



CLIENT ALERT

Social Engineering Threats Escalate in the Age of AI

Human Trust Has Become the New Attack Surface

Social engineering attacks are escalating rapidly in frequency, severity, and sophistication. What was once considered a peripheral cyber threat has become the primary entry point for many modern cyber incidents. Fueled by the rapid advancement and weaponization of Generative AI and Agentic AI, cybercriminals now leverage voice cloning, deepfakes, and highly personalized impersonation tactics to deceive employees with unprecedented realism.

As organizations have strengthened their technical cybersecurity defenses, threat actors have adapted. Rather than attempting to penetrate increasingly secure networks, attackers are focusing on exploiting human trust. Traditional perimeter defenses and basic security awareness programs are no longer sufficient to address today's evolving threat landscape.

For years, cybersecurity experts warned that employees were the "weakest link" in security. Today, employees are not merely a vulnerability; they have become the primary target.

Practical Steps Organizations Should Consider

1. Evolve Security Awareness Programs

Organizations should reassess traditional cybersecurity training approaches and consider adopting a broader Human Risk Management (HRM) or Security Behavior Management framework. Effective programs focus not only on recognizing threats, but also on understanding and influencing decision-making behaviors that attackers seek to exploit.

2. Train Employees for Deepfake-Driven Attacks

Deepfake-enabled fraud continues to grow in sophistication. Awareness training should emphasize behavioral judgment and robust verification processes rather than relying solely on employees' ability to identify manipulated audio or video content.

High-pressure requests that appear to originate from executives, regulators, clients, or trusted business partners can significantly impair judgment and increase the likelihood of successful attacks. Organizations should also train employees to be mindful of requests coming from seemingly trusted internal operational contacts, such as other employees or the IT help desk, as attackers may impersonate internal personnel to exploit their familiarity and trust. Whether urgent or routine in nature, requests involving sensitive information, system access, or financial transactions should be verified through established channels.

3. Strengthen Verification Protocols

Organizations should consider implementing enhanced verification procedures for sensitive requests, including:

- Rotating authentication code words or challenge-response protocols
- Independent call-backs using pre-established contact information
- Multi-person approval requirements for high-risk transactions
- Defined escalation procedures for unusual or urgent requests

The goal is to create friction in situations where attackers rely on urgency and authority to override normal controls.

4. Reassess Hiring and Onboarding Processes

HR and IT departments should review onboarding procedures to address emerging social engineering risks, including:

- Live identity verification during the interviewing and hiring process
- Sandboxed screening of resumes and applicant materials
- Out-of-band delivery of credentials and access instructions
- Enhanced validation of remote employees and contractors

As threat actors increasingly target recruitment and onboarding processes, these controls can help reduce organizational exposure.

Review Risk Transfer Strategies

Organizations should also evaluate how social engineering risks are addressed within their broader risk management and risk transfer programs.

Insurance and Contractual Protections

Review insurance policies and contractual risk allocation provisions holistically. Social engineering losses may trigger multiple coverage forms, and the interaction between cyber, crime, professional liability, and other policies can have a significant impact on recovery outcomes.

Because social engineering incidents continue to evolve, policy language may not always align perfectly with emerging loss scenarios. Organizations should be prepared to advocate for coverage based on the specific facts and circumstances of a claim.

Prepare for Incident Response Before an Event Occurs

A well-defined response plan can materially improve recovery outcomes following a fraudulent transfer or funds diversion event.

Organizations should consider pre-identifying legal counsel and recovery specialists capable of initiating a financial institution "kill chain" process and coordinating a 24/7 response. In many cases involving wire transfers or ACH fraud, recovery prospects are significantly improved when action is taken within the first 48 hours.

In addition, organizations should notify their cyber and other potentially responsive insurers as quickly as possible following an incident to maximize recovery opportunities and preserve coverage rights.

Key Takeaway

AI-powered social engineering attacks are shifting cyber risk from a predominantly technical problem to a human-centered challenge. Organizations that combine strong employee training, robust verification controls, effective incident response planning, and a comprehensive risk transfer strategy will be better positioned to defend against this rapidly evolving threat landscape.



Ready to be EPIC?

For more information about how EPIC can help your business, visit us at epicbrokers.com.