L'AKADÉMIE DU DIGITAL · TRAINING PROGRAMME Qualiopi certification being prepared

Parcours Cyber Essentiels

PF-CYBER-P2 · Cybersecurity & Compliance

Les réflexes essentiels pour se protéger, déjouer les fraudes et respecter la protection des données

DURATION
21 heures — 3 modules de 7h

PRICE
1?147,50 € HT

AUDIENCE
Companies & individuals

ACCESS
Access within 2 working days after validation of needs and prerequisites.

Remise parcours ?15 % incluse. Tarif indicatif, applicable à partir de 2 participants ; pour une formation à titre individuel hors session, nous contacter.

Main objective

Donner à tout collaborateur ou petite organisation un socle complet et accessible de cybersécurité : adopter les bons réflexes d'hygiène numérique, savoir déjouer les tentatives de manipulation et de phishing, et comprendre les obligations essentielles de protection des données personnelles.

Le parcours progresse des bons réflexes d'hygiène numérique (initiation) vers la résistance aux manipulations (ingénierie sociale & phishing), puis la conformité des données (RGPD) — du comportement individuel à la responsabilité collective.

Learning objectives

- Comprendre les menaces numériques courantes et appliquer les bonnes pratiques d'hygiène numérique
- Repérer et déjouer les tentatives d'ingénierie sociale et de phishing
- Comprendre les principes du RGPD et les obligations essentielles de protection des données
- Réagir et signaler correctement en cas d'incident ou de doute

Target audience

- Tout collaborateur, quel que soit son niveau technique
- Salariés, indépendants, responsables associatifs et personnels administratifs
- Fonctions exposées (accueil, administratif, comptabilité, RH, commercial)
- TPE et particuliers souhaitant sécuriser leurs usages

Prerequisites

- Une utilisation régulière de la messagerie et des outils numériques du quotidien suffit. Aucune compétence technique préalable n'est exigée. Un formulaire de pré-requis spécifique est associé à chaque module composant

le parcours.

Programme

FOR-CYBER-M1-A · Initiation à la Cybersécurité (7h)

Théorie : enjeux, panorama des menaces, vocabulaire (menace/risque/vulnérabilité), bonnes pratiques. Atelier : auto-diagnostic, analyse de phishing, checklist d'hygiène numérique, plan d'action.

Objective : Comprendre les risques et adopter les bons réflexes d'hygiène numérique.

Assessment : Évaluation formative + checklist + plan d'action + quiz final. Réussite ? 60 %.

FOR-CYBER-M4-A · Ingénierie Sociale & Phishing (7h)

Théorie : leviers psychologiques, panorama des techniques (phishing, vishing, smishing…), signaux d'alerte. Atelier : analyse de faux messages, jeu de rôle, fiche réflexe, mini-campagne de sensibilisation.

Objective : Comprendre et déjouer les manipulations humaines de la cyberfraude.

Assessment : QCM + analyse de cas + fiche réflexe + plan de sensibilisation. Réussite ? 60 %.

FOR-CYBER-M2-A · RGPD – L'essentiel (7h)

Théorie : principes, bases légales, droits des personnes, DPO/CNIL, violations. Atelier : registre des traitements, qualification, analyse de conformité, plan d'action.

Objective : Comprendre et appliquer la protection des données.

Assessment : QCM + registre + analyse de conformité + plan d'action. Réussite ? 60 %.

Teaching methods and resources

En présentiel dans nos locaux ou dans vos locaux. Parcours organisé en 3 modules de 7h, séquençables selon le calendrier.

- Les stagiaires doivent disposer d'un PC avec le Wifi (16 Go de RAM recommandés pour le module d'initiation).
- 5 à 6 places par session.
- Tarifs applicables à partir de 2 participants ; pour une formation à titre individuel hors session, nous contacter.

Assessment methods

Learning outcomes are assessed during and at the end of the training; an attendance certificate is given to every learner.

Accessibility

Training accessible to people with disabilities. Contact us before registering so we can study the adjustments needed.

Funding

Quote or training agreement on request. Qualiopi certification is being prepared: eligibility for OPCO funding will open once it is obtained.

Certification audit planned for T1 2027. No OPCO eligibility before it is obtained.
