Salarié·es cybervigilant·es

Les contenus seront adaptés en fonctions des besoins et spécificités de chaque groupe.

Publics : salarié·es utilisant des appareils numériques dans leur travail
Prérequis : si non francophone, niveau B1 minimum
Durée : 18h, 3 jours

Cette formation s'adresse aux salarié·es utilisant des appareils numériques dans leur travail.

Objectifs généraux :

- **Participer** à la sécurité informatique de son entreprise
- **Avoir confiance** dans ses comportements numériques
- **Prévenir** les cyber-risques

Objectifs opérationnels :

- Développer ses capacités d'analyse des risques numériques
- Apprendre les bonnes pratiques de sécurité informatique
- Mieux utiliser ses appareils digitaux

Contenus :

Partie 1 : Etat des lieux

1. Les principales cyberattaques contre les entreprises
2. Les principales conséquences d'une attaque réussie

Partie 2 : Développer ses compétences de détection

1. L'ingénierie sociale : la faille de sécurité la plus importante
2. L'hameçonnage ou le phishing
3. Différencier une donnée personnelle et une donnée sensible
4. Les sites web frauduleux
5. Les fichiers vérolés : analyser les processus anormaux sur son PC

Partie 3 : Les bonnes pratiques de cybersécurité

1. Faire les mises à jour « facultatives », du système d'exploitation, et d'applications/logiciels
2. Installer des logiciels/applications de manière sécurisée
3. La question de l'antivirus
4. Techniques pour avoir des mots de passe uniques, robustes et s'en souvenir
5. Gérer les spams
6. Sécuriser ses sauvegardes et appareils connectés
7. Acheter et partager sur internet grâce aux données chiffrées
8. Paramétrer sa visibilité sur le web
9. Les bons comportements en cas de soupçon d'intrusion

Méthode, spécificités et outils pédagogiques :

- Alternance d'apports théoriques et d'exercices pratiques
- Matériel : ordinateurs, tablettes, imprimante/scanner…
- Supports : dossier papier GO-ON formation, application GO-ON formation, présentation PowerPoint…