Former et sensibiliser les utilisateurs à la sécurité informatique

Ref : 4-SE-WIND

Prochaines dates

Aucune date pour le moment

Durée : 1 jour(s)

Objectifs

Etre sensibilisé aux menaces informatiques auxquelles les collaborateurs peuvent être directement confrontés dans leur activité professionnelle et privée
Comprendre les problématiques liées à la sécurité informatique
Comprendre en quoi la prévention est nécessaire
Adopter les bonnes attitudes et réflexes
Savoir mettre en ?uvre les solutions concrètes proposées

Pré-requis

Toute personne concernée par une démarche sécurité au sein de l?entreprise

Plan de cours

La sécurité et l'entreprise
Quelques exemples concrets de piratage
Facteurs techniques : système, logiciel, réseau, web, données
Facteur humain
Identifier la valeur : Ce qu'il n'est pas « grave » de perdre, Quels sont les biens à protéger ?
Les moyens pour garantir une meilleure sécurité
A quoi sert une charte d'utilisation des ressources informatiques ?

Loi et sécurité informatique
Le cadre législatif de la sécurité
Les responsabilités civile et pénale
Le rôle de la CNIL et son impact pour la sécurité en entreprise
Le règlement intérieur.
Synthèse : charte morale,interne / loi

Les mots de passe
Ce que l'on peut faire avec le mot de passe d'autrui
Qu'est-ce qu'une attaque par dictionnaire ?
Pourquoi peut-on être forcé de respecter une stratégie de nomenclature ?
Ne pas confondre la base de compte locale et celle du serveur
Les devoirs et comportements à adopter vis-à-vis des tiers.
Les comportements à l'intérieur de l'entreprise.
Les comportements à l'extérieur de l'entreprise.

Les périphériques et le poste de travail
Les risques encourus avec les périphériques USB, CD, DVD
Le poste de travail pour Windows (C :, D :, E :, ...)
Disque interne/externe, clé USB, réseau : quelles différences pour les risques ?
Exemple de propagation de virus par clef USB
Les réflexes à adopter avec les « corps étranger »

Comprendre les bases du réseau
(20 minutes seulement sur ce module)
Chaque équipement (PC, Serveur, ...) dispose d'une adresse IP
Vocabulaire réseau de base (passerelle, DNS, DHCP)
Chaque application est référencée par un numéro (port)

Que fait un firewall d'entreprise ?
Et ce qu'il ne fait pas à la place des utilisateurs ...
Risques liés à l'accueil du portable d'un visiteur dans l'entreprise
Intérêts d'utiliser un serveur Proxy en entreprise pour accéder au Web

Comportement par rapport à la messagerie
Le mail un simple fichier texte ?
La réception des messages (SPAM, faux messages...)
Le mauvais usage de la retransmission des messages
Les courriers électroniques de taille importante
L'usurpation d'identité

Risques liés à Internet
Navigation et surprises !
Les problèmes liés au téléchargement de fichiers
Limites de l'ultra protection des navigateurs
Peut-on « rattraper » une information divulguée ?
La téléphonie utilise maintenant les réseaux de données

Synthèse et conclusion
Synthèse des points abordés
Savoir évaluer les risques

Règles de bonnes conduites