MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

PHISHING SIMULATION AUDIT: ASSESSES THE ORGANIZATION\'S SUSCEPTIBILITY TO PHISHING ATTACKS THROUGH SIMULATED EXERCISES

“Auditing Human Risk by Simulating Real-World Phishing Scenarios to Strengthen Cyber Resilience”

Schedule

Date	Venue	Fees (Face-to-Face)
20 – 24 Apr 2026	London, UK	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training

Introduction

Phishing remains one of the most common and dangerous forms of cyber attack, targeting the human element within organizations. Even with advanced security tools, human error continues to be a key vulnerability. Phishing simulation audits help organizations assess their susceptibility by testing real-time employee responses to simulated phishing scenarios.

This course empowers IT auditors, security professionals, and compliance officers with the tools and techniques to plan and execute phishing simulation audits. Participants will learn to design effective phishing tests, monitor results, measure risk exposure, and recommend targeted awareness training based on data-driven insights.

Objectives

By the end of this course, participants will be able to:

- Understand phishing tactics, attacker strategies, and organizational vulnerabilities
- Plan, conduct, and evaluate phishing simulation audits ethically and legally
- Design phishing email templates and response tracking mechanisms
- Interpret simulation data to identify risk trends and human factors
- Report findings and recommend security awareness improvements

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

By the end of this course, participants will be able to:

- Understand phishing tactics, attacker strategies, and organizational vulnerabilities
- Plan, conduct, and evaluate phishing simulation audits ethically and legally
- Design phishing email templates and response tracking mechanisms
- Interpret simulation data to identify risk trends and human factors
- Report findings and recommend security awareness improvements

Target Audience

This program is designed for:

- IT auditors and cybersecurity professionals
- Information security and risk managers
- GRC (Governance, Risk & Compliance) officers
- IT compliance and internal control staff
- Training and awareness coordinators

Individual Benefits

Key competencies that will be developed include:

- Phishing simulation planning and execution
- Cyber risk communication and user behavior analysis
- Phishing incident lifecycle tracking
- Use of industry-standard phishing tools and reporting dashboards
- Design of training interventions based on audit outcomes

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved awareness of social engineering risks across the organization
- Data-driven targeting of cybersecurity awareness programs
- Better measurement of user resilience to phishing campaigns
- Compliance with security frameworks requiring periodic testing (e.g., NIST, ISO 27001)
- Enhanced cybersecurity posture through behavioral monitoring

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Social engineering, phishing tactics, audit frameworks (NIST, CIS)
- Case Studies – Real-world phishing attacks and response failures
- Workshops – Design phishing emails, simulate campaigns, analyze user actions
- Peer Exchange – Lessons learned from phishing response and audit experience
- Tools – Phishing simulation platforms (e.g., KnowBe4, Cofense), email templates, response metrics

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Training Hours: 7:30 AM – 3:30 PM Daily Format: 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Understanding Phishing and Social Engineering

- Module 1: Introduction to Phishing Threat Landscape (07:30 – 09:30) • Types of phishing (spear phishing, clone phishing, whaling)
- Module 2: Psychology of Phishing – Why Users Click (09:45 – 11:15) • Social engineering tactics, urgency, curiosity, fear
- Module 3: Organizational Vulnerabilities and Risk Context (11:30 – 01:00) • Email security, user behavior, attack vectors
- Module 4: Workshop – Analyze Real Phishing Emails (02:00 – 03:30) • Dissect phishing examples to identify red flags

Day 2: Phishing Simulation Planning and Tools

- Module 1: Setting Audit Objectives and Scope (07:30 – 09:30) • User targeting, simulation frequency, consent/legal review
- Module 2: Choosing a Simulation Platform (09:45 – 11:15) • Tool comparison (KnowBe4, Cofense, Microsoft Defender)
- Module 3: Email Template Design and Delivery Tactics (11:30 – 01:00) • Language, branding, trigger types (links, attachments)
- Module 4: Workshop – Build a Phishing Simulation Campaign (02:00 – 03:30) • Create and configure a test campaign using a simulation tool

Day 3: Conducting the Simulation Audit

- Module 1: Ethical and Legal Considerations (07:30 – 09:30) • Employee consent, data privacy, policy integration
- Module 2: Execution and Monitoring of Simulation (09:45 – 11:15) • Tracking clicks, submissions, reporting behavior
- Module 3: Handling User Responses and Escalations (11:30 – 01:00) • Helpdesk involvement, incident simulation
- Module 4: Workshop – Run a Live or Simulated Campaign (02:00 – 03:30) • Test execution and live result interpretation

Day 4: Data Analysis and Risk Interpretation

- Module 1: Metrics and Indicators from Simulation Results (07:30 – 09:30) • Click rate, report rate, failure to report, response time
- Module 2: User Risk Profiling and Segmentation (09:45 – 11:15) • Heatmaps, department comparison, user trends
- Module 3: Linking Results to Risk Management Frameworks (11:30 – 01:00) • Integrating into enterprise risk dashboards
- Module 4: Workshop – Analyze Campaign Data and Identify Risk Gaps (02:00 – 03:30) • Visualize and interpret results for executive use

Day 5: Reporting and Security Awareness Integration

- Module 1: Writing the Phishing Audit Report (07:30 – 09:30) • Executive summary, methodology, key findings
- Module 2: Recommendations for Risk Reduction and Training (09:45 – 11:15) • Tailored security awareness planning
- Module 3: Final Case Study – Phishing Simulation Audit Presentation (11:30 – 01:00) • Prepare and present simulation audit findings
- Module 4: Wrap-Up and Certification (02:00 – 03:30) • Course review, feedback, and certificate distribution

Certification

Participants will receive a Certificate of Completion in Phishing Simulation Audit, validating their ability to assess and improve organizational cybersecurity awareness by simulating real-world phishing attacks and analyzing behavioral risk data.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**