+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 22/08/2025

Sign up

Cybersecurity training for all: best practices and digital hygiene

1 day (7 hours)

Presentation

Our "Cybersecurity for all: good practices and digital hygiene" training course is aimed at all employees who wish to understand digital risks and adopt the right reflexes on a daily basis to secure their professional uses.

You'll discover how to integrate good digital security practices into your business, from password management and terminal protection to detecting common threats and reacting in the event of an incident. We'll also look at the impact of new technologies, notably artificial intelligence, which are revolutionizing both attack methods (more credible phishing, identity theft, deepfakes) and defense solutions.

Over the course of the day, you'll learn how to recognize the most common threats, such as phishing, ransomware and identity theft, which now affect all business environments. You'll also learn how to protect your digital tools on a daily basis, from secure password management to updates, regular backups and best practices for all your digital equipment (PCs, laptops, smartphones, tablets).

The course will also guide you through the steps to take in the event of a suspected incident, so that you can react effectively without aggravating the situation. Finally, you'll discover how everyone can contribute to developing a genuine culture of cybersecurity within their organization, by sharing best practices and reinforcing collective vigilance.

At the end of the course, you'll be able to identify the main risks, strengthen your vigilance in the face of cyber-attacks and secure your day-to-day digital uses, while helping to spread best practices within your team and organization.

Objectives

- Understand the challenges of cybersecurity in a professional context.
- Identify the main IT threats and at-risk behaviors.
- Adopt best practices to ensure effective day-to-day digital hygiene.

Target audience

- Anyone wishing to learn about cybersecurity best practices.

Prerequisites

- No prerequisites

Program of our Cybersecurity training for all: best practices and digital hygiene

[Day 1 - Morning]

Introduction: why does cybersecurity concern everyone?

- Overview of the issues: costs of a breach, reputational impact, business continuity
- Real-life examples: recent attacks on SMEs, hospitals and local authorities
- Risks in everyday life (e-mail, web browsing, social networking, mobile use)
- Simple notions of governance and responsibility (who does what in a company?)
- Practical workshop: Deciphering cyber news and identifying the human errors involved.

Common threats and risky behavior

- Recognize the most common attacks: phishing, ransomware, identity theft, bogus technical support
- The most common human errors (untimely clicks, weak passwords, personal/pro use)
- The evolution of threats with AI: "intelligent" phishing, deepfakes and more credible impersonations
- Best practices to reduce risks (digital hygiene accessible to all)
- Practical workshop: Analysis of suspicious e-mails (with real examples), sorting between legitimate and phishing e-mails.

[Day 1 - Afternoon]

Adopting good digital hygiene

- Good everyday habits
- Password management (MFA, password safe)
- Regular backups and updates
- Terminal security (PCs, smartphones, tablets)
- Access management and locking of workstations
- Good mobility practices (public Wi-Fi, telecommuting)
- Practical workshop: Setting up your "10 personal cybersecurity rules".

Reacting effectively to an incident

- Recognizing warning signals
- What to do (and what not to do) in the event of a suspected attack?
- Alert and escalation procedures in a professional environment
- Case study: Simulation of a phishing attack. Individual and collective reaction, debriefing.

Creating a cyber culture at work

- Sharing best practices with colleagues
- Integrate cyber security into your daily routine
- Collective approach: cyber ambassadors, regular reminders
- Anticipate developments: remain vigilant in the face of new digital uses and the growing exploitation of AI by attackers
- Stay up to date: consult simple alerts (ANSSI, CNIL, CERT-FR simplified), follow internal company communications, use awareness-raising media (posters, newsletters, short video clips).

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.

Training organization registered under number 11 75 54743 75. This registration does not constitute government approval.
Ambient IT 2015-2025. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg