
Programme de Formation

Sécurité informatique : Sensibilisation des collaborateurs aux cybermenaces

Description

Formation pratique pour identifier les menaces, adopter les bons réflexes et sécuriser efficacement son activité numérique grâce à une approche pratique et opérationnelle.

Points Forts

Formation immersive basée sur des cas réels et des mises en situation concrètes pour ancrer durablement les bons réflexes et permettre aux utilisateurs de sécuriser leur environnement dès le retour en poste.



Public visé

- Tous les utilisateurs ayant accès au système d'information de leur entreprise via un poste informatique



Objectifs pédagogiques

- Être sensibilisés aux menaces informatiques auxquelles vous pouvez être directement confrontés dans votre activité professionnelle et privée
- Comprendre les problématiques liées à la sécurité informatique
- Comprendre pourquoi la prévention est nécessaire
- Prendre conscience du rôle que vous avez à jouer
- Adopter les bonnes attitudes et réflexes
- Participer à la mise en oeuvre des solutions exposées et veiller à leur application

Organisation

Durée : 7 heures

Mode d'organisation : Mixte

Contenu pédagogique



Description

La sécurité informatique : comprendre les menaces et les risques

- Introduction : Cadre général, qu'entend-on par sécurité informatique ?
- Analyse des risques, des vulnérabilités et des menaces
- Comment une négligence peut créer une catastrophe ?

Les hackers

- Sociologie des pirates, réseaux souterrains et motivations
- Quelles sont leurs cibles ?
- Quelles sont leurs armes ?

Loi et sécurité informatique

- Le cadre législatif de la sécurité
- Les responsabilités civile et pénale des responsables et des salariés de l'entreprise
- Les responsabilités civile et pénale des pirates



- Le rôle de la CNIL et son impact pour la sécurité en entreprise
- Le règlement intérieur à l'entreprise et les chartes informatiques

Les notions techniques

- Les composantes d'un SI et leurs vulnérabilités : systèmes d'exploitation client et serveur
- Réseaux d'entreprise (locaux, site à site, accès par Internet)

L'authentification de l'utilisateur

- Contrôles d'accès : authentification et autorisation
- Pourquoi l'authentification est-elle primordiale ?
- Qu'est-ce qu'un bon mot de passe ?

La protection de l'information et la sécurité du poste de travail

- Vocabulaire : confidentialité, signature et intégrité
- Comprendre les contraintes liées au chiffrement
- Schéma général des éléments cryptographiques
- Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles : la problématique des ordinateurs portables et des téléphones portables
- Comment gérer les failles de sécurité : le port USB, le rôle du firewall et de l'antivirus
- Accès distant via Internet : comprendre les VPN, qu'est-ce qu'un serveur proxy ?
- L'intérêt d'une DMZ
- Réseaux sans fil et mobilité. Les applications à risques : Web, messagerie ...
- Les risques du cloud

Conclusion

- La sécurité au quotidien. Les bons réflexes.



Prérequis

- Un questionnaire de positionnement sera réalisé au préalable pour adapter la formation à vos besoins



Modalités pédagogiques

- Exercices concrets
- Cas pratiques
- Quiz d'évaluation des connaissances



Moyens et supports pédagogiques

- Mise à disposition de postes de travail
- Vidéoprojecteur, tableau blanc, supports numériques
- Documentation pédagogique numérique



Modalités d'évaluation et de suivi

- Positionnement en amont de la formation :
 - Un quiz de consolidation des pré-requis sera administré en amont de la formation
- Suivi « pendant » :
 - Feuilles de présence
 - Exercices pratiques
 - Évaluation « fin de formation »
 - Évaluation des acquis en fin de formation
 - Formulaire d'évaluation de la formation
- Évaluation à froid :
 - Suivi post-formation : Questionnaire de satisfaction à j+30