IDEPRO FORMATION
Développeur de compétences

SÉCURITÉ NUMÉRIQUE : PRÉPARER LES DIRIGEANTS AUX ENJEUX CYBER

Objectifs de la formation :

- Sensibiliser les dirigeants aux cybermenaces qui les ciblent spécifiquement.
- Identifier et comprendre les types d'attaques ciblées et leurs impacts.
- Mettre en place des pratiques de cybersécurité adaptées et réagir efficacement en cas de compromission.
- Favoriser une culture de vigilance et sensibiliser l'organisation aux risques.

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 - Identification des menaces ciblant les dirigeants :
Reconnaître les techniques d'ingénierie sociale et d'attaques spécifiques qui visent les cadres et dirigeants (ex. : spear-phishing, whaling, menaces internes).

2 - Développement de comportements cyber-sécurisés :
Adopter des pratiques rigoureuses et des comportements appropriés pour réduire les risques de compromission des comptes et des informations sensibles.

3 - Réponse aux incidents :
Savoir réagir en cas de compromission, notamment en alertant les équipes appropriées et en assurant la continuité d'activité.

4 - Sensibilisation à l'ingénierie sociale :
Comprendre les techniques de manipulation employées par les attaquants pour inciter les dirigeants à divulguer des informations ou à accéder à des ressources critiques.

Durant la formation :

Étude de cas sur de cyberattaques ciblant les dirigeants : présentation de cas réels d'attaques de haut niveau ayant compromis des dirigeants pour illustrer les techniques employées par les cybercriminels et l'importance d'une vigilance accrue.

Démonstrations d'attaques d'ingénierie sociale : simulation de spear-phishing et d'usurpation d'identité pour sensibiliser les dirigeants à la manière dont ils peuvent être ciblés et à l'importance de la détection.

Atelier pratique sur la sécurité personnelle et numérique : atelier pour appliquer des mesures de protection renforcées, comme la double authentification, la gestion des mots de passe et l'usage de moyens de communication sécurisés.

NOUS CONTACTER

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