MAWA EVENTS

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

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

SOCIAL ENGINEERING AUDIT: ASSESSES THE SUSCEPTIBILITY OF EMPLOYEES TO SOCIAL ENGINEERING ATTACKS, SUCH AS PHISHING

"Strengthening Your Organization's Defenses Against Phishing and Social Engineering Attacks"

Schedule

Date	Venue	Fees (Face-to-Face)
06– 10 Jul 2026	London, UK	USD 3495 per delegate

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

Introduction

The Social Engineering Audit course is designed to help organizations assess their susceptibility to social engineering attacks, such as phishing, baiting, and pretexting. Social engineering exploits the human element of cybersecurity, often bypassing even the most robust technical defenses. This course will equip participants with the skills to recognize and counter social engineering tactics, assess vulnerabilities within their organizations, and implement safeguards against these increasingly common threats.

Through a blend of theoretical learning and practical exercises, participants will learn how to simulate social engineering attacks, identify potential human vulnerabilities, and build a culture of awareness and vigilance among employees to defend against social engineering threats.

Objectives

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

- Assess organizational susceptibility to social engineering attacks
- Recognize various social engineering tactics, including phishing, pretexting, and baiting
- Implement effective strategies to counter social engineering threats
- Conduct social engineering simulations to test employee response to security risks
- Design training programs to raise awareness and reduce human vulnerabilities to social engineering

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

- Learn how social engineering attacks bypass technical defenses by exploiting human psychology
- Gain practical skills to identify and mitigate common social engineering tactics
- Learn how to perform social engineering audits and simulate phishing attacks to test employee awareness
- Understand the best practices for developing a security-conscious organizational culture
- Build your capability to safeguard your organization against costly social engineering breaches

Target Audience

This program is designed for:

- IT security professionals and auditors
- HR managers and training coordinators responsible for employee awareness
- Risk managers and compliance officers
- Anyone involved in cybersecurity awareness training or security policy development
- Business leaders and managers who oversee teams and organizational security

Individual Benefits

Key competencies that will be developed include:

- Proficiency in identifying and evaluating social engineering risks
- Ability to conduct social engineering vulnerability assessments and phishing simulations
- Enhanced knowledge of human-centered security threats and how to address them
- Skills in designing and implementing security awareness training programs
- Capability to lead efforts to improve organizational resistance to social engineering

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved ability to assess and mitigate social engineering threats targeting employees
- Enhanced capacity to protect organizational data and systems from human-based vulnerabilities
- A well-defined process for regularly auditing employee susceptibility to social engineering attacks
- Knowledge of how to implement organization-wide awareness campaigns to defend against phishing and other social engineering tactics
- A stronger security posture through human-centric security measures

Instructional Methodology

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

- Strategy Briefings – Introduction to social engineering tactics, risks, and mitigation strategies
- Case Studies – Analysis of real-world social engineering attacks and how they were handled
- Workshops – Hands-on exercises to simulate phishing attacks, pretexting, and baiting scenarios
- Peer Exchange – Group discussions on experiences with social engineering and lessons learned
- Tools – Templates for conducting social engineering audits, phishing tests, and awareness training programs

MAWA EVENTS

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

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

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

Detailed 5-Day 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: Introduction to Social Engineering and Human-Centered Security

- Module 1: Understanding Social Engineering (07:30 – 09:30)
- The psychology behind social engineering attacks
- Common social engineering techniques (e.g., phishing, baiting, pretexting)
- Human vulnerabilities in cybersecurity
- Module 2: The Social Engineer’s Playbook (09:45 – 11:15)
- Analyzing attack methods and tactics used by social engineers
- Real-world examples of successful social engineering breaches
- Identifying the motives and goals of social engineering attackers
- Module 3: Organizational Vulnerabilities to Social Engineering (11:30 – 01:00)
- Conducting internal assessments to identify social engineering risks
- Mapping human vulnerabilities to organizational workflows and processes
- The role of employees in mitigating or exacerbating social engineering risks

Day 2: Social Engineering Attack Simulation and Assessment

- Module 4: Designing and Conducting Phishing Simulations (07:30 – 09:30)
- Creating realistic phishing campaigns to assess employee awareness
- Evaluating employee responses and identifying gaps in security awareness
- Tools and techniques for running phishing tests
- Module 5: Conducting Pretexting and Baiting Scenarios (09:45 – 11:15)
- Understanding the difference between phishing, pretexting, and baiting
- Designing realistic pretexting and baiting scenarios
- Assessing the success of simulated attacks and analyzing results
- Module 6: Analyzing Social Engineering Vulnerabilities (11:30 – 01:00)
- Identifying organizational weak points in human security
- Understanding the root causes of human-centered vulnerabilities
- Building a profile of the organization\'s risk areas

Day 3: Mitigation Strategies and Countermeasures

- Module 7: Securing Against Phishing Attacks (07:30 – 09:30)
- Effective strategies to mitigate phishing risks
- Email security tools and techniques to defend against phishing
- Employee training and awareness programs for phishing prevention
- Module 8: Preventing Pretexting and Baiting Attacks (09:45 – 11:15)
- Securing communications channels to prevent pretexting attacks
- Implementing policies to safeguard against baiting scenarios
- Best practices for reducing human errors in social engineering threats
- Module 9: Developing an Employee Awareness Program (11:30 – 01:00)
- Designing a comprehensive social engineering awareness training program
- Promoting a security-conscious culture among employees
-

Best practices for continual learning and employee engagement

Day 4: Evaluating and Improving Organizational Security

- Module 10: Measuring the Effectiveness of Security Training (07:30 – 09:30)
- Tracking the success of social engineering awareness programs
- Using metrics and analytics to measure employee vulnerability
- Continuous improvement of security training programs
- Module 11: Policy Development for Social Engineering Prevention (09:45 – 11:15)
- Creating policies and guidelines to mitigate social engineering risks
- Ensuring that policies are well-communicated and enforced across the organization
- Establishing incident response protocols for social engineering attacks
- Module 12: Conducting Ongoing Social Engineering Audits (11:30 – 01:00)
- Best practices for regular social engineering audits
- Setting up recurring phishing tests and vulnerability assessments
- Reviewing and updating security policies based on audit findings

Day 5: Final Assessment and Certification

- Module 13: Group Exercise: Social Engineering Attack Simulation (07:30 – 09:30)
- Simulating a full-scale social engineering attack on the organization
- Analyzing the response of employees and effectiveness of security measures
- Peer feedback and review of audit results
- Module 14: Final Review and Q&A (09:45 – 11:15)
- Recap of key lessons learned and strategies for social engineering defense
- Addressing final questions and providing additional resources for continued learning
- Module 15: Certification and Closing Remarks (11:30 – 01:00)
- Distribution of certificates of completion
- Final remarks and action steps for improving organizational security

Certification

Participants will receive a Certificate of Completion in Social Engineering Audit, confirming their ability to assess, prevent, and mitigate social engineering threats in the workplace.

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.

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