Training Course on Detecting and Responding to AI-Powered Phishing Attacks

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapidly evolving threat landscape demands sophisticated defense mechanisms against **AI-powered phishing attacks**. Traditional cybersecurity measures are increasingly insufficient as **generative AI** enables cybercriminals to craft highly convincing, **hyper-personalized phishing emails**, **deepfake voice phishing (vishing)**, and **synthetic video scams (smishing/quishing)** at an unprecedented scale. Training Course on Detecting and Responding to AI-Powered Phishing Attacks is designed to equip individuals and organizations with the essential knowledge and **practical skills** to **identify, analyze, and effectively respond** to these advanced social engineering threats. We will delve into the nuances of how **machine learning** and **natural language processing (NLP)** are weaponized by attackers, and crucially, how to leverage **AI-driven detection tools** and **behavioral analytics** for robust **cyber defense**.

In today's digital age, human error remains a significant vulnerability. With AI dramatically increasing the **sophistication of phishing lures** and enabling **multi-channel attacks** (email, SMS, voice, QR codes), proactive **security awareness training** is no longer optional—it's imperative. This program focuses on building a **resilient security culture** by empowering employees to become the first line of defense. Through **hands-on simulations**, **real-world case studies**, and comprehensive modules on **threat intelligence** and **incident response**, participants will gain the confidence to navigate the complex world of **AI-driven cyber threats**, safeguarding sensitive data and preserving organizational integrity.

Programme Curriculum

Training Course on Detecting and Responding to AI-Powered Phishing Attacks

Introduction

The rapidly evolving threat landscape demands sophisticated defense mechanisms against **AI-powered phishing attacks**. Traditional cybersecurity measures are increasingly insufficient as **generative AI** enables cybercriminals to craft highly convincing, **hyper-personalized phishing emails**, **deepfake voice phishing (vishing)**, and **synthetic video scams (smishing/quishing)** at an unprecedented scale. Training Course on Detecting and Responding to AI-Powered Phishing Attacks is designed to equip individuals and organizations with the essential knowledge and **practical skills** to **identify, analyze, and effectively respond** to these advanced social engineering threats. We will delve into the nuances of how **machine learning** and **natural language processing (NLP)** are weaponized by attackers, and crucially, how to leverage **AI-driven detection tools** and **behavioral analytics** for robust **cyber defense**.

In today's digital age, human error remains a significant vulnerability. With AI dramatically increasing the **sophistication of phishing lures** and enabling **multi-channel attacks** (email, SMS, voice, QR codes), proactive **security awareness training** is no longer optional—it's imperative. This program focuses on building a **resilient security culture** by empowering employees to become the first line of defense. Through **hands-on simulations**, **real-world case studies**, and comprehensive modules on **threat intelligence** and **incident response**, participants will gain the confidence to navigate the complex world of **AI-driven cyber threats**, safeguarding sensitive data and preserving organizational integrity.

Course Duration

5 days

Course Objectives

1. Comprehend the progression of phishing tactics from traditional methods to advanced AI-generated deepfakes, vishing, and smishing in 2025.
2. Develop keen observation skills to spot subtle indicators of AI-crafted phishing, including flawless grammar, contextual relevance, and psychological manipulation techniques.
3. Learn to distinguish between typical human errors in phishing and the seamless, highly convincing content produced by Large Language Models (LLMs).
4. Acquire expert techniques for scrutinizing obfuscated URLs, sender spoofing, and email metadata to unmask malicious origins.
5. Train to detect synthetic media artifacts in voice clones and deepfake video calls used in CEO fraud and business email compromise (BEC).
6. Explore and understand the functionality of AI-powered email filters, endpoint detection and response (EDR), and security information and event management (SIEM) solutions in mitigating AI phishing.
7. Cultivate a zero-trust mindset and implement multi-factor authentication (MFA), password managers, and out-of-band verification strategies.
8. Learn to create and execute robust phishing incident response protocols, including reporting, containment, and recovery for AI-powered attacks.
9. Gain expertise in designing and deploying AI-driven phishing simulations to test employee resilience and identify vulnerabilities.
10. Utilize current threat intelligence feeds and AI-driven analytics to stay updated on emerging phishing trends and attacker methodologies.
11. Grasp the implications of GDPR, CCPA, and other data privacy regulations in the context of phishing breaches.
12. Foster an organizational environment where cybersecurity awareness is ingrained, promoting prompt reporting and continuous learning.

13. Apply metrics like click-through rates, reporting rates, and dwell time to continuously enhance human firewall effectiveness.

Organizational Benefits

- Significantly lowers the likelihood of successful **AI-powered phishing breaches**, minimizing data loss, financial fraud, and system compromise.
- Strengthens the organization's overall **cybersecurity resilience** by transforming employees into a proactive human firewall.
- Mitigates the exorbitant financial costs associated with data breaches, regulatory fines, legal fees, and business disruption.
- Helps meet stringent **regulatory compliance** requirements related to data protection and incident reporting.
- Safeguards brand reputation and customer trust by preventing public relations crises stemming from security incidents.
- Empowers employees with the knowledge and tools to confidently identify and report suspicious communications, fostering a sense of shared responsibility.
- Enables quicker detection and more efficient **phishing incident response**, reducing dwell time and minimizing potential damage.
- Establishes a culture of continuous learning and adaptation to evolving **AI-driven cyber threats**, ensuring long-term security.

Target Audience

1. IT and Cybersecurity Professionals.
2. Security Awareness Program Managers.
3. Human Resources (HR) and Compliance Officers.
4. Senior Management and Executives.
5. General Employees.
6. Remote and Hybrid Workers.
7. Customer Service Representatives
8. Legal and Risk Management Teams.

Course Outline

Module 1: The Evolving Landscape of AI-Powered Phishing

- Introduction to AI in Cybersecurity
- Understanding Generative AI's Role
- The Rise of Deepfakes
- Multi-Channel Phishing
- **Case Study:** The "AI-Generated CEO Voice Scam" – Analysis of a real-world incident where a finance executive was tricked into a multi-million dollar transfer by an AI-cloned voice.

Module 2: Anatomy of an AI-Powered Phishing Attack

- Reconnaissance & Hyper-Personalization
- Crafting Convincing Lures with NLP
- Evading Traditional Defenses
- Adaptive Attack Chains
- **Case Study:** "The Perfect Phish" – Examination of a sophisticated spear phishing campaign where AI created a highly personalized email, mimicking an internal communication style,

resulting in credential compromise.

Module 3: Advanced Detection Techniques for AI Phishing

- Beyond Typo Hunting
- Analyzing Email Headers and URLs.
- Detecting Deepfake Visual and Audio Cues.
- Leveraging AI-Driven Security Tools
- **Case Study:** "The Quishing QR Code Incident" – Analysis of an attack where AI generated a seemingly legitimate invoice with a malicious QR code, demonstrating advanced visual inspection techniques.

Module 4: Incident Response for AI-Powered Phishing

- Phishing Incident Response Lifecycle
- Immediate Action Protocol.
- Reporting and Escalation Procedures.
- Digital Forensics in Phishing Incidents
- **Case Study:** "Rapid Response to a Vishing Attack" – A scenario where an organization's quick thinking and pre-established response plan minimized damage from an AI-voice vishing attempt.

Module 5: Proactive Defense Strategies & Technologies

- Multi-Factor Authentication (MFA) & Password Managers
- Secure Browse Habits & Software Updates.
- AI in Defensive Strategies
- Security Architecture Enhancements.
- **Case Study:** "Implementing a Behavioral AI Security Solution" – How a company integrated an AI-driven platform to detect unusual login patterns, preventing a major credential stuffing attack.

Module 6: Building a Human Firewall & Security Culture

- The Human Element in Cybersecurity
- Effective Security Awareness Training
- Fostering a Reporting Culture
- Gamification and Reinforcement.
- **Case Study:** "Transforming Susceptibility to Resilience" – A success story of an organization that drastically reduced its phishing click rate through consistent, engaging, and AI-simulation-driven training.

Module 7: Phishing Simulation & Measurement

- Designing Realistic AI Phishing Simulations
- Measuring Phishing Resilience
- Personalized Training Remediation
- Automated Simulation Platforms.
- **Case Study:** "Targeted Training for High-Risk Users" – How an organization identified and provided specialized training to employees frequently targeted by AI-powered spear phishing, showing significant improvement in their resilience.

Module 8: Legal, Ethical, and Future Considerations

- Data Privacy Regulations and Phishing
- Ethical Implications of AI in Cyber Warfare
- Emerging AI-Powered Threats.
- Staying Ahead of the Curve
- **Case Study:** "The Regulatory Aftermath of a Deepfake Breach" – Analysis of the legal and reputational consequences for a company that suffered a breach due to an AI-powered deepfake attack, highlighting the importance of compliance.

Training Methodology

- Instructor-Led Sessions
- Hands-On Labs & Exercises.
- Live Phishing Simulations (Controlled Environment.
- Case Study Analysis
- Group Discussions & Peer Learning
- Q&A Sessions
- Resource Handouts & Checklists
- Post-Training Assessments.

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	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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