Social Engineering and Phishing Attack Simulation Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Social Engineering and Phishing Attack Simulation Training Course is designed to transform employees from an organization's weakest link into its strongest Human Firewall. We move beyond generic awareness to provide practical, real-world defense strategies against increasingly sophisticated psychological manipulation. Participants will master the art of recognizing, reporting, and mitigating social engineering tactics like Pretexting, Vishing, and Business Email Compromise (BEC). This training is crucial for organizations seeking to significantly reduce data breach risks, enhance their overall security posture, and comply with evolving regulatory frameworks by building a pervasive, resilient security culture.

This program offers a hands-on, gamified learning experience centered on adaptive phishing simulations and immersive social engineering red-flag training. Participants will not only learn about threats like Spear Phishing and Deepfake attacks but will actively participate in controlled exercises to build muscle memory for threat detection. By leveraging Threat Intelligence and Behavioral Science, the course fosters a proactive mindset, enabling immediate and correct responses to suspicious activities. Ultimately, the goal is to cultivate cyber resilience across all departments, ensuring that every employee is an informed defender against the persistent, evolving landscape of cyber threats and can contribute to a measurable reduction in the organization's attack surface.

Programme Curriculum

Social Engineering and Phishing Attack Simulation Training Course

Introduction

Social Engineering and Phishing Attack Simulation Training Course is designed to transform employees from an organization's weakest link into its strongest Human Firewall. We move beyond generic awareness to provide practical, real-world defense strategies against increasingly sophisticated psychological manipulation.

Participants will master the art of recognizing, reporting, and mitigating social engineering tactics like Pretexting, Vishing, and Business Email Compromise (BEC). This training is crucial for organizations seeking to significantly reduce data breach risks, enhance their overall security posture, and comply with evolving regulatory frameworks by building a pervasive, resilient security culture.

This program offers a hands-on, gamified learning experience centered on adaptive phishing simulations and immersive social engineering red-flag training. Participants will not only learn about threats like Spear Phishing and Deepfake attacks but will actively participate in controlled exercises to build muscle memory for threat detection. By leveraging Threat Intelligence and Behavioral Science, the course fosters a proactive mindset, enabling immediate and correct responses to suspicious activities. Ultimately, the goal is to cultivate cyber resilience across all departments, ensuring that every employee is an informed defender against the persistent, evolving landscape of cyber threats and can contribute to a measurable reduction in the organization's attack surface.

Course Duration

10 days

Course Objectives

1. Cultivate a workforce capable of achieving organizational cyber resilience against human-centric attacks.
2. Master the immediate identification of various phishing vectors, including Spear Phishing, Smishing, and Vishing.
3. Equip all employees to function as a crucial layer of the Human Firewall and frontline defense.
4. Develop protocols to effectively detect and mitigate high-impact threats like Business Email Compromise and CEO Fraud.
5. Understand the behavioral science and psychological principles exploited by social engineers
6. Gain practical experience in recognizing simulated attacks through Adaptive Phishing Simulations and Gamified Training.
7. Recognize the emerging risks and red flags associated with AI-powered Deepfake attacks
8. Identify and counteract physical social engineering tactics, such as Tailgating and Baiting
9. Establish and reinforce clear, efficient incident reporting protocols for suspicious communications.
10. Understand the link between human error and the compromise of sensitive assets like PII and Confidential Data.
11. Drive the adoption of a continuous, proactive Security Culture throughout the organization.
12. Implement best practices for Multi-Factor Authentication (MFA) and robust, unique password management.
13. Ensure employee awareness aligns with key requirements from frameworks like GDPR, HIPAA, and PCI DSS.

Target Audience

1. All Organizational Employees.
2. Executive and Senior Leadership.
3. IT and Security Teams.
4. Finance and Accounting Departments.
5. HR and Administration Staff.
6. Remote and Hybrid Workers.
7. Compliance and Legal Officers.
8. New Hires and Contractors

Course Modules

1. Fundamentals of Social Engineering and Human Vulnerabilities

- Define Social Engineering and its core principles
- Explore the psychological triggers.
- The human as the Attack Vector and the technical system.
- Understanding the Cyber Kill Chain.
- Case Study: The RSA SecurID Breach (2011).

2. Deep Dive into Phishing Attacks

- Anatomy of a Phishing Email.
- Differentiating between generic Phishing, Spear Phishing, and Whaling
- Emerging Vectors.
- Advanced techniques.
- Case Study: The 2020 Twitter Attack

3. Business Email Compromise (BEC) and Financial Fraud

- Identifying the distinct phases of a BEC attack
- Specific focus on Invoice Fraud and fake wire transfer requests.
- Protocols for verifying sensitive requests
- The danger of email-only financial approvals and how to secure them.
- Case Study: FACC Wire Transfer Fraud (2016).

4. Recognizing Social Engineering Red Flags

- Practical tips for spotting urgent, unusual, or out-of-character requests.
- Techniques for safely inspecting email headers and hidden URLs
- The importance of questioning and verifying before acting
- Recognizing the difference between legitimate corporate communication and a ruse.
- Case Study: Fake Vendor/IT Support Calls.

5. Physical Social Engineering and Insider Threats

- Methods of physical intrusion.
- Securing physical workspaces.
- The psychology of Quid Pro Quo and Baiting
- Differentiating between malicious and negligent Insider Threats.
- Case Study: The Target Data Breach (2013) Vendor Access.

6. AI-Powered Attacks: Deepfakes and Advanced Impersonation

- Understanding how Generative AI facilitates hyper-realistic phishing and Vishing
- New red flags for verifying identity during video calls and voice communications.
- Protecting personal/professional social media accounts from Reconnaissance.
- The threat of Deepfake CEO Fraud demanding urgent transfers.
- Case Study: Deepfake Voice Scam on Energy Firm CEO.

7. Phishing and Smishing Simulation Exercises

- Review of simulation results and personalized training feedback.

- Analysis of top-clicked phishing templates
- Guided analysis of realistic Smishing and Vishing scripts.
- Practice using the organization's official Phish Alert/Reporting Button.
- Case Study: Simulation Campaign Successes.

8. Strong Authentication and Credential Protection

- The critical role of Multi-Factor Authentication and Zero Trust principles.
- Best practices for creating and managing long, unique passwords
- Dangers of password reuse, saving credentials, and using personal devices
- Securely handling and sharing credentials in professional settings.
- Case Study: Cloud Service Credential Harvesting.

9. Social Media and Remote Work Security

- The risk of oversharing PII on platforms like LinkedIn and Facebook
- Securing home networks, public Wi-Fi, and using VPNs.
- Company policy reminders on acceptable use and data handling outside the office.
- Managing devices, especially for the hybrid workforce.
- Case Study: Reconnaissance via Social Media.

10. Malware, Ransomware, and Malicious Links

- Understanding how phishing enables Ransomware and other Malware deployment.
- The relationship between malicious attachments and file extensions.
- The danger of Scareware and fake security alerts.
- How to safely handle unknown or unexpected file downloads.
- Case Study: WannaCry and NotPetya Dissemination.

11. Data Classification and Incident Reporting

- Defining and classifying organizational data
- Understanding the legal and financial impact of a Data Breach.
- The step-by-step process for immediate Incident Reporting and escalation.
- Importance of being a "Reporter" rather than a "Clicker" in building security culture.
- Case Study: Equifax Data Breach (2017).

12. Security Policy and Regulatory Compliance

- Overview of employee responsibilities under company Acceptable Use Policy.
- Connecting security awareness to regulatory bodies
- The concept of Least Privilege and why it's a non-human defense.
- Understanding your role in protecting customer and client data.
- Case Study: Fines for Lack of Training.

13. Advanced Pretexting Scenarios

- In-depth role-play.
- Learning to spot the inconsistencies and factual errors in a complex pretext.
- Techniques for politely but firmly ending a suspicious interaction
- Case Study: The Con-Man Strategy.

14. Creating a Security-Conscious Culture

- How to be a Security Champion and mentor colleagues.
- Moving from security compliance to continuous Security Awareness.
- Techniques for making security a positive, ongoing conversation, not a scare tactic.
- Sustaining the learning with micro-training and regular communication.
- Case Study: Company-Wide Security Award Program.

15. Measuring and Sustaining Awareness

- Key metrics for success.
- Strategy for running iterative and increasingly difficult simulations.
- The importance of executive buy-in and visible security leadership.
- Developing a year-round, adaptive awareness calendar.
- Case Study: Year-Over-Year Improvement.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com