

Caractéristiques

Durée : 1 jour
Modalité : présentiel
Niveau : débutant
Type : professionnalisation
Taux de satisfaction : NP*

Méthodes pédagogiques

- Pédagogie par objectif
- Alternance de pédagogie par exposé et de pédagogie participative sur cas pratiques professionnels
- Productions individuelles

Modalités d'évaluation

- Évaluation et régulations individualisées
- Questionnaire d'évaluation et certificat de stage

Moyens et supports

- Salles à définir suivant la demande (quantité, géolocalisation)
- Postes de travail en réseau sous Windows 10 Pro ou ultérieur
- Kit de vidéo projection ou grand écran connecté
- Supports de cours et d'exercices papiers et/ou numériques
- Supports complémentaires possibles par Internet
- Formateur professionnel de plus de 5 ans d'expérience et/ou expert de Bac+3 à Bac +7

Tarif

- Pour connaître les tarifs de la formation en Inter, en Intra et nos délais d'accès à cette formation, merci de nous contacter

Accessibilité aux personnes handicapées

- En cas de formation réalisée en présentiel les locaux seront garantis accessibles aux PMR. Pour d'autres handicaps, nous contacter pour la mise en place des moyens de compensation
- Contactez notre référent PSH (Tél 0262 81 87 90)

Objectifs

- Sensibiliser aux risques numériques les plus courants.
- Promouvoir une culture de cybersécurité accessible à tous.
- Apprendre à détecter, éviter et réagir aux menaces.

Prérequis

- Aucun prérequis technique.
- Être utilisateur régulier d'un poste de travail, email, internet.

Public concerné

- Tout collaborateur, quelle que soit sa fonction, utilisant des outils numériques.
- Idéal pour des équipes non techniques : administratif, RH, communication, commerce, etc.

Programme

Introduction à la cybersécurité (0,75H)

- Pourquoi la cybersécurité concerne tout le monde ?
- Exemples concrets d'attaques réussies (cas d'entreprise, phishing).
- Chiffres clés et impacts.

Panorama des menaces (1H)

- Phishing, ransomwares, faux sites, fuites de données.
- Démonstration de cas réels ou simulés.
- Quiz interactif : vrai/faux sur les idées reçues.

Bonnes pratiques numériques (1,75H)

- Créer et gérer des mots de passe solides.
- Activer l'authentification à deux facteurs.
- Mise à jour des logiciels, gestion des accès.
- Reconnaître les signes d'un mail ou d'un site douteux.

Utilisation sécurisée des outils pro/perso (1,25H)

- Travailler à distance en sécurité (VPN, Wi-Fi public, cloud).
- Séparer les usages pro/perso, sécuriser les smartphones.

Réagir à un incident (1H)

- Qui prévenir ? Que faire ?
- Procédures internes et premiers réflexes.
- Limiter les impacts.

Quiz & mise en situation (1,25H)

- Scénarios ludiques : simulation de mail frauduleux, gestion d'un incident.
- Quiz de fin + rappel des messages clés.
- Échanges libres, partage d'expériences.