

Protéger vos Données

(Durée estimée : 0h45)

Objectifs

- Identifier et classifier les différents types d'informations confidentielles au travail (données des employés, de l'entreprise et des clients).
- Distinguer clairement les concepts de confidentialité et de vie privée au sein de l'environnement professionnel.
- Appliquer les mesures de protection fondamentales pour empêcher la fuite de données et le vol d'identité.
- Créer, sécuriser et mémoriser des mots de passe robustes et difficiles à compromettre.
- Comprendre et configurer l'authentification multifacteur (MFA) pour sécuriser l'accès aux comptes numériques.
- Sécuriser l'utilisation des appareils portables (smartphones, PC portables) et des supports de stockage amovibles (clés USB, disques durs externes).
- Adopter les bons réflexes de sécurité physique pour protéger les locaux, les équipements et les actifs de l'entreprise contre les menaces intentionnelles et non intentionnelles.

Contenu de la formation

INTRODUCTION

- Qu'est-ce qu'une donnée confidentielle ? Définir ce qu'est une donnée confidentielle. Identifier les différents types de données sensibles : Données des collaborateurs. Données de l'entreprise. Données des clients. Comprendre les risques liés à la divulgation d'informations.
- Comment protéger les informations confidentielles ? Adopter les bonnes pratiques de protection des données. Différencier confidentialité et vie privée. Prévenir les fuites de données et le vol d'identité. Réagir correctement en cas d'incident de sécurité.

BONNES PRATIQUES DE CYBERSÉCURITÉ

- Créer et gérer des mots de passe robustes Comprendre les caractéristiques d'un mot de passe sécurisé. Utiliser un gestionnaire de mots de passe. Éviter les erreurs courantes. Mettre en place de bonnes habitudes de gestion des identifiants.
- Guide de l'authentification multifacteur (MFA) Comprendre le principe de la MFA. Découvrir les différents facteurs d'authentification. Configurer la MFA sur les principaux services. Reconnaître les tentatives de contournement.
- Sécuriser les appareils portables et les supports amovibles Protéger les ordinateurs portables et smartphones. Sécuriser les clés USB et les disques externes. Chiffrer les données sensibles. Adopter les bonnes pratiques lors des déplacements.
- Assurer la sécurité physique des locaux et des équipements Contrôler l'accès aux locaux. Protéger les postes de travail. Prévenir les intrusions et les vols. Adopter les bons réflexes face aux risques physiques.

CONCLUSION

- Synthèse Récapitulatif des notions essentielles. Les réflexes à adopter au quotidien. Les erreurs les plus fréquentes à éviter. Ressources utiles pour aller plus loin.

Moyens pédagogiques

- Parcours e-learning structuré en modules progressifs.
- Apports théoriques illustrés par des exemples concrets.
- Vidéos pédagogiques explicatives.
- Supports de cours numériques consultables en ligne.
- Quiz d'auto-évaluation tout au long de la formation.
- Synthèses et rappels des notions essentielles.
- Possibilité de revoir les contenus autant de fois que nécessaire.

Moyens techniques

- Plateforme de formation e-learning accessible 24h/24 et 7j/7.
- Connexion Internet requise.
- Ordinateur, tablette ou smartphone compatibles.
- Navigateur web récent (Chrome, Edge, Firefox, Safari).
- Lecteur audio et vidéo intégré à la plateforme.
- Suivi automatique de la progression et des résultats aux quiz.
- Accès sécurisé à l'espace personnel de formation.

Modalités d'encadrement

- Formation réalisée en autonomie.
- Assistance technique disponible en cas de difficulté d'accès.
- Suivi de la progression assuré par la plateforme.

Evaluation des acquis

Quiz final permettant de mesurer l'acquisition des compétences visées.

Pré-requis

- Aucun prérequis en cybersécurité n'est nécessaire.
- Savoir utiliser un ordinateur, une tablette ou un smartphone et naviguer sur Internet.
- Disposer d'un équipement connecté à Internet permettant d'accéder à la plateforme de formation.
- Comprendre le français à l'oral et à l'écrit.

Public visé

- Salariés du secteur public ou privé souhaitant acquérir les fondamentaux de la cybersécurité.
- Agents de collectivités territoriales, administrations et établissements publics.
- Toute personne utilisant un ordinateur, une messagerie électronique ou des outils numériques dans le cadre de son activité professionnelle.
- Débutants ne disposant d'aucune connaissance préalable en cybersécurité.

Tarif

150 € HT

Tarif indicatif. Nous consulter pour un devis personnalisé.

Modalités d'accès

INTRA entreprise

Délais d'accès

1 jour(s) ouvré(s)

Accessibilité

Formation accessible aux personnes à mobilité réduite en présentiel ou en classe virtuelle. Pour plus de précision, nous contacter.

Contact

Campus26 — Cité numérique du Pensio, 4 rue du PNDF, 43000 Le Puy-en-Velay

Téléphone : 04 15 49 00 03

Courriel : contact@campus26.com

Mise à jour du programme : 13/10/2026