

Cybersecurity Awareness for Digital Safety Skills

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Cybersecurity Awareness for Digital Safety Skills

Course Overview:

Cybersecurity Awareness Training: Digital Skills & Online Safety equips employees with the digital capabilities and secure behaviours required to work confidently in modern organisations. Based on the DigComp 2.2 framework, UNESCO's Digital Literacy Global Framework, the Essential Digital Skills Standards 2026 and ENISA cybersecurity-awareness guidance, the course combines practical Digital Skills Training with workplace-focused cyber risk awareness.

Participants learn to recognise phishing, social engineering, online scams, business email compromise and AI-enabled deception. The Cyber Security Awareness Course also develops safe practices for passwords, multifactor authentication, digital identity, mobile devices, cloud platforms and remote working. Through Employee Cybersecurity Training scenarios, participants examine how everyday actions such as opening attachments, sharing files, joining online meetings or entering information into AI tools can expose organisational data.

Unlike a purely technical Cybersecurity Awareness Course, this programme connects Information Security Awareness Training with digital communication, information evaluation, privacy, secure collaboration and responsible technology use. Participants practise verifying suspicious messages, protecting accounts, managing permissions and reporting incidents without delay. The course therefore supports both cybersecurity resilience and workplace productivity. By combining Workplace Cybersecurity Training, Cyber Hygiene Training and Online Safety Training, it enables employees to become safer, more critical and more responsible users of digital technology while contributing to a positive organisational security culture.

Target Audience:

- Employees using computers, mobile devices, email or cloud platforms
- Administrative and office-support employees
- Customer service and contact-centre representatives
- Human resources and recruitment professionals
- Finance, accounting and payroll employees
- Sales, marketing and business-development teams
- Procurement and supply-chain personnel
- Project coordinators and team leaders
- Remote and hybrid employees

AGILE LEADERS
Training Center

Targeted Organizational Departments:

- Information Technology and Information Security
- Human Resources and Learning and Development
- Finance, Accounting and Payroll
- Administration and Corporate Services
- Sales, Marketing and Communications
- Procurement and Supply Chain
- Customer Service and Call Centres
- Legal, Risk and Compliance
- Project Management Offices
- Operations and Business Support

Targeted Industries:

- Banking, insurance and financial services
- Government and public-sector organisations
- Healthcare and pharmaceutical services
- Education and training institutions
- Oil, gas, energy and utilities
- Telecommunications and technology
- Retail, hospitality and e-commerce
- Transportation, aviation and logistics
- Construction, engineering and real estate
- Professional and consulting services
- Manufacturing and industrial organisations
- Non-governmental and international organisations

Course Offerings:

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

- Explain common cybersecurity threats and their organisational consequences.
- Apply essential digital skills safely in everyday workplace activities.
- Recognise phishing emails, malicious attachments and deceptive links.
- Detect social engineering, impersonation and business email compromise attempts.
- Identify warning signs of AI-generated phishing and deepfake-enabled scams.
- Create stronger passwords and use password managers appropriately.
- Explain how multifactor authentication protects workplace accounts.
- Protect personal, customer and organisational information.
- Manage privacy, application permissions and digital identities.
- Use email, cloud storage and collaboration platforms more securely.
- Apply safe practices when working remotely or using mobile devices.
- Evaluate the reliability of online and AI-generated information..

Training Methodology:

The course uses an interactive, behaviour-focused methodology designed for employees with different levels of technical knowledge. Short facilitator-led sessions introduce the essential principles of Digital Skills and Cybersecurity Training, followed by realistic workplace examples that show how cyber incidents begin and how employees can interrupt them.

Participants examine simulated emails, text messages, QR codes, login pages, cloud-sharing invitations and AI-generated communications during Phishing Awareness Training and Social Engineering Awareness Training activities. Small groups identify warning signs, discuss appropriate responses and compare their decisions with recommended cyber-hygiene practices. Business email compromise cases demonstrate how urgency, authority, confidentiality and financial pressure are used to manipulate employees.

Guided demonstrations illustrate password protection, MFA, account permissions, secure file sharing, mobile-device security and Remote Working Cybersecurity. Scenario discussions address lost devices, accidental data disclosure, ransomware warnings and suspicious account activity. Participants also evaluate online sources and AI-generated content to strengthen digital judgement and Online Scam Awareness.

Daily knowledge checks, facilitated feedback and reflection sessions reinforce correct behaviours. The methodology draws on ENISA awareness principles by focusing on audience relevance, practical communication and behavioural change. Activities develop observable workplace actions rather than technical administration skills, making the programme suitable for organisation-wide Cybersecurity Awareness Training.

AGILE LEADERS
Training Center

Course Toolbox:

- Cybersecurity Awareness Participant Guide
- Digital Skills Self-Assessment Checklist
- Phishing Warning Signs Checklist
- Suspicious Email Evaluation Guide
- Social Engineering Scenario Cards
- Business Email Compromise Case Studies
- AI-Enabled Phishing Identification Guide
- Password and Passphrase Checklist
- Multifactor Authentication Reference Guide
- Account Security Review Checklist
- Mobile Device Security Checklist
- Personal Data Classification Examples

Note: Software, cybersecurity platforms and commercial tools are **not** provided. The course introduces relevant tools through explanations, examples and guided demonstrations where appropriate.

Course Agenda:

Day 1: Essential Digital Skills and Cybersecurity Foundations

- **Topic 1:** Understanding Cybersecurity Awareness Training and the employee's role in protecting organisational information
- **Topic 2:** Digital Skills Training for safe, confident and productive workplace technology use
- **Topic 3:** Understanding cyber threats, vulnerabilities, risk, attacks and their business consequences
- **Topic 4:** Managing workplace files, folders, cloud information and secure digital records
- **Topic 5:** Evaluating online information, websites, search results and AI-generated content
- **Topic 6:** Building cyber hygiene habits for Safe Internet Use at Work
- **Reflection & Review:** Reviewing personal digital habits and identifying opportunities to improve workplace cybersecurity

AGILE LEADERS
Training Center

Day 2: Phishing, Social Engineering and Online Scams

- **Topic 1:** Phishing Awareness Training: recognising deceptive emails, messages, links and attachments
- **Topic 2:** Social Engineering Awareness Training: manipulation through urgency, authority, fear and trust
- **Topic 3:** Email Security Awareness: checking senders, domains, requests, attachments and embedded links
- **Topic 4:** Business Email Compromise Training: detecting executive, supplier and payment impersonation
- **Topic 5:** Online Scam Awareness: identifying fraudulent websites, QR codes, calls and social media messages
- **Topic 6:** AI-Enabled Phishing Awareness: deepfakes, voice cloning and highly personalised deception
- **Reflection & Review:** Analysing suspicious communications and explaining the safest response to each scenario

Day 3: Passwords, Accounts and Digital Identity

- **Topic 1:** Password Security Training: creating strong, unique and manageable credentials
- **Topic 2:** Password managers, passphrases and the risks of password reuse
- **Topic 3:** Multifactor Authentication Training: understanding authentication methods and login challenges
- **Topic 4:** MFA Awareness Training: recognising MFA fatigue, verification-code theft and approval scams
- **Topic 5:** Account Security Training: responding to unfamiliar logins and account compromise
- **Topic 6:** Identity Theft Awareness and Access Control Awareness in workplace environments
- **Reflection & Review:** Developing a personal account-protection plan based on secure access principles

AGILE LEADERS
Training Center

Day 4: Data, Devices and Secure Digital Work

- **Topic 1:** Data Protection Awareness Training: identifying personal, confidential and sensitive information
- **Topic 2:** Mobile Device Security Training: securing smartphones, tablets, applications and connections
- **Topic 3:** Remote Working Cybersecurity: protecting information outside the normal workplace
- **Topic 4:** Cloud Security Awareness: safe storage, permissions, links and external file sharing
- **Topic 5:** Secure Digital Collaboration through email, messaging, video meetings and shared workspaces
- **Topic 6:** Digital Security Training for software updates, backups, approved applications and removable media
- **Reflection & Review:** Evaluating a remote-working scenario and selecting appropriate security controls

Day 5: Malware, Incident Reporting and Cybersecurity Culture

- **Topic 1:** Recognising malware, ransomware, malicious downloads and unusual device behaviour
- **Topic 2:** Immediate employee actions following a suspicious click, attachment or information disclosure
- **Topic 3:** Cyber incident reporting: what to report, when to report it and what information to provide
- **Topic 4:** Protecting digital privacy, managing permissions and maintaining a professional digital identity
- **Topic 5:** Employee responsibilities, organisational policies and acceptable technology use
- **Topic 6:** Building a sustainable workplace cybersecurity culture through continuous awareness
- **Reflection & Review:** Consolidating key lessons and preparing a personal Cyber Hygiene Training action plan

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

No formal qualifications or technical cybersecurity experience are required. Participants should have basic familiarity with workplace devices, email and internet use. The course is designed for technical and non-technical employees and explains cybersecurity concepts in clear, practical language.

AGILE LEADERS
Training Center

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20-25 hours of instruction.

Is this course technical, and will participants learn to configure cybersecurity systems?

The course is an employee-focused Information Security Awareness Training programme rather than a technical cybersecurity administration course. Participants learn to recognise threats, protect information, secure accounts and respond appropriately to suspicious activity. Technical tools may be explained or demonstrated as examples, but system configuration and advanced security engineering are outside the course scope.

How This Course is Different from Other Cybersecurity Awareness Training Courses:

Cybersecurity Awareness Training: Digital Skills & Online Safety goes beyond presenting lists of cyber threats. It connects security awareness with the digital skills employees use every day, including searching for information, creating content, communicating online, sharing cloud files and using AI-supported tools. This integrated approach reflects DigComp 2.2, UNESCO's Digital Literacy Global Framework and the Essential Digital Skills Standards 2026.

The course places particular emphasis on human behaviour. Participants do not simply learn definitions of phishing, ransomware or identity theft; they analyse realistic messages, make decisions and practise appropriate reporting actions. Phishing Prevention Training, Business Email Compromise Training and AI-Enabled Phishing Awareness are presented through situations involving executives, suppliers, colleagues and customers.

The programme also addresses areas that traditional Cyber Security Awareness Courses may treat separately, including digital identity, information reliability, privacy settings, Secure Digital Collaboration, mobile devices and remote work. ENISA awareness principles are reflected through audience-relevant communication, repeated reinforcement and practical behavioural outcomes.

The course remains accessible to non-technical participants while providing sufficient workplace depth for managers and risk-sensitive departments. It does not promise or provide commercial security tools. Instead, participants receive objective insights, realistic examples, reference materials and practical checklists that help them use organisational technology more safely and responsibly.

AGILE LEADERS
Training Center

Training Course Categories

- Agile PM and Project Management Training Courses
- Agribusiness & Food Security Training Courses
- Aviation Management and Operations Training Courses
- Certified Courses By International Bodies
- Communication and Public Relations Training Courses
- Crisis Management and Business Continuity Training Courses
- Data Analytics Training and Data Science Courses
- Digital Government & Public Service Training Courses
- Education and Learning Development Training Courses
- Environment & Sustainability Training Courses
- Facilities and Real Estate Training Courses
- Finance and Accounting Training Courses
- Governance, Risk and Compliance Training Courses
- Healthcare Management Training Courses
- Heritage Conservation and Museum Management Training Courses
- Hospitality and Tourism Training Courses
- Human Resources Training and Development Courses
- IT Security Training & IT Training Courses
- Leadership and Management Training Courses
- Legal Training, Procurement and Contracting Courses
- Maintenance Training and Engineering Training Courses
- Marketing, Customer Relations, and Sales Courses
- NGO, Humanitarian and Development Management Training Courses
- Occupational Health, Safety and Security Training Courses
- Oil & Gas Training and Other Technical Courses
- Personal & Self-Development Training Courses

AGILE LEADERS
Training Center

Training Course Categories

- Quality and Operations Management Training Courses
- Secretarial and Administration Training Courses
- Shipping, Maritime and Ports Training Courses

AGILE LEADERS
Training Center

Training Cities

Abu Dhabi UAE	**Accra** Ghana	**Addis Ababa** Ethiopia
Amman Jordan	**Amsterdam** Netherlands	**Athens** Greece
Baku Azerbaijan	**Bali** Indonesia	**Bangkok** Thailand
Barcelona Spain	**Berlin** Germany	**Cairo** Egypt
Cape town South Africa	**Casablanca** Morocco	**Chicago** USA
Doha Qatar	**Dubai** UAE	**Frankfurt** Germany
Geneva Switzerland	**Istanbul** Turkey	**Jakarta** Indonesia
Johannesburg South Africa	**Kuala Lumpur** Malaysia	**Kuwait** Kuwait
Lagos Nigeria	**Langkawi** Malaysia	**Lisbon** Portugal
London UK	**Madrid** Spain	**Manama** Bahrain
Marbella Spain	**Milan** Italy	**Montreux** Switzerland
Munich Germany	**Muscat** Oman	**Nairobi** Kenya

AGILE LEADERS
Training Center

Training Cities

New York USA	**Nice** France	**Paris** France
Phuket Thailand	**Port Louis** Mauritius	**Porto** Portugal
Prague Czech Republic	**Rome** Italy	**San Diego** USA
Seoul South Korea	**Sharm El-Sheikh** Egypt	**Singapore** Singapore
Tashkent Uzbekistan	**Tbilisi** Georgia	**Tokyo** Japan
Toronto Canada	**Trabzon** Turkey	**Vienna** Austria
Zanzibar Tanzania	**Zoom** Online Training	**Zurich** Switzerland