2025

WHITEPAPER

Securing Your Organization Against Email Threats

FSET Inc.
Address: 201-610 Lakeview Drive Kenora, ON P9N 3P7
Phone: (833) 468-0174
Email: info@fset.ca

CONTENTS

Executive Summary

Email remains the backbone of business communication, and one of the most exploited attack surfaces in the digital era. While security technologies have advanced rapidly, threat actors have evolved just as quickly. Artificial intelligence now amplifies phishing campaigns with language perfection, personalization at scale, and even deepfake audio or video that can deceive seasoned professionals.

Since 2022, the volume and sophistication of email-based attacks have surged. Phishing incidents now account for the majority of initial breaches across industries, costing organizations millions in downtime, remediation, and reputational damage. Traditional defenses such as multi-factor authentication and secure email gateways can no longer be relied upon as standalone safeguards.

In Canada, the Canadian Anti-Fraud Centre reported $647 million CAD in total fraud losses for 2024, with $67.5 million attributed specifically to spear phishing and business email compromise. These figures likely understate the true impact—CAFC estimates only 5-10% of victims report fraud incidents.

This paper examines how modern email threats have changed and what safeguards organizations must implement to protect against them. It explores emerging risks like AI-generated phishing, QR-code scams, and MFA bypass techniques—and outlines the layered protections that define today's standard for trustworthy communication.

For organizations operating in high-trust environments—from municipalities to healthcare systems—the difference between resilience and exposure often begins with how well email security is understood, managed, and continuously improved.

The Evolving Threat Landscape

AI-Powered Attacks and Traditional Defenses

Email threats no longer hinge on careless clicks or crude scams. Attackers now operate at industrial scale, using automation and AI to produce messages that mirror legitimate communications complete with correct branding, localized language, and context scraped from public data. To many recipients, the first sign anything is wrong appears only after a compromise.

Traditional defenses still matter but can't carry the load alone. Secure email gateways and filters struggle with adaptive attacks, and even multi-factor authentication is being sidestepped through fatigue tactics, session hijacking, and adversary-in-the-middle kits. The result is a risk environment defined less by volume and more by precision. AI handles the drafting and targeting at scale; humans step in to validate responses, push transactions, and pivot laterally through compromised accounts.

One of the most significant shifts in the threat landscape is the rise of attacks originating from compromised legitimate accounts. Roughly 44 percent of phishing emails now come from verified domains or known partners—accounts that have already passed authentication checks. When a trusted colleague, vendor, or partner's email is hijacked, the attacker inherits existing trust relationships, bypassing traditional filters and making detection far more difficult. These insider-style attacks create substantial delays in investigation and remediation, as security teams must carefully distinguish legitimate communications from malicious ones sent through authentic channels.

The takeaway isn't to abandon controls; it's to evolve them. Organizations need authentication and domain protections as table stakes, but resilience now depends on phishing-resistant MFA, account-takeover detection, QR-code controls, and training that accounts for AI-perfect language and executive deepfakes. This is the new baseline for trustworthy communication.

91%

of cyber attacks begin with a phishing email, making it the primary entry point for data breaches, ransomware, and business email compromise.

4,151%

increase in phishing attacks since late 2022 following the public release of ChatGPT and other generative AI tools.

$4.88 million

is the average cost of a phishing breach in 2024, up 9.7% from 2023.

$1.8 billion

in losses resulted from business email compromise in 2024, with wire transfer attacks increasing 33% in Q1 2025.

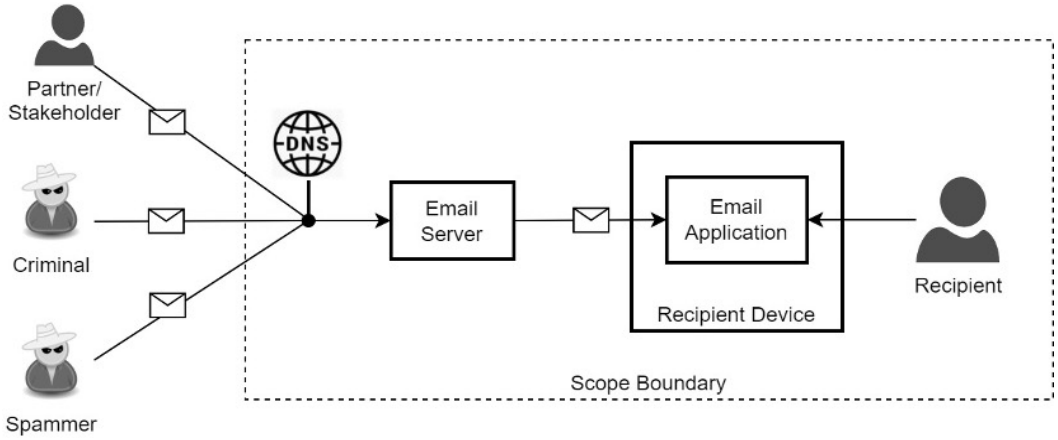
84.2%

of phishing attacks successfully bypass DMARC authentication, one of the most common email security protocols.

Email-Based Threats

How Modern Threat Actors Exploit the Inbox

What began as generic spam campaigns has evolved into a continuous, data-driven assault on organizations of every size and sector. Attackers now use automation, machine learning, and social engineering to craft credible messages that easily bypass legacy filters. For security and IT leaders, the challenge is no longer identifying whether an attack will happen, but recognizing how it will unfold, and whether the organization is prepared to contain it.



Who's Behind the Attacks

The actors driving email-based threats span a wide spectrum of capability and intent. At one end are organized criminal groups focused on profit—running large-scale phishing and ransomware operations designed to steal credentials, extort victims, or redirect financial transactions. Their operations increasingly resemble legitimate businesses, complete with service desks and affiliate programs.

A growing share of these operations are powered by Phishing-as-a-Service (PhaaS) platforms that package ready-made phishing kits—Tycoon 2FA, EvilGinx, WormGPT, and FraudGPT among them—for sale to less skilled attackers. These kits automate everything from fake login pages to session hijacking and token theft, making sophisticated attacks accessible to anyone with minimal technical knowledge.

State-sponsored threat actors pursue longer-term goals such as espionage, data theft, and strategic disruption. Their campaigns are often quiet, persistent, and narrowly focused on credential harvesting or infiltrating specific institutions. Meanwhile, insider threats—whether malicious or unintentional—add another layer of risk. Attacks launched from compromised or legitimate internal accounts are especially effective because they appear to come from trusted senders.

Traditional Phishing Threats

While today's attackers deploy increasingly sophisticated tools, many still rely on classic phishing techniques that exploit fundamental gaps in human judgment and basic security hygiene. These traditional methods remain effective because they target universal behaviors—trust, haste, and routine—allowing even unsophisticated actors to achieve high success rates.

- Credential Theft

Phishing is generally the most common starting point for cyber intrusions. Today's campaigns no longer rely on clumsy messages or broken English. Many now mimic legitimate multi-step login flows, complete with fake MFA prompts or OAuth consent screens that trick users into granting access to malicious applications.

Targeted variants such as spear phishing and whaling use publicly available information to impersonate executives, board members, or trusted partners. Business Email Compromise (BEC) scams, for example, have grown into billion-dollar criminal enterprises. In 2024 alone, BEC activity caused roughly $1.8 billion in losses, with 44 percent of phishing messages now sent from previously compromised legitimate accounts, giving them built-in credibility and a high success rate.

- Malware Delivery

Phishing emails also remain the leading delivery method for malware. Ransomware, remote access trojans (RATs), banking trojans, spyware, and keyloggers are routinely distributed through email attachments or embedded links. Attackers often exploit software vulnerabilities to install these payloads as the first step in multi-stage intrusions. Roughly 54 percent of ransomware infections still begin with a phishing email, and once inside, malware can exfiltrate data, steal credentials, or establish persistent remote access for future attacks.

- Spam and System Overload

Spam may seem trivial, but high-volume campaigns can serve strategic purposes including distributing phishing links at scale, testing the effectiveness of filters, or saturating systems so targeted messages slip through unnoticed. Even benign spam consumes time, bandwidth, and employee attention—costs that compound quickly in large organizations.

Emerging and Advanced Threats

Beyond familiar phishing tactics, a new generation of threats is reshaping the email security landscape. Artificial intelligence, automation, and novel attack surfaces like QR codes and multi-factor authentication are enabling adversaries to bypass even well-defended environments. Understanding these advanced tactics is essential to anticipating where email-based risk is headed next.

- AI-Powered Phishing

Artificial intelligence has fundamentally altered how phishing campaigns are created and deployed. In 2024, an estimated 67 percent of phishing attacks incorporated some form of AI. These systems can generate flawless grammar and tone, analyze open-source data to personalize messages instantly, and adapt in real time based on recipient behavior.

Deepfake voice and video tools now allow attackers to convincingly impersonate executives or colleagues. One multinational organization lost $25 million after an employee participated in a deepfake video call featuring what appeared to be the CFO and other leaders. Researchers have shown that a generative-AI model can produce a full phishing campaign—from email text to a cloned login page—in less than 20 seconds.

Dark-web tools such as WormGPT and FraudGPT have stripped away ethical safeguards from commercial AI

models, making them purpose-built for malicious use. Even if only a small fraction of total phishing emails are currently identifiable as AI-generated, the trend is accelerating. Since the public release of ChatGPT, global phishing volume has surged more than 4,000 percent—a clear signal that AI is scaling attacker capabilities faster than most defenses can adapt.

• QR-Code Phishing (Quishing)

The rapid adoption of QR codes in legitimate workflows has opened a new attack vector known as quishing. By embedding malicious QR codes in email messages or PDF attachments, attackers bypass URL scanners and traditional filters that inspect links.

Quishing succeeds because it exploits habit and convenience. Users frequently scan QR codes on personal smartphones—devices that may lack corporate protection—even when the message originated on a secure work system. Unlike traditional URLs that can be visually inspected before clicking, QR codes are not human-readable, making it impossible for users to verify the destination before scanning. Common lures include fake MFA verification requests, package-delivery notifications, and fraudulent parking or payment systems.

Between 2021 and 2024, the share of phishing attacks using QR codes jumped from 0.8 percent to roughly 12 percent. Reported incidents continue to rise 25 percent year over year, with executives targeted dozens of times more frequently than average employees. Sectors such as finance, healthcare, education, and manufacturing have seen a disproportionate share of these attacks, reflecting the high value of their credentials and transaction data.

• MFA Bypass and Account Takeover

Multi-factor authentication remains a critical safeguard, but it is no longer impenetrable. In 2024, 83 percent of account-takeover incidents successfully bypassed MFA through one of several techniques.

Adversary-in-the-Middle (AiTM) attacks use phishing kits—such as Tycoon 2FA, EvilGinx, and Mamba 2FA—to proxy authentication between the user and legitimate service. When a victim enters credentials and approves MFA, the attacker captures session cookies and reuses them to log in directly. Early 2025 saw more than 3,000 accounts compromised across 900 Microsoft 365 tenants using Tycoon-based AiTM frameworks.

Other methods include MFA fatigue, where attackers repeatedly trigger push notifications until users approve one out of frustration; session hijacking, which exploits stolen browser tokens; SIM-swapping to intercept SMS codes; OAuth token theft through malicious app consent; and device-code phishing, which abuses legitimate login flows for non-browser devices.

SMS-based and single-tap push MFA remain particularly vulnerable. Organizations relying solely on these implementations face elevated exposure even while appearing compliant with authentication best practices.

• Compromised Accounts and Supply-Chain Intrusions

A growing portion of phishing now originates from legitimate—but compromised—accounts. Roughly 44 percent of phishing emails come from verified domains or known partners, and about 8 percent originate directly within the supply chain. Once a vendor or partner account is breached, malicious messages inherit existing trust relationships, bypassing authentication protocols such as SPF and DMARC.

These insider-style attacks are difficult to detect and devastating when successful. More than half of surveyed organizations in 2024 reported falling victim to phishing that appeared to come from trusted suppliers. Nearly 80 percent of account-takeover events began with credentials stolen via phishing. The takeaway is clear: effective email security must now account not only for inbound threats but also for the integrity of the broader ecosystem an organization communicates with.

Weaknesses and Vulnerabilities
Breaking Down the Gaps in Email Defense

Why Attackers Target Humans and Systems

Email-based attacks exploit the intersection of human behavior and system design. Attackers don't need to "break in" so much as convince, confuse, or overwhelm people into giving them access. At the same time, gaps in authentication, outdated infrastructure, and inconsistent processes create fertile ground for exploitation. Understanding both sides—human and technical—is critical to building lasting resilience.

Human Vulnerabilities

Modern phishing campaigns are as much psychological as they are technical. Attackers prey on instinctive cognitive biases that shape how people perceive urgency, authority, and trust.

- **Authority and hierarchy** are among the most easily manipulated dynamics. Messages that appear to come from executives, IT administrators, or government agencies trigger compliance reflexes, especially in organizations where hierarchical communication is strong.
- **Urgency and fear** accelerate mistakes. When an email warns that an account will be locked within 24 hours or a payment is overdue, logic often gives way to panic-driven action.
- **Social proof and brand familiarity** play equally powerful roles. People tend to trust messages that mimic recognizable companies or established vendors, particularly when combined with familiar visual cues.
- **Cognitive overload** compounds the risk. Busy professionals juggling dozens of emails daily are more likely to skim, click, and move on without verification.

Artificial intelligence has raised the stakes dramatically. For years, awareness training relied on red flags such as bad grammar or awkward phrasing. Those cues no longer exist. AI-generated phishing emails are linguistically perfect and visually polished, making even trained employees vulnerable.

Deepfake technology has further eroded trust. Humans are wired to believe what they see and hear, and attackers now exploit that instinct with synthetic audio or video impersonations. A convincing voice on the phone or face on a video call can override every other security safeguard. In many cases, the most sophisticated social engineering attacks today don't just fool the system; they fool the senses.

Technical Vulnerabilities

The technical side of email security has evolved unevenly, leaving persistent weaknesses that attackers know how to exploit.

Email System Gaps

Email authentication remains a cornerstone of trust, but only when implemented correctly. Domains lacking SPF, DKIM, or DMARC controls can be spoofed

with minimal effort, allowing attackers to send messages that appear to come from legitimate sources. Even where these controls are in place, configuration errors or permissive policies can render them ineffective. Recent studies show that more than 84 percent of phishing messages still bypass DMARC validation and secure email gateways.

QR codes add another layer of complexity. Because they're embedded as images, many email security tools fail to detect malicious URLs hidden within them. Additionally, QR codes are not human-readable—users cannot preview or verify the destination URL before scanning, removing a critical layer of user-based verification that exists with traditional hyperlinks. This creates a blind spot that attackers increasingly exploit, particularly in hybrid work environments where employees use personal smartphones to scan work-related QR codes.

Legacy systems also contribute to exposure. Older platforms such as Active Directory Federation Services (ADFS) lack the adaptive, risk-based authentication that modern environments require. When combined with inconsistent patching and poor visibility across hybrid infrastructure, these systems give attackers multiple points of entry.

Attackers also exploit the inherent trust and technical infrastructure of major email providers such as Gmail and Microsoft. Phishing messages sent from these platforms benefit from the providers' strong domain reputation, making them more likely to pass authentication checks and reach inboxes. Additionally, these providers use large, distributed IP address pools and route traffic through data centers worldwide, which can bypass traditional geographic blocking rules and IP-based reputation filters. Security teams cannot simply block entire IP ranges without disrupting legitimate communication, creating a persistent detection gap that attackers routinely exploit.

Software and Device Vulnerabilities

Email remains the delivery mechanism of choice for exploiting unpatched software. Roughly one-third of ransomware incidents originate from vulnerabilities that had already been disclosed but not yet remediated. Common targets include PDF readers, office applications, browsers, and mobile operating systems—any tool capable of opening attachments or following links.

Mobile devices pose a particularly stubborn challenge. As employees increasingly rely on personal phones for two-factor authentication or quick QR scans, attackers take advantage of devices that fall outside corporate monitoring. Without mobile endpoint protection, a single compromised device can undermine an entire organization's defenses.

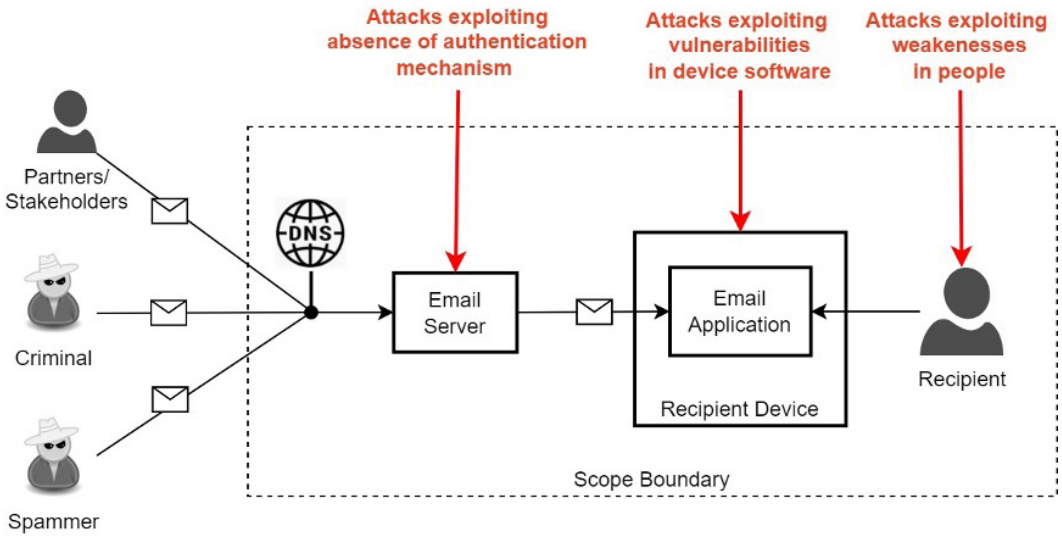
Authentication and Session Weaknesses

Authentication controls are only as strong as their weakest factor. SMS-based MFA remains highly susceptible to SIM-swapping attacks, while push-notification MFA is easily defeated by fatigue techniques—flooding users with approval requests until one is accepted out of frustration. Even advanced MFA implementations can be bypassed through session hijacking or stolen browser cookies, which allow attackers to maintain access without reauthentication.

OAuth and app-permission abuse have also become major risk vectors. By tricking users into authorizing malicious applications, attackers gain persistent, legitimate-looking access to email accounts and data. Device-code phishing follows a similar pattern of exploiting trust in legitimate authentication workflows for non-browser devices.

Organizational and Process Gaps

Even the best technology falters without disciplined process. Across industries, the weakest points often come down to training, timing, and response.



Despite years of investment, many awareness programs are still rooted in outdated examples, such as focusing on misspelled emails instead of AI-generated impersonations or deepfakes. It's no surprise that 95 percent of cybersecurity professionals report ongoing anxiety about email threats.

Delayed updates further compound the issue. The average phishing breach now takes 277 days to identify and contain, during which time attackers may already have pivoted across systems or exfiltrated sensitive data.

Authentication policy is another common failure point. Many organizations continue to rely on SMS-based or push MFA, fully aware of their weaknesses, because stronger alternatives seem complex to deploy. And when breaches do occur, inadequate incident response procedures often leave compromised accounts active far longer than they should be.

Persistent Traditional Scams

Despite advances in security technology and awareness training, traditional social engineering scams continue to succeed. Gift card fraud, requests to change banking information via email, and invoice manipulation schemes still generate losses—often in smaller amounts per incident, but with significant cumulative impact. These attacks may lack technical sophistication, but they exploit authority, urgency, and trust with remarkable effectiveness.

The harm extends beyond immediate financial loss. When an employee falls victim to a gift card scam or processes a fraudulent banking change, it damages internal trust, creates doubt in established processes, and can strain relationships with vendors and partners. The psychological impact on victims—feelings of embarrassment, guilt, or inadequacy—further compounds organizational risk by discouraging timely reporting of incidents.

Addressing these weaknesses calls for cultural and procedural maturity. Regular risk reviews, phishing simulations modeled on AI-crafted messages, and rehearsed response playbooks can drastically shorten recovery windows and limit the damage of inevitable incidents.

Impacts
The Cost of Email Compromise

The Ripple Effect of a Breach

When an email-based attack succeeds, its effects ripple far beyond the inbox. The consequences reach individuals, institutions, and entire supply chains. For organizations that rely on constant communication—especially in healthcare, government, and critical infrastructure—the damage is often measured not only in financial losses, but in trust, time, and human wellbeing.

Injuries to Stakeholders

The most immediate victims of phishing and email compromise are often the people who rely on an organization's systems. Exposed personal or financial data can upend lives, erode confidence, and strain relationships between service providers and the communities they serve.

Privacy losses remain the most visible form of harm. Breached email systems often expose personal identifiers, patient records, or confidential correspondence, creating a chain of downstream risks including identity theft and fraud. **Financial losses** can follow quickly, whether through direct theft, fraudulent transfers, or costs associated with credit monitoring and remediation.

The psychological toll is harder to quantify but equally real. Victims of phishing and identity theft report persistent anxiety, guilt, and distrust in digital communication. In critical sectors such as healthcare or public safety, these emotional consequences are compounded by the potential for **physical harm**. A single compromised email account can disrupt hospital operations, delay treatment, or interrupt communications essential to emergency response.

41.9%

is the baseline phish-prone percentage for healthcare—the highest of any sector.

Healthcare, in particular, is one of the most vulnerable industries. With a baseline phish-prone percentage of 41.9 percent—the highest of any sector—hospitals and medical networks have become prime targets. In 2025, multiple U.S. healthcare systems suffered ransomware-related shutdowns traced back to phishing emails, halting patient care and forcing emergency diversions. For industries where uptime equals safety, an inbox click can translate directly into harm.

Impacts

Consequences to Organizations

Financial Impact

$4.88 million

is the average cost of a phishing-related breach in 2024, covering investigation, forensics, legal counsel, data recovery, and reputational repair.

$1.8 billion in losses

Business Email Compromise (BEC) alone accounted for this staggering total in losses, with fraudulent wire transfers typically ranging from **$39,000 to $129,000 per incident.**

$10 million

is average recovery cost per ransomware event in healthcare, driven by system rebuilds, regulatory penalties, and prolonged service disruption.

68%

increase in ransomware-related insurance claims in 2024, with the average covered loss nearing **$353,000.**

Operational Impact

Beyond direct expenses, email incidents disrupt the rhythm of business. Compromised accounts and widespread phishing campaigns trigger system shutdowns, quarantines, and manual review processes that paralyze productivity. In the aftermath of ransomware attacks, system rebuilds and data restoration can stretch into weeks, even with recent backups.

Loss of data is common, either through encryption that renders files unusable or public exposure of stolen information. These operational halts create hidden costs that ripple across teams, clients, and supply chains.

Reputational Impact

Trust, once lost, is difficult to rebuild. Customers, partners, and regulators all expect transparency and accountability after a breach, but disclosure often amplifies reputational damage. Clients who once saw an organization as dependable may look elsewhere, while investors and partners question governance and resilience.

The loss of goodwill can be long-lasting, particularly for organizations that handle sensitive or high-stakes information. Brand damage often outlasts the technical remediation phase by years.

Regulatory and Compliance Impact

Every breach carries regulatory implications. Under frameworks such as GDPR, fines for inadequate data protection can reach into the millions. In the United States, industries governed by HIPAA, PCI DSS, SOX, or federal contracting standards face mandatory reporting, audits, and potential legal action. Contractual penalties may also apply if a breach violates service-level agreements or data protection clauses.

For many organizations, compliance costs now exceed the expense of prevention. Regulatory oversight has shifted from reactive to proactive, placing the burden squarely on organizations to demonstrate not only that they've secured data, but that they can prove how.

Cascading Effects

Modern attacks rarely end with a single compromise. Once an attacker gains access, stolen credentials can be reused to target new victims or infiltrate other environments. This creates a domino effect across vendors, customers, and affiliates.

Compromised organizations often become unwilling participants in secondary attacks against their own networks—a phenomenon now common in complex supply chains. Multi-stage intrusions that begin with phishing frequently escalate into data theft, privilege abuse, and large-scale ransomware deployment. The persistence of stolen credentials means that exposure continues long after an initial incident has been "resolved."

Detecting and stopping these secondary attacks presents unique challenges. When malicious emails originate from hijacked legitimate accounts, technical controls alone cannot reliably distinguish between authentic and fraudulent messages. Users must perform additional assessment—evaluating context, tone, unusual requests, and timing—to determine whether an email from a "known and trusted" sender is legitimate. This places significant cognitive burden on recipients and increases the likelihood that sophisticated attacks will succeed, particularly during high-volume or high-stress periods.

A Broader Measure of Impact

The real measure of an email breach isn't just the dollars lost; it's the disruption to trust and continuity. A single successful phishing email can expose an entire network, halt critical operations, and damage reputations built over decades. For stakeholders, it can mean anxiety, financial uncertainty, or in the most sensitive sectors, physical risk.

For leadership, it underscores a simple truth: email security is not a technical issue alone. It's an organizational risk that spans people, process, and perception.

Summary of Key Email Security Risks

Email-Based Threats Table

ID	Email-Based Threat	Weaknesses / Vulnerabilities Exploited	Potential Impacts	Additional Information
T-1	Credential Phishing	Human susceptibility to social engineering; lack of domain authentication; weak or absent MFA; trust in brand impersonation.	Loss of privacy; financial theft; account takeover; reputational damage; operational disruption.	Phishing remains the leading initial attack vector. Spear-phishing and whaling target specific individuals or executives. In 2025, 22% of breaches involved stolen credentials as the initial access vector.
T-2	Malware Delivery via Phishing	Social engineering; absence of domain authentication; software vulnerabilities; unpatched systems.	Ransomware infection; data theft; downtime; privacy and financial loss; service disruption.	54% of ransomware infections begin with a phishing email. Ransomware accounted for 44% of confirmed breaches in 2024, with healthcare recovery costs averaging $10 million per incident.
T-3	Spam and Unsolicited Email	Weak or absent domain authentication; poor filtering configuration.	Productivity loss; bandwidth and storage consumption; potential gateway for phishing or malware.	Roughly 3.4 billion spam emails are sent daily. Spam campaigns are often precursors to credential theft or malware delivery.
T-4	AI-Powered Phishing	Overreliance on language or formatting cues; limited training on AI-generated content.	All impacts from T-1 and T-2; executive impersonation; large-scale fraud; detection challenges.	67.4% of phishing attacks in 2024 used AI. Attack volume grew 4,151% since late 2022. One firm lost $25 million to a deepfake video call impersonating executives. AI phishing is projected to reach 17 % of cyberattacks by 2027.
T-5	QR-Code Phishing (Quishing)	QR codes bypass content scanning; user trust in QR usage; multi-device exploitation; physical tampering.	Credential theft; financial loss; privacy breach; productivity loss.	Quishing rose from 0.8% (2021) to ≈12% (2024). Only 36% of victims recognize it. The UK recorded £3.5 million in losses (Apr 2024–Apr 2025). Executives are 42 × more likely to be targeted.
T-6	MFA Bypass and Account Takeover	Adversary-in-the-Middle kits; token theft; session hijacking; MFA fatigue; SIM swapping; OAuth exploitation.	Complete account compromise; lateral movement; persistent unauthorized access; data exfiltration; financial loss.	83% of account takeovers in 2024 bypassed MFA. The Tycoon 2FA framework compromised 3,000 accounts across 900 Microsoft 365 tenants with 50% success. 79% of account takeovers start with phishing.
T-7	Supply-Chain and Compromised-Account Phishing	Inbound trust in vendor or partner domains; inadequate anomaly detection; weak authentication oversight.	Data exposure; regulatory and reputational damage; secondary compromises across connected organizations.	44% of phishing emails originate from compromised legitimate accounts, 8% from vendor or partner domains. 51% of organizations were hit by supply-chain phishing in the past year. 84% of phishing attempts pass DMARC authentication, underscoring systemic trus

Recommended Email Safeguards

The table on the next page specifies the safeguards that are recommended to protect against email-based threats. These safeguards are designed to prevent, detect, and respond to attacks, reducing risk to levels that should be acceptable to most organizations.

Critical Note On

Email Authentication

Email authentication is now a basic requirement, not a best practice. As of early 2024 (Google / Yahoo) and 2025 (Microsoft), bulk senders must configure SPF, DKIM, and DMARC to avoid delivery failures. Without these records, legitimate messages may be rejected or quarantined. Beyond compliance, domain authentication supports trust across the wider email ecosystem—every organization that implements it helps reduce fraud for everyone else.

Implementation Priority

Each safeguard plays a specific role, but not all organizations will have the capacity to deploy every control immediately. Implementation should follow a risk-based sequence informed by assessment results. Leadership should review and accept any deferred items through formal governance to maintain accountability.

Deployment Considerations

Safeguards can be implemented through on-premise tools, managed services, or cloud platforms. The right approach depends on operational structure, regulatory environment, and in-house capability. What matters is consistent upkeep: controls that aren't reviewed or updated will eventually fail against evolving threats.

Alignment with Industry Frameworks

The safeguards outlined in this document align with established cybersecurity frameworks, including the MITRE ATT&CK® knowledge base. Email-based threats correspond primarily to MITRE Technique T1566 (Phishing) and its sub-techniques, which detail the various methods attackers use to deliver malicious content via email. Organizations already using MITRE ATT&CK for threat modeling and detection engineering can map these safeguards directly to their existing defensive strategies, enhancing integration with security operations and incident response workflows.

Email Safeguards Table

ID	Email Safeguard	Threats Mitigated	Notes
S-1	Email Domain Authentication	T-1, T-2, T3-, T-4, T-5, T-7	Enables servers to verify sender authenticity through SPF, DKIM, and DMARC records. Required by Google / Yahoo (Feb 2024) and Microsoft (May 2025). Only 33% of top domains have valid DMARC, and more than half use weak policies. Maintain spam rates below 0.3% to stay deliverable.
S-2	Email Server Configuration for DMARC	T-1, T-2, T3-, T-4, T-5, T-7	Implements DMARC policy enforcement on receiving mail servers. Start with p=none for monitoring, progress to p=quarantine and p=reject. Add rua/ruf reporting for visibility. Even with DMARC, 84% of phishing attempts still pass authentication—making this a baseline, not a standalone defense.
S-3	Spam Filtering	T-3	Filters unwanted or high-volume email before it reaches users. Use multi-layered filtering at the perimeter, mail server, and endpoint. Combine machine learning with domain reputation analysis and tune regularly to reduce false positives.
S-4	DNS Filtering and Threat Intelligence	T-1, T-2, T-3, T-4, T-5, T-7	Blocks communication with known malicious domains and IP addresses using real-time blacklists (RBLs) and threat intelligence feeds. Update lists frequently and integrate with endpoint and network defenses.
S-5	Endpoint Protection for Recipient Devices	T-2, T-4	Stops malware introduced through email attachments or links. Should include anti-malware, anti-exploit, and behavior-based detection. Extend protection to mobile devices used to scan QR codes. Patch management is critical—32% of ransomware starts from unpatched software.
S-6	Phishing-Resistant MFA	T-1, T-4, T-6, T-7	Protects accounts even when credentials are stolen. Replace SMS and push-based MFA with FIDO2 or WebAuthn hardware keys. Monitor for fatigue attacks, enforce session management, and apply context-based authentication. 83% of account takeovers bypass weak MFA.
S-7	Advanced Email Security Solutions	T-1, T-2, T-4, T-5, T-6, T-7	Goes beyond traditional SEGs, which 84% of phishing attacks now bypass. Use AI analysis, behavioral monitoring, URL sandboxing, QR-code scanning, and deepfake detection. Integrate with identity providers for contextual risk scoring and real-time alerts.

EMAIL SAFEGUARDS TABLE

ID	Email Safeguard	Threats Mitigated	Notes
S-8	Security Awareness and Training for Email Recipients	T-1 through T-7	Builds user recognition and response capability through realistic, current examples. Training should address AI-generated phishing, QR code fraud, deepfakes, MFA fatigue, and OAuth abuse. Run simulations, measure phish-prone rates, and deliver ongoing refreshers — not one-time sessions.
S-9	Account Takeover Detection and Response	T-1, T-6, T-7	Identifies compromised accounts by monitoring for unusual logins, session anomalies, or mass email activity. Automate session termination, credential rotation, and account isolation. Average breach containment takes 277 days — automation cuts that dramatically.
S-10	QR Code Security Controls	T-5	Detects and blocks malicious QR codes embedded in images and PDFs. Policies should define when users may scan codes and how to verify them. Educate users on previewing URLs, spotting tampered stickers, and reporting suspicious codes.
S-11	Periodic Backups and Recovery	T-2, T-4	Maintains isolated, tested backups to enable recovery after ransomware or destructive attacks. Store backups offline or immutable, test restores regularly, and retain multiple generations. Effective backups cut recovery costs significantly.
S-12	Incident Management and Response	All Threat Categories	Defines organization-wide procedures for phishing triage, compromised accounts, malware containment, and BEC investigation. Include communication protocols, tabletop exercises, and law-enforcement coordination. Document lessons learned and update continuously.
S-13	Secondary Verification and Multi-Person Approval Controls	T-1, T-4, T-6, T-7	Requires additional human verification steps for high-risk activities such as banking changes, wire transfers, or access provisioning. Policies should mandate out-of-band confirmation (e.g., phone verification using a known, verified number — not one provided in the email) before processing financial or access-related requests received via email. For particularly sensitive operations, implement segregation of duties requiring two authorized individuals to complete separate, dependent steps in the process. For example, Person A initiates a bank account change but cannot complete it; Person B must independently verify and approve the change using separate authentication. Neither person can complete the full transaction alone. These controls create organizational friction intentionally, recognizing that the inconvenience of verification is vastly preferable to the consequences of fraud. They also provide psychological protection for employees, who can explain that "policy requires me to verify this another way" when faced with suspicious requests from apparent authority figures.

Implementation & Prioritization

Security maturity is rarely achieved all at once. Every organization balances time, talent, and resources against a constantly expanding threat surface. What matters most is sequencing, meaning the order in which safeguards are deployed determines how quickly risk begins to decline. The right path starts with what keeps communication alive, protects identity, and builds human awareness, then expands outward to detection, recovery, and resilience.

Where to Begin

The first phase should always focus on the essentials that decide whether an organization can communicate and operate safely. Email authentication (S-1 and S-2) is now non-negotiable. It's what separates legitimate messages from impersonation, and in 2025, it literally determines whether a message is delivered. Without SPF, DKIM, and DMARC, business communication can disappear into spam folders or be rejected entirely.

Alongside that foundation comes identity protection. Phishing-resistant MFA (S-6) closes the gap left by weak factors like text messages and push notifications, which adversaries have learned to exploit through fatigue and SIM-swapping. Hardware-based or FIDO2 authentication neutralizes most of those tactics.

And finally, people. Security awareness and training (S-8) turn the last line of defense into an active one. When users can recognize a deepfake request, a fake login screen, or a QR code that doesn't belong, technology suddenly has backup. These three safeguards—authentication, MFA, and awareness—form the triage phase of modern email security.

Building the Second Layer

Once the core controls are in place, the next focus is visibility into what's happening inside the system instead of only defending at the edge. Advanced email security platforms (S-7) fill this role. They use AI to recognize behavioral anomalies and language patterns that legacy gateways miss. They're the analytical layer that spots when a trusted account starts acting untrustworthy.

Account takeover detection (S-9) and QR-code security controls (S-10) extend that same visibility. Together they monitor for compromised identities and the increasingly creative methods attackers use to bypass filters. Each one adds context and depth to the earlier safeguards, closing the loop between prevention and detection.

Resilience for the Long Term

The third phase shifts from stopping attacks to surviving them. Endpoint protection (S-5) ensures that even if a malicious attachment slips through, it can't detonate freely. Backups and recovery (S-11) provide the lifeline when ransomware or destructive attacks succeed despite best efforts. And incident management (S-12) defines how the organization responds under pressure—who leads, how information flows, and what's restored first. These safeguards don't stop every attack, but they determine whether an incident becomes a headline or a footnote.

The Work That Never Ends

Some elements of protection are ongoing by design. Spam and DNS filtering (S-3 and S-4) are part of the Internet's plumbing; they require constant tuning as attackers shift domains and infrastructure. More broadly, every safeguard needs maintenance. Threat actors evolve weekly. Configuration drift, unpatched systems, or expired certificates quietly reopen the doors you thought were closed. Security is a cycle of refinement.

Balancing Resources

For organizations with limited capacity, progress doesn't have to be perfect to be meaningful. Start with the controls that have immediate, measurable impact—S-1 and S-2 to keep communication deliverable, S-6 to protect identity, and S-8 to educate the human perimeter. Each one offers a disproportionate return on investment.

Where internal expertise stops, managed security service providers can extend it. Many modern email platforms already include baseline security capabilities that only need configuration and monitoring. What matters most is knowing what has been implemented, what hasn't, and which risks leadership has consciously accepted. That awareness is what turns resource limitation into managed risk.

Financial Realities for Non-Profit and Public Sector Organizations

For non-profit and public sector agencies, the financial pressure to implement comprehensive email security can be particularly acute. These organizations often operate with constrained IT budgets, limited technical staff, and competing priorities for scarce resources. Yet they handle sensitive personal information, manage public trust, and are increasingly targeted precisely because attackers perceive them as softer targets.

The cost of inaction, however, typically far exceeds the cost of prevention. A single successful ransomware attack can cost a public agency millions in recovery expenses, regulatory penalties, and lost productivity—funds that could otherwise support core mission activities. For non-profits, a breach can permanently damage donor confidence and community trust.

Many security safeguards—particularly email authentication (S-1, S-2), phishing-resistant MFA (S-6), and security awareness training (S-8)—can be implemented at relatively low cost, especially when leveraged through existing platforms or managed service providers. Grant funding, government cybersecurity assistance programs, and collaborative purchasing agreements can further reduce barriers to implementation. The key is recognizing that email security is not a luxury—it's a prerequisite for operational continuity and stakeholder protection.

Measuring Progress

Effectiveness in cybersecurity can't be assumed; it has to be measured. Metrics connect technical outcomes to business language. Authentication pass rates, DMARC enforcement percentages, and phishing-simulation results show whether controls are working. Response time and containment rates show whether teams can act quickly when something slips through. Over time, these indicators tell a story: fewer successful phishing attempts, faster detection, fewer compromised accounts, and smaller financial losses.

Measurement also reinforces accountability. When executives can see tangible results—such as a drop in phish-prone percentage or a reduction in MFA bypass attempts—security becomes less abstract and more operationally real.

Continuous Evolution

No safeguard remains effective forever. New exploits, new toolkits, and new regulations arrive faster than annual reviews can keep pace. Organizations that stay resilient build iteration into their culture. They review configurations quarterly, refresh training content to reflect current tactics, and participate in peer information-sharing communities. Penetration tests and phishing simulations aren't box-checking exercises. They're living diagnostics of how threats actually behave against your defenses.

The more an organization treats improvement as part of its routine, the less likely it is to be caught off guard when the next evolution of email threats emerges.

From Compliance to Confidence

Every safeguard outlined in this paper shares a single goal: restoring trust in the channel that drives modern business. Email has become both indispensable and dangerous, and the line between the two is defined by how seriously each organization treats its responsibility to secure it.

The fundamentals are clear. Authentication keeps legitimate communication intact. Phishing-resistant MFA protects identity at its core. Advanced analysis detects what filters miss. Awareness keeps people alert when technology falters. Detection, response, and recovery complete the loop. Together, these safeguards transform email from a persistent vulnerability into a managed risk.

The challenge is no longer awareness—it's action. Regulations and provider mandates have already shifted the baseline; compliance now determines whether messages even reach their destination. What separates the resilient from the reactive is execution: configuring what's required, testing what's deployed, and reviewing what's learned.

Each control improves the next. Each lesson strengthens the system. The organizations that adapt fastest—updating policies, retraining teams, refining configurations—are the ones that stay ahead of threats that no longer wait for manual response.

Email security is not just a technical discipline; it's an operational promise to customers, partners, and communities. Implement it thoughtfully, maintain it continuously, and treat it as an essential function of trust.

About FSET

FSET is a modern, security-first Managed Services Provider delivering forward-thinking solutions to organizations across the public and private sectors since 1999.

Our ISO 27001:2022 certification reflects our commitment to security—Secure by Design, Secure by Default. Whether serving highly regulated industries or organizations that simply value the protection of their information assets, we ensure enterprise-grade security practices are standard, not optional, for every client we serve.

As an IAPP member organization, we bring the same discipline to privacy—Privacy by Principle. FSET delivers the expertise to protect your organization today and into the future.

Learn more at fset.inc.

Assess Your Email Security Posture

FSET offers email domain security assessments to identify gaps in your SPF, DKIM, and DMARC configurations and provide a roadmap to full enforcement. Contact info@fset.ca or call (833) 321-3738 to schedule a consultation.

FSET Inc.

Address: 201-610 Lakeview Drive
Kenora, ON P9N 3P7

Phone: (833) 468-0174

Email: info@fset.ca

References

[1] Verizon, “2025 Data Breach Investigations Report (DBIR),” 2025. Online. Available: verizon.com/business/resources/reports/dbir/ (Accessed: Oct 25, 2025).

[2] IBM Security, “Cost of a Data Breach Report 2024,” 2024. Online. Available: ibm.com/reports/data-breach (Accessed: Oct 25, 2025).

[3] APWG, “Phishing Activity Trends Reports, 2024–2025,” 2024–2025. Online. Available: apwg.org/trends-reports (Accessed: Oct 25, 2025).

[4] FBI Internet Crime Complaint Center (IC3), “2024 Internet Crime Report,” 2024. Online. Available: ic3.gov (Accessed: Oct 25, 2025).

[5] CISA, “Phishing Guidance and Resources,” 2023. Online. Available: cisa.gov (Accessed: Oct 25, 2025).

[6] Canadian Centre for Cyber Security (CCCS), “Implementation Guidance: Email Domain Protection (ITSP.40.065),” 2023. Online. Available: cyber.gc.ca/.../ITSP40065_0.pdf (Accessed: Oct 25, 2025).

[7] Google, “Email Sender Guidelines,” Feb. 2024. Online. Available: support.google.com/a/answer/81126 (Accessed: Oct 25, 2025).

[8] Microsoft, “Email Authentication Requirements for Microsoft Consumer Email,” May 2025. Online. Available: (official Microsoft page URL) (Accessed: Oct 25, 2025).

[9] Sophos, “State of Ransomware 2024,” 2024. Online. Available: (official Sophos report URL) (Accessed: Oct 25, 2025).

[10] Proofpoint, “Tycoon 2FA: Phishing Kit Being Used to Bypass MFA,” Dec. 2024. Online. Available: proofpoint.com/.../tycoon-2fa-phishing-kit-mfa-bypass (Accessed: Oct 25, 2025).

[11] Abnormal Security, “MFA Bypass: How & Why It Works,” June 2025. Online. Available: abnormal.ai/glossary/mfa-bypass (Accessed: Oct 25, 2025).

[12] Egress, “Phishing Threat Trends Report (Apr 2024; Oct 2024),” 2024. Online. Available: egress.com/phishing-threat-trends-report (Accessed: Oct 25, 2025).

[13] Hoxhunt, “2025 Phishing Trends Report,” 2025. Online. Available: hoxhunt.com/guide/phishing-trends-report (Accessed: Oct 25, 2025).

[14] Action Fraud (UK), “Quishing Alert,” Apr. 2025. Online. Available: actionfraud.police.uk/news/qr-codes (Accessed: Oct 25, 2025).

References

[15] Barracuda, “The Evolving Use of QR Codes in Phishing Attacks,” Oct. 2024. Online. Available: blog.barracuda.com/ (Accessed: Oct 25, 2025).

[16] Darktrace, “AiTM Phishing Kits Abusing Legitimate Services,” Apr. 2025. Online. Available: darktrace.com/blog/ (Accessed: Oct 25, 2025).

[17] Fortinet, “Ransomware Statistics 2025,” 2025. Online. Available: fortinet.com/resources/cyberglossary/ransomware-statistics (Accessed: Oct 25, 2025).

[18] RCMP, “Business Email Compromise (BEC),” n.d. Online. Available: rcmp-grc.gc.ca/en/business-email-compromise-bec (Accessed: Oct 25, 2025).

[19] CybelAngel, “The Rise of AI-Powered Phishing 2025,” Feb. 2025. Online. Available: cybelangel.com/blog/rise-ai-phishing/ (Accessed: Oct 25, 2025).

[20] Keepnet Labs, “QR Code Phishing Statistics and Trends,” Sept. 2025. Online. Available: keepnetlabs.com/blog/qr-code-phishing-trends... (Accessed: Oct 25, 2025).

[21] MITRE Corporation, “ATT&CK Framework,” 2025. Online. Available: attack.mitre.org (Accessed: Dec 3, 2025).

[22] MITRE Corporation, “Phishing, Technique T1566 - Enterprise | MITRE ATT&CK,” 2025. Online. Available: attack.mitre.org/techniques/T1566 (Accessed: Dec 3, 2025).

Innovation Empowering People.

Developed by:
FSET Inc.