Advanced E-mail Security and Phishing Defense 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

The digital landscape is continuously challenged by increasingly sophisticated and pervasive cyber threats, with email remaining the primary attack vector. Traditional perimeter defenses and legacy anti-spam filters are no longer sufficient to combat modern threats like AI-enhanced phishing, Business Email Compromise (BEC), and complex Zero-Day Exploits. Advanced E-mail Security and Phishing Defense Training Course provides advanced knowledge and proactive defense strategies necessary to build a resilient human firewall and implement a layered security architecture. Participants will move beyond basic awareness to master cutting-edge email authentication protocols, threat intelligence integration, and incident response methodologies essential for protecting organizational assets in a constantly evolving threat environment.

This intensive program focuses on practical, real-world applications to drastically reduce the organizational human risk score. We will deep-dive into the technical and behavioral aspects of email security, equipping security teams and high-risk employees with the expertise to defend against highly targeted attacks such as Spear Phishing, Whaling, and the emerging threat of QR Code Phishing. By emphasizing a blend of technical controls and a strong security-first culture, this training is critical for maintaining compliance, preserving business continuity, and achieving a robust cyber resilience posture against the most financially damaging forms of modern cybercrime.

Programme Curriculum

Advanced E-mail Security and Phishing Defense Training Course

Introduction

The digital landscape is continuously challenged by increasingly sophisticated and pervasive cyber threats, with email remaining the primary attack vector. Traditional perimeter defenses and legacy anti-spam filters are no longer sufficient to combat modern threats like AI-enhanced phishing, Business Email Compromise (BEC), and

complex Zero-Day Exploits. Advanced E-mail Security and Phishing Defense Training Course provides advanced knowledge and proactive defense strategies necessary to build a resilient human firewall and implement a layered security architecture. Participants will move beyond basic awareness to master cutting-edge email authentication protocols, threat intelligence integration, and incident response methodologies essential for protecting organizational assets in a constantly evolving threat environment.

This intensive program focuses on practical, real-world applications to drastically reduce the organizational human risk score. We will deep-dive into the technical and behavioral aspects of email security, equipping security teams and high-risk employees with the expertise to defend against highly targeted attacks such as Spear Phishing, Whaling, and the emerging threat of QR Code Phishing. By emphasizing a blend of technical controls and a strong security-first culture, this training is critical for maintaining compliance, preserving business continuity, and achieving a robust cyber resilience posture against the most financially damaging forms of modern cybercrime.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Analyze and Differentiate Advanced Phishing Tactics including Whaling, Vishing, Smishing, and Quishing.
2. Implement and validate Advanced Email Authentication protocols.
3. Architect a Layered Email Security framework integrating Cloud Email Security Gateways and Zero Trust principles.
4. Identify and mitigate Business Email Compromise and Executive Impersonation attacks using anti-spoofing and anomaly detection.
5. Utilize Threat Intelligence feeds and Social Engineering Reconnaissance techniques to preemptively block targeted campaigns.
6. Master Email Incident Response protocols, including Triage, Containment, and Post-Incident Remediation.
7. Recognize and defend against AI-Enhanced Phishing and Deepfake voice/video impersonation threats.
8. Conduct effective, high-fidelity Phishing Simulations and calculate the organizational Human Risk Score.
9. Secure and monitor Cloud Email Environments against Configuration Exploitation.
10. Implement Data Loss Prevention and Email Encryption to prevent sensitive data exfiltration via email.
11. Develop and reinforce a proactive Security-First Culture and frictionless Suspicious Email Reporting mechanisms.
12. Understand the impact and mitigation strategies for Reply Chain Attacks and supply chain email compromise.
13. Apply the MITRE ATT&CK Framework to map and model advanced email threat adversary techniques.

Target Audience

1. IT Security Analysts/Engineers
2. Security Operations Center (SOC) Staff
3. IT Administrators
4. Information Security Managers and Directors
5. Compliance and Risk Management Professionals
6. High-Risk Employees

7. System/Network Administrators
8. Cybersecurity Consultants

Course Modules

1. The Advanced Phishing Threat Landscape

- Evolution of Phishing.
- Deep-Dive into Emerging Vectors.
- AI's Role in Cybercrime.
- Financial and Reputational Impact.
- Case Study: Analysis of a recent large-scale Deepfake voice impersonation attack used to authorize a multi-million-dollar wire transfer, focusing on the email initiation phase and red flags.

2. Advanced Email Authentication and Anti-Spoofing

- Mastering DMARC.
- SPF, DKIM, and Identifier Alignment.
- Brand Indicators for Message Identification.
- MTA-STS and TLS-RPT.
- Case Study: A company's struggle to achieve DMARC Enforcement due to third-party marketing services, and the step-by-step remediation process that protected their domain from spoofing.

3. Layered Email Security Architecture (CESG & Zero Trust)

- The Zero Trust Model for Email.
- Cloud Email Security Gateway (CESG) Deep Dive.
- Sandboxing and Detonation Chambers.
- Post-Delivery Protection
- Case Study: An organization's migration from a legacy perimeter solution to a modern CESG, demonstrating how sandboxing stopped a zero-day fileless malware delivered via a seemingly harmless email attachment.

4. Defending Against Business Email Compromise (BEC) and EAC

- BEC Scenarios
- Anomaly Detection.
- Internal Email Security.
- Implementing Financial Controls.
- Case Study: The FBI's Public Service Announcement on a BEC scam where an attacker intercepted an email chain to change vendor payment details, highlighting the red flags in the compromised chain.

5. Email Threat Intelligence and Threat Hunting

- Integrating STIX/TAXII Feeds.
- Open-Source Intelligence.
- Email Header Analysis Mastery.
- Mapping to MITRE ATT&CK.
- Case Study: A threat hunt initiated by a single user report, which used email header analysis and OSINT to uncover a broad campaign targeting the entire executive leadership team.

6. Phishing Simulation and Human Risk Management

- Designing High-Fidelity Simulations.
- Metrics and Measurement.
- Targeted Remedial Training.
- Gamification and Security Champions.
- Case Study: A retail company?ÇÖs successful 12-month program that reduced the employee click-rate from 18% to under 2% through continuous, gamified phishing simulations and immediate micro-training.

7. Email Incident Response and Forensics

- The Incident Response Lifecycle.
- Triage and Containment
- Digital Forensics for Email.
- Communication Planning.
- Case Study: A major university's detailed incident response plan activated after a successful credential harvesting attack, detailing the speed of isolation and multi-team coordination required.

8. Data Loss Prevention (DLP) and Email Compliance

- Defining Sensitive Data.
- DLP Policy Creation.
- End-to-End Encryption
- Monitoring and False Positive Reduction.
- Case Study: A healthcare provider's DLP policy rollout that prevented a major HIPAA violation by automatically encrypting an email containing patient health information (PHI) mistakenly sent to an external, unsecure recipient.

9. Securing Cloud Email Platforms

- Configuration Hardening.
- Multi-Factor Authentication (MFA) Enforcement.
- Cloud Logging and Auditing.
- Advanced Threat Protection Features.
- Case Study: A successful Account Takeover (ATO) where an attacker exploited a legacy email protocol (POP3/IMAP) not covered by MFA, leading to a review and enforcement of a strict Modern Authentication only policy.

10. Malware, Ransomware, and Malicious Attachments

- Malware Delivery Techniques.
- Fileless Malware and Zero-Day Exploits.
- Advanced Attachment Analysis.
- Ransomware Kill Chain via Email.
- Case Study: An organization that suffered a Ransomware infection initiated by a malicious Excel attachment; the analysis focuses on the email's social engineering lure and the security gaps that failed to detonate the payload.

11. Social Engineering Deep Dive for Email Defense

- Psychology of the Attack.
- Reconnaissance and Tailoring.
- Reply Chain Attacks.

- Defensive Deconstruction.
- Case Study: A highly effective Reply Chain Attack where an attacker hijacked a vendor's email thread and successfully inserted a fraudulent invoice, demonstrating the power of contextual social engineering.

12. Policy Development and Regulatory Compliance

- Acceptable Use Policy (AUP) for Email.
- Incident Reporting Policy.
- Retention and Archiving Policy.
- Global Compliance Landscape.
- Case Study: A global company's policy revision to mandate frictionless reporting after discovering a long-running, unreported Spear Phishing campaign that had compromised several high-value accounts.

13. Mobile and Non-Traditional Phishing Defense

- Securing Email on Mobile Devices.
- SMS Phishing.
- Voice Phishing.
- QR Code Attack Vector Mitigation.
- Case Study: A finance employee who almost fell for a Quishing attempt where a QR code in an urgent-themed email led to a perfect clone of their corporate login portal, highlighting the challenge of mobile detection.

14. Advanced Threat Modeling for Email Systems

- STRIDE Model Application.
- Asset and Data Flow Mapping.
- Proactive Risk Assessment.
- Red Team Exercises.
- Case Study: A manufacturing firm's Threat Modeling exercise that identified the Accounts Payable department as the highest BEC risk, leading to immediate implementation of multi-factor payment approvals.

15. The Future of Email Security

- Post-Quantum Cryptography Impact.
- AI for Defense.
- E-mail as an Identity Layer.
- Continuous Adaptive Risk and Trust Assessment.
- Case Study: Examination of a major email security vendor's roadmap, focusing on their shift towards AI-powered behavioral analysis and micro-segmentation for internal email flow.

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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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