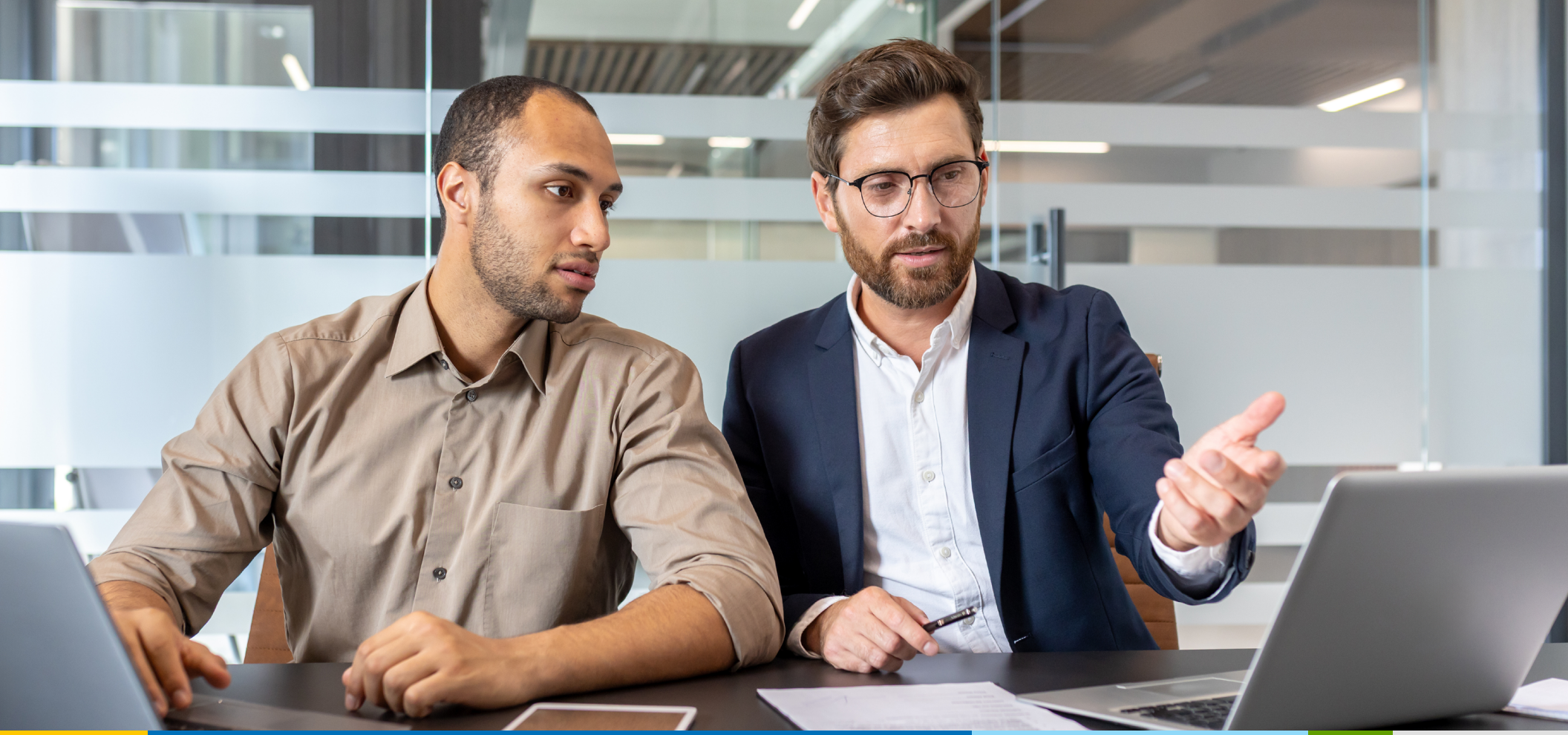


Bottomline®

Phishing in Commercial Banking: **A Systemic Threat to Trust**

bottomline.com

A Critical Inflection Point

Commercial banks stand at the center of global economic activity, trusted to move trillions of dollars securely and efficiently. That trust is under siege. Phishing has emerged as the most prevalent—and fastest-evolving—form of financial cybercrime. It is no longer limited to amateur email scams; today's attacks are driven by coordinated groups using AI-powered tactics, social engineering, and sophisticated impersonation schemes.

What was once viewed as a nuisance has become a systemic risk. Phishing campaigns now target both internal staff and external clients, with entry points ranging from email and SMS to QR codes and deepfake calls. Each breach represents not only a potential financial loss but a direct challenge to a bank's operational continuity, regulatory posture, and reputation in the marketplace.

As phishing tactics become more targeted and harder to detect, commercial banks must reframe the conversation. This threat is not a problem that technology alone can solve. It requires an enterprise-wide strategy that integrates behavioral awareness, adaptive technology, regulatory intelligence, and cross-industry coordination.

The Data Behind the Danger: **Phishing by the Numbers**

Every day, over 3.4 billion phishing emails circulate globally, comprising 1.2% of all email traffic. These messages serve as the launchpad for an estimated 91% of all cyberattacks, with phishing contributing to 36% of cybersecurity breaches across industries. [1]

The rise of artificial intelligence has further escalated the threat. AI-powered, multi-channel phishing campaigns are proving 42% more successful than traditional email-only scams. While AI-generated phishing messages accounted for just 0.7% to 4.7% of attacks in 2024, projections indicate that generative AI will be involved in 17% of cyberattacks by 2027. [2]

Suspicious Activity Reports (SARs), which serve as a critical early warning system for financial institutions, further highlight the scale of the crisis in the banking sector. Consider these three fraud areas that often incorporate phishing tactics:

- **Account takeover SARs soared to approximately 178,000 in 2024—a 65% increase since 2022.** [3]
- **Wire fraud SARs escalated by over 40% in the past two years, reaching 188,000 in 2024.** [4]
- **Identity fraud SARs rose by 44% during a two-year timeframe, with 108,000 reports in 2024.** [5]

The message is clear: **The scale, sophistication, and persistence of phishing threats demand heightened vigilance and proactive countermeasures from commercial banks.**

94% of organizations were victims of phishing attacks and 96% of those were negatively impacted [6]

[1] Gary Smith, "Top Phishing Statistics for 2025: Latest Figures and Trends." StationX, 2025.

[2] Denys Spys and Anna Solovei, "Phishing Attack Statistics 2025: Reasons to Lose Sleep Over." TechMagic, 2025.

[3] Frank on Fraud. "New SAR Data: ATO, Identity Theft and Wire Fraud Are Up Big," 2025.

[4] Ibid.

[5] Ibid.

[6] "Must-know phishing statistics for 2024." Egress, 2024.

A Many-Headed Hydra: **The Proliferation of Modern Phishing Threats**

Phishing has matured into a sophisticated and relentless threat. No longer confined to poorly written email scams, modern phishing campaigns are multi-vector, personalized, and technologically advanced—placing commercial banks directly in the crosshairs. Here are the most common and emerging types of phishing, grouped by channel.

Email-Based Phishing

Email Phishing

The most common form of phishing, where attackers send fraudulent emails pretending to be from legitimate sources, often with malicious links or attachments.

Business Email Compromise (BEC)

Attackers impersonate executives, colleagues, or vendors using compromised or spoofed email accounts to manipulate employees into wiring funds or sharing confidential information.

Spear Phishing

A more targeted version of email phishing that uses personal details to tailor messages to a specific individual or organization, increasing the likelihood of success.

Whaling

Spear phishing aimed specifically at high-level executives (like CEOs or CFOs), often crafted to trick them into authorizing payments or disclosing sensitive data.

Clone Phishing

A legitimate email is copied, altered with a malicious link or attachment, and resent to the original recipients to trick them into taking harmful action.

Text Message & Messaging App-Based Phishing

SMS Phishing (Smishing)

Fraudulent messages sent via SMS or messaging apps that include harmful links or urgent calls to action, such as verifying an account or claiming a prize.

Angler Phishing

Occurs on social media platforms, where attackers pose as customer support agents or trusted contacts to steal login credentials or redirect victims to phishing sites.

Phone Call-Based Phishing

Voice Phishing (Vishing)

Attackers call victims and pretend to be from banks, government agencies, or tech support to extract personal or financial information.

Deepfake Phishing

AI-generated voices are used in real-time calls to convincingly impersonate executives or colleagues, making fraudulent requests sound authentic.

Web & Network-Based Phishing

Pharming

A technique where users are redirected to fake websites, even after typing the correct web address, typically through compromised DNS settings or malware.

Search Engine Phishing

Fake websites are optimized to appear in search results for common services (e.g., banking or tech support), tricking users into visiting and entering sensitive data.

Man-in-the-Middle (MitM) Phishing

Attackers intercept communication between a user and a legitimate service (often over unsecured Wi-Fi) to steal data or alter transactions.

QR Code Phishing (Quishing)

Malicious QR codes are placed in emails, ads, or physical locations, leading users to phishing sites or prompting unintended app downloads.

Evil Twin Phishing

Attackers create fake Wi-Fi hotspots that mimic legitimate networks. When users connect, their data is intercepted or stolen.

AI-Enhanced Phishing: **A New Era of Precision Attacks**

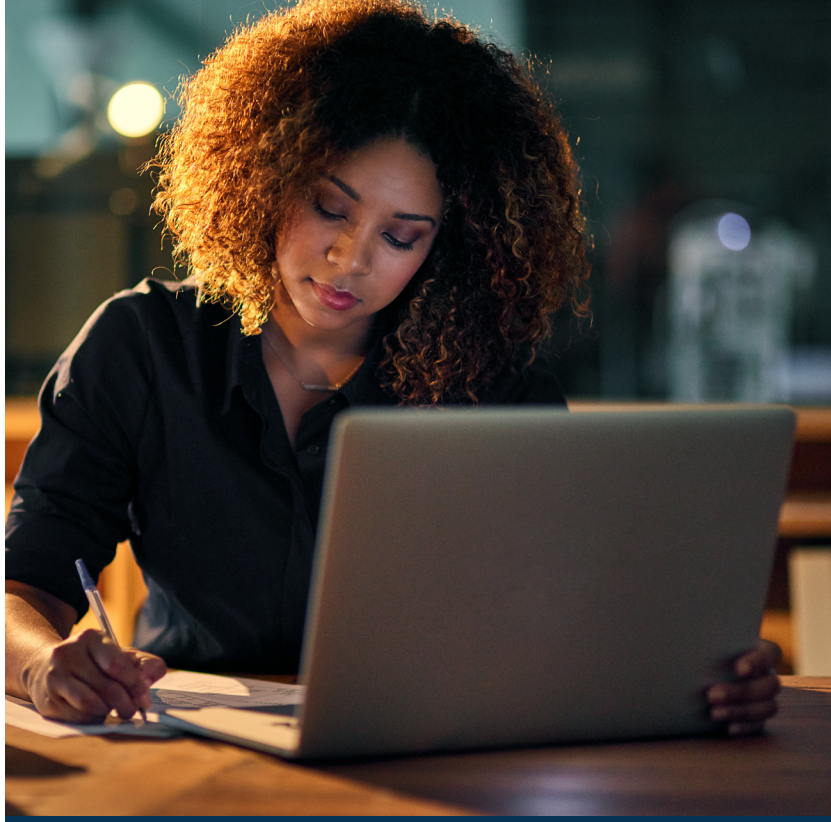
Artificial intelligence has transformed the phishing landscape. Commercial banks must now contend with adversaries who possess the same tools that legitimate institutions use to improve personalization, automate processes, and analyze behavior—only these tools are being turned against them.

Attackers increasingly rely on AI to create hyper-personalized phishing emails that mimic the language, tone, and timing of legitimate internal communications. Language models can analyze prior interactions and individual roles to tailor messages that are contextually accurate and psychologically persuasive. Voice cloning and deepfake technologies allow fraudsters to place seemingly-authentic calls to staff or clients.

AI also accelerates scam site generation and churn. Phishing domains are now produced, deployed, and retired in rapid succession, often with automated styling and content scraped from real financial institutions. This makes detection and takedown efforts far more challenging.

Moreover, AI is being used to defeat defensive technologies. Behavioral analytics and biometric-based authentication methods that once added strong layers of protection can now be manipulated. Attackers employ AI to simulate typing patterns, mouse movements, or even mimic facial expressions to bypass liveness detection and fraud scoring systems.

To defend against this evolving threat, banks must re-evaluate their anti-phishing strategies in light of adversaries who are no longer operating manually but at incredible speed and scale. AI is no longer just a competitive advantage in business: it is a critical tool in cybersecurity.



Phishing attacks powered by AI are faster, smarter, and harder to detect. Every successful impersonation is a signal to adapt, not just react.

Damage Alert: **The High Cost of Phishing in Commercial Banking**

Phishing attacks are exacting a steep toll on commercial banks. What may begin as a single fraudulent email can quickly escalate into a full-scale operational crisis. The damage ripples outward quickly:

Financial losses from compromised accounts and fraudulent transactions can reach millions per incident, especially when attackers exploit internal workflows or impersonate executives to authorize wire transfers.

Operational disruption is often immediate and widespread. Investigations, system isolation, and recovery efforts divert teams from day-to-day responsibilities, delaying critical banking functions and customer service delivery.

Reputational damage can be long-lasting. Commercial clients rely on their banks for security and stability; a phishing breach undermines that trust and may prompt clients to reevaluate their banking relationships.

Increased regulatory scrutiny is a near certainty after a phishing-related breach. Institutions may face audits, mandated corrective actions, or fines—especially if oversight or preventative controls are found lacking.

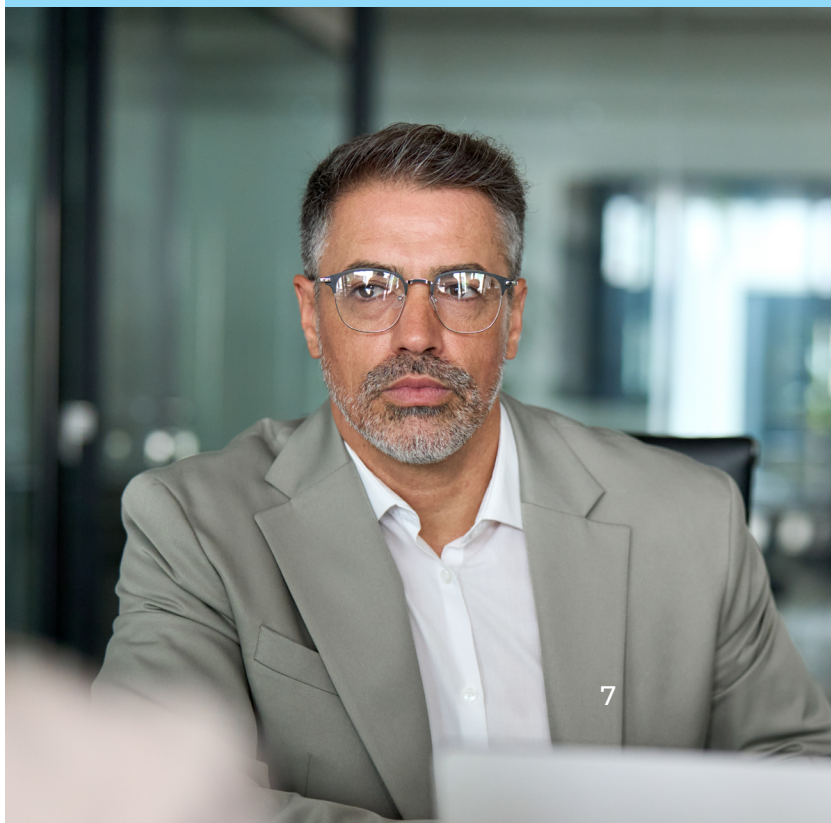
Slower onboarding and transaction processing occur as banks implement tighter security protocols in response to phishing threats. While necessary, these changes can frustrate clients and introduce friction into the customer experience.

Rising cyber insurance premiums often follow a breach. Insurers may raise rates, reduce coverage, or impose stricter conditions, reflecting the heightened risk profile of the affected bank.

The breadth and depth of these impacts make one thing clear: phishing results in a systemic disruption. To protect financial integrity, client relationships, and operational continuity, commercial banks must implement coordinated, enterprise-wide defenses.

$4.88M
average cost per phishing breach [7]

[7] IBM Cost of a Data Breach Report 2024.



Strategic Imperatives: **Technology, Education, and Collaboration**

The escalating scale and complexity of phishing require commercial banks to move from a reactive posture to one of strategic resilience. This transformation encompasses people, processes, and technologies—each playing a critical role in reducing exposure and accelerating detection.

Robust email protection is foundational.

Banks must implement authentication protocols such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM) to validate sender domains and block impersonation. Inconsistent adoption leaves institutions vulnerable compared to their better-secured peers.

Customer authentication needs to move beyond outdated methods.

While multi-factor authentication (MFA) is a standard control, phishing kits now routinely bypass one-time passwords (OTPs) via man-in-the-middle proxies. Banks should invest in phishing-resistant protocols such as WebAuthn and incorporate dynamic, context-aware detection layers.

Artificial intelligence must be enlisted defensively.

Advanced systems can analyze behavioral deviations, identify spear phishing markers, and detect unusual network origins in real time. Integrating threat intelligence feeds from peer institutions and law enforcement can increase visibility and accelerate coordinated responses.

Education remains a vital pillar.

Commercial customers must be trained to recognize new threats, including quishing, smishing, and vishing. Regular reinforcement of communication protocols—such as never requesting login credentials by email—builds vigilance and supports faster incident reporting.

Public-private partnerships and cross-bank collaboration must deepen.

Shared fraud data platforms can illuminate coordinated campaigns and enable faster defense across the industry. Collective readiness is now a strategic advantage in the phishing fight.

Strategic Imperatives: **Governance, Controls, and Oversight**

Resilience against phishing extends beyond technical defenses. Governance, oversight, and vendor risk management are equally essential to ensure that countermeasures are aligned with ever-expanding threats.

Banks must track emerging techniques.

Evolving attack vectors—particularly those involving artificial intelligence, such as deepfakes and voice cloning—increase the believability and effectiveness of phishing campaigns. Governance frameworks should be regularly updated to account for these advances and codify requirements for internal security, third-party oversight, and client protection.

Board-level engagement is increasingly necessary.

Executive leadership must understand the reputational and financial risks posed by phishing and direct resources toward mitigation strategies. Phishing resilience should be integrated into broader risk governance, including assessments of fraud risk tolerance, incident response maturity, and regulatory compliance posture.

Vendor ecosystems represent a growing attack surface.

Commercial banks must rigorously evaluate third-party providers—especially those handling transactions, communications, or authentication mechanisms. Regular audits and security reviews help ensure that vendor vulnerabilities do not become institutional weaknesses.

Operational readiness demands continuous investment.

Phishing defense cannot be a static program; it must adapt in real time as attacker tactics shift. Banks should assess their incident detection-to-response timelines and establish contingency plans for high-impact breaches. Simulated phishing drills, red teaming, and tabletop exercises further reinforce institutional muscle memory.

Regulatory expectations are shifting.

Agencies increasingly scrutinize how banks detect and report phishing-related fraud. Strengthening SAR-related analytics and demonstrating real-time monitoring capabilities can not only improve compliance but also offer earlier warning of large-scale fraud campaigns.

Securing Trust in an Age of Intelligent Threats

Phishing is a full-scale assault on the trust that underpins commercial banking. As attacks grow more sophisticated—due in large part to AI—the risks extend beyond financial loss to include regulatory exposure, operational disruption, and reputational damage. This is a systemic threat, and it requires a systemic response.

Defending against modern phishing schemes demands more than a checklist of controls. It calls for strategic integration across people, processes, and technology. Advanced email authentication must be reinforced with real-time behavioral analytics. Employee training must go hand-in-hand with client education. Strong governance should inform every aspect of fraud response, from vendor oversight to board-level risk planning. And collaboration—both within the industry and across public-private partnerships—must become a core competency.

At its heart, phishing is not just a cybersecurity problem. It is a business resilience imperative. Banks that recognize this will be better prepared to safeguard not only their digital assets, but also their relationships, reputations, and long-term competitiveness.

The stakes are not hypothetical. The adversaries are both determined and dangerous—and they are moving fast.

Bottomline®

About Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 35 years of experience, moving more than $16 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $179 billion in assets under management.

For more information, visit **www.bottomline.com**

REV US092925KG

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
info@bottomline.com

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
emea-info@bottomline.com