Comprehensive Cyber Security Awareness Training Program

27 September – 1 October 2027
London (UK)

UK Traininig
PARTNER



Comprehensive Cyber Security Awareness Training Program

Ref: 322411_198249 **Date:** 27 September – 1 October 2027 **Location:** London (UK) **Fees:** 6100 GBP

Why This Course

Cybersecurity awareness is one of the first and most important lines of defense against digital threats. Many security incidents begin with everyday actions such as opening a suspicious email, using weak passwords, ignoring software updates, or sharing sensitive information without proper precautions. Building awareness helps individuals and organizations reduce risk, protect data, and respond more confidently to potential threats.

This intensive 1-week Cybersecurity Awareness Training program equips participants with practical knowledge and everyday security habits to identify, prevent, and respond to common cyber risks. Through real-world scenarios, hands-on exercises, phishing examples, device security checks, and guided action planning, participants will learn how to protect personal and organizational information, use digital tools safely, and contribute to a stronger security culture.

What You'll Learn and Practice

By joining this program, you will:

- Understand fundamental cybersecurity concepts and terminology.
- Recognize the current threat landscape and common attack trends.
- Understand the CIA triad: confidentiality, integrity, and availability.
- Identify personal and organizational cybersecurity responsibilities.
- Build strong password habits and use multi-factor authentication.
- Secure personal devices, networks, and Wi-Fi connections.
- Understand the importance of software updates and patch management.
- Recognize social engineering tactics and phishing attempts.
- Apply safe email, browsing, and internet usage practices.
- Protect against malware, ransomware, and suspicious digital activity.
- Understand data privacy regulations and proper data handling practices.
- Develop a personal cybersecurity action plan for ongoing protection.



The Program Flow

Day 1: Introduction to Cybersecurity

- Understand cybersecurity fundamentals and key terminology.
- Explore the current threat landscape and common attack trends.
- Learn basic security principles through the CIA triad.
- Identify common digital risks affecting individuals and organizations.
- Understand personal and organizational responsibilities in cybersecurity.

Day 2: Securing Devices and Networks

- Create and manage strong, unique passwords.
- Set up and use multi-factor authentication on key accounts.
- Apply secure configuration practices for personal and work devices.
- Understand network security basics and Wi-Fi safety.
- Apply software update and patch management best practices.

Day 3: Social Engineering and Phishing

- Identify different types of social engineering attacks.
- Recognize common signs of phishing emails, links, and messages.
- Apply best practices for secure email usage.
- Understand how malware and ransomware attacks occur.
- Practice safe responses to suspicious messages and digital requests.

Day 4: Safe Internet Usage and Data Privacy

- Apply secure browsing techniques and browser security settings.
- Understand digital footprints and how to manage online exposure.
- Review key data privacy concepts and regulations such as GDPR and CCPA.
- Apply proper data handling, sharing, and storage practices.
- Reduce privacy risks when using websites, applications, and online services.

Day 5: Incident Response and Future Trends

- Understand basic incident response procedures.
- Learn how and when to report security incidents and breaches.
- Explore emerging cybersecurity threats and technologies.
- Review good habits for long-term digital protection.
- Develop a personal cybersecurity action plan for continued awareness and safety.



Individual Impact

- Build confidence in identifying and avoiding common cyber threats.
- Improve daily digital habits related to passwords, devices, email, and browsing.
- Strengthen awareness of privacy, data handling, and online safety.
- Gain practical skills for responding to suspicious activity.
- Develop a clear personal action plan for ongoing cybersecurity protection.

Work Impact

- Reduce the risk of human-error-related cybersecurity incidents.
- Strengthen organizational security culture and employee awareness.
- Improve safe handling of business data and sensitive information.
- Support faster reporting of suspicious activity and potential breaches.
- Help protect organizational systems, reputation, and digital assets.

Training Methodology

This program combines awareness-building with practical application through:

- Real-world cybersecurity scenarios and examples.
- Hands-on password and multi-factor authentication exercises.
- Phishing recognition and secure email practice activities.
- Personal device security audit exercises.
- Data privacy and safe browsing discussions.
- Guided development of a personal cybersecurity action plan.

Beyond the Course

Upon completion, participants will be able to:

- Create and maintain strong password and authentication practices.
- Secure personal and work devices more effectively.
- Recognize phishing, social engineering, malware, and ransomware risks.
- Apply safe browsing, email, and data handling habits.
- Report suspicious activity and respond appropriately to basic cyber incidents.
- Maintain a practical cybersecurity action plan for ongoing protection.

