Sensibilisation à la Cybersécurité

OBJECTIFS PEDAGOGIQUES :

- Comprendre les différents types de menaces en cybercriminalité
- Identifier les risques majeurs pour son entreprise
- S'acculturer aux bonnes pratiques
- Reconnaître les menaces numériques
- Mettre en place des bonnes pratiques de cybersécurité
- Utiliser des outils simples et efficaces pour sécuriser leurs appareils et échanges numériques.
- Développer des réflexes sécuritaires adaptés pour prévenir et réagir en cas de cyberattaque.
- Mettre en œuvre une charte informatique à partager en interne

Public visé :
Tout public

Prérequis :
Ordinateur équipé d'une connexion stable

Durée :
7h/ 1 jour

Méthodes pédagogiques :

- Adaptation de la formation au niveau d'expérience des participants
- Alternance de contenus théoriques et d'exercices pratiques
- Un ordinateur par stagiaire avec logiciel installé
- Mise en situation, exercices réflexifs, travail de groupe…

Modalités :
Formation en Distanciel ou présentiel

Suivi et Evaluation :
Contrôle continu (Exercices,quizz...)
Émargement feuille de présence
Certificat de réalisation

Tarif Inter :
445€ net de taxes par personne
(Min 4 à 10 stagiaires)
Tarif Intra :
(Min 1 à 10 stagiaires)
Nous consulter

Délai d'accès :
D'une semaine à 2 mois, selon le type de financement

Contact :
contact@envoll.fr
04 42 92 29 72

Accessibilité :
Cliquez ici

Programme

Introduction

- Accueil inclusif
- Présentation du déroulé de la formation
- Présentation/tour de table des participants : leur entreprise/service, leur métier, leur expérience, leur formation initiale, leur(s) besoins et attentes

1. Les enjeux de la cybersécurité et menaces actuelles

- Apports théoriques
- Présentation interactive : panorama des cyberattaques.
- Étude de cas récents (PME touchée).

2. Comprendre et anticiper les cyberattaques

- Détection phishing/ransomware.
- Analyse d'un email suspect en sous-groupes.
- Discussion sur les réflexes (ne pas cliquer, vérifier).

3. Les bonnes pratiques de cybersécurité au quotidien

- Créer un mot de passe fort (ex. "Boulangerie2025!")
- Activer l'authentification à deux facteurs (MFA) sur Gmail
- Sécuriser un Wi-Fi (changer mot de passe par défaut)
- Gérer les accès (ex. limiter droits sur PC partagé)

4. Prévenir et réagir face à une cyberattaque

- Rédiger un plan de réponse (ex. "1 : déconnecter PC, 2 : contacter expert").
- Gérer un ransomware avec actions immédiates (éteindre, signaler).
- Discussion sur les priorités (sauvegarde, alerte)

Conclusion

- Évaluation de la satisfaction
- Modalité de suivi post-formation
- Bilan et clôture de la formation