Cybersécurité : maîtriser les règles de base

OBJECTIFS DE LA FORMATION

• Comprendre les concepts fondamentaux de la cybersécurité.
• Identifier les principales menaces et vulnérabilités.
• Apprendre les meilleures pratiques de sécurité informatique.
• Acquérir des compétences de base en protection des données et gestion des incidents de sécurité.

INFORMATIONS

Durée : 1 jour / 7h

Horaires : 9h - 12h30 / 13h30 - 17h00

Nombre de participants : 3 à 10

Réf : 2500

POUR QUI

• Employés utilisant des systèmes informatiques dans leur travail quotidien
• Toute personne voulant apprendre à se protéger numériquement

PROGRAMME

Matin

1- Concepts fondamentaux et menaces
• Définition de la cybersécurité.
• Importance de la cybersécurité dans le monde actuel.
• Exemples de cyberattaques célèbres.

2 - Principales menaces de cybersécurité
• Malware (virus, vers, chevaux de Troie, ransomware).
• Phishing et ingénierie sociale.
• Attaques par déni de service (DoS/DDoS).
• Intrusions et attaques de réseau.

3 - Vulnérabilités et expositions courantes
• Vulnérabilités logicielles (failles de sécurité dans les logiciels).
• Vulnérabilités matérielles (problèmes liés aux périphériques physiques).
• Erreurs humaines (mauvaises pratiques et erreurs d'utilisation).

4 - Sécurité des réseaux
• Concepts de base des réseaux (LAN, WAN, VPN).
• Protocoles de sécurité (SSL/TLS, HTTPS).
• Firewalls et systèmes de détection/prévention des intrusions (IDS/IPS).

Après-midi

5 - Meilleures pratiques de sécurité
• Gestion des mots de passe (création, stockage, gestion).
• Sécurisation des dispositifs (ordinateurs, smartphones, tablettes).
• Mise à jour et patching des systèmes et logiciels.

6 - Protection des données
• Chiffrement des données (au repos, en transit).
• Sauvegarde et récupération des données.
• Règles et réglementations (RGPD, HIPAA).

7 - Introduction à la gestion des incidents
• Détection et réponse aux incidents de sécurité.
• Processus de gestion des incidents (identification, confinement, éradication, récupération).
• Plan de réponse aux incidents et rôles des membres de l'équipe.

8 - Cas Pratiques et simulations
• Études de cas réels de cyberattaques.
• Simulations de scénarios d'attaques et réponses.
• Exercices de groupe pour identifier et réagir aux incidents.