IDEPRO FORMATION
Développeur de compétences

DEVELOPPER LES BONNES PRATIQUES EN MATIERE DE CYBERSECURITÉ

Objectifs de la formation :

- Comprendre l'importance de la cybersécurité pour protéger l'entreprise.
- Adopter un comportement responsable pour sécuriser les données et prévenir les incidents.
- Réduire les risques de sécurité en appliquant des pratiques sécurisées.
- Renforcer la résilience face aux cybermenaces pour protéger les informations sensibles.
- Encourager des habitudes durables en matière de sécurité numérique.

Public visé : Salariés de tous niveaux : tous les employés de l'entreprise, indépendamment de leur fonction ou de leur niveau de responsabilité, car chaque membre peut contribuer à renforcer la sécurité de l'information.
Niveau requis : Tous les utilisateurs ayant accès au système d'information via un poste informatique.

Modalités
Groupe : 6 personnes maximum.
Attestation : en fin de formation.
Formateurs : Expert en sécurité de l'information
Moyens pédagogiques : vidéoprojecteur, ordinateurs portables, supports de formation.

Délai d'accès : Inscription par mail- Au plus tard 15 Jours avant le démarrage de la session

Durée : 0,5 jour – 4 heures en présentiel

Méthodes pédagogiques : Nous alternerons plusieurs méthodes expositives mais surtout actives avec des apports techniques, de synthèses, des études de cas, des exercices et des mises en situations.

Modalités Évaluation :

- Des évaluations formatives des acquis en cours, et en fin de formation, Exercices pratiques, études de cas.
- Une évaluation sommative via un questionnaire de satisfaction à la fin de la formation.

V1-1 – MAJ 02/2025

PROGRAMME

1 - Identifier les menaces de cybersécurité :

Savoir reconnaître les différentes formes de menaces (phishing, ransomware, attaques de malware, etc.) qui peuvent affecter l'entreprise.

2 - Adopter des pratiques sécurisées au quotidien

Intégrer les bonnes pratiques dans les usages professionnels et personnels (gestion des mots de passe, mise à jour des logiciels, vigilance face aux e-mails suspects, etc.).

3 - Assurer une protection proactive de l'information

Comprendre et mettre en œuvre des comportements permettant de sécuriser les données sensibles de l'entreprise.

4 - Promouvoir une culture de cybersécurité :

Être capable de sensibiliser et d'encourager ses collègues à adopter les bonnes pratiques pour renforcer la sécurité collective.

Durant la formation :

Démonstrations en temps réel : présentation d'exemples concrets en direct, tels que des attaques de phishing ou de malware simulées, pour montrer comment ces menaces se manifestent et les réactions appropriées. Ces démonstrations aident les participants à mieux comprendre le fonctionnement des cybermenaces et les mesures de protection.

Simulations et mises en situation : exercice de simulation de phishing, identification d'e-mails frauduleux, et exercices de gestion des mots de passe pour sensibiliser aux attaques courantes et permettre aux participants de réagir face aux cybermenaces.

Discussions et partages d'expériences : séances d'échanges où les participants peuvent partager leurs propres expériences et discuter des bonnes pratiques. Cela permet de renforcer la sensibilisation par des exemples concrets et de créer une dynamique d'apprentissage collectif.

NOUS CONTACTER

contact@idepro formation.com
06 92 61 53 28
02 62 92 06 91
idepro formation.com