

Phishing Attack Training for Higher Management

Training Duration: 2 Days

Day 1: Understanding Phishing Attacks

Session 1: Introduction to Phishing

- **Duration:** 1 hour
- **Topics Covered:**
 - **Definition of Phishing:**
 - Explanation of what phishing is and how it works.
 - **History and Evolution of Phishing:**
 - Timeline of phishing from its inception to modern-day techniques.
 - **Importance of Awareness in Higher Management:**
 - Role of higher management in mitigating phishing risks.
 - Examples of high-profile phishing attacks on executives.

Session 2: Types of Phishing Attacks

- **Duration:** 1.5 hours
- **Topics Covered:**
 - **Email Phishing:**
 - Traditional phishing emails and common tactics.
 - **Spear Phishing:**
 - Targeted attacks on specific individuals or organizations.
 - **Whaling:**
 - Attacks aimed at senior executives and high-profile targets.
 - **Smishing (SMS Phishing):**
 - Phishing attacks via text messages.
 - **Vishing (Voice Phishing):**
 - Phishing attacks conducted over the phone.
 - **Pharming:**
 - Redirecting users to fraudulent websites without their knowledge.
- **Activity:**
 - Interactive quiz to reinforce understanding of different types of phishing attacks.

Session 3: Anatomy of a Phishing Attack

- **Duration:** 1.5 hours
- **Topics Covered:**
 - **How Phishing Attacks are Crafted:**
 - Step-by-step breakdown of a phishing attack.
 - **Common Techniques Used:**
 - Social engineering, spoofing, and other tactics.
 - **Case Studies of Major Phishing Attacks:**
 - Analysis of notable phishing incidents and their impact.
- **Activity:**
 - Examination of real phishing emails and discussion on their characteristics.

Session 4: Phishing Attack Impact

- **Duration:** 1 hour
- **Topics Covered:**
 - **Financial Impact:**
 - Cost implications of phishing attacks on organizations.
 - **Reputational Damage:**
 - How phishing attacks can harm a company's reputation.
 - **Legal and Regulatory Consequences:**
 - Potential legal ramifications and regulatory fines.
- **Activity:**
 - Group discussion on hypothetical scenarios and their impacts.

Session 5: Identifying Phishing Attacks

- **Duration:** 1 hour
- **Topics Covered:**
 - **Red Flags and Warning Signs:**
 - Indicators of phishing emails and websites.
 - **Analyzing Email Headers:**
 - Techniques for examining email headers to detect phishing.
 - **Suspicious Links and Attachments:**
 - Identifying and handling suspicious links and attachments.

- **Activity:**
 - Hands-on exercise to identify phishing emails from a set of samples.

Day 2: Mitigation and Response Strategies

Session 6: Prevention Strategies

- **Duration:** 1 hour
- **Topics Covered:**
 - **Email Filtering and Anti-Phishing Tools:**
 - Overview of tools and technologies to block phishing emails.
 - **Security Awareness Training for Employees:**
 - Importance of regular training and awareness programs.
 - **Best Practices for Email Security:**
 - Tips and strategies to enhance email security.
- **Activity:**
 - Discussion and brainstorming session on implementing effective prevention strategies.

Session 7: Incident Response Plan

- **Duration:** 1 hour
- **Topics Covered:**
 - **Developing an Incident Response Plan:**
 - Steps to create an effective response plan for phishing attacks.
 - **Roles and Responsibilities:**
 - Defining roles and responsibilities within the organization during an incident.
 - **Communication Plan During an Attack:**
 - Establishing a communication plan for internal and external stakeholders.
- **Activity:**
 - Creating a sample incident response plan in small groups.

Session 8: Legal and Regulatory Requirements

- **Duration:** 1 hour
- **Topics Covered:**
 - **GDPR, CCPA, and Other Regulations:**

- Overview of relevant data protection regulations.
 - **Reporting Obligations:**
 - Understanding mandatory reporting requirements in the event of a breach.
 - **Legal Recourse and Actions:**
 - Potential legal actions and how to pursue them.
- **Activity:**
 - Case study analysis on the legal implications of a phishing attack and group discussion.

Session 9: Tools and Technologies

- **Duration:** 1 hour
- **Topics Covered:**
 - **Anti-Phishing Solutions:**
 - Review of popular anti-phishing solutions available in the market.
 - **Security Information and Event Management (SIEM):**
 - Role of SIEM in detecting and responding to phishing attacks.
 - **Threat Intelligence Platforms:**
 - Utilizing threat intelligence to stay ahead of phishing threats.
- **Activity:**
 - Demonstration of various anti-phishing tools and how they work.

Session 10: Developing a Security Culture

- **Duration:** 1.5 hours
- **Topics Covered:**
 - **Building Awareness Programs:**
 - Strategies for creating effective security awareness programs.
 - **Encouraging Reporting of Suspicious Activities:**
 - Fostering a culture where employees report suspicious emails and activities.
 - **Continuous Improvement and Monitoring:**
 - Importance of ongoing monitoring and improvement of security practices.
- **Activity:**

- Role-playing exercises on phishing scenarios to reinforce learning.

Session 11: Executive Briefing and Q&A

- **Duration:** 1 hour
- **Topics Covered:**
 - **Summary of Key Takeaways:**
 - Recap of important points covered during the training.
 - **Open Discussion:**
 - Opportunity for participants to share their thoughts and insights.
 - **Q&A Session with Experts:**
 - Panel of experts to answer questions and provide additional guidance.