L’AKADÉMIE DU DIGITAL · PROGRAMME DE FORMATION Certification Qualiopi en cours de préparation

Initiation à la Cybersécurité

FOR-CYBER-M1-A · Cybersécurité & Conformité

Comprendre les bases et les appliquer

DURÉE
7 h

TARIF
450 € HT

PUBLIC
Entreprises & particuliers

DÉLAI D’ACCÈS
Accès sous 2 jours ouvrés après validation du besoin et des prérequis.

Tarifs indiqués « à partir de », hors devis spécifique et promotions. Prix HT, à partir de 2 participants. TVA 20 %.

Objectifs pédagogiques

- Comprendre les enjeux de la cybersécurité dans la vie personnelle et professionnelle
- Comprendre les principales menaces numériques : phishing, ransomware, usurpation d'identité, malware, fuite de données, ingénierie sociale
- Comprendre les notions de risque, menace, vulnérabilité, attaque et donnée sensible
- Appliquer les bonnes pratiques essentielles d'hygiène numérique
- Renforcer la sécurité de ses comptes, appareils et usages numériques
- Réagir de manière adaptée en cas de suspicion d'incident cyber
- Construire un plan d'action simple pour améliorer sa sécurité numérique

Public concerné

- Salariés d'entreprise, dirigeants, indépendants, responsables associatifs
- Personnels administratifs et utilisateurs réguliers d'outils numériques
- Particuliers souhaitant sécuriser leurs usages personnels
- Apprenants ou étudiants découvrant les enjeux cyber

Prérequis

Les participants doivent savoir utiliser un ordinateur ou un smartphone, utiliser régulièrement une messagerie électronique, naviguer sur Internet et disposer d'une expérience basique des outils numériques du quotidien (comptes en ligne, fichiers, mots de passe, applications, navigateur web). Aucune compétence préalable en informatique, réseau ou cybersécurité n'est exigée. Ces éléments sont validés par un formulaire en ligne et / ou un entretien préalable.

- Savoir utiliser un ordinateur ou un smartphone.
- Utiliser régulièrement une messagerie électronique et naviguer sur Internet.

- Disposer d'une expérience basique des outils numériques du quotidien (comptes, fichiers, mots de passe).
- Aucune compétence préalable en informatique, réseau ou cybersécurité n'est exigée.

Programme

THÉORIE Module Théorique — Comprendre les risques cyber et les bons réflexes

Ce premier module introduit les notions fondamentales de la cybersécurité et permet de comprendre pourquoi la sécurité numérique concerne tout le monde, dans la sphère personnelle comme professionnelle. Il aborde les principales menaces du quotidien (phishing, ransomware, usurpation d'identité, arnaques en ligne, fuite de données, logiciels malveillants, ingénierie sociale) à travers des exemples simples et concrets. Les recommandations s'appuient notamment sur les ressources de l'ANSSI et de Cybermalveillance.gouv.fr.

Objectif : comprendre les risques numériques courants et identifier les bons réflexes à adopter pour limiter les incidents cyber dans un contexte personnel ou professionnel.

- Approche accessible à un public non technique, avec des exemples du quotidien (email, smartphone, cloud, réseaux sociaux, banque en ligne).
- Vulgarisation du vocabulaire cyber : menace, vulnérabilité, risque, attaque, donnée sensible.
- Identification des signaux d'alerte d'une tentative de fraude ou de phishing.
- Introduction aux bonnes pratiques : mots de passe robustes, MFA, sauvegardes, mises à jour, vigilance face aux liens et pièces jointes.

Évaluation : évaluation formative : questions orales de compréhension, exercices de reformulation, identification de situations à risque, quiz intermédiaire et correction collective.

Accueil & présentation	15 min	Présenter le programme, les objectifs et le déroulé. Présentation orale, support visuel (slides), tour de table.	
Pourquoi la cybersécurité ?	40 min	Enjeux personnels et professionnels ; conséquences d'un incident. Exposé interactif, exemples concrets, échanges.	Questions orales de compréhension.
Panorama des menaces	1h00	Phishing, ransomware, usurpation, malware, fuite de données, ingénierie sociale. Exposé illustré, exemples réels, ressources ANSSI / Cybermalveillance.	Identification de situations à risque.
Vocabulaire cyber	45 min	Menace, vulnérabilité, risque, attaque, donnée sensible. Exposé, exercices de reformulation, échanges participatifs.	Exercices de reformulation.
Bonnes pratiques essentielles	40 min	Mots de passe robustes, MFA, sauvegardes, mises à jour, vigilance liens/pièces jointes. Exposé, démonstrations, signaux d'alerte du phishing.	Quiz intermédiaire.
Synthèse & correction	10 min	Résumer les points clés ; correction collective. Récapitulatif, correction collective, feedback.	Correction collective des acquis.

ATELIER Atelier Pratique — Construire son hygiène numérique

Ce second module est un atelier pratique consacré à l'application des bonnes pratiques. Les participants réalisent un auto-diagnostic de leurs usages numériques, analysent des situations concrètes de phishing et construisent un plan d'action personnel ou professionnel. Les recommandations sur les mots de passe et l'authentification multifacteur s'appuient notamment sur les ressources de la CNIL. Aucun vrai mot de passe ou identifiant personnel n'est demandé pendant l'atelier.

Objectif : mettre en pratique les bons réflexes de cybersécurité et construire une checklist d'hygiène numérique applicable immédiatement après la formation.

- Atelier concret et orienté action : auto-diagnostic des pratiques numériques.
- Analyse de faux emails de phishing et repérage des signaux suspects.
- Construction d'une checklist d'hygiène numérique et priorisation des actions.
- Élaboration d'un plan d'action individuel ou professionnel, dans le respect de la confidentialité.

Évaluation : évaluation pratique : grille d'auto-diagnostic complétée, analyse de cas de phishing, checklist d'actions prioritaires, plan d'action final, restitution orale courte et quiz final de validation.

Lancement de l'atelier	15 min	Présenter l'objectif : une checklist d'hygiène numérique. Présentation, rappel de confidentialité (aucun vrai mot de passe).	
Auto-diagnostic	45 min	Évaluer ses propres usages numériques. Grille d'auto-diagnostic, travail individuel, accompagnement.	Grille d'auto-diagnostic complétée.
Analyse de phishing	1h00	Analyser de faux emails et repérer les signaux suspects. Étude de cas de phishing, repérage collectif des indices.	Analyse de cas de phishing.
Checklist & priorisation	45 min	Construire une checklist et prioriser les actions. Atelier de construction, matrice impact/facilité.	Checklist d'actions prioritaires.
Plan d'action & restitution	35 min	Élaborer un plan d'action et le présenter. Modèle de plan d'action, restitution orale courte, feedback.	Plan d'action final + quiz final.
Enquête de satisfaction	10 min	Recueillir la satisfaction à chaud. Questionnaire de satisfaction.	Enquête de satisfaction.

Modalités et moyens pédagogiques

Formation en présentiel dans nos locaux ou dans vos locaux, en groupe restreint. Alternance d’apports théoriques, d’ateliers pratiques et de mises en situation.

Matériel requis :

16 Go de Ram

Modalités d’évaluation

Évaluation des acquis en cours et en fin de formation, attestation de fin de formation remise à chaque stagiaire.

Accessibilité

Formation accessible aux personnes en situation de handicap. Contactez-nous avant l’inscription pour étudier les aménagements nécessaires.

Financement

Devis ou convention de formation sur demande. La certification Qualiopi est en cours de préparation : l’éligibilité aux financements OPCO sera ouverte après son obtention.

Audit de certification prévu au T1 2027. Aucune éligibilité OPCO avant l’obtention.