

Comprehensive Cyber Security Awareness Training Program

2026 16 - 12
Paris (France)

UK Traininig

PARTNER



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.

A graphic featuring the text 'UK Training PARTNER' in black, with 'PARTNER' in a larger, bold font. The text is positioned above a chessboard with several chess pieces (a king, a queen, and a pawn) and concentric circles radiating from the pieces, suggesting a strategic or digital theme.

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.

A graphic of a chessboard with several chess pieces (a king, a queen, and a pawn) in the foreground. The text 'UK Training' is in a smaller font above the word 'PARTNER' in a large, bold, black font.

UK Training
PARTNER