

Cybersécurité au quotidien : les bons réflexes à adopter

3 heures et 30 minutes

Programme de formation

Public visé

Salariés TPE

Pré-requis

Aucun prérequis technique spécifique. Être utilisateur basique d'un ordinateur et de la messagerie suffit. Une sensibilisation minimale aux risques numériques est un plus.

Objectifs pédagogiques

- Comprendre les enjeux et les principales menaces numériques.
- Identifier les principaux risques numériques dans son environnement de travail
- Adopter les bons réflexes de sécurité informatique au quotidien
- Expérimenter des situations réalistes pour renforcer la vigilance.

Description / Contenu

Activité 1 - Introduction à la cybersécurité

- Chiffres clés : statistiques sur les cyberattaques en TPE/PME
- Panorama des menaces : phishing, ransomware, fuites de données, erreurs humaines
- Contexte réglementaire

Activité 2 - Cartographie des risques

- Identification des risques possibles dans le quotidien professionnel (mot de passe, Wi-Fi, mobilité, partage de données)
- Discussion guidée autour des pratiques actuelles et des vulnérabilités
- Introduction des bonnes pratiques (gestion des accès, MFA, sauvegardes, cloisonnement réseau)

Activité 3 - Les réflexes de sécurité informatique

- Mettre en pratique les réflexes de sécurité via des scénarios réalistes
- Lister les bonnes pratiques



Modalités pédagogiques

Approche interactive et ludique privilégiée. Alternance d'apports théoriques et de mises en pratique.

Jeu de rôle / serious game via des scénarios inspirés du quotidien d'une entreprise fictive (carte d'incident, quiz en équipe, mini-énigmes de type escape game).

Moyens et supports pédagogiques

- Support de type "diaporama"
- Jeu type escape game
- Accès aux ressources liées à l'actualité sur notre site internet bakertilly.fr

Modalités d'évaluation et de suivi

- Un questionnaire de positionnement en amont et après la formation
- Quiz final
- Enquête de satisfaction