ACE MULTIPASS
Cybersécurité - Méthodes agiles

TRAINING DATASHEET

Training Provider

Cybersecurity Awareness Training

A 4-hour course to learn the fundamentals of cybersecurity and adopt the right day-to-day habits, at work and at home, through hands-on, interactive workshops (Bitwarden, Have I Been Pwned, encryption...).

DURATION	PRICE	SCHEDULE
4 hours	**€450**	**4-hour session** *(morning or afternoon)*

OVERVIEW

This course provides the fundamentals of cybersecurity and helps participants adopt the right day-to-day habits, at work and at home. It presents the main high-risk situations as well as the essential best practices for limiting threats.

Participants work on password and account management through a Bitwarden workshop. Risks related to email and web browsing are addressed in a practical way, notably through a Have I Been Pwned workshop that raises awareness of data exposure.

Protecting the working environment is also covered, with best practices for workstation security, backups and data encryption, illustrated by a workshop.

Finally, the course covers electronic signatures, working on the go, the distinction between professional and personal use, and physical security issues.

A practical, interactive approach allows cybersecurity best practices to be applied immediately.

Note: this course can also be delivered in-house at your company's premises.

LEARNING OBJECTIVES

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

- Define and apply cybersecurity best practices on a daily basis.
- Identify the main risks to personal and professional data.
- Understand the impact of digital practices on personal and professional environments.
- Secure their accounts and passwords using a dedicated password manager.
- Detect whether their data has been exposed or compromised.
- Adopt safe habits when using email, the web and mobile devices.

- Implement simple data protection measures (backup, encryption).

TARGET AUDIENCE AND PREREQUISITES

Target population: Workers – Employees – Skilled employees – Managers – Senior managers.

Intended audience: anyone wishing to raise their awareness of cybersecurity.

Prerequisites: none.

PROGRAMME

Module 1 · Introduction & Concepts

- What's at stake
- The GDPR
- Cybersecurity concepts
- Vulnerabilities, threats and attacks

Module 2 · Risk Situations

- The delicate balance between productivity and security
- Phishing & social engineering
- Anatomy of an advanced attack
- Insider fraud
- Personnel security
- Unauthorized access breaches
- Viruses
- Denial of service (DDoS)
- BYOD (Bring Your Own Device)

Module 3 · Best Practices

- Passwords and accounts
- Email and web
- Strong authentication, YubiKey security keys

Workshop — Password manager.

Demo — Enabling two-factor authentication.

Workshop — Have I Been Pwned.

Module 4 · Protecting Your Computer

- Applications
- Updates
- Antivirus
- BIOS password
- Hardening

Module 5 · Backup & Encryption

- Disk encryption
- Backups
- Backup media

Workshop — 7-Zip.

Demo — Microsoft BitLocker.

Module 6 · Electronic Signatures

- Cryptography basics
- Symmetric and asymmetric algorithms
- Hash functions
- Certificates
- Cryptographic tokens
- Electronic signatures

Demo — Signing a PDF electronically with a smart card.

Module 7 · Working on the Go

- Public Wi-Fi
- Charging stations
- VPN
- Precautions when travelling

Module 8 · Professional vs Personal Use

Module 9 · Physical Security

- Photocopiers and printers
- Equipment security (privacy screens, anti-theft locks…)

Wrap-up — Interactive quiz to validate learning.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Each session can be adapted to the needs of people with disabilities. Participants concerned are invited to let us know before the start of the course so that we can examine possible arrangements together: room access conditions, adaptation of materials and teaching methods, or rescheduling of the session.

TEACHING AND TECHNICAL RESOURCES

Sessions are delivered using a variety of tools: audiovisual materials, documents handed out to trainees, practical exercises with their solutions for operational courses, and real-world case studies or lessons learned for more theoretical sessions.

At the end of each session, ACE-MULTIPASS gives trainees a satisfaction questionnaire, the results of which are then reviewed by the teaching team.

An attendance sheet is signed every half-day and handed in at the end of the course; a certificate of attendance is also issued to trainees who have attended the entire session.

TRAINER EXPERTISE

Our trainers are chosen for their expertise in the fields they teach. Each one is selected by our teaching team, which checks both their technical command of the subject and their ability to teach and lead a group. They generally have at least five to ten years of professional experience and hold or have held positions of responsibility in their sector.

ASSESSMENT METHODS

Throughout the course, the trainer measures trainees' progress through various exercises: multiple-choice questionnaires, role-plays or practical exercises.

A positioning test is also carried out before and after the course to measure the skills acquired by each participant.