# Former et sensibiliser les utilisateurs à la sécurité informatique

*Mise à jour : Fév. 2024*

**Durée :** 1 jour - 7 heures

**OBJECTIFS PÉDAGOGIQUES**

- 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

**PRÉREQUIS**

- Pas de prérequis spécifiques

**PARTICIPANTS**

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

**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

**MODALITÉS D'ÉVALUATION**

- Feuille de présence signée en demi-journée
- Evaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

**MOYENS TECHNIQUES EN PRÉSENTIEL**

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

**MOYENS TECHNIQUES DES CLASSES À DISTANCE**

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants reçoivent une invitation avec un lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

**ORGANISATION**

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

**PROFIL FORMATEUR**

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

**ACCESSIBILITÉ**

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

# Programme de formation

**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

**Règles de bonnes conduites**