

Salarié·es cybervigilant·es

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

Public : Salarié·es utilisant des appareils numériques dans leur travail

Prérequis : si non francophone, niveau B1 minimum

Durée : 18h - 3 jours

Les objectifs généraux

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

Les objectifs opérationnels

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



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...

Programme:

- **Partie 1 : Etat des lieux**
 - Les principales cyberattaques contre les entreprises
 - Les principales conséquences d'une attaque réussie
- **Partie 2 : Développer ses compétences de détection**
 - L'ingénierie sociale : la faille de sécurité la plus importante
 - L'hameçonnage ou le phishing
 - Différencier une donnée personnelle et une donnée sensible
 - Les sites web frauduleux
 - Les fichiers vérolés : analyser les processus anormaux sur son PC
- **Partie 3 : Les bonnes pratiques de cybersécurité**
 - Faire les mises à jour « facultatives », du système d'exploitation, et d'applications/logiciels
 - Installer des logiciels/applications de manière sécurisée
 - La question de l'antivirus
 - Techniques pour avoir des mots de passe uniques, robustes et s'en souvenir
 - Gérer les spams
 - Sécuriser ses sauvegardes et appareils connectés
 - Acheter et partager sur internet grâce aux données chiffrées
 - Paramétrer sa visibilité sur le web
 - Les bons comportements en cas de soupçon d'intrusion