An Expert Guide to lowering social engineering risks

verizon

Fraudsters exploit human psychology—fear, excitement, urgency—to cloud judgment and steal information or valuables using tactics like phishing, where emails mimic trusted entities to extract private data, or baiting, which offers something enticing to deliver malware.

Pretexting is another example in which attackers manipulate victims into divulging sensitive information by posing as a legitimate entity. Say an employee receives a call from someone claiming to be from the IT department, asking for their login details to perform a routine security check. Yet it's not IT, and the employee has just handed over their credentials to a bad actor. The infiltration has begun.

According to Verizon's 2023 Data Breach Investigations Report (DBIR), such incidents have nearly doubled, constituting 50% of all social engineering incidents. At the same time, more easily recognized social engineering attacks such as pretexting, which includes business email compromise (BEC) are also rising in number and cost. BEC, in which an attacker masquerades as an executive or trusted partner and attempts to manipulate an employee into transferring money or sharing confidential data, accounts for a median loss of $50,000 per incident, according to the 2023 DBIR.

Meanwhile, the use of AI and deep fake technologies can also create highly convincing phishing campaigns, manipulating audio and video to impersonate trusted individuals and deceive victims. For example, a CEO's voice is cloned into a voicemail message, instructing an employee to transfer funds to a fraudulent account immediately so the company can avoid some important problem.

These advances can enable attackers to bypass traditional security measures, and will make it increasingly difficult to distinguish between legitimate and malicious communications. As Jennifer Varner, Verizon's Sr Director of Cyber Security Solution Sales, explains, "The integration of AI into cyberattacks represents a significant shift in attack tactics. It's not just about defending against known threats. It's about anticipating attack methods that leverage cutting-edge technologies."

Rising Losses from Social Engineering

Meanwhile, the volume and financial costs of social engineering attacks on organizations are substantial and rising. The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) received 21,489 BEC complaints with adjusted losses over $2.9 billion in 2023 alone.[1]

And the 2023 DBIR found the median cost of BEC incidents has risen steadily from $20,000 in 2019 to the $50,000 mark in 2023.

Given the rise of AI and deep fakes alongside traditional phishing, smishing, and other social engineering tactics, there's a growing need to increase cybersecurity awareness everywhere, for everyone, all at once. "Organizations need stronger, multi-faceted cybersecurity protections that incorporate the latest technical defenses, along with ongoing security awareness training for employees. This can create a stronger culture of security that helps reduce social engineering risks," Varner explained.

What's more, continuous adaptation is needed to address new and dynamic cyber threats, which are evolving with alarming speed and require a proactive and agile response from organizations.

Because social engineering stands out for its cunning exploitation of human trust, Verizon offers expert guidance to help reduce the impact of threats that organizations may face.

Building a Layered Defense Plan

At the heart of Verizon's social engineering cybersecurity strategy is a layered approach to defense, designed to mitigate risks across multiple points of potential exploitation. This comprehensive strategy encompasses:

- **Employee Awareness Training.** It's crucial to continually educate employees, partners and third parties on security red flags (e.g., solicited personal information) and how to protect their devices with virtual private networks (VPNs) and multifactor authentication (MFA). Training exercises such as phishing, vishing, smishing and quishing tests are critical to keep people on alert. "Employees are key targets for social engineering," Varner said, stressing the importance of empowering employees to recognize and resist social engineering attack methods.

  Since a company's accounting team is probably not as aware of current cybersecurity threats as the company's security team, Verizon Consulting Services supports security training for customers including phishing attacks to foster a culture of vigilance. "Inevitably, some employees are likely to click on the wrong thing," Varner noted. "So we must continually educate ourselves and our personnel to understand what to look for to reduce those risks."

- **Detection and Incident Response.** Verizon's technological defenses include a multi-layered approach that combines near real-time detection and response capabilities that are critical to help decrease the effect of cyber incidents for your organization. Verizon's capabilities include security operations services, endpoint and network security monitoring and incident response services that drill deeper to include:

  – Honeypot reporting/response

  – Investigating and helping to remediate the cause of the incident

  – Forensic data support

  In the event of a breach, swift and comprehensive incident response and containment can help reduce impacts. "Verizon's Rapid Response team is at the ready 24/7 in the event of a breach," Varner explained. Forensic analysis and root cause identification can also help organizations strengthen defenses by understanding how to address vulnerabilities.

- **Ongoing Testing and Reporting.** Ensure that you have a team with knowledge that's up-to-date on social engineering tactics, and a team that conducts regular security positioning assessments. Verizon offers testing and reporting capabilities that include:
  - Penetration testing
  - Tabletop exercises
  - Ransomware assessments
  - Daily dark web intelligence
  - Cyber risk quantification
- **Mobile security policy.** Institute a company-wide mobile security policy. Consider using corporate-liable mobile devices to help ensure that employees discuss business on business phones. Maintain consistent policy and protection controls across all devices. Help support regulatory compliance, along with chain of custody and forensics. Measure organizational wireless performance.

  Many existing cybersecurity measures already used in customer organizations can be effective against social engineering in many cases. Start by understanding what's in place now. Then work with experts to identify gaps and understand specific improvements that can be deployed to help close social engineering vulnerabilities. "It's not about displacing existing investments, but enhancing them," Varner explained.
- **Security protection controls.** Security and access controls should be applied at all levels, from each device, to every network, and across all channels, including third parties. Key elements include:
  - Email, chat, mobile, SMS and voice defense solutions
  - Zero-trust and secure service edge architectures
  - Identity and access management
  - Multifactor authentication (MFA) and Fast IDentity Online 2 (FIDO2)
  - Encryption technologies
  - Third-party security access controls

  To help strengthen supply chain protection, companies should work closely with their partners to ensure security measures are uniformly strong across the entire supply chain, since protections are only as strong as the weakest link. The ITRC 2023 report underscored the magnitude of the threat, citing a 2,600% increase in organizations impacted by supply chain attacks since 2018.[2] Steps to achieve better supply chain security include rigorous vetting of third-party vendors, continuous monitoring of third-party risks, and the implementation of contractual agreements that enforce strict cybersecurity standards among all parties in the supply chain.

Verizon's integrated solutions can help strengthen an organization's security investments, enhance security and help manage supply chain risk for greater resilience.

These five components represent Verizon's comprehensive strategy to help organizations better manage social engineering risks, focusing on awareness, mobile security policies, detection and incident response, ongoing testing and reporting, and security protection controls to enhance existing cybersecurity measures within organizations.

Verizon: Your Partner in Cyber Vigilance

Verizon blends technical innovation, human-centered training, and proactive incident response as a blueprint to help boost cybersecurity defenses. What's more, Verizon's extensive experience and proven track record in combating social engineering can help improve your organization's ability to combat this type of threat.

In one specific instance, Varner offers a glimpse into a real-world success story. "We've worked with very large banks, actively monitoring and shutting down fraudulent text messages as they go out to customers," she explained, highlighting an example in which Verizon was able to help defend against social engineering smishing attacks.

Reach out to us today.

Learn how you can enhance organizational resilience and foster a culture of security awareness that is critical in today's interconnected world. If you have questions or need help, contact your Verizon Business Account Manager, reach out to us here, or learn more by visiting: verizon.com/business/products/security/.

verizon

1. ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2. idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/