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

Updated 03/27/2025

Sign up

Digital security training

1 day (7 hours)

Presentation

Our training course on securing your digital practices will teach you all you need to know about the challenges of good CyberSecurity practices in companies, as well as the various regulations governing personal data.

These days, laws governing the protection of personal data are multiplying. Whether it's to protect companies from cyberthreats or to safeguard consumers' rights, it's crucial to know what's at stake and what regulations govern the market.

Our training program will teach you not only theoretical knowledge of cyber vigilance and personal data management, but also practical skills in using tools to protect your IT equipment and in acquiring good practices to adopt on a daily basis.

Objectives

- Understanding the challenges of CyberSecurity in the enterprise
- Raising awareness of the regulatory framework (RGPD)
- Identify the main IT risks (phishing, ransomware, human vulnerabilities, etc.).
- Implementing good safety practices
- Use simple, effective tools to secure digital equipment and exchanges
- Prevent and manage the risks associated with digital attacks (identify the players and the right reflexes to adopt in the event of an attack)
- Disseminate and develop appropriate safety reflexes in daily activities

Target audience

- Anyone working in a professional environment
- Anyone with an infrastructure to protect
- Anyone handling personal data

Prerequisites

- General computer skills

Program of our training course on securing digital practices (Cybersecurity / RGPD)

Cybersecurity challenges for businesses

- Why Cybersecurity is a major issue for companies of all sizes (increase in cyberattacks and impact on business)
- Cybercrime: the international threat increases tenfold with AI
- Possible consequences of a lack of safety vigilance (financial losses, production , legal sanctions, negative image)
- Useful glossary (CNIL, ANSSI, RSSI, DPO, BYOD, Blue / Red Team, logs, etc.)
- The role of each employee in Cybersecurity: individual behavior can protect or endanger the company
- Key statistics
- A look back at high-profile incidents (retail, healthcare, telecoms...)
- Practical workshop: Case study of a real cyberattack, analysis by participants of the mistakes made and discussion of solutions to avoid them in the future.

Regulatory framework (RGPD)

- Fundamental principles of the RGPD (General Data Protection Regulation)
- Purpose of personal data protection
- Legal obligations for companies and users' rights (access, rectification, deletion of data)
- Best practices for day-to-day RGPD compliance
- Risks in the event of non-compliance
- Opening and quick presentation of NIS2, DORA, and Cyber Resilience Act (CRA)
- Practical workshop: Setting up a fictitious company where certain practices do comply with the RGPD. Identify non-compliances and propose corrective measures.

Good safety practices in everyday life

- Adopt a strong password policy
- Securing your work equipment (PC, smartphone) with tools
- Best practices for e-mails and attachments
- Protect sensitive company data
- Best practices when teleworking or travelling
- Practical workshop: Training in best practices.

Use of simple cybersecurity tools

- Basic protection tools
  - antivirus
  - personal firewall
  - automatic updates (OS, Firmware, Drivers)
  - Encryption and backup policy
- Use a password manager
- Two-factor authentication (2FA)
- Secure web browsing (VPN)
- Secure data exchange (e.g. Signal)
- Cyber Threat Intelligence
- Practical workshop: Building a checklist of best practices
- Opening up to more advanced techniques (IAM, Zero Trust, CDN, etc.)

Risk prevention and cyberthreats

- Overview of cybermalveillance.gouv.fr (the French government portal) & ANSSI
- Identify today's main cyber threats:
  - phishing
  - ransomware
  - malware (viruses, spyware)
  - social engineering attacks.
- Understanding the methods used by attackers
- Apply preventive measures on a daily basis
- How to react when in doubt
- Alert CERT-FR
- Practical workshop: Threat simulation, collective analysis a fictitious phishing email received by an employee, to identify the signs of a scam and decide what action to take (deletion, reporting).

Developing the right safety reflexes

- Integrate safety into your work routine
- Strengthening the company's safety culture and training its teams
- Presentation of the ANSSI MOOC
- Maintain acquired good habits over the long term
- Practical workshop: Interactive conclusion, final quiz covering the key points of the training, followed by a discussion in which each participant describes a safety reflex that he or she undertakes to apply on a daily basis.

Companies concerned

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

Positioning on entry to training

Positioning on entry to training complies with Qualiopi quality criteria. As soon as enrolment is confirmed, the learner receives a self-assessment questionnaire enabling us to

assess their estimated level of proficiency in different types of technology, and their expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or internal security difficulties within the company (intra-company or virtual classroom) that 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, brainstorming sessions and group work.

Validation

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

Sanction

A certificate will be issued to each trainee who completes the course.