Sécurité SI, Sensibilisation des Utilisateurs

Code : SE02 **Durée** : 1 jour **Classe** : Présentiel / à distance

Public

- Cette formation sécurité informatique s'adresse à toute personne concernée par une démarche sécurité au sein de l'entreprise.

Prérequis

- AUCUN

Objectifs

- Etre sensibilisés de manière interactive et créative aux menaces informatiques auxquelles ils peuvent être directement confrontés dans leur activité professionnelle et privée
- Comprendre les problématiques liées à la sécurité informatique
- Comprendre pourquoi la prévention est nécessaire
- Prendre conscience du rôle qu'ils ont à jouer
- Adopter les bonnes attitudes et réflexes
- Etre force de proposition pour participer à la mise en oeuvre des solutions exposées et veiller à leur

Programme détaillé

1-La sécurité et l'entreprise

- Quelques exemples concrets de piratage
- Les « briques » concernées par la sécurité (système, logiciel, réseau, web, données)
- Et bien sûr le facteur humain (développé durant toute la formation) ...
- 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 ?

2- Loi et sécurité informatique

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

3- 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.

Sécurité SI, Sensibilisation des Utilisateurs

Code : SE02 **Durée** : 1 jour **Classe** : Présentiel / à distance

4- 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 étrangers »

5- Comprendre les bases du réseau

- 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

6- Inventaire du matériel et des logiciels

- L'automatisation de la remontée d'information
- Comparaison des deux plugins Fusion Inventory et OCS Inventory NG
- Installation de Fusion Inventory sur les clients
- Gestion des équipements « identiques » (gabarit)

7- 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

8- 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

9- Quelques démonstrations :

- L'automatisation de la remontée d'information
- Comparaison des deux plugins Fusion Inventory et OCS Inventory NG
- Installation de Fusion Inventory sur les clients
- Gestion des équipements « identiques » (gabarit)

10- Synthèse et conclusion

- Synthèse des points abordés