Essential Information for Business Clients

Mitigating Insider threats

Phishing Trends Report (2025)

The **2025 Phishing Trends Report** highlights the growing threat of phishing attacks that bypass email filters, focusing on the human-error element of CyberSecurity threats:

- **68% of breaches involve human error**, with 80-95% initiated by phishing attacks.
- **Attacks have increased by 4,151% since 2022**, partly due to AI advancements like ChatGPT.
- **Each phishing breach costs an average of $4.88M.**
- **Proper training can improve phishing detection 6x in 6 months** and reduce incidents by 86%.

Key Trends & Statistics from the article (as of 2025):

- **64% of businesses faced BEC attacks**, averaging $150K per loss.
- **80% of phishing campaigns target cloud credentials** (e.g., Microsoft 365, Google Workspace).
- **80% of phishing sites use HTTPS to appear legitimate.**
- **30% of organizations report fake call scams** impersonating executives.
- **25% increase in QR code phishing** attacks.
- **Deepfake phishing increased 15%**, targeting finance and HR.
- **40% of attacks now spread beyond email** to Slack, Teams, and social media.
- **35% rise in phishing emails** mimicking agencies like the IRS.
- **Readily available kits on the dark web have increased 50%**, lowering entry barriers for attackers.
- **Facebook alone saw 44,750 phishing attacks using its name** in domains.

**** This incident highlights the Importance of mitigating potential insider phishing attacks by enhancing a firm's security stance.***

Proposed course of Action:

To mitigate phishing risks, organizations should adopt a multi-layered security approach, including:

- AI-driven email security solutions to detect and filter phishing attempts.
- Behavior-based phishing awareness training to improve employee resilience.

Sources:

- Phishing Awareness Training
- Email Filtering And Protection

Strengthening Access Controls

New Era Life Insurance Companies Data Breach Impacts 335K Individuals

- An unauthorized party accessed within Life insurance company systems between December 9 and December 18, 2024.
- During this period, specific files were copied from the systems.
- A review of the exposed files was completed on January 31, 2025.

Compromised Data from the incident:

- **Affected individuals include policyholders, agents, and insurance carrier partners.**
- **Exposed files included:**
  - **Names**
  - **Birth dates**
  - **Insurance ID numbers**
  - **Claim details (potentially including diagnosis/treatment information)**
  - **Social Security numbers**

****This data breach highlights the potential negative outcomes of insecure access controls, emphasizing the importance of strengthening systems to prevent unauthorized access.***

Proposed course of Action:

To avoid Data breaches via weak access controls :

A multi-layered approach combining advanced technologies like SOAR, SIEM, and XDR with a robust Zero Trust security model and the NIST Cybersecurity Framework.

- This approach can provide a comprehensive strategy for mitigating cybersecurity risks.
- It helps ensure continuous monitoring, automated response capabilities, and proactive defense measures.

Helps organizations stay one step ahead of cybercriminals.

Sources:

- SOAR vs SIEM vs XDR
- Zero Trust Security Principles
- NIST Framework

Securing Third-Party access

Grubhub Suffers Data Breach in Third-Party Vendor Incident

- Unusual activity detected, later traced to an account of a third-party customer support provider.
- The company swiftly revoked access of the compromised account and removed the provider from its systems.
- Names, email addresses, and phone numbers of campus diners, merchants, drivers, customer service users, Partial payment card details, and Hashed passwords for certain legacy systems were compromised as a result.

***This breach primarily highlights security risks in outsourcing third party vendors and the potential for phishing and social engineering attacks.**

Proposed course of Action:

To avoid third-party vendor risks:

- Conduct thorough vendor risk assessments to safeguard the supply chain.
- Enhance assessment processes using a comprehensive security assessment matrix to strengthen vendor relationships.
- Continuously refine security strategies to improve overall security posture.
- Leverage available tools and insights to drive security programs forward proactively.

Sources:

- Conducting Vendor Risk Assessments