Sécurité informatique - Sensibilisation des utilisateurs

1 j (7 heures) Ref : SISU

Public

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

Pré-requis

Aucun

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Exposés, cas pratiques, synthèse
Assistance post-formation pendant trois mois
Vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

Catalogue de formation OCAPIAT :

- Inscription en présentiel à Toulouse

Objectifs

Etre 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

Programme détaillé

LA SECURITE 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 SECURITE 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 SECURITE 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.