

## FORMER ET SENSIBILISER LES UTILISATEURS À LA SÉCURITÉ INFORMATIQUE

<b>Durée</b>	<b>1 jour</b>	<b>Référence Formation</b>	<b>4-SE-WIND</b>
--------------	---------------	----------------------------	------------------

### 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 œuvre les solutions concrètes proposées

### Participants

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

### Pré-requis

Pas de prérequis spécifiques

### Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours.

### PROGRAMME

#### 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 civiles et pénales
- 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



**CAP ÉLAN FORMATION**

[www.capelanformation.fr](http://www.capelanformation.fr) - Tél : 04.86.01.20.50

Mail : [contact@capelanformation.fr](mailto:contact@capelanformation.fr)

Organisme enregistré sous le N° 76 34 0908834  
version 2024