Phishing and social engineering are a major problem in Cybersecurity and the most costly forms of cybercrime for both businesses and consumers. Phishing attacks are continuously increasing, and the techniques used for the attacks are getting more sophisticated. In 2025, AI-generated phishing attacks are in the lead with 82.6% of phishing emails use AI (Zscaler,2025). Over 3.4 billion phishing emails are sent daily with an average cost of $4.88 millions of data breach. (Martin, 2025). Phishing channels are expanding rapidly as well, with more than 40% of the attacks include vishing and smishing. (Martin, 2025).

“Employees are four to eight times more likely to fall for phishing attacks on smartphones due to distraction and less focused attention.” (Zscaler,2025). This includes phishing through email applications. KnowBe4’s 2025 Phishing by industry benchmark report analyzed data from 14.5 million users across 62,400 organizations and 67.7 million simulated phishing tests. The report showed that top 3 industries at risk were healthcare, insurance and retail. It showed that 90 days of training can reduce phishing risk by over 40%. (knowbe4, 2025).

Attackers combine traditional psychological manipulation with modern tools (AI, deepfakes, QR codes, and automated platforms) to scale and tailor scams. Financial/payment brands continue to be heavily targeted (APWG: ~30% of attacks focused on payments/financial services in early 2025). BEC focuses on wire-transfer-capable targets, finance teams, payroll, and procurement. (APWG, 2025).

Types of Phishing and Social Engineering Techniques:

1- Email phishing:  
Mass emails that impersonate familiar brands (banks, payment services, SaaS providers) to steal credentials or deliver malware, it could be:

-Clone phishing: an attacker sends a slightly altered copy of a legitimate message (same sender/subject) with malicious links or attachments.

-Spoofing: forging the visible sender address to appear as a trusted source.

2- Spear phishing and whaling:  
Targeted messages researched to appear highly credible to a specific individual or role (e.g., finance staff, executives). Whaling is spear phishing aimed at senior executives with the goal of large transfers or sensitive data.

3- Business Email Compromise (BEC) / CEO fraud:  
Attackers impersonate executives, vendors, or partners to request wire transfers, change payment details, or authorize invoices. These are high-value attacks that typically avoid malware and rely on social engineering and misdirected trust.

4- Smishing and vishing:

-Smishing: phishing via SMS (text messages), often contains malicious links, QR codes, or prompts to call a number.

-Vishing: voice calls where attackers pose as support, finance, or authority figures to extract credentials or payments.

5- QR-code phishing:  
Phishing that relies on QR codes in emails, posters, or SMS. Scanning redirects victims to credential-harvesting pages or malware downloads.

6- Social media and messaging attacks  
Phishing via social platforms (DMs, posts) that harvest login details or deliver malicious links. Attackers use platform features and trust networks to increase credibility and trust.

7- Pretexting and impersonation:  
An attacker invents a scenario (IT support, auditor, vendor rep) to coax information or access. May combine with in-person methods like tailgating (physical entry) or a phone call.

8- Baiting, quid pro quo, and watering-hole:

-Baiting: attackers leave physical media (USB) or tempting offers online that result in compromise.

-Quid pro quo: attacker offers help or a service in exchange for credentials or access.

-Watering-hole: compromising websites frequented by a target organization to infect visitors.

9- AI-enhanced and deepfake attacks:  
Generative AI creates natural-sounding emails, voice deepfakes, or personalized content at scale—improving believability and click-through success.

Attackers use generative models to produce convincing emails, voice messages, and social posts, enabling mass personalized attacks with higher success rates. Reports in 2025 show AI-enhanced campaigns can be multiple times more effective than human-only crafted phishing.

Recommended mitigations (for both businesses and consumers):

Technical controls:

* Multi-factor authentication (MFA): Enforce MFA for all remote access and email accounts (blocks the majority of credential-based takeovers).
* Email security stack: Use combined protections—sender policy framework (SPF), DKIM, DMARC, advanced threat protection (sandboxing, URL rewriting), and anti-phishing filters that perform reputation and content analysis. (PC Gamer, 2025)
* Endpoint detection & response: Monitor for suspicious link clicks, abnormal sign-ins, and lateral movement.
* Limit wire-transfer workflows: Implement multi-person approvals, out-of-band verification (phone calls to known numbers), and vendor invoice verification processes.

People:

* Targeted awareness & phishing simulations: Regular, role-specific training and realistic phishing simulations (include SMS and voice scenarios).
* Playbooks & incident response: Have clear BEC/wire fraud playbooks and rapid reporting channels (finance freeze, bank contact steps).
* Least privilege and segmentation: Reduce the blast radius of credential compromise by limiting admin rights and segmenting networks.

Consumer guidance:

* Verify unexpected payment requests by phone (use numbers from official sites, not message replies).
* Treat QR codes and SMS links with caution, inspect destination URLs and use mobile device security settings.
* Report suspicious messages to providers and law enforcement.

References:

* Fox, J. (2025, October 17). *People are falling for AI phishing attempts 4.5× more often than human ones—but the solutions are the same as ever.* PC Gamer.
* Anti-Phishing Working Group. (2025, July 2). *Phishing activity trends report, 1st quarter 2025*
* Desai, D., Hegde, R., & Shtil, D. (2025, April 24). *Beyond the inbox: ThreatLabz 2025 Phishing Report reveals how phishing is evolving in the age of GenAI*. Zscaler.
* Tech-Adv. (n.d.). *AI cyber attack statistics*. Tech-Adv.
* KnowBe4. (2025). *2025 Phishing By Industry Benchmarking Report*
* World Economic Forum. (2025, January). *Global Cybersecurity Outlook 2025*