Digital and artificial intelligence

Cybersecurity Awareness

A half day so that every employee recognises the most common attacks and knows what to do: phishing email, fake call from an executive, fraudulent request to change bank details, rigged USB stick, ransomware. Examples are drawn from company situations, good habits stay simple and the session ends with your company's reporting procedure.

Duration : 0.5 day

Objectives

1. Recognise a fraudulent email, message or call
2. Apply the basic rules: strong passwords, a password manager, two-factor authentication
3. Explain how ransomware enters a company and what limits the damage
4. Protect company information when travelling, working remotely and on social media
5. Report an incident or a doubt without delay, following the internal procedure

Programme

Half day

• Why attackers target employees: phishing, identity theft, CEO fraud, fake bank detail changes

• Exercise: spotting the clues in a series of genuine and fake emails

• Passwords, two-factor authentication, updates, USB sticks and personal devices

• AI assistants and information leaks: what must never be copied into an online tool

• What to do in case of doubt or incident, the company's reporting procedure, final quiz

Teaching methods

• Reconstructed examples of fraudulent emails and messages

• Interactive quiz throughout the session

• Role play: the urgent call from a fake supplier asking to change its bank details

• Can be delivered in French or Darija for field teams

• A one-page reflex card handed to each participant

Assessment and documents

Final knowledge quiz and end-of-course survey the next day. Numbered certificate, verifiable online, for each participant; training report handed to the company, with the questions that caused the most difficulty.

Bilingual materials for every participant; each classroom course comes with its digital twin on OmniLearn.

Good to know

A short format that can be scheduled for several successive groups, including shift teams. For the rules on personal data, see “Personal Data: Law 09-08 and CNDP”.

Practical information

Duration	0.5 day
Audience	All employees who use a computer, email or a work phone
Prerequisites	No prerequisites
Group size	Groups of 6 to 12 participants, in-company
Format	In-company, face to face on your site
Language	French, Darija or English; bilingual materials
Funding	OFPPT special training contracts (TFP), GIAC, Maroc PME: we prepare the applications with you, at no extra cost.
Programme customisation	Programme adapted to your procedures, your equipment and your audience

Frequently asked questions

Do I need IT knowledge?

No. The session is for any employee who uses email, a computer or a work phone. No technical term is used without being explained with an example.

Does the course replace technical protections?

No, it complements them. Antivirus, filtering and backups reduce risk, but a large share of attacks go through an employee who clicks, replies or forwards. The session works on that link.

How does it differ from the ISO/IEC 27001:2022 course?

ISO/IEC 27001:2022 is for people who build or audit an information security management system. This half day is for all employees and covers everyday good habits.