COURSE BROCHURE

Cybersecurity Awareness

A foundation course that shows employees the cyber threats they meet every day and trains safe habits for email, passwords, data handling and devices.

Code	HT-IT-101
Category	IT & Cybersecurity
Duration	1 week
Level	Beginner
City	London

Introduction

Many cyber incidents begin with a simple action by a well-meaning employee: a click on a fake link, a reused password, or a file sent to the wrong person. That is why staff awareness stays the first line of defense.

Objectives

- Understand the main cyber threats aimed at employees and why they succeed
- Recognize phishing and social engineering attempts across different channels
- Protect accounts with strong passwords and multi-factor authentication
- Handle information and devices according to their sensitivity
- Report suspected incidents quickly and through the right channel

Who should attend

- Staff across departments who use email and business systems daily
- Reception and customer service staff handling outside contacts
- Executive assistants and office managers with access to sensitive information
- New employees as part of their onboarding program

Skills you will develop

- Phishing detection
- Safe password management
- Information classification and sharing
- Incident reporting

Learning Outcomes

- Analyze a suspicious message and name at least three signs that it is phishing
- Set up a strong passphrase and enable multi-factor authentication on a work account
- Decide the classification of a document and how to share it safely inside and outside the organization
- Submit a clear report on a suspected incident with the details the security team needs

Course Outline

Day 1: Cyber Threats in Plain Language

- Why attackers target people and not only systems
- Malware, ransomware and online fraud
- The value of the data each employee handles in daily work

Day 2: Phishing and Social Engineering

- Warning signs in phishing emails, text messages and phone calls
- Executive impersonation and requests to transfer money or change supplier details
- Checking links and attachments before opening them

Day 3: Passwords and Account Protection

- Passphrases and password managers
- Multi-factor authentication and how it stops account takeover
- Shared accounts and alerts about unusual sign-ins

Day 4: Data, Devices and the Workplace

- Classifying information and the rules for sharing and sending it
- Removable storage, printing and the clean desk policy
- Mobile phones, public Wi-Fi and remote work

Day 5: Reporting and Safe Habits

- When and how to report a suspected incident, and what not to do
- Social media and oversharing personal and work information
- Applied project: a safe-behavior checklist for the participant's own job, with a walkthrough of reporting a phishing message

Training methodology

Group inspection of sample phishing messages that hide their clues in the details
Hands-on comparison of weak passwords and strong passphrases
A walk through a mock office to spot information protection lapses
A reporting drill in which participants escalate a suspicious message to the security team

Certification

Participants receive a Harbor Training Center certificate of attendance on completing the course.

Upcoming dates

City	Dates	Language	Fee
London	7 – 11 December 2026	AR	EUR 5,800
London	7 – 11 June 2027	EN	EUR 5,800

Fees are per participant.

Contact us

Email info@harbor4training.com

Address istanbul Turkey

To register and for details, scan the code or visit:

https://harbor4training.com/en/courses/cybersecurity-awareness