Programme de Formation

HYGIENE CYBER POUR COLLABORATEUR

Organisation

Durée : 7 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

Tout collaborateur utilisant un poste informatique, un smartphone professionnel ou accédant à des documents numériques, quel que soit son secteur d'activité.

Objectifs pédagogiques

- Comprendre les menaces numériques qui touchent les organisations.
- Adopter les bons réflexes de sécurité au quotidien.
- Savoir réagir efficacement en cas d'incident cyber.

Description

Introduction

- pourquoi la cybersécurité concerne tous les secteurs, évolution des cybermenaces, rançongiciels, vols de données et fraudes, lien avec les activités quotidiennes, outils numériques, échanges de documents et mobilité

Panorama des menaces : Comprendre les principales attaques

- Phishing, ransomware, vol de données et usurpation d'identité, ingénierie sociale et fraudes aux virements

Règles d'hygiène numérique au quotidien : les bons réflexes sur son poste de travail

- bons réflexes sur poste de travail, mobile et internet, gestion des mots de passe et authentification multi-facteur, détection des mails frauduleux, bonnes pratiques sur smartphones et tablettes, gestion des supports externes, clés USB et disques durs

Sécurité des équipements et environnements de travail

- protection des outils numériques, objets connectés, capteurs IoT et solutions embarquées, risques liés aux accès des prestataires et sous-traitants

Réagir face à un incident : que faire en cas de cyberattaque ?

- reconnaissance des signaux d'alerte, gestes réflexes, prévenir, isoler et garder son calme, conduite à tenir en cas de cyberattaque, procédures et bonnes pratiques

Construire une culture sécurité : la cybersécurité est l'affaire de tous

- la cybersécurité comme responsabilité collective, importance du signalement des comportements suspects, communication interne et rôle des référents sécurité, exercice pratique, élaboration collective d'une checklist hygiène cyber, cas concret de propagation d'un ransomware suite à un mail non signalé

Bilan de la formation

- synthèse des acquis et rappels des bonnes pratiques

Prérequis

- Être utilisateur d'un poste informatique ou mobile professionnel.
- Savoir naviguer sur internet et consulter des mails.

- Aucune compétence technique en cybersécurité n'est requise.

Modalités pédagogiques

- Alternance de méthode expositive et démonstrative, mises en situation actives, temps de réflexivité, questions/réponses, application et démonstration.
- Postes informatiques, supports pédagogiques numériques, objets connectés utilisés dans le cadre des mises en situation.

Moyens et supports pédagogiques

- Support vidéo, autoformation sur plateforme informatique
- Diaporama
- Livret de formation
- QCM.

Modalités d'évaluation et de suivi

- Évaluation de la progression,
- Manipulation encadrée d'outils et objets connectés,
- Remise d'une attestation de formation.

Informations sur l'admission

Cette formation ne nécessite **aucun prérequis de diplôme**. Une expérience professionnelle en lien avec la thématique est recommandée pour optimiser l'apprentissage.

Pour toute question sur les conditions d'admission, contactez notre équipe :
07 52 64 73 30 — ✉ contact@clem-formation.fr

Informations sur l'accessibilité

CLEM CERTIFICATION s'engage pour l'**accessibilité des formations aux personnes en situation de handicap**. Nos locaux sont accessibles aux personnes à mobilité réduite.

Un **référent handicap** est disponible pour étudier avec vous les aménagements nécessaires.
07 52 64 73 30 — ✉ contact@clem-formation.fr