

Sensibilisation à la cybersécurité

Durée

1 heure

Modalité

100 % distanciel

Disponibilité

3 mois à partir de la première connexion

Langues

Français

Objectifs

- Identifier les principales cybermenaces (phishing, ransomware, ingénierie sociale) et reconnaître les signaux d'alerte
- Adopter au quotidien les bons réflexes de sécurité numérique : mots de passe, mises à jour, navigation, télétravail
- Réagir efficacement en cas d'incident ou de doute, et savoir qui alerter au sein de l'entreprise

Prérequis

- Aucun prérequis technique en informatique n'est nécessaire
- Maîtrise du français, à l'oral et à l'écrit

Public cible

- Tous les collaborateurs de l'entreprise, quel que soit leur poste
- Managers et encadrants, fonctions administratives, télétravailleurs, nouveaux arrivants, dirigeants

Financement

- OPCO, dans certains cas
- Plan de développement des compétences de l'entreprise
- Autofinancement

Accessibilité

- Étude au cas par cas des situations de handicap — nous contacter

Programme

I. Piratage informatique, protégez votre entreprise

- Comprendre les enjeux du piratage informatique pour l'entreprise
- Identifier les objectifs des pirates : vol de données, vol d'argent, blocage des systèmes, chantage
- Adopter les bons réflexes pour limiter les risques

II. Reconnaître un email de phishing / frauduleux

- Distinguer attaques de masse et attaques ciblées
- Repérer les signaux d'un email ou d'un message frauduleux
- Adopter les bons réflexes de vigilance au quotidien

III. Bonnes pratiques pour un mot de passe solide

- Construire un mot de passe fort (longueur, complexité)
- La phrase de passe : une méthode simple et efficace
- Ne jamais réutiliser ni partager ses mots de passe

IV. Gérer ses mots de passe

- Authentification unique : usages et précautions
- Le gestionnaire de mots de passe (coffre-fort numérique)
- Double authentification et autres mécanismes de sécurisation

V. Protection des données personnelles et professionnelles

- Comprendre les cyberattaques et leurs conséquences pour l'entreprise
- Sécuriser les données personnelles et professionnelles au quotidien
- Adopter les bons réflexes en cas d'attaque

VI. RGPD

- Comprendre le Règlement Général sur la Protection des Données
- Ce qui change pour les utilisateurs et pour les entreprises
- Pourquoi le RGPD est essentiel

VII. Le ransomware

- Comprendre le fonctionnement d'un rançongiciel
- Les bonnes pratiques pour s'en prémunir
- Réagir efficacement en cas d'attaque

VIII. Être prudent avec le nomadisme

- Les risques liés aux périphériques et appareils connectés
- Séparer usages personnels et professionnels
- Sécuriser ses déplacements numériques

IX. L'intelligence artificielle et la cybersécurité

- Utiliser l'IA en toute sécurité au quotidien
- Vérifier les informations produites par une IA
- Se prémunir contre les usages malveillants de l'IA (phishing, deepfakes vocaux)

Modalités d'évaluation

- Évaluation continue tout au long de la sensibilisation
- QCM de validation des acquis en fin de parcours
- Délivrance d'une attestation de suivi de sensibilisation
- Bilan individuel du niveau de sensibilisation acquis

Méthodes mobilisées

- Apports théoriques et pratiques
- Informations essentielles et repères concrets
- Supports vidéos illustrant des cas concrets