source, they **wire funds to the attacker’s account**

Step 5: Funds Laundering

- Money quickly moved through:
 - Mule accounts
 - Crypto exchanges
 - Shell corporations
- Often untraceable after 48 hours

Real-World Examples

- **Toyota Boshoku (2019):** \$37 million loss via BEC impersonating a vendor
- **Scoular Co. (2014):** \$17 million transferred to China due to a fake acquisition invoice
- **City of El Paso (2019):** Paid \$3.1 million to a scammer posing as a construction contractor

Why It Works

Exploited Factor	Description
Familiar Relationship	Victim recognizes the vendor and trusts the brand
Realistic Language & Format	Attackers copy tone, template, and invoice details
Infrequent Verification	Vendor details rarely cross-checked for each payment
Busy Accounting Teams	Pressure to process payments quickly, especially EOM

Psychological Triggers Used

- **Authority Bias:** Request often appears to come from a senior vendor contact

- **Urgency Stress:** “We’ll apply late fees if unpaid today”
 - **Familiarity Bias:** Victim feels safe due to known relationship
-

♥ Defense Tactics

- **Payment Policy Hardening:**
 - Never change bank account details without **verbal confirmation**
 - Implement **multi-person approval chains**
 - **Email Authentication:**
 - Use **DMARC, SPF, DKIM** to detect spoofing
 - **Vendor Callback Protocol:**
 - Call a **known number** from your contact book—not from the email
 - **Monitor for Domain Lookalikes:**
 - Alert staff to subtle visual spoofs (vendor-pay.com vs. vend0r-pay.com)
 - **Automated Email Anomaly Detection:**
 - Use AI tools to flag unexpected changes in vendor messaging patterns
-

□ Key Takeaways

- Vendor impersonation BEC attacks are **highly targeted, socially engineered, and financially devastating**
- The attacker doesn’t break in—they **blend in**
- Prevention depends on **human-process-technology alignment**

Business Email Compromise (BEC)

3.1.3 CEO Fraud Psychological Profiling

“The con works best when the victim wants to obey.”

□ Definition: CEO Fraud

CEO fraud is a form of **executive impersonation** in which an attacker poses as a high-ranking official (often the CEO or CFO) to trick employees—typically in finance, HR, or IT—into **transferring funds, credentials, or sensitive data**.

□ “When the email says it’s from the CEO, who stops to question it?”

□ Psychological Profile of the Victim (Target Employee)

1. Obedient by Role

- **Administrative assistants, junior accountants, or IT staff**
- Trained to **serve and support higher-ups** without questioning their requests
- Often believe refusal = **risk to job security**

2. Conditioned to Urgency

- Familiar with real urgent tasks from executives
- Perceive **speed as loyalty**
- May skip standard checks under stress

3. Fear of Escalation

- Concerned about appearing **incompetent or insubordinate**
- May worry that asking for clarification will cause delay or embarrassment

4. Limited Security Training

- May not understand spoofing, domain lookalikes, or email header inspection
 - Vulnerable to emotionally charged, urgent, or confusing messages
-

🔗 Psychological Profile of the Attacker (Impersonator)

1. Manipulative Communicator

- Uses **authority tone**, commands, minimal detail
- Relies on psychological levers like:
 - **Urgency**: “Need this before EOD”
 - **Exclusivity**: “Confidential—do not discuss with others”
 - **Flattery**: “I trust you with this. You’re the only one I can rely on.”

2. Emotionally Detached

- Views victims as **transactional instruments**
- Understands fear, stress, and compliance but **feels no empathy**

3. Tactically Patient

- May **study internal communications** first:
 - Signature styles
 - Scheduling norms
 - Executive communication tone

📋 Behavioral Manipulation Techniques

Technique	Purpose	Example
Authority Bias	Triggers obedience	“This is from the CEO.”
Time Pressure	Shuts down scrutiny	“I need this wire sent in the next 20 minutes.”
Secrecy	Prevents verification	“Don’t inform anyone in Finance just yet.”
Role Reversal	Makes victim feel in control (illusion)	“Can I trust you to handle this for me?”

📋 Real-World Examples

- **FACC (Austria, 2016)**: \$47 million stolen when attacker posed as CEO requesting a confidential acquisition payment
- **Pathé Films (France, 2018)**: Finance execs wired \$21M after “CEO” said it was for a top-secret Chinese acquisition
- **Toyota Boshoku (2019)**: \$37 million transferred due to fake CEO email

with urgent tone and secrecy clause

♥ Defense Strategies: Psychologically Informed

✓ For Employees

- **Train for psychological red flags:** secrecy, excessive flattery, unverified urgency
- **Empower refusal culture:** “Even the CEO can wait for protocol”
- **Scripted pushback phrases:**
 - “Can you please confirm this by phone?”
 - “Per policy, I need dual authorization before proceeding.”

✓ For Organizations

- **Role-specific simulations:** Target finance, HR, and executive assistants
 - **Escalation pathways:** Clear procedures for urgent or unusual requests
 - **CEO impersonation alerts:** Systems that flag spoofed exec messages
 - **Publicly reinforce caution:** Executives should regularly remind staff not to bypass procedures—**even for them**
-

□ Key Takeaways

- CEO fraud thrives on **status, obedience, and fear**
- Attackers know how to **sound like leaders and exploit team dynamics**
- Defense isn’t just technical—it’s **psychological readiness and empowered resistance**

Business Email Compromise (BEC)

3.1.4 Invoice Scam Forensic Signatures

“If it looks almost real, it’s already dangerous.”

Definition: Invoice Scams in BEC

Invoice scams are a form of **financial fraud** where attackers manipulate or fabricate **invoices** from trusted vendors, contractors, or internal departments to trick targets into sending payments to fraudulent bank accounts.

“It’s not just about spoofed emails. The invoice itself is the trap.”

Forensic Signatures of Invoice Fraud

Below are key indicators (technical, stylistic, and behavioral) that can be used to **identify forged, manipulated, or tampered invoices** in BEC scams.

1. Metadata Red Flags

Signature	Description
Recently created document	Timestamps show invoice was generated minutes before email was sent
Different software version	Invoice created in older/different version than usual (e.g., Word 2010 vs. Word 365)
Missing revision history	No edit metadata for reused templates (suggests forgery)
Metadata mismatch	Author field does not match vendor employee name

Forensic tools like ExifTool, DocuChecker, or PDF metadata readers can reveal hidden anomalies.

2. Linguistic & Formatting Tells

Red Flag	Description
Grammar inconsistencies	Subtle differences in tone, tense, or punctuation
Inconsistent currency formats	“\$5,000.00” vs. “5000 USD” used irregularly
Decimal separator differences	“1.000,00” vs. “1,000.00” (regional mismatch)
Typos in invoice numbers	Skipped/inverted sequences (e.g., INV-1009 → INV-1090)

These are often seen when scammers forge documents using templates they don’t fully understand.

3. Visual Anomalies

Clue	Why It Matters
Misaligned logos or text	Poor formatting in forged documents
Low-resolution company logo	Indicates logo was copied from web or email signature
Different font weights/sizes	Mixed formatting in headers, totals, or contact sections
Embedded (not linked) signatures	Often attackers insert static images of signatures rather than using dynamic digital ones

4. Banking & Payment Clues

Element	Fraud Indicator
New or unrecognized bank	Bank not used by vendor in past invoices
Urgent bank detail change	“Use this new account due to audit/system upgrade”
Different country code or SWIFT/BIC format	International transfer to unknown jurisdiction
Mismatch in remittance address vs. past invoices	Subtle attempt to bypass human pattern recognition

Always cross-check against **previous legitimate invoices**.

5. Behavioral Patterns in Email Context

Signal	Possible Sign of Fraud
Slight change in email address	e.g., @vendor . co instead of @vendor . com
Change in payment instructions timing	“Please pay this invoice today” (on an unusual day of week or outside normal cycle)
No CC to known vendor contact	Breaks normal communication pattern

These social engineering signals often accompany forged invoices to **pressure fast processing**.

□ Why They Work

- **Familiarity bias:** Targets recognize the vendor name/logo
- **Routine automation:** Accounting staff process dozens of similar invoices—small changes go unnoticed
- **Trust layering:** Email appears real → invoice appears real → action taken quickly

♥ Detection and Defense Tactics

✓ Technical

- Use **file metadata scanners** on attachments
- Deploy **email anomaly detection** for BEC patterns
- Implement **document hash-checking** for high-value invoices

✓ Procedural

- **Multi-factor invoice approval** for vendor payments
- Require **call-back verification** for any change in bank details
- Keep a **vendor verification register** with approved account numbers and formats
- Train AP staff to recognize **forensic invoice red flags**

□ Key Takeaways

- Forged invoices often look **98% legitimate**—but that 2% hides millions in losses
- Forensic markers lie in **document metadata, formatting quirks, and context shifts**
- Protecting against invoice scams requires a **combination of technical checks and skeptical human review**

Evasion Techniques

3.2.1 Homoglyph Domain Algorithms (e.g., “AppIe.com”)

“If you can’t see it, you’ll believe it.”

▣ Definition: Homoglyph Domains

Homoglyph domains use characters that **look visually identical or similar** to legitimate ones but are actually different Unicode or Latin characters. These domains are used in phishing, impersonation, and Business Email Compromise (BEC) attacks to evade detection and trick human perception.

Example: AppIe.com (with a **capital “I”**, not a lowercase “l”)
Looks like: Apple.com — but it’s not.

🔍 How Homoglyph Attacks Work

▣ Visual Deception Engineered

- Exploits **visual similarity** between characters:
 - Latin “a” vs. Cyrillic “a”
 - Uppercase “I” vs. lowercase “l”
 - “rn” (r + n) vs. “m”

Legitimate	Homoglyph	Difference Hidden
paypal.com	paypal.com	Cyrillic “p”, “a”
apple.com	appIe.com	Uppercase “I”
microsoft.com	microsoft.com	Cyrillic “o”

⚙️ Algorithmic Generation of Homoglyph Domains

▣ What Attackers Use:

- **Homoglyph generators:** Tools that produce thousands of lookalike domains
- **Punycode encoding** (xn- - prefix): Allows Unicode to appear as ASCII in domain registrations
- **Automated domain spoofing kits:** Identify popular brands, scan for

available lookalikes, and register them

Example:

xn--google-qta.com → **Looks like** google.com

❑ Common Use Cases in Social Engineering

1. Phishing Sites

- Fake login portals that mimic Google, Microsoft, PayPal, etc.
- Harvest credentials through:
 - Email links
 - QR codes
 - SMS (smishing)

2. Email Spoofing in BEC

- billing@microsoft-support.com sends realistic payment instructions
- Victim doesn't notice subtle character change in sender domain

3. Ad Fraud & SEO Spoofing

- Lookalike domains used in:
 - Malvertising campaigns
 - Google Ads targeting typos
 - Affiliate theft or scam promotions

❑ Detection Techniques

✓ Human-Level Defense (Awareness-Based)

- Train users to **hover over links**
- Read domains **character-by-character**
- Use **browser warning features** for punycode detection

✓ Technical Detection

Technique	Description
Levenshtein distance scanning	Detects domain names similar to trusted ones
Punycode flagging tools	Detects Unicode domain tricks (e.g., xn--)
Homoglyph lookup services	Tools like <u>DNSTwist</u> simulate attacks

SSL fingerprinting	Identify phishing SSL certificates or patterns
Email security gateways	Can flag domain mismatch using DMARC/DKIM/SPF

❑ Real-World Examples

- **2020 Google Docs Phishing:** Users tricked into visiting `googIe.docs.com`—a domain registered with a capital “i” instead of an “l”
 - **“Apple ID Locked” scam:** Fake domain `appIeid-verify.com` led to credential theft and payment fraud
 - **Office 365 Spoofing:** Attackers sent fake invoice links from `oFFice365billing.com` (with zero instead of “O”)
-

❑ Why It Works

- Relies on **human pattern-matching errors**
 - Bypasses many **email filters and blacklists**
 - Trust built on brand recognition and speed of reading
-

♥ Defense Strategies

✓ Technical

- Enforce **Domain Name Allowlisting**
- Use **homoglyph-aware browsers or plug-ins**
- Implement **email domain authentication** (DMARC, DKIM, SPF)
- Use **AI-based URL scanning tools** in secure email gateways

✓ Procedural

- Train staff to **inspect domains with skepticism**, especially in financial transactions
 - **Disallow** payments or sensitive actions from **new domains without manual verification**
 - Keep a **registry of trusted vendor domains** to verify against
-

❑ Key Takeaways

- Homoglyph domain attacks are **subtle, scalable, and devastating**
- Attackers don’t break through—they **blend in**
- Vigilance, technical safeguards, and **visual literacy** are key defenses

Evasion Techniques

3.2.2 Dynamic HTML Obfuscation

“The code says one thing. The screen shows another.”

Definition: Dynamic HTML Obfuscation

Dynamic HTML obfuscation is the use of **JavaScript**, **CSS tricks**, and **DOM manipulation** to disguise the **true intent or destination of web elements**, such as phishing links or fake login forms. The goal is to **evade detection by security scanners and fool human users**.

“The HTML file looks harmless—until it runs.”

How It Works: Layers of Deception

1. JavaScript-Based Link Manipulation

- **Obfuscated URLs** using JavaScript string assembly:

```
jsCopyEditvar part1 = "https://secure-";  
var part2 = "login";  
var part3 = ".com";  
document.write(part1 + part2 + part3);
```

- Final rendered link: `https://secure-login.com` (malicious site)
 - Static scanners miss this due to **delayed DOM rendering**
-

2. Hidden Input Fields & Overlays

- Fake login fields appear identical to real ones but:
 - Use `display:none` or z-index layering to **mask data exfiltration**
 - May route entered credentials to **attacker-controlled endpoints**

The **real-looking form** is just a styled decoy. The data goes elsewhere.

3. CSS Misdirection

- CSS can **mask real links** behind text:

```
htmlCopyEdit<a href="http://malicious.com" style="color:white;">https://apple.com</a>
```

- Or swap visible vs. clickable content via:
 - `text-indent`
 - `visibility: hidden`
 - Negative margin-top tricks

❑ 4. On-the-Fly HTML Injection

- Attackers inject malicious code **only after user interaction**:
 - Click triggers hidden JavaScript loader
 - Phishing content dynamically generated from a benign-looking stub

“Nothing seems wrong—until you click.”

❑ 5. Time-Delayed Rendering

- Malicious content appears **after a set delay** using:

```
jsCopyEditsetTimeout(function(){ showPhishForm(); }, 8000);
```

- Bypasses scanners that only scan content during initial page load

✂ Why Attackers Use Dynamic Obfuscation

Objective	How It Helps
Evade static analysis	Code appears benign to automated filters
Defeat sandboxing tools	Payload loads only under real-user conditions
Bypass blacklists	Final phishing domain not visible in source code
Confuse human analysts	Complex, split, or encoded scripts take longer to analyze

❑ Real-World Use Cases

- **HTML Phishing Attachments:**
 - Sent via email with subject like “Secure Document View”
 - Opens a local `.html` file that dynamically loads credential fields
- **Dynamic Login Spoofs:**
 - Fake Microsoft or Google login pages rendered via obfuscated inline scripts

- **Malvertising:**
 - Click redirects hidden in dynamic ad creatives that load **only in specific geolocations**
-

□ Why It Works

- **Security tools scan static HTML**—not runtime behavior
 - Users trust clean-looking interfaces and may not view source code
 - Attackers exploit the **gap between code visibility and browser behavior**
-

♥ Detection and Defense Techniques

✓ For Analysts & Tools

Technique	Benefit
JavaScript deobfuscation tools	Reveal hidden strings, encoded URLs
Sandbox + delayed execution	Detect time-based or interaction-based payloads
DOM snapshot analysis	Compare initial and final rendered states
Behavioral phishing scanners	Look at user interaction sequences, not just content

✓ For End Users

- Warn users against **opening .html attachments** from email
 - Train to **hover-check URLs**, but also watch for **delayed redirects**
 - Use **browser extensions** that highlight **DOM changes or hidden scripts**
-

□ Key Takeaways

- Dynamic HTML obfuscation is **code-based deception** engineered to evade both humans and machines
- The attack **lives in runtime**, not in the source file
- The solution lies in **runtime behavior detection** and **layered user awareness**

Evasion Techniques

3.2.3 Attachment Sandbox-Breaching Methods

“If the sandbox is watching, wait until it blinks.”

Definition: Sandbox Breach Techniques

Modern email gateways and antivirus tools often **detonate attachments in a sandbox**—a controlled, virtual environment designed to detect malicious behavior. Sandbox-breaching methods are **evasion techniques** attackers use to **bypass or delay detection**, ensuring the payload activates **only on a real victim’s machine**.

“To beat the sandbox, the malware must play dead—or act human.”

Common Sandbox Evasion Methods

1. Environment Awareness

Malware checks if it’s inside a **virtual machine (VM)** or sandbox.

Check Type	Example Behavior
Process check	Detects tools like vboxservice.exe, vmtoolsd.exe
Hardware fingerprinting	Low CPU/RAM → “Not a real system”
Mouse movement timing	No mouse movement or keyboard → “Sandbox detected”
Unusual usernames/paths	C:\Users\Sandbox, JohnDoe-VM → abort execution

If suspicious, malware **stays dormant** or exits without triggering red flags.

2. Time-Delayed Execution

The payload uses **sleep timers** or countdowns to **outwait the sandbox**.

Technique	Example
Sleep(600000) (10	

minutes)	Sandboxes typically run 1–2 minute sessions
Timebomb logic	Only runs after certain date/time (e.g., > July 16, 2025)
User idle check	Waits until the user has been inactive for X seconds

A sandbox sees nothing because it doesn't wait long enough.

3. User Interaction Requirements

Payload stays hidden unless there is **human behavior**.

Trigger Type	How It Works
Enable content	Office files with malicious macros activate only when user clicks "Enable Macros"
Click-to-decrypt	PDF or ZIP file asks for password that only the attacker sent to the victim
Form interaction	Malware triggers after typing in a field or pressing "Submit"

Sandboxes don't simulate complex user actions—so the malware stays quiet.

4. Payload Fragmentation

The malicious code is split into **multiple parts**, each harmless alone.

Fragment Strategy	What It Does
Staged downloads	Main payload fetched from C2 (Command & Control) server only if passed checks
Embedded file chains	ZIP inside DOCX inside another ZIP—only executed step-by-step
Macro-based triggers	Uses Excel 4.0 macros, PowerShell loaders, or custom DLL calls

Sandboxes may only analyze **top-layer content**, missing hidden depths.

5. File Format Tricks

Files appear safe or broken—but act maliciously only after execution.

Format Abuse	Example
Polyglot files	One file valid in multiple formats (e.g., PDF+ZIP)
Corrupted headers	Prevents analysis tools from parsing the file
Encrypted attachments	Require password entry (sandbox can't decrypt)

❑ Real-World Payload Vectors

- **Malicious Office Docs:** .docm, .xlsm with macro-based droppers
- **Embedded Scripts:** JavaScript inside .html or .hta attachments
- **PDF Triggers:** JavaScript-based exploits in PDFs disguised as invoices
- **Password-Protected ZIPs:** Contain EXE payloads or backdoors hidden from scanners

❑ Why It Works

Reason	Description
Sandboxes are time-limited	Malware delays execution beyond scan window
Sandboxes are resource-limited	Malware uses environment checks to abort in emulated spaces
Sandboxes are userless	Malware waits for interaction that never happens

♥ Detection & Defense Strategies

✓ Technical Controls

- **Cloud-based sandboxing with extended runtime**
- Use **behavioral analysis**, not just static signatures
- Scan **embedded scripts, links, and macro chains**
- Block **high-risk attachment types**: .exe, .scr, .hta, .js, .vbs, .iso, .img

✓ Organizational Policy

- Train users to **never enable macros** unless verified
- Restrict users from opening **HTML attachments** from unknown senders
- Implement **content disarm and reconstruction (CDR)** for incoming docs
- Use **zero-trust file access** and isolate opened files in containers

□ Key Takeaways

- Sandbox-breaching attachments are **patient, intelligent, and evasive**
- They rely on **time, human behavior, and multi-stage concealment**
- Defending requires **layered detection**, extended monitoring, and **user restraint**

QR Phishing (Quishing)

4.1.1 Physical-Digital Bridge Exploits (Malicious Posters)

“Scan me—and surrender your credentials.”

□ Definition: Quishing

Quishing is a phishing attack that uses **QR codes** to direct users to **malicious websites**, login pages, or malware downloads. It bypasses traditional email link filters by delivering the **attack vector via image**, often embedded in **posters, flyers, emails, or packaging**.

“It’s not in your inbox anymore—it’s on the wall.”

□ The Physical-Digital Bridge: Malicious Posters

□ What Are They?

Posters, handouts, stickers, or even public screens placed in physical locations—such as:

- Cafés
- Airports
- Bulletin boards
- Conference booths
- Office printers

They display **fake QR codes** disguised as:

- Wi-Fi login prompts
- Event registrations
- Survey forms
- Coupon claims
- COVID-19 check-ins
- Tech support stickers

Example: “Scan to win AirPods!” or “Parking validation—scan here.”

✂ How the Attack Works

□ 1. Setup & Deployment

- Attacker prints a **professional-looking poster** or sticker
- QR code leads to a **phishing domain** or malware-hosting site
- Often placed over real signage, Wi-Fi boards, or public service displays

❑ 2. Lure & Engagement

- QR code promises something urgent or valuable:
 - “Secure campus Wi-Fi access”
 - “Check vaccine status”
 - “Employee feedback survey – win rewards!”

❑ 3. Execution Upon Scan

- QR directs mobile browser to:
 - **Credential-harvesting** site (Google, Office365, banking)
 - **Malware APK** (on Android)
 - **Fake payment gateway** for wallet drain
 - **Session hijackers** via auto-login traps

❑ 4. Post-Scan Exploitation

- Attacker may harvest:
 - Login credentials
 - 2FA tokens (with real-time man-in-the-middle forwarding)
 - Credit card/payment info
 - Device fingerprint data

❑ Why Quishing via Posters Works

Human Factor	Exploited Behavior
Trust in the environment	Assumes posters in cafés, libraries, or offices are legit
Visual authority	Logos & branding add credibility (e.g., fake Apple or Google)
Low alertness on mobile	Users rarely inspect QR-linked URLs closely on phones
URL cloaking	QR code hides the actual destination until clicked

Unlike emails, **QR codes bypass link previews and security filtering.**

▮ Real-World Examples

- **Germany (2023):** QR codes on parking meters redirected users to a

phishing page imitating a payment portal

- **USA (2022):** COVID-19 check-in signs in public libraries were tampered with, redirecting to credential-harvesting pages
 - **UK universities:** Students scanned fake “Wi-Fi QR codes” posted in dorm halls, leading to Office365 login theft
-

♥ Detection & Defense Strategies

✓ For Organizations

- **Physically secure signage:** Laminate posters, check for overlays or replacements
- **Rotate QR codes periodically** with unique identifiers
- **Log all QR-based scans** using dynamic redirection platforms
- **Train staff to verify QR signage source and placement**

✓ For Users

- **Preview QR destinations** before clicking (some camera apps or browsers show URLs)
 - **Use trusted QR scanner apps** with built-in phishing detection
 - **Avoid scanning unknown QR codes in public spaces**
 - **Check for HTTPS and proper domain spelling**
 - **Never enter credentials or payments on sites reached by QR unless verified**
-

□ Advanced Quishing Techniques (Emerging)

- **Geofenced QR attacks:** Payloads only activate in certain locations
 - **Device fingerprinting via QR:** Gathers sensor or OS data during scan
 - **Dynamic redirection:** Malicious sites change after time or based on device
-

□ Key Takeaways

- Quishing attacks blend **physical trust with digital exploitation**
- Malicious posters weaponize QR codes in **non-technical environments**
- Defense requires a combination of **user skepticism, physical security, and mobile browser awareness**

QR Phishing (Quishing)

4.1.2 QR Code Generation Toolkits

“You don’t need to code malware—just generate a QR code to it.”

□ Definition: QR Code Toolkits in Phishing

QR Code Generation Toolkits are tools or services used by attackers to create **weaponized QR codes** that direct victims to malicious URLs, phishing pages, or downloadable malware. These toolkits often offer **automation, obfuscation, and analytics**, making quishing campaigns scalable and evasive.

“With a few clicks, your phishing link becomes a clean-looking QR code—even branded.”

⚙️ How Attackers Use QR Code Toolkits

□ Step 1: Target Page or Payload Setup

- Create phishing page (e.g., fake login portal)
- Or host malicious file (e.g., APK, PDF, PowerShell loader)

□ Step 2: QR Code Generation

- Use a **QR code generator toolkit** to encode the URL
- Customize:
 - **Logo insertion** (e.g., fake Microsoft or bank logo)
 - **Color, background, call-to-action (CTA)**
 - **Shortened or cloaked URL** (to hide real destination)

□ Step 3: Print or Embed

- Insert generated QR codes into:
 - Email attachments (e.g., PDF “Invoices” or “Secure Docs”)
 - Physical flyers, stickers, or posters
 - Social media graphics or event slides

□ Step 4: Monitor Interactions

- Some advanced toolkits include:
 - IP logging

- Device fingerprinting
- Real-time click analytics
- Geolocation data from scan events

✂ Popular QR Code Generation Tools Used in Legit + Malicious Ways

Toolkit / Platform	Capabilities	Quishing Risk
qr-code-generator[.]com	Custom QR, logo embedding, analytics	★★★★☆
GoQR.me	Simple generator, used in malicious PDFs	★★★☆☆
QRTiger	Dynamic QR codes, password-protected, redirectable	★★★★★
QRCode Monkey	Highly customizable, export as SVG/PNG for print use	★★★★☆
Malicious GitHub Toolkits	QR autogeneration with embedded C2 links, phishing URLs	★★★★★

Tools are **legitimate** by design but **exploitable** in phishing kits.

📦 Notable Malicious Features in Attack Toolkits

Feature	Malicious Use Case
Dynamic Redirection	QR destination changes after initial scan (evasion)
Analytics Dashboards	Attacker sees who scanned, where, and on what device
URL Cloaking + Shorteners	qr.page.link/abc123 masks true malicious domain
Steganography (rare)	Malicious payload hidden in the QR image data (research phase)

🔍 Why Attackers Prefer QR Toolkits

Advantage	Description
Bypass email filters	QR images not scanned like URLs in text
Device targeting	QR codes mainly scanned by mobile phones

User trust	QR seen as utility—not a threat
Scalable + printable	Can mass-print malicious posters, invoices, surveys

📄 Observed Use in the Wild

- **Email campaigns:** Attachments with QR codes linking to Microsoft 365 login clones
 - **Malvertising:** Social media or influencer posts with “Giveaway QR Codes”
 - **Fake event posters:** QR leads to “attendee check-in” but harvests credentials
 - **Sticker campaigns:** On ATMs, parking meters, and public chargers
-

🛡️ Defense Recommendations

✓ Technical Controls

- **QR scanners with reputation checks**
- Use **AI email filtering** that scans QR code images for embedded links
- **Disallow QR code attachments** in enterprise email unless whitelisted
- **Analyze PDF attachments** for embedded base64 QR images

✓ User Training

- Teach staff to:
 - **Preview URLs after scanning**
 - **Avoid QR-based login pages**
 - **Report suspicious QR posters or stickers**
-

📄 Future Threats

- **AI-generated phishing pages + dynamic QR codes**
 - **QR-malware hybrids:** Combining QR tricks with zero-click exploits
 - **QR steganography:** Hidden instructions in visual layers of the QR code
-

📄 Key Takeaways

- QR toolkits make phishing **easy, fast, and scalable**
- The **tool isn’t malicious—but the link it hides is**
- Defenses must extend beyond the inbox to **image-based threat vectors**

Collaboration Platform Threats

4.2.1 Slack/Microsoft Teams Malware Delivery

“Where we work is where they strike.”

□ Definition: Threats via Collaboration Platforms

Slack, Microsoft Teams, Discord, and similar platforms have become **new attack surfaces** for cybercriminals. These platforms are used to **deliver malware, harvest credentials, and conduct internal reconnaissance**, especially as organizations shift from email to real-time messaging.

“If attackers can’t get through your inbox, they’ll drop a file in your DMs.”

□ How Slack/Teams Are Exploited

□ 1. Malware File Drops

Attackers share:

- **Malicious Office files** (.docm, .xlsb)
- **Scripts** (.vbs, .js, .ps1)
- **LNK shortcuts** to weaponized payloads
- **Compressed malware** inside .zip or .rar files

Example: A Teams message says, “Here’s the updated project plan,” but the file installs an info-stealer.

□ 2. Link-Based Attacks

- **Obfuscated phishing links** disguised as company portals
- Use of **URL shorteners** (e.g., bit.ly, tinyurl) to bypass previews
- **OAuth token stealers** in fake “login” pages

Users trust internal chats more than email—so **scrutiny drops**.

□ 3. Internal Account Takeover (ATO)

- If one user is compromised:
 - Malware or phishing links are sent **from a trusted teammate**
 - Attack spreads **laterally inside the org**

- Attacker gains **visibility into team channels, chats, files, and auth tokens**

4. Malicious App Integrations

- Attacker convinces a user to **authorize a third-party app**
- App requests excessive scopes:
 - `files.read.all`, `chat.readwrite`, `user.read`, etc.
- Once approved, attacker gains **persistent access** even if password changes

These OAuth-style threats bypass passwords entirely.

Why Collaboration Tools Are Effective Attack Vectors

Advantage for Attackers	Reason
User trust	Messages seem to come from coworkers
Fewer filters	Fewer scanning rules than email
Always logged in	Persistent sessions on browser/mobile apps
High engagement	Users click on links or files in chat more rapidly than in email
Third-party integrations	Users accept app permissions without scrutiny

Real-World Examples

- **Slack:**
Attackers upload `.js` files pretending to be code snippets or scripts. One campaign targeted developers, dropping **clipboard-monitoring malware** via Slack file shares.
- **Microsoft Teams (2023):**
Microsoft reported **APT29/Russian group “Midnight Blizzard”** delivering malicious `.zip` files via Teams chats to internal users. They impersonated IT admins and used **token theft** to bypass MFA.
- **Discord (2021–Present):**
Used as a **C2 channel and payload host** for ransomware droppers and credential stealers embedded in game modding communities.

♥ Detection and Defense Techniques

✓ Technical Controls

Control	Description
Limit file types	Block .exe, .js, .vbs, .lnk, etc. from being shared
Scan shared files	Integrate DLP or antivirus at file-upload points
Restrict app permissions	Review OAuth scopes for third-party integrations
Monitor API activity	Detect mass downloads, unusual chats, or app installs
Enable link previews	Detect obfuscated URLs before click-through

✓ Organizational Defenses

- **Train users to:**
 - Treat links/files in Teams/Slack with **email-level caution**
 - Never approve third-party app permissions unless vetted by IT
- **Enforce role-based access control (RBAC)** in collaborative channels
- Conduct **lateral movement drills** simulating ATO within messaging apps

□ Emerging Threats

- **AI-generated chat impersonation**
 - Bots that mimic writing style of real coworkers
- **Token-based session hijacking**
 - Stealing Teams OAuth tokens to **persist inside org chat**
- **Voice/video phish inside Teams meetings**
 - Fake “screen share” attacks using pre-recorded overlays

□ Key Takeaways

- Collaboration platforms are **trusted but underprotected attack vectors**
- Malware, phishing, and account hijacking happen **inside the firewall**
- Defense requires **technical controls, user training, and token governance**

Collaboration Platform Threats

4.2.2 Fake Meeting Links (Zoom/WebEx)

“You’re not joining a meeting—you’re joining a trap.”

□ Definition: Fake Meeting Link Attacks

Fake meeting link attacks involve **social engineering tactics** where attackers craft and send **phishing links disguised as invites** to legitimate platforms like Zoom, WebEx, Microsoft Teams, or Google Meet. These links lead to **credential-harvesting portals, malware drops, or MFA token theft**.

“Your 2 PM meeting is actually a 2-second compromise.”

🔍 How the Attack Works

□ 1. The Lure: Contextual Meeting Invite

Attackers send messages via:

- **Email** (“Join urgent Zoom call with HR”)
- **Calendar invites**
- **Slack/Teams messages**
- **SMS or WhatsApp (smishing)**

Subject: “Security Incident Briefing – Join Now”
Link: zoom-login-support[.]com/verify

□ 2. The Trap: Lookalike Login Page

Victim clicks link → lands on **spoofed meeting login portal** mimicking:

- Zoom, WebEx, or Teams
- Google/Office 365 login page (SSO trap)
- MFA prompt (real-time token harvesting via man-in-the-middle)

□ 3. Post-Click Exploitation

- **Credentials harvested**
- Or browser downloads malicious file: Zoom_Installer_Update.pdf.exe
- Or attacker sets up a **reverse proxy** (e.g., Evilginx) to steal

cookies/tokens

❑ Why It Works

Psychological Trigger	Exploited Assumption
Urgency	“Join right now” creates pressure to act fast
Familiarity	Zoom/Teams/WebEx branding makes link feel safe
Routine behavior	Users often click meeting links without verifying
Mobile targeting	Phone users can’t hover to preview URLs easily

❑ Attack Variants

❑ Credential Harvesting

Fake Zoom/WebEx login pages capture usernames and passwords, then forward victims to real meetings or error pages to avoid suspicion.

❑ Malware Delivery

File downloads disguised as:

- “Zoom Plugin Update”
- “WebEx Recording Viewer”
- “Teams Meeting Patch”

❑ Reverse Proxy Phishing

Attackers use tools like **Evilginx2** or **Modlishka** to intercept:

- Live credentials
- Session cookies
- MFA tokens

Once token is stolen, attackers **bypass MFA** and log in directly.

❑ Real-World Examples

- **Zoom (2020-2023):**
Multiple phishing campaigns used `zoom-verify[.]net`, `zoomvideoconferencelogin[.]com` to steal Zoom/Office365 credentials during remote work boom.

- **WebEx (2021):**
Malicious ICS calendar files sent with spoofed sender addresses (“admin@webexevents[.]com”) led users to malware download pages.
 - **Hybrid Threats:**
In some cases, attackers invited victims to **real meetings**, then shared **malicious links in the chat** or ran screen-share scams.
-

♥ Detection & Defense Strategies

✓ Technical Measures

Defense	Description
Email URL scanning	Detect lookalike domains and Punycode (e.g., zo0m.com)
Safe Link rewriting	Microsoft Defender / Proofpoint rewrites links in real-time
Anti-phishing gateways	Catch suspicious meeting invites, ICS files, calendar traps
Reverse proxy detection	Detect token theft via impossible travel or device mismatch

✓ User Training

- Don't enter credentials into **meeting links**
 - Always **check domain spelling**
 - Beware of urgent “Join Now” messages from unknown senders
 - On mobile, **long-press links** to preview before clicking
-

□ Red Flags for Users

- URL is **not from official domain**:
 - ✓ zoom.us → ✓ OK
 - ✗ zoom-security-login[.]xyz → □ Phish
 - Login request appears **before** seeing meeting details
 - File download offered **instead of** direct join
 - Sender email or display name seems **off-brand**
-

□ Key Takeaways

- Fake meeting links weaponize our **trust in routine workplace platforms**
- They combine **brand impersonation**, urgency, and real-looking portals

- Defense requires **technical filters** + **user vigilance**, especially on mobile

DMARC Deep Dive

5.1.1 Policy Enforcement Hierarchies (p=none → quarantine → reject)

“DMARC is your domain’s security guard—but only if you give it authority.”

□ What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an **email authentication protocol** that uses **SPF** and **DKIM** to prevent domain spoofing. It enables domain owners to tell receivers **how to handle unauthenticated emails** claiming to be from their domain.

□ “DMARC doesn’t just detect spoofed email—it decides what happens to it.”

□ Policy Enforcement Hierarchy: How DMARC Evolves

DMARC uses a **policy tag (p)** to instruct receiving mail servers on how to treat email that fails DMARC checks. There are **three policy levels** in increasing order of enforcement:

✓ 1. p=none (Monitor Only)

□ “Watch, but don’t act.”

- The **starting point** for DMARC adoption
- No enforcement; emails that fail SPF/DKIM **still get delivered**
- Used to **gather data** on who is sending email “as you”

□ Use Case:

- Low risk, testing phase
- Ideal for identifying **unauthorized senders**, configuration gaps

□ Sample DNS Record:

```
iniCopyEditv=DMARC1; p=none; rua=mailto:dmarc-reports@example.com;
```

□ Note:

If you leave your domain at p=none forever, **attackers can spoof you with zero consequence.**

⚠ **2. p=quarantine (Warn & Filter)**

▮ “If it fails, don’t trust it—put it in spam.”

- Unauthenticated emails are **flagged and diverted** (e.g., junk folder)
- Signals to recipients and filters that this email is **suspicious**
- Enables “soft enforcement” while monitoring impact

▮ **Use Case:**

- Midpoint in rollout
- Useful when you’re **not 100% confident** that all legitimate senders are correctly authenticated

▮ **Sample DNS Record:**

```
iniCopyEditv=DMARC1; p=quarantine; rua=mailto:dmarc-reports@example.com;
```

🚫 **3. p=reject (Full Enforcement)**

▮ “If it fails, drop it completely.”

- Unauthenticated emails are **rejected at the server**
- Provides **maximum protection** against spoofing and phishing
- Only use when all legitimate sources are **SPF and/or DKIM aligned**

▮ **Use Case:**

- Mature, hardened domain
- Government, banking, and public-facing domains
- Strong brand protection via **BIMI** (Brand Indicators for Message Identification) often requires p=reject

▮ **Sample DNS Record:**

```
iniCopyEditv=DMARC1; p=reject; rua=mailto:dmarc-reports@example.com;
```

📈 **Why a Hierarchy?**

Policy Level	Purpose	Risk Level	Action on Failures
Visibility & data			

p=none	gathering	📄 Low	No action — monitor only
p=quarantine	Soft protection	⚠ Medium	Send to spam/junk
p=reject	Full protection	🚫 High	Block delivery entirely

Smart DMARC rollout follows this **progressive path** to avoid breaking legitimate mail flows.

📋 Implementation Strategy: Phased Rollout

1. **Start with** p=none
 - Enable **reporting** (rua)
 - Analyze sources, fix misconfigured SPF/DKIM
2. **Move to** p=quarantine
 - Catch more spoof attempts
 - Monitor if any **legitimate emails are quarantined**
3. **Enforce** p=reject
 - Only when confident that **all sending systems are aligned**

🔔 Supporting Tags You Should Know

Tag	Purpose
rua	Aggregate report URI (daily reports)
ruf	Forensic report URI (per-message, optional)
pct	Percent of messages to apply policy to
sp	Subdomain policy (separate from root)
aspf/adkim	Alignment mode (strict vs relaxed)

♥ Why DMARC Hierarchy Matters

Threat Avoided	How DMARC Helps
Spoofed emails	Rejects or filters unauthenticated senders
Brand impersonation	Ensures only verified sources send as you
Phishing attacks	Blocks forged login pages, invoice scams
Inbox pollution	Improves deliverability by enforcing trust

□ Key Takeaways

- DMARC is only **as strong as the policy you set**
- $p=\text{none}$ → quarantine → reject is a **stepwise journey**, not a toggle
- Full enforcement ($p=\text{reject}$) provides **true anti-spoofing protection**

DMARC Deep Dive

5.1.2 Forensic Reporting Analysis Tools

“Your inbox is under attack—DMARC tells you when, where, and how.”

What Are DMARC Forensic Reports?

DMARC forensic reports (also known as **failure reports** or **ruf reports**) provide **real-time, message-level diagnostics** when an email fails DMARC checks. They include:

- The **original message headers**
- **Sending IP**
- **From domain**
- SPF/DKIM alignment results
- Sometimes even a **snippet of the email content**

These reports are sent to the address specified in the `ruf=` tag in your DMARC DNS record.

How They Differ From Aggregate Reports (rua)

Feature	Aggregate Report (rua)	Forensic Report (ruf)
Frequency	Daily summary	Real-time (per message)
Detail Level	High-level stats	Full technical diagnostics
Contains email content?	✗ No	✓ Sometimes includes headers/body
Ideal use case	Trends & traffic analysis	Deep-dive into spoof attempts
Format	XML	Encrypted/Plaintext EML/XML

What’s in a Forensic Report?

Typical forensic report fields:

- **Envelope sender**
- **Header “From”**
- **SPF & DKIM results**

- **IP address of sender**
- **Auth failure reason**
- Optional: **Original email headers or content** (redacted by some providers)

❑ How to Receive Them

✓ DMARC DNS Record Example:

```
txtCopyEditv=DMARC1; p=quarantine; rua=mailto:dmARC-agg@example.com;
ruf=mailto:forensics@example.com; fo=1;
```

❑ fo=1 means:

- Send report if **either SPF or DKIM fails**
- Use secure, monitored email addresses—**forensic reports may contain sensitive data.**

❑ Challenges in Handling Forensic Reports

- Often **sent in non-standard formats** (multipart, raw EML)
- Not all providers support ruf reports (e.g., Google doesn't send them)
- High **volume of data**—can be overwhelming for large domains
- Reports may include **partial or redacted content** for privacy

❑ Forensic Report Analysis Tools (Top Options)

Tool / Platform	Features	Free?
Postmark's DMARC Digests	Parses both rua and ruf; user-friendly UI	✓
Dmarcian Forensic Viewer	Displays IP, reason, message trace with filters	✗
Agari DMARC Protection	Enterprise-grade dashboard with forensic correlation	✗
EasyDMARC	Aggregates forensic + threat mapping, flag-based visualization	✓ (limited)
OpenDMARC Forensic Parser	CLI tool for parsing raw reports (Linux CLI)	✓
Fraudmarc	Cloud-based forensic report visualizer with IP reputation data	✓

🔍 What to Look For in a Forensic Report

Indicator	Description
SPF=fail, DKIM=fail	Email not authenticated—likely spoofed
Unrecognized source IP	Sent from a non-authorized server
Bad “From” domain	Display name spoofing (e.g., CEO@realcompany.com)
Geographic anomalies	Sender IP from unexpected region
Repetition pattern	Mass spoofing attempt underway

♥ Best Practices for Using Forensic Reports

1. **Set up** `ruf=` **only on a secure, monitored address**
 2. **Encrypt reports** via `ruf=mailto:you@example.com!rsa:your_public_key`
 3. **Automate parsing** with tools to extract key indicators
 4. **Correlate with logs** (e.g., SIEM, mail gateway, SPF logs)
 5. **Use findings to harden SPF/DKIM policies** and block rogue senders
-

🔑 Key Takeaways

- Forensic reports offer **deep insight into spoofing and misconfigurations**
- Require **secure handling** due to potential content exposure
- Best used alongside **aggregate reports** for full DMARC intelligence
- Tools like **Dmarcian**, **EasyDMARC**, and **OpenDMARC** make parsing easier

DMARC Deep Dive

5.1.3 Subdomain Policy Inheritance Risks

“Your main domain may be locked down—but your subdomains might be wide open.”

❑ What Is DMARC Subdomain Policy Inheritance?

By default, when you set a DMARC policy (`p=quarantine` or `p=reject`) on your **primary domain**, that policy is automatically **inherited by all subdomains**—unless you explicitly override it using the `sp=` (subdomain policy) tag.

If no `sp=` tag is set, subdomains fall back to the parent domain’s policy—but this can lead to **inconsistent enforcement** or **accidental exposure**.

❑ Understanding Policy Inheritance

Tag	Scope	Description
<code>p=</code>	Primary domain only	Governs DMARC action for mail claiming to be from <code>example.com</code>
<code>sp=</code>	Subdomains only	Applies DMARC policy for subdomains like <code>mail.example.com</code> , <code>marketing.example.com</code>

! Subdomain Inheritance Risk Scenarios

❑ 1. Unused Subdomains with No Email Protections

Attackers register a subdomain like `secure.example.com` and use it for spoofing:

- No SPF/DKIM records for that subdomain
- No `sp=` override → may inherit `p=none`, or fallback inconsistently

❑ 2. Third-Party Services with Legitimate Subdomain Usage

- You delegate `mail.example.com` to an email service provider
- They send DMARC-failing messages if **SPF/DKIM isn’t aligned**
- If you haven’t enforced `sp=reject`, these messages **go through or hit spam**, not fully rejected

3. Shadow IT or Misconfigured Subdomain Apps

- Internal teams use form.example.com, campaigns.example.com for SaaS mailers
- These systems send **unauthenticated or misaligned** emails
- Without strict subdomain policies, this exposes the brand to **reputation damage**

🔑 Common Attack Vectors on Subdomains

Threat Type	Exploited Weakness
Subdomain spoofing	No DKIM/SPF on subdomain + no enforced sp=
Lookalike subdomain phishing	E.g., pay-secure.example.com sends fake invoices
Subdomain takeovers	Abandoned apps/services reused to host phishing content

🛡️ Best Practices for Subdomain Policy Enforcement

Practice	Why It Matters
✓ Set sp=reject	Prevents spoofing from <i>all subdomains</i>
✓ Lock down unused subdomains	Prevent wildcard spoofing or takeover
✓ Publish explicit SPF/DKIM	For all known subdomains that send email
✓ Monitor subdomain DMARC reports	Catch unauthorized usage before it becomes a breach
✓ Use strict alignment (aspf=s, adkim=s)	Prevent loose matches on subdomain headers

📄 DNS Record Example with Secure Subdomain Policy

txtCopyEditv=DMARC1; p=reject; sp=reject;
rua=mailto:dmarc@example.com;

- p=reject: Full protection on root domain
- sp=reject: Explicitly applies the same to **all subdomains**

□ How to Detect Subdomain Abuse

Use DMARC reports and tools to analyze:

- **Unknown sources** sending from *.example.com
- SPF/DKIM **failures from subdomains**
- Geo/IP anomalies or **unusual volume spikes**
- Misalignment between envelope and header From

□ Tools: Dmarcian, EasyDMARC, Postmark, or OpenDMARC (self-hosted)

□ Key Takeaways

- **Subdomain spoofing is a major blind spot** if sp= is not explicitly enforced
- Don't assume your root domain's DMARC policy **automatically secures everything**
- Always define sp=reject or sp=quarantine based on business needs
- Audit and monitor all subdomains—**especially those unused or legacy**

BIMI Implementation

5.2.1 Verified Mark Certificate (VMC) Requirements

“Let your logo build trust—only if you’ve earned it.”

♥ What Is BIMI?

BIMI (Brand Indicators for Message Identification) allows organizations to display their **official brand logo** next to authenticated emails in supported inboxes (like Gmail, Apple Mail, Yahoo, etc.).

But to display a logo, you must have:

- **Strong domain authentication (DMARC enforcement)**
- A **Verified Mark Certificate (VMC)** issued by a trusted Certificate Authority (CA)

BIMI turns your email into a **visual identity asset**, but only after you’ve proven you’re legitimate.

□ What Is a VMC?

A **Verified Mark Certificate** is a **digital certificate** that proves your organization legally owns its logo and domain. Issued by trusted providers (like Entrust or DigiCert), it’s **required** to display your logo in BIMI-enabled email clients.

□ VMC Requirements Checklist

Requirement	Description
✓ Trademarked Logo	Your logo must be registered with a recognized trademark office (e.g., USPTO, EUIPO)
✓ SVG Logo Format	Logo must be provided as a BIMI-compliant SVG Tiny 1.2 file
✓ DMARC at p=quarantine or p=reject	You must have full DMARC enforcement —no p=none
✓ VMC Issuer Validation	Your organization undergoes identity vetting (similar to EV SSL certs)
✓ Matching Domain Ownership	The domain shown in email must match the DMARC and VMC domain

✓ **Proper BIMI DNS Record** You must publish a valid DNS default._bimi TXT record pointing to the logo and VMC

□ Sample BIMI DNS Record

```
txtCopyEditdefault._bimi.example.com IN TXT "v=BIMI1;  
l=https://example.com/logo.svg; a=https://example.com/vmc.pem"
```

Field	Meaning
v=BIMI1	BIMI protocol version
l=	URL to your brand logo (SVG)
a=	URL to your VMC file (PEM format)

🔍 Who Issues VMCs?

CA Provider	Services Offered	Notes
Entrust	VMC + trademark verification	Widely used, fast turnaround
DigiCert	VMC with onboarding guidance	Strong presence in enterprise
Sectigo	VMC in partnership with logo consultants	Emerging support

Expect **manual validation**, similar to Extended Validation SSL certificates.

□ Why Is a VMC Important?

- **Trust at a glance:** Users see your verified logo next to your email
- **Phishing resistance:** Helps users identify legitimate brand emails
- **Reputation building:** Makes your brand stand out in crowded inboxes
- **BIMI requirement:** Most major inboxes (like Gmail) **require a VMC**

□ Common Pitfalls & Gotchas

Mistake	Consequence
✗ No trademark registration	Cannot obtain VMC at all
✗ Using non-compliant SVG format	BIMI will not display logo
✗ DMARC at p=none	Email won't qualify for BIMI, even

	with VMC
✗ Wrong logo hosting or HTTPS issues	BIMI record may be ignored

💡 Pro Tips

- ☐ Use a **legal entity name** that matches your domain registrant for VMC validation
 - 🔍 Use **BIMI testing tools** (like BIMI Inspector by Agari or Gmail BIMI Preview) to validate setup
 - ☐ Ensure your **VMC PEM file is hosted securely** on HTTPS and accessible publicly
 - ☐ Consider VMC/BIMI as part of your **email trust & brand strategy**, not just security
-

☐ Key Takeaways

- VMC is **mandatory** to use BIMI in Gmail and other major inboxes
- You must have a **DMARC policy of** quarantine **or** reject, and a **registered trademark logo**
- The process involves **CA-level identity validation** and proper DNS record setup
- BIMI + VMC boosts brand visibility while reinforcing **anti-phishing protections**

BIMI & Brand Protection

5.2.3 Logo Spoofing Countermeasures

“If they can copy your logo, they can borrow your trust.”

What Is Logo Spoofing?

Logo spoofing is a **visual phishing tactic** where attackers imitate or copy a brand’s logo to:

- Trick recipients into **trusting fraudulent emails**
- Lure users into **credential phishing, malware installs, or fraudulent transactions**
- Create **brand confusion** in both email and web environments

Often combined with domain lookalikes or compromised senders, spoofed logos **bypass technical filters** by exploiting human trust.

Common Use Cases of Logo Spoofing in Email

Attack Vector	Example
Phishing emails	Fake Office365 login page showing Microsoft logo
Business Email Compromise (BEC)	CEO impersonation email includes copied company letterhead/logo
Fake invoice scams	Vendor impersonator uses a lookalike logo to increase legitimacy
Credential harvesting	Login page shows your bank’s or company’s favicon/logo

Why It Works

Psychological Factor	Explanation
Visual trust bias	Users trust emails more if they “look right” visually
Low scrutiny	Logos trigger recognition, not analysis
Mobile UI constraints	On phones, users see the logo before the sender’s full domain

♥ Logo Spoofing Countermeasures

✓ 1. Implement BIMI with VMC

Strongest visual anti-spoofing control

- Use **Brand Indicators for Message Identification (BIMI)** with a **Verified Mark Certificate (VMC)**
- Ensures only **authenticated senders** can display your logo in inboxes (e.g., Gmail, Apple Mail)
- Requires:
 - p=reject or p=quarantine in DMARC
 - Trademarked logo
 - VMC issued by CA (Entrust, DigiCert)

✓ Prevents spoofed logos from displaying in supported clients

✓ 2. DMARC, SPF, DKIM Enforcement

Stops unauthorized senders—even with your logo in body

- **DMARC with p=reject** prevents spoofed “From” domains
- **SPF** validates envelope sender (MAIL FROM)
- **DKIM** ensures message wasn’t modified in transit

✓ Even if attackers use your logo, their spoofed domain gets blocked

✓ 3. Brand Monitoring Services

Detect your logo in phishing campaigns

- Use tools like:
 - **ZeroFox**
 - **Bolster**
 - **BrandShield**
 - **PhishLabs**

They scan:

- Phishing kits using your logo
- Web pages impersonating your brand
- Social media or dark web usage

✓ Gives early warning + takedown options

✓ 4. Image Recognition in Email Security

▮ Detects spoofed logos inside email body

Some advanced Secure Email Gateways (SEGs) and email threat detection engines:

- Use **OCR (optical character recognition)** and **visual similarity scoring**
- Flag emails where the **logo doesn't match sender domain**

Tools:

- **Microsoft Defender for Office 365**
- **Proofpoint TAP**
- **Mimecast Targeted Threat Protection**

✓ *Blocks emails with mismatched logos and spoofed content*

✓ 5. User Training on Visual Deception

▮ Human firewall against logo-driven scams

Train users to:

- **Verify sender domain**, not just logo or design
- Understand that **anyone can copy a logo**
- Use **hover checks** on URLs and file names
- Be skeptical of emails that mix urgency + brand elements

✓ *Reduces risk from brand impersonation, especially in BEC*

✓ 6. Trademark & Legal Enforcement

▮ Take action against repeat spoofers

- Register your logo with:
 - **USPTO, EUIPO**, etc.
- Send **takedown notices** to hosting providers
- Report abuse to:
 - **Google Safe Browsing**
 - **Microsoft SmartScreen**
 - **Abuse mailboxes of hosting services**

✓ *Protects logo use legally and helps domain reputation providers act faster*

▮ Key Takeaways

- Logo spoofing works because **visual cues override caution**
- BIMI + VMC is the **strongest countermeasure** for email trust indicators

- Combine **technical protections (DMARC, DKIM, image recognition)** with **brand monitoring** and **user awareness**
- Always monitor for **unauthorized logo use**, not just domain spoofing

Natural Language Processing (NLP) in Cybersecurity

6.1.1 Linguistic Anomaly Detection Models

“When a message sounds human—but something feels off, NLP finds the fraud.”

□ What Is Linguistic Anomaly Detection?

Linguistic anomaly detection is the use of **NLP models** to identify **unusual, deceptive, or malicious patterns in language**, particularly in **phishing, scam, or social engineering attempts**.

These models help detect:

- **Suspicious phrasing or non-native writing patterns**
- **Tone mismatch** (e.g., urgency from an otherwise formal sender)
- **Psychological triggers** (like fear, urgency, authority)
- **Domain impersonation messages** using unnatural grammar

Think of it as **spam filters 2.0**—with context, tone, and subtlety awareness.

🔍 How Linguistic Anomaly Detection Works

Component	Function
Baseline Language Models	Learn “normal” communication style for a user, brand, or group
Anomaly Detection Layer	Flags deviations from expected syntax, structure, or tone
Contextual Embeddings	NLP embeddings (e.g., BERT, RoBERTa) detect semantic oddities
Sentiment & Intent Analysis	Detects manipulation tactics like fear, trust, urgency

□ Example Detection Logic

- **“Hi, please pay this invoice today urgently.”**
→ Unusual tone + mismatched grammar for the CFO → flagged
- **“Dear Esteemed Beneficiary, you have won...”**

- Obsolete/formal diction + over-flattery → anomaly trigger
- “Verify your account to avoid suspension.”
 - Keyword pattern matches phishing + threatening tone → high risk

Types of NLP Models Used

Model Type	Use Case
n-gram Models	Detect repetitive spam phrases and statistical oddities
Transformer Models	BERT, RoBERTa, GPT-based models for deeper language understanding
LSTM/RNNs	Older deep learning for sequence prediction and structure matching
One-Class SVMs	Used for outlier detection when only “normal” data is labeled
Autoencoders	Reconstruct known language patterns and detect reconstruction errors in anomalous emails

Applications in Cybersecurity

Use Case	How It Works
Phishing detection	NLP flags suspicious language patterns in messages
BEC threat profiling	Models detect tone change in CEO’s typical writing style
Insider threat monitoring	Tracks abnormal message content from internal users
Chatbot abuse detection	Finds users generating harmful or manipulated content
Fake tech support scams	Spots fake professionalism, scripted phrases

Challenges & Risks

Challenge	Why It Matters
False positives	Legit unusual language might be flagged
Language diversity	Attackers mix languages, misspellings to evade models
Evasion by AI-	Attackers use GPT-style text to sound human

generated text

Model drift

Anomaly baselines change as writing styles evolve

▣ Tools & Platforms That Use It

Platform	NLP Feature
Microsoft Defender ATP	Phishing and impersonation detection via NLP
Proofpoint TAP	Linguistic anomaly modeling for BEC
Abnormal Security	Behavioral and linguistic AI detection stack
Darktrace	Combines NLP with behavioral anomaly models
NLP libraries (open-source)	spaCy, HuggingFace Transformers, fastText, OpenNLP

▣ Key Takeaways

- Linguistic anomaly detection helps flag **fraudulent communication** by spotting **subtle changes in tone, grammar, and content**
- Uses a blend of **NLP, behavioral modeling, and machine learning**
- Most effective against **low-volume, high-impact threats** like **BEC and spear-phishing**
- Requires careful tuning to balance **false positives and evasion resistance**

Adversarial AI Techniques

6.2.1 Generative Adversarial Network (GAN) Training

“When AI learns to lie—and gets rewarded for doing it well.”

▣ What Are GANs?

Generative Adversarial Networks (GANs) are a type of **machine learning architecture** composed of two neural networks:

- A **Generator** that **creates synthetic data** (e.g., fake images, voices, text)
- A **Discriminator** that **evaluates whether data is real or fake**

The two models are trained together in a **zero-sum game**, constantly trying to **outsmart each other**.

GANs are used to create **deepfakes**, **phishing content**, **spoofed voices**, and **synthetic identities**—making them a rising threat in social engineering.

⚙️ How GAN Training Works

Component	Role
Generator (G)	Learns to create realistic fake data from random noise
Discriminator (D)	Learns to distinguish fake data from real data
Training Loop	G generates → D evaluates → G improves to fool D

▣ Training Process Flow

1. **Initialize** G and D with random weights
2. **Generator (G)** takes in random noise and **outputs fake samples**
3. **Discriminator (D)** is fed a mix of **real data + fake data**, and tries to classify them
4. **Loss is calculated:**
 - G is penalized when D correctly spots fakes
 - D is penalized when it fails to detect fakes
5. **Backpropagation** updates both models
6. Repeat **for thousands of epochs**, until G creates highly convincing fakes

▣ Example: GANs for Phishing Text

Step	Description
G generates	A fake password reset email using realistic language
D evaluates	Whether this looks like a legitimate corporate message
Result	G keeps improving tone, grammar, formatting until D can't tell

▣ Use Cases in Cybersecurity Threats

Use Case	How GANs Are Applied
Deepfake videos & audio	G generates realistic CEO voices or video instructions
Synthetic phishing pages	G designs pages that mimic banking or login portals
Fake identities & documents	G creates passports, ID cards, LinkedIn profiles
Phishing content generators	GANs craft messages with authentic tone and formatting
CAPTCHA solving	G learns to generate patterns that fool CAPTCHA systems

✂ Training Challenges

Challenge	Description
Mode collapse	Generator learns to produce limited variations of fakes
Training instability	G and D may overpower each other, leading to failure
Convergence difficulty	GANs can be very slow and sensitive to hyperparameters
Data quality	Poor training data leads to obvious or malformed fakes

📖 GAN Variants You Should Know

Variant	Purpose
DCGAN	Deep Convolutional GAN for images

CycleGAN	Style transfer (e.g., convert photo to painting)
StyleGAN	High-quality human face generation
TextGAN	Generates realistic human language text
AudioGAN	Generates spoofed voice/audio samples

🔒 Security Implications of GAN Training

- **Weaponization Risk:** Attackers use well-trained GANs to create **socially persuasive deepfakes, scam emails, or voice clones**
- **Detection Evasion:** GAN-generated content can **bypass filters**, fool humans, or impersonate trusted parties
- **Disinformation:** GANs can flood platforms with **synthetic articles, fake videos, and mass-produced propaganda**

🛡️ Defensive Countermeasures

Defense Strategy	Purpose
GAN fingerprinting	Detect subtle patterns left by generative models
Deepfake detection models	CNNs or transformer-based tools to catch audio/video forgeries
Watermarking AI content	Embed invisible tags during generation
Behavioral analysis	Spot inconsistencies in context or interaction
Source validation	DMARC, PGP, SSL validation for media and email

📌 Key Takeaways

- GANs create **synthetic but realistic content** that can be used for **fraud, impersonation, or phishing**
- Training GANs requires balancing a **generator and a discriminator** in a feedback loop
- While powerful for good (e.g., art, medicine), GANs pose rising risks in **adversarial AI and cyber deception**
- Defensive AI must evolve to **detect, disrupt, and trace** GAN-generated threats

Behavioral AI in Cybersecurity

6.2.1 Mouse Movement Biometrics

“Your cursor movements are as unique as your fingerprint.”

▣ What Is Mouse Movement Biometrics?

Mouse movement biometrics use **behavioral AI** to identify and authenticate users (or detect anomalies) based on **how they move the mouse**—not just **what** they click, but **how** they move, drag, and interact with UI elements.

This behavioral data is then used for:

- **Fraud detection**
- **Session hijacking alerts**
- **Insider threat identification**
- **Silent MFA (multi-factor authentication)**

Even if an attacker has valid login credentials, they often **can’t mimic the victim’s unique cursor rhythm.**

▣ What Features Are Measured?

Mouse Behavior Metric	Description
👉 Speed	How fast the cursor moves across different distances
▣ Acceleration/Deceleration	Smoothness or suddenness in movements
▣ Trajectory	Curved, angular, or straight path styles
🖱️ Click behavior	Timing, pressure (in touchpads), location clustering
⌂ Hover patterns	How long users pause over fields or buttons
▣ Scroll and drag	Consistency in drag-drop or scroll speeds
🕒 Time to target	Delay between seeing a UI element and clicking on it

▣ How Behavioral AI Learns from It

Behavioral AI builds a **unique user profile** by collecting multiple sessions of:

- Mouse + keyboard behavior
- Screen resolution & device type
- Response time and interface familiarity

These profiles are stored securely and compared **in real time** against future sessions to:

- Validate the user
- Flag anomalies

📌 Use Cases in Security

Use Case	How Mouse Biometrics Help
Credential theft detection	Attacker logs in—but moves differently than real user
Bot & malware detection	Bots have predictable or inhuman patterns (perfect curves, constant speed)
Silent authentication (continuous MFA)	User is re-authenticated invisibly based on ongoing behavior
Insider threat analytics	Detects when a user is behaving “unusually” under same login
Fraud in fintech/web apps	Banks, crypto exchanges, and KYC tools use it to detect imposters

🔧 Tools & Platforms That Use It

Platform / Vendor	Capabilities
BehavioSec	Enterprise-grade behavioral biometrics engine
BioCatch	Leader in mouse & session behavior analytics for fraud prevention
Zighra	AI-driven behavioral biometrics for mobile + desktop
Kount (Equifax)	Identity trust platform using movement + velocity models
TypingDNA (keyboard+mouse)	Behavioral authentication using keystroke and cursor dynamics

📌 Behavioral Biometrics vs. Static Biometrics

Feature Type	Static Biometrics	Behavioral Biometrics
Example	Fingerprint, face scan	Mouse movement, typing rhythm
When it's captured	Once, at login	Continuously, in real time
Can be stolen?	✓ Yes	✗ Harder—based on behavior
Easy to spoof?	Moderate (deepfake risk)	Very hard—complex behavior patterns
Privacy risk	Higher (stored images)	Lower (abstract data patterns)

⚠ Challenges & Limitations

Challenge	Description
Device sensitivity	Patterns vary across mouse types or touchscreen vs. trackpad
Accessibility concerns	Differently abled users may not follow consistent patterns
Privacy transparency	Needs clear consent & anonymized usage to avoid legal risk
Cold start problem	AI needs several sessions to “learn” a new user baseline

📌 Key Takeaways

- Mouse movement biometrics offer **passive, continuous authentication** based on **unique behavior**
- They enhance fraud detection and make session hijacking **much harder**
- Best used in **sensitive apps (finance, government, SaaS)** where subtle cues matter
- Must be deployed **ethically and transparently** to avoid privacy violations

Behavioral AI & Threat Anticipation

6.2.2 Session Hijacking Prediction Algorithms

“Don’t just detect the hijack—predict it before it happens.”

□ What Is Session Hijacking?

Session hijacking occurs when an attacker **takes over a legitimate user’s session**—often by stealing cookies, tokens, or exploiting unsecured connections—**without needing credentials**.

Modern behavioral AI systems are now trained to **predict** and preempt these takeovers before damage occurs.

□ What Are Session Hijacking Prediction Algorithms?

These are **machine learning and AI-based models** trained to recognize **early indicators of session anomalies**. Instead of reacting after a hijack, they:

- **Analyze session behavior in real-time**
 - **Compare current activity to historical norms**
 - Predict whether the session has been **compromised or overtaken**
-

□ How It Works (Step-by-Step)

1. **Behavioral Baseline Creation**
 - Models learn each user’s typical:
 - Login timing
 - Mouse movement
 - Click paths
 - Page scroll speed
 - Navigation habits
2. **Real-Time Monitoring**
 - As the session unfolds, every movement and request is tracked.
3. **Anomaly Scoring**
 - Session gets a **risk score** based on behavioral deviation.
4. **Pre-Hijack Indicators Trigger Prediction**
 - If the risk score spikes **before credential change, transaction, or logout**, preemptive actions can occur:

- Trigger re-authentication
- Lock session
- Notify security team

🔍 Key Features Analyzed

Behavioral Signal	Why It's Important
IP geolocation change	Sudden jumps (e.g., from Pakistan to Germany)
User-agent mismatch	Desktop session now acts like a mobile device
Mouse/click behavior drift	Erratic or robotic movement vs. known patterns
Keystroke/typing patterns	Unusual speed, delay, or rhythm
Session timing mismatch	Activity at strange hours for that user
API call frequency	Unusual frequency of requests (scraping or automation)
Unusual navigation path	Pages visited in strange or reversed order

🧠 Common Algorithms Used

Algorithm Type	Function
Random Forests / XGBoost	Flag risk based on decision trees from user behavior stats
Autoencoders	Reconstruct normal sessions; fail on unseen patterns
One-Class SVM	Anomaly detection with only normal behavior as baseline
RNN / LSTM	Track sequential behavior for deviations (e.g., page flows)
Bayesian Networks	Predict likely outcomes based on multiple behavior cues
Isolation Forests	Identify outlier sessions from multivariate behavior sets

📖 Example Attack Prediction Scenario

Legit User Pattern:

- Login from Karachi (Pakistan)
- Moves mouse in curved, drag-heavy style
- Opens “Invoices” → “Download” → “Logout”

Hijacked Session:

- Same token reused from Berlin (Germany)
- Straight-line mouse movement
- Opens “Invoices” → tries to change bank account number

❑ **Prediction Triggered:**

- Risk score spikes due to **geolocation, behavioral mismatch, and unauthorized intent**

✓ **System logs user out + alerts SOC**

✂ **Tools and Vendors Using Prediction Models**

Platform	Feature
BioCatch	Behavioral biometrics to detect session anomalies
Arkose Labs	Risk-based session scoring with prediction AI
ThreatMetrix (LexisNexis)	Continuous authentication via behavioral profiles
Microsoft 365 Defender	Session hijacking risk analytics via Azure AD
PingOne Risk	Real-time session behavioral decision engine

📈 **Challenges & Considerations**

Challenge	Description
False positives	Legit travel or VPN use may mimic hijack indicators
Cold start learning	New users require time to build baselines
Privacy risks	Behavior tracking must be anonymized and consented
Evasion by advanced attackers	Some hijackers may mimic prior behavior using AI

❑ **Key Takeaways**

- Session hijacking prediction uses **behavioral analytics + AI** to catch takeover attempts **before malicious action**
- Monitors **subtle cues** like movement, timing, flow, and intent
- Tools like **BioCatch**, **ThreatMetrix**, and **Arkose Labs** are already using these models at scale
- Most effective when paired with **multi-factor authentication**, **risk scoring**, and **session sandboxing**

Microlearning Modules for Security Awareness

7.1.1 90-Second Threat Recognition Drills

“Train the reflex, not just the memory.”

What Are 90-Second Threat Recognition Drills?

90-second drills are ultra-short, focused **microlearning experiences** that train users to **instantly recognize and respond to cyber threats**. Designed to fit into daily workflows, these drills help build **muscle memory** for detecting phishing, scams, and manipulative digital tactics.

Instead of annual security training, think **bite-sized reps for behavioral change**.

Core Objectives

- Rapidly **build pattern recognition** for digital threats
- Develop **reflexive responses** to phishing, social engineering, and scams
- Reinforce lessons using **micro-exposure + spaced repetition**
- Target **real-world simulations** like fake invoices, fake login pages, spoofed links

Structure of Each Drill

Segment	Time (seconds)	Description
🔍 Scenario Preview	0–20	Realistic email, message, or interface shown to user
📋 Quick Decision Task	20–60	User chooses: safe / unsafe / suspicious
🎓 Instant Feedback	60–90	Explains why it was (or wasn’t) a threat + bonus tip

- ✓ Designed for **email, mobile, or desktop popups**
- ✓ Optimized for daily exposure without interrupting workflow

Drill Content Examples

Drill Theme	Threat Simulated
-------------	------------------

Phishing Email Drill	Fake password reset or urgent bank notice
QR Code Quiz	“Scan this for your rewards!” on a fake poster
Invoice Verification Drill	Look for fake vendor logos and manipulated PDF metadata
Meeting Link Scam	Spot fake Zoom/WebEx invitation URLs
CEO Fraud Test	“Wire money urgently to this account...” in spoofed email
Social Media Scam	Suspicious Instagram or WhatsApp DM with shortened links
Domain Spoof Drill	“AppIe.com” vs. “Apple.com” (homoglyph training)

📖 Why It Works (Psychology & Neuroscience)

Principle	Effect
🕒 Time-pressured decision	Mirrors real-world urgency in social engineering
🔁 Spaced repetition	Reinforces retention over time
🧠 Dopamine loop	Immediate feedback triggers learning reinforcement
📖 Micro-cognitive load	Easy to absorb during work without fatigue
💡 Pattern-based exposure	Improves subconscious detection reflexes

Employees move from “trained once” to “trained instinctively.”

🛠️ Delivery Platforms

Platform	Features
KnowBe4	Phishing simulators with micro-lesson follow-ups
Curricula Living Security	Gamified short-form learning with 90s episodes
Hoxhunt	“Threat Flash” drills with feedback in <2 mins
Custom LMS integration	Adaptive email threat recognition micro-exercises
	Embedding 90s modules into daily tool usage

🔗 Integration Ideas

- **Browser extensions** that show random drills weekly
- **Email plugins** (Outlook, Gmail) that inject sample threats
- **Slack/Teams bots** that quiz users during idle time
- **Onboarding checklists**: Include 90s drills for new employees
- **Gamified leaderboards**: Track top scorers per department

⚠ Challenges to Address

Issue	Solution
Drill fatigue	Vary themes and interleave with real alerts
Overconfidence bias	Include trick questions and gray-area scenarios
No follow-through	Link to full lessons for deeper exploration post-drill
Accessibility	Ensure mobile-friendly, voice-over capable design

📌 Key Takeaways

- 90-second drills are **microlearning bursts** that train users to spot and react to cyber threats reflexively
- Designed to be **fast, frequent, and feedback-driven**
- Improve **threat literacy, reaction speed, and security culture** organization-wide
- Ideal for **embedding into daily tools** like Slack, Outlook, Chrome, or LMS platforms

Microlearning Modules

7.1.2 Just-in-Time Mobile Learning (JITML)

“The right security lesson, at the exact moment it matters most.”

□ What Is Just-in-Time Mobile Learning (JITML)?

Just-in-Time Mobile Learning (JITML) is a **context-aware microtraining method** that delivers short, actionable cybersecurity content to users **at the point of risk or need**—typically on **mobile devices**.

Rather than scheduled or mandatory training, JITML offers **real-time interventions** during risky behavior or as immediate reinforcements after user actions.

Think of it as a **digital coach** that taps your shoulder just before you click something dangerous.

□ Core Objectives

- Reinforce secure behavior **at the moment of decision**
 - Educate users on **why something is risky**, not just that it is
 - Reduce training fatigue with **mobile-first, moment-specific content**
 - Enable **bite-sized security awareness** that scales across devices
-

⚙️ When & How It’s Triggered

Trigger Moment	Example Scenario
□ Clicking on a suspicious email	User taps a phishing link in mobile Gmail → JITML launches a drill
👉 Downloading an unverified app	System shows a 30s alert on app risk + safe alternatives
□ Scanning a QR code	Popup lesson warns about quishing risks before proceeding
□ Connecting to public Wi-Fi	JITML triggers a microlesson on MITM (man-in-the-middle) attacks
□ Clicking suspicious SMS links	Drill explains smishing tactics in under 90 seconds

□ Structure of a JITML Module

Segment	Duration	Description
🔊 Intervention Alert	5–10s	“Hold on—this action could be risky.”
👁️ Visual Scenario	10–20s	Screenshot/animation of similar threat
📄 Micro-Explanation	30–40s	What’s happening + how to recognize it next time
✅ Quick Quiz	10–15s	Reinforce learning with 1–2 choice-based questions

📈 Benefits of JITML

Benefit	Explanation
Contextual learning	Users remember more when taught in the moment
Behavior reinforcement	Increases chance of future safe behavior
Minimal interruption	Fits into natural workflows—no classroom or LMS needed
Mobile-first	Works during commutes, remote work, or BYOD scenarios
Personalized risk education	Delivered based on user activity, device, and context

🛠️ Tools & Platforms Using JITML

Platform / App	Capability
Hoxhunt	Delivers adaptive, real-time phishing training
Elevate Security	Pushes mobile security nudges based on live user behavior
Cybermaniacs	Micro-nudges on user actions + gamified mobile training
Living Security Edge	AI-based timing of microlessons during risky moments
Custom MDM + LMS integration	Companies embed JITML into internal apps or mobile device management tools

📐 Design Principles Behind JITML

Principle	Role in Effectiveness
-----------	-----------------------

□ Just-in-time	Timing + context makes learning stick
□ Microlearning	Small units prevent overload
□ Repetition + variation	Builds long-term memory through reinforcement
🔗 Behavioral trigger awareness	Links user action to security context
□ Real-time feedback	Turns mistakes into learning moments, instantly

⚠️ Implementation Challenges

Challenge	Solution
User resistance	Keep modules short, relevant, and non-intrusive
Privacy concerns	Anonymize user data and get opt-in consent
Device fragmentation	Ensure compatibility across Android, iOS, and hybrid MDMs
False triggers	Use behavior scoring to avoid unnecessary interruptions

□ Key Takeaways

- JITML delivers **bite-sized, mobile-based training** exactly **when risky behavior is detected**
- Helps build **real-time threat awareness** with **minimal user disruption**
- Ideal for phishing, app risk, unsafe networks, smishing, and BYOD environments
- Works best when integrated with **behavioral AI, mobile MDM tools, or email clients**

Human-Centered Security Awareness Design

7.3.1 Ethical Boundaries in Trauma-Inducing Scenarios

“Security awareness should build resilience—not cause harm.”

▣ What Are Trauma-Inducing Scenarios in Cybersecurity Training?

These are **hyper-realistic simulations** or **scare-based campaigns** designed to elicit **strong emotional reactions**—such as fear, shame, or panic—in order to:

- Simulate the **stress of a real cyberattack**
- “Shock” users into better awareness
- Test how employees react under **emotional pressure**

Examples include:

- Fake ransomware screens locking a user’s device
- Simulated data leak notifications involving personal data
- Vishing calls threatening legal action or account deletion
- Deepfake videos of company leaders issuing threats

While powerful, these can easily cross ethical lines and **psychologically harm** users—especially vulnerable populations.

⚖️ Why Ethical Boundaries Matter

Risk	Impact
☹️ Emotional distress	May trigger anxiety, guilt, PTSD (especially past victims)
▣ Breach of trust	Users feel deceived or manipulated by their own employer
📉 Productivity loss	Emotional fatigue from high-stress simulations
👊 Resistance to training	Backlash, disengagement, and long-term distrust
⚠️ Legal and HR exposure	Mental health violations, ADA violations, or harassment claims

❑ Psychological Red Flags in Training Scenarios

Flagged Tactic	Why It's Problematic
❑ Simulated termination emails	May trigger real fear of job loss or trauma from past layoffs
❑ Fake police/legal threats	Can cause panic, especially in vulnerable communities
❑ Data breach alerts with PII	Resembles real-world trauma of identity theft
● Hyper-real ransomware popups	May induce panic or helplessness if not clearly labeled
● Impersonation of loved ones	Ethical violation if family/friend names are spoofed

❑ Ethical Design Principles for Realistic Training

Principle	Implementation Example
✓ Informed consent	Users opt into high-intensity simulations explicitly
✓ Layered realism	Realistic—but with non-personal or non-violent scenarios
✓ Debrief immediately	Explain the simulation and its purpose right after execution
✓ Psychological safety net	Offer opt-outs, mental health resources, and anonymous feedback
✓ Role-based tailoring	Avoid trauma-sensitive simulations for high-risk or vulnerable roles
⊘ No personal targeting	Never simulate attacks using real user names, family data, or medical info

❑ Safer Alternatives to Traumatic Scenarios

Intention	Harmful Version	Ethical Alternative
Instill urgency	Fake ransomware lockout	Timed phishing quiz with escalating urgency
Simulate risk	Fake job termination email	“Unauthorized access detected—what’s your next step?” drill
Raise awareness	Fake leak of personal emails	“How would you respond to a generic email breach?”
Test fear response	Threatening vishing call	Polite impersonation of helpdesk asking for OTP

♥ Frameworks & Guidelines to Follow

Standard / Body	Relevance
NIST SP 800-50/53/181	Emphasizes positive, role-based, and non-coercive awareness methods
ISO/IEC 27002:2022	Calls for awareness campaigns to avoid inducing panic or guilt
ADAA / APA (US)	Mental health guidelines: avoid triggers, shame, or coercion
HR & DEI policies	Avoid simulations that may target or disproportionately affect marginalized groups

□ Key Takeaways

- Cybersecurity training must **never come at the cost of mental safety**
- Trauma-inducing scenarios are **ethically risky, legally questionable, and psychologically harmful** if not handled properly
- Ethical boundaries involve **consent, transparency, and empathy**
- Simulations should **educate, not intimidate**—focusing on **empowerment over fear**

Executive Protection Protocols

8.1.1 Digital Executive Shielding (DES) Frameworks

“Your C-suite isn’t just high-value — it’s high-risk.”

♥ What Is Digital Executive Shielding (DES)?

Digital Executive Shielding (DES) is a cybersecurity strategy designed to protect high-profile executives from targeted digital attacks such as:

- Spear-phishing
- Deepfake impersonations
- Credential stuffing
- Business Email Compromise (BEC)
- Executive doxxing and harassment
- Exploitation of executive social media and brand footprint




C-level executives are **prime targets** for cybercriminals due to their access, visibility, and influence.

▣ Core Goals of DES Frameworks

- Prevent **digital impersonation or account takeovers**
- Shield executives from **reputation-damaging leaks**
- Reduce **attack surface** through proactive hardening
- Provide **real-time visibility** into executive-specific threats
- Implement **continuous monitoring** and **identity validation**

▣ DES Framework Components

Layer	Description
▣ Account Hardening	Enable MFA, disable password reuse, rotate credentials regularly
👁️ Surface Monitoring	Scan for exposed executive data on the dark web, forums, and leaks
🔗 Spoof Prevention	DMARC, SPF, and DKIM for domain protection against fake exec emails
▣ Social Media Lockdown	Lock down public visibility, set alerts for impersonation attempts
🔒	Use watermarking, VMCs, and face/voice verification

Impersonation Defenses	for deepfake detection
 Attack Simulation	Run executive-targeted phishing or vishing simulations
 White Glove IT Protocols	Prioritize exec devices for patching, threat hunting, and forensics
 Awareness Training	Deliver tailored sessions on modern attack tactics (e.g., AI-enhanced phishing)

❑ Why Executives Are Uniquely Vulnerable

Risk Factor	Why It Matters
High authority	A fake message from a CEO gets fast responses (Authority Bias)
Public visibility	Info for spear-phishing is often already on LinkedIn/press
VIP status in org chart	Attackers know executives bypass security workflows
Brand association	Attacks on execs damage company reputation and stock value
Limited security habits	Execs often use personal assistants, unmanaged devices, or delegate digital tasks

❑ Tools & Services Supporting DES

Tool / Vendor	Capability
ZeroFox	Executive protection + social media impersonation takedowns
Constella Intelligence	Doxxing & leak monitoring for VIPs across open/dark web
BlackCloak	Personal cybersecurity for executives and high-net-worth users
Proofpoint TAP + VIP Scoping	Enhanced email protection for executive identities
Human (formerly White Ops)	Detection of synthetic bots and fake interactions

❑ Operational Best Practices

Practice	Benefit
✓ Segmentation of accounts	Separate personal + corporate assets to reduce compromise blast radius
✓ Dedicated SOC playbooks	Fast incident response tailored for VIP-level breaches
✓ Third-party exposure checks	Ensure executive data isn't leaking through PR agencies, vendors, or assistants
✓ Legal/PR crisis readiness	Pre-written statements and protocols in case of reputational attack

⚖️ Ethical & Privacy Considerations

- DES must **respect executive privacy** (e.g., personal device scans must be opt-in)
- Avoid **over-surveillance**; data must be **minimally invasive and encrypted**
- Maintain **clear policy separation** between company and personal protection

📌 Key Takeaways

- Executives face **elevated risk** due to their digital footprint, authority, and access
- Digital Executive Shielding (DES) frameworks provide **layered, proactive defense**
- Success requires **technical controls + behavioral awareness + policy alignment**
- DES must balance **security, privacy, and visibility** in high-stakes environments

Executive Protection Protocols

8.1.2 Family Office Threat Mitigation

“When wealth, trust, and legacy intersect—so does risk.”

▣ What Is Family Office Threat Mitigation?

Family Office Threat Mitigation refers to the **specialized cybersecurity strategies** used to protect ultra-high-net-worth individuals (UHNWIs), their families, and the private wealth management teams who oversee their assets, communications, and digital estates.

Unlike corporate environments, **family offices** are **lightly staffed**, **highly targeted**, and often **soft security targets** for elite attackers.

▣ Key Threats to Family Offices

Threat Type	Example Scenario
📧 Targeted spear-phishing	CFO receives a fake wire transfer request from a spoofed family member
🏠 IoT & smart home hacking	Cameras or door locks accessed by hackers to track daily routines
💰 Wealth impersonation fraud	Attackers pose as family members to request fund access
📱 Mobile device compromise	Family members use unprotected apps or devices
🏢 Vendor compromise	Nanny agencies, chauffeurs, private pilots used as access points
🗣️ Social engineering attacks	Staff tricked via LinkedIn or WhatsApp into sharing travel or asset info
🎭 Deepfake & AI impersonation	Synthetic voice calls from “Dad” requesting urgent crypto transfers

▣ Family Office Security Layers





Layer	Description
▣ Personal	MFA, password rotation, privacy settings on family

Account Hardening	platforms
 Network & Device Security	Mobile Device Management (MDM), encrypted comms, Wi-Fi firewalls
 Security Culture Training	All family & staff educated on scams, phishing, vishing, deepfakes
 Threat Monitoring & Response	Dark web scans for leaked info, impersonation alerts, executive SOC access
 Discretion Protocols	Social media restrictions, anonymized asset ownership, secure travel planning
 Vendor Risk Controls	Background checks + cyber hygiene audits for accountants, house staff, travel agents
 Legal & Digital Estate Planning	Pre-breach incident playbooks, crypto estate protection, account inheritance plans

Tools & Services Supporting Family Office Security

Vendor / Platform	Service Provided
BlackCloak	Personal cybersecurity for UHNW families (devices, accounts, comms)
Constella Intelligence	Identity monitoring, VIP digital risk alerts
DarkOwl / SpyCloud	Exposure of emails, passwords, addresses on dark web
Qomplx / Axio	Cyber risk quantification + threat modeling for family offices
iTrust Capital / BitGo	Crypto asset protection with secure wallets and inheritance handling

Common Weak Points in Family Offices

Weakness	Consequence
 BYOD (Bring Your Own Device)	Family or staff may use unsecured phones or tablets
 Untrained relatives	Children or spouses may post travel or wealth indicators online
 Unvetted third parties	Pilots, nannies, chefs may be digitally manipulated
 Unencrypted communications	Use of iMessage, WhatsApp, or Zoom without protection

🏠 Legacy tech

Aging routers, NAS systems, or surveillance gear with no updates

📌 Best Practices for Threat Mitigation

1. Personal Cyber Hygiene

- Dedicated secure email for financial matters
- Disallow personal social media sharing of real-time location or assets

2. Private DNS + VPN Routing

- All home and travel networks routed through corporate-grade VPN and DNS filtering

3. Family Security Briefings

- Monthly updates on new scams, tactics, breaches, and response drills

4. Incident Playbooks

- Predefined response paths for stolen devices, hacked accounts, or financial fraud

5. Cyber Insurance Tailored to Family Offices

- Including coverage for ransomware, data leaks, impersonation fraud, and mobile theft

⚖️ Legal & Ethical Safeguards

Category	Consideration
🏛️ Digital Estate Planning	Ensure family digital assets have legal continuity and access rules
📄 Power of Attorney Clauses	Include cybersecurity authorities for crisis delegation
📄 Consent-Driven Monitoring	Family/staff must be aware and agreeable to oversight systems

📌 Key Takeaways

- Family offices face **unique, high-stakes cybersecurity risks** due to wealth, visibility, and small team structures
- Effective mitigation blends **technical controls, awareness, and personalized threat intelligence**
- Tools like **BlackCloak, Constella, and DarkOwl** help protect high-value individuals and their inner circle
- Risk isn't just digital—it's **social, reputational, and emotional**, and must be treated holistically

Finance Team Defense

8.2.1 Payment Redirection Scenario Drills

“Train your finance team for the fraud that’s one email away.”

▣ What Are Payment Redirection Scenario Drills?


Payment redirection drills are simulated training exercises designed to test and improve how finance teams **identify, respond to, and report** attempts at **fraudulent fund transfers**. These drills recreate **realistic business email compromise (BEC)** scenarios, where attackers try to reroute legitimate payments into fraudulent accounts.

These simulations are crucial because **finance teams** are the **primary targets** in most BEC attacks.

▣ Objectives of the Drills

- Strengthen internal verification procedures (call-backs, dual approvals)
- Train staff to recognize **subtle deception techniques** in emails or invoices
- Reduce **response time to suspicious payment requests**
- Improve **incident reporting habits** and **cross-team communication**

▣ Anatomy of a Redirection Attack

Phase	Attacker Action
▣ Hook	Spoofed email from vendor, executive, or partner
▣ Bait	Modified invoice or urgent wire transfer instruction
▣ Switch	New bank details inserted (“we’ve changed banks—see new IBAN”)
 Execution	Employee processes payment to attacker-controlled account
▣ Fallout	Funds lost, audit trails exposed, legal and reputational damage

▣ Drill Types by Scenario

Drill Type	Simulation Goal
Vendor Impersonation Drill	Mimics a supplier changing banking instructions
Executive Spoof Drill	Fake email from CFO requesting urgent transfer
Invoice Tampering Drill	Tests detection of altered invoice metadata or totals
Domain Homoglyph Drill	Detect email from @suppIyco.com instead of @supplyco.com
Bank Account Switch Drill	Simulated follow-up email with suspicious new IBAN/SWIFT

III Difficulty Calibration (Example)

Level	Characteristics	Outcome Tested
● Easy	Generic spoof, broken grammar, single redirection cue	Baseline awareness
● Medium	Believable vendor name, new account number, no phone call	Judgment under ambiguity
▣ Hard	Domain spoof + urgent exec tone + invoice match	Process override vs. instinct
● APT-Level	Multi-step thread hijack with valid attachments & call	End-to-end fraud resilience test

▣ Behavioral Cues to Train For

Cue	Red Flag
▣ “Bank account change”	Sudden switch in payment destination
⚡ “Urgent wire request”	Pressure to bypass standard approval
👤 Suspicious sender domain	Homoglyphs, extra characters, misspellings
▣ Avoids verification	“Do not call; I’m traveling” or “Can’t take calls”
▣ Attachment metadata mismatch	Invoice number/date mismatch or altered PDF properties

▣ Response Protocols Tested

Step	Drill Expectation
------	-------------------

□ Verify request verbally	Call vendor or executive on file (not the number in email)
□ Check vendor records	Confirm new payment details with registered info
□ Report the email	Alert internal IT/security immediately
⊗ Do not process payment	Halt transaction until confirmed through secondary channels
□ Log the incident	Record in internal fraud/incident management system

✂ Tools to Support Drills

Platform / Service	Capability
KnowBe4 Phishing Platform	Create customizable payment fraud simulations
Hoxhunt Smart Campaigns	Adaptive redirection-themed phishing emails
Cofense Vision	Visibility into real-time email fraud attempts
Proofpoint ThreatSim	Simulated invoice fraud and role-targeted campaigns
Custom Runbooks	Finance-SOC coordinated simulation with audit logging

📖 Complementary Training Modules

- Role-based BEC awareness (CFOs, AP clerks, procurement staff)
- Anti-fraud checklists & dual approval processes
- Secure invoice management practices
- Vendor authentication workflows
- Email domain verification (DMARC/SPF/DKIM alignment awareness)

□ Key Takeaways

- Payment redirection is one of the **most financially damaging** forms of social engineering
- Drills prepare finance staff to **pause, question, verify** before releasing funds
- A successful program includes **realistic scenarios, graded difficulty, and well-defined response playbooks**
- Repetition builds muscle memory—**awareness must be operationalized**

Emerging Threats in Web3

8.3.1 Cryptocurrency Wallet Social Engineering

“No firewall can stop a user from giving away their seed phrase.”

🔒 What Is Cryptocurrency Wallet Social Engineering?

Cryptocurrency wallet social engineering refers to **manipulative psychological tactics** used by attackers to **trick individuals into revealing private wallet credentials**, such as:

- Seed phrases
- Private keys
- Recovery codes
- QR codes or keystore files
- Wallet access on browser extensions (like MetaMask)

Unlike traditional malware or brute-force methods, these attacks **exploit trust, confusion, and urgency**, often **bypassing all technical protections**.

“Not your keys, not your coins” — but **social engineers make those keys theirs**.

📌 Core Objectives of These Attacks

- Gain full access to a victim’s wallet
 - Transfer out funds (ETH, BTC, stablecoins, NFTs)
 - Steal wallet-linked identities (ENS, PFPs, DAOs)
 - Create long-term backdoors (browser plugins, phishing clones)
-

🔗 Top Social Engineering Tactics by Attack Vector

Attack Type	Description
Fake Wallet Support Scams	Impersonators offer help on Reddit, Discord, Twitter (“DM me”)
Phishing Websites	Cloned wallet interfaces (e.g., fake MetaMask or Phantom sites)
Seed Phrase Harvesting Games	“Connect wallet to play & win!” — backend steals seed

Malicious Airdrops	Users claim “free tokens” → grant smart contract approvals
Fake NFT Marketplace Listings	Users click links to fake OpenSea/Rarible → approve malicious txs
Browser Extension Impersonators	Chrome Store wallets that harvest credentials on install
QR Code Phishing	“Scan to import wallet” tricks victims into syncing with attacker
Giveaway/Impersonation Bots	Fake Elon Musk or Vitalik bots promise returns for crypto sent

🔍 Anatomy of a Common Scam

Scenario: A victim posts a help message in a crypto Discord after a failed wallet transaction.

1. 🧑‍🚒 **Impersonator Pounces**
 - Fake admin DMs: “I can help restore your access.”
2. 🗝️ **Asks for Seed Phrase**
 - Claims it’s required “just to check your wallet state.”
3. 📲 **Transfers Funds Immediately**
 - Victim’s entire balance disappears within minutes.
4. 🧹 **Cleanup & Disappear**
 - Scammer deletes Discord profile or switches handle.

🔍 Common Behavioral Manipulation Cues

Manipulative Cue	Example Phrase
👤 Authority bias	“I’m from MetaMask support.”
⌚ Urgency	“You must act now before your wallet is locked.”
👥 Social proof	“Others have already recovered their funds this way.”
🔒 False security cues	“We’re using encrypted channels, it’s safe.”
🔄 Reciprocity	“You’re receiving this free NFT drop, just connect wallet.”

🛡️ Defensive Practices & Tools

Layer	Defensive Action
🚫 Never share	Treat like the keys to your vault — <i>never share</i>

seed	<i>under any context</i>
❑ Hardware wallets	Use cold wallets (e.g., Ledger, Trezor) for high-value storage
❑ Transaction simulation tools	Tools like Revoke.cash or [Etherscan's token approvals] to check permissions
❑ Regular permission audits	Revoke smart contract permissions after dApp use
❑ URL verification	Always type wallet URLs directly; never trust Discord/Twitter links
❑ Block social DMs	Disable unsolicited messages on Discord, Telegram, Twitter
❑ Education	Train users that real support never asks for private keys

❑ Psychological Weaknesses Exploited

Cognitive Bias	How It's Exploited
Urgency bias	"Do this in the next 5 minutes or funds are lost forever!"
Trust in platforms	If scam happens on Reddit or Discord, users assume it's safe
FOMO (Fear of Missing Out)	"Claim your airdrop now or lose access forever."
Overconfidence	Crypto-native users may believe they "can't be scammed"

❑ Key Takeaways

- **Social engineering is the #1 threat** to crypto wallet security — not malware
- Attacks often target users on **Discord, Telegram, X (Twitter), Reddit, and Google search ads**
- Wallet security depends on **behavioral hygiene, transaction awareness, and education**, not just technology
- Seed phrases, once leaked, are **irreversible vulnerabilities**

Regulated Sector Incident Management

9.1.1 HIPAA-Compliant Response: Patient Data Ransomware Negotiation

“When healthcare data is held hostage, every decision must balance legality, ethics, and urgency.”

□ What Is a HIPAA-Compliant Ransomware Response?

In the context of U.S. healthcare, a **HIPAA-compliant ransomware response** refers to actions taken after an incident where **Protected Health Information (PHI)** is encrypted or stolen by ransomware actors, in line with the **Health Insurance Portability and Accountability Act (HIPAA)** regulations.

When ransomware hits:

- **PHI is often considered compromised, even if not exfiltrated**
 - Covered entities and business associates must respond within strict **privacy and security frameworks**
 - Every action—including **negotiation**—must be **documented, risk-assessed, and legally justifiable**
-

□ What Counts as a HIPAA Violation During Ransomware?

Action/Failure	HIPAA Consequence
✗ Inadequate security controls	Failure to meet HIPAA Security Rule
✗ Late breach notification	Breach Notification Rule violation
✗ Insufficient documentation	Non-compliance with audit trail/logging requirements
✗ Paying ransom without risk analysis	Potential violation of HITECH and OCR expectations
✗ Disclosure of PHI during negotiation	Breach of Privacy Rule

△ When Ransomware Triggers a HIPAA Breach

According to **HHS guidance**, ransomware typically counts as a **reportable breach** unless:

- You can **demonstrate a low probability of compromise** through a documented risk assessment
- No unauthorized access or exfiltration of PHI occurred

☐ **Notification Requirements:**

- **To Affected Individuals:** Within 60 days
- **To HHS OCR:** Immediately if over 500 individuals are affected
- **To Media:** If breach affects 500+ residents in a single jurisdiction

☐ Legal Ransomware Negotiation in HIPAA Context

Step	HIPAA-Compliant Practice
🔍 Triage & Containment	Secure systems, stop lateral spread, preserve logs
☐ Risk Assessment	Evaluate encryption level, attacker access, data at risk
☐ Documentation	Every step logged: files hit, systems involved, PHI types
☐ Negotiation Prep	Engage legal counsel, breach coaches, and external negotiators
🚫 No PHI Disclosure	Never confirm or disclose PHI during negotiation chats
⚖️ Legal Review	Review OFAC/FinCEN sanctions list before payment
☐ Payment (if chosen)	Only after consulting counsel, law enforcement, and cyber insurer
☐ Post-Breach Notification	Notify stakeholders, HHS OCR, and patients per timeline

HIPAA does **not prohibit ransom payment**, but the **decision must be risk-justified and aligned with patient protection obligations**.

♥️ Key Partners in a HIPAA-Compliant Response

Role	Responsibility
HIPAA Privacy Officer	Ensures breach evaluation, notices, documentation

IT Security Team	Isolates infection, collects forensics, starts recovery
Legal Counsel	Validates actions with HIPAA, OFAC, and state laws
Cyber Insurer / Broker	Covers payment logistics and negotiation strategy
Third-Party Negotiator	Anonymous, experienced mediators with ransomware actors
Public Relations Lead	Coordinates breach messaging to patients and media
HHS/OCR Reporting Liaison	Coordinates formal notification to federal regulators

III HIPAA-Compliant Decision-Making Flow (Ransomware Case)

```
plaintextCopyEdit[Incident Detected]
    ↓
[Contain & Preserve Evidence]
    ↓
[Conduct Risk Assessment]
    ↓
[Determine if PHI was Accessed/Exfiltrated]
    ↓
[If breach → Notify HHS/OCR + Affected Individuals]
    ↓
[Engage Legal + Negotiation Experts]
    ↓
[Decide Whether to Pay Ransom]
    ↓
[If paid → Justify + Document + Monitor Systems]
    ↓
[Post-Incident Review & Compliance Updates]
```

✓ Best Practices for HIPAA-Aligned Response

Practice	Benefit
□ Full audit trail	Protects you during HHS OCR investigations
□ Least-privilege access control	Reduces risk of future PHI compromise
□ Regular tabletop exercises	Trains staff in ransomware drills + compliance response

📖 Updated risk analysis & policy	Prevents repeat findings in post-breach OCR reviews
☐ Use of sanctioned screeners	Prevents violation of OFAC guidelines (e.g., if attacker is on a sanctions list)

☐ Key Takeaways

- HIPAA-compliant ransomware response demands **fast action**, **clear documentation**, and **patient-first decision-making**
- **Ransom payment is not illegal**, but it must be **risk-justified**, **legally vetted**, and **properly reported**
- Notification timelines and privacy safeguards are **non-negotiable under HIPAA**
- Negotiation should always be conducted by **trained experts**, not internal IT or staff

Regulated Sector Incident Management

9.2.1 Medical Device Phishing Vectors (IoT Risks)

“Every connected device is a potential backdoor to patient care.”

What Are Medical Device Phishing Vectors?

Medical Device Phishing Vectors refer to attack surfaces where social engineering and phishing tactics are used to:

- Exploit networked or IoT-enabled medical equipment
- Manipulate the healthcare personnel managing these devices
- Gain lateral access to hospital systems, Electronic Health Records (EHRs), or protected health information (PHI)

These attacks target human weaknesses around complex devices—where users may click, scan, or connect without verifying.

Common IoT-Phishing Attack Paths

Vector	Phishing Scenario Example
Fake firmware update emails	“Critical update for your insulin pump controller. Click here to download patch.”
QR-code based calibration	QR codes stuck on devices lead to credential-harvesting sites
Fake service technician calls	Attackers pose as biomedical support, tricking staff into granting remote access
Supply chain compromise	Vendors send tampered USB updates or infected companion apps
Web interface phishing	Doctors are emailed fake login pages for cloud-connected imaging devices
Rogue mobile apps	Fake apps mimicking infusion pump controllers or EHR viewers
Internal spear-phishing	Emails target specific nurses or clinical engineers who manage connected gear

Why Medical Devices Are Prime Targets

Reason	Impact
--------	--------


⚙️ Device ubiquity	From MRI machines to pacemakers, thousands of devices are connected
⚡ Clinical urgency	Staff often bypass safety checks under pressure
✖ Weak authentication	Legacy or factory-default passwords still in use
🏠 Poor segmentation	Devices often share the same flat network as admin systems
🔧 Low patching discipline	Updating firmware may risk voiding certification or disrupting treatment
🔍 High-value PHI collection	Devices log diagnostics, patient profiles, and usage patterns

⚠️ Red Flag Behaviors Exploited





Behavior	Phishing Risk
🕒 Clicking urgent alerts	“Device update required in 15 mins or connectivity will fail.”
🔑 Using default admin portals	Pre-auth login pages mimic real interfaces
📎 Opening unverified attachments	Fake vendor invoices with infected PDFs targeting biomedical teams
📱 Scanning random QR codes	Placed on IV pumps, lab equipment, or even hospital signage
🏢 Trusting “known vendors”	Attackers spoof familiar equipment brands or reseller logos

🛡️ Defensive Strategies: Technical + Human

Defense Layer	Practice
🔌 IoT Segmentation	Put medical devices on isolated VLANs/firewalled zones
🔒 Phishing Simulations	Role-specific tests for biomedical engineers, nurses, radiologists
👁️ Visual Verification Protocols	Require badge-based identity checks for in-person support
⚙️ Patch Management Policy	Only apply verified updates from signed sources with offline validation
🔍 Audit Logs & Monitoring	Track login anomalies on device portals or mobile apps
📱 Mobile App	Allow only official, vetted apps on hospital-

Whitelisting	provided devices
 Just-in-Time Microtraining	“Pause before you patch” protocols for device updates and links

Specialized Training for Healthcare Staff

Role	Key Awareness Area
 Nurses & Clinicians	QR code threats, spoofed app warnings, suspicious USB/media
 Biomedical Engineers	Web interface credential hygiene, firmware validation
 IT Administrators	Patch cycles, firmware rollback plans, network zoning
 InfoSec / Compliance Teams	Incident triage, breach notification flow, HIPAA + FDA overlap

Standards & Regulations to Align With

Standard / Guidance	Relevance
HIPAA Security Rule	Requires protection of devices storing/transmitting PHI
FDA Premarket Guidance for Cybersecurity in Medical Devices	Details software lifecycle and update hygiene expectations
NIST SP 800-53 (rev. 5)	Provides controls for IoT segmentation, monitoring, and access
ISO/IEC 80001-1	Risk management of medical IT networks

Key Takeaways

- Medical device phishing attacks blend **technical exploitation** with **human manipulation**
- Vulnerable points include **updates, QR codes, web interfaces**, and **vendor trust chains**
- Best defense includes a **segmented infrastructure, staff training**, and **rigorous update controls**
- Attackers target not just data—but **continuity of care**
- Responses must align with **HIPAA, FDA, and patient safety** obligations

Regulated Sector Incident Management

9.2.2 Telemedicine Exploits: Fake Patient Portal Tactics

“The front door to care is now digital—and attackers are standing on the porch.”






What Are Fake Patient Portal Tactics?

Fake patient portal tactics are a type of **social engineering and phishing strategy** in which attackers clone or mimic legitimate telehealth platforms to:

- Harvest patient login credentials
- Steal sensitive health records (PHI)
- Inject ransomware or malware through fake updates
- Perform insurance fraud or identity theft

These portals often resemble those used by **MyChart, FollowMyHealth, Teladoc, Amwell**, or local hospital systems.

Why Patient Portals Are Targeted

Reason	Exploitable Opportunity
 Centralized PHI access	One login unlocks full EHR, test results, prescriptions
 Appointment urgency	Patients are eager to check results or join virtual consults
 Email & SMS dependency	Telehealth platforms rely on digital notifications
 Trust in healthcare brands	People don’t expect fake “doctor login” pages
 Expanding user base	More elderly, rural, and low-tech users entering telemedicine

Common Fake Portal Attack Methods

Vector	Description
Spoofed login pages	Cloned portals with legit logos and domain typos (mychart-logn.com)

Fake appointment alerts	Emails/texts with “Confirm Your Visit” links → phishing site
Fraudulent password resets	“Reset your patient portal password due to suspicious activity”
Deepfake chatbot popups	Fake AI-based chat agents asking users to “reverify identity”
Malicious mobile apps	Lookalike apps on Android stores disguised as telehealth tools
QR code phishing on flyers	QR codes in hospitals leading to spoofed scheduling pages

□ Anatomy of a Telemedicine Phishing Attempt

1. □ **Lure**
 - Email: “Your lab results are ready. Log in to review.”
2. □ **Redirect**
 - Links to fake portal (very close domain name or styling)
3. □‡ **Credential Harvest**
 - Captures username, password, 2FA if possible
4. □ **Exploit**
 - Logs into real portal, harvests data, injects insurance claim forms
5. □ **Optional Payload**
 - May deliver malware under guise of “health record download”

⚠ Red Flags for End-Users

Indicator	What to Watch For
🔍 URL mismatches	Domains with typos, added dashes, .net instead of .org
⌚ Expiring time pressures	“Link will expire in 15 minutes!”
🔑 Unusual verification steps	Asking for full SSN, card number, or insurance credentials
📄 Medical grammar errors	Poor formatting, awkward phrasing like “Doctor results await”
📎 Unexpected attachments	PDFs or ZIP files claiming to contain x-rays or blood test reports

□ Defensive Measures for Healthcare Providers

Implementation Suggestion

Control Type

📄 Patient Education Campaigns	Posters, texts, and portal banners warning against fake sites
🔍 Domain Spoof Monitoring	Use services like Proofpoint or ZeroFox to track similar domains
✉ Email/SMS Filtering	Scan for common bait phrases like “lab results,” “reschedule,” etc.
📱 Official App Promotion	Enforce trusted mobile app use via QR codes or Play Store links
🔑 2FA Enforcement	Require strong authentication for all portal access
🛡 SSO & OAuth Hygiene	Avoid open redirects and token replay attacks
🕒 Session Behavioral Monitoring	Detect abnormal access patterns or credential stuffing attempts

📖 HIPAA Implications

- **Unauthorized PHI access** via phishing = **reportable breach**
- Providers must:
 - Log **attempted and successful access**
 - Notify affected users if **data compromise** occurred
 - Document **training, controls, and mitigation efforts**

Failure to secure a portal—even if cloned—can still reflect **risk under HIPAA’s Security Rule**.

📌 Key Takeaways

- Fake patient portals exploit **trust, urgency, and digital inexperience**
- Tactics range from **lookalike domains** to **fake app stores**
- Defenses must combine **patient awareness, domain intelligence, and technical hardening**
- Under HIPAA, even **attempted social engineering** carries **disclosure and audit implications**

Regulated Sector Incident Management

9.2.3 EHR System Credential Harvesting

“A single login can expose the entire hospital.”

❑ What Is EHR Credential Harvesting?

EHR (Electronic Health Record) credential harvesting is a targeted cyberattack tactic where threat actors **steal usernames and passwords** of healthcare professionals to access **sensitive medical systems**. These credentials can:

- Unlock access to **PHI** (Protected Health Information)
- Enable **billing fraud**
- Be used in **ransomware deployment**
- Create **persistent backdoors** via legitimate user accounts

This attack **often starts with phishing, vishing, or malware**, but may also include credential stuffing or insider manipulation.

❑ Why EHR Systems Are High-Value Targets

Reason	Exploitable Benefit to Attackers
🔑 All-in-one access	One login = diagnostics, billing, imaging, prescriptions
🏛️ Regulatory value	HIPAA penalties & lawsuits make extortion easier
💰 Monetizable data	PHI fetches \$1000+ per record on dark markets
💳 Financial crossover	Access to insurance, payment, and SSN details
❑ Persistent credentials	Medical staff reuse passwords across departments/devices

🔗 Common Harvesting Methods

Attack Vector	Description
Phishing Emails	“You’ve been logged out of Epic. Click to re-authenticate.”
Fake EHR Portals	Cloned login pages for Cerner, Epic, Allscripts, Meditech

QR Code Phishing	Posters/flyers with QR links to fake mobile logins
Vishing (Phone Call Spoofing)	“This is IT—your credentials have expired. What’s your login?”
Credential Stuffing	Reuse of breached passwords from unrelated platforms
Keylogging Malware	Delivered via email or USB, records user input into EHR systems
Session Hijacking	Steals session tokens from shared computers or outdated browsers

🔍 Anatomy of a Credential Harvesting Attack

1. 📧 **Email Spoof**
 - “Your Epic session has timed out. Log in again to avoid record loss.”
2. 🔗 **Phishing Link**
 - Leads to domain like `ehr-updateportal.com`
3. 📝 **Credential Entry**
 - Username + password harvested immediately
4. 👤 **Attacker Login**
 - Uses credentials to explore real EHR system
5. 📤 **Exfiltration or Monetization**
 - Exports PHI, injects billing fraud, or drops ransomware

⚠ Behavioral Red Flags to Monitor

User Action	Suspicious Indicator
🕒 After-hours login	Unusual time access from non-privileged user
🌐 Remote geolocation	Logins from IPs outside hospital region
🔑 Repeated login failures	Indicates password guessing or credential stuffing
⌚ Long idle sessions	May indicate hijacked sessions
📄 Sudden bulk record exports	Unusual activity from billing staff or clinicians

🛡 Defensive Strategies

Layer	Control
🔒 Multi-Factor Authentication	Enforce across all staff and device types

📍 Geofencing & IP filtering	Limit access to approved physical zones/networks
📊 SIEM-based anomaly detection	Flag deviations in login patterns, session length
📧 Phishing simulation campaigns	Test awareness using EHR-themed attacks
📅 Just-in-time training	Post-click microtrainings for those who fail drills
👁️ Login CAPTCHA or device binding	Prevents automated attacks and session abuse
🔍 Audit logs with alerting	Enable fine-grained visibility and compliance tracking
🔄 Regular credential rotation	Especially for admin, billing, and IT roles

🔒 HIPAA & Regulatory Requirements

Requirement	What It Means
📋 Audit Controls	Must track access to PHI, including who, when, and why
🔑 Access Control Policy	Limit user access based on job role (least privilege)
📢 Breach Notification Rule	Must notify patients, OCR, and media if PHI is compromised
🛡️ Security Rule Compliance	Required safeguards include technical, physical, and administrative controls

🧠 Psychological Manipulation in EHR Scams

Social Engineering Hook	Impact
“You’ve been locked out.”	Panic creates urgency
“Your records are incomplete.”	Triggers concern about patient safety
“We’re migrating to a new platform.”	Confusion enables manipulation
“This is the security team.”	Authority bias leads to over-compliance

🔑 Key Takeaways

- Credential harvesting against EHRs is a **human-first attack** with technical consequences
- Targets include doctors, nurses, administrative staff, and billing teams
- Defense requires **layered authentication, smart monitoring, and social engineering resistance**
- A single login compromise could **breach HIPAA and impact patient care**

Financial Infrastructure Safeguards

10.1.1 SWIFT Network Protections: Transaction Verification Dual-Control Systems

“In the world of high-value transfers, one human isn’t enough.”

□ What Is SWIFT? Why Protect It?

The **SWIFT network** (Society for Worldwide Interbank Financial Telecommunication) is a **global financial messaging system** used by over 11,000 institutions to process trillions in daily transactions.

While SWIFT itself doesn’t move money, it **facilitates bank-to-bank communication** (e.g., fund transfer requests). Attackers target:

- **Credentials to initiate fraudulent SWIFT messages**
 - **Lax internal approval workflows**
 - **Insecure endpoints connected to SWIFT**
-

□ What Are Dual-Control Systems?

Dual-control systems are security protocols that require **two or more authorized individuals** to verify, approve, or release a sensitive transaction—**before it is submitted to SWIFT**.

They act as a **human firewall** against:

- Fraud
- Insider threats
- Credential misuse
- Malware-injected SWIFT messages

If one user is compromised, the system won’t execute without **independent second-party validation**.

✂ How Dual-Control Systems Work

Phase	Description
□ Message Drafting	Operator A enters SWIFT message (e.g., MT103) into system Operator A verifies and digitally signs with a secure

👁 **First Review** token

✓ **Second Approval** Operator B independently reviews transaction details

📄 **Release to SWIFT** Only after dual consent, the system releases the message

Often paired with:

- **Hardware tokens / smartcards**
- **Privileged session monitoring**
- **Transaction whitelisting**
- **Segregation of duties (SoD)**

📄 **Why This Matters: Real-World Breach Examples**

Case	What Went Wrong
Bangladesh Bank Heist (2016)	Malware manipulated SWIFT interface; no second-layer checks
Ecuador Banco del Austro (2015)	\$12M stolen via forged SWIFT messages using stolen credentials
Nepal Rastra Bank (2017)	Internal lack of review allowed rogue SWIFT transfers

💡 **SWIFT CSP (Customer Security Programme) Requirements**

To be SWIFT-compliant under its CSP, banks must implement:

SWIFT Control ID	Description
2.4 - Logging and Monitoring	Detect suspicious SWIFT transactions
5.1 - Logical Access Control	Limit access to only authorized operators
6.2 - Transaction Integrity	Dual controls for payment creation, modification, and release
6.3 - Operator Session Restrictions	Time/session-based access limits

📄 **Roles Involved in Dual-Control Enforcement**

Role	Responsibility
------	----------------

SWIFT Operator (Initiator)	Creates or edits transaction messages
SWIFT Approver (Reviewer)	Validates and releases messages after review
Security Administrator	Manages access policies and cryptographic tools
Compliance Officer	Ensures system meets CSP, AML, and internal audit rules
Auditor	Reviews logs for SoD violations and privilege abuse

□ Technology & Tools That Support Dual-Control

Tool / Control	Function
□ Role-Based Access Control (RBAC)	Enforces strict segregation between initiators and approvers
□ AI-Based Anomaly Detection	Flags transactions that deviate from norms (e.g., timing, amount)
□ Predefined Approval Limits	Escalation required if transaction > X amount
□ Transaction Simulation Tools	Run “dry runs” to test fraud detection and approval workflows
🔍 SIEM Integration	Monitor login patterns, approvals, and exception triggers

□ Key Takeaways

- Dual-control systems are **non-optional safeguards** in SWIFT environments
- They help prevent fraud by introducing **independent human verification**
- Compliance with **SWIFT CSP, internal audit, and AML protocols** relies on dual-control enforcement
- Technical enforcement must be backed by **training, rotation, and audit visibility**

AI-Augmented Social Engineering

11.1.1 Generative Phishing: GPT-Phish Campaign Case Studies

“AI doesn’t just write essays—it writes convincing lies at scale.”

▣ What Is GPT-Phish?

GPT-Phish refers to phishing campaigns enhanced or entirely generated using **large language models (LLMs)** like GPT. These campaigns:

- Use **highly personalized language**
- Can auto-generate **hundreds or thousands of unique phishing emails**
- Mimic specific **tone, syntax, industry jargon, or sender persona**

Instead of crude scam emails, attackers now send **linguistically perfect, highly contextual messages** at enterprise scale.

▣ Case Study 1: HR Payroll Phishing via GPT Clone

▣ **Target:** Mid-sized HR department of a healthcare group

🔗 **Tactic:**

- GPT-generated phishing emails mimicked internal HR communications
- Included precise references to **benefits plans, open enrollment deadlines**, and **employee first names**

▣ **Key Indicators:**

Feature	Human-Like Detail
▣ Tone	“Just a reminder to select your 2024 health options.”
▣ Context	Referenced actual HR provider (e.g., Cigna, Aetna)
▣ Malicious Link	Fake portal styled as “Workday” login page
📊 Result	38% click rate, 12% credential submission

▣ Case Study 2: Vendor Invoice Spear-Phishing

📌 **Target: Procurement officers in logistics firm**

💡 **Tactic:**

- GPT-powered email mimicked a known vendor
- Included real invoice templates, shipment references, and a “payment update form”

🔍 **Phishing Hooks:**

Element	Customization Level
📦 Vendor tone	“Please find the attached shipping log and remittance advice.”
📎 Attachment style	Excel file with macro payload named “Q2_Balance_Review.xlsx”
🔍 Metadata spoofing	Used cloned email signature, logo, and reply-to header
📁 Outcome	2 compromised finance logins, \$118k wire transfer blocked just in time

📌 **Case Study 3: CEO Executive Impersonation via GPT**

📌 **Target: Assistant to CEO at a fintech startup**

💡 **Tactic:**

- Email mimicked CEO’s writing style using GPT prompts like:
“Write like a busy but polite startup executive asking for a document review under time pressure.”

📧 **Email Content:**

“Hey — I need you to urgently go through the attached equity package and send it to legal before noon.
Please don’t loop in anyone else for now — it’s a sensitive investor matter.”

📎 **Attachment:** Malicious PDF → Remote Access Trojan (RAT)

📌 **Result:**

- Assistant opened file on shared workstation
- RAT accessed investor presentation files + M&A planning docs

❏ Why GPT-Phish Works So Well



Capability	Advantage to Attackers
❏ Contextual Fluency	GPT can match tone, subject, even slang used by targets
❏ Email Personalization	Auto-injects names, project references, sender traits
🕒 Rapid Scaling	Thousands of variations generated in minutes
❏ Document Generation	AI can also write fake invoices, HR forms, or press releases
❏ Multilingual Delivery	Fluent phishing in dozens of languages

❏ Mitigation Techniques for AI-Generated Phishing

Layer	Defense Strategy
❏ Linguistic Anomaly Detection	NLP-based filters to flag unnatural variability patterns
🔗 Email Fingerprinting Tools	Detect structure similarity across “unique” GPT emails
❏ Content-Aware Filters	Scan attachments and embedded URLs for evasive payloads
❏ Role-Based Email Hygiene Training	Tailored for HR, Finance, Executive Assistants
❏ Phishing Simulations (AI-style)	Use AI to train against AI-based threats
❏ Behavioral Threat Models	Identify suspicious behavior post-click (e.g., strange logins, access spikes)

⚖️ Regulatory & Ethical Implications

Concern	Relevance
❏ LLM Misuse Policies	Enterprises must set boundaries on how internal LLMs can be used
⚠️ Attribution Difficulty	AI-generated emails leave little forensic signature

 Liability Shift	Failure to recognize or mitigate known AI-based threats may carry legal risk
 Content Responsibility	LLMs used in phishing may become part of future criminal and civil cases

□ Key Takeaways

- GPT-powered phishing is **adaptive, hyper-personalized, and scalable**
- Real-world campaigns have already bypassed legacy filters and fooled professionals
- Defenses must include **linguistic detection, human training, and AI-informed policy shifts**
- If AI is writing the phish, AI must help detect it

AI-Augmented Social Engineering

11.1.2 Personalized Lure Generation Engines

“It doesn’t just know your name—it knows what you care about.”






▣ What Are Personalized Lure Generation Engines?

Personalized lure generation engines use AI, data mining, and behavioral analytics to craft **hyper-targeted phishing or social engineering messages**. These lures exploit:

- A target’s job role, relationships, online behavior
- Recent activities, preferences, or language use
- Public or breached data (LinkedIn, GitHub, past leaks, social media)

Unlike mass phishing, these engines generate **individualized bait**, making attacks harder to detect and more likely to succeed.

▣ How It Works: End-to-End Attack Pipeline

Stage	Description
 Data Harvesting	Gathers open-source intel (OSINT), LinkedIn bios, conference talks, GitHub posts
 Behavioral Profiling	Analyzes interests, tone, habits (e.g., uses Outlook, posts on Medium)
 AI Prompting	Uses templates like: <i>“Write a calendar invite from [CEO] to [target] referencing [event] in a casual tone.”</i>
 Lure Generation	Produces custom phishing email, document, voice call script, or fake webpage
 Payload Delivery	Delivered via email, chat apps, social DMs, or fake scheduling links

▣ Example Scenarios

▣ Case Study 1: Tech Employee Job Scam

- **Target:** Senior engineer actively job hunting
- **Input Data:** GitHub profile, Medium blog, recent Twitter activity
- **Lure:**

- Email from “Meta Recruitment” about a remote AI role
- Custom PDF with fake NDA (embedded malware)
- Included compliments on a specific open-source repo

▣ Case Study 2: CFO Invoice Fraud

- **Target:** CFO at a B2B SaaS firm
- **Input Data:** Quarterly investor call transcript, LinkedIn, Form D filing
- **Lure:**
 - Email from known vendor rep, referencing invoice + a recent earnings milestone
 - GPT-generated Excel sheet + embedded macro payload
 - Used same sign-off and wording as prior vendor threads (from past breach data)

▣ Case Study 3: Executive Assistant Quishing

- **Target:** Executive assistant at a luxury goods brand
- **Input Data:** Instagram stories, past travel photos, office blog posts
- **Lure:**
 - Printed QR flyer for “exclusive luxury retreat” left on desk
 - QR led to fake travel portal phishing page
 - Page mimicked company’s booking system and captured credentials

💡 Why These Engines Are Dangerous

Strength	Attack Benefit
▣ Contextual Relevance	Increases trust and emotional engagement
✍️ Language Imitation	Matches known writing styles (CEO, HR, vendor)
🕒 Scalability via AI	Can auto-generate lures for hundreds of employees simultaneously
▣ Multi-Channel Output	Works across email, SMS, Slack, WhatsApp, social media
🌀 Bypasses Generic Detection	No boilerplate phrasing, each lure is linguistically unique

▣ Defensive Strategies

Layer	Protection Method
-------	-------------------

🔍 Linguistic Fingerprinting	NLP tools to spot synthetic but non-human phrasing
📧 Zero Trust Email Gateways	Evaluate message context, not just source and sender
🎓 Context-Aware Phishing Training	Teach staff to spot ultra-specific, emotionally crafted lures
🔒 Public Exposure Minimization	Limit detailed role/job/project data in public bios
📊 Digital Exhaust Monitoring	Track where employee details are being scraped or sold
🎭 Deception Decoys	Honeypot social profiles or dummy emails to lure attacker activity
🚨 Just-In-Time Alerts	Prompt staff when their name/project is trending on attacker forums or OSINT aggregators

🛠️ Toolkits & Techniques Used by Attackers

Tool / Method	Purpose
🕸️ <i>Maltego, SpiderFoot, Recon-ng</i>	OSINT automation on targets
🗨️ <i>ChatGPT, LLM APIs, Custom Prompt Chains</i>	Natural-language lure creation
📄 <i>Fake Invoice/Offer Generators</i>	Auto-generate PDFs, job letters, or invites
🌐 <i>Social Graph Mapping</i>	Map out professional connections for BEC-style targeting
📅 <i>Calendar API Exploits</i>	Inject phishing into shared meeting invites

⚖️ Ethical and Legal Ramifications

Concern	Relevance
🔍 Deep Profiling of Targets	May violate data privacy or surveillance laws
🤖 AI Weaponization	Enterprise LLM misuse may fall under insider threat governance
🏛️ Data Compliance Breaches	Use of scraped or breached info could trigger GDPR/CCPA fines
🕵️ Attribution Barriers	Generative attacks are harder to link to origin or pattern

□ Key Takeaways

- Personalized lures powered by AI are **highly effective, scalable, and evasive**
- Attackers combine **OSINT, LLMs, and payload automation** to mimic trust relationships
- Defenses must shift from **static rules to dynamic, context-aware analysis**
- Awareness training must emphasize **personalization tactics**, not just “bad grammar” red flags

Emerging Threat Vectors

11.2.1 Quantum Computing Risks: Post-Quantum Cryptography (PQC) Migration

“Quantum computers won’t break the internet overnight—but they will if we wait too long.”

What Is the Quantum Threat?

Quantum computers—especially large-scale, fault-tolerant ones—pose a unique threat to current digital security. They can break widely used encryption systems by exploiting their **immense parallel processing power**.

Traditional Crypto	Quantum Threat Example
RSA (e.g., 2048-bit)	Broken by Shor’s Algorithm —factorization
ECC (Elliptic Curve)	Also broken by Shor’s
AES	Safe (but vulnerable to Grover’s Algorithm which halves its effective key length)

Why It Matters

Quantum computers could:

- **Decrypt encrypted backups** stolen today (“Harvest Now, Decrypt Later”)
 - **Compromise TLS/SSL**, breaking website, VPN, and email privacy
 - **Forge digital signatures** (used in software, contracts, certificates)
 - Undermine **cryptocurrency security**, blockchain, and smart contracts
-

What Is Post-Quantum Cryptography (PQC)?

PQC refers to **encryption and digital signature algorithms** designed to resist quantum attacks. Unlike current public-key systems, PQC relies on problems **believed to be hard even for quantum computers** (e.g., lattice-based, code-based, hash-based schemes).

📅 PQC Migration Timeline

Phase	Milestone
⌘ 2016–2022	NIST launched a global competition for PQ-safe algorithms
✓ 2022–2024	Finalists selected (e.g., CRYSTALS-Kyber , Dilithium , FALCON)
📅 2024–2025	Testing & integration with real-world systems (TLS, VPN, email, blockchain)
📅 2025–2030	Mass adoption and transition phase (especially government & finance)

🏛️ Standards Bodies & Recommendations





Organization	Role
NIST (USA)	Leads PQC standardization; recommends Kyber for encryption and Dilithium for signatures
NSA	Mandated transition for national security systems
ENISA (EU)	Advises migration timelines and sector-specific implementations
ISO/IEC	Working on cryptographic protocol updates
IETF	Integrating PQC into TLS, SSH, DNSSEC, S/MIME

🔑 Common Post-Quantum Algorithms







Function	Recommended PQC Algorithm (as of 2025)
🔑 Key Exchange	CRYSTALS-Kyber (lattice-based)
✍️ Digital Signatures	CRYSTALS-Dilithium , FALCON , SPHINCS+
🔒 Hybrid TLS	Kyber + traditional ECDHE (for smoother transition)
📁 File Encryption	Hybrid AES + PQ wrapper (AES for speed, PQC for key wrapping)

⚠️ Migration Challenges






Challenge	Risk / Issue
🔄 Backward compatibility	PQC not yet supported in legacy devices/software

 Resource overhead	PQC operations are often slower or larger in size
 Algorithm trust maturity	PQC algorithms are newer and less battle-tested
 Deployment complexity	Requires updating protocols, certificates, firmware
 Long-term secrecy risk	Data encrypted today could be vulnerable in 10–15 years

♥ Best Practices for PQC Readiness

Action	Purpose
 Crypto Inventory Audit	Identify where vulnerable algorithms (RSA/ECC) are used
 Hybrid Crypto Implementation	Use both classical + PQ crypto during transition phase
 Pilot Deployments	Test PQC in VPN, email, and certificate infrastructure
 Vendor PQC Readiness Assessment	Ensure software and hardware vendors offer PQ-safe options
 Agile Key Rotation Policies	Prepare for future-proof cryptographic agility
 Quantum Risk Modeling	Quantify data-at-rest exposure timelines

Use Cases at Risk

Sector	Quantum Risk Scenario
 Finance	Smart contracts, token signing, payment gateway certs
 Communications	End-to-end encryption in email, VoIP, chat apps
 Healthcare	Patient data stored in encrypted archives
 Web Infrastructure	TLS certificates for websites, CDNs, VPNs
 Defense/Gov	Classified data with 20–50 year secrecy requirements

Key Takeaways

- Quantum computers may not be ready yet—but the **crypto migration needs to begin now**
- PQC algorithms like **Kyber and Dilithium** will replace RSA/ECC in secure systems
- The transition must be **phased**, using **hybrid models and crypto agility**
- Sectors with long-term data confidentiality (e.g., gov, finance, healthcare) should **act first**
- The threat is **real, silent, and time-sensitive**: data stolen today may be decrypted tomorrow

Quantum Computing Risks






11.2.2 Q-Day Preparedness Checklists

“Q-Day” = the day quantum computers can break today’s cryptography.




What Is Q-Day?

Q-Day refers to the point in time when quantum computers become powerful enough to **break widely used public-key cryptography** (e.g., RSA, ECC). While estimates vary (2030–2045), **data being stolen today can be decrypted then, so preparation must begin now.**

Executive-Level Q-Day Preparedness Checklist

Focus Area	Action Item
 Strategic Awareness	Ensure C-suite understands what Q-Day is and its business impact
 Risk Assessment	Include quantum threats in enterprise cyber risk models
 Data Longevity Mapping	Identify data that must stay secure for 10–30 years
 Board Reporting	Include post-quantum risk in cyber governance updates
 Industry Monitoring	Track NIST, NSA, ISO, and sector-specific PQC guidance

Technical Cryptography Audit Checklist

System/Protocol Area	Action Item
 Crypto Inventory	Identify all uses of RSA, ECC, DH, DSA, etc. across your systems
 Certificate Infrastructure	Map where TLS certificates and digital signatures are used (web, email, code)
 Encrypted Archives	Locate long-term encrypted backups, files, databases

🔒 VPN & Comms	Audit encryption in VPNs, VoIP, and messaging apps
💰 Financial Transactions	Check cryptography in payment gateways, blockchain wallets
📶 IoT Devices	Note hardcoded keys or legacy crypto that may be unpatchable

🔒 PQC Transition Preparation Checklist






Category	Action Item
🔒 Crypto Agility	Ensure systems can switch algorithms without reengineering entire platforms
🔒 Pilot PQC Algorithms	Test NIST finalists (Kyber, Dilithium, FALCON) in lab environments
🔗 Hybrid Deployment	Implement dual classical + post-quantum algorithms (e.g., hybrid TLS)
🔒 Key Rotation Planning	Prepare for large-scale key rollover events
👤 Third-Party Crypto Reviews	Evaluate vendor readiness and crypto lifecycle support
👥 Staff Training	Upskill teams on PQC standards and crypto hygiene

🔗 Vendor & Supply Chain Checklist






Dependency Area	Action Item
📦 Critical Vendors	Ask suppliers: “What’s your Q-Day migration roadmap?”
🔒 PKI/CA Providers	Confirm if your certificate authorities will offer PQC certs
☁️ Cloud & SaaS Platforms	Demand transparency on PQC support for cloud storage, mail, collaboration tools
📄 Contracts & SLAs	Add clauses that require PQC readiness and crypto agility
🗂️ Risk of Inherited Insecurity	Assess if vendors store or transmit your long-term sensitive data

🔒 Compliance & Policy Checklist

Regulation Area

Action Item	
 Government Regulations	Monitor compliance with NSA, NIST, GDPR, HIPAA, or sector-specific guidelines
 Data Classification	Mark datasets that require >10-year confidentiality as PQ-priority
 Security Policies	Update encryption, key management, and data retention policies
 Incident Response Playbooks	Prepare for future “Q-Day-leveraged” data breach escalations
 Awareness Campaigns	Train staff on emerging threats like “harvest-now, decrypt-later”

Red Team/Blue Team Simulation Checklist

Security Practice Area	Simulation Element
 Red Team	Attempt data exfiltration simulating HNDL (Harvest Now, Decrypt Later)
 Blue Team	Simulate PQC key rotation drills
 Patch Simulation	Test firmware updates for crypto-switching in IoT/embedded systems
 Log Analysis	Train detection systems to identify future post-quantum payloads
 Deception Infrastructure	Deploy honeypots with “quantum-bait” to watch future adversary interest

Key Takeaways

- Q-Day **is coming**—uncertain when, but certain *that*
- If you store long-term sensitive data (finance, healthcare, legal, national security), you must **act now**
- Inventory → Audit → Pilot → Transition → Monitor = your Q-Day roadmap
- Post-quantum security is not just cryptographic—it’s **strategic, operational, and vendor-based**

Incident Response Protocols

12.1.1 Triage Procedures: Compromised Account Containment Ladders

“Respond fast. Contain smarter. Escalate wisely.”

▢ What Is a Containment Ladder?

A **Compromised Account Containment Ladder** is a **tiered, stepwise response model** used to **isolate, control, and neutralize user account compromises** based on:

- Severity of the compromise
- Business role and privilege level
- Real-time threat behavior

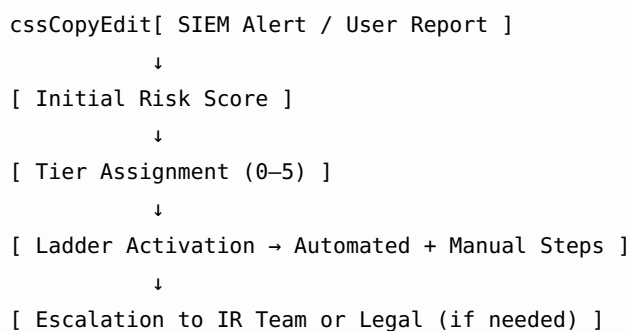
This ladder approach ensures that containment is **proportional**, **automated where possible**, and **escalated quickly when needed**.

🔑 Containment Ladder Tiers

Tier	Name	Trigger Conditions	Actions Taken
0	Suspicion (Soft Signal)	Unusual login (geo/time anomaly), flagged email behavior, MFA fails	- Silent monitoring (SIEM alert) - Increase MFA challenge - Log anomaly in user risk profile
1	Early Containment	Confirmed login from suspicious IP/device, phishing link click	- Revoke active session tokens - Reset password (force user login) - Notify user and helpdesk
2	Moderate Compromise	Email forwarding rule set, suspicious OAuth app, internal phish sent	- Block email/calendar access - Isolate device (if enrolled in EDR) - Notify SOC and start forensic snapshot

3	High-Risk Access	Admin credentials, finance systems, vendor portals affected	<ul style="list-style-type: none"> - Lock account and escalate to IR lead - Revoke federated auth tokens (SSO, O365, G-Suite) - Log off all sessions across SaaS, VPN, endpoint - Global password reset + YubiKey required
4	Lateral Movement Detected	Credentials used on multiple systems or detected in attacker tooling (C2)	<ul style="list-style-type: none"> - Suspend AD account / domain trust temporarily - Block associated IP addresses and create IOCs
5	Privilege Abuse/Exfiltration	Data accessed/downloaded from HR, Legal, or IP systems	<ul style="list-style-type: none"> - Trigger breach notification playbook - Perform legal review + DLP logging - Full digital forensics and incident closure

□ Containment Decision Flow



✂ Tools Commonly Involved at Each Tier

Tier Level	Tool Examples
0–1	Azure Risky Sign-In Reports, Okta Behavior Detection, Proofpoint TAP CrowdStrike / SentinelOne (EDR), M365 Purview (audit logs),

2–3	Google Admin SDK
4–5	Splunk SOAR, EnCase Forensics, Varonis, FTK Imager, Tanium, or XDR platforms

□ Why Use a Ladder Model?

Benefit	Description
□ Repeatable Playbooks	Teams can respond consistently without reinventing steps each time
⚖ Proportional Response	Prevents overreacting to minor issues or underreacting to major ones
⚡ Automation-Friendly	Enables step-wise integration into SOAR (Security Orchestration tools)
📈 Improved Metrics & RCA	Each tier yields clearer KPIs for tracking containment speed and effectiveness

□ Example: Real-World Application

□ Scenario: Employee clicks credential phishing email, logs in from Nigeria

- **Tier Triggered:** Tier 2
- **Actions Taken:**
 - O365 access revoked
 - MFA reset
 - Login sessions purged
 - User notified & re-onboarded after credential hygiene training

□ Key Takeaways

- A **containment ladder** lets teams respond faster and smarter to account takeovers
- Tiered responses balance **security, user friction, and investigation depth**
- Integration with SOAR/XDR makes this process **scalable and semi-automated**
- As threats escalate (e.g., BEC, exfiltration), the ladder ensures proper **legal and forensic escalation**

Advanced Adversary Tactics

12.2.1 Threat Actor Communication Protocols

“The way attackers talk reveals how far they’ve already infiltrated.”

❑ What Are Threat Actor Communication Protocols?

These refer to **structured communication methods and behavioral patterns** used by threat actors—especially ransomware groups, APTs, and cyber extortionists—when interacting with victims, between themselves, or with intermediaries.

They can involve:

- Ransomware negotiations
- Phishing follow-up emails
- Social engineering back-and-forth
- Internal C2 (command-and-control) messaging
- Dark web market communications
- AI-assisted deception scripting

Understanding these protocols improves **attribution, containment, and negotiation response**.

❑ Common Communication Channels Used

Channel Type	Use Case	Common Tools/Examples
❑ Encrypted Chat	Ransomware negotiation, C2 comms	TOX, Jabber, Signal, Element (Matrix)
❑ Web Portals	Ransomware victim portals, data leak sites	Custom .onion sites or pastebin clones
❑ Email	BEC, phishing reply chains, extortion warnings	ProtonMail, Yandex, Tutanota, fastmail
🌐 Dark Web Forums	Access broker sales, data auctions	Exploit, RAMP, XSS, BreachForums clones
❑ Bots/Scripts	Auto-replies, payment instructions, scam support	Telegram bots, Discord fake support agents

▢ Typical Protocol Structures

▢ 1. Pretexting (Initial Social Engineering)

“Hi, I’m James from compliance—your credentials were flagged for review. Please reset them using the secure link below.”

- Often **scripted**, using natural language or GPT-generated
- Timed to exploit work hours, holidays, or high-stress periods

📦 2. Ransomware Negotiation Phases

Phase	Communication Behavior
▢ Initial Hook	Friendly tone (“We’re willing to cooperate...”)
▢ Price Setting	High ransom with discount promises (“30% if paid in 48h”)
▢ Proof of Breach	Screenshots of stolen data, test decryption of 1 file
🔊 Escalation	Threat of public leak or reaching media/regulators
⌚ Deadline Pressure	Timer countdowns, psychological stress tactics

🖥️ 3. BEC Thread Hijacks

- Attackers hijack real email threads (invoice, HR discussions)
- Insert **fake follow-up messages** in matched tone:

“Sorry for the delay—please use the attached updated bank details.”

- Often delay replies to mimic human response times
- May use **business hours**, typos, and regional greetings to blend in

🔪 4. Internal Threat Actor Comms (TTP Intelligence)

Captured from breaches of ransomware groups or law enforcement ops:

Communication Content	Purpose
Task delegation logs	“User XYZ handles negotiation, User ABC handles exfil”
Exploitation instructions	“Use Follina for lateral movement, then Cobalt Strike”
Progress updates	“Domain access confirmed, syncing files to host1...”

Financial splits	“50/50 after Monero clears, send wallet ID”
------------------	---

📋 Behavioral Patterns to Track

Signal	What It Suggests
🗨️ Formal vs. casual tone	Organized group vs. lone actor
🕒 Deliberate delay or timing	Human operator, timezone mimicry
📄 Repetition across incidents	Templated message = same threat actor
📄 Message reuse	Language reuse may tie to ransomware families
📍 Localization cues	Grammar, slang, currency, cultural hints

🔍 Forensic Techniques to Analyze Comms

Method	Purpose
📄 NLP + stylometry	Detect reused phrasing or tone patterns across incidents
✉️ Email header analysis	Reveal routing paths, fake reply-tos, and hidden C2 domains
🌐 Portal scraping	Track .onion ransomware portals, parse past messages
📄 LLM prompt fingerprinting	Analyze if GPT-like tools were used to generate lures
📦 Message metadata	Timestamps, file hashes, attachment behavior

🛡️ Response & Mitigation Practices

Situation	Response Action
📄 Ransom demand received	Use burner email for legal-controlled reply, engage IR & legal
📄 Email thread hijack	Notify all parties, review SPF/DKIM/DMARC, revoke credentials
📄 Bot-based comms	Block bot domains, log interaction paths for reverse-engineering
🌐 Leak site threat	Monitor data exposure, start breach notification timelines

□ AI-generated comms	Employ linguistic anomaly detection tools (NLP AI red-teaming)
----------------------	--

⚠️ Legal & Ethical Considerations

Concern	Risk Level	Guidance
Negotiating with actors	⚠️ Legal gray zone	Follow jurisdictional laws + legal counsel
Messaging back (baiting)	⚠️ Traceable risk	Should only be done under IR supervision
Paying ransom	! Sanction risk	Consult OFAC lists and legal teams
Threat actor impersonation	⚠️ Ethics issue	Avoid unless part of controlled deception ops

□ Key Takeaways

- Threat actor communication is often **scripted, stylized, and psychologically engineered**
- Monitoring and analyzing this communication provides valuable **intel for attribution and containment**
- Defenders must recognize **protocol patterns**, not just technical indicators
- Tools like **linguistic forensics**, **NLP analysis**, and **metadata correlation** are critical
- Legal and ethical lines must be **clearly defined in communication responses**

Forensic Investigation

12.2.1 Browser Artifact Analysis (IndexedDB, Cache)






“Your browser remembers more than you think.”

🔍 What Is Browser Artifact Analysis?

Browser artifact analysis involves extracting and interpreting **locally stored web data** from browsers to reconstruct user activity, uncover malicious scripts, detect exfiltration, or track phishing events. Key forensic sources include:

- **IndexedDB**: A client-side database for storing structured data
- **Browser Cache**: Temporary files, scripts, media, and pages
- **Cookies, LocalStorage, SessionStorage**
- **History & Downloads**

📦 Why IndexedDB and Cache Matter in Forensics

Artifact Source	What It Reveals
 IndexedDB	App-specific databases—used by modern apps like Gmail, ChatGPT, Outlook Web
 Cache	Cached JS, HTML, CSS, media files—shows accessed content & timestamps
 Timestamps	Help correlate attacker interaction timeframes
 Offline Data	IndexedDB may retain data even after logout or connection loss
 Payload Trace	Cache/IndexedDB may contain phishing pages, credentials, crypto wallet data, tokens

📁 Where These Artifacts Live

Browser	IndexedDB Path Example	Cache Path Example
Chrome	C:\Users\ [User Name]\AppData\Local\Google\Chrome\User Data\Default\IndexedDB	... \Cache\ or C:\Users\ [User Name]\AppData\Local\Google\Chrome\User Data\Default\Cache

(Windows)	[User]\AppData\Local\Google\Chrome\User Data\Default\IndexedDB	Service Worker\CacheSto
Firefox	...\Profiles\ [Random].default\storage\default\ (leveldb format)	...\cache2\entr
Edge	Follows Chrome paths (Chromium-based)	Same as Chrome

🔗 Forensic Tools to Extract & Analyze

Tool/Method	Use Case
🔍 Browser History Examiner	Visualize IndexedDB and Cache activity
📦 ChromeCacheView	Extract & timestamp Chrome cache contents
📦 DB Browser for SQLite	Open LevelDB/IndexedDB databases (manual method)
📦 Autopsy/Sleuth Kit	Full disk forensics + browser artifact modules
📦 Python (Shutil, LevelDB parsers)	Custom script parsing for IndexedDB

📋 Sample IndexedDB Use Cases in Threat Intel

🔑 Case 1: Webmail Token Harvesting

- Threat actor accesses corporate Gmail
- IndexedDB contains:
 - OAuth session token
 - Email draft cache (exfiltrated content)
 - Timestamps of login, drafts, and JS file origin

📦 Case 2: Fake Crypto Wallet DApp

- Malicious web app stores private keys in browser IndexedDB
- Forensics reveal:
 - IndexedDB entry for wallet ID and recovery phrase
 - Cache contains fake UI that mimics MetaMask
 - Timestamps match phishing email timeline

🔑 Case 3: QR Phishing Artifact

- QR code leads user to fake web app
 - Browser cache reveals:
 - Cached version of malicious landing page
 - ServiceWorker cache shows offline persistence
 - IndexedDB retains user email, input fields, device fingerprint
-

📁 Investigation Workflow

1. 📁 **Identify Target Browser(s)**
Review system logs or user reports for used browsers.
 2. 📁 **Isolate Browser Profile Directory**
Securely copy user's browser data directories (Chrome, Firefox, etc.)
 3. 🔍 **Extract IndexedDB**
Use LevelDB viewer, SQLite browsers, or specialized tools.
 4. 📦 **Analyze Cache + Service Worker Data**
Look for malicious JS, phishing HTML, injected payloads.
 5. 📁 **Correlate Artifacts with Timeline**
Link to login attempts, phishing emails, lateral movement, or session hijacking.
 6. 📁 **Preserve for Legal/IR**
Export copies of IndexedDB/Cache with hashes for evidentiary chain-of-custody.
-

♥ Detection & Defense

Defensive Technique	Description
📁 Auto-Clearing Sensitive Storage	Enforce browser hygiene on logout (IndexedDB, LocalStorage)
📁 Browser Hardening GPOs	Disable persistent storage for sensitive web apps
🔍 XDR/SIEM Integration	Alert on abnormal IndexedDB/storage access
📁 Behavioral Web Scanning	Detect unauthorized DApp clones or malicious cached JS
👤 End-User Training	Educate on dangers of QR-based or browser-based phishing

📁 Key Takeaways

- IndexedDB and browser cache are **goldmines of forensic insight** in phishing, session hijack, or web-based exfiltration
- Many modern apps (email, crypto, chat) **store sensitive session data locally** in these areas

- Forensic workflows should **include browser-level investigation** alongside network and memory analysis
- Automated tooling + timeline correlation is **critical** for threat reconstruction

Mobile Device Forensics

12.3.1 Mobile Device SMS Acquisition Techniques

“Text messages may be short—but forensics makes them speak volumes.”

Why SMS Matters in Forensics

SMS data can provide:

- **2FA codes** intercepted in account takeovers
- **Phishing or smishing messages** with malicious links
- **Ransomware negotiations or extortion messages**
- **Communication trails in insider threat cases**
- **Time-anchored evidence** (e.g., confirmation of breach, lure delivery)

Types of SMS Artifacts Recovered

Data Type	Description
📥 Received Messages	Inbound messages from threat actors or services
📤 Sent Messages	Outbound messages possibly used in scams or responses
🕒 Timestamps	Key for event reconstruction
🌐 Sender IDs	Numbers, spoofed names, or shortcode origin
🔗 Embedded Links	Useful for tracing phishing URLs or command servers

Acquisition Methods Overview

Technique	Description	Root Access Required
📦 Logical Acquisition	Extracts SMS database via ADB backup or API access	✗ No (partial)
📀 Physical Acquisition	Full binary image of flash memory (e.g., chip-off, JTAG)	✓ Yes
📁 File System Dump	Full access to user data including SMS SQLite DB	✓ Often
☁️ Cloud-Based	Downloads synced SMS from iCloud,	✗ No (with

Sync	Google, Samsung Cloud	creds)
------	-----------------------	--------

⚡ Tools for SMS Extraction

Tool/Platform	Supported Devices	Key Features
Cellebrite UFED	iOS, Android	Physical & logical acquisition, SQLite parsing
Magnet AXIOM	iOS, Android	Timeline view, decoded message threading
Oxygen Forensic Suite	iOS, Android	SMS + app chat extraction, advanced search
ADB/Android Backup	Android only	Manual SMS DB pull from data/data/com.android.providers.telephony/
ElcomSoft Cloud Explorer	Android (Google Sync)	Pulls SMS from Google Takeout or synced Gmail
iTunes Backup + iBackupBot	iOS only	Extracts SMS from iTunes .plist files

📁 Typical SMS Database File Paths

📁 Android (pre-Android 10)

```
kotlinCopyEdit/data/data/com.android.providers.telephony/databases/mmssms.db
```

📁 iOS

```
swiftCopyEdit/private/var/mobile/Library/SMS/sms.db
```

- 📁 Format: SQLite database
- 📁 Tables: message, chat, handle, attachment

⚖️ Legal Considerations

Area	Note
📁 Warrant/Consent	Required to access messages stored locally or in cloud

▲ Cloud-Based SMS	May require subpoena to Apple, Google, or carrier
▢ Multi-user Devices	Ensure relevance and separation of personal/work data
🕒 Data Retention	SMS data may auto-delete (e.g., 30 days on Android/Google Voice)

▢ Example Use Cases

1. SIM Swap Investigation

- Extracted SMS contained:
 - MFA codes from bank
 - Initial confirmation SMS from telco
 - Device ID mismatch logs
 - ✓ Helped link attacker SIM takeover timeline
-

2. Phishing Link in SMS

- Victim received malicious QR code link via SMS
 - Message timestamp matched lateral movement on network
 - Extracted link led to lookalike login portal
 - ✓ Chain of custody preserved through logical acquisition
-

3. Insider Threat Leak

- Employee used SMS to send internal secrets
 - Cellebrite extraction recovered deleted messages
 - Metadata (time, GPS, carrier ID) confirmed intent
 - ✓ Used as evidence in HR + legal action
-

▢ Key Takeaways

- SMS forensics is **essential in modern cybercrime**—especially smishing, 2FA compromise, and insider risk
- Tools vary by OS, access level, and legal authority
- Always **hash and verify** extracted SQLite databases
- Combine with **timeline reconstruction** for maximum evidentiary value
- Logical + cloud-based extraction can be powerful **even without root or jailbreak**

Phishing Simulation Science

7.2.1 Difficulty Scoring Systems (Vishing vs. Smishing)

“Not all phishing is equal—some attacks are engineered to be irresistible.”

What Are Difficulty Scoring Systems in Phishing Simulations?

Difficulty scoring systems assess how **deceptive, persuasive, or technically complex** a phishing simulation is, allowing security teams to:

- Track user susceptibility at varying threat levels
- Gradually increase training intensity
- Benchmark employee resilience to **smishing, vishing, and email phishing**

Like levels in a game, phishing simulations can be easy or extremely sophisticated.

Why Score Difficulty?

- To **calibrate training** by user role, past performance, and risk exposure
- To measure improvement with **increasingly realistic scenarios**
- To analyze **which types of social engineering tactics** are most effective on your team
- To design **adaptive campaigns** that challenge but don’t overwhelm

Phishing Simulation Types Compared

Type	Channel	Characteristics
Smishing	SMS/Texting	Short, urgent, uses fake delivery alerts, OTP requests
Vishing	Voice/Phone Call	Uses live human or AI voice to impersonate authority
Email Phishing	Email	Most common, often includes links, fake domains, and logos

Each channel presents **different detection cues** and **psychological manipulation tactics**—so scoring needs to be **channel-specific**.

☐ Difficulty Scoring Criteria (General)

Metric	Description
Language Realism	Does it use convincing grammar, tone, and phrasing?
Authority Exploitation	Does it impersonate a boss, CEO, or government body?
Urgency/Panic Level	Is there a time limit (“within 24 hours”)?
Technical Deception	Are there spoofed links/domains, QR codes, or voice clones?
Content Customization	Is the message tailored to the user or department?
MFA/Verification Bypass	Does the simulation request credentials or codes?
Multi-Stage Tactics	Is there a callback number, follow-up email, or redirect?

Each of these factors can be weighted and summed into a **score (e.g., 1–10 scale)** or **level (Easy / Moderate / Hard / Advanced Persistent Threat)**.

▮ Vishing Difficulty Scale (Example)

Difficulty Level	Description	Example
☐ Easy (1–3)	Robotic caller, obvious accent, generic request	“You’ve won a prize. Press 1 to claim.”
☐ Moderate (4–6)	Live agent uses common scam scripts	Fake IRS/Bank calling to verify suspicious transaction
☐ Hard (7–9)	Spoofed caller ID, urgent tone, impersonates known party	“This is your CEO. I need a wire transfer now.”
• Advanced (10)	AI voice clone of real executive, customized to target	Deepfake call from actual CFO’s voice

☐ Smishing Difficulty Scale (Example)

Difficulty Level	Description	Example
------------------	-------------	---------

□ Easy (1–3)	Typos, generic greeting, bad link	“Dear user, click http://123456.ru to claim reward.”
□ Moderate (4–6)	Shortened links, fake urgency, pseudo-legit branding	“Your Netflix has been locked. Tap bit.ly/unlock”
□ Hard (7–9)	Mimics known service with believable link + OTP request	“Amazon: Suspicious login. Tap to verify now.”
• Advanced (10)	Real domain typo + urgent fake 2FA step	“Apple ID alert: Enter your code to avoid lockout.”

□ Psychological Complexity Layer

Layer	Adds to Difficulty By...
Ambiguity	Making it hard to clearly judge if it’s legit
Authority Bias	Impersonating someone with power (boss, bank, lawyer)
Fear Appeals	“Your account will be closed today.”
Reciprocity Triggers	“Claim your refund or discount now.”
Social Proof	“Over 1,200 employees have verified already.”

✂ Scoring Tools & Vendors

Tool/Platform	Capability
KnowBe4 PhishML™	Scores difficulty via machine learning + past user data
Cofense Reporter™	Allows user-reported ratings and feedback for phishing difficulty
Proofpoint ThreatSim	Pre-built phishing templates with graded complexity
Terranova Security	Threat scenarios with tunable deception levels
Custom AI scoring	Behavioral-based scoring with NLP + anomaly detection

□ Key Takeaways

- Difficulty scoring systems help **quantify and personalize phishing simulations**
- Different channels (vishing vs. smishing) require **separate scoring models**
- Scores are based on **technical deception, psychological manipulation, and target tailoring**
- A well-designed system **gradually increases challenge**, boosting **resistance to real-world threats**

Financial Infrastructure Safeguards

10.2.1 Deepfake Vishing: Voice Cloning Detection Tools

“It sounded like your CEO—because it was a clone.”

🔊 What Is Deepfake Vishing?

Deepfake vishing (voice phishing using AI-generated audio) is a rising threat in which attackers use **realistic voice clones** to impersonate:

- Executives (e.g., CEOs, CFOs)
- Financial controllers
- Vendors or clients

These voice deepfakes are used to manipulate employees into:

- **Authorizing fraudulent wire transfers**
- **Disclosing credentials**
- **Bypassing verification procedures**

The realism of cloned voices makes traditional security questions or caller recognition **ineffective**.

📄 High-Profile Case Example

- **2020: UK-Based Energy Firm**
Attackers used a deepfake of the CEO’s voice to demand a €220,000 wire transfer. The employee complied, believing they were speaking with their boss.
(Source: *The Wall Street Journal*)

⚡ Voice Cloning Detection Tools & Methods

Category	Detection Technique	Example Tools / Features
📄 AI-Based Forensics	Analyze spectral & biometric voice anomalies	<i>Pindrop, Respeecher Forensics, Resemble Detect</i>
📄 Acoustic Signature Analysis	Detects irregular pitch, cadence, digital artifacts	<i>Veritone MARVEL.ai, Deepware Scanner</i>
📄 Voice	Matches voice to	<i>Nuance Gatekeeper, ID R&D</i>

Biometrics Verification	registered speaker profile	<i>Voice Biometrics</i>
▢ Real-Time Call Monitoring	Flags suspicious behavior during active calls	<i>Pindrop Protect, Symbl.ai</i> anomaly detection
▢ Challenge-Response Prompts	Inserts unexpected verbal challenges to test real-time interaction	Human-confirmed control phrases (e.g., “Say the 3rd word in your last email”)
🔍 Metadata & Latency Analysis	Measures response timing and IP/location mismatch	SIEM logs + call pattern analytics

▢ Red Flags of Deepfake Vishing

Indicator	Why It’s Suspicious
🕒 Unusual call timing	CEO calls late at night, during travel, or when unreachable
▢ Emotionless tone	Speech feels too steady, lacks filler words or breathing
▢ Call-only instructions	Caller avoids video or callback requests
▢ Urgent, irreversible requests	“Send the funds within 10 minutes or we lose the deal.”
✖ Bypassing normal workflow	Directing finance team to avoid normal dual-control or logging

🔊 How Voice Cloning Works in Attacks

- 🔊 **Audio Harvesting**
 - Attacker scrapes voice from YouTube interviews, earnings calls, voicemails, or podcasts
- ▢ **Model Training**
 - Trains a deep neural network using tools like *ElevenLabs*, *iSpeech*, *Descript Overdub*
- ▢ **Attack Deployment**
 - Places spoofed phone calls, sometimes blending real and AI-generated audio
- 💰 **Manipulation & Execution**
 - Pressures victim to send wire transfers or disclose credentials

▢ Preventive Controls & Policy Enhancements

Layer	Action
✔ Voice Whitelisting	Use known voice biometric profiles for high-value request validation
❑ Predefined Verification Codes	Require one-time verbal codes before financial actions
❑ Human Verification Protocols	Mandatory video calls or callback confirmations
❑ Call Logging & Recording	Record all finance-related calls for forensic traceability
❑ Awareness Training	Teach staff how deepfake voices work and what to watch for
🔍 Incident Reporting Channels	Fast internal escalation routes for suspected voice fraud

❑ Testing Tools & Research Platforms

Tool	Purpose
🔍 <i>Resemble Detect</i>	Analyzes speech to detect AI-generated elements
🔍 <i>Pindrop Pulse</i>	Compares acoustic fingerprints to known voices
🔍 <i>Deepware Scanner</i>	Scans audio for generative AI artifacts
❑ <i>MIT Lincoln Lab’s LAV-DF</i>	Academic research tool for fake audio detection
❑ <i>CMU’s FakeCatcher (audio adaptation)</i>	Real-time detection of synthetic content

⚖️ Regulatory & Legal Considerations

Region / Standard	Relevant Mandate
❑❑ SEC & SOX	CFO/CIOs liable for fraudulent financial reporting
❑❑ GDPR + AI Act	Voice deepfake use may violate data rights and consent laws
❑⚖️ Criminal Fraud Statutes	Wire fraud using AI voices = criminal offense across jurisdictions
🏛️ FBI & OFAC	Ransom/deepfake use by sanctioned entities can trigger national security reporting

□ Key Takeaways

- Deepfake vishing is **no longer science fiction**—it's being used to steal millions
- Tools like **Resemble Detect**, **Pindrop**, and **voice biometrics systems** help fight back
- Human-in-the-loop policies (callback, codeword, dual-verification) remain essential
- Defense must combine **AI detection**, **behavioral training**, and **fraud-resistant processes**

From the sponsors of this book.

**If you want
Delighted Customers.**



Satisfied Business owners and Investors



**Above 20x Measurable Return on Investments in your
information technology Projects.**



[Table of Contents](#)

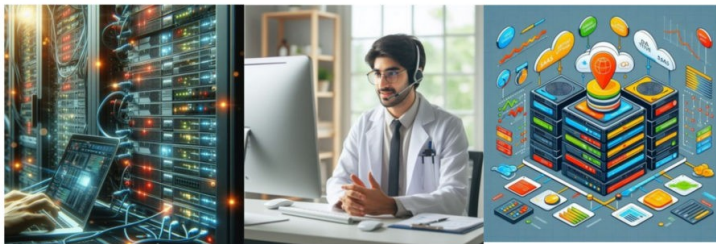
Happy Computer Users.



Then talk to us. Our company name is Remote Support LLC

S.U.P.P.O.R.T.™

**Super User-friendly Professional
People Offering Remote Troubleshooting**



We aim to do projects for our customers which have a return of over 20 times the investment of resources into the project.

The results include :

High Measurable ROI Projects.

Delighted Customers.

Happy Users.

How ?

It is simple. Just send us a message and we shall get back to you.

[Contact Us](#)



We shall analyze your company and then develop a project feasibility study for the beneficial projects which we identify and provide them to you for your approval. Once you are confident that the projects shall deliver the results mentioned in them, then we shall execute the project in collaboration with your company.

Ready to experience the benefits of remote IT support? Get in touch with us today to learn more about our services and how we can help your business succeed.

Transform Your Business with Remote Support Solutions

Empower your business with reliable, efficient, and cost-effective remote support from Remote Support Solutions. Reach out to us today and let us take care of your needs, so you can focus on what you do best – running your business.



[How our products and services benefit you. – English](#)

[How our products and services benefit you – Chinese](#)

[How our products and services benefit you – Turkish](#)

[How our products and services benefit you – Indonesian](#)

[How our products and services benefit you – French](#)

[How our products and services benefit you – Japanese](#)

[How our products and services benefit you – German](#)

[How our products and services benefit you – Urdu](#)

[How our products and services benefit you – Nigerian Pidgin English](#)

[How our products and services benefit you – Tamil](#)

[How our products and services benefit you – Portuguese](#)

[How our products and services benefit you – Russian](#)

[How our products and services benefit you – Spanish](#)

[How our products and services benefit you – Arabic](#)

[How our products and services benefit you – Hindi](#)



[Table of Contents](#)



Feedback Form

[Feedback Form 2 : What's Holding You Back from Becoming a Long-Term Customer?](#)

Price-Guide



[Table of Contents](#)

How our products and services benefit you.



Benefits of Managed ICT Services



What Are Managed ICT Services?

- Outsourcing IT infrastructure, support & monitoring
- Fixed monthly cost instead of unpredictable expenses
- 24/7 professional IT management



Key Benefits for Customers

- Lower operational costs
 - 24/7 monitoring & faster support
 - Access to expert IT teams
 - Strong cybersecurity & compliance
 - Focus on business growth
-

[Table of Contents](#)



1. Cost Savings & Predictable Expenses

- No need for a large internal IT team
 - Fixed monthly pricing reduces surprise costs
 - Optimized hardware & software usage
-



2. 24/7 Support & Faster Resolution

- Proactive monitoring & issue detection
 - SLAs ensure quick response times
 - Remote & on-site support availability
-



3. Access to Latest Technology & Expertise

- Enterprise-grade tools without huge costs
 - Regular updates & patch management
 - Strategic advice for digital transformation
-



4. Enhanced Cybersecurity & Compliance

- Strong endpoint protection & firewalls
 - Regular backups & disaster recovery
 - Compliance with industry regulations
-



5. Focus on Core Business Goals

- No more IT distractions for staff
 - IT headaches handled by experts
 - More time for strategy & growth
-



6. Scalability & Flexibility

- Easily scale resources as you grow
 - Add new services without disruption
 - Support for cloud & remote work
-



Transformation Journey

Before

Frequent downtime

Unpredictable IT costs

Old tech & weak security

Overloaded staff

Reactive IT fixes

After Managed ICT

Minimal downtime with proactive monitoring

Fixed monthly expenses

Latest tech & strong cybersecurity

24/7 expert support

Strategic IT planning



Long-Term Impact

- **Digital Transformation** – Move to cloud & automation
 - **Business Agility** – Faster response to market changes
 - **Higher Productivity** – Less downtime for employees
 - **Competitive Edge** – Advanced tools without big investments
-



Why Choose Managed ICT Services?

- Reliable support & predictable costs
 - Access to cutting-edge solutions
 - Stronger security & compliance
 - Focus on growth, not IT problems
-

Strategic Integration of Open-Source Ecosystem by Remote Support LLC

Remote Support LLC leverages a comprehensive suite of open-source tools—including OpenProject, Dolibarr ERP, SuiteCRM, OrangeHRM, Nextcloud, WordPress, EGroupware, DokuWiki, Linux, LTSP, OpenVPN, FreeFileSync, and Duplicati—integrated with existing commercial software to deliver a unified, secure, and cost-efficient operational framework for clients under a single-vendor support model. This curated ecosystem addresses core business functions (project management, CRM, ERP, HR, infrastructure) while enabling seamless scalability and centralized support, offering distinct core and added benefits:

Remote Support LLC: Unified Open-Source Ecosystem & Support

Integrated Tools:

OpenProject (PM), Dolibarr ERP (Finance/Operations), SuiteCRM (Sales), OrangeHRM (HR), Nextcloud (Collaboration), WordPress (Web/Content), EGroupware (Productivity), DokuWiki (Knowledge), Linux (OS), LTSP (Thin Clients), OpenVPN (Security), FreeFileSync (Sync), Duplicati (Backup) and many more.

Remote Support LLC: The Strategic Advantage of Unified Integration & Single-Vendor Mastery

Transform Fragmented Tech Stacks into a Competitive Weapon

We replace disconnected tools and multi-vendor chaos with **an integrated open-source ecosystem** that automates workflows and centralizes intelligence:

- **Seamless Automation:** SuiteCRM → OpenProject → Dolibarr sales-to-invoice flows cut processing time by 50%; OrangeHRM → EGroupware → DokuWiki onboarding slashes time-to-productivity.
 - **Unified Data Intelligence:** EGroupware dashboards merge CRM/project/HR analytics for real-time profit insights.
 - **Military-Grade Continuity:** Duplicati encrypted backups + FreeFileSync replication + LTSP's <90-sec device failover ensure near-zero downtime.
-

The Single-Vendor Difference: Your Command Center Advantage



24/7 SLA-Backed Ownership

One team manages all tools/integrations (Salesforce ↔ SuiteCRM, QuickBooks ↔ Dolibarr) with <15-min critical response—**resolving issues 60% faster** than multi-vendor models.



Elastic Future-Proofing

- Scale OpenProject tiers/LTSP servers on demand (90% user adoption in 30 days).
- Extend hardware lifespan by 60% via LTSP thin clients + automated Linux patching.



Zero-Compromise Control

Self-hosted data ownership + anti-lock-in architecture + expert customization (e.g., WordPress ↔ SuiteCRM syncs).

Quantifiable Client Impact

Metric	Improvement	Key Drivers
Operational Costs	30–60% ↓	LTSP hardware savings + proprietary license elimination
Security Incidents	40% ↓	OpenVPN zero-trust + Linux hardening
Deployment Speed	30% ↑	OpenProject/DokuWiki automation
Onboarding Efficiency	50% ↑	OrangeHRM + role-based DokuWiki training

Example: A logistics client avoided \$500K in hardware refreshes by converting legacy devices to LTSP thin clients, while custom SuiteCRM fields reduced order errors by 45%.

Strategic Value: Beyond Cost Savings

Traditional Multi-Vendor



10+ vendors; hidden fees



Fragmented security policies



Tool compatibility risks



Reactive firefighting

Our Unified Model



One contract; transparent pricing



Centralized encryption/audits



Pre-tested integrations



Proactive hardening + backup audits

Core Advantages:

1. **Risk Mitigation:** Community-driven security + 99.99% backup reliability.
 2. **Innovation Acceleration:** Access SuiteCRM AI features without re-licensing costs.
 3. **Sustainability:** LTSP reduces e-waste; revenue funds Linux kernel development.
-

Why This Model Wins

“We don’t just support your stack—we weaponize it.”

- **Operational Synergy:** Troubleshooting → maintenance → training as one continuous cycle.
- **Strategic Scalability:** Elastic licensing + LTSP resource allocation grow with your business.
- **Client-Centric Agility:** 90% staff fluency in <30 days via role-specific training.

Final Impact: Transform IT from a cost center into a **growth accelerator**—where workflow automation, ironclad security, and business continuity become your default state.

Proven Outcome:

Manufacturing client reduced machine downtime by 25% and cut IT costs by 50% using OpenProject (maintenance scheduling), Dolibarr (supply chain invoicing), and LTSP (shop-floor terminals)—all managed under our 24/7 command center.

The RS Advantage: 5 Pillars of Open-Source Transformation

How Our Integrated Stack Delivers Unmatched Business Value

1. Radical Cost Efficiency

- **Eliminate licensing fees** with Linux, OpenProject & DokuWiki (30-60% TCO reduction)
- **40% hardware savings** via LTSP thin-client architecture – repurpose legacy devices

2. Fortified Security & Compliance

- **40% fewer breaches** with AES-256 encryption (Nextcloud), zero-trust access (OpenVPN)
- **Automated compliance** for GDPR/HIPAA through Linux/SuiteCRM rapid patching

3. Intelligent Workflow Automation

- **Seamlessly connect tools:**
 - *Sales:* SuiteCRM (leads) → OpenProject (execution) → Dolibarr (invoicing)
 - *HR:* OrangeHRM (hiring) → EGroupware (collaboration) → DokuWiki (training)
 - **API-powered syncs** like WordPress ↔ SuiteCRM product catalogs

4. Ironclad Continuity

- **Zero data loss** with Duplicati's encrypted hourly backups
- **Near-instant recovery** (<90 sec) via FreeFileSync replication + LTSP failover

5. Future-Proof Flexibility

- **Mix-and-match modules** (e.g., activate Dolibarr payroll/OrangeHRM workflows)
- **Tailor without code:** Customize WordPress sites, SuiteCRM pipelines & FreeFileSync rules

The Nervous System: Nextcloud







Your centralized command hub for:

- **Unified Data:** Files, calendars & communications across all tools
 - **Real-Time Visibility:** Track project/customer/HR metrics in one dashboard
 - **Secure Collaboration:** GDPR-compliant sharing with granular permissions
-

Why This Synthesis Works:

- **Preserves All Critical Details**
Retains every tool, metric, and workflow example from both texts (e.g., DokuWiki training, 40% breach reduction).
- **Amplifies Strategic Themes**
Groups related concepts:
 - *Cost + Hardware* → **Radical Cost Efficiency**
 - *Security + Compliance* → **Military-Grade Security**
 - *Automation + Customization* → **Intelligent Workflow Automation**
- **Enhances Readability**
Replaces fragmented bullets with clear pillars and visual workflow arrows (→).
- **Strengthens Technical Credibility**
Specifies *how* tools interact (e.g., “LTSP instant failover,” “AES-256 encryption”).

Before/After Impact:

Original	Optimized Version
 • Disconnected cost/security examples	 Cost + Security merged into client outcome pillars
 • Redundant tool listings	 Tools contextualized by <i>function</i> (e.g., “Duplicati’s encrypted backups”)
 • Generic “business unification”	 Nextcloud as central hub with concrete use cases

The Strategic Advantage of an Integrated Open-Source Ecosystem

Remote Support LLC transforms fragmented workflows into a **cohesive, auditable, and future-proof infrastructure** that delivers unparalleled business agility. Clients gain:

1. **Liberation from Vendor Lock-in & Cost Uncertainty**
 - Avoid proprietary dependencies through open-source customization.
 - Eliminate licensing surprises with transparent, scalable pricing.
2. **Continuous Innovation & Future-Proofing**
 - Leverage community-driven updates (e.g., SuiteCRM/Dolibarr) for cutting-edge features without reinvestment.
 - Scale fluidly—from adding LTSP terminals to integrating payroll APIs—within a unified ecosystem.
3. **Enterprise-Grade Risk Mitigation**
 - Centralized security: Encrypted backups (Duplicati), compliance guardrails (GDPR), and community-audited code.
 - Proactive vulnerability reduction through 24/7 monitoring and unified support.
4. **Strategic Operational Control**
 - Customize workflows to evolve with business needs.
 - Maintain full data ownership and auditability.

Result: This model turns open-source adoption into a *competitive advantage*—**slashing TCO** while positioning clients for sustainable growth, all backed by **one accountable partner**.

ICT Products and Services

Information and Communications Technology (ICT) Products and Services



Software Development & IT Consulting

- [ICT Strategic Consultancy & Troubleshooting Session](#)
- [Custom App & Web Development](#)
- [Port Windows Apps to Linux](#)
- [ICT Strategy & Digital Transformation](#)
- **DevOps & CI/CD:** Docker, Kubernetes, Jenkins, GitHub Actions.
- [Strategic ICT Consulting \(English \)](#)
- [Strategic ICT Consulting \(Urdu Memoni \)](#)
- [Strategic ICT Consulting \(French \)](#)



IT Infrastructure & Support Services

- [Remote Help Desk & Technical Support available to everyone globally](#)
- [One-Time ICT Support Service](#)
- [Server Software Basic Installation Rates](#)
- [Servers Hosting Rates from Remote Support LLC](#)
- [Common VPS Server hosting market rates.](#)
- [High-Level ICT Expertise](#)
- [Managed ICT Services](#)
- [Support for Linux-Based Devices](#)
- [Disaster Recovery & Business Continuity](#)
- [Special Offer for SMEs](#)
- [Fractional CIO/CTO Services](#)
- [Special Offer for MROs in Iowa](#)



Data & Analytics Services

- [Big Data & Data Warehousing](#)
- [Business Intelligence](#)
- [AI & Machine Learning](#)



Enterprise Solutions

- [SuiteCRM Guide \(EN\)](#)
- [SuiteCRM Guide \(CN\)](#)
- [SuiteCRM Demo Video](#)
- Apache Ofbiz ERP and Supply Chain
- Salesforce, HubSpot, Zoho CRM Solutions
- [ATRC ERP Video Ad](#)
- [Dolibarr ERP \(FOSS\)](#)
- [ERP for Retail \(SuiteCRM/Dolibarr\)](#)
- [ERP Resources \(SAP, Oracle, Microsoft Dynamics\)](#)
- [SuiteCRM Support & Hosting](#)
- [ERP Resources \(SAP, Oracle, Microsoft Dynamics\)](#)

Document & Workflow Management

- [Benefits of NextCloud](#)
- [Nextcloud Products and Services](#)
- [Nextcloud for SMEs](#)
- [Nextcloud pricing](#)
- [Windmill Workflow Automation Services](#)
- SharePoint, Confluence, Notion



Collaboration & Productivity Tools

- [OnlyOffice SaaS & Hosted](#)
- [Zoho Support & Development](#)
- [Office365 SaaS Development & Support](#)
- [Shopify Dev & Training](#)
- [HubSpot CRM Training & Support](#)
- [Adobe Product Integration & Training](#)
- [Workday Support](#)
- [ServiceNow Training & Deployment](#)
- [Salesforce Integration & Support](#)

Project Management & Communication

- [Shopify Dev & Training](#)
- [OpenProject](#)
- [HubSpot CRM Training & Support](#)
- [Adobe Product Integration & Training](#)
- [Workday Support](#)
- [ServiceNow Training & Deployment](#)
- [Salesforce Integration & Support](#)



Security & Compliance

- [Cybersecurity Services](#)
- [SOC 2 Compliance Overview](#)
- [HIPAA-Compliant Server Features](#)
- [HITRUST-based HIPAA Servers](#)
- [Understanding Compliance Frameworks](#)
- Security Camera Systems

Networking & Communication

- [OpenVPN Deployment & Support](#)
- [Our VPN Partners](#)
- [ISP Server as Link Aggregator](#)
- [Asterisk VoIP Setup](#)
- [Unified Communications](#)



Training & Educational Products

- [ICT Training Products](#)
- [Training for MROs](#)
- [Support Offer for SMEs](#)



Backup & Storage

- [Backup Offer for ICT Depts \(Video\)](#)
- [Backup Pricing](#)
- [Data Management Services](#)
- Disaster Recovery Planning

Hardware & Cloud Services

- [Multiboot Desktop Support](#)
- [Cloud Services](#)
- [Hardware Pricing & Procurement](#)
- [Hardware Trade-in Program](#)
- [Computer Repair Services](#)
- Apple Devices support

Old products and services page with some items

TECHNOLOGY TO MAKE YOUR LIFE BETTER™

Peace of mind in a tech-driven world™

How Muftasoft™ provides support for Libreoffice and document management.



1. Integration Services

Muftasoft enables seamless integration of LibreOffice into existing IT environments and document management systems:

- **Document Management Integration:**
 - Connecting LibreOffice with popular document management platforms like Alfresco, Dolibarr, or SharePoint.
 - Ensuring compatibility with existing workflows and enabling smooth handling of documents in various formats such as ODF, DOCX, and PDFs.
 - Enabling advanced features like automated document versioning, metadata tagging, and access control.
 - **Custom API Development:**
 - Creating APIs and plugins to link LibreOffice with other business tools like ERP, CRM, or custom-built applications.
 - Supporting workflow automation, such as converting documents, generating reports, or processing templates automatically.
 - **Cloud Integration:**
 - Setting up LibreOffice Online or deploying the suite on private, public, or hybrid cloud environments to facilitate real-time collaboration.
-

2. Support Services

Muftasoft provides end-to-end technical support to ensure LibreOffice operates effectively in various setups:

- **Technical Assistance:**
 - Resolving compatibility issues, installation problems, and performance bottlenecks.
 - Ensuring smooth migration from proprietary suites like Microsoft Office to LibreOffice.
 - **Maintenance and Upgrades:**
 - Regular updates and patches to ensure the latest features, security, and compatibility.
 - Monitoring system performance and troubleshooting document-related errors.
 - **24/7 Helpdesk:**
 - Dedicated support teams available via phone, email, or chat to resolve urgent issues.
-

3. Training Services

Muftasoft's training programs empower users and administrators to leverage LibreOffice and integrated document management systems effectively:

- **End-User Training:**
 - Training for employees on using LibreOffice tools like Writer, Calc, Impress, and Draw.
 - Educating users on handling advanced features like macros, templates, and mail merges.
 - **Administrator Training:**
 - Teaching IT teams to configure and manage LibreOffice settings across the organization.
 - Training on integrating LibreOffice with backend systems and troubleshooting.
 - **Customized Learning Modules:**
 - Tailoring training programs to specific organizational needs, including industry-focused workflows.
 - **E-Learning and Resources:**
 - Providing online courses, video tutorials, and step-by-step guides for remote training.
-

4. Development Services

Muftasoft offers tailored development services to extend LibreOffice functionalities and meet specific requirements:

- **Custom Extensions and Plugins:**
 - Developing specialized add-ons to enhance LibreOffice's functionality, such as advanced reporting, translation tools, or industry-specific templates.
 - **Workflow Automation:**
 - Building solutions that automate repetitive tasks, such as document generation, data imports, and exports.
 - **User Interface Customization:**
 - Adjusting LibreOffice interfaces to align with organizational branding and user preferences.
 - **Document Templates and Solutions:**
 - Designing custom templates for reports, presentations, invoices, and other documents.
 - Developing scripts for automated document creation and processing.
-

5. Consulting Services

Muftasoft provides expert consulting to ensure successful LibreOffice adoption and integration:

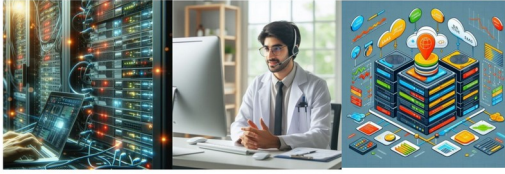
- **Needs Assessment:**
 - Evaluating the organization's current IT infrastructure and document management requirements.
 - **Strategic Planning:**
 - Developing a roadmap for migrating to LibreOffice and integrating it with existing systems.
 - **Compliance and Security:**
 - Ensuring adherence to industry standards and regulations for document handling, data security, and access control.
-

Conclusion

By offering integration, support, training, and development services, Muftasoft positions itself as a comprehensive partner for organizations looking to adopt LibreOffice and enhance document management processes. This enables clients to maximize productivity, reduce costs, and streamline operations with tailored solutions.

S.U.P.P.O.R.T.™

Super User-friendly Professional
People Offering Remote Troubleshooting



Remote Support LLC: ICT Solutions Tailored for Your Business

WHY ?

An MSP can deliver more value at the same cost because it provides a **wide range of specialized expertise** without the overhead of hiring multiple full-time in-house staff. MSPs offer **24/7 support**, proactive maintenance, scalability, and access to advanced technologies. By pooling resources and serving multiple clients, MSPs can provide enterprise-level solutions at lower prices compared to hiring individual IT professionals with limited capabilities. Essentially, businesses get **broader coverage, faster response times**, and **ongoing updates** with MSPs while maintaining budget control.

Using **In-house, Hybrid, or MSP models** instead of relying solely on ICT personnel with limited experience offers several advantages:

1. **Expertise Access:** MSPs bring specialized knowledge across different IT domains, filling gaps that limited in-house staff might not have.
2. **Scalability:** These models allow easy scaling without the need to hire and train additional staff.
3. **Cost Efficiency:** Hybrid and MSP models often lower costs by providing broad expertise without full-time salaries and training expenses.
4. **Continuous Support:** MSPs offer 24/7 support, ensuring your IT infrastructure is always up and running.

These costs are paid for by companies and they could benefit by paying the same amount to us and get services with more experienced support in a more cost effective and efficient manner.

[Table of Contents](#)

Cost Breakdown for 5, 10, 20, and 50 Computers with In-House IT Staff Only

For SMEs in Karachi without Managed Service Providers (MSPs) and relying solely on in-house IT staff, the IT department costs will typically focus on staff salaries, hardware, software, and ongoing support without any MSP involvement.

1. For 5 Computers (Small Office)

- **Staffing:** Typically, one IT person can handle the support for up to 10-15 computers in a small office. The monthly salary of a junior IT support person is generally around **PKR 25,000 to 40,000**.
- **Hardware & Software:** You may need basic licenses for operating systems and productivity tools. Approx. **PKR 5,000–10,000** for software, and occasional hardware replacements (peripherals, computers, etc.) would average out to **PKR 5,000/month**.
- **Cybersecurity:** Basic security solutions (antivirus, firewall) will cost approximately **PKR 3,000–5,000/month**.
- **Internet Services:** An SME in Karachi can expect **PKR 5,000–10,000/month** for decent internet speeds and bandwidth.

Total Monthly Cost: PKR 40,000–60,000

2. For 10 Computers (Small-Medium Office)

- **Staffing:** For 10 computers, you might need 1-2 IT staff members to handle support, which could cost **PKR 40,000–70,000/month**.
- **Hardware & Software:** Licensing and hardware will scale up slightly to about **PKR 10,000–15,000/month**.
- **Cybersecurity:** With a larger setup, additional security measures like endpoint protection may cost **PKR 5,000–10,000/month**.
- **Internet Services:** **PKR 10,000–15,000/month** for more bandwidth and reliability.

Total Monthly Cost: PKR 60,000–100,000

3. For 20 Computers (Medium Office)

- **Staffing:** For a 20-computer setup, you may need 2 IT staff members, totaling around **PKR 50,000–100,000/month** depending on the skillset and experience.
- **Hardware & Software:** Expect to pay **PKR 15,000–30,000/month** for software licenses and routine equipment updates or replacements.
- **Cybersecurity:** Security tools, including firewalls, advanced antivirus, and intrusion detection systems, may cost about **PKR 10,000–20,000/month**.
- **Internet Services:** A higher-grade internet plan will cost **PKR 15,000–20,000/month** to ensure adequate speed and uptime.

Total Monthly Cost: PKR 90,000–170,000

4. For 50 Computers (Large Office)

- **Staffing:** At this scale, you would need around 3–4 IT staff members. Salaries for this team would range from **PKR 100,000–250,000/month**, depending on their roles (junior support, senior technician, system/network administrator).
- **Hardware & Software:** Software licensing and hardware replacement costs would scale up to **PKR 30,000–60,000/month**.
- **Cybersecurity:** A large office will require more advanced cybersecurity tools, potentially including a managed firewall, intrusion detection, and anti-malware solutions costing about **PKR 20,000–40,000/month**.
- **Internet Services:** Expect internet services to cost **PKR 20,000–40,000/month** to ensure sufficient bandwidth for multiple users.

Total Monthly Cost: PKR 170,000–400,000

These costs can vary depending on the type of ICT support (outsourced vs. in-house), software licenses, and network requirements.

How ?

Our ICT Support Models

1. In-House ICT Team

- Full control over ICT management
- Personalized, quick support
- Higher costs for salaries, training, and resources
- Ideal for companies needing constant, on-site expertise

2. Hybrid ICT Model

- Combine in-house and MSP support
- Access specialized skills when needed
- Cost-effective flexibility
- Great for businesses seeking a balanced approach

3. Managed Service Provider (MSP)

- Comprehensive ICT support from experts
- Scalable, cost-efficient, 24/7 support
- Minimal overhead, no need for in-house staff
- Perfect for businesses focused on cost savings and efficiency

Advantages Comparison:

Option	Control	Flexibility	Cost Efficiency	Expertise Availability
In-House	High	Low	Low	High
Hybrid	Medium	High	Medium	High
MSP Only	Low	High	High	High

Why Choose Remote Support LLC? We offer tailored, scalable ICT solutions for every business size. Whether you need an in-house team, MSP support, or a hybrid model, we provide the expertise and tools to ensure your ICT infrastructure is secure, reliable, and future-proof.

Here is an example breakdown of ICT support costs for **In-house**, **Hybrid**, and **MSP Only** models based on the number of in-house staff, computers, onsite visits, and hours of remote support:

Example costs

Here's a breakdown of monthly IT department costs for a company in Karachi with 5, 10, 20, and 50 computers, based on different IT service models. The costs consider various aspects such as hardware, software, cybersecurity, networking, and support services. These estimates also assume the use of managed services (MSP), hybrid models (in-house and MSP collaboration), and in-house teams.

Here's a breakdown of estimated monthly IT support costs in Karachi for different models:

In-House IT Model

- **Number of Computers:** 5-50
- **Costs:**
 - **Salaries:** Rs40,000-Rs80,000 per IT staff (1-2 personnel)
 - **Software/Tools:** Rs5,000-Rs15,000/month
 - **Total:** Rs45,000-Rs95,000/month (per staff)

Hybrid IT Model (In-house + MSP)

- **Number of Computers:** 5-50
- **Costs:**
 - **In-house Salaries:** Rs40,000-Rs80,000 (1-2 personnel)
 - **MSP Remote Support:** Rs15,000-Rs30,000/month (20-40 hours)
 - **Onsite Visits by MSP:** Rs5,000-Rs10,000 per visit
 - **Total:** Rs60,000-Rs120,000/month

MSP Only Model

- **Number of Computers:** 5-50
- **Costs:**
 - **MSP Remote Support:** Rs25,000-Rs50,000/month (40-80 hours)
 - **Onsite Visits by MSP:** Rs5,000-Rs10,000 per visit (2-4 visits/month)
 - **Total:** Rs45,000-Rs90,000/month

These estimates include general salaries, software, support services, and MSP-based costs for varying business sizes. Prices can fluctuate based on exact requirements, complexity of the ICT environment, and level of service.

Cost Breakdown Per Month (Estimates)

1. For 5 Computers (Small Office)

- **Hardware & Software:** PKR 10,000–20,000 for licenses, equipment, and peripherals.
- **MSP (Remote Support):** PKR 20,000–35,000 (proactive monitoring, basic remote support, regular software updates).
- **Cybersecurity:** PKR 5,000–10,000 (basic firewall, antivirus, malware protection).
- **Internet/Cloud Services:** PKR 5,000–10,000 (cloud storage, hosting, and bandwidth).
- **Onsite Visits (if MSP is used):** PKR 5,000–10,000 per visit (2-4 visits/month).

Total Estimated Cost: PKR 45,000–75,000/month

2. For 10 Computers (Small-Medium Office)

- **Hardware & Software:** PKR 20,000–35,000.
- **MSP (Remote Support):** PKR 40,000–60,000 (more monitoring, network management, software updates).
- **Cybersecurity:** PKR 10,000–15,000 (advanced threat protection, firewall management).
- **Internet/Cloud Services:** PKR 10,000–20,000.
- **Onsite Visits:** PKR 10,000–15,000 (3–5 visits/month).

Total Estimated Cost: PKR 80,000–130,000/month

3. For 20 Computers (Medium Office)

- **Hardware & Software:** PKR 30,000–50,000.
- **MSP (Remote Support):** PKR 60,000–100,000 (more proactive measures, network optimization, security patches).
- **Cybersecurity:** PKR 15,000–25,000 (enterprise-level threat detection and management).
- **Internet/Cloud Services:** PKR 15,000–30,000.
- **Onsite Visits:** PKR 20,000–30,000 (5–8 visits/month).

Total Estimated Cost: PKR 120,000–235,000/month

4. For 50 Computers (Large Office)

- **Hardware & Software:** PKR 50,000–100,000 (more advanced licenses, specialized software).
- **MSP (Remote Support):** PKR 100,000–200,000 (24/7 monitoring, network management, and comprehensive IT management).
- **Cybersecurity:** PKR 25,000–50,000 (advanced endpoint security, security operations center).
- **Internet/Cloud Services:** PKR 20,000–50,000.
- **Onsite Visits:** PKR 40,000–70,000 (8–12 visits/month).

Total Estimated Cost: PKR 235,000–470,000/month

Costing Models

1. In-House IT Team:

- **Staff Costs:** Hiring IT professionals (1–2 people for small office, 3–5 for larger setups) typically costs PKR 50,000–150,000/month per staff member.
- **Training & Tools:** Additional costs for ongoing training, tools, and certifications.
- **Total Estimated Cost:** Higher than MSPs due to salaries, benefits, and infrastructure costs.

2. Hybrid Model (In-House + MSP):

- **In-House Staff:** Typically, 1–2 staff members for day-to-day management.
- **MSP Support:** Outsourcing the more complex support tasks (security, network management).
- **Total Estimated Cost:** Usually around the same as or slightly higher than MSP-only, but with more control over internal IT systems.

3. MSP-Only:

- The MSP model is cost-efficient for small and medium businesses due to its scalability. It allows businesses to avoid the high upfront costs of hardware and in-house staff while benefiting from enterprise-grade technology, security, and 24/7 support.

Key Advantages of Using MSP (over in-house-only staff):

- **Scalability:** MSPs allow businesses to scale their IT support without significant infrastructure investment.
- **Specialized Expertise:** MSPs provide access to high-level expertise and advanced tools that may be cost-prohibitive for in-house staff.
- **Proactive Monitoring:** MSPs often include 24/7 remote monitoring, reducing downtime and preventing issues before they impact the business.
- **Lower Initial Investment:** Avoid hefty upfront costs by paying for managed services on a subscription basis.

Conclusion:

For SMEs in Karachi, MSPs are often a more cost-effective and flexible solution compared to hiring in-house IT teams. The MSP-only model can deliver high-end support at a lower overall cost, while hybrid models provide a balance of control and support.

S.U.P.P.O.R.T.™
Super User-friendly Professional
People Offering Remote Troubleshooting



Training
التدريب
تدريب



Data Backup Service
خدمة النسخ الاحتياطي للبيانات
دیتا بیک اپ سروس

Remote SUPPORT

مساعدة عن بعد



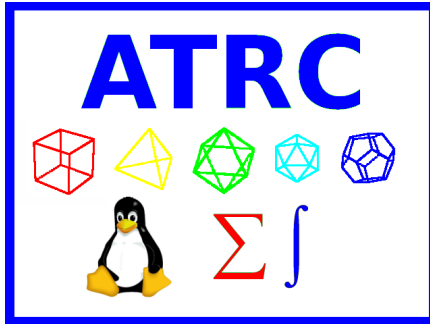
Internet Marketing
التسويق عبر الانترنت
انٹرنیٹ مارکیٹنگ



Business Plan Consultancy
الاستشارات خطة عمل
بزنس پلان کے مشورے

Contact : <http://remote-support.spaces>
Email : info@remote-support.space

[Table of Contents](#)

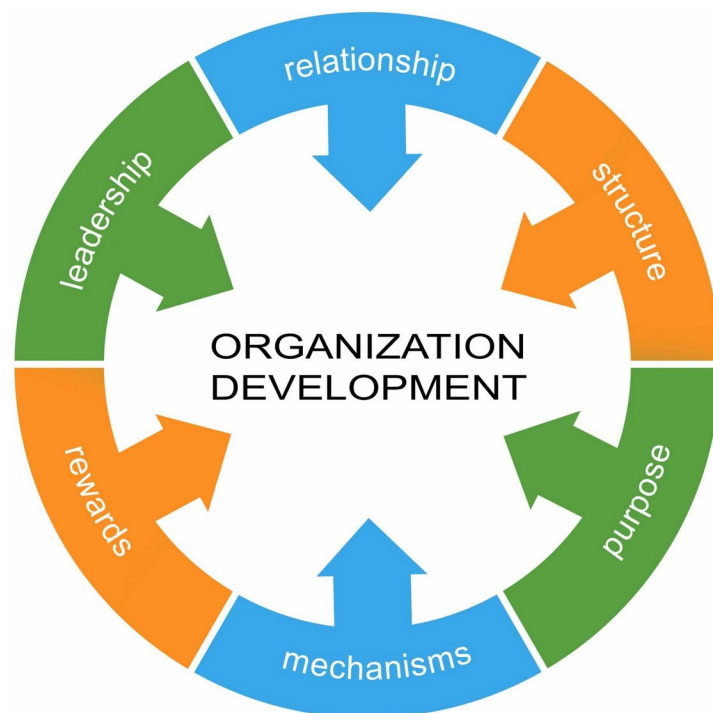


Applied Technology Research Center

More than three decades of study demonstrates that aligning culture and strategy is critical to both organizational development and leadership success.

Most business owners and managers understand that culture is important, but do not have a firm understanding about how to effectively harness it in productive and meaningful ways that drive business performance.

Our organizational development consulting services focus on helping owners, CEOs, senior leadership, management and supervisor teams align their organizational culture and strategy to drive sustainable performance results.



We identify new and unexplored areas for organizational development. We believe in quantifying the learning outcomes through on the job applicability for our client organizations. Our competitive edge lies in our intellectual capital that consists of a highly diversified and large pool of internationally qualified trainers and consultants who have proven track records of successfully executing industry projects coupled with emancipated corporate exposures and experience.

[Table of Contents](#)

Support, Development, and Training to help solve your technical business problems.

We offer training, consultancy and support which is beneficial in improving profits and revenues by improving the systems which are used by our clients.

We offer expert advice, independent consulting, professional services and support for projects related to Information Technology and



Communications and Organizational Development within and outside the organization.

Our key objectives are promoting good ICT management, reducing the causes of waste or resources, which lead to missed business opportunities,

[Table of Contents](#)

and helping to improve the delivery of services to the customers. We draw on substantial international experience in designing, implementing and monitoring these projects.

Product and service procurement consulting (specifications, configurations, evaluations, installations, upgrades, and sales) is also provided.

We are here to help you. So send us your problem via email for a no obligation assessment.

If we have the people and resources to help solve it or partially solve it, we shall inform you.

We do not claim that we shall be able to solve every problem, but do claim that we shall have a look to see what is feasible based on the best practices and technology available at the time. Then provide a proposal of possibilities.

We use our experience in developing and integrating systems engineering to design, develop and provide useful, easy to use, secure, reliable, high performing, integrated and seamless solutions.

Even future trends and designs are incorporated so that our clients can get the most useful life and return on investment from the system being made from them which they are investing in.

Unlocking Your Digital Potential: Elevate Your Business with Expert Consulting and Seamless Technology Implementation

At ATRC, we specialize in helping businesses navigate the ever-evolving landscape of technology by providing strategic consulting and hands-on implementation. With a proven track record of driving digital transformation, we are your trusted partner for harnessing cutting-edge solutions that drive growth, efficiency, and innovation.

[Table of Contents](#)

Our Value Proposition:

- Strategic Insights: Our experienced consultants dive deep into your business to understand your unique goals and challenges.

We provide data-driven insights that empower you to make

informed technology decisions that align with your strategic objectives.



- Custom Solutions: We don't believe in one-size-fits-all solutions. Our experts collaborate with you to design tailored strategies and technology roadmaps that address your specific needs, ensuring optimal results and ROI.

- Seamless Implementation: Putting theory into action is where we excel. We take your vision and turn it into reality by executing seamless technology implementations. From software integration to process optimization, we guide you every step of the way.

- Future-Proofing: Technology evolves rapidly. We stay at the forefront of industry trends and emerging technologies, ensuring that your business

[Table of Contents](#)

remains adaptable and competitive in the face of change.

- Measurable Impact: Our success is measured by your success. We're committed to delivering tangible results, whether it's improved operational efficiency, enhanced customer experiences, or increased revenue.



- Collaboration and Empowerment: We're not just consultants; we're collaborators. We work side by side with your team, sharing knowledge and building internal capabilities so that your business can thrive independently.



Experience the ATRC Advantage:

Transform your business with a strategic partner that combines industry expertise, technological acumen, and a passion for innovation. Let's embark on a journey to unlock your digital potential and achieve new heights of success.

[Table of Contents](#)

If you are interested in getting help to improve your business with practical solutions supported with real world feasibility studies, contact us today to discuss how we can tailor our consulting and technology solutions to your unique business needs.



Projects Done

ICT Related Projects:

- Artificial Intelligence for Banking: KYC, AML, and CFT.
- Digital Currencies Exchange Development.
- E-commerce with Warehouse Integration.
- DevOps: Agile, PMP, SDLC, Kubernetes, Jenkins, Docker, AWS, EC2, Appsoy, and Kabanero.

Projects That Make Money:

- Recession Management Business Strategy Development for a Service-Based Client in the UAE.
- Development of Small and Large Scale Economically Feasible Solar and Wind Power Units for Sigma Energy.
- Internet Business Feasibility Studies for Investors.
- Supervising Research on Cost Competitive Solar Power Production.
- Designed, Developed, and Implemented 5 Cities VoIP-Based Satellite Network for Inter-cities and International Call Origination and Termination.

Projects That Made Totally New Technology:

- Design, Development, Testing, and Production of the Fastest File and Device Replication System to Allow Extremely Fast Replication of a Virtual Machine for Disaster Recovery Purposes. This is 20 to 100 Times Faster Than Rsync, Which Was the Fastest Method Available for Files.

Projects That Save Money:

- Development of Digital Banking Security Systems Based on High Security, Reliability, and Performance Experience Gained from the Internet and Telecom Industries. June 2017 and Ongoing Research.
- Researching Businesses for Alternative Energy in Bio-Diesel, Fusion, and Wind Power.
- Developed and Implemented Several ISPs' Customized Billing Software and Bandwidth Management.
- Outsourced IT Support Design and Implementation, LAN, and Printer Sharing Configuration for Cogent, Dubai.
- Design and Implementation of Solar Powered Agricultural Water Pumping Solutions for Farms near Nawabshah, Sindh.

Projects That Save Time:

- Development Faster Deployment of Servers by Evaluating Various DevOps Technologies and Integrating the Best Open Source Software Available. Jan 2019 and Ongoing Research.
- Disaster Recovery of NAS Storage for a marketing company in Media City in Dubai, UAE.
- Remote Server Troubleshooting and Administration Services.

- Installation and Development of Automated Scripts for Backups. Linux-Based File and Print Server with Windows Client Integration. Design and Implementation of a Business Continuity and Disaster Recovery Plan for Data on the Linux-Based File Server and MS Exchange Server. Anti-virus Installation, Monitoring, and Management for the Entire Company. Relay Block List Removal for Company's MS Exchange Mail Server for a Reinsurance Company in Dubai.

Projects That Build Relationships:

- Developed and Proposed the Idea of PSEB's Opensource Resource Center (OSRC).
- **Organized the First Opensource Conference in Pakistan for IBM, PSEB, TReMU, ATRC, PIMSAT, and Ministry of IT from Concept to Finish.**

Projects That Make Work Easier:

- IT Department Setup, Servers for Email, File Sharing, User Management, Automated Backups, and Continuous Monitoring for an Marine supplier based in UAE, Bahrain, and Saudi Arabia.
- Consultancy for Accounting and ERP Software for an Investment company in Karachi, Pakistan.
- Development of Support Infrastructure for Open Source Collaboration Software.
- Implementation and Support for a Network-Based Fax System for a Client in the UAE.
- Implementation and Support for a Web-Based Invoicing System for a Client in the UAE.
- Oracle, Open Source Migration, and E-commerce Infrastructure Management Support for Companies Including: Airlines,

Manufacturing companies, Financial institutions, Distribution, Retail and Pharma companies in Pakistan and UAE.

- Implemented POS, Modified POS Software in Java and Netbeans to Meet Restaurant's Requirements. Added Wireless Printing for a multiple restaurants, Grocery stores, tailoring shops and Shisha joints in Dubai.
- Converted a POS to wireless for a large seating area restaurant in Karachi.

Projects That Expand the Business:

- Development of Appliance Servers: NAS, Mail, Proxy, LDAP, and Backup.
- Developing and Maintaining Call Centers and VoIP Telecoms Networks for Several Investors.

Projects That Retain Existing Customers:

- Security Implementation and Audit of Intensive E-commerce Applications.
- Support for Open Source ERP/CRM/SCM/BI Systems for Organizations.
- Optimized and Secure Proxy Server Designs for Cybercafes.
- Security Policy and Implementation for ISPs.
- Linux and TCP/IP Training of System Administrators of Controller of Naval Accounts (CNA) on AS/400.
- BCMSN, CCNA, CCNP Course for British Petroleum Network Administrators.

Projects Which Attract New Customers:

- Supervising Feasibility Analysis of Elsbett Engine Redesign Costs.
- Support for Open Source ERP/CRM/SCM/BI Systems for Organizations.
- Development of E-commerce Courses as New Offerings.

- Open Source Migration Support and Training and Research for Large Scale Multinational and Government Clients.
- Provided Consultancy and Advice for Mobile Wallets and Payments from Kiosks to Instanet Dubai.
- ERP and CRM Installation and Startup Training for Aesthetic Interiors in Al Ain.
- SAMBA and Squid Proxy Server for electrical contractor and power parts distribution company in Jebel Ali, UAE.

Projects That Solved Specific Problems:

- Developed a MAC Address Based WIFI Server for Hotspots. Added Extreme Proxy Facilities and Utilization of Higher Speed CPUs and More Memory Than the Products Available in the Market. This Project Is a Product Developed for ATRC.
- Created a Software-Based System to Detect Stock Market Manipulation for the Securities and Exchange Commission of Pakistan (SECP).
- Troubleshooting of VoIP Quality Issues on Linux for a Call Center in Karachi.
- E-commerce Security Consultancy for Stock Exchange Companies.
- Designing and Configuration of HTTPS via Squid Based Reverse Proxy Servers on Linux for Outlook Web Access.
- Configuration Debugging for Micropoint's Cisco-Based IP Phones and IVR Telephony System in Dubai.
- Email Server Disaster Recovery for Retailer Group in Sharjah.
- Diagnosed, Troubleshooted, and repaired a wheat quality checking equipment LAB system used by exporters for a University in Pakistan.

Projects That Made Companies More Competitive:

- Installed, Configured, and Continued Support for a Regulatory Authority Linux-Based Servers for Mail Relay, Reverse Proxy, Migration of MS Exchange to Kerio, Win AD Integrated SAMBA Server, Cisco ASA Firewall Configuration. Dubai and Abu Dhabi Offices. Complete Troubleshooting Support for MS Outlook-Based Clients Connecting to Kerio Mail Server.
- Installed, Configured, and Continued Support for a CERT's Linux-Based Servers for Relay Server as a Front End for Exchange with SMTP Two-Way Relay, Reverse Proxy for Outlook Web Access, POP3 Relay Server, Cisco ASA Firewall Settings. Dubai.
- Provision of Analysis, Selection, Deployment, and Maintenance Services for ERP/CRM/SCM Systems for a pharma manufacturer in Pakistan.
- Extremely Effective Implementation of a CRM System for a Client in UAE.
- Security Design, Implementation, and Continuous Monitoring for Organizations.
- Integration of MS Exchange Server with Linux-Based Mail Relays.
- Configuration of Windows and Apple-Based LANs and Internet Connectivity for a satellite insurance company in Dubai.



Trainings done

- Computer security
- Secure programming and coding
- Ethical Hacking (CEH)
- Entrepreneurship
- Project Management
- Maintenance and Reliability Best Practices: Lowering Life Cycle Cost of Equipment
- Network Management and Security
- Marketing and Selling
- Operating systems
- Labor Union Management
- Software project management
- Software engineering
- Enterprise resource planning
- Economic evaluation of prospects and producing properties in oil and gas
- Search engine optimization
- Social Media marketing
- Internet Marketing



[Table of Contents](#)

- Sales force automation
- Ecommerce
- Information and Communication Technology in Management
- Redhat RHCE/RHCT
- Linux professional institute (LPI)
- MS Office
- Staroffice/Openoffice/Libreoffice
- Web development
- Customer relationship management (CRM)
- Supply chain and logistics
- Final Semester Project
- LAMP Linux/Apache/Mysql/PHP
- PostgreSQL
- MS SQLServer
- Oracle
- Data communications
- Linux
- CCNA
- CCNP
- BCMSN
- Virtualization
- Cloud computing
- Funding for entrepreneurship
- Solaris
- Perl/CGI
- Introduction to Programming
- WAP Programming
- Unix
- Advanced Networking
- Computer Graphics
- Distributed operating systems
- Basic Reservoir Engineering for oil and gas.
- Basic oil and gas processing and production.
- Effective Record-keeping in Oil and Gas



- Fundamentals of oil and gas

Contact :

Mr. Khawar Nehal

CEO

Applied Technology Research Center

Email : khawar@atrc.net.pk

S.U.P.P.O.R.T.™
Super User-friendly Professional
People Offering Remote Troubleshooting



Mobile :

+1 563 231 7041

+92 343 2702 932



<http://remote-support.space>

https://atrc.net.pk/dokuwiki/doku.php?id=atrc_website:contact

<http://atrc.net.pk/>

Some of our clients.

[http://atrc.net.pk/dokuwiki/lib/exe/fetch.php?media=atrc_website:clients -](http://atrc.net.pk/dokuwiki/lib/exe/fetch.php?media=atrc_website:clients_-_22_may_2023-1.pdf)

[_22 may 2023-1.pdf](http://atrc.net.pk/dokuwiki/lib/exe/fetch.php?media=atrc_website:clients_-_22_may_2023-1.pdf)

[Table of Contents](#)

Dolibarr

ERP/CRM

<https://www.dolibarr.org/>



1. Dolibarr ERP Support Pricing

Dolibarr Cloud Starter

For personal usage or for very small businesses

Your Dolibarr ERP & CRM

PKR 3000 / month / user

Services provided:

1. ATRC support 24/7 Email English, Voice English and Urdu
2. Dolibarr ERP & CRM (all official modules - [examples](#))
3. Access from everywhere, any browser, any OS
4. Availability 24/7
5. 4 Gb (around 80,000 common invoices, 1€ per extra GB)
6. 2,000 API calls per month
7. Email sending is unlimited if you use the SMTP of your email provider, otherwise 500 emails/day with default setup
8. Support for migration
9. Technical support (by Email in English or French)
10. Functional support (via community forums)
11. Upgrade of version included (on can be requested from the customer dashboard)
12. Daily backup (30 rolling days)
13. Datacenter in France
14. Immediate availability. You decide when you want to cancel (no commitment). Your data can be retrieved. No entry or exit fees
15. Remote SSH, SFTP, rsync and database access
16. Updating or Adding extensions or sourcecode is possible (you can deploy them yourself)

Dolibarr Enhanced

For larger companies

Your Dolibarr ERP & CRM with extended support

PKR 9000 / month + PKR 3600 / month / user

Services provided:

- ATRC support 24/7 Email English, Voice English and Urdu
- Dolibarr ERP & CRM (all official modules - [examples](#))
- Access from everywhere, any browser, any OS
- Availability 24/7
- **20 GB** (around 400,000 common invoices, 1€ per extra GB)
- **5,000 API calls** per month
- Email sending is unlimited if you use the SMTP of your email provider, otherwise 500 emails/day with default setup
- Support for migration
- Technical support (**by priority email** in English or French)
- Functional support (**by email** in English or French)
- Upgrade of version included (can be requested from the customer dashboard)
- Daily backup (30 rolling days)
- Datacenter in France
- Immediate availability. You decide when you want to cancel (no commitment). Your data can be retrieved. No entry or exit fees
- Remote SSH, SFTP, rsync and database access
- Updating or Adding extensions or sourcecode is possible (you can deploy yourself **or request us to deploy**)

[Table of Contents](#)



2. Support Rates for Enterprise Softwares from MuftaSoft™

Hosted on customer premises, in other data centers, multiple locations, or in our data centers.

General	Cost	Free (If the software is completely FOSS/OSI compliant)	Rs 600K per year Rs 50K per month	Rs 1M per year Rs 83K per month
	Number of incidents	0	5 per month	10 per month
	Additional Incidents	0	Rs 25,000 per incident	Rs 17K per incident
Availability	Working Hours	None	9:00 – 17:00 Monday to Thursday and Saturday 9:00 – 12:00 and 14:00 – 17:00 on Friday	9:00 – 17:00 Monday to Thursday and Saturday 9:00 – 12:00 and 14:00 – 17:00 on Friday
Response times	High Priority	Best Effort	Less than 4 Hours	Less than 4 Hours
	Medium Priority	Best Effort	Less than 12	Less than 12

[Table of Contents](#)

			Hours	Hours
	Low Priority	Best Effort	Next business day	Less than 12 Hours
Support Channels	Discussion Forum	Included	Included	Included
	In App Chat	Not included	Included	Included
	Email Support	Not included	Included	Included
	Phone Support	Not included	Not Included	Included
Upgrades	Priority Bug Fixes	Not included	Included	Included
	Major Releases	Not included	Included	Included
	Minor Releases	Not included	Included	Included
	Hot Fix Releases	Not included	Not included	Included
	Small Customizations	Not included	Not included	Included
Service		Description		Price / Cost / Rate
Installation		<p>One-time installation fee. This assumes that you have an account with a hosting provider and just need help installing the software.</p> <ul style="list-style-type: none"> • Basic Installation • Custom Domain • Configure Application • Configure Email • Configure Backups • Configure Monitoring • Configure HTTPS <p>Details are software dependent.</p>		Rs 125K per server

Upgrade	<p>One-time upgrade fee. This assumes that you have a working application installation based on an official release.</p> <ul style="list-style-type: none"> • Latest Releases • Hotfixes <p>Details are software dependent.</p>	Rs 42K per server
Support Incident / Troubleshooting	<p>If you've encountered a problem with your self-hosted server you can request support from us.</p> <ul style="list-style-type: none"> • Screen share Session • Review Server Logs <p>Details are software dependent.</p>	Rs 25K per server
Implementation & Configuration	<p>Includes costs involved in configuring the software as well as implementing your organization's workflows. This can usually be done in-house but may require external resources in cases where technical expertise is not available. This should also include the cost of data backup / restoring processes and contingency plans if the software becomes unavailable due to power/Internet outages and hardware failures.</p>	Rs 83K per server

Online Training	<p>The cost to train employees to use the software, which may include training materials like documentation, tutorials, videos, etc. This will likely be an on-going cost as you'll have to train new employees and update training materials as the software evolves. On-premise training is also available.</p>	<p>Rs 100K per session</p>
------------------------	---	----------------------------

<p>Data Migration</p>	<p>If your organization is using another software system (even if it's just Excel) to manage your supply chain data you'll probably want to move that data to the new software. In either case, you will need to export (e.g. download as CSV), transform (e.g. re-format the data to be imported), clean (e.g. remove duplicate and obsolete data) and most importantly test your data before you can start using the new system. This process can range from manual data-entry to automated data importing using APIs and other data migration tools.</p> <p>Data migrations usually include the following data:</p> <ul style="list-style-type: none"> • Users • Roles • Facilities • Internal Locations • Products • Stock Levels • Current Inventory • Stock History <p>Details are software dependent.</p>	<p>Rs 42K per data item.</p>
------------------------------	--	------------------------------

Data Synchronization	<p>If you plan to host a server in the cloud as well as on-premise, then you'll likely want to configure data replication between your servers.</p> <ul style="list-style-type: none"> • Database Replication • 1 Cloud Server • 1 On-Premise Server <p>Details are software dependent.</p>	<p>Rs 2M per environment</p> <p>NOTE: This does not include on-going maintenance and support.</p>
Custom Report	<p>If you need a custom report or dashboard KPI we can usually turn these around fairly quickly unless we need to build a new data structure.</p> <p>Details are software dependent.</p>	<p>Rs 82K per report</p>

Custom Development	<p>Hopefully the enterprise softwares do everything you need. But in some cases you may need to hire a developer to build new features or improve existing ones. You can purchase Custom Development in chunks of time based on our Estimated Hours. Once the purchase has been made, we will allocate a project manager and developer and begin the requirements gathering process.</p> <p>Estimated Hours</p> <ul style="list-style-type: none"> • Bug Fix (5 Hours) • Improvement (10 - 25 Hours) • New Feature (25 - 50 Hours) • Integration (100+ Hours) 	Rs 20K per hour
---------------------------	--	-----------------

Integration	<p>At some point your organization may want to integrate with an external system i.e. accounting software or an old enterprise resource planning (ERP) system. Integration costs depend on how complicated it will be to communicate between the two systems. Today, most software utilize REST APIs to facilitate communication between systems while older systems use EDI (electronic data interchange) or XML. Integration costs should also include updates to standard operating procedures (SOPs) which may require re-training.</p>	<p>Starts at Rs. 2M</p>
--------------------	---	-------------------------

Discounts

If you would like to purchase larger increments in order to develop multiple customization at one time, we'd be happy to discuss discounted rates. Contact our Support Team, provide them with details about your requirements and we'll get back to you with a quote.

Non-Profits

If you are a non-profit or small business and feel like you cannot afford these rates, please let us know. We can reach out to some of our partners for cheaper quotes. Provide details to our Support Team and we'll refer you to one of our partners.

Business Comprehension



3. Business Comprehension[™] : ERP & SCM Services

Welcome to Business Comprehension[™], your trusted partner for comprehensive ERP

and SCM services. Our cutting-edge solutions empower businesses to streamline operations, enhance productivity, and optimize supply chain management.

Enterprise Resource Planning (ERP)

1. Integrated Modules

- Finance and Accounting
- Human Resources
- Sales and Marketing
- Inventory Management
- Project Management

2. Real-time Analytics

Leverage data-driven insights for informed decision-making and business intelligence.

3. Customization

Tailor our ERP system to meet the unique needs of your business.

4. Scalability

Grow your business with confidence, as our ERP system scales seamlessly.

Supply Chain Management (SCM)

1. End-to-End Visibility

Monitor and control every aspect of your supply chain in real time.

2. Inventory Optimization

Reduce costs and improve efficiency with optimized inventory management.

3. Supplier Collaboration

Strengthen relationships and enhance collaboration with suppliers.

4. Order Fulfillment

Streamline order processing and enhance customer satisfaction.

Why Choose Business Comprehension[™] Solutions?

- **Proven Expertise:** With years of experience, we have successfully implemented ERP and SCM solutions for diverse industries.
- **Customer-Centric Approach:** Our solutions are tailored to meet the unique needs of each client, ensuring maximum value.
- **24/7 Support:** Our dedicated support team is available around the clock to address your queries and concerns.
- **Future-Ready Technology:** Stay ahead in the digital landscape with our innovative and future-ready technologies.

Get Started Today!

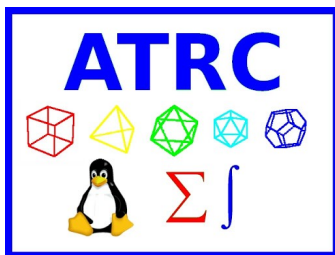
Transform your business with Business Comprehension™ services. Contact us today for a consultation and take the first step toward achieving operational excellence.

Phone: +92 343 270 2932

Email: erp@atrc.net.pk

Website: <http://atrc.net.pk/>

Business Comprehension™ and Dubai Computer Services™ is a part of ATRC.



[Table of Contents](#)



Get your ERP on premise, hybrid or completely in the cloud NOW. Money back guarantees and service level agreements (SLA) available.

Features :

Sales and CRM, Human Resources Management, Products, Stock, Inventory and Warehouse management, Marketing, Productivity, Finance and billing, Integration and Development, Content Management Services, Website, Point of Sale, and many more add on features.

We provide servers for Enterprise Resource Planning (ERP), Customer Resource Management (CRM), Supply Chain Management (SCM), Project Management (PM) Collaboration between teams Special servers for SMEs.

An SME is an organizations with less than 1000 employees. and many more.

These servers allow you to take your organization to new levels of productivity, efficiency, performance and profits.

**Contact : +92 343 270 2932
servers@atrc.net.pk <http://atrc.net.pk>**

Implementation, Consultancy, and Development Services for Dolibarr.

Installation/Setup

User training / Development training

Help and support

Custom development

Dolibarr web hosting (SaaS or cloud hosting)

By :  Muftasoft



Karachi Computer Services

Contact :

<http://atrc.net.pk>

+92 343 270 2932

info@atrc.net.pk

Features

[Table of Contents](#)

CRM & Sales...

Prospects /
Customers



Opportunities



Proposals



Sale Orders



Contracts /
Subscriptions



Help Desk /
Tickets



Human Relationship Management (HR)

Employees



Expense Reports



Leave Requests



Timesheets



Recruitment



Membership



CMS, Website, E-Commerce, POS

CMS / Website



E-Commerce



Point Of Sale



Product & Stock

Products, Services



Stocks



Purchase,
Approvisionnement



Shipments



Manufacturing



Finance & Billing

Billing & Payments



Bank
reconciliation



Double entry
accounting



Productivity

Projects, Tasks



Interventions



Agenda



Marketing

Emailing



Surveys



Integration, Development

API



Connectivity with
external tools



Import, Export



Module Builder for
developers



Prospects and Customers

Track your prospects and customers, and reuse them in other modules.

Create your prospects or customers

17. Just enter the name of the third party and the type of third party (prospect and/or customer) to create it in your database. A unique customer reference code will be automatically generated according to **your numbering rule**.
18. Record any other data (email, address, language, tags, ...) for a more complete and accurate management of your third party database. If the predefined fields do not suit you, you can easily **create all the attributes you need as custom fields** with the datatype of your choice (string, amount, date, combo list, checkbox, ...)
19. **Attach any notes or files** to your prospect/customer sheet.
20. If you have plenty of sales representatives in your team, then you can **assign them to dedicated prospects or customers**, so that you can get statistics per sales representative (Sales, Margins, Events etc.).
21. **Merge third parties** to remove duplicate records.

The screenshot shows the 'MyBig Company' software interface. The top navigation bar includes links for Home, Third parties, Products/Services, Commercial, Financial, Bank/Cash, Projects, HRM, Tools, Point of sale, Documents, and Agenda. The user 'Alice' is logged in. The left sidebar contains a search bar and several menu categories: Third party (New third party, List, List of prospects, New prospect, List of customers, New customer, List of suppliers, New supplier), Contacts/Addresses (New contact/address, List, Prospects, Customers, Suppliers, Other), Custo./Prosp. categories (New tag/category), Contacts tags/categories (New tag/category), Suppliers tags/categories (New tag/category), and Bookmarks (The foundation, Online documentation, Official portal). The main content area has tabs for Third party, Card, Prospect/Customer, Projects, Related items, Bank accounts, Margins, Notifications, Notes, and Linked files. The 'Card' tab is selected, showing the details for 'Company Corp 1'. The company information includes address (21 Green Hill street, Los Angeles, 75500, United States), phone (444123456), email (companycorp1@example.com), and website (http://companycorp1.com). Below this is a table with two columns: Prospect / Customer and Customer tags/categories. The table contains fields like Supplier, Customer code, Bar code, Prof Id, VAT is used, Use second tax, VAT number, Third party type, and Staff. To the right of the table is a section for 'Customers tags/categories' with tags like 'VIP' and 'Regular customer'. Below the table is a 'Linked files' section with a 'Doc template' dropdown, a 'Generate' button, and a list of files including 'FG9800 manualqianann.pdf'. At the bottom right, there are buttons for 'Send email', 'Modify', 'Merge', and 'Delete'.







Create alternative contacts/addresses

If you want, you can create **one or several alternative addresses** for each of your prospects or customers (one record/address for the director, another one for his or her assistant, another one for the

[Table of Contents](#)

delivery or legal service representative etc.). Assign such contacts to any business document (commercial proposals, orders, etc.) so that the correct name will be automatically filled in on any documents which are generated automatically by the system (such as PDF documents).

Contacts/addresses for this third party Create contact/address



Name	Position	Address / Phone / Email	Status	
<input type="text"/>			Enabled	<input type="text"/>
 Einstein	Genius	United States 333444555 genius@example.com	Enabled	 
 Laurent Smith	Director	45 Big road, Seattle, 897, United States	Enabled	 

Set status and potential of your prospects

If you want, you can set **a contact status and a potential** to your prospect. You can define the different prospect potentials/levels according to your business needs.

No need to spend time in modifying the Prospect status after a conversation is completed. **Just modify the status in one click** from the list view without even opening the prospect sheet.

For more advanced prospecting management, you can also use the [lead management module](#).

Company	Customer code	City	Zip Code	Third party type	Phone	Potential	Prospect status	Status	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Prospect	From: None to Medium	Never contacted	Open
A FUTURE CUSTOMER	CU1702-0004					Prospect	To be contacted - x		
MY PROSPECT	CU1702-0003					Prospect	Low	Contact in process - x	

Create and convert your Quotes, Commercial proposals, Sale Orders, Interventions, Invoices, ...

Create rich documents using a WYSIWYG editor while reusing data such as predefined products and prices according to the modules/features that you have enabled, like [Quotes or Commercial proposals](#), [Sales Orders](#), [Interventions](#), [Invoices](#), etc. Manage documents from dedicated menus or directly from the third party sheet. Your prospects can be **converted into customers automatically** when a Quote or Commercial proposal is accepted.

Follow-up your prospects, and your customers

List and filter your database **based on any attribute, tag or status**.

Send emails to your contacts directly from the application, using **predefined email templates**.

Reuse your prospect or customer database to send mass emails with the [Mass emailing module](#)

Export your database with the [Export module](#) to **reuse your qualified records with other external tools**.

[Table of Contents](#)

Find all the events related to your prospects and customers, such as proposal creation, invoice validation, and many other events using the events recorded automatically as per the settings configured in the [module Agenda](#)

Home

Third parties

Products/Services

Commercial

Financial

Bank/Cash

Projects

HRM

Tools

Point of sale

Documents

Agenda

MyBig Company

Search

Third party

New third party

List

List of prospects

New prospect

List of customers

New customer

List of suppliers

New supplier

Contacts/Addresses

New contact/address

List

Prospects

Customers

Suppliers

Other

Custo./Prosp. categories

New tag/category

Contacts tags/categories

New tag/category

Suppliers tags/categories

New tag/category

Dolibarr 5.0.3

Third party

Card

Prospect/Customer

Projects 1

Related items

Bank accounts

Margins

Notifications

Notes

Linked files 1

Events/Agenda

Company Corp 1

21 Green Hill street, Los Angeles, 75500, United States

444123456

companycorp1@example.com

http://companycorp1.com

Created by

Albert Einstein

Creation date

07/10/2010 06:35 PM PHP Time (server) / 07/10/2010 04:35 PM Client time (user)

Modified by

Alice Adminson

Latest modification date

05/12/2017 11:06 AM PHP Time (server) / 05/12/2017 09:06 AM Client time (user)

Create event

Events about this third party

Ref.	Label	Date	Type	Owner	Status
327	Email sent by MyBigCompany To Einstein	05/12/2017 01:53 PM	Automatically inserted events	Alice Adminson	
318	Proposal PR1702-0029 validated	02/16/2017 01:46 AM	Automatically inserted events	PR1702-0029 Alice Adminson	
282	Order CO7001-0023 validated	02/16/2017 12:05 AM	Automatically inserted events	CO7001-0023 Alice Adminson	
270	Order CO7001-0011 validated	02/16/2017 12:05 AM	Automatically inserted events	CO7001-0011 Alice Adminson	
268	Order CO7001-0009 validated	02/16/2017 12:05 AM	Automatically inserted events	CO7001-0009 Alice Adminson	
16	Société Mon client ajoutée dans Dolibarr	07/10/2010 06:35 PM	Other	Albert Einstein	

Opportunities

4. Create and follow all your leads/commercial opportunities

Create your Lead/Opportunity

Create your lead or opportunity.

Include **predefined products** to save you time, or enter **full content manually**. Attach **any external document**.

If predefined fields do not match your needs, **add your own custom fields of any type** (string, amount, date, checkbox, combo list, ...) to the form.

The screenshot displays the MyBig Company software interface. The top navigation bar includes tabs for Home, Agenda, Third parties, Products | Services, Commercial, Billing / Payment, Accountancy, Bank/Cash, Projects, HRM, Tools, Documents, and Point of sale. The left sidebar contains a search bar and a menu with sections: Projects (New project, List, Statistics), Tasks/activities (New task, List, Statistics), Time spent, and Tags/categories (New tag/category). The main content area shows the details for project PJ1607-0001, identified as PROJALICE1, with a third party of NLTechno (The OpenSource company). The project is in the 'Open' state. A table lists project details: Visibility (Project contacts), Opportunity status (Qualification), Opportunity probability (20 %), Opportunity amount (8,000 €), Start date - End date (07/30/2016 12:00 AM - ?), Budget (5,000 €), and Priority (3). To the right, a description field contains 'The Alice project number 1' and a tags/categories field is empty. Action buttons for Modify, Close, Clone, and Delete are visible. Below the project details, there is a 'Linked files' section showing a document 'PJ1607-0001.pdf' (15406 Bytes, 10/10/2017 01:25 PM) and a 'Latest 10 linked events' section with two entries: a phone call by Alice Adminson on 01/31/2017 08:52 PM and a phone call by Charle Commercy on 07/01/2016 10:00 AM.

Ref.	By	Type	Event	Date
240	Alice Adminson	Phone call	Call the boss	01/31/2017 08:52 PM
237	Charle Commercy	Phone call	Phone call with Mr Vaalen	07/01/2016 10:00 AM

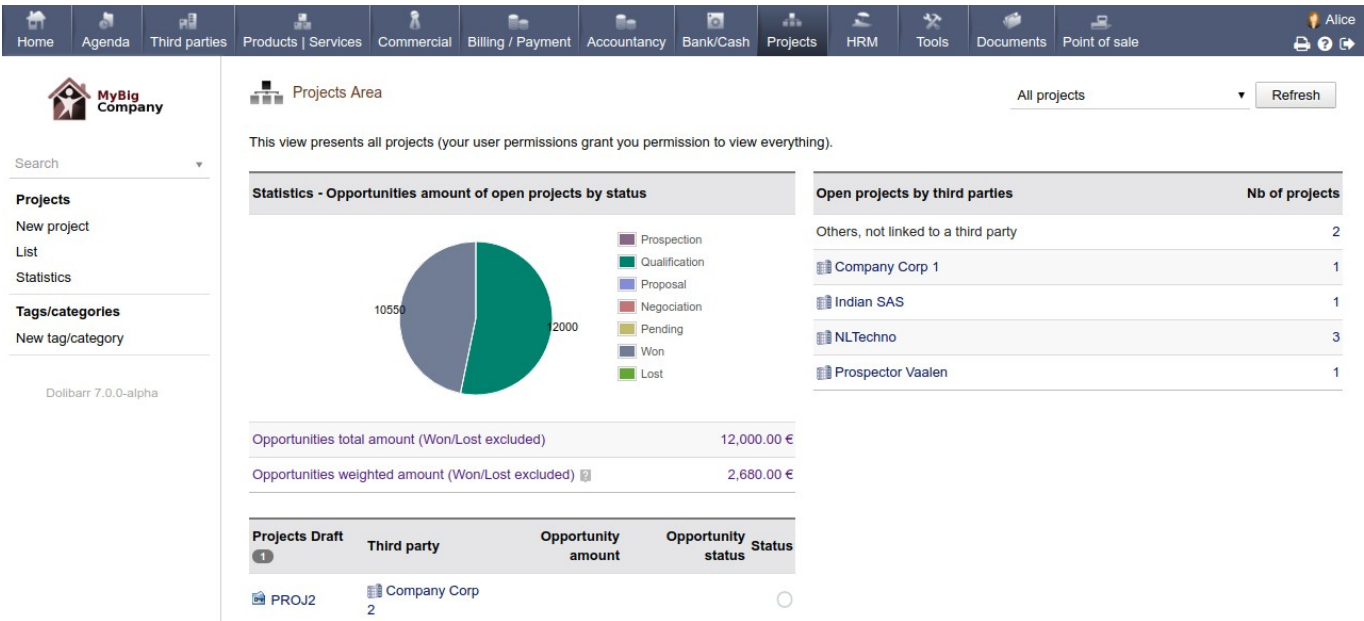
Use your opportunities for a 360 degree view

Create your **quotes as well as commercial proposals** and send them by Email from within the application. Enter events or setup reminders in the agenda. **Link any data (events, quotes, orders, ...)**

[Table of Contents](#)

to your opportunities, so that you can easily find all information from the past with respect to the opportunity.

Define an amount and a probability for winning your opportunities, so that you can have an idea of what will be your **expected turnover** (opportunity amount averaged with the probability)



Change the status of your opportunities into "Won" or "Lost". If the lead is won, you can also **reuse the project to create new tasks** to begin and track the project execution.

Follow your open opportunities

List and display all your open or closed opportunities. **Choose** which information you want to see on your lists. Filter and sort them based on **any criteria**.

Like any other data, export your Opportunities with the [Export module](#), so you can **reuse them with third-party tools**, or connect your existing Data analysis tool directly to the open database for Big Data analysis.

Quotes and Proposals

5. Create and send professional-looking proposals to your prospects and customers instantly...

Create your Quote or Commercial Proposal

Create your quote from your prospect/customer sheet, or just in one click by reusing a previous proposal.

Include **predefined products** to save time, or enter **the full list of products and services manually**. If predefined fields do not match your needs, then add your own custom fields of any type (string, amount, date, checkbox, combo list, ...) to the form.

The screenshot displays the 'MyBig Company' software interface. The top navigation bar includes links for Home, Agenda, Third parties, Products | Services, Commercial, Billing / Payment, Accountancy, Bank/Cash, Projects, HRM, Tools, Documents, and Point of sale. The user 'Alice' is logged in. The left sidebar contains a search bar and a menu with categories: Commercial proposals, Customer orders, Suppliers orders, Contracts/Subscriptions, Interventions, and Supplier proposals. The main content area shows a 'Commercial proposal' form for 'PR1702-0028'. The form includes fields for Ref. customer, Third party (Indian SAS), and Project. It also features a 'Draft (needs to be validated)' status. The form is divided into several sections: Discounts, Date, Validity ending date, Payment terms, Delivery date, Availability delay, Shipping method, Source, and Payment type. A table on the right shows financial details: Amount (net of tax), Amount tax, Amount tax 2, Amount tax 3, Amount (inc. tax), and Margins (Selling price, Cost price, Margin, Margin rate). A table at the bottom lists products and services with columns for Description, Sales tax, U.P. (net), Qty, Reduc., Cost price, Margin rate, and Total (net). The products listed are COMP-XP4548 - Computer XP4523, COMP-XP4523 - Computer XP4523, and COMP-XP4548 - Computer XP4523.

Description	Sales tax	U.P. (net)	Qty	Reduc.	Cost price	Margin rate	Total (net)
COMP-XP4548 - Computer XP4523	0%	100.00	4		0.00	n/a	400.00
COMP-XP4523 - Computer XP4523							
COMP-XP4548 - Computer XP4523							

Process your commercial proposal

The PDF of your commercial proposal is automatically generated and updated.

Send your quote or a selection of quotes via Email, directly from within the application. Use your **predefined email templates** so you don't even have to type any text.

[Table of Contents](#)

Depending on the modules/features you have enabled, you can also convert your commercial proposal into an order (module order), a contract (module contract), intervention (module intervention), invoice (module invoice), or a combination of these. If the module **margin** is enabled, you can also review the margin of your proposals.

Modify the status of your proposals to "Refused" or "Signed". Your prospects are **converted into customers automatically**, as soon as a commercial proposal is signed.

Follow the status of your commercial proposals

List and display all your quotes. Choose which information you want to see in your lists. Filter and sort them based on any criteria.

MyBig Company

Search

Commercial proposals

New proposal

List

Drafts

Open

Signed (needs billing)

Not signed (closed)

Billed

Statistics

Customer orders

New order

List

Statistics

Suppliers orders

New order

List

Statistics

Contracts/Subscriptions

New contract/subscription

List

Services

Interventions

New intervention

List

Statistics

List of commercial proposals (30)

25 1 2 >

Third parties with sales representative: Linked to a particular user contact:

Including product/service with tag:

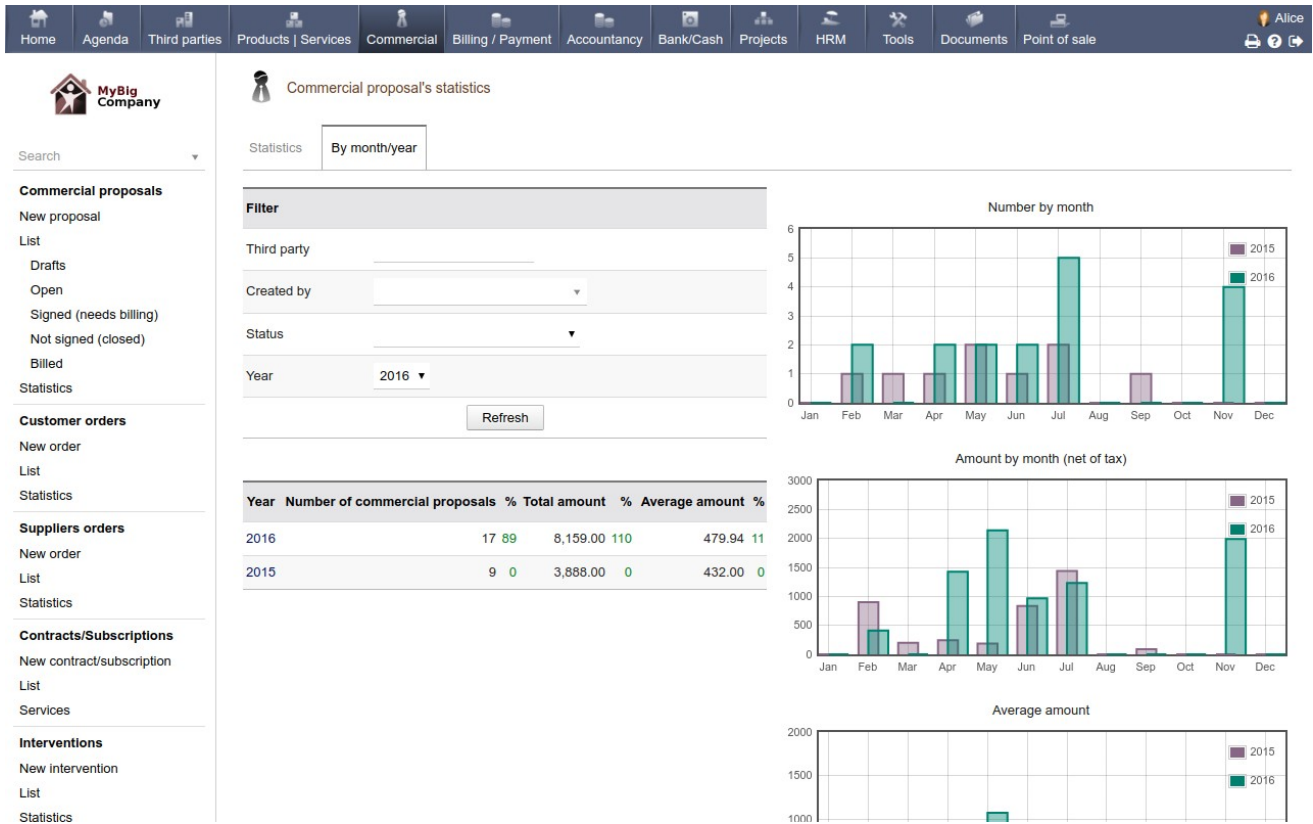
Ref.▲	Ref. customer	Third party	Date	End date	Amount (net of tax)	Author	Creation date	Status
PR1702-0030		Magic Food Store	11/12/2016	11/27/2016	608.00	demo	02/16/2017 01:46 AM	Open
PR1702-0029		Company Corp 1	06/24/2016	07/09/2016	720.00	aeinstein	02/16/2017 01:46 AM	Open
PR1702-0028		Indian SAS	05/01/2016	05/16/2016	400.00	demo	02/16/2017 01:46 AM	Open
PR1702-0027		Indian SAS	07/23/2015	08/07/2015	1,000.00	demo	02/16/2017 01:46 AM	Open
PR1702-0026		Magic Food Store	07/30/2015	08/14/2015	440.00	demo	02/16/2017 01:46 AM	Open
PR1702-0025		Swiss Touch	11/12/2016	11/27/2016	300.00	aeinstein	02/16/2017 01:46 AM	Open
PR1702-0024		Indian SAS	04/03/2016	04/18/2016	710.00	demo	02/16/2017 01:46 AM	Open
PR1702-0023		Spanish Comp	07/09/2016	07/24/2016	1,018.00	aeinstein	02/16/2017 01:46 AM	Open
PR1702-0022		Generic customer	11/13/2016	11/28/2016	250.00	demo	02/16/2017 01:46 AM	Open
PR1702-0021		Dupont Alain	04/03/2016	04/18/2016	715.00	demo	02/16/2017 01:46 AM	Open
PR1702-0020		Patient SuperIII	11/13/2016	11/28/2016	70.00	aeinstein	02/16/2017 01:46 AM	Draft
PR1702-0019		Indian SAS	09/23/2015	10/08/2015	89.00	aeinstein	02/16/2017 01:46 AM	Open
PR1702-0018		Patient SuperIII	11/13/2016	11/28/2016	830.00	aeinstein	02/16/2017 01:46 AM	Open
PR1702-0017		Dupont Alain	03/30/2015	04/14/2015	200.00	demo	02/16/2017 01:46 AM	Open

Ref. Ref. customer Third party City Zip Code State/Province Country Third party type Date End date Amount (net of tax) Amount tax Amount (inc. tax)

Analyze your performance

Use the **predefined yet dynamic statistics pages** to get useful information about your company or your sales representative's performance.

[Table of Contents](#)



Export your proposals with the [Export module](#) to **reuse them with external tools**, or connect your existing BI suite directly to the open database for Big Data analysis.

Sale Orders

6. Manage your customer or supplier orders.
- Manage your order workflow and product stock according to your rules.

Create your Order

Create your orders from your customer sheet, or in a single click by reusing a signed proposal or contract to save time.

Include **predefined products** to save you time, or enter **the list of products and services manually**. If predefined fields do not match your needs, add your own custom fields of any type (string, amount, date, checkbox, combo list, ...) to the form.

Home

Agents

Third

Products

Company

Billing

Accounts

Bank

Project

HRM

Tools

ECon

Docu

Memt

Monit

saa

Web

File n

SelfY

Point

Alice

MyBig Company

Search

Bookmarks

My dashboard

Setup

Company/Organisation

Modules/Applications

Menus

Display

Translation

Default values

Widgets

Alerts

Security

Limits and accuracy

PDF

Emails

SMS

Dictionaries

Other setup

Admin tools

Customer order

Order card

Contacts/Addresses

Shipments

Notes

Linked files

Log

CO7001-0027

Ref. customer : NLTechno (The OpenSource company) (Other orders)

Third party : NLTechno (The OpenSource company) (Other orders)

Project :

Delivered

Discounts

This customer has no relative discount by default. This customer still has credit notes for 12.00 Euros.

Date

02/23/2015

Planned date of delivery

Shipping method

Catch

Payment terms

Due Upon Receipt

Payment type

Currency

EUR - Euros

Currency conversion rate

1

Availability delay

Channel

Phone campaign

Incoterms

Amount (net of tax)

50.00 €

Amount tax

0.00 €

Amount tax 2

0.00 €

Amount tax 3

0.00 €

Amount (inc. tax)

50.00 €

Margins

Selling price

Cost price

Margin

Margin rate

Margin / Products

50.00

0.00

50.00

Margin / Services

0.00

0.00

0.00

Total Margin

50.00

0.00

50.00

Description

Sales tax

U.P. (net)

U.P. (currency)

Qty

Reduc.

Cost price

Margin rate

Total (net)

Total (net in currency)

Process your Order

The PDF of your order is automatically generated and updated.

Send your order acknowledgement by Email directly from within the application. Use your predefined email templates, so you don't even have to type any text.

[Table of Contents](#)

If you decide to manage shipments, **then you can close your orders automatically when all the shipments are completed.** Depending on your setup, if you need to manage stock, your stock may also be automatically increased or decreased as applicable.

List and display all your orders. Choose which information you want to see in your list views. Filter and sort your lists based on any criteria.

Home Agen Third Prod. Comm Billing Accou Bank Proje HRM Tools ECon Docu Ment Monit aaa Webs File r SellY Point

Commercial proposals
[New proposal](#)
[List](#)
[Statistics](#)

Customer orders
[New order](#)
[List](#)
[Draft](#)
[Validated](#)
[In process](#)
[Delivered](#)
[Canceled](#)
[Statistics](#)

Suppliers orders
[New order](#)
[List](#)
[Statistics](#)

Contracts/Subscriptions

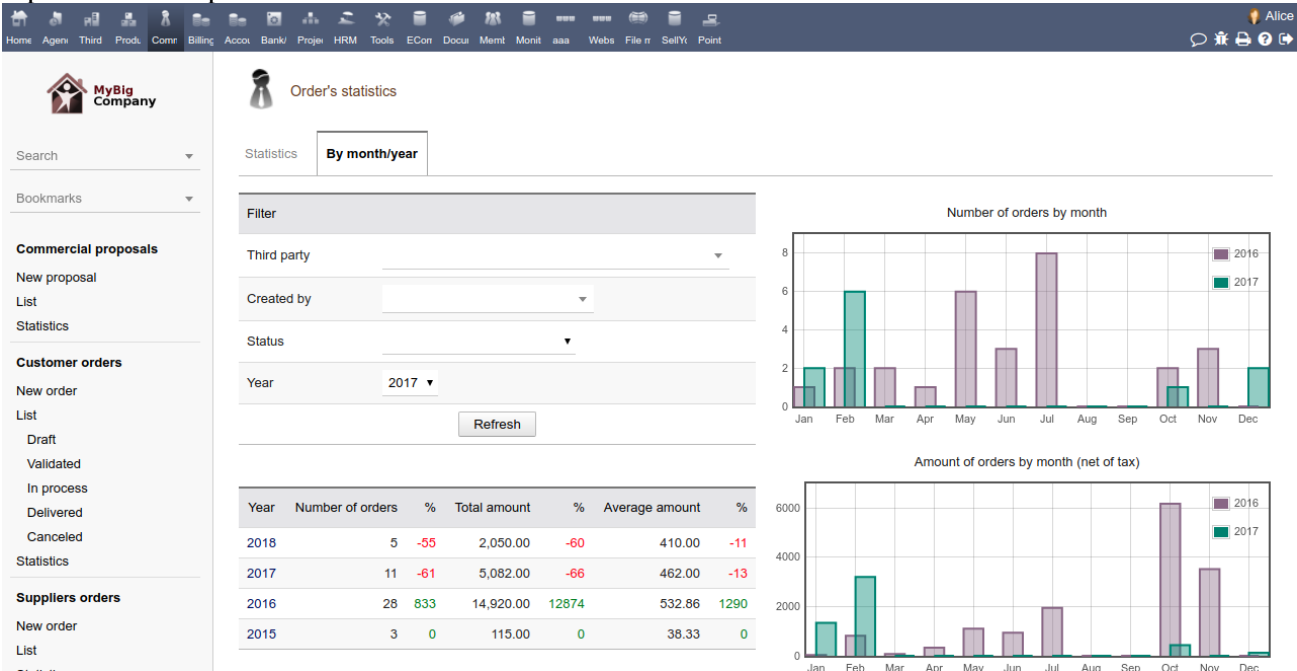
List of orders (67)

Third parties with sales representative:
 Including product/service with tag:
 Linked to a particular user contact:

Ref.	Ref. order for customer	Third party	Order date	Planned date of delivery	Amount (net of tax)	Status	Billed
CO7001-0050	100000019	Customer 1 Customer last	01/10/2018	01/10/2018	500.00	In process	No
CO7001-0049	100000018	Customer 1 Customer last	01/10/2018	01/10/2018	500.00	In process	No
CO7001-0048	100000016	Customer 1 Customer last	01/10/2018	01/10/2018	500.00	In process	No
CO7001-0047	100000016	Customer 1 Customer last	01/10/2018	01/10/2018	500.00	In process	No
CO7001-0046	100000011	Customer 1 Customer last	10/30/2016	10/30/2016	5,250.00	In process	No
CO7001-0045	100000015	Prénom Nom	01/10/2018	01/10/2018	50.00	In process	Yes
CO7001-0044	100000013-1	Prénom Nom	01/10/2018	01/10/2018	45.00	Canceled	No
CO7001-0043	100000013	Prénom Nom	01/10/2018	01/10/2018	150.00	Canceled	No
CO7001-0042	100000011-1	Customer 1 Customer last	11/23/2016	11/23/2016	3,465.00	Validated	No
CO7001-0041	100000008	Customer 1 Customer last	06/08/2016	06/08/2016	210.00	In process	No
CO7001-0040	100000006	Customer 1 Customer last	05/27/2016	05/27/2016	250.00	Processed	Yes

Table of Contents

Use **predefined and dynamic statistics pages** to get useful information about your sales representative's performance.



Export your orders with the [Export module](#) to **reuse them with third-party tools**, or connect your existing BI suite directly to the open database for Big Data analysis.

Contracts and Subscriptions

7. Manage customer/supplier contracts and subscriptions.
Generate recurring invoices of subscriptions automatically.

Create Contract with subscribed services

Create your contract from your prospect/customer sheet, or just in one click by reusing a proposal or an order.

Include **predefined products/services** to save your time, or enter the **full list of products and services manually**.

If predefined fields do not match your needs, add your own custom fields of any type (string, amount, date, checkbox, combo list, ...) to the form.

A PDF of your contract is automatically generated and updated.

The screenshot displays the MyBig Company software interface. The top navigation bar includes various icons and labels such as Home, Agenda, Third p..., Product..., Comm..., Billing / ..., Accoun..., Bank/C..., Projects, HRM, Tools, ECom..., Docum..., Members, Monitori..., aaa, Websites, File ma..., SellYou..., and Point of... The user 'Alice' is logged in. The left sidebar contains a search bar, bookmarks, and a menu with categories: Commercial proposals (New proposal, List, Statistics), Customer orders (New order, List, Statistics), Suppliers orders (New order, List, Statistics), and Contracts/Subscriptions (New contract/subscription, List, Services, Services not active, Running services). The main content area shows the 'Contract card' for 'CT1712-0004'. It includes fields for 'Ref. customer' (abc), 'Ref. supplier', 'Third party' (SweetCustomer), and 'Project'. A progress bar indicates '2 Services: 0 2 0 0'. Below this, there are sections for 'Discount' (This customer has no relative discount by default. This customer has no discount credit available.) and 'Date' (12/05/2017 06:54 PM). The contract details are presented in two tables. The first table, 'Service #1', shows 'DOLICLOUD-...K-Dolibarr - Instance Dolibarr ERP & CRM' with a sales tax of 0%, U.P. (net) of 0.00, U.P. (currency) of 0.00, a quantity of 1, and a status of 'Running, not expired'. The second table, 'Service #2', shows 'Additional users' with a sales tax of 20%, U.P. (net) of 108.00, U.P. (currency) of 0.00, a quantity of 1, and a status of 'Running, not expired'. At the bottom, there are buttons for 'Send by Email', 'Modify', 'Create Invoice', 'Create Order', 'Clone', 'Close all contract lines', and 'Delete'.

Service #1	Sales tax	U.P. (net)	U.P. (currency)	Qty	Reduc.
DOLICLOUD-...K-Dolibarr - Instance Dolibarr ERP & CRM	0%	0.00	0.00	1	
Planned start date: 12/30/2017 - Planned end date: 12/30/2018					
Status of service: Running, not expired					
Real start date: 12/05/2017					

Service #2	Sales tax	U.P. (net)	U.P. (currency)	Qty	Reduc.
Additional users	20%	108.00	0.00	1	
Planned start date: 12/30/2017 - Planned end date: 12/30/2018					
Status of service: Running, not expired					
Real start date: 12/05/2017					

Change the status of your services ("Running", "Disabled") and update the end date at any time. **Attach notes or files** to your contract.

Convert your customer contract into one-time invoices or recurring invoices

[Table of Contents](#)

You can convert your contract into one or several **invoices**. If your contract is supposed to track a **recurring service, then convert it into a recurring template invoice**: Define the frequency, amount, date of the first invoice and/or a maximum number of invoices to generate. Your template invoice will be pre-filled with the data of your contract services, and the invoices will be generated automatically.

The screenshot shows the 'MyBig Company' software interface. The top navigation bar includes links like Home, Agents, Third, Products, Contracts, Billing, Accounts, Bank, Projects, HRM, Tools, E-commerce, Documents, Meetings, Monitoring, Analytics, Websites, File sharing, Selling, and Point of Sale. The left sidebar contains a search bar, bookmarks, and a menu with sections: Customer Invoices (New invoice, List, List of templates, Payments, Reporting, Statistics), Supplier Invoices (New invoice, List, Payments, Reporting, Statistics), Billable orders, Donations, and Special expenses (Social/fiscal taxes). The main content area is titled 'Template invoice for CT1712-0004' and includes a 'Back to list' link. It displays the following information:

- Third party:** SweetCustomer
- Project:** [icon]
- Author:** Alice Adminson
- Amount (net of tax):** 40.50 €
- Amount tax:** 0.00 €
- Amount (inc. tax):** 40.50 €
- Payment terms:** Due Upon Receipt
- Payment type:** Stripe
- Note (public):** [icon]
- Note (private):** [icon]
- Bank Account Number:** [icon]
- Doc template:** [icon]
- Recurrence:**
 - Frequency:** Every 12 months
 - Date for next invoice generation:** 12/30/2017
 - Max nb of invoice generation:** [icon]
 - Status of generated invoices:** Draft (needs to be validated)
 - Nb of invoice generation already done:** 0
 - Date of latest generation:** [icon]

Below this information is a table with the following columns: Description, Sales tax, U.P. (net), Qty, Reduc., Total (net). The table contains one row:

Description	Sales tax	U.P. (net)	Qty	Reduc.	Total (net)
1 DOLICLOUD-PACK-Dolibarr - Instance Dolibarr ERP & CRM	0%	45.00	1	10.00%	40.50

At the bottom, there is a dropdown menu with the text 'Not a predefined entry of type'.

A link is maintained between your template invoice and your contract so that **any invoices generated will also be linked to the contract**.

You can change, at any time, the content of your contract or the content of your template invoice and the way you will bill your customer **without having to break this link**.

Follow and manage your contracts and services

Check which service is expired or is about to be expired. Renew your contract/service before the end date or close them if required.

[Table of Contents](#)

Home

Agenda

Third p...

Product...

Comme...

Billing / ...

Accoun...

Bank/C...

Projects

HRM

Tools

ECom...

Docum...

Members

Monitori...

aaa

Websites

File ma...

SellYou...

Point of...

Alice

MyBig Company

Search

Bookmarks

Commercial proposals

New proposal

List

Statistics

Customer orders

New order

List

Statistics

Suppliers orders

New order

List

Statistics

Contracts/Subscriptions

New contract/subscription

List

Services

Services not active

Running services

List of running services (5)

25

Including product/service with tag:

Contract	Service	Third party	Real start date	Planned end date	Status	
					Running	Q X
CONTRACT1	CAKECONTRIB - Cake making cont...	Spanish Comp	Nov 14, 2017		Draft	
CONTRAT1	CAKECONTRIB - Cake making cont...	Teclib	Jul 10, 2010	Feb 13, 2017	Expired	
CT1712-0004	DOLICLOUD-PACK-Dolibarr - Instance Dolibar...	SweetCustomer	Dec 05, 2017	Dec 30, 2017	Expired	
CT1712-0004	Additional users	SweetCustomer	Dec 05, 2017	Dec 30, 2018	Not expired	
CT1712-0005	DOLICLOUD-PACK-Dolibarr - Instance Dolibar...	a	Dec 22, 2017		Not expired	

Export your Contracts and Services along with their status with the [Export module](#) to **reuse them with third-party tools**, or connect your BI suite directly to the open database for Big Data analysis.

8. Manage a help desk / follow issues.

A portal for your partner or customers to report tickets or issues

Text soon available...

Follow and answer tickets

Text soon available...

Create tickets automatically from emails

Use the module **Email Collector** to scan input mailboxes and create tickets automatically.

Employees and Users

9. Manage your users, user groups, and permissions

Create your employee/user accounts

Create user accounts for your employees (**internal users**) and/or for your customers, suppliers, or partners (**external users**). Creating an account for your employees will allow them to access data in Dolibarr and to interact with all the application features such as Third parties, Business documents, and other applicable modules according to the access control permissions that have been defined.

Creating a user only requires saving a **name**, a **login name**, and a **password**. Many other options and data can be set, such as **job position**, **gender**, **notes**, **attaching external files**, **status** etc. You can also set a **user color** so that you can identify user events easily on the [agenda](#) module.

MyBig Company

Rechercher

Marque-pages

Mon tableau de bord

Configuration

Société/Organisation

Modules/Applications

Menus

Affichage

Traduction

Valeurs/Filtres/Tri par défaut

Widgets

Alertes

Sécurité

Limites et précision

PDF

Emails

SMS

Dictionnaires

Divers

Outils d'administration

Utilisateurs & Groupes

Dolibarr 9.0.0-beta

Utilisateur

Fiche utilisateur

Permissions

Interface utilisateur

Import calendriers externes

Notifications

Configuration Google

Note de frais

HR et banque

Note

Fichiers joints

Suivi

Alice Adminson

testidr9@dolicloud.com

Retour liste


Actif

Identifiant	admin	Couleur de l'utilisateur	
Mot de passe	*****	Tags/catégories	
Administrateur	Oui	Dernière connexion	26/10/2018 14:35
Type	Interne	Connexion précédente	26/10/2018 13:25
Genre	Femme	Environnement	Toutes les entités
Salarié	Oui	aaa	
Responsable hiérarchique	Zack Zeceo	Lien tiers / contact	Cet utilisateur n'est ni un prospect, ni un client, ni un fournisseur
Poste/fonction	Admin Technical	Lien adhérent	Utilisateur non lié à un adhérent
Tarif horaire moyen	50.00 €	Signature	Alice - 123 __USER_LASTNAME__ __MYCOMPANY_NAME__
Tarif journalier moyen			
Salaire			
Heures de travail (par semaine)			
Date d'embauche			
End date of Employment			
Date de naissance			
Compte comptable			



ENVOYER EMAILMODIFIER

Define the hierarchy of your employees/users



Set the hierarchy of your employees, so that when filling in [leave requests](#), [expense reports](#), and in other respective modules, the supervisor of the employee will be notified to validate the request.































List of users (Hierarchical view)
List view

Hierarchical view

 Undo expand
 |
  Expand all

Status

<div>  Laurent Destailleur (ldestailleur) </div>	
<div>  <div>  Zack Zeceo (zzeceo) </div> </div>	
<div>  <div>  Alice Adminson ★ (admin) </div> </div>	
<div>  <div>  Charle Commercy (ccommercy) </div> </div>	
<div>  Commerson Charle1 (cc1) </div>	
<div>  Commerson Charle2 (cc2) </div>	
<div>  Bob Bookkeeper  (bbookkeeper) </div>	
<div>  David Doe (demo) </div>	
<div>  <div>  Sam Scientol (sscientol) </div> </div>	
<div>  Pierre Curie (pcurie) </div>	
<div>  Marie Curie (mcurie) </div>	
<div>  Albert Einstein (aeinstein) </div>	

Define an hourly rate for each of your employees

Define an **hourly rate** for each employee, so that if they use the [timesheet feature](#), their time spent will be converted into a value in your currency. If you use the [module Project](#), you will be able to see the cost applicable for the time spent by your employees as part of the profitability of your projects.

Set an user e-mail and a nice corporate email signature

Saving an **e-mail address** on the user's card will allow the user to send emails from within Dolibarr. Their **signature** will be displayed in each email sent from Dolibarr.

Set permissions for your users or groups

You can prevent users from having access to certain Dolibarr features and confidential data by defining appropriate user permissions on the user card's 'permissions' tab.

If you have a lot of users, then you must consider **creating user groups, define permissions on those user groups, and assign users to those groups.**

Personalize the display for each user

Each user can personalize the environment, including language, theme, entry page, and also the dashboard.

Leave requests, expenses reports, and timesheets

Depending on which applications are enabled and which permissions have been assigned, users will have the ability to create [leave requests](#), [expense reports](#), and [timesheets](#). Leave requests and expense reports will have to be approved by the user's supervisor, who will be notified via email when a leave request or expense report is submitted by the user.

[Table of Contents](#)

Expense Reports

10. Let your employees record their expense reports. Approve and follow their payment.

Expenses reports feature offers a workflow to let your employees make their expense report. The manager will receive alerts to refuse or approve the expense report. You can also follow if it has been paid or not.

Expense report requests

Let your employees fill in their expenses reports. A permission system tell who can and can't record such requests.

Join any files (proof of purchase, receipts, bills, ...) to the expense report.

Expense report

ADMIN-ER00002-150101

User: Alice Adminson

Period: From 01/01/2015 to 01/03/2015

Validation date: 01/22/2016 07:06 PM

User responsible for approval: Alice Adminson

Payments	Date	Type	Bank account	Amount
1	02/16/2017	Check		5.00
2	02/16/2017	Check	LUXBAC	1.00
Already paid:				6.00
Amount claimed:				60.00
Remaining unpaid:				54.00

Line no.	Date	Project	Type	Description	Sales tax	U.P. (inc. tax)	Qty	Amount (net of tax)	Amount (inc. tax)
1	01/01/2015	PROJ1	Lunch		20%	10.00	1	8.33	10.00
2	01/08/2015	PJ1607-0003	Transportation	Taxi to Paris	0%	50.00	1	50.00	50.00

1 linked files

MODIFY VALIDATE AND SUBMIT FOR APPROVAL CLONE DELETE

Define the type of expense reports in the dictionaries, so you will be able to have **accurate statistics**. If you use the module [Accounting](#), each type of expense may be dispatched into a different accounting account.

Link expense reports to your **lead/projects** and retrieve them in the project overview.

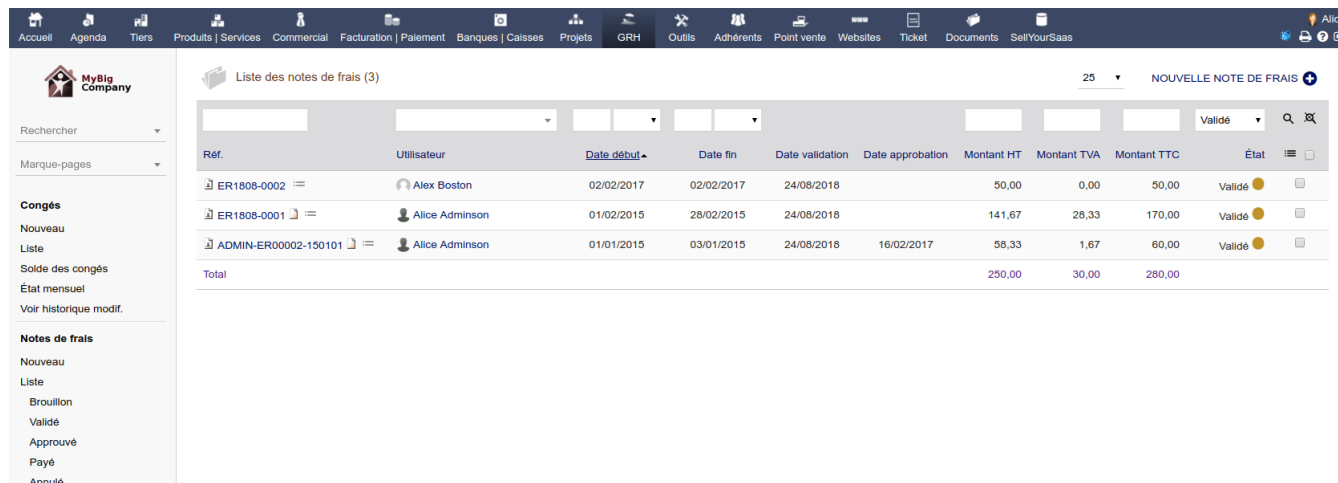
Validate and send e-mail for approval

[Table of Contents](#)

Validate your expense report for approval. An E-mail is generated automatically and sent to the employee supervisor.

Approve the expense report

As a manager, find all the expense reports waiting for your approval, and validate or refuse them.



Réf.	Utilisateur	Date début	Date fin	Date validation	Date approbation	Montant HT	Montant TVA	Montant TTC	État
ER1808-0002	Alex Boston	02/02/2017	02/02/2017	24/08/2018		50,00	0,00	50,00	Validé
ER1808-0001	Alice Adminson	01/02/2015	28/02/2015	24/08/2018		141,67	28,33	170,00	Validé
ADMIN-ER00002-150101	Alice Adminson	01/01/2015	03/01/2015	24/08/2018	16/02/2017	58,33	1,67	60,00	Validé
Total						250,00	30,00	280,00	

Refuse the expense report or **approve it**. And let your employee know why an request was refused.

Pay the expense report

Follow which expense report was paid or not.

Export data

Use the **export wizard** to export all the data required by your **bookkeeper** or by any **payroll providers**.

[Table of Contents](#)

Leaves

11. Allows your employees to make leave requests.
Once the leave request is approved, the system automatically decreases the leave balance.


Define different types of leaves/holidays

According to your country and its laws, define all the types of leaves and define how the leave requests are managed.

Code	Label	Manage a counter	Notice period	New by month	Country	Status		
LEAVE_OTHER	Other leave	0	0	0.00000	-			
LEAVE_PAID	Paid vacation	1	7	0.00000	-			
LEAVE_SICK	Sick leave	0	0	0.00000	-			
LEAVE_PAID_FR	Paid vacation	1	30	2.08334	FR - France			
LEAVE_RTT_FR	RTT	1	7	0.83000	FR - France			

Create a leave request

Give your employees the permission to create their own leave requests.



Search

Bookmarks

Employees

New employee

List

Leave

New

List

Draft

Awaiting approval

Approved

Canceled

Refused

Balance of leave

Monthly statement

View change logs

Expenses reports


New

List

Leave

Card

Linked files



HL1810-0002

Back to list

Awaiting approval

User

Alice Adminson

Type

Sick leave

Start date (First day of vacation)

10/25/2018 Morning

End date (Last day of vacation)

10/25/2018 Afternoon

Number of days of vacation consumed

1

Description

Requested by

Alice Adminson

Will be approved by

Alice Adminson

Creation date

10/25/2018 11:59 AM

APPROVE

REFUSE

CANCEL

Approve or refuse each leave request

[Table of Contents](#)

As a supervisor, you will receive an **e-mail which contains a direct link to the leave request record** of your subordinate. You can use the link to navigate into the system and accept or reject the leave request. The employee will get a notification informing him or her about the status of the leave request.

Analyze and update the balance of leave/holidays

The application will **update automatically (or not), the balance** for each type of leave/holidays.

List and filter leave requests

List and **filter all leave requests according to their status, date, employee, or any other property.** Export your data into text files.

Get a **monthly statement** of leave requests.

As a Human Resources manager, **edit the balance of each user, for each type of holiday or leave,** at any time.

Track leave requests and remaining leave/holidays

As an employee, consult the status of all your leave requests and your balance of remaining leave/holidays.

The screenshot displays the MyBig Company HRM interface. The top navigation bar includes links for Home, Agenda, Memb..., Third..., Produ..., Com..., Billing..., Bank..., Accou..., Leads..., HRM, Tools, Ticket, Docu..., Webs..., DoICl..., Point..., and Point... The user profile for Alice Adminson is shown, with a photo, name, email (testid9@dolicloud.com), and status (Enabled). Below the profile, the leave balance is 15 days, and the paid vacation is 15 days. A button labeled 'MAKE A LEAVE REQUEST' is visible. The main section displays a table of leave requests for Alice Adminson (All entities).

Ref.	Creation date	Employee	Approbator	Type	Days consumed	Start date	End date	Status	
HL1810-0001	10/25/2018	Alice Adminson	Alice Adminson	Sick leave	1 days	10/24/2018 (Morning)	10/24/2018 (Afternoon)	Refused	
HL1810-0002	10/25/2018	Alice Adminson	Alice Adminson	Sick leave	1 days	10/25/2018 (Morning)	10/25/2018 (Afternoon)	Awaiting approval	
HL1803-0003	03/20/2018	Alice Adminson	Alice Adminson	Sick leave	1 days	03/20/2018 (Morning)	03/20/2018 (Afternoon)	Approved	
158	03/20/2018	Alice Adminson	Alice Adminson	Sick leave	0.5 days	03/31/2018 (Afternoon)	04/02/2018 (Afternoon)	Canceled	
157	03/20/2018	Alice Adminson	Alice Adminson	Sick leave	4 days	03/14/2018 (Morning)	03/19/2018 (Afternoon)	Approved	
155	03/20/2018	Alice Adminson	Alice Adminson	Sick leave	2 days	02/28/2018 (Morning)	03/01/2018 (Afternoon)	Approved	
154	02/09/2018	Alice Adminson	Alice Adminson	Other leave	1 days	02/09/2018 (Morning)	02/09/2018 (Afternoon)	Approved	

[Table of Contents](#)

Timesheets

12.
- Enter the time spent on user-friendly timesheets. See the impact on the project's profit.

Fill your timesheet using the interface that suits your needs.

Several solutions are available to enter your timesheets, from a **weekly grid**, to a **daily grid** and **monthly grid**...

Home

Ager

Mem

Thirt

Prod

Com

Billin

Bank

Acco

Leac

HRM

Tool

Tick

Docu

Web

Doll

Poin

Poin

MyBig Company

Search

Bookmarks

Leads | Projects

New lead or project

List

List open leads

List open projects

Statistics

Tags/categories

Tasks/activities

New task

List

Statistics

Time spent

Dolibarr 9.0.0-beta

Time spent

Input per week

Input per day

This view is limited to projects or tasks you are a contact for. Only open projects are visible (projects in draft or closed status are not visible). Only tasks assigned to you are visible. Assign task to yourself if it is not visible and you need to enter time on it.

Task executive

Assign task to me

< 2018, Week 43 > (Today)

Refresh

User: Alice Adminson (All entities)

Project

Third Party

Task	Planned workload	Declared progress	Time spent (Everybody)	Time spent (Alice)	Mon 10/22/18	Tue 10/23/18	Wed 10/24/18	Thu 10/25/18	Fri 10/26/18	Sat 10/27/18	Sun 10/28/18	
Total - Expected worked hours per week: 0					05:00	08:00	09:00	06:00	07:00	00:00	00:00	35:00
PROJ1 - Company Corp 1 - Project One												
TK1810-0001 Analyze	10:00	0 %	02:30	--:--								
TK1810-0003 Specification	05:00	25 %	03:00	01:00								
TK1810-0002 Development	--:--	0 %	01:00	--:--	5:00	6:00	6:00					
TK1810-0004 Tests	88:00	0 %	--:--	--:--					7:00			
RMLL - Project management RMLL												
2 Heberger site RMLL	--:--	0 %	19:00	19:00		02:00	03:00	06:00				
Total - Expected worked hours per week: 0					05:00	08:00	09:00	06:00	07:00	00:00	00:00	35:00

Save

Input per week

[Table of Contents](#)

MyBig Company

Search

Bookmarks

Leads | Projects

New lead or project

List

List open leads

List open projects

Statistics

Tags/categories

Tasks/activities

New task

List

Statistics

Time spent

Dolibarr 9.0.0-beta

Time spent **Input per week** **Input per day**

This view is limited to projects or tasks you are a contact for. Only open projects are visible (projects in draft or closed status are not visible). Only tasks assigned to you are visible. Assign task to yourself if it is not visible and you need to enter time on it.

Task executive Assign task to me

Friday 10/26/2018 (Today) Refresh

User Alice Adminson (All entit... Project Third Party

Task	Planned workload	Declared progress	Time spent (Everybody)	Time spent (Alice)	Start hour	Duration	Note
Total						08:00	
PROJ1 - Company Corp 1 - Project One							
TK1810-0001 Analyze	10:00	0 %	03:30	01:00	00 : 00	01:00 + 3 : mn	Reading documentation
TK1810-0003 Specification	05:00	25 %	03:00	01:00	00 : 00	+ 4 : mn	Meeting marathon
TK1810-0002 Development	--:--	0 %	01:00	--:--	00 : 00	+ H : mn	
TK1810-0004 Tests	88:00	0 %	--:--	--:--	00 : 00	+ H : mn	
RMLL - Project management RMLL							
2 Heberger site RMLL	--:--	0 %	19:00	19:00	00 : 00	+ H : mn	
Total						08:00	

Save

Input per day
or from the **project** , or from a specific **task**...

Enter the **progress (optional)** at the same time that you enter the **time spent** on a task.

See the impact of time spent on the project's profit

If an hourly rate has been defined for the user on his or her user record, then the **time spent is automatically converted into your currency** and this is included into **your project's profit overview**.

[Table of Contents](#)

Home

Agenda

Memb...

Third ...

Produ...

Com...

Billing...

Bank [...]

Accou...

Leads...

HRM

Tools

Ticket

Docu...

Websi...

DotiCl...

Point ...

Point ...

Alice

MyBig Company

Search

Bookmarks

My Dashboard

Setup

Company/Organization

Modules/Applications

Menus

Display

Translation

Default values/filters/sorting

Widgets

Alerts

Security

Limits and accuracy

PDF

Emails

SMS

Dictionaries

Other Setup

Admin Tools

Users & Groups

Dolibarr 9.0.0-beta

Project

Project

Project contacts 3

Overview

Tickets

Notes 1

Linked files

Tasks 4

Time spent ...

Events/Agenda

PROJ1

Project One

Third Party : Company Corp 1 (alias)

Open

Visibility

Project contacts

Lead status

Lead probability

Lead amount

Start date - End date 07/09/2010 - ?

Budget

Description

Tags/categories

From

to

Refresh

Profit

Element	Number	Amount (net of tax)	Amount (inc. tax)
Customers invoices	5	900.00	901.65
Expense reports	1	-8.33	-10.00
Time spent on tasks	4	-693.50	-832.20
Profit		198.17	59.45

List of the commercial proposals related to the project

Select element

Link to element

Create proposal

Analyze and Export your timesheets

Use the [Export module](#) to **export the timesheets** of users and projects.

Review the predefined reports, or connect your data analysis tools directly to the database in order to perform an accurate analysis of your projects.

Recruitment

13. Define your job positions, publish them, track applications.

The module recruitment is designed to manage the recruitment of your new employees.

Define Job positions

Enter the information for your new **job positions**.

Publish your open job positions

A public page is available to publish all your job positions.

Manage the recruitment process

Record all applications, follow and update the status of each applications.

Record applications automatically with the Email Collector

You can setup the Email collector module to automatically create applicants and record all applications for a job position.

All emails exchanged during process can also be collected and linked to the application.

Membership management

14. Manage the memberships of an association or a foundation.

15. A CMS module to build your Website in few minutes.

Build your company's public website or private intranet quickly and **reuse all the information available in your ERP** to make your website dynamic.

Create your website

Use **existing website templates** to save you precious time, so you can get your website ready in just a few seconds.

Or, create a website and build the page content from scratch using the website editor. You don't need any technical knowledge to use the website editor. However, if you are an experienced developer or webmaster, then you can use the HTML and CSS embedded editor to build a fully custom website.

You can **export, clone** and **import** a full website in just a few clicks.

Use the container/page architecture to organize content

Organize pages or content into containers. Include any container/page into other containers/pages. For example, you can have a top-level container to define the template of a website that includes a container for your header, another one for your footer and another one for the main content. There is no limit on the number of levels for embedded containers/content, so you have a more powerful and more flexible CMS than any other traditional CMS like Joomla, Wordpress or Drupal, in which case the position of the content is defined by a template.

Test your website with no need of any external web server

Dolibarr includes its own web server, so you can preview your website content without the need to install a web server.

Include dynamic content on your website

Because the website is integrated into your ERP system, you can include any data coming from your ERP system easily. All the objects required to read your data are available automatically and can be accessed and manipulated using PHP code snippets that you can embed into your web pages/containers whenever you need them.

Serve your website with your own server like Apache or Nginx

[Table of Contents](#)

Once your website is ready to be online, just create a virtual host in your favorite web server like Apache, Nginx, or other server that points to the directory where your website pages are generated and your website is running, including dynamic content provided by your ERP, even if your ERP is not exposed to the Internet.

eCommerce

16. Sell online with your own E-commerce platform or use the embedded E-commerce CMS.

If you use an external eCommerce solution

If you have an online shop/eCommerce platform, you can synchronize it with Dolibarr ERP and CRM by using external synchronisation modules. You may find external modules developed by third parties on www.dolistore.com for most major Open Source E-Commerce solutions.

Most eCommerce solutions are fully or partially supported, such as **Prestashop**, **Magento**, **OsCommerce**, **Woocommerce**, **OpenCart**, etc.

If you use the embedded eCommerce solution

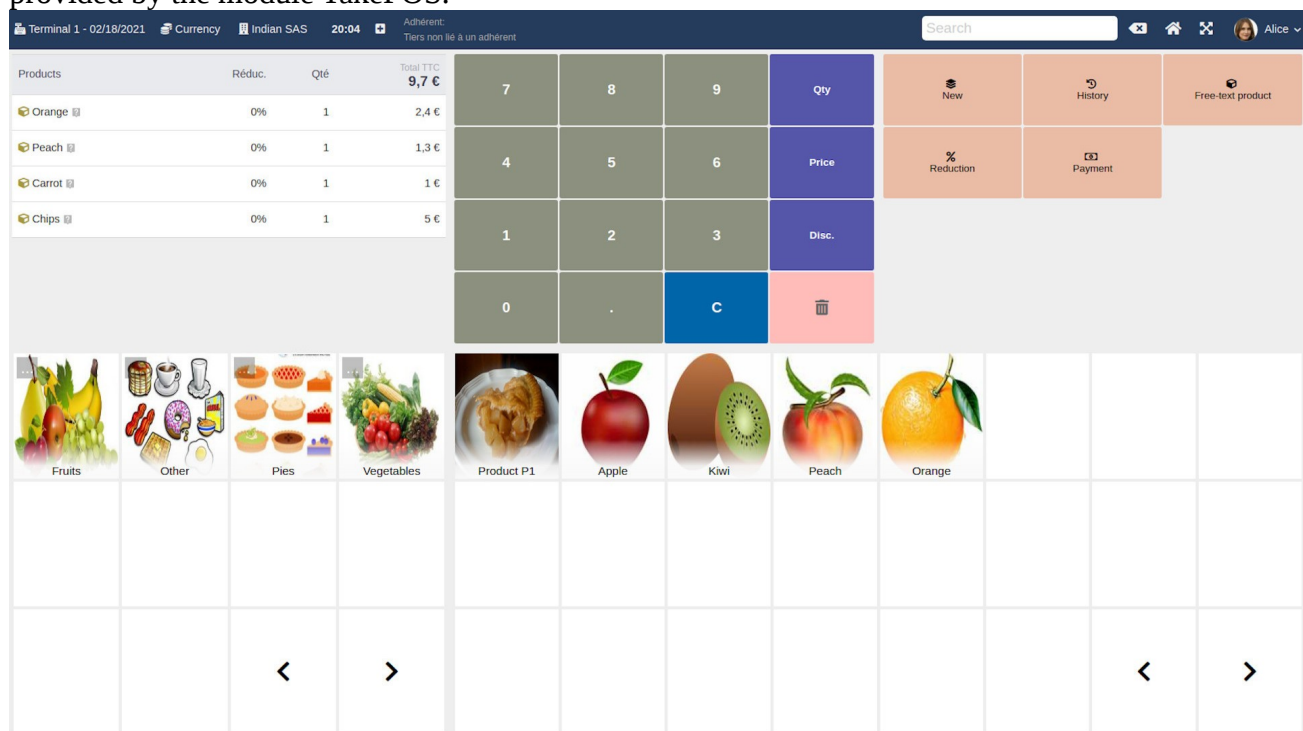
In the future, Dolibarr will provide its own eCommerce module, so you won't need to install any integration and synchronisation services between your ERP and your eCommerce platforms. The integration will be readily available in the box. The tentative date of availability is: the end of 2022.

Point Of Sale (POS)

17. Use TakePOS, the latest generation of Point Of Sale system, to record orders or payments in your shop, bar, or restaurant

A touchscreen POS

Dolibarr provides a **POS interface (Point Of Sale)** for traditional shops as well as for Bars and Restaurants. All the features you need to manage a Point Of Sale with one or several POS terminals is provided by the module TakePOS.



Manage Bars and Restaurants

Define your floors, rooms, and tables with a drag and drop interface. You can assign orders and invoices to any given table on the floor.

Display a QRCode in your bar or restaurant, so your customers can access an interface for contactless, self-order

This feature called "Auto Order" allows you to display a QR Code in your shop, bar, or restaurant so that each customer, by scanning the QR code, can access a simple application and place the order themselves.

[Table of Contents](#)

Automatic Stock update

You can set the application to automatically decrease your stock when an order is processed, so that your stock is always up to date in real-time.

Make the cash fence of the day...

More documentation coming soon...

Products and Services

18. Manage your product and service catalog, and your prices and margins

Manage your product and service catalog

Create and update your product or service catalog. You will be able to reuse the catalogs in all the other features available in the application with one click (proposals/quotations, orders, invoices, and stocks). Manage **the sale or purchase status**.

A lot of native data can be defined on the product and service cards such as **sale prices, tax rate, duration or dimension, cost price, accounts, accounting, stocks, notes** or add your **own personalized custom fields....** Describe your products or services in any language of your choice. Any data can be reused in other modules, thus saving you a lot of time.

Attach any files (Pictures, Photos, PDF notices, ...) to your products.

The screenshot displays the 'Product card' for 'COMP-XP4523 Computer XP4523'. The interface is divided into a top navigation bar, a left sidebar, and a main content area. The sidebar includes 'My dashboard' and 'Setup' options. The main content area has tabs for 'Card', 'Selling prices', 'Buying prices', 'Translation', 'Virtual product', 'Statistics', 'Related items', 'Variants', and 'Stock'. The 'Card' tab is active, showing product details such as Type (Product), Barcode type (EAN13), Barcode value (0000000000001), Accounting codes, Use lot/serial number (Yes), Description (A powerfull computer XP4523), Public URL, and Default warehouse (WAREHOUSEHOUSTON). It also displays physical attributes like Weight (1.7 kg), Length x Width x Height, Area, Volume, Customs / Commodity / HS code (USXP765), Origin country (United States), Ecotax, and Tags/categories (SaaS Products). The product is marked as 'For sale' and 'For purchase' with green indicators.

Clone Products and Services to **create new ones in just a few clicks**, or reuse the Variant feature to generate variant products (similar products with a different color or size, for example)

Manage your selling and buying prices

Define your selling and/or buying prices, and **keep a history of all your changes**. Define your prices **per customer segment, per quantity, or per customer**.

[Table of Contents](#)

Track the performance of your products or services

Filter your product catalog on any property of your choice.

Products (14) 20 New product

Tags/categories:

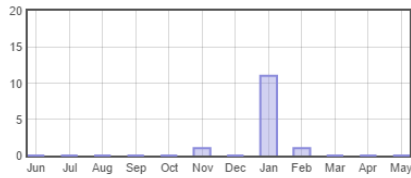
For purchase

Ref.	Label	Selling price	Best buying price	WAP	Physical stock	Virtual stock	Creation date	Modif. date	Status (Sales)	Status (Purchases)	
APPLEPIE	Apple Pie	5.00 Net of tax	9.00 Net of tax	10.00	991	964	07/10/2010 04:44 PM	04/24/2018 12:27 PM	For sale	For purchase	
APPLEPIE_J1_A1	Apple Pie	5.00 Net of tax		0.00	0	0	11/26/2017 11:39 PM	04/24/2018 12:27 PM	For sale	For purchase	
APPLEPIE_J1_L1_A1	Apple Pie	5.10 Net of tax		0.00	0	0	11/26/2017 11:39 PM	04/24/2018 12:27 PM	For sale	For purchase	
APPLEPIE_J2_L2_A1	Apple Pie	5.00 Net of tax		0.00	0	0	11/26/2017 11:39 PM	04/24/2018 12:27 PM	For sale	For purchase	
CAKECONTRIB	Cake making contribution	5.00 Net of tax		0.00	887	872	07/09/2010 02:30 AM	04/24/2018 12:27 PM	For sale	For purchase	
COMP-XP4523	Computer XP4523	100.00 Net of tax		0.00	100	61	12/31/2008 02:00 AM	04/24/2018 12:27 PM	For sale	For purchase	
		100.00									

Predefined and dynamic statistical reports allow you to view graphs, charts, and tables showing you the quantity and amount of products and services offered in proposals, orders and/or invoices.

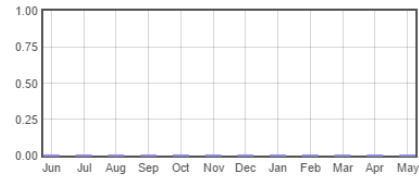
✓ Statistics in number of products/services units / Statistics in number of referring entities

Number of units on proposals in past 12 months



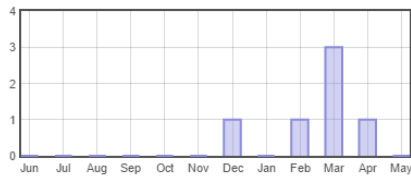
Build on 05/09/2017 02:59 PM

Number of units on supplier proposals in past 12 months



Build on 05/09/2017 02:59 PM

Number of units on customer orders in past 12 months



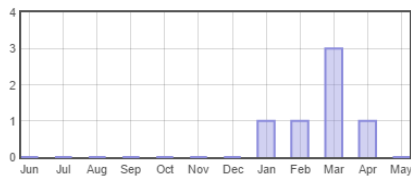
Build on 05/09/2017 02:59 PM

Number of units on supplier orders in past 12 months

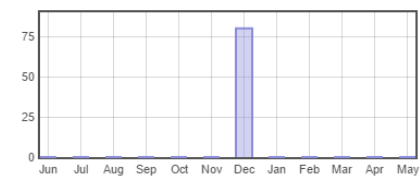


Build on 05/09/2017 02:59 PM

Number of units on customer invoices in past 12 months



Number of units on supplier invoices in past 12 months



Margins

If you use the purchase features, the [margins module](#) may help you to review financial data and margins for each product or service.

And more...

Kit/Virtual products

Define virtual products with quantities of sub-products, so that when the stock of your virtual product is modified, **stocks of sub-products will also be modified automatically.**

Variant products

If you want to sell variants of a product (for example, a dress can be pink or blue, size S or XL etc.), use the **variant editor** to create your product variants quickly and easily.

Stock, lots, and serial management

[Table of Contents](#)

Choose the way Dolibarr will **manage your stock automatically** for you. Decide at a product level if you need to follow **serial or lot numbers**, by using the [Stock module](#) and let the application calculate your **Weighted Average Price (WAP)**.

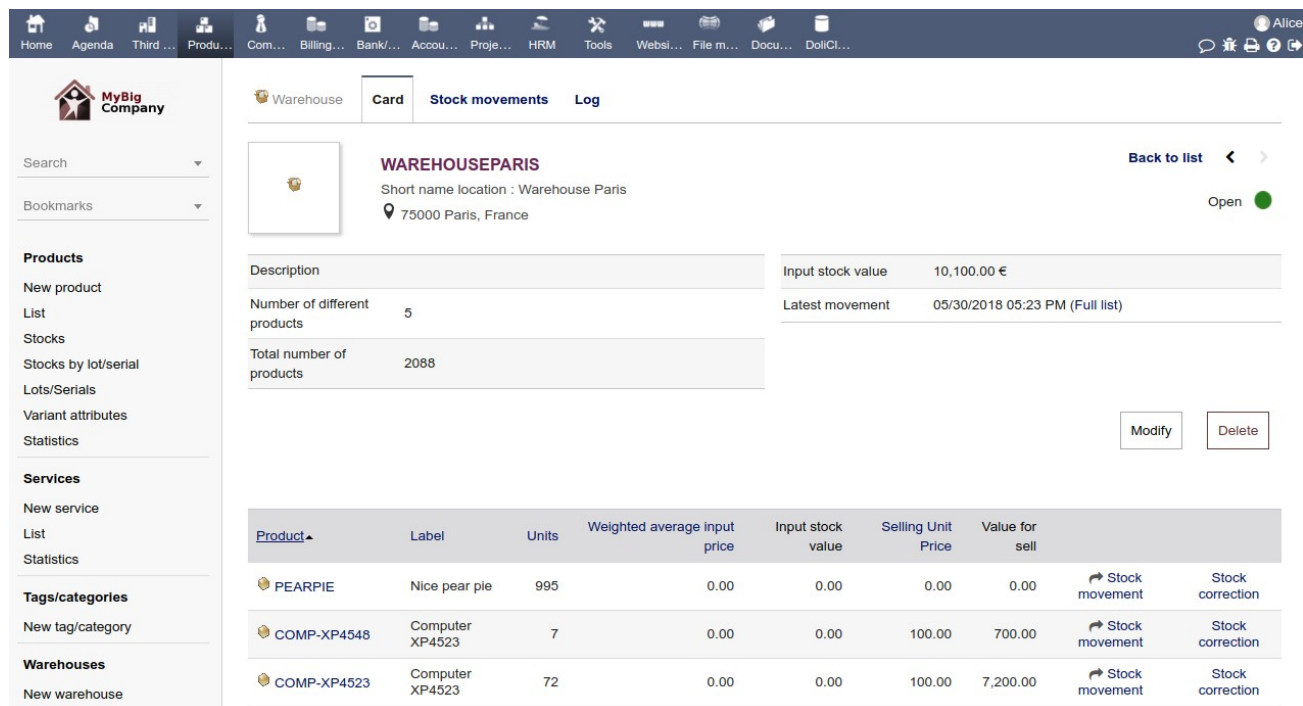
Stock and Warehouse Management

19. Manage stock and warehouses (emplacement)
If you need to, you can add support for Lots or Serial numbers

Warehouses

Organize your warehouses and emplacements. Use them to store your products and define stock movements. Track you stock based on **product reference, warehouse, date, and/or lot/serial number**.

Get an updated visualization of your stock using **Weighted Average Price calculation** or **Standard calculation**.



MyBig Company

Search

Bookmarks

Products

- New product
- List
- Stocks
- Stocks by lot/serial
- Lots/Serials
- Variant attributes
- Statistics

Services

- New service
- List
- Statistics

Tags/categories

- New tag/category

Warehouses

- New warehouse

Warehouse Card

WAREHOUSEPARIS

Short name location : Warehouse Paris

75000 Paris, France

Back to list

Open

Description

Input stock value 10,100.00 €

Number of different products 5

Latest movement 05/30/2018 05:23 PM (Full list)

Total number of products 2088

Modify Delete

Product	Label	Units	Weighted average input price	Input stock value	Selling Unit Price	Value for sell	Stock movement	Stock correction
PEARPIE	Nice pear pie	995	0.00	0.00	0.00	0.00	↻ Stock movement	Stock correction
COMP-XP4548	Computer XP4523	7	0.00	0.00	100.00	700.00	↻ Stock movement	Stock correction
COMP-XP4523	Computer XP4523	72	0.00	0.00	100.00	7,200.00	↻ Stock movement	Stock correction

Stock Movements

Record your stock movement **manually** and/or configure **your application to increase or decrease your stock automatically** (on invoice, on order, or on shipment validation...)

Retrieve any stock movement in your log record

[Table of Contents](#)

List of stock movements (55) 20 1 2 3 >

Ref.	Date	Product ref.	Lot/Serial	Warehouse	Author	Inv./Mov. code	Movement label	Origin	Qty
23	11/13/2017 03:17 PM	CAKECONTRIB	789	Personal stock Laurent Destailleur	Adminson ...	171113151748	Correction du stock pour le produit CAKECONTRIB		789
17	02/16/2017 04:12 AM	COMP-XP4523	5599887766452	WAREHOUSEHOUSTON	Adminson ...		Expédition SH1702-0002 supprimée		1
31	11/24/2017 06:19 PM	COMP-XP4523	5599887766452	WAREHOUSEHOUSTON	Adminson ...		Expédition SH1711-0004 validée	SH1711-0004	-1
34	12/01/2017 08:34 PM	COMP-XP4523	5599887766452	WAREHOUSEHOUSTON	Adminson ...		Expédition SH1712-0006 validée	SH1712-0006	-2
38	12/01/2017 08:53 PM	COMP-XP4523	5599887766452	WAREHOUSEHOUSTON	Adminson ...		Expédition SH1712-0008 validée	SH1712-0008	-1
25	11/24/2017 06:02 PM	COMP-XP4523	5599887766452	Stock personnel hosting	Adminson ...	171124180235	Transfert de stock du produit COMP-XP4523 dans un autre entrepôt		5

Automatic virtual stock and easy replenishment process

Take your stock workflow setup into consideration to always display the real stock or virtual stock (ie. stock position once all your customer or supplier orders are shipped).

Use both your real stock and virtual stock to **make your replenishment in just a few clicks.**

Make mass stock change, inventory or transfer in one step

Use the stock transfer page to record in **one transaction, several stock transfers.**

Home

Agenda

Third ...

Produ...

Com...

Billing...

Bank/...

Accou...

Proje...

HRM

Tools

Websi...

File m...

Docu...

DollCI...

Alice

MyBig Company

Search

Bookmarks

Products

New product

List

Stocks

Stocks by lot/serial

Lots/Serials

Variant attributes

Statistics

Services

New service

List

Statistics

Tags/categories

New tag/category

Warehouses

New warehouse

Mass stock transfer

Select a product, a quantity, a source warehouse and a target warehouse, then click "Select". Once this is done for all required movements, click onto "Record transfer".

Product ref.	Lot/Serial	Source warehouse	Target warehouse	Qty	
APPLEPIE_J1_L1_A1 - Apple Pie	123456	Personal stock Alex Theceo	WAREHOUSEHOUSTON	5	
APPLEPIE_J1_L1_A1 - Apple Pie	123457	Personal stock Alex Theceo	WAREHOUSEHOUSTON	3	
APPLEPIE_J2_L2_A1 - Apple Pie		Personal stock Charly Commery	WAREHOUSEPARIS	4	
COMP-XP4548 - Computer XP4523		Personal stock Charly Commery	WAREHOUSEPARIS	10	
COMP-XP4548 - Computer XP4523		Personal stock Charly Commery	WAREHOUSEPARIS	-3	

Movement or inventory code

20180530171201

Movement label

Stock transfer 2018-05-30 17:12

Record transfer

Define a **desired quantity for each product** so that the replenishment tool will be able to generate supplier orders automatically to restore the stock. See the page [Purchase/Approvisionnement](#).

Lots and serial management

If you need to, you can **use the Lot/Serial number management**. Products defined to be managed by Lots will require a lot number for tracking. You can also set **properties to your lot like Sell-by date or Eat-by-date**.

Retreive **details of stocks and movements for a particular lot** at any time.

Purchase And Supply

20. Manage your Purchase Order Workflows, Restock your Warehouses.

Purchase Orders

Create Purchase Orders, Approve, Receive and Bill your Purchase Orders . Grant users and groups **permissions on the workflows**. Define **the thresholds** which will **automatically trigger email notifications** when they are breached.

Home

Aggr

Thirc

Prod

Com

Bilin

Banl

Acco

Proj

HRN

Tools

Merr

Web

File

Incid

Doc

Dolk

Alice

MyBig Company

Search

Bookmarks

Commercial proposals

New proposal

List

Statistics

Customer Orders

New order

List

Statistics

Purchase orders

New order

List

Draft

Validated

Approved

Ordered

Partially received

All products received

Canceled

Refused

Statistics

Contracts/Subscriptions

New contract/subscription

List

Services

Vendor proposals

Purchase order

Order card

Contacts/Addresses

Item receipts

Notes

Linked files 1

Events/Agenda

PO1806-0001

Ref. vendor

Third party : Book Keeping Company

Project

Request author Einstein Albert

Discounts You have no default relative discount from this supplier.
You have no discount credit available from this supplier.

Payment terms

Payment type

Planned date of delivery

Delivery delay in days

Incoterms

Amount (net of tax) 5,090.00 €

Amount tax 509.00 €

Amount tax 2 0.00 €

Amount tax 3 0.00 €

Amount (inc. tax) 5,599.00 €

Description	Supplier's product ref.	Sales tax	U.P. (net)	Qty	Reduc.	Total (net)
1 APPLEPIE - Apple Pie		12.5%	0.00	1		0.00
2 COMP-XP4523 - Computer XP4523		10%	509.00	10		5,090.00

SEND EMAIL

DISAPPROVE

MAKE ORDER

CREATE INVOICE

CLONE

CANCEL ORDER

DELETE

Linked files

Doc template muscadet English (United St...) Generate

Concat PDF file

PO1806-0001.pdf 15 Kb 06/16/2018 02:53 PM

Events on order

CREATE EVENT

Ref.	By	Type	Title	Date
1725	Adminson Alice	Auto	Order PO1806-0001 approved	06/16/2018 02:52 PM

Receive your Products

If you are tracking your stock, then use the stock dispatching wizards to receive products in your warehouses.

Home

Ager

Thirc

Prod

Com

Billin

Bank

Accc

Proj

HRM

Tools

Merr

Web

File

Incid

Doc

Dolk

Alice

MyBig Company

Search

Bookmarks

Commercial proposals

New proposal

List

Statistics

Customer Orders

New order

List

Statistics

Purchase orders

New order

List

Draft

Validated

Approved

Ordered

Partially received

All products received

Purchase order

Order card

Contacts/Addresses

Item receipts

Notes

Linked files 1

Events/Agenda

PO1806-0001

Ref. vendor :

Third party : Book Keeping Company

Project :

Back to list

Ordered

Date

June 16, 2018, 12:00 AM

Method

Fax

Request author

Einstein Albert

Description	Qty ordered	Qty dispatched	Qty to dispatch	Warehouse
<div>APPLEPIE - Apple Pie</div> <div>This product does not use lot/serial number</div>	1	1		
			1	WAREHOUSEHOUSTON (Stock:-5)
<div>COMP-XP4523 - Computer XP4523</div> <div>FG789</div>	15	9		
			2	WAREHOUSEPARIS (Stock:72)
<div>AZ896</div>			4	WAREHOUSEHOUSTON (Stock:24)

The status of your stock is always kept up to date. Calculation of **Weighted Average Price** can be done automatically.

Procurement Management

Use the wizard to provision and stock your warehouses based on **defined optimal quantities**. Take into consideration, **open customer orders and open purchase orders** and automatically calculate the correct quantity to buy. **Generate** your Purchase Orders automatically.

Home

Aggr

Thirt

Prod

Com

Billin

Bank

Accc

Proj

HRM

Tool

Merr

Web

File

Incid

Docc

Doll

MyBig Company

Search

Bookmarks

Products

New product

List

Stocks

Stocks by lot/serial

Lots/Serials

Variant attributes

Statistics

Services

New service

List

Statistics

Tags/categories

New tag/category

Warehouses

New warehouse

Replenishment

Status

Replenishment orders

This is a list of all products with a stock lower than desired stock (or lower than alert value if checkbox "alert only" is checked). Using the checkbox, you can create supplier orders to fill the difference.
Current selection mode: Virtual stock - Use physical stock

Supplier

Filter

Alerts only

Draft

Q

X

<input type="checkbox"/>	Ref	Label	Desired optimal stock	Limit for alert	Virtual stock	Ordered	To order	Supplier's product ref.
<input type="checkbox"/>	COMP-XP4523	Computer XP4523	200	150	<div>85</div>	<div>15</div>	<div>100</div>	-- No supplier price/qty defined for this product --
<input type="checkbox"/>	COMP-XP4548	Computer XP4523	200	150	<div>-6</div>	<div>0</div>	<div>206</div>	-- No supplier price/qty defined for this product --
<input type="checkbox"/>	DOLIDROID	DollDroid, Android app for Dollibarr			<div>-15</div>	<div>0</div>	<div>15</div>	-- No supplier price/qty defined for this product --
<input type="checkbox"/>	PINKDRESS	Pink dress			<div>-46</div>	<div>0</div>	<div>46</div>	NLTechno - aaa - 100 €/1 Unit

Create orders

[Table of Contents](#)

Shipments

21. Use the shipping module to track your picking list, orders and quantity to ship or shipped

Create your shipments in **one click from any order**. Compare the quantity shipped with the quantity to ship.

Define the planned date of delivery for each of your shipment so you can process them by priority or follow late shipments. If you need more information on your shipment, you can setup application to manage any other custom fields you need.

MyBig Company

Home Agenda Third ... Produ... Com... Billing... Bank [...] Accou... Proje... HRM Tools Websi... Incide... Docu... DoliCL...

Search

Bookmarks

Products

- New product
- List
- Stocks
- Stocks by lot/serial
- Lots/Serials
- Variant attributes
- Statistics

Services

- New service
- List
- Statistics

Tags/categories

- New tag/category

Warehouses

- New warehouse
- List
- Movements
- Mass stock transfer
- Replenishment

Shipments

- New shipment
- List
- Draft
- Validated

Shipment card

SH1712-0006

Ref. customer :
Third party : Prospector Vaalen
Project :

Validated

Ref. order : CO7001-0008

Creation date : 12/01/2017 08:34 PM

Planned date of delivery :

Weight : 3.4 kg

Width :

Height :

Depth :

Volume :

Shipping method : Transporter

Tracking number :

Incoterms :

Products	Qty ordered	Qty in other shipments	Qty to ship	Source warehouse	Lot/Serial	Calculated weight	Calculated volume
1 PEARPIE - Nice pear pie	2		2	WAREHOUSEPARIS	NA	0 kg	0 m³
2 CAKECONTRIB - Cake making contribution	1		1	WAREHOUSEHOUSTON	Lot/Serial details	0	0
3 COMP-XP4523 - Computer XP4523	4		2	WAREHOUSEHOUSTON	Lot/Serial details	3.4 kg	0 m³

SEND EMAIL CREATE INVOICE GENERATE DELIVERY RECEIPT CLOSE DELETE

Linked files

Events on shipment

CREATE EVENT




Doc template merou English (United St... Ref. By Type Title Date

When creating a new picking sheet, **weight or volume** of your items can be both **calculated automatically from predefined product data** or **manually defined**.

Your **stock is updated automatically** when you make a new shipment. And record of your stock movement are directly linked to the shipment.

[Table of Contents](#)

Easily track your shipment with a direct **link to the transporter tracking tool** that is automatically filled.

Shipping method		UPS
Tracking number		201703ZZ_ABYH
Incoterms		

Generate the PDF of the shipment sheet and **print it** for your transporter or send it by email directly from the application to any partner.

My Big Company

Shipment sheet

Ref. shipment : SH1703-0003
Planned date of delivery : 03/11/2017
Customer code : CU1702-0005

Sender:

My Big Company

Adresse
ZIP VILLE

Phone: 0123456789 - Fax: 0987654321
Email: contact@mybigcompany.com

Recipient:

A CUSTOMER

Ref. order : CO1702-0003
Order date : 02/27/2017

Incoterm : -

Tracking number : 201703ZZ_ABYH
Link to track your package
Shipping method: UPS : [201703ZZ_ABYH](#)

Description	Weight/Vol.	Qty ordered	Qty to ship
pd1 - Product 1		2	2

If necessary, you can also manage / generate a **delivery receipt**.

[Table of Contents](#)

Manufacturing

22. Bills Of Materials and Materials Resources Planning

BOMs (Bills Of Materials)

Create your nomenclatures (BOMs) to define how to consume raw products or services to produce manufactured products (Quantity to consume, efficiency, stock impact, ...).

Home

Third...

MRP

Produ...

Proje...

Com...

Billing...

Banks...

HRM

Docu...

Agenda

Ticket

Tools

Websi...

POS

12.0.1

Alice

Search

Bills of material

New bill of material

List

Manufacturing Orders

New Manufacturing Order

List

BOM

Notes

Linked files

Events

BOM1911-0001

Enabled

Label

BOM For the Home Apple Pie

Estimated duration

Product

APPLEPIE

Warehouse for production

Quantity

1.00

Total cost

7.00

Description

Unit cost

7.00

Description	Qty	Frozen Qty	Stock change disabled	Manufacturing efficiency	Cost price
POS-APPLE - Apple	4			1	0.00
CAKECONTRIB - Cake making contribution	1		Yes	1	0.00
PEARPIE - Pear Pie	1	Yes		1	7.00

BACK TO DRAFT

DISABLE

CREATE MO

CLONE

DELETE

Linked files

Doc template

template_bom.odt

English (United St...

GENERATE

BOM1911-0001_bom.odt

28 Kb

07/07/2020 10:19 PM

Latest 10 linked events

See all

Create event

Ref.	By	Type	Title	Date
659	Alice	Auto	Nomenclature (BOM) validée	07/07/2020 10:19 PM

Manufacturing Orders

Reuse the predefined BOMs to generate your Manufacturing Orders.

Produce your Manufacturing Order in one or several steps.

If the stock of produced product is being increased and the stock of consumed product is being decreased automatically, you can get a view of all such changes in your history.

[Table of Contents](#)

The application will calculate, **in real time**, the virtual stock taking into account all the open Manufacturing Orders.

The screenshot shows a software interface for managing Manufacturing Orders. The top navigation bar includes icons for Home, Third-party, MRP, Production, Stock movements, Notes, Linked files, and Events. The main content area displays details for a specific Manufacturing Order (MO2001-0006) under the 'Production' tab. The order is for 'Calculation Power' and is currently 'In progress'. The interface includes a 'BOM' (Bill of Materials) section with a table showing the components and their quantities. Below this, there are buttons for 'CONSUME OR PRODUCE', 'CONSUME AND PRODUCE ALL', 'CLOSE', and 'CANCEL'. At the bottom, there are two tables: 'Consumption' and 'Production', which show the current status of the order and the materials consumed.

Product	Qty	Qty already consumed	Warehouse	Lot/Serial
POS-APPLE	4	1		
01/13/2020 03:13 PM				
CAKECONTRIB	1	0	WAREHOUSEH1	

Product	Qty	Qty already produced	Warehouse	Lot/Serial
APPLEPIE	1	0		

Lots and Serial Management

If you need to, you can activate the **Lot/Serial number management** feature. Products defined to be managed by Lots will require a **lot number** to be manufactured.

Follow your production by Lots and retrieve **details of stock movements for a particular lot** at any time, starting from the production process to the customer shipment.

Export your Manufacturing Orders with the [Export module](#) to **reuse them with external tools**, or connect your existing BI suite directly to the open database for Big Data analysis.

Billing and Payments

23. Manage the invoices and payments of your customers and suppliers

Create your Invoices

Create your invoices (**common invoices**, **down payments**, **credit notes**) from scratch or from your customer sheet. Depending on the modules / features you have enabled, you can also generate your invoice from your proposals (Proposal module), your orders (Order module), your contracts (Contract module) and / or interventions (Intervention module). If the module **Margin** is enabled, margin can be calculated from the best supplier, the cost price or the average weight price of your products. You will get margin statistics per product, customer, date etc.

Include **predefined products** to save you time, or enter **full content manually**.

If predefined fields do not match your requirements, add your own fields of any type (string, amount, date, checkbox, combo list etc.) to the invoice form.

Your invoices can also be **generated automatically** using the recurring template invoices.

The document of your invoice (PDF, ODT etc.) is automatically generated and updated.

The screenshot displays the MyBig Company software interface. The top navigation bar includes various icons and the user's name 'Alice'. The left sidebar contains a search bar, bookmarks, and a menu for 'Customer Invoices' and 'Supplier Invoices'. The main content area shows a 'Customer Invoice' card for 'FA1801-0067'. The card includes details such as 'Ref. customer', 'Third party', and 'Project'. Below the card, there are two tables: one for invoice details and another for payments and margins.

Type	Standard invoice
Discounts	This customer has no relative discount by default. This customer has no discount credit available.
Invoice date	01/13/2018
Payment terms	Due Upon Receipt
Payment due on	01/13/2018
Payment type	Debit payment order
Bank account	
Incoterms	

Amount (net of tax)	2,450.00 €
Amount tax	245.00 €
Amount (inc. tax)	2,695.00 €

Payments	Date	Type	Bank account	Amount
PAY1801-0040	01/13/2018	Direct debit payment order	LUXBAC	1,000.00
Already paid (without credit notes and down payments) :				1,000.00
Billed :				2,695.00
Remaining unpaid :				1,695.00

Margins	Selling price	Cost price	Margin	Margin rate
Margin / Products	2,450.00	1,900.00	550.00	28.95%
Margin / Services	0.00	0.00	0.00	
Total Margin	2,450.00	1,900.00	550.00	28.95%

[Table of Contents](#)

Send your invoice and manage payments

Send your invoice via Email directly from the application. Use **predefined email templates** so that the email content is automatically filled in.

Generate a **Direct Debit SEPA file** for automatic bank payments in batch and follow the integration steps specific to your bank. **Close your invoice by automatically changing it to the paid status** once the bank has processed your SEPA file.

Provide your customer a **link to pay online** using [Paypal](#), [Stripe](#), Paybox, PayZen, etc.





Welcome on our online payment service

This screen allow you to make an online payment to MyBig Company.

This is information on payment to do :

Creditor	MyBig Company
Third party	Indian SAS
Description	Payment invoice FA1801-0067 Download document
Amount	1,695.00 Euros
Payment code	INV=FA1801-0067.CUS=1

 Pay with Credit or Debit Card (Paybox)

 Pay with Credit or Debit Card (Stripe)

 Pay with Paypal (Credit Card or Paypal)

Reuse down payment into another invoice to **reduce the amount to pay** or reuse a credit note into another invoice **to reduce the remaining amount to pay**.

Follow the status of your open Invoices

List and display all your orders. Choose which information you want to see in your lists. Filter and sort based on any criteria.

With the batch feature, **get reminded about all your unpaid invoices**.

[Table of Contents](#)

Customers invoices (4)

-- Select action -- Confirm 25

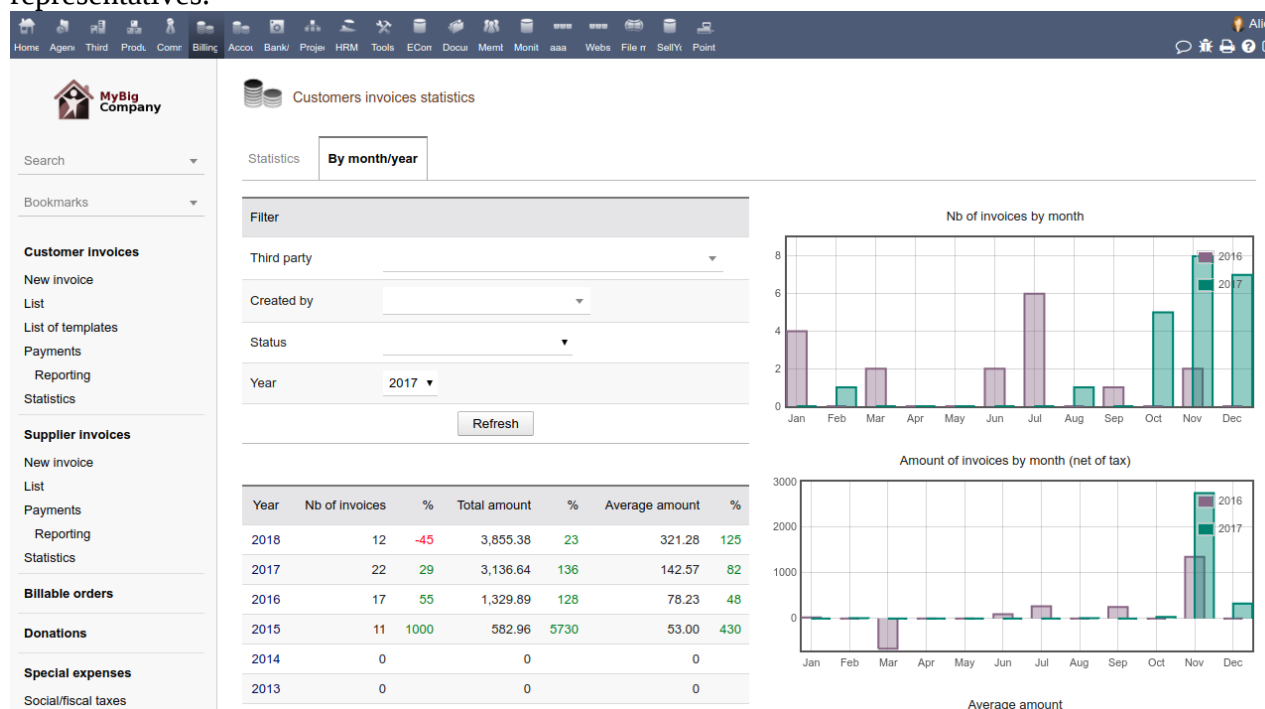
-- Select action --
Send by EMail
PDF Merge

Third parties with sales representative: Linked to a particular user contact: Pending product/service with tag:

Ref.	Ref. customer	Invoice date	Due date	Third party	City	Zip Code	Payment type	Amount (net of tax)	Status
FA1702-0004		02/28/2017	03/01/2017	CLIENT 1				125.00	Not paid
FA1701-0001		01/13/2017	01/14/2017	CLIENT 1				25.00	Paid
FA1701-0005		01/13/2017	01/14/2017	CLIENT 1				50.00	Not paid
FA1701-0002		01/13/2017	01/14/2017	CLIENT 1				50.00	Not paid
Total								250.00	

Analyze your billing performance

Use **predefined statistic pages** to get useful information about the performance of your sales representatives.



Reuse your invoices with other modules

Export your **invoices into the ledger** of the [accounting module](#) to get your accountancy done automatically in just a few clicks.

Export your Invoices and payments with the [Export module](#) to **reuse them with external tools**, or connect your existing BI suite directly to the open database for Big Data analysis.

[Table of Contents](#)

Banking and Reconciliation

24. Perform reconciliation to detect any missing or typing errors in payment records

Make the reconciliation of your bank account from the same menu as your bank entries. Use filters to **mark several line items at once** as reconciled.

Home

Agenda

Members

Third Parties

Products | Services

Commercial

Billing | Payment

Bank | Cash

Leads | Projects

HRM

Tools

Ticket

Documents

Websites

DoitCloud

Point of sales

MyBig Company

Search

Bookmarks

Bank | Cash

New financial account

List

List entries

List entries/category

Internal transfer

Tags/Categories

Tags/Categories of transaction...

Checks deposits

Bank accounts

Account for cash

Luxemburg Bank Account

Reconcile

Swiss bank account

Reconcile

Swiss bank account old

Reconcile

Dolibarr 9.0.0-beta

Account

Card

Bank entries

Planned entries

Monthly reporting

Graphics

Account statements

Linked files

LUXBAC

Luxemburg Bank Account

Luxembourg

Back to list

Open

Choose the bank statement related with the conciliation. Use a sortable numeric value: YYYYMM or YYYYMMDD: 201810

Eventually, specify a category in which to classify the records:

Then, check the lines present in the bank statement and click

Save statement only

or

Reconcile

or

Cancel

Last account statements : 201702 201706 201708 201802 201803 201804 201810

Bank entries (38)

16 1 2 3 Page 1/3

Oper. Date : From to Value date : From to Tags/Categories of transactions :

Ref

Description

Oper. Date

Type

Number

Third Party

Debit

Credit

Balance (before)

Balance

Account statement

Reconciled

243

Customer payment

10/16/2023

Check

aaaaaa (aaa aaa)

8.00

-

-

No

206

Customer payment

03/07/2018

Cash

Customer 1
Customer last
(Magento id 1)

400.00

-

-

No

185

RE Payment

04/28/2018

Check

40.00

-

-

201804

No

176

Customer payment

04/13/2018

Check

Generic customer

12.00

-

-

No

175

Customer payment

03/31/2018

Check

fff

Customer 1
Customer last
(Magento id 1)

5.00

-

-

No

137

Sales tax refund

02/05/2018

Bank transfer

5.00

-

-

No

136

Sales tax payment

02/05/2018

Credit card

10.00

-

-

No

135

Supplier

01/25/2018

Credit card

Book Keeping
Comment

1.00

-

-

No

Get alerts when the number of records not reconciled becomes too high.

Maintain a **history of your bank receipts** and review them without having to leave the application.

[Table of Contents](#)

Home	Agenda	Members	Third Parties	Products Services	Commercial	Billing Payment	Bank Cash	Leads Projects	HRM	Tools	Ticket	Documents	Websites	Dolibarr	Point of sales	Alice
------	--------	---------	---------------	---------------------	------------	-------------------	-------------	------------------	-----	-------	--------	-----------	----------	----------	----------------	-------

Search

Bookmarks

Bank | Cash
New financial account
List
List entries
List entries/category
Internal transfer
Tags/Categories
Tags/Categories of transact...
Checks deposits
Bank accounts
Account for cash
Luxemburg Bank Account
Reconcile
Swiss bank account
Reconcile
Swiss bank account old
Reconcile

Account statement 201803 - Bank account LUXBAC

Account statement 201803

Oper. Date	Value date	Type	Description	Debit	Credit	Balance
Initial balance :						-56,959.39
07/30/2016	07/30/2016	+	(Initial balance)		0.00	-56,959.39
01/04/2018	01/04/2018	+	Credit card Customer payment Company Corp 1 - Payment		4.00	-56,955.39
01/05/2018	01/05/2018	+	Credit card (DonationPayment) (paiement)		1.00	-56,954.39
01/05/2018	01/05/2018	+	Check Customer payment Company Corp 1 - Payment		1.00	-56,953.39
06/01/2018	06/01/2018	+	Bank transfer Customer payment aaaaaa - Payment		1.00	-56,952.39
06/06/2018	06/06/2018	+	Bank transfer RE Payment Payment	21,158.00		-78,110.39
10/01/2018	10/01/2018	+	Credit card Customer payment Generic customer - Payment		431.81	-77,678.58
				Total :	21,158.00 438.81	
End balance :						-77,678.58

Double Entry Accounting

25. Use all your data to automatically generate your ledger

Dolibarr has a **dedicated and independent feature** to setup your accountancy and dispatch all the data already recorded (products, sales, purchases, expense reports, salaries, ...) into your **ledger tables**. This means that your accountancy can be done in just a few clicks, with little to no knowledge of accounting and bookkeeping.

Setup your chart of accounts and your accounting number

Use a **predefined chart of accounts** or setup your **own chart of accounts**.

When you create a new customer, vendor, predefined product, bank account, vat rate, or type of expense report, **you can set up the accounting number during the creation**. Instead, if the users have no accounting knowledge, a bookkeeper can **set them up in one step** using dedicated setup pages. You can also mix and match these two methods.

[Table of Contents](#)

Validate the accounting number before they are added into your Ledger

At the frequency of your choice, analyze all accounting records (sales, purchases, bank transactions, expense reports) and use the wizard to track input errors. Fix records manually if particular changes are required.
Add validated records into your Ledger.

Analyze your Ledger, balance, ...

Use predefined reports to analyze your accounting records. Track input errors, at the frequency of your choice, analyze all accounting records (sales, purchases, bank transactions, expense reports) and use the wizard to fix manually when particular changes are required.
Review and add validated records into your ledger.

Export your ledger in the format of your choice

Once your ledger is complete, you can export the full set of records or just a filtered date range of records in a pre-defined accounting software format such as CSV, EBP, CogiLog, CEGID, SAGE etc.

The screenshot displays the 'Configuration of the module accounting expert' window in the MyBig Company software. The interface includes a top navigation bar with various icons and a sidebar on the left with a search bar and a list of menu items under 'Accounting' and 'Setup'. The main content area is titled 'Configuration of the module accounting expert' and contains several sections: 'Options', 'Specify the prefix for the file name' (set to 'myprefix'), 'Model of export', 'Select a model of export' (with a dropdown menu open), 'Other options', 'Select the format for the file', 'Column separator for export file', 'Select the carriage return type', and 'Date format for export file' (set to '%d%m%Y'). The dropdown menu for 'Select a model of export' is open, showing a list of export options: 'Classic export', 'Export towards CEGID Expert Comptabilité', 'Export towards Sage Coala', 'Export towards Sage BOB 50', 'Export towards Sage Ciel Compta or Compta Evolution', 'Export towards Quadratus QuadraCompta', 'Export towards EBP', 'Export towards Cogilog', 'Export towards Agiris', and 'Export Configurable'. A 'Modify' button is located at the bottom right of the configuration area.

Mass Emailing

26. Create and send mass e-mailing campaigns without any external tool

Create your Emailing content with a friendly editor

Create emailing campaigns using an **easy to use WYSIWYG editor** or for advanced users, an **HTML editor**. You can also **attach files** to your sent emails.

Personalize the e-mail template using variables that will be replaced with personalized values for each recipient, like

- First name, Last name, Email of recipient, signature of emailing author.
- Invisible markers to track if email is read or not.
- An easy to use links to allow recipients to unsubscribe in one click to your mass emailing campaigns.
- And more variables depending on other modules you activated...

The screenshot displays the Dolibarr 5.0.0-rc2 email campaign editor. On the left, a 'Bookmarks' sidebar lists links like 'The foundation', 'Online documentation', 'Official portal', 'DoliStore', 'Facebook page', 'Google+ page', and 'Twitter channel'. The main area is titled 'E-mail' and shows a status of 'Validated' with 2 distinct recipients. It includes fields for 'Email topic' (set to 'Buy my product'), 'Attached files' (none), and 'Default background color'. A right-hand panel lists variables for personalization, such as `__ID__` for ID, `__EMAIL__` for email, and `__LASTNAME__` for last name. Below these is a WYSIWYG editor with a toolbar for text formatting and alignment. The preview area shows a dark blue header with the 'DoliCloud' logo and social media icons. The main body text describes Dolibarr ERP CRM as a web hosting solution, followed by a red button labeled 'Test Dolibarr ERP CRM on Dolicloud →'. The footer includes 'DoliCloud team' and links to 'Unsubscribe' and 'View on web browser'.

Select your recipients from your existing data

Select the recipients of your emailing campaign among a list of predefined targets : You can select among **any customer, supplier, partner, employees or from an external source**. The recipients

[Table of Contents](#)

selector gives the ability to choose mail addresses depending on a lot of criteria for an accurate targeting.
Combine different sources if you need. The application will **automatically discard duplicated emails**.


Test your campaign in one click















Send your email to few **test emails** to validate your setup with a real email reader.

Send your emailing campaign

Send your email campaign **from the web interface** or **from command line**. Use your **own or third party external SMTP server**.

Track sending status per recipient to know which email was sent or not, who has opened the email and who has decided to unsubscribe.

 Selected recipients (26) 25 1 2 >

E-mail	Last name	First name	Other informations	Source	Date sending	Status
<input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text"/> <input type="button" value="Q"/> <input type="button" value="X"/>
abademail@aa.com	Swiss customer supplier				2017-01-29 21:36:40	Sent 
alan.smith@example.com	Smith,Alan				2017-01-29 21:36:40	Read 
alice.bigo@example.com					2017-01-29 21:36:40	Sent 
bob.markus@example.com					2017-01-29 21:36:40	Sent 
djay@example.com	Djay	Djay			2017-01-29 21:36:40	Sent 
emailtest1@example.com	Name 1	Firstname 1			2017-01-29 21:36:40	Sent 
emailtest2@example.com	Name 2	Firstname 2			2017-01-29 21:36:40	Sent 
emailtest3@example.com	Name 3	Firstname 3			2017-01-29 21:36:40	Sent 
emailtest4@example.com	Name 4	Firstname 4			2017-01-29 21:36:40	Read 
emailtest5@example.com	Name 5	Firstname 5			2017-01-29 21:36:40	Don't contact anymore 
herbert@example.com	Ducanseen	Herbert			2017-01-29 21:36:40	Sent 
johndoe@example.com	Do	John			2017-01-29 21:36:40	Error 
kathy.bowl@example.com	Bowl	Kathy			2017-01-29 21:36:40	Read 
mycustomer1@example.com	Customer 1				2017-01-29 21:36:40	Sent 
mycustomer2@example.com	Customer 2					Not sent
mycustomer3@example.com	Customer 3					Not sent
mycustomer4@example.com	Customer 4					Not sent

Duplicate your campaign to quickly restart it later

Once the e-mailing campaign is sent, the status is updated letting you know whether the e-mails have been sent properly or not. If all the mails have not been sent, you can retry to send them later.
Or just **duplicate your campaign, content and/or recipients to start a new campaign** in few clicks.

[Table of Contents](#)

For further features...

If you prefer using the web interface (and not only the SMTP service) of a third party E-mailing service (**MailChimp**, **SendInBlue**, **SendGrid**, ...), you can check if a connector is available for your version on the [Dolistore](#).

[Table of Contents](#)

Surveys and Polls

27. Ask your employees or partners their choice or opinion on any topic by running a poll/survey.
Give your contacts online access to your polls.

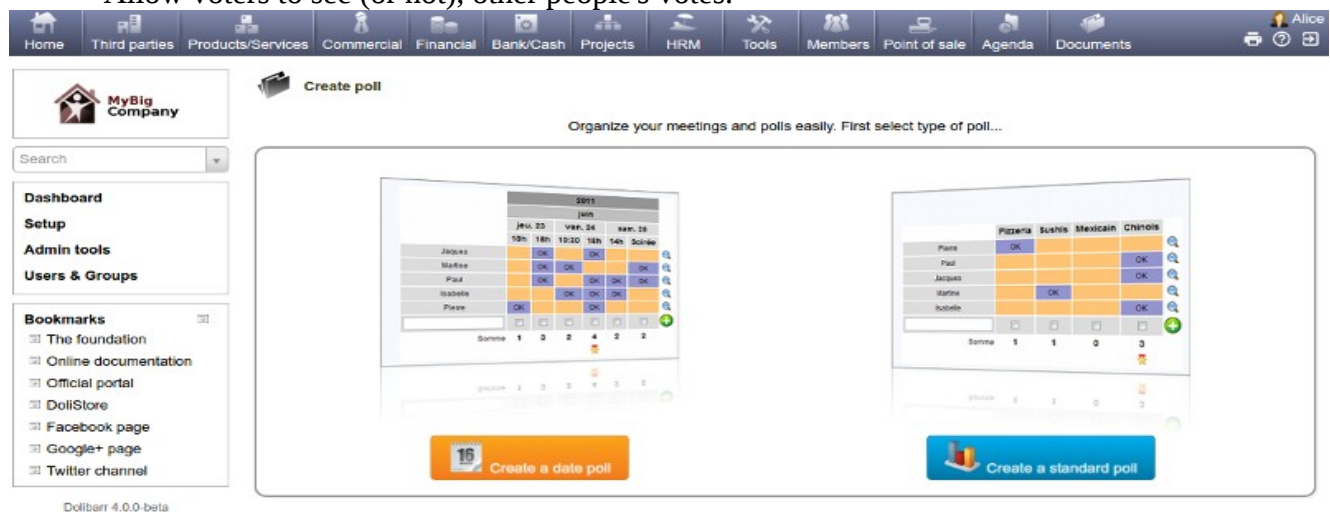
You can create polls to determine the best date for a meeting, to take vote for an election, or any other topic. Several options such as receiving email for each vote, writing comments, and making votes public or private can be enabled.

Create the poll or survey and add the questions you want to ask

Choose the best type of poll that matches your needs (date poll to select different days/hours in a calendar, or vote/standard poll to select with a list of yes/no or for/against). Define the title, a closing date, and a description that will be displayed on the public or private poll page. Create as many questions/answers as you need.

For each poll, choose among several options like :

- Receive an email for each vote.
- Allow voters to add comments in the poll.
- Allow voters to see (or not), other people's votes.



The module will **give you an URL link to your survey** to allow people to vote with any web browser...

Ask your employees, colleagues or partners to vote

[Table of Contents](#)

Send the created poll link by email or publish the poll link online on your website, so people can vote and post comments. Get all of this done in just a few clicks.



You are invited to vote for this poll

If you agree to vote in this poll, you have to give your name, choose the values that fit best for you and validate with the plus button at the end of the line.

Best date for a Doli Brunch ?

Please choose date your prefer for the Doli Brunch ?

	2016					
	March					
	Tue 22		Wed 23		Thu 24	
	9h-10h	10h-11h	9h-10h	9h30-10h30	10h-11h	
Martin Hugues	OK	KO	KO	OK	OK	Edit
Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Comments of voters:

Laurent Destailleur: I may be late the 24th

You can add a comment into poll...

Name:

You can also use the [mass-emailing module](#) of Dolibarr to inform your contacts about the availability of your poll!

Read and download the poll results

In the end, you can administer your polls and surveys, read, download and analyze the results of your polls and surveys from the back office.

[Table of Contents](#)

Home

Mem

Thirc

Prod

MRP

Proje

Com

Billin

Bank

Acco

HRM

Docu

Ager

Ticke

Took

Colle

FTP

lkjlkj

Web

Sell'y

Test

POS

16.0.0-alpha

Alice

Search

Email templates

EMailings

New emailing

List

Export Assistant

New Export

Import Assistant

New Import

Resources

New resource

List

Print barcode

Unalterable logs

Poll

New poll

List

OVH invoices import

OVH servers

Poll

Results

m4467s2mtk6khmxc

Back to list

Open

Type

Type date

Title

Date of next brunch

Description

What is your prefered date for a brunch

Email

@myemail@aaa.com

Limit date

03/07/2023

Author

fdfds

URL to communicate to get a direct access to poll

https://myportal.com/surve

EXPORT RESULT SPREADSHEET (.CSV)

You are allowed to change all vote lines of this poll with button "Edit". You can, as well, remove a column or a line with . You can also add a new column with Add.

2017

Add

January

January

Add

Thu 1

Tue 3

Add

John Doe

OK

KO

EDIT

Martial Bill

KO

OK

EDIT

Marissa Campbell

OK

OK

EDIT

Name

+

Total

2

2

Retrieve all your polls, closed or open. Find a summary of votes, details for each voter, and read comments. Close or re-open a poll at any time.

[Table of Contents](#)

Opportunities, Projects and Tasks

28. Projects and tasks are useful to track leads, opportunities and timesheets. Track how much revenue your projects are bringing back to your company, and their profit or loss statistics.

Create Projects, Leads or Opportunities

Use the Dolibarr project module according to your needs. Track **Leads, Opportunities, Internal, Customer or Supplier Projects**.

Add the predefined fields of your choice to make the data more managable, complete and as accurate as you need it to be.

Home

Agenda

Third parties

Products | Services

Commercial

Billing / Payment

Accountancy

Bank/Cash

Projects

HRM

Tools

Documents

Point of sale

Alice

MyBig Company

Search

Projects

New project

List

Statistics

Tasks/activities

New task

List

Statistics

Time spent

Tags/categories

New tag/category

Dolibarr 7.0.0-alpha

Project

Project

Project contacts 1

Overview

Notes

Linked files 1

Tasks 4

Gantt 4

Events/Agenda

PJ1607-0001

PROJALICE1

Third party : NLTechno (The OpenSource company)

Visibility

Project contacts

Opportunity status

Qualification

Opportunity probability

20 %

Opportunity amount

8,000 €

Start date - End date

07/30/2016 12:00 AM - ?

Budget

5,000 €

Priority

3

Description

The Alice project number 1

Tags/categories

Back to list

Open

Modify

Close

Clone

Delete

Linked files

Doc template

beluga

English (United St...

Generate

PJ1607-0001.pdf

15406 Bytes

10/10/2017 01:25 PM

Latest 10 linked events

Create event

See all

Ref.	By	Type	Event	Date
240	Alice Adminson	Phone call	Call the boss	01/31/2017 08:52 PM
237	Charlie Commercy	Phone call	Phone call with Mr Vaalen	07/01/2016 10:00 AM

Define who can view or edit the project

[Table of Contents](#)

Make the **project public or select the employees and/or partners** who can participate in the project. Users will be able to **enter the time spent** if you decide to use the [timesheet feature](#).

Create tasks

If you need to track dedicated tasks, map them to your projects. You can define properties on your tasks like **planned workload** and **assign specific users**.

You can also **create sub-tasks** and have a hierarchy of tasks.

Record the time spent on Projects/Tasks

If you decide to use Dolibarr projects to track the time spent, **then allow each user to declare their time** on a **daily basis** with a dedicated interface, or on a **weekly or monthly basis** with a different interface for the same.

Enter the **estimated progress of your tasks/project during the same step** in which the time spent is entered, so that the progress is always captured and compared with the time spent.

If an hourly rate is set in your user card, then **a cost for the time spent will also be automatically calculated** and reported.

More information is available in the following page: [timesheet feature](#).

Follow your project or tasks

Follow your projects:

If you use opportunities, **get the potential turnover of your leads instantly, weighed with the probability**, to get a calculated (propable) future turnover.

If you decide to use tasks, **track their progress and compare the progress with what you had initially planned**. You can review the plan using the **Gantt view**.

Project overview

[Table of Contents](#)

Projects offer an overview tab displaying a lot of information about projects and linked elements in Dolibarr such as proposals, invoices, orders, etc.

All these data allow you to determine profit and loss resulting from the project.

Interventions

29. Create intervention records.
Convert your interventions into invoices in order to bill your customers.

Create intervention records to **track interventions that are to be done or are already done**. Attach your intervention to a project if you want to have your intervention visible in the 360 degree view of projects.

Use any predefined products or services to fill your intervention records quickly, or provide specific descriptions.

MyBig Company

Search
Bookmarks

Commercial proposals
New proposal
List
Statistics

Customer Orders
New order
List
Statistics

Purchase orders
New order
List
Statistics

Contracts/Subscriptions
New contract/subscription
List
Services

Interventions
New intervention
List
ModelList
Statistics

Vendor proposals

Intervention card **Card** Intervention contact Resources Notes Linked files Log

FI1511-0003
Third Party : **Teclib**
Project :
Validated

Description
Contract

Total duration 10:00

Description	Date	Duration
Intervention on building windows 1	11/18/2015 09:00 AM	09:00
Intervention on building windows 2	01/22/2016 12:00 AM	01:00

MODIFY SEND EMAIL CREATE PROPOSAL CREATE INVOICE OR CREDIT NOTE CLASSIFY "DONE" CLONE DELETE

Linked files

Doc template soleil French Generate

FI1511-0003.pdf 18 Kb 10/31/2018 12:35 PM

Actions on intervention CREATE EVENT

Ref.	By	Type	Title	Date
None				

Related Objects Link to...

Type	Ref.	Date	Amount (net)	Status
------	------	------	--------------	--------

Link your interventions with events on agenda, projects, orders, etc...

Convert your **interventions into commercial proposals or invoices** according to your desired workflow.

[Table of Contents](#)

Agenda

30. An embedded Agenda, like any common calendar, enhanced with features dedicated to your ERP and CRM system (links to your customers, employees, projects, invoices, ...)

Manually create events in the past or future

Record your events in the embedded agenda: **Past events for tracking purpose**, or **Future events for reminder purpose**. Assign events to a customer/contact, project, and/or users.

The screenshot shows the 'Create an event' form within the MyBig Company application. The top navigation bar includes links for Home, Third parties, Products/Services, Commercial, Financial, Bank/Cash, Projects, HRM, Tools, Members, Point of sale, Agenda, and Documents. The left sidebar contains a search bar and sections for Dashboard, Setup, Admin tools, Users & Groups, and Bookmarks (The foundation, Online documentation, Official portal, DollStore, Facebook page, Google+ page, Twitter channel). The main form area is titled 'Create an event' and contains the following fields:

- Type:** A dropdown menu.
- Title:** A text field containing 'Rendez-Vous with Mr X'.
- Event on all day(s):** A checkbox.
- Start date:** A date field set to '03/02/2016' with time set to '10:00' and a 'Now' button.
- End date:** A date field with a 'Now' button.
- Status / Percentage:** A dropdown menu set to 'Not applicable'.
- Location:** A text field.
- Event assigned to:** A dropdown menu showing 'Alice Adminson (Owner)' and an 'Add' button.
- My availability:** A checkbox labeled 'Busy' which is checked.
- Task about company:** A dropdown menu set to 'All'.
- Task about contact:** A dropdown menu.
- Project:** A dropdown menu with a 'Create project' link.
- Priority:** A text field.
- Description:** A rich text editor with a toolbar including Source, Bold, Italic, Underline, Strikethrough, Text color, Background color, Bulleted list, Numbered list, Indent, Outdent, Link, Unlink, Image, Table, and a link icon.

The version 'Dolibarr 4.0.0-beta' is displayed at the bottom left of the sidebar.

If the module **Resources** is activated, you can also **assign resources to your event**, for example, to track which room is occupied, which car is hired, or which video projector is reserved, when it was reserved, and by whom.

Setup module to define the events which need to be recorded automatically

Using the setup of the Agenda module, you can decide to automatically **record events related to any business action** that occurs in the application (For example, track your order, proposal, or invoice status change, track creation, or deletion of new customers, ...)

Home

Third parties

Products/Services

Commercial

Financial

Bank/Cash

Projects

HRM

Tools

Members

Point of sale

Agenda

Documents

Alice

MyBig Company

Events and agenda module setup

Back to modules list

Agenda

Miscellaneous

Automatic filling

Export calendar

Import external calendars

Complementary attributes

Search

Dashboard

Setup

Company/Foundation

Modules

Menus

Display

Translation

Boxes

Alerts

Security

Limits and accuracy

PDF

E-mails

SMS

Dictionaries

Other setup

Admin tools

Users & Groups

Bookmarks

The foundation

Online documentation

Official portal

DoliStore

Facebook page

Google+ page

Twitter channel

Define here events for which you want Dolibarr to create automatically an event in agenda. If nothing is checked (by default), only manual actions will be included in agenda. Only elements from [enabled modules](#) are shown.

Events for which Dolibarr will create an action in agenda automatically		All/None
COMPANY_SENTBYMAIL	Mails sent from third party card	<input checked="" type="checkbox"/>
COMPANY_CREATE	Third party created	<input checked="" type="checkbox"/>
PROPAL_CLOSE_SIGNED	Customer proposal closed signed	<input type="checkbox"/>
PROPAL_CLASSIFY_BILLED	Customer proposal set billed	<input type="checkbox"/>
PROPAL_CLOSE_REFUSED	Customer proposal closed refused	<input type="checkbox"/>
PROPAL_VALIDATE	Customer proposal validated	<input checked="" type="checkbox"/>
PROPAL_SENTBYMAIL	Commercial proposal sent by mail	<input checked="" type="checkbox"/>
ORDER_VALIDATE	Customer order validated	<input checked="" type="checkbox"/>
ORDER_CLOSE	Customer order classify delivered	<input type="checkbox"/>
ORDER_CLASSIFY_BILLED	Customer order classify billed	<input type="checkbox"/>
ORDER_CANCEL	Customer order canceled	<input type="checkbox"/>
ORDER_SENTBYMAIL	Customer order sent by mail	<input checked="" type="checkbox"/>
BILL_VALIDATE	Customer invoice validated	<input checked="" type="checkbox"/>
BILL_PAYED	Customer invoice payed	<input checked="" type="checkbox"/>
BILL_CANCEL	Customer invoice canceled	<input checked="" type="checkbox"/>
BILL_SENTBYMAIL	Customer invoice sent by mail	<input checked="" type="checkbox"/>
BILL_UNVALIDATE	Customer invoice unvalidated	<input checked="" type="checkbox"/>
ORDER_SUPPLIER_VALIDATE	Supplier order recorded	<input checked="" type="checkbox"/>
ORDER_SUPPLIER_APPROVE	Supplier order approved	<input type="checkbox"/>

View events in different agenda views

View and search events using filters to view only the events you are interested in (by user, customer, project, status, or type).

Home

Third parties

Products/Services

Commercial

Financial

Bank/Cash

Projects

HRM

Tools

Members

Point of sale

Agenda

Documents

Alice

MyBig Company

Search

Dashboard

Setup

Admin tools

Users & Groups

Bookmarks

The foundation

Online documentation

Official portal

DollStore

Facebook page

Google+ page

Twitter channel

Dolibarr 4.0.0-beta

Agenda

Day view

Week view

Month view

Per user view

List view

Google agenda

Events assigned to

Alice Adminson

or Group

Type

Status

Third party

All

Project

Refresh

Internal calendar

Show birthday's contacts

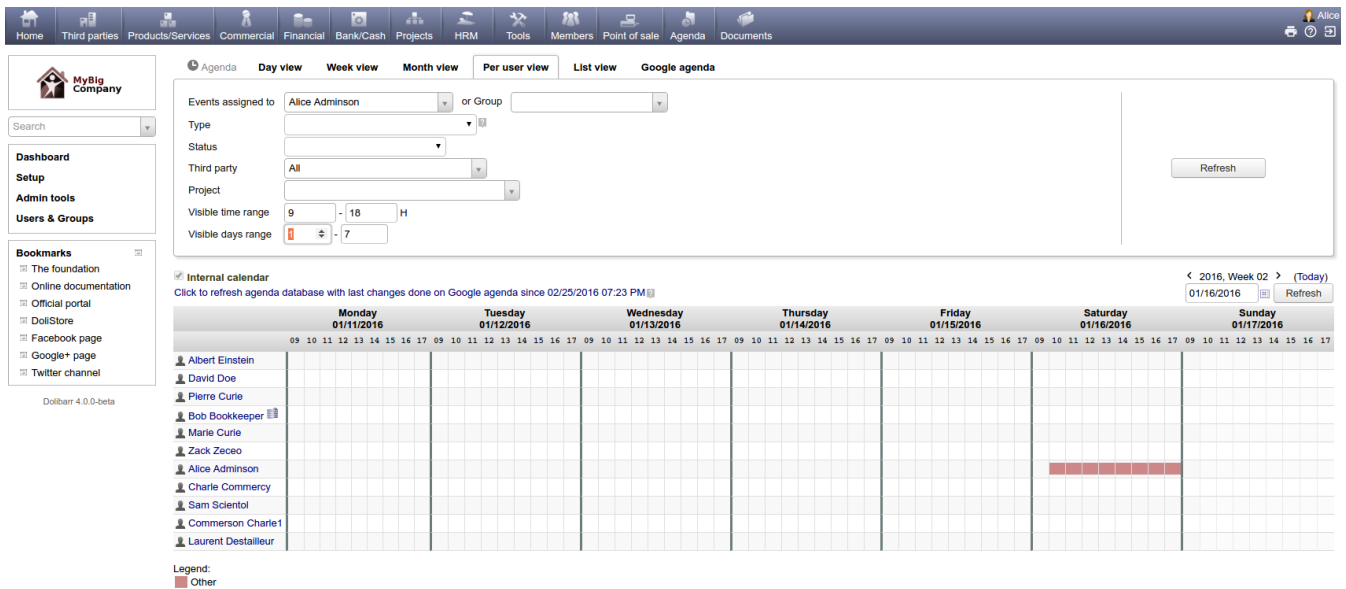
Click to refresh agenda database with last changes done on Google agenda since 02/25/2016 06:57 PM

< Jan 2016 > (Today)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
28	29	30	31	01	02	03
04	05	06	07	08	09	10
11	12	13	14	15	16 10:00-18:56 Rendez-vous	17
18	19	20	21	22 18:54 Invoice 16 validat... Indian SAS	23 18:54 Invoice 16 validat... Indian SAS	24
25	26	27	28	29	30	31

If required, **you can include in the agenda view, any events that are recorded into an external calendar** (in read-only mode using the ical/ics import). Or, **export your events into any external calendar** using the ical/ics export link.

You can use different rendering views to review your events (view **by day, by week, by month, by user, or the simple list**). For example, the view "per month" or "per week" is interesting to show past or upcoming events while the view "per user" is great to know which user is busy or free to find the best time slot to create a new meeting request.



API, Triggers, and Hooks

31. Integrate your ERP with any other application using Dolibarr's APIs, Triggers, and Hooks

REST APIs

Extract any data or **insert, update, or delete** records using our new REST APIs. Using standard HTTP and JSON formats, the REST APIs are compatible with any programming language (PHP, Java, Ruby, Python, C#, C++, JavaScript, JQuery, Basic, ...). Use the embedded **API explorer tool** to test APIs or get generated URLs to use in your own code.



root	Show/Hide	List Operations	Expand Operations	Raw
agendaevents	Show/Hide	List Operations	Expand Operations	Raw
bankaccounts	Show/Hide	List Operations	Expand Operations	Raw
categories	Show/Hide	List Operations	Expand Operations	Raw
contacts	Show/Hide	List Operations	Expand Operations	Raw
dictionnarycountries	Show/Hide	List Operations	Expand Operations	Raw
dictionnarytowns	Show/Hide	List Operations	Expand Operations	Raw
expensereports	Show/Hide	List Operations	Expand Operations	Raw
invoices	Show/Hide	List Operations	Expand Operations	Raw

GET

/invoices

List invoices

GET

/invoices/{id}

Get properties of a invoice object

POST

/invoices

Create invoice object

PUT

/invoices/{id}

Update invoice

DELETE

/invoices/{id}

Delete invoice

Response Class

string

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
id	12345678	Invoice ID	path	integer

Try it out!

Hide Response

Request URL

http://localhostgit:80/dolibarr_dev/htdocs/api/index.php/invoices/12345678

Triggers and Hooks

Execute your own code every time a business event such as Create, Update, or Delete is performed on any object in Dolibarr ERP and CRM by adding your own trigger code. Adding a trigger is as easy as adding a file with just few lines of code into the directory /core/triggers.

```

/**
 * Class of triggers for demo module
 */
class InterfaceDemo extends DolibarrTriggers
{
    public $family = 'demo';
    public $picto = 'technic';
    public $description = "Triggers of this module are empty functions. They have no effect. They are provided for tutorial purpose only.";
    public $version = self::VERSION_DOLIBARR;

    /**
     * Function called when a Dolibarr business event is done.
     * All functions "runTrigger" are triggered if file is inside directory htdocs/core/triggers or htdocs/module/code/triggers (and declared)
     *
     * @param string      $action      Event action code
     * @param Object      $object      Object concerned. Some context information may also be provided into array property object->context.
     * @param User        $user        Object user
     * @param Translate    $langs      Object langs
     * @param conf         $conf       Object conf
     * @return int         <0 if KO, 0 if no triggered ran, >0 if OK
     */
    public function runTrigger($action, $object, User $user, Translate $langs, Conf $conf)
    {
        // Put here code you want to execute when a Dolibarr business events occurs.
        // Data and type of action are stored into $object and $action

        if ($action == 'BILL_MODIFY')
        {
            // My own code using $object, $user, $langs, $conf....
            //....
        }
    }
}

```

And more...

Dolibarr also provides plenty of other possibilities such as **hooks**, **modules options**, **menu editor**, **low level setup** etc. to tune the Dolibarr application to cater to very specific needs. You can also hire any **PHP developer** to develop or customize any behavior. Knowledge of the **PHP language is the only prerequisite** required to develop a Dolibarr ERP and CRM addon.

[Table of Contents](#)

Connectivity and Interfaces

32. Connect your ERP and CRM application with most popular services

A lot of external services can be linked to your Dolibarr ERP CRM using the provided interface modules or using external modules...

LDAP

Use your own LDAP server so your users will **share same password**. Or reuse data in your LDAP to create users in application. Synchronize user data in the direction of your choice.

Online Payment Services

Use the Payment modules (for example, **Paypal, Stripe, Paybox, ...**) to offer your customer an interface to pay their invoice online. You can also include **payment links into your sent email** automatically. Dolibarr is also SCA ready (Strong Customer Authentication).

SMTP

Define the SMTP properties of your SMTP email hosting provider so your emails will be sent **using your own email provider platform**. All emails you send also appears into your "Sent" repository of your email box.

Google

Integrate **Google services** like Google Maps, Google Contacts, Google Calendar and more using external modules.

eCommerce

Install external modules to **synchronize your ERP with your eCommerce** platform (like Prestashop, Magento, WooCommerce, ...)

Computer Telephony Integration (CTI)

Use the generic **clickToDial** module to call your partners by a simple click on your application. Input calling may also be trapped to open directly your customer card using external modules.

[Table of Contents](#)

One Time Password (OTP) or 2-Steps Authentication

Add features to support **OTP** or **2-Steps Authentication** using systems like **Google Authenticator**. Several addons are available on the [Dolistore market place](#)

RSS

Integrate external **RSS inside your dashboard**.

and more connectors...

Find a lot of external module on the [Dolistore market place](#) to integrate your favorite external services into your CRM and ERP, like Emails, SMS, Banks interface, Legal document generation...

[Table of Contents](#)

Import and Export

33.
- Use the import or export wizard to help you to import or extract any data into or from your application

The import wizard allows to **import a lot of data from any external application** from a CSV or Excel file. Make your import in **Insert or Update mode**.

The export wizard allows you to **export any data of application** in a CSV or Excel file.

Export

Use the wizard to export any data in several steps:

- Choose the data to export among a list of predefined export profiles.
- Define which field you want to export.
- Define your filters and position of fields.
- Save your export profile so you can remake the export later at any time in few clicks.
- Build and download the exported file.

MyBig Company

Search

Bookmarks

Emails templates

EMailings

New emailing

List

Export assistant

New export

Import assistant

New import

Resources

New resource

List

Unalterable logs

Print bar code

Poll

New export

Step 1

Step 2

Step 3

Step 4

Step 5

Module/Application

Invoices

Dataset to export

Customer invoices and invoice's lines

Exported fields

Company Id, Company name, Address, Zip Code, City, Country code, Phone, Professional ID 1, Professional ID 2, Professional ID 3, Professional ID 4, Customer accounting code, Vendor accounting code, Sales Tax/VAT ID, Invoice id, Invoice ref., Type, Invoice creation date, Invoice date, Due date, Total (net of tax), Total (inc. tax), Total tax, Pending, Invoice paid, Invoice status, Note (private), Note (public), User id who created, User login who created, User id who validated, User login who validated, Project ref., Id of line, Description of line, Unit price of line, VAT Rate of line, Quantity for line, Amount net of tax for line, Amount of VAT for line, Amount with tax for line, Start date, End date, Special code, Type of line (0=product, 1=service), Product/service id, Product ref., Product label, Accounting code (sale)

Filtered fields

None

Now, select the file format in the combo box and click on "Generate" to build the export file...

Available formats	Library used	Library version
<input type="checkbox"/> CSV	Dolibarr	9.0.0-alpha
<input checked="" type="checkbox"/> Excel 2007	PhpExcel	1.8.0
<input checked="" type="checkbox"/> Excel 95	PhpExcel	1.8.0
<input type="checkbox"/> TSV	Dolibarr	9.0.0-alpha

Linked files

Save your export profiles to be able to redo the same export later, in one click.

Module

Products

Dataset to export

Products

Choose fields you want to export, or select a predefined export profile

MyExportProfile

Select

Import

Use the import wizard to **load or update data** in your database.

Import from any **CSV or Excel** files. You can get a predefined empty source files, but any source file can be used.

File to import must have one of following format

☐ Csv

[Download example of empty source file](#)

☒ Excel 2007

[Download example of empty source file](#)

Make a mapping between fields in your source file and Dolibarr fields, so **you can import files with any format**, or reuse a previously saved import profiles to save your time if you need to make frequently the same import / update.

Fields in source file	Target fields in Dolibarr database (bold=mandatory)		
Field 1 (Ref. * (p.ref))	=> Product	Ref.	
Field 2 (Label* (p.label))	=> Product	Label	
Field 3 (Description (p.descripti...))	=> Product	Description	
Field 4 (Public URL (p.url))	=> Product	Public URL	
Field 5 (Accountancy code (sale) ...)	=> Product	Accountancy code (sale)	
Field 6 (Accountancy code (purcha...))	=> Product	Accountancy code (purchase)	
Field 7 (Note (p.note))	=> Product	Note	
Field 8 (Length (p.length))	=> Product	Length	
Field 9 (Surface (p.surface))	=> Product	Area	
Field 10 (Volume (p.volume))	=> Product	Volume	
Field 11 (Weight (p.weight))	=> Product	Weight	
Field 12 (Duration (p.duration))	=> Product	Duration	
Field 13 (Customs code (p.customco...))	=> Product	Customs code	
Field 14 (Selling price (net of ta...))	=> Product	Selling price (net of tax)	
Field 15 (Selling price (inc. tax) ...)	=> Product	Selling price (inc. tax)	
Field 16 (Sales tax (p.tva_tx))	=> Product	Sales tax	

Run the simulator so you can **know result of import with no data change**. Once the simulation is successful, you can run the real import.

Number of lines with no errors and no warnings: 90.

Errors on 2 source record(s)

* Line 1
> Wrong value for field number 17 (value 'For sale' (p.tosell) does not match regex rule ^[0|1]\$)
> Wrong value for field number 18 (value 'For purchase' (p.tobuy) does not match regex rule ^[0|1]\$)
> Wrong value for field number 19 (value 'Type' (p.fk_product_type) does not match regex rule ^[0|1]\$)
> Wrong value for field number 21 (value 'Creation date (p.datec)' does not match regex rule ^[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]\$)
* Line 2
> Wrong value for field number 17 (value '0 or 1' does not match regex rule ^[0|1]\$)
> Wrong value for field number 18 (value '0 or 1' does not match regex rule ^[0|1]\$)
> Wrong value for field number 19 (value '0 for product/1 for service' does not match regex rule ^[0|1]\$)

Check result of import simulation. If everything is ok, launch the definitive import.

Module Builder for Developers

34. A complete low-code and no-code studio to help developers build a full application within few minutes.

The **Module Builder tool** is an embedded RAD (Rapid Application Development) tool with a code generator and source file editor to allow developers and advanced users to build a complete application including new objects, new permissions, new menus, news APIs, etc.

Create the Module that you want to manage

Use the **module builder** tool to initialize your module. A skeleton with working code will be generated. Then, use all the tools provided to you to setup all the features that you need (menus, translations, permissions hooks, triggers, widgets, automated tasks, ...)

HomeAgendaThird partiesProducts | ServicesCommercialBilling / PaymentAccountancyBank/CashProjectsHRMToolsDocumentsPoint of sale

MyBig Company

Search

My dashboard

Setup

Admin tools

About Dolibarr

About Browser

About OS

About Web Server

About PHP

About Database

Backup

Restore

Upgrade / Extend

Purge

Audit

Users session

External resources

Mass VAT change

Module Builder

Scheduled jobs

Direct Printing jobs

Mass barcode init

Users & Groups

Dolibarr 7.0.0-alpha

Module Builder

This tools must be used by experienced users or developers. It gives you utilities to build or edit your own module (Documentation for alternative manual development is here). Path where modules are generated/edited (first alternative directory defined into conf/conf.php): /home/destailleur/git/dolibarr/htdocs/custom

Modules/ApplicationsNewMonModuleSellYourSaasDanger zone

☐ This module was not activated yet. Go into Home-Setup-Modules/Applications to make it live or click here: OFF

DescriptionSpecificationsLanguagesObjectsMenusPermissionsHooksTriggersWidgetsScheduled jobsBuild package/documentation

NewElevesPackagesDanger zone

File for PHP DAO CRUD class : monmodule/class/eleves.class.php

File for PHP API class : monmodule/class/api_eleves.class.php

File for PHP Unit Test class : monmodule/test/phpunit/ElevesTest.php

PageForLib : monmodule/lib/eleves.lib.php

PageForPicto : monmodule/img/object_eleves.png

Sql file : monmodule/sql/lx_eleves.sql

Sql file for complementary attributes : monmodule/sql/lx_eleves_extrafields.sql

Sql file for keys : monmodule/sql/lx_eleves.key.sql

PHP page for list of record : monmodule/eleves_list.php

PHP page to create/edit/view a record : monmodule/eleves_card.php

PHP page for event tab : monmodule/eleves_agenda.php

PHP page for document tab : monmodule/eleves_document.php

PHP page for note tab : monmodule/eleves_note.php

Go to API explorer

DropTableIfEmpty

Properties

Property (Example)	Label	Type	Array of key-val	Not NULL	Database Index	Position	Enabled	Visible	Is a measure	Used for 'search all'
rowid	TechnicalID	integer		1	X	1	1			

Your module is ready to be activated immediately, and the new features will be available inside your ERP system in just a few minutes.

[Table of Contents](#)

Define the new Objects that you want to manage

Enter the name of your module and the description of each object, field and permission that you want to manage. The Module Builder will generate for you, the code to add the new menu entries, and the create, view and edit screens to manage your objects. The Module Builder also generates the necessary SQL files, APIs interfaces, etc.

The new menu entries, new tables, and new screens will appear instantly inside your application.

Activate and test your application, change source code on the fly

You can switch between your external IDE (like Eclipse or any PHP IDE) and the embedded IDE available in Module Builder to review and/or modify the generated source code of your module without losing any code.

If you have permission, you can edit the source code with the editor of your choice, even when your application is online, and you can test the results immediately.

Build the package and generate documentation in one click

Use the package generator to build a zip file containing your module, ready to be distributed to any other Dolibarr instance. The package is also ready to be distributed or sold, as a new addon, on marketplaces like www.dolistore.com

Use the documentation generator to build a HTML or PDF documentation with all the technical information and business rules, which you can share with your business users and IT partners.

[Table of Contents](#)



Applied Technology Research Center (ATRC) Information and Communications Technology (ICT) services

36. Solutions

[Automation for businesses](#)

[Business critical systems](#)

[Data and AI solutions](#)

[ICT services for industries](#)

[Infrastructure services](#)

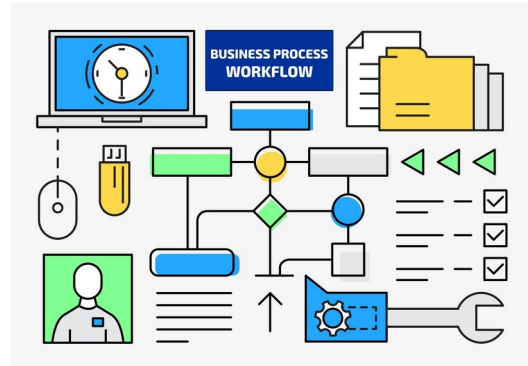
[Services to increase reliability](#)

Automation for businesses

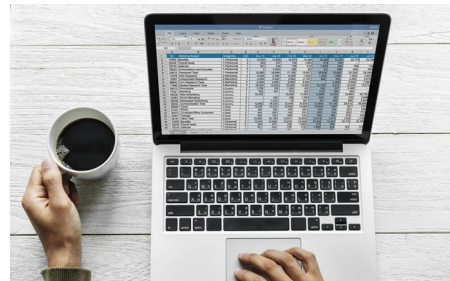
Automation services for businesses encompass a range of solutions aimed at streamlining processes, improving efficiency, reducing errors, and ultimately increasing productivity. Here are some common automation services tailored for businesses:

22. **Robotic Process Automation (RPA):** RPA involves using software robots or "bots" to automate repetitive tasks and workflows typically performed by humans. These bots can interact with applications, manipulate data, trigger responses, and communicate with other systems to execute tasks efficiently.

23. **Workflow Automation:** Workflow automation involves automating entire business processes, including the routing of tasks, approvals, and notifications. It ensures that tasks are completed in a predefined sequence with minimal manual intervention, leading to faster turnaround times and improved consistency.



24. **Document Management Automation:** Document management automation solutions streamline the creation, processing, storage, retrieval, and sharing of documents within an organization. This includes automated document classification, indexing, version control, and archival processes to improve accessibility and compliance.



25. **Data Entry and Processing Automation:** Automation services can be employed to automate data entry tasks such as data extraction, validation, and transformation. This reduces manual errors, accelerates data processing times, and enhances data accuracy and consistency.

26. **Customer Relationship Management (CRM) Automation:** CRM automation tools automate various aspects of customer relationship management, including lead management, sales pipeline tracking, email marketing, and customer support. These tools improve customer engagement, enhance sales efficiency, and enable personalized interactions.



27. **Inventory and Supply Chain Management Automation:** Automation services can optimize inventory management and supply chain operations by automating inventory tracking, replenishment, order



processing, and shipment scheduling. This helps minimize stockouts, reduce carrying costs, and improve order fulfillment efficiency.

28. **Finance and Accounting Automation:** Finance and accounting automation solutions automate routine financial tasks such as invoice processing, expense management, accounts payable/receivable reconciliation, and financial reporting. This streamlines financial operations, enhances accuracy, and facilitates compliance with regulations.

29. **Human Resources (HR) Automation:**

HR automation services automate various HR processes, including employee onboarding, payroll processing, leave management, performance evaluations, and compliance reporting. This improves HR efficiency, reduces administrative overhead, and enhances employee satisfaction.



30. **IT Operations Automation:** IT operations automation solutions automate routine IT tasks such as system provisioning, configuration management, software deployment, monitoring, and troubleshooting. This accelerates IT service delivery, improves system reliability, and frees up IT staff to focus on strategic initiatives.

31. **Compliance and Risk Management Automation:** Automation services can assist organizations in automating compliance monitoring, risk assessment, audit trails, and regulatory reporting. This ensures adherence to industry standards and regulations while reducing the risk of non-compliance.

These automation services can be tailored to meet the specific needs and workflows of businesses across various industries, enabling them to operate more efficiently, reduce costs, and remain competitive in today's rapidly evolving business landscape.

Business critical systems

Run your Enterprise System on Linux for better reliability and security.

Running an enterprise system on Linux offers several advantages, particularly in terms of reliability. Here are some reasons why:

- **Stability and Robustness:** Linux is known for its stability and robustness. It's designed to handle heavy workloads and operate continuously without crashing or experiencing significant downtime. This reliability is crucial for enterprise systems that need to be available 24/7.
- **Community Support:** Linux has a large and active community of developers and users who contribute to its development and provide support. This means that if issues arise, there are numerous resources available for troubleshooting and resolving them quickly.
- **Security:** Linux is inherently more secure than some other operating systems due to its open-source nature. Security vulnerabilities are typically identified and patched quickly by the community, reducing the risk of system breaches and data loss.
- **Customization:** Linux offers a high degree of customization, allowing enterprises to tailor the operating system to their specific needs. This flexibility enables organizations to optimize performance and reliability for their particular use cases.
- **Scalability:** Linux can scale easily to accommodate growing enterprise needs. Whether an organization is small or large, Linux can be deployed across a wide range of hardware configurations and can scale horizontally (adding more servers) or vertically (increasing resources on existing servers) as needed.
- **Cost-Effectiveness:** Linux can reduce operating costs for enterprises if they have in house trained system administrators and users.
- **Compatibility:** Linux supports the most amount of hardware platforms and architectures as compared to any other operating system in the world today, making it the most suitable for deploying enterprise systems across diverse environments. This compatibility ensures that organizations can leverage existing infrastructure investments without worrying about vendor lock-in or limited options.



- **Reliable File System:** Linux typically uses robust file systems like ZFS and ext4, which are designed for reliability, data integrity, and performance. This ensures that data stored on Linux-based enterprise systems is less prone to corruption or loss.

Overall, the combination of stability, security, flexibility, and cost-effectiveness makes Linux an excellent choice for running enterprise systems where reliability is paramount.

Data and AI solutions

Data and AI solutions offer businesses the ability to leverage their data assets to drive insights, make informed decisions, automate processes, and enhance customer experiences. Here are some common data and AI solutions for businesses:

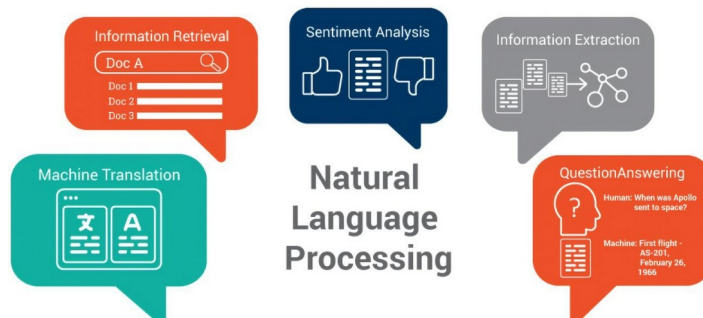
- **Data Analytics and Business**

Intelligence (BI): These solutions involve analyzing structured and unstructured data to uncover patterns, trends, and insights that can inform strategic decision-making. Business Intelligence tools provide dashboards, reports, and visualizations to help stakeholders understand data more easily.



- **Machine Learning (ML) and Predictive Analytics:** ML algorithms analyze historical data to identify patterns and make predictions about future outcomes. Predictive analytics models can forecast customer behavior, demand trends, equipment failures, and other business metrics, enabling proactive decision-making and risk mitigation.

- **Natural Language Processing (NLP) and Text Analytics:** NLP technologies analyze and interpret human language data, including text from customer feedback, social media, emails, and documents. Text analytics solutions extract insights, sentiment analysis, entity recognition, and topic modeling to derive actionable insights from unstructured text data.



- **Computer Vision:** Computer vision technologies analyze and interpret visual data from images and videos. These solutions can be used for applications such as facial recognition, object detection, quality inspection, and augmented reality, enabling businesses to automate visual inspection tasks and enhance customer experiences.
- **Recommendation Systems:** Recommendation systems analyze customer preferences and behaviors to deliver personalized product recommendations, content, and marketing offers. These systems utilize collaborative filtering, content-based filtering, and other algorithms to improve customer engagement and drive sales.
- **Anomaly Detection:** Anomaly detection algorithms identify unusual patterns or outliers in data that may indicate fraud, cybersecurity threats, equipment malfunctions, or other anomalies. These solutions enable businesses to detect and respond to abnormal events in real-time, reducing risks and minimizing downtime.

- **Optimization and Decision Support:** Optimization algorithms optimize business processes, resource allocation, scheduling, and logistics to maximize efficiency and minimize costs. Decision support systems provide recommendations and insights to assist human decision-makers in complex, data-driven scenarios.
- **Chatbots and Virtual Assistants:** Chatbots and virtual assistants use AI technologies such as NLP and ML to interact with users via text or speech, answer questions, provide assistance, and automate customer support tasks. These solutions enhance customer service, improve response times, and reduce service costs.
- **Data Governance and Compliance:** Data governance solutions enforce policies, standards, and regulations for data management, privacy, and security. These solutions ensure data quality, integrity, and compliance with legal and regulatory requirements, mitigating risks and protecting sensitive information.
- **Data Integration and Management:** Data integration and management platforms consolidate, cleanse, and harmonize data from disparate sources to create a single source of truth for analysis and decision-making. These platforms enable businesses to manage their data lifecycle efficiently and ensure data consistency across the organization.

These data and AI solutions empower businesses to unlock the full potential of their data assets, drive innovation, and gain a competitive edge in today's data-driven economy. By leveraging advanced analytics, machine learning, and automation technologies, businesses can transform data into valuable insights and actionable intelligence that drive business growth and success.

Information and Communication Technology (ICT) services for various industries. Information and Communication Technology (ICT) services play a crucial role in enabling digital transformation and driving innovation across various industries. Here are some common ICT services tailored for different sectors:

- **Healthcare:**

- Electronic Health Records (EHR) systems for efficient patient record management.
- Telemedicine solutions for remote consultations and healthcare delivery.
- Health Information Exchange (HIE) platforms for secure data sharing among healthcare providers.
- Medical imaging and diagnostic systems for enhanced patient care.
- Wearable health monitoring devices for remote patient monitoring and preventive care.

- **Finance and Banking:**

- Core banking systems for transaction processing and customer account management.
- Online banking and mobile banking applications for convenient customer access to financial services.
- Fraud detection and prevention systems for safeguarding against financial fraud and cyber threats.
- Risk management and compliance solutions for regulatory compliance and risk mitigation.
- Data analytics and business intelligence solutions for customer insights and personalized financial services.

- **Manufacturing:**

- Enterprise Resource Planning (ERP) systems for integrated production planning, inventory management, and supply chain optimization.
- Industrial Internet of Things (IIoT) solutions for real-time monitoring and predictive maintenance of machinery and equipment.
- Computer-Aided Design (CAD) and Computer-Aided Manufacturing (CAM) software for product design and manufacturing process optimization.
- Digital twin technology for virtual simulation and optimization of manufacturing processes.
- Supply chain management solutions for end-to-end visibility and traceability of goods and materials.



- **Retail and E-commerce:**

- E-commerce platforms for online product catalog management, shopping cart functionality, and payment processing.
- Customer Relationship Management (CRM) systems for personalized marketing, customer engagement, and loyalty programs.
- Point-of-Sale (POS) systems for in-store transactions and inventory management.
- Omnichannel retail solutions for seamless shopping experiences across online and offline channels.
- Analytics and data-driven insights for demand forecasting, pricing optimization, and inventory management.
- **Education:**
 - Learning Management Systems (LMS) for course delivery, content management, and student engagement.
 - Virtual classrooms and online learning platforms for remote education and distance learning.
 - Student Information Systems (SIS) for student enrollment, grading, and academic records management.
 - Educational technology tools for interactive learning experiences, such as virtual reality (VR) and gamification.
 - Analytics and assessment tools for tracking student performance and personalized learning.
- **Transportation and Logistics:**
 - Fleet management systems for vehicle tracking, route optimization, and maintenance scheduling.
 - Transportation management systems for freight forwarding, carrier selection, and shipment tracking.
 - Warehouse management systems for inventory control, order picking, and distribution.
 - Logistics analytics for performance monitoring, cost optimization, and supply chain visibility.
 - Last-mile delivery solutions for efficient and timely delivery of goods to customers.
- **Government and Public Sector:**
 - E-government services for online citizen engagement, digital identity management, and public service delivery.



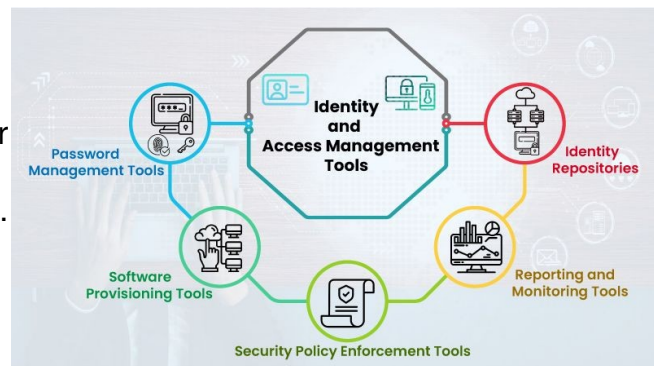
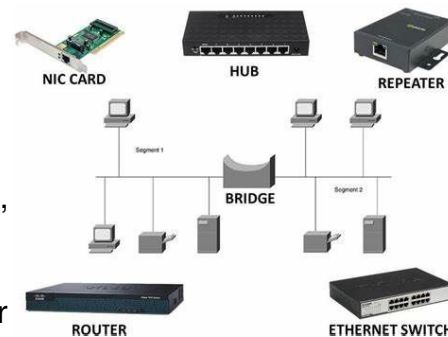
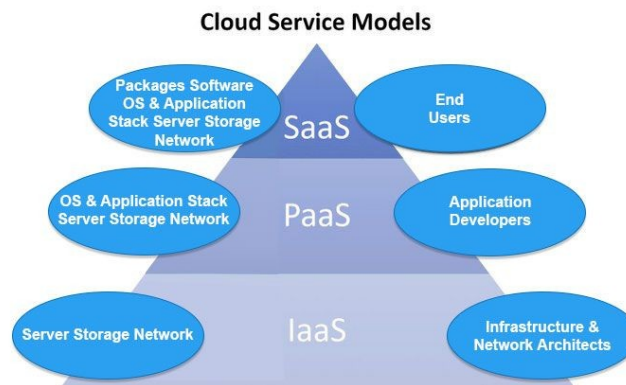
- Geographic Information Systems (GIS) for spatial data analysis, urban planning, and disaster management.
- Public safety and emergency response systems for law enforcement, firefighting, and emergency medical services.
- Tax administration and revenue management systems for tax collection, compliance monitoring, and financial reporting.
- Open data initiatives for promoting transparency, accountability, and innovation in government services.

These ICT services help industries digitize their operations, improve efficiency, enhance customer experiences, and stay competitive in today's rapidly evolving business landscape. By leveraging technology solutions tailored to their specific needs, organizations can drive innovation, optimize processes, and achieve their business objectives.

Infrastructure services

Infrastructure services encompass a wide range of offerings that provide the foundational IT resources and capabilities necessary for organizations to operate their IT systems effectively. These services support the hardware, software, networking, and storage components required to run applications, store data, and facilitate communication within an organization. Here are some common infrastructure services:

- **Compute Services:** Compute services involve the provision of computing resources such as servers, virtual machines (VMs), and containers. This includes services for provisioning, managing, and scaling compute instances to run applications and workloads.
- **Storage Services:** Storage services offer scalable and reliable storage solutions for storing and managing data. This includes block storage, object storage, and file storage services, as well as backup and disaster recovery solutions to ensure data resilience and availability.
- **Networking Services:** Networking services provide the infrastructure for connecting devices, systems, and users within an organization. This includes services such as virtual private networks (VPNs), load balancing, content delivery networks (CDNs), and domain name system (DNS) management.
- **Database Services:** Database services offer managed database solutions for storing, querying, and managing structured and unstructured data. This includes relational databases, NoSQL databases, data warehouses, and database migration services.
- **Identity and Access Management (IAM):** IAM services provide authentication, authorization, and access control mechanisms to ensure secure access to IT resources. This includes services for managing user identities, roles, permissions, and single sign-on (SSO) authentication.
- **Monitoring and Logging Services:** Monitoring and logging services offer tools and platforms for monitoring the performance, availability, and security of IT infrastructure and applications. This includes real-time monitoring, log aggregation, alerting, and troubleshooting capabilities.



- **Reliability and Security Services:** Security services provide authorized access to data and prevent unauthorized access to IT systems and data. This includes services such as updating software to prevent bugs, implementing required configurations and testing their validity to allow authorized access while preventing unwanted access. And user training related to phishing and social engineering.
- **Backup and Disaster Recovery (DR):** Backup and DR services offer solutions for data backup, replication, and recovery to ensure business continuity in the event of data loss or system failure. This includes regular backups, data replication across multiple locations, and automated failover mechanisms.
- **Cloud Migration and Hybrid Cloud Integration:** Cloud migration and hybrid cloud integration services help organizations migrate their IT infrastructure and workloads to the cloud and integrate on-premises and cloud environments seamlessly. This includes assessment, planning, migration, and optimization services.
- **Automation and Orchestration:** Automation and orchestration services enable organizations to automate routine IT tasks and workflows, such as provisioning, configuration management, and scaling. This includes infrastructure-as-code (IaC) tools, configuration management platforms, and workflow orchestration frameworks.

These infrastructure services are essential for building and managing modern IT environments that are scalable, reliable, and secure. By leveraging these services, organizations can optimize their IT operations, improve efficiency, and accelerate innovation to meet the demands of today's digital economy.



Services to increase reliability

Increasing the reliability of ICT (Information and Communication Technology) services is crucial for ensuring smooth operations, minimizing downtime, and delivering a consistent user experience. Here are several services and strategies that organizations can implement to enhance the reliability of their ICT services:

- **Redundancy and Failover Solutions:**

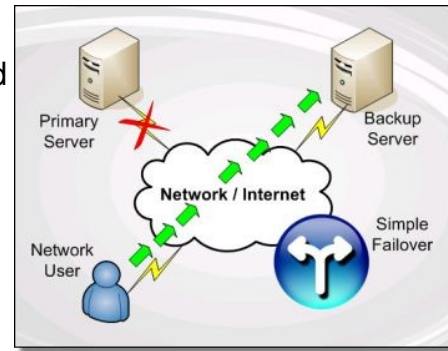
Implement redundant components and failover mechanisms to ensure continuous availability of critical systems and services. This includes redundant power supplies, network connections, and backup systems that can automatically take over in case of hardware or software failures.

- **High Availability Architectures:** Design and implement high availability architectures that distribute workloads across multiple servers or data centers to prevent single points of failure. This may involve clustering, load balancing, and geographic redundancy to maintain service availability in the event of hardware or network failures.

- **Monitoring and Alerting Services:** Deploy comprehensive monitoring and alerting solutions to proactively monitor the health and performance of ICT infrastructure and applications. This includes monitoring key performance indicators (KPIs), system metrics, and application availability, and alerting IT staff or automated systems of any abnormalities or issues.
- **Disaster Recovery Planning:** Develop and maintain a robust disaster recovery plan that outlines procedures for recovering from major disruptions or outages. This includes regular backups, data replication, and contingency plans for restoring services in the event of natural disasters, cyber attacks, or other emergencies.

- **Patch Management Services:** Implement a rigorous patch management process to keep operating systems, software, and firmware up to date with the latest security patches and updates. This helps mitigate security vulnerabilities and reduce the risk of system failures or breaches due to unpatched software.

- **Load Testing and Capacity Planning:** Conduct load testing and capacity planning exercises to identify potential bottlenecks and capacity limits in ICT infrastructure and applications. This helps ensure that systems can handle peak loads and unexpected spikes in demand without experiencing performance degradation or downtime.



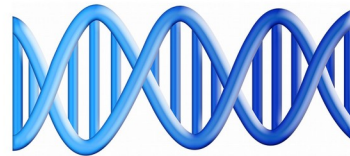
- **Incident Management and Response Services:** Establish an incident management and response framework to promptly address and resolve ICT incidents and service disruptions. This includes defining escalation procedures, assigning responsibilities, and coordinating responses to restore services as quickly as possible.
- **Continuous Monitoring and Improvement:** Implement a culture of continuous monitoring and improvement to regularly assess the reliability and performance of ICT services and identify opportunities for optimization. This involves conducting post-incident reviews, performance tuning, and implementing feedback loops to drive continuous improvement.
- **Security and Compliance Services:** Ensure that ICT services are secured against threats and comply with relevant regulations and standards. This includes implementing complete reliability measures, access controls, encryption, and regular tests by administrators to confirm configurations are properly operational and working as expected to allow authorized access and prevent denied access.
- **Employee Training and Awareness Programs:** Educate employees about the importance of reliability and best practices for maintaining ICT services. This includes providing training on reliability and security awareness, incident response procedures, and proper use of ICT resources to minimize human errors and mitigate risks.



By implementing these services and strategies, organizations can increase the reliability of their ICT services, minimize downtime, and deliver a consistent and dependable user experience to customers, employees, and stakeholders.

Three reasons to use Heavy Data Backup products.

HEAVY DATA
BACKUP



Data recovery services are expensive and time consuming. Also they are not guaranteed to get all of the data back.



If the media is totally lost due to misplacement, theft, fire, age related failure or any other reason then the recovery chances are near zero.

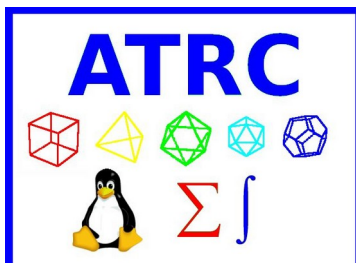
If a business faces a significant data loss, then the chances of the business being merged into another competitor business or closing withing the next 1 year becomes very high.

Because if you do not take care of your customers, then someone else will.

Contact : info@atrc.net.pk

Web : <http://atrc.net.pk>

Phone : +92 343 270 2932, +92 331 2036 422



Karachi Computer Services



Network Attached Storage (NAS)

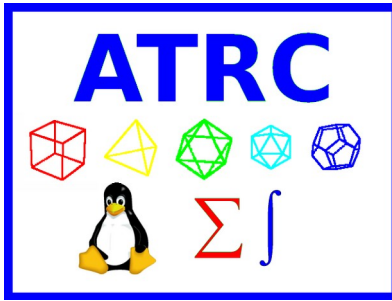


Page with links to a lot of resources.

<https://atrc.net.pk/dokuwiki/doku.php?id=start>

ATRC.NET.PK

[Table of Contents](#)



S.U.P.P.O.R.T. TM
Super User-friendly Professional
People Offering Remote Troubleshooting



How Investing Time and Resources in Strategic ICT Helps Your Business

in [English](#), [Urdu](#), [Spanish](#), [Chinese](#), [French](#), [Arabic](#), [Bengali](#), [Russian](#), [Japanese](#), [Indonesian](#), [Malay](#)

Peace of mind in a tech-driven world TM

English

Investing in strategic ICT (Information and Communication Technology) enables businesses to achieve sustainable growth, improve efficiency, and maintain a competitive edge. Here's how it delivers value:

1. Aligns Technology with Business Goals

Strategic ICT ensures your technology investments are aligned with your business objectives. It enables you to adopt tools and systems that directly contribute to your goals, such as increasing revenue, improving customer satisfaction, or expanding into new markets.

2. Improves Operational Efficiency

Implementing ICT solutions streamlines workflows, automates routine tasks, and reduces manual errors. This leads to enhanced productivity, faster turnaround times, and more efficient use of resources.

3. Supports Informed Decision-Making

With advanced data analytics and reporting tools, strategic ICT helps businesses gather actionable insights. Decision-makers can analyze trends, predict outcomes, and make data-driven choices that minimize risks and capitalize on opportunities.

[Table of Contents](#)

4. Enhances Customer Experiences

ICT investments enable better customer engagement through personalized experiences, faster service delivery, and seamless interactions. Tools like CRM systems and chatbots help build stronger relationships and increase customer loyalty.

5. Facilitates Innovation and Scalability

Strategic ICT promotes innovation by adopting emerging technologies that transform business models. Scalable solutions ensure that your systems grow with your business, enabling you to enter new markets or handle increasing demand effortlessly.

6. Boosts Security and Compliance

Proactively addressing cybersecurity risks protects your business from data breaches and cyberattacks. ICT solutions also help ensure compliance with industry regulations, safeguarding your reputation and avoiding penalties.

7. Reduces Costs and Increases ROI

By eliminating inefficiencies, replacing outdated systems, and adopting cost-effective solutions, ICT investments deliver better value for money. The long-term ROI often outweighs the initial investment.

8. Prepares for the Future

A strategic ICT approach ensures your business is ready to adapt to technological advancements. Future-proofing your operations allows you to stay competitive in a rapidly changing landscape.

Conclusion

Investing time and resources in strategic ICT is more than a technological upgrade—it's a business transformation. It drives growth, improves efficiency, and positions your company for long-term success, making it an essential aspect of modern business strategy.

میں وقت اور وسائل کی سرمایہ کاری آپ کے کاروبار کو کس طرح مدد دیتی ہے۔ ICT اسٹریٹجک

اسٹریٹجک آئی سی ٹی (انفرمیشن اینڈ کمیونیکیشن ٹیکنالوجی) میں سرمایہ کاری کاروباروں کو پائیدار ترقی حاصل کرنے، کارکردگی کو بہتر بنانے اور مسابقتی برتری کو برقرار رکھنے کے قابل بناتی ہے۔ یہاں یہ ہے کہ یہ کس طرح قیمت فراہم کرتا ہے:

1. ٹیکنالوجی کو کاروباری اہداف کے ساتھ ہم آہنگ کرتا ہے۔

اسٹریٹجک آئی سی ٹی یقینی بناتا ہے کہ آپ کی ٹیکنالوجی کی سرمایہ کاری آپ کے کاروباری مقاصد کے ساتھ ہم آہنگ ہے۔ یہ آپ کو ایسے ٹولز اور سسٹمز کو اپنانے کے قابل بناتا ہے جو آپ کے اہداف میں براہ راست حصہ ڈالتے ہیں، جیسے کہ آمدنی میں اضافہ، کسٹمر کی اطمینان کو بہتر بنانا، یا نئی منڈیوں میں توسیع کرنا۔

2. آپریشنل کارکردگی کو بہتر بناتا ہے۔

آئی سی ٹی سلوشنز کو لاگو کرنا ورک فلو کو ہموار کرتا ہے، معمول کے کاموں کو خودکار کرتا ہے، اور دستی غلطیوں کو کم کرتا ہے۔ اس سے پیداواری صلاحیت میں اضافہ، تیزی سے تبدیلی کے اوقات اور وسائل کا زیادہ موثر استعمال ہوتا ہے۔

3. باخبر فیصلہ سازی کی حمایت کرتا ہے۔

کاروباری اداروں کو قابل عمل بصیرت جمع کرنے میں مدد ICT جدید ڈیٹا اینالیٹکس اور رپورٹنگ ٹولز کے ساتھ اسٹریٹجک کرتا ہے۔ فیصلہ ساز رجحانات کا تجزیہ کر سکتے ہیں، نتائج کی پیشن گوئی کر سکتے ہیں، اور ڈیٹا پر مبنی انتخاب کر سکتے ہیں جو خطرات کو کم کرتے ہیں اور مواقع سے فائدہ اٹھا سکتے ہیں۔

4. کسٹمر کے تجربات کو بڑھاتا ہے۔

سرمایہ کاری ذاتی تجربات، تیز تر سروس ڈیلیوری، اور بغیر کسی رکاوٹ کے تعاملات کے ذریعے صارفین کی بہتر ICT سسٹمز اور چیٹ بوٹس جیسے ٹولز مضبوط تعلقات بنانے اور کسٹمر کی وفاداری بڑھانے CRM مصروفیت کو قابل بناتی ہے۔ میں مدد کرتے ہیں۔

5. جدت اور توسیع پذیری کی سہولت۔

اسٹریٹجک آئی سی ٹی ابھرتی ہوئی ٹیکنالوجیز کو اپنا کر جدت کو فروغ دیتا ہے جو کاروباری ماڈلز کو تبدیل کرتی ہے۔ توسیع پذیر حل اس بات کو یقینی بناتے ہیں کہ آپ کے سسٹمز آپ کے کاروبار کے ساتھ ترقی کریں، آپ کو نئی منڈیوں میں داخل ہونے یا بڑھتی ہوئی طلب کو آسانی سے سنبھالنے کے قابل بناتے ہیں۔

6. سیکیورٹی اور تعمیل کو بڑھاتا ہے۔

سائبرسیکیورٹی کے خطرات کو فعال طور پر حل کرنا آپ کے کاروبار کو ڈیٹا کی خلاف ورزیوں اور سائبر حملوں سے بچاتا حل صنعت کے ضوابط کی تعمیل کو یقینی بنانے، آپ کی ساکھ کی حفاظت اور جرمانے سے بچنے میں بھی مدد ICT ہے۔ کرتے ہیں۔

میں اضافہ کرتا ہے۔ ROI اخراجات کو کم کرتا ہے اور 7.

سرمایہ کاری پیسے کی بہتر ICT، ناکاریوں کو ختم کرکے، فرسودہ نظاموں کو تبدیل کرکے، اور لاگت سے موثر حل اپنانے سے اکثر ابتدائی سرمایہ کاری سے زیادہ ہوتا ہے۔ ROI قیمت فراہم کرتی ہے۔ طویل مدتی مستقبل کے لیے تیاری کرتا ہے۔ 8.

ایک اسٹریٹجک آئی سی ٹی نقطہ نظر اس بات کو یقینی بناتا ہے کہ آپ کا کاروبار تکنیکی ترقی کے مطابق ڈھالنے کے لیے تیار ہے۔ آپ کے آپریشنز کو مستقبل میں پروف کرنے سے آپ کو تیزی سے بدلتے ہوئے منظر نامے میں مسابقتی رہنے کی اجازت ملتی ہے۔

نتیجہ

میں وقت اور وسائل کی سرمایہ کاری ایک تکنیکی اپ گریڈ سے زیادہ ہے - یہ ایک کاروباری تبدیلی ہے۔ یہ ICT تزویراتی ترقی کو آگے بڑھاتا ہے، کارکردگی کو بہتر بناتا ہے، اور آپ کی کمپنی کو طویل مدتی کامیابی کے لیے پوزیشن دیتا ہے، جو اسے جدید کاروباری حکمت عملی کا ایک لازمی پہلو بناتا ہے۔

Spanish

Cómo la inversión de tiempo y recursos en TIC estratégicas ayuda a su empresa

La inversión en TIC estratégicas (tecnologías de la información y la comunicación) permite a las empresas lograr un crecimiento sostenible, mejorar la eficiencia y mantener una ventaja competitiva. Así es como aporta valor:

1. Alinea la tecnología con los objetivos empresariales

Las TIC estratégicas garantizan que sus inversiones en tecnología estén alineadas con sus objetivos empresariales. Le permiten adoptar herramientas y sistemas que contribuyen directamente a sus objetivos, como aumentar los ingresos, mejorar la satisfacción del cliente o expandirse a nuevos mercados.

2. Mejora la eficiencia operativa

La implementación de soluciones de TIC agiliza los flujos de trabajo, automatiza las tareas rutinarias y reduce los errores manuales. Esto conduce a una mayor productividad, tiempos de respuesta más rápidos y un uso más eficiente de los recursos.

3. Apoya la toma de decisiones informada

Con herramientas avanzadas de análisis de datos y generación de informes, las TIC estratégicas ayudan a las empresas a recopilar información útil. Los responsables de la toma de decisiones pueden analizar tendencias, predecir resultados y tomar decisiones basadas en datos que minimicen los riesgos y aprovechen las oportunidades.

4. Mejora las experiencias de los clientes

Las inversiones en TIC permiten una mejor interacción con los clientes a través de experiencias personalizadas, una entrega de servicios más rápida e interacciones fluidas. Herramientas como los sistemas CRM y los chatbots ayudan a construir relaciones más sólidas y aumentar la lealtad de los clientes.

5. Facilita la innovación y la escalabilidad

[Table of Contents](#)

Las TIC estratégicas promueven la innovación mediante la adopción de tecnologías emergentes que transforman los modelos comerciales. Las soluciones escalables garantizan que sus sistemas crezcan con su negocio, lo que le permite ingresar a nuevos mercados o manejar la creciente demanda sin esfuerzo.

6. Aumenta la seguridad y el cumplimiento

Abordar de manera proactiva los riesgos de ciberseguridad protege a su negocio de las violaciones de datos y los ciberataques. Las soluciones de TIC también ayudan a garantizar el cumplimiento de las regulaciones de la industria, salvaguardando su reputación y evitando sanciones.

7. Reduce los costos y aumenta el ROI

Al eliminar ineficiencias, reemplazar sistemas obsoletos y adoptar soluciones rentables, las inversiones en TIC brindan una mejor relación calidad-precio. El ROI a largo plazo a menudo supera la inversión inicial.

8. Prepara para el futuro

Un enfoque estratégico de TIC garantiza que su negocio esté listo para adaptarse a los avances tecnológicos. La preparación de sus operaciones para el futuro le permite seguir siendo competitivo en un panorama que cambia rápidamente.

Conclusión

Invertir tiempo y recursos en TIC estratégicas es más que una actualización tecnológica: es una transformación empresarial. Impulsa el crecimiento, mejora la eficiencia y posiciona a su empresa para el éxito a largo plazo, lo que la convierte en un aspecto esencial de la estrategia empresarial moderna.

Chinese

如何将时间和资源投入战略 ICT 来帮助您的业务

投资战略 ICT（信息和通信技术）可使企业实现可持续增长、提高效率并保持竞争优势。以下是它如何实现价值：

1. 将技术与业务目标相结合

战略 ICT 可确保您的技术投资与您的业务目标保持一致。它使您能够采用直接有助于实现目标的工具和系统，例如增加收入、提高客户满意度或拓展新市场。

2. 提高运营效率

实施 ICT 解决方案可简化工作流程、自动化日常任务并减少人工错误。这可提高生产力、缩短周转时间并更有效地利用资源。

3. 支持明智的决策

借助先进的数据分析和报告工具，战略 ICT 可帮助企业收集可付诸行动的见解。决策者可以分析趋势、预测结果并做出数据驱动的选择，以最大限度地降低风险并利用机会。

4. 增强客户体验

ICT 投资通过个性化体验、更快的服务交付和无缝互动实现更好的客户参与度。CRM 系统和聊天机器人等工具有助于建立更牢固的关系并提高客户忠诚度。

5. 促进创新和可扩展性

战略 ICT 通过采用改变商业模式的新兴技术来促进创新。可扩展的解决方案可确保您的系统与业务一起发展，使您能够进入新市场或轻松应对不断增长的需求。

6. 提高安全性和合规性

主动解决网络安全风险可保护您的企业免受数据泄露和网络攻击。ICT 解决方案还有助于确保遵守行业法规，维护您的声誉并避免受到处罚。

[Table of Contents](#)

7. 降低成本并提高投资回报率

通过消除低效率、更换过时的系统并采用具有成本效益的解决方案，ICT 投资可实现更高的性价比。长期投资回报率通常超过初始投资。

8. 为未来做好准备

战略性 ICT 方法可确保您的业务随时适应技术进步。为您的运营做好未来准备可让您在快速变化的环境中保持竞争力。

结论

在战略性 ICT 上投入时间和资源不仅仅是技术升级，更是业务转型。它可以推动增长、提高效率，并为您的公司带来长期成功，使其成为现代商业战略的一个重要方面。

French

Comment investir du temps et des ressources dans les TIC stratégiques peut aider votre entreprise

Investir dans les TIC stratégiques (technologies de l'information et de la communication) permet aux entreprises d'atteindre une croissance durable, d'améliorer leur efficacité et de conserver un avantage concurrentiel. Voici comment cela apporte de la valeur :

1. Aligner la technologie sur les objectifs de l'entreprise

Les TIC stratégiques garantissent que vos investissements technologiques sont alignés sur vos objectifs commerciaux. Elles vous permettent d'adopter des outils et des systèmes qui contribuent directement à vos objectifs, tels que l'augmentation des revenus, l'amélioration de la satisfaction client ou l'expansion sur de nouveaux marchés.

2. Améliorer l'efficacité opérationnelle

La mise en œuvre de solutions TIC rationalise les flux de travail, automatise les tâches de routine et réduit les erreurs manuelles. Cela conduit à une productivité accrue, à des délais d'exécution plus rapides et à une utilisation plus efficace des ressources.

3. Favorise la prise de décision éclairée

Grâce à des outils avancés d'analyse et de reporting des données, les TIC stratégiques aident les entreprises à recueillir des informations exploitables. Les décideurs peuvent analyser les tendances, prédire les résultats et faire des choix basés sur les données qui minimisent les risques et capitalisent sur les opportunités.

4. Améliore l'expérience client

Les investissements dans les TIC permettent un meilleur engagement client grâce à des expériences personnalisées, une prestation de services plus rapide et des interactions fluides. Des outils tels que les systèmes CRM et les chatbots aident à établir des relations plus solides et à accroître la fidélité des clients.

5. Facilite l'innovation et l'évolutivité

[Table of Contents](#)

Les TIC stratégiques favorisent l'innovation en adoptant des technologies émergentes qui transforment les modèles commerciaux. Les solutions évolutives garantissent que vos systèmes évoluent avec votre entreprise, vous permettant ainsi de pénétrer de nouveaux marchés ou de gérer une demande croissante sans effort.

6. Renforce la sécurité et la conformité

La gestion proactive des risques de cybersécurité protège votre entreprise contre les violations de données et les cyberattaques. Les solutions TIC contribuent également à garantir la conformité aux réglementations du secteur, à préserver votre réputation et à éviter les pénalités.

7. Réduit les coûts et augmente le retour sur investissement

En éliminant les inefficacités, en remplaçant les systèmes obsolètes et en adoptant des solutions rentables, les investissements dans les TIC offrent un meilleur rapport qualité-prix. Le retour sur investissement à long terme dépasse souvent l'investissement initial.

8. Prépare l'avenir

Une approche TIC stratégique garantit que votre entreprise est prête à s'adapter aux avancées technologiques. En préparant vos opérations pour l'avenir, vous restez compétitif dans un environnement en constante évolution.

Conclusion

Investir du temps et des ressources dans les TIC stratégiques est plus qu'une simple mise à niveau technologique : c'est une transformation de l'entreprise. Cela stimule la croissance, améliore l'efficacité et positionne votre entreprise sur la voie du succès à long terme, ce qui en fait un aspect essentiel de la stratégie commerciale moderne.

Arabic

كيف يساعد استثمار الوقت والموارد في تكنولوجيا المعلومات والاتصالات الاستراتيجية عملك

الاستثمار في تكنولوجيا المعلومات والاتصالات الاستراتيجية يمكّن الشركات من تحقيق نمو مستدام وتحسين الكفاءة والحفاظ على ميزة تنافسية. وإليك كيفية تقديم القيمة

مواءمة التكنولوجيا مع أهداف العمل 1.

تضمن تكنولوجيا المعلومات والاتصالات الاستراتيجية أن استثمارك في التكنولوجيا تتوافق مع أهداف عملك. فهي تمكنك من تبني الأدوات والأنظمة التي تساهم بشكل مباشر في تحقيق أهدافك، مثل زيادة الإيرادات، وتحسين رضا العملاء، أو التوسع في أسواق جديدة.

تحسين الكفاءة التشغيلية 2.

يعمل تنفيذ حلول تكنولوجيا المعلومات والاتصالات على تبسيط سير العمل، وأتمتة المهام الروتينية، والحد من الأخطاء اليدوية. وهذا يؤدي إلى زيادة الإنتاجية، وأوقات استجابة أسرع، واستخدام أكثر كفاءة للموارد.

دعم اتخاذ القرارات المستنيرة 3.

بفضل أدوات تحليل البيانات المتقدمة وإعداد التقارير، تساعد تكنولوجيا المعلومات والاتصالات الاستراتيجية الشركات على جمع رؤى قابلة للتنفيذ. يمكن لصناع القرار تحليل الاتجاهات، والتنبؤ بالنتائج، واتخاذ خيارات تعتمد على البيانات لتقليل المخاطر والاستفادة من الفرص.

تعزيز تجارب العملاء 4.

تمكن استثمارات تكنولوجيا المعلومات والاتصالات من تحسين تفاعل العملاء من خلال تجارب مخصصة، وتسريع تقديم الخدمة، والتفاعل السلس. تساعد أدوات مثل أنظمة إدارة علاقات العملاء والروبوتات الدردشة في بناء علاقات أقوى وزيادة ولاء العملاء.

تسهيل الابتكار وقابلية التوسع 5.

تعزز تكنولوجيا المعلومات والاتصالات الاستراتيجية الابتكار من خلال تبني التقنيات الناشئة التي تحول نماذج الأعمال. تضمن الحلول القابلة للتطوير نمو أنظمتك مع عملك، مما يتيح لك دخول أسواق جديدة أو التعامل مع الطلب المتزايد دون عناء.

تعزيز الأمان والامتثال 6.

يعمل التعامل بشكل استباقي مع مخاطر الأمن السيبراني على حماية عملك من خروقات البيانات والهجمات الإلكترونية. تساعد حلول تكنولوجيا المعلومات والاتصالات أيضًا في ضمان الامتثال للوائح الصناعة، وحماية سمعتك وتجنب العقوبات.

تقليل التكاليف وزيادة العائد على الاستثمار 7.

من خلال القضاء على عدم الكفاءة، واستبدال الأنظمة القديمة، وتبني حلول فعالة من حيث التكلفة، توفر استثمارات تكنولوجيا المعلومات والاتصالات قيمة أفضل مقابل المال. غالبًا ما يفوق العائد على الاستثمار الطويل الأجل الاستثمار الأولي.

الاستعداد للمستقبل 8.

يضمن النهج الاستراتيجي لتكنولوجيا المعلومات والاتصالات جاهزية عملك للتكيف مع التطورات التكنولوجية. يتيح لك تأمين عملياتك للمستقبل البقاء قائمًا على المنافسة في بيئة سريعة التغير.

الخلاصة

إن استثمار الوقت والموارد في تكنولوجيا المعلومات والاتصالات الاستراتيجية هو أكثر من مجرد ترقية تكنولوجية - إنه تحول تجاري. إنه يدفع النمو ويحسن الكفاءة ويضع شركتك في وضع يسمح لها بالنجاح على المدى الطويل، مما يجعلها جانبًا أساسيًا من استراتيجية الأعمال الحديثة.

Bengali

কৌশলগত আইসিটি-তে সময় এবং সম্পদ কীভাবে বিনিয়োগ করা আপনার ব্যবসাকে সাহায্য করে

কৌশলগত আইসিটি (তথ্য ও যোগাযোগ প্রযুক্তি) তে বিনিয়োগ ব্যবসাগুলিকে টেকসই প্রবৃদ্ধি অর্জন করতে, দক্ষতা উন্নত করতে এবং একটি প্রতিযোগিতামূলক প্রান্ত বজায় রাখতে সক্ষম করে। এটি কীভাবে মান সরবরাহ করে তা এখানে:

1. ব্যবসায়িক লক্ষ্যগুলির সাথে প্রযুক্তিকে সারিবদ্ধ করে

কৌশলগত আইসিটি নিশ্চিত করে যে আপনার প্রযুক্তি বিনিয়োগগুলি আপনার ব্যবসার উদ্দেশ্যগুলির সাথে সামঞ্জস্যপূর্ণ। এটি আপনাকে এমন সরঞ্জাম এবং সিস্টেমগুলি গ্রহণ করতে সক্ষম করে যা সরাসরি আপনার লক্ষ্যগুলিতে অবদান রাখে, যেমন রাজস্ব বৃদ্ধি, গ্রাহক সন্তুষ্টি উন্নত করা বা নতুন বাজারে প্রসারিত করা।

2. অপারেশনাল দক্ষতা উন্নত করে

আইসিটি সমাধানগুলি কার্যকর করা কর্মপ্রবাহকে স্ট্রীমলাইন করে, রুটিন কাজগুলিকে স্বয়ংক্রিয় করে এবং ম্যানুয়াল ত্রুটিগুলি হ্রাস করে। এটি বর্ধিত উপাদানশীলতা, দ্রুত পরিবর্তনের সময় এবং সম্পদের আরও দক্ষ ব্যবহারের দিকে পরিচালিত করে।

3. অবহিত সিদ্ধান্ত গ্রহণ সমর্থন করে

উন্নত ডেটা বিশ্লেষণ এবং রিপোর্টিং সরঞ্জামগুলির সাথে, কৌশলগত আইসিটি ব্যবসাগুলিকে কার্যকর অন্তর্দৃষ্টি সংগ্রহ করতে সহায়তা করে। সিদ্ধান্ত গ্রহণকারীরা প্রবণতা বিশ্লেষণ করতে পারে, ফলাফলের পূর্বাভাস দিতে পারে এবং ডেটা-চালিত পছন্দ করতে পারে যা ঝুঁকি কমিয়ে দেয় এবং সুযোগগুলিকে পুঁজি করে।

4. গ্রাহকের অভিজ্ঞতা বাড়ায়

আইসিটি বিনিয়োগগুলি ব্যক্তিগতকৃত অভিজ্ঞতা, দ্রুত পরিষেবা সরবরাহ এবং নির্বিঘ্ন মিথস্ক্রিয়াগুলির মাধ্যমে আরও ভাল গ্রাহকের অংশগ্রহণকে সক্ষম করে। CRM সিস্টেম এবং চ্যাটবটগুলির মতো সরঞ্জামগুলি শক্তিশালী সম্পর্ক গড়ে তুলতে এবং গ্রাহকের আনুগত্য বাড়াতে সাহায্য করে।

5. উদ্ভাবন এবং পরিমাপযোগ্যতা সুবিধা দেয়

কৌশলগত আইসিটি উদীয়মান প্রযুক্তি গ্রহণ করে উদ্ভাবনের প্রচার করে যা ব্যবসায়িক মডেলকে রূপান্তরিত করে। পরিমাপযোগ্য সমাধানগুলি নিশ্চিত করে যে আপনার সিস্টেমগুলি আপনার ব্যবসার সাথে বৃদ্ধি পায়, আপনাকে নতুন বাজারে প্রবেশ করতে বা কর্মমবর্ধমান চাহিদা অনায়াসে পরিচালনা করতে সক্ষম করে।

6. নিরাপত্তা এবং সম্মতি বাড়ায়

[Table of Contents](#)

সক্রিয়ভাবে সাইবার নিরাপত্তা ঝুঁকি মোকাবেলা করা আপনার ব্যবসাকে ডেটা লঙ্ঘন এবং সাইবার আক্রমণ থেকে রক্ষা করে। আইসিটি সমাধানগুলি শিল্পের বিধি-বিধানের সাথে সম্মতি নিশ্চিত করতে, আপনার খ্যাতি রক্ষা করতে এবং জরিমানা এড়াতে সহায়তা করে।

7. খরচ কমাও এবং ROI বাড়াও

অদক্ষতা দূর করে, পুরানো সিস্টেম প্রতিস্থাপন করে এবং শাস্ত্রীয় সমাধান গ্রহণ করে, আইসিটি বিনিয়োগ অর্থের জন্য আরও ভাল মূল্য প্রদান করে। দীর্ঘমেয়াদী ROI প্রায়শই প্রাথমিক বিনিয়োগের চেয়ে বেশি হয়।

8. ভবিষ্যতের জন্য প্রস্তুত করে

একটি কৌশলগত আইসিটি পদ্ধতি নিশ্চিত করে যে আপনার ব্যবসা প্রযুক্তিগত অগ্রগতির সাথে খাপ খাইয়ে নিতে প্রস্তুত। আপনার ক্রিয়াকলাপগুলির ভবিষ্যত-প্রুফিং আপনাকে দ্রুত পরিবর্তনশীল ল্যান্ডস্কেপে প্রতিযোগিতামূলক থাকতে দেয়।

উপসংহার

কৌশলগত আইসিটিতে সময় এবং সংস্থান বিনিয়োগ করা একটি প্রযুক্তিগত আপগ্রেডের চেয়ে বেশি - এটি একটি ব্যবসায়িক রূপান্তর। এটি বৃদ্ধিকে চালিত করে, দক্ষতা উন্নত করে এবং দীর্ঘমেয়াদী সাফল্যের জন্য আপনার কোম্পানিকে অবস্থান করে, এটিকে আধুনিক ব্যবসায়িক কৌশলের একটি অপরিহার্য দিক করে তোলে।

Russian

Как инвестирование времени и ресурсов в стратегические ИКТ помогает вашему бизнесу

Инвестирование в стратегические ИКТ (информационно-коммуникационные технологии) позволяет компаниям достигать устойчивого роста, повышать эффективность и сохранять конкурентное преимущество. Вот как это обеспечивает ценность:

1. Согласовывает технологии с бизнес-целями

Стратегические ИКТ гарантируют, что ваши технологические инвестиции соответствуют бизнес-целям. Они позволяют вам внедрять инструменты и системы, которые напрямую способствуют достижению ваших целей, таких как увеличение доходов, повышение удовлетворенности клиентов или выход на новые рынки.

2. Повышают операционную эффективность

Внедрение решений ИКТ оптимизирует рабочие процессы, автоматизирует рутинные задачи и сокращает количество ручных ошибок. Это приводит к повышению производительности, сокращению сроков выполнения и более эффективному использованию ресурсов.

3. Поддерживает принятие обоснованных решений

Благодаря передовым инструментам анализа данных и отчетности стратегические ИКТ помогают компаниям собирать действенные идеи. Лица, принимающие решения, могут анализировать тенденции, прогнозировать результаты и делать выбор на основе данных, чтобы минимизировать риски и извлекать выгоду из возможностей.

Инвестиции в ИКТ позволяют улучшить взаимодействие с клиентами за счет персонализированного опыта, более быстрой доставки услуг и бесперебойного взаимодействия. Такие инструменты, как CRM-системы и чат-боты, помогают строить более прочные отношения и повышать лояльность клиентов.

5. Способствует инновациям и масштабируемости

[Table of Contents](#)

Стратегические ИКТ способствуют инновациям, внедряя новые технологии, которые преобразуют бизнес-модели. Масштабируемые решения гарантируют, что ваши системы будут расти вместе с вашим бизнесом, позволяя вам выходить на новые рынки или легко справляться с растущим спросом.

6. Повышает безопасность и соответствие требованиям

Проактивное устранение рисков кибербезопасности защищает ваш бизнес от утечек данных и кибератак. ИКТ-решения также помогают обеспечить соответствие отраслевым нормам, защищая вашу репутацию и избегая штрафов.

7. Снижает затраты и увеличивает рентабельность инвестиций

Устраняя неэффективность, заменяя устаревшие системы и внедряя экономически эффективные решения, инвестиции в ИКТ обеспечивают лучшее соотношение цены и качества. Долгосрочная рентабельность инвестиций часто превышает первоначальные инвестиции.

8. Подготовка к будущему

Стратегический подход к ИКТ гарантирует, что ваш бизнес готов адаптироваться к технологическим достижениям. Подготовка ваших операций к будущему позволяет вам оставаться конкурентоспособными в быстро меняющейся среде.

Заключение

Инвестирование времени и ресурсов в стратегические ИКТ — это больше, чем просто технологическое обновление, это трансформация бизнеса. Это стимулирует рост, повышает эффективность и позиционирует вашу компанию для долгосрочного успеха, что делает его важным аспектом современной бизнес-стратегии.

Japanese

戦略的 ICT に時間とリソースを投資することでビジネスにどのようなメリットがあるか

戦略的 ICT (情報通信技術) に投資することで、企業は持続可能な成長を達成し、効率性を高め、競争力を維持できます。その価値の実現方法は次のとおりです。

1. テクノロジーをビジネス目標に合わせる

戦略的 ICT により、テクノロジーへの投資がビジネス目標に合致することが保証されます。収益の増加、顧客満足度の向上、新規市場への進出など、目標に直接貢献するツールやシステムを導入できます。

2. 運用効率の向上

ICT ソリューションを実装すると、ワークフローが合理化され、日常的なタスクが自動化され、手作業によるエラーが削減されます。これにより、生産性が向上し、処理時間が短縮され、リソースをより効率的に使用できるようになります。

3. 情報に基づいた意思決定をサポート

高度なデータ分析およびレポート作成ツールにより、戦略的 ICT は企業が実用的な洞察を収集するのに役立ちます。意思決定者は、傾向を分析し、結果を予測し、リスクを最小限に抑えて機会を活かすデータ主導の選択を行うことができます。

4. 顧客体験の向上

ICT 投資により、パーソナライズされた体験、より迅速なサービス提供、シームレスなインタラクションを通じて、顧客エンゲージメントが向上します。CRM システムやチャットボットなどのツールは、より強固な関係を構築し、顧客ロイヤルティを高めるのに役立ちます。

5. イノベーションとスケーラビリティの促進

戦略的 ICT は、ビジネス モデルを変革する新しいテクノロジーを採用することでイノベーションを促進します。スケーラブルなソリューションにより、システムがビジネスとともに成長し、新しい市場に参入したり、増大する需要に簡単に対応したりできるようになります。

6. セキュリティとコンプライアンスの強化

サイバーセキュリティのリスクに積極的に対処することで、データ侵害やサイバー攻撃からビジネスを保護できます。ICT ソリューションは、業界規制への準拠を保証し、評判を守り、罰金を回避するのに役立ちます。

7. コストを削減し、ROI を向上

非効率性を排除し、時代遅れのシステムを置き換え、費用対効果の高いソリューションを採用することで、ICT 投資は費用対効果を高めます。長期的な ROI は、多くの場合、初期投資を上回ります。

8. 将来に備える

戦略的な ICT アプローチにより、ビジネスが技術の進歩に適応する準備が整います。業務を将来に備えることで、急速に変化する環境でも競争力を維持できます。

結論

戦略的な ICT に時間とリソースを投資することは、単なる技術のアップグレードではなく、ビジネスの変革です。成長を促進し、効率性を向上させ、長期的な成功に向けて会社を位置づけるため、現代のビジネス戦略に不可欠な要素となります。

Indonesian

Bagaimana Investasi Waktu dan Sumber Daya dalam TIK Strategis Membantu Bisnis Anda

Investasi dalam TIK (Teknologi Informasi dan Komunikasi) strategis memungkinkan bisnis untuk mencapai pertumbuhan berkelanjutan, meningkatkan efisiensi, dan mempertahankan keunggulan kompetitif. Berikut ini adalah cara memberikan nilai:

1. Menyelaraskan Teknologi dengan Tujuan Bisnis

TIK strategis memastikan investasi teknologi Anda selaras dengan tujuan bisnis Anda. Ini memungkinkan Anda untuk mengadopsi alat dan sistem yang secara langsung berkontribusi pada tujuan Anda, seperti meningkatkan pendapatan, meningkatkan kepuasan pelanggan, atau memperluas ke pasar baru.

2. Meningkatkan Efisiensi Operasional

Penerapan solusi TIK menyederhanakan alur kerja, mengotomatiskan tugas-tugas rutin, dan mengurangi kesalahan manual. Hal ini mengarah pada peningkatan produktivitas, waktu penyelesaian yang lebih cepat, dan penggunaan sumber daya yang lebih efisien.

3. Mendukung Pengambilan Keputusan yang Terinformasi

Dengan alat analitik data dan pelaporan yang canggih, TIK strategis membantu bisnis mengumpulkan wawasan yang dapat ditindaklanjuti. Para pengambil keputusan dapat menganalisis tren, memprediksi hasil, dan membuat pilihan berdasarkan data yang meminimalkan risiko dan memanfaatkan peluang. 4. Meningkatkan Pengalaman Pelanggan

Investasi TIK memungkinkan keterlibatan pelanggan yang lebih baik melalui pengalaman yang dipersonalisasi, penyampaian layanan yang lebih cepat, dan interaksi yang lancar. Berbagai alat seperti sistem CRM dan chatbot membantu membangun hubungan yang lebih kuat dan meningkatkan loyalitas pelanggan.

5. Memfasilitasi Inovasi dan Skalabilitas

[Table of Contents](#)

TIK strategis mendorong inovasi dengan mengadopsi berbagai teknologi baru yang mengubah model bisnis. Solusi yang dapat diskalakan memastikan bahwa sistem Anda tumbuh bersama bisnis Anda, memungkinkan Anda memasuki pasar baru atau menangani peningkatan permintaan dengan mudah.

6. Meningkatkan Keamanan dan Kepatuhan

Menangani risiko keamanan siber secara proaktif melindungi bisnis Anda dari pelanggaran data dan serangan siber. Solusi TIK juga membantu memastikan kepatuhan terhadap peraturan industri, menjaga reputasi Anda, dan menghindari penalti.

7. Mengurangi Biaya dan Meningkatkan ROI

Dengan menghilangkan inefisiensi, mengganti sistem yang sudah ketinggalan zaman, dan mengadopsi solusi yang hemat biaya, investasi TIK memberikan nilai yang lebih baik untuk uang. ROI jangka panjang sering kali lebih besar daripada investasi awal.

8. Mempersiapkan Masa Depan

Pendekatan TIK strategis memastikan bisnis Anda siap beradaptasi dengan kemajuan teknologi. Mempersiapkan operasi Anda untuk masa depan memungkinkan Anda untuk tetap kompetitif dalam lanskap yang berubah dengan cepat.

Kesimpulan

Investasi waktu dan sumber daya dalam TIK strategis lebih dari sekadar peningkatan teknologi—ini adalah transformasi bisnis. Ini mendorong pertumbuhan, meningkatkan efisiensi, dan memposisikan perusahaan Anda untuk kesuksesan jangka panjang, menjadikannya aspek penting dari strategi bisnis modern.

Malay

Bagaimana Melabur Masa dan Sumber dalam ICT Strategik Membantu Perniagaan Anda

Melabur dalam ICT strategik (Teknologi Maklumat dan Komunikasi) membolehkan perniagaan mencapai pertumbuhan yang mampan, meningkatkan kecekapan dan mengekalkan kelebihan daya saing. Begini cara ia menyampaikan nilai:

1. Menjajarkan Teknologi dengan Matlamat Perniagaan

ICT strategik memastikan pelaburan teknologi anda sejajar dengan objektif perniagaan anda. Ia membolehkan anda menggunakan alat dan sistem yang menyumbang secara langsung kepada matlamat anda, seperti meningkatkan hasil, meningkatkan kepuasan pelanggan atau berkembang ke pasaran baharu.

2. Meningkatkan Kecekapan Operasi

Melaksanakan penyelesaian ICT memperkemas aliran kerja, mengautomasikan tugas rutin dan mengurangkan ralat manual. Ini membawa kepada produktiviti yang dipertingkatkan, masa pemulihan yang lebih cepat dan penggunaan sumber yang lebih cekap.

3. Menyokong Pembuatan Keputusan Termaklum

Dengan alat analisis dan pelaporan data lanjutan, ICT strategik membantu perniagaan mengumpul cerapan yang boleh diambil tindakan. Pembuat keputusan boleh menganalisis arah aliran, meramalkan hasil dan membuat pilihan berasaskan data yang meminimumkan risiko dan memanfaatkan peluang.

4. Meningkatkan Pengalaman Pelanggan

Pelaburan ICT membolehkan penglibatan pelanggan yang lebih baik melalui pengalaman yang diperibadikan, penyampaian perkhidmatan yang lebih pantas dan interaksi yang lancar. Alat seperti sistem CRM dan chatbots membantu membina hubungan yang lebih kukuh dan meningkatkan kesetiaan pelanggan.

5. Memudahkan Inovasi dan Skalabiliti

ICT strategik menggalakkan inovasi dengan mengguna pakai teknologi baru muncul yang mengubah model perniagaan. Penyelesaian berskala memastikan sistem anda berkembang bersama perniagaan anda, membolehkan anda memasuki pasaran baharu atau mengendalikan permintaan yang semakin meningkat dengan mudah.

6. Meningkatkan Keselamatan dan Pematuhan

Menangani risiko keselamatan siber secara proaktif melindungi perniagaan anda daripada pelanggaran data dan serangan siber. Penyelesaian ICT juga membantu memastikan pematuhan terhadap peraturan industri, menjaga reputasi anda dan mengelakkan penalti.

7. Mengurangkan Kos dan Meningkatkan ROI

Dengan menghapuskan ketidakcekapan, menggantikan sistem yang lapuk, dan menerima pakai penyelesaian yang kos efektif, pelaburan ICT memberikan nilai yang lebih baik untuk wang. ROI jangka panjang selalunya melebihi pelaburan awal.

8. Bersedia untuk Masa Depan

Pendekatan ICT yang strategik memastikan perniagaan anda bersedia untuk menyesuaikan diri dengan kemajuan teknologi. Kalis masa hadapan operasi anda membolehkan anda kekal berdaya saing dalam landskap yang berubah dengan pantas.

Kesimpulan

Melabur masa dan sumber dalam ICT strategik adalah lebih daripada peningkatan teknologi—ia merupakan transformasi perniagaan. Ia memacu pertumbuhan, meningkatkan kecekapan dan meletakkan syarikat anda untuk kejayaan jangka panjang, menjadikannya satu aspek penting dalam strategi perniagaan moden.