



**Training sheet**  
**Cybersecurity awareness**

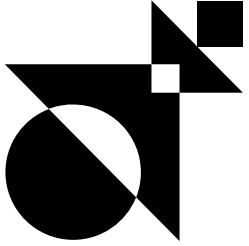
**CONTACT FOR THIS TRAINING**

Miora RAHARINIRINA  
Almond Institute coordinator  
almond.institute@almond.eu  
07 64 42 71 56

→ Version 1.0

→ 08/12/2023

## Course overview



This training aims to make your teams aware of computer risks and their consequences. This module presents the techniques commonly used by hackers, while popularizing the subject for a non-technical audience. It details the best practices to adopt to protect against most attacks.

01. ■

Understand **the most common cybersecurity risks**

02. ■

Acquire **the best practices in terms of security**

03. ■

**Detect and react** to the signs of a cyber attack

## Useful informations

### Who should attend?

- Anyone in an organization who needs to use the information system: workstation, e-mail, smartphone. The course is designed to be accessible to all, with no prior knowledge of IT.

### Entry requirements

- No prerequisites

### Method of assessment

**Production of a final online questionnaire** covering all the concepts learned.

### How and when to access

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

**Registration requests can be sent up to 10 working days before the start of the training.**

### To go further

This training course is a preparation for the following training course:

- Risk Fundamentals

### Accessibility

Whether you are recognized as having a disability or not, making our training accessible to everyone is part of our commitment. If you need compensation or adaptation for the content, the supports, the "venue", the material used, the schedules, the rhythm, **we are at your disposal.**

## Face-to-face and distance learning

### Course curriculum

Introduction – Cybersecurity stakes	Equipment weakness	Security for mobile devices	Weak passwords	Malware	Social engineering
<ul style="list-style-type: none"><li>→ The multiplication of attacks and their impact</li><li>→ Important data leaks</li><li>→ CNIL sanctions</li><li>→ Received ideas</li><li>→ The impact of a security incident</li><li>→ Attacker typology</li><li>→ The black market in vulnerabilities"</li></ul>	<ul style="list-style-type: none"><li>→ Risks of USB equipment</li><li>→ Recommendations</li></ul>	<ul style="list-style-type: none"><li>→ The risks of nomadism</li><li>→ Data encryption</li><li>→ Data erasure</li><li>→ Recommendations</li></ul>	<ul style="list-style-type: none"><li>→ Types of password attacks</li><li>→ Examples of massive data leaks</li><li>→ Recommendations</li></ul>	<ul style="list-style-type: none"><li>→ Internal network security</li><li>→ Antivirus</li><li>→ Updates</li><li>→ Recommendations"</li></ul>	<ul style="list-style-type: none"><li>→ How to detect it?</li><li>→ Fraud by email, telephone, to the president</li><li>→ Recommendations</li></ul>

### Training benefits

- Training by an expert in offensive security who has carried out numerous intrusion tests.
- Operational recommendations

### Price and informations



- **Duration:** 2 hours
- **Price:** Contact us
- **Financing:** OPCO support