CYBERSÉCURITÉ & BONNES PRATIQUES NUMÉRIQUES

Durée :	Public :	Prérequis :	Modalité :
1 jour	Tout le personnel	Bases informatiques et messagerie	Intra-entreprise

OBJECTIFS PÉDAGOGIQUES

→ Comprendre les principales cybermenaces qui pèsent sur les entreprises
→ Adopter les bons réflexes face au phishing, ransomware et ingénierie sociale
→ Gérer ses mots de passe et ses données numériques de manière sécurisée
→ Appliquer la politique de sécurité numérique de l'entreprise au quotidien

DÉROULÉ PÉDAGOGIQUE

01 PANORAMA DES CYBERMENACES

→ Phishing, spear phishing, ransomware, usurpation d'identité numérique
→ Exemples d'attaques réelles subies par des PME françaises
→ Coûts et conséquences d'un incident cyber pour l'entreprise

02 BONNES PRATIQUES AU QUOTIDIEN

→ Mots de passe robustes : longueur, complexité, gestionnaires dédiés
→ Mises à jour, antivirus, pare-feu et sauvegardes régulières
→ Wi-Fi public, appareils personnels (BYOD) et clés USB inconnues

03 RÉGLEMENTATION & SIGNALEMENT

→ RGPD : obligations de l'entreprise et droits des salariés
→ Procédure interne de signalement d'un incident de sécurité
→ Ressources officielles : cybermalveillance.gouv.fr, ANSSI

MOYENS PÉDAGOGIQUES & ÉVALUATION

→ Quiz interactif de sensibilisation et cas pratiques d'attaques simulées
→ Supports de sensibilisation et affiche bonnes pratiques remis
→ Formateur expert cybersécurité

Évaluation de fin de stage — Quiz de validation des connaissances en fin de stage

V1 — Avril 2026 — Document non contractuel, programme susceptible d'adaptation selon les besoins.