Sécurité SI, sensibilisation des utilisateurs

★★★★★

PL-48 **1 Jours (7 Heures)**

Description

Faire connaître les risques et les conséquences d'une action utilisateur portant atteinte à la sécurité du système d'information. Expliquer et justifier les contraintes de sécurité imposées par la politique de sécurité. Découvrir et comprendre les principales parades mises en place dans l'entreprise.

À qui s'adresse cette formation ?

Pour qui

Tous les utilisateurs ayant accès au système d'information via un poste informatique.

Prérequis

Aucune

Les objectifs de la formation

- Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles
- Identifier les mesures de protection de l'information et de sécurisation de son poste de travail
- Favoriser la conduite de la politique de sécurité SI de l'entreprise

Programme de la formation

La sécurité informatique : comprendre les menaces et les risques

- Introduction : Cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ? Comment une négligence peut créer une catastrophe.
- Quelques exemples.
- La responsabilité.
- Les composantes d'un SI et leurs vulnérabilités.
- Systèmes d'exploitation client et serveur.
- Réseaux d'entreprise (locaux, site à site, accès par Internet).
- Réseaux sans fil et mobilité.
- Les applications à risques : Web, messagerie .
- Base de données et système de fichiers.
- Menaces et risques.
- Sociologie des pirates.
- Réseaux souterrains.
- Motivations.
- Typologie des risques.
- La cybercriminalité en France.
- Vocabulaire (sniffing, spoofing, smurfing, hijacking.
-).

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.
- Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ? Le port USB.
- Le rôle du firewall client.

L'authentification de l'utilisateur et les accès depuis l'extérieur

- Contrôles d'accès : authentification et autorisation.
- Pourquoi l'authentification est-elle primordiale ? Le mot de passe traditionnel.
- Authentification par certificats et token.
- Accès distant via Internet.
- Comprendre les VPN.
- De l'intérêt de l'authentification renforcée.

Comment s'impliquer dans la sécurité du SI

- Analyse des risques, des vulnérabilités et des menaces.
- Les contraintes réglementaires et juridiques.
- Pourquoi mon organisme doit respecter ces exigences de sécurité.
- Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.
- Agir pour une meilleure sécurité : Les aspects sociaux et juridiques.
- La CNIL, la législation.
- La cybersurveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.
- La sécurité au quotidien.
- Les bons réflexes.
- Conclusion.