MAWA EVENTS

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

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

SOCIAL MEDIA SECURITY AUDIT: EXAMINES THE SECURITY RISKS ASSOCIATED WITH THE ORGANIZATION\'S USE OF SOCIAL MEDIA PLATFORMS

“Defending Against Cyber Threats on Social Media Platforms”

Schedule

Date	Venue	Fees (Face-to-Face)
13 – 17 Jul 2026	London, UK	USD 4995 per delegate

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

Introduction

The Social Media Security Audit course is designed to help organizations assess and mitigate security risks associated with their use of social media platforms. Social media has become a significant vector for cyber-attacks, including data breaches, phishing, and brand impersonation. This course focuses on identifying vulnerabilities in social media accounts and organizational practices, implementing best practices for secure social media usage, and ensuring that social media activities do not compromise organizational security.

Through a mix of practical exercises and real-world case studies, participants will gain the skills to audit their organization\'s social media security, identify potential risks, and develop effective strategies to protect against cyber threats and social engineering attacks targeting social media.

Objectives

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

- Assess the security risks associated with the organization\'s social media presence
- Identify vulnerabilities in social media accounts and organizational practices
- Implement best practices for securing social media accounts and content
- Conduct audits to ensure that social media practices comply with organizational security policies
- Develop a strategy for mitigating social media-related cyber threats and brand impersonation

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

- Understand the security risks and threats posed by social media platforms
- Learn how to secure social media accounts and prevent unauthorized access
- Gain insights into the latest trends in social media hacking and data breaches
- Learn how to develop and enforce social media security policies across your organization
- Understand how to mitigate the risks of brand impersonation, data theft, and social engineering attacks via social media

Target Audience

This program is designed for:

- IT security professionals and auditors
- Social media managers and digital marketers
- Risk managers and compliance officers
- Brand managers and PR professionals responsible for social media oversight
- Anyone involved in the management of social media accounts and security protocols

Individual Benefits

Key competencies that will be developed include:

- Proficiency in identifying and evaluating social media security risks
- Ability to audit social media accounts for vulnerabilities and security gaps
- Enhanced understanding of social media-specific cyber threats, including phishing and data breaches
- Capability to create and implement social media security best practices
- Skills in developing policies and training employees to mitigate social media-related risks

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- A well-defined process for auditing and securing social media accounts and activities
- An improved security posture regarding social media presence and online engagement
- Stronger brand protection against social media impersonation and reputation damage
- Better compliance with organizational policies for secure social media usage
- Ability to create a culture of security awareness around the risks of social media within the organization

Instructional Methodology

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

- Strategy Briefings – Overview of social media security risks and compliance guidelines
- Case Studies – Real-world examples of social media security breaches and their impact
- Workshops – Hands-on exercises to audit social media accounts and develop mitigation strategies
- Peer Exchange – Group discussions on challenges and best practices in social media security
- Tools – Templates for social media security audits, risk assessments, and policy development

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 Media Security and Risks

- Module 1: Understanding Social Media Security (07:30 – 09:30)
- The role of social media in organizational communication and cybersecurity
- Overview of security threats specific to social media platforms
- Case studies of social media security breaches
- Module 2: Social Media Attack Vectors (09:45 – 11:15)
- Phishing, brand impersonation, and data breaches on social media
- Common attack methods targeting social media accounts and profiles
- Recognizing the signs of a compromised social media account
- Module 3: Identifying Vulnerabilities in Social Media Practices (11:30 – 01:00)
- Assessing the organization\'s social media security policies and practices
- Vulnerabilities in access control, privacy settings, and third-party integrations
- Evaluating employee practices and awareness of social media security

Day 2: Conducting a Social Media Security Audit

- Module 4: Performing Social Media Account Audits (07:30 – 09:30)
- Step-by-step guide to auditing social media accounts for security risks
- Best practices for securing social media accounts and user permissions
- Tools and techniques for monitoring social media account activity
- Module 5: Analyzing Social Media Data Privacy Risks (09:45 – 11:15)
- Understanding the risks of data privacy violations on social media platforms
- Analyzing permissions, data sharing, and privacy settings across social media profiles
- Identifying data leaks and unauthorized information sharing
- Module 6: Assessing Brand Impersonation Risks (11:30 – 01:00)
- Techniques for identifying and addressing brand impersonation on social media
- Tools to monitor for fake accounts and fraudulent social media activity
- Strategies for reporting and mitigating impersonation attacks

Day 3: Social Media Security Best Practices

- Module 7: Securing Social Media Accounts (07:30 – 09:30)
- Implementing strong password policies and two-factor authentication
- Managing social media account access and permissions effectively
- Creating a social media account recovery and incident response plan
- Module 8: Social Media Security Policies (09:45 – 11:15)
- Developing organization-wide social media security policies
- Guidelines for safe social media usage for employees and third-party vendors
- Establishing protocols for secure social media engagement
- Module 9: Educating Employees on Social Media Security (11:30 – 01:00)
- Creating awareness training programs for employees on social media risks
- Addressing social engineering attacks targeting social media accounts
-

Reinforcing best practices for secure social media use in the workplace

Day 4: Implementing Mitigation Strategies for Social Media Risks

- Module 10: Mitigating Phishing and Social Engineering Attacks (07:30 – 09:30)
- Recognizing and preventing phishing attacks via social media
- Techniques to safeguard sensitive information shared on social media platforms
- Role of social media security in the broader cybersecurity strategy
- Module 11: Developing a Social Media Incident Response Plan (09:45 – 11:15)
- Creating a plan to respond to security breaches on social media
- Guidelines for escalating incidents and engaging with law enforcement if necessary
- Real-world examples of effective incident response strategies
- Module 12: Continuous Monitoring and Auditing of Social Media Accounts (11:30 – 01:00)
- Best practices for continuous monitoring of social media accounts and security activity
- Leveraging automated tools and analytics for ongoing social media security
- Reviewing and updating social media security measures regularly

Day 5: Final Assessment and Certification

- Module 13: Group Exercise: Social Media Security Audit (07:30 – 09:30)
- Hands-on exercise to audit an organization\'s social media presence
- Identifying key vulnerabilities and proposing solutions in a team environment
- Peer feedback and group discussion of audit findings
- Module 14: Final Review and Q&A (09:45 – 11:15)
- Recap of key lessons learned and final Q&A session
- Review of social media security measures and mitigation strategies
- Module 15: Certification and Closing Remarks (11:30 – 01:00)
- Distribution of certificates of completion
- Final remarks and strategies for implementing social media security measures

Certification

Participants will receive a Certificate of Completion in Social Media Security Audit, validating their expertise in securing social media platforms and protecting organizational data and reputation from online threats.

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**