Programme de Formation

CYBER REFLEXES : SE PROTEGER SOI-MEME, PROTEGER SON ENTREPRISE

Organisation

Durée : 7 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

- Collaborateur , Dirigeant
- Toute personne utilisant un poste informatique, un smartphone professionnel ou accédant à des documents numériques.

Objectifs pédagogiques

À l'issue de la formation, les participants seront capables de :

- Identifier les principales menaces cyber
- Appliquer les règles d'hygiène numérique au quotidien
- Adopter les bons réflexes face à une situation à risque
- Réagir de manière adaptée en cas d'incident de cybersécurité

Description

Accueil et présentation

- Présentation des objectifs de la formation
- Recueil des attentes et présentation des participants

Pourquoi la cybersécurité concerne votre entreprise

- Attaques récentes dans le secteur (rançongiciels, vols de plans,
- fraudes)
- Liens avec les pratiques professionnelles (échanges numériques)
- Exercice : identification des risques cyber du quotidien

Panorama des principales menaces

- Phishing, ransomware, vol de données, usurpation d'identité
- Ingénierie sociale et fraudes aux virements
- Études de cas concrets

Règles d'hygiène numérique au quotidien

- Bonnes pratiques sur poste de travail, mobile et Internet
- Mots de passe, MFA, gestion des mails et supports externes
- Exercices pratiques et mises en situation

Sécurité des dossiers et équipements connectés

- Protection des outils et équipements connectés
- Gestion des accès des sous-traitants
- Atelier collaboratif

Réagir face à un incident

- Reconnaître les signaux d'alerte
- Gestes réflexes à adopter

- Jeux de rôle et cas concrets

Construire une culture sécurité

- Responsabilité collective
- Signalement des comportements à risque
- Élaboration d'une checklist Hygiène Cyber

Bilan de la formation

- Échanges, synthèse et questionnaire de satisfaction

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
- Mise en situation (active), temps de réflexivité, questions/réponses, application, démonstration.

Moyens et supports pédagogiques

- Supports vidéos;
- Diaporama;
- Livrets;
- Supports de cours.

Modalités d'évaluation et de suivi

- Évaluation de la progression
- Utilisation des 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