

# PROGRAMME DE FORMATION

## Former et sensibiliser les utilisateurs à la sécurité informatique

### Organisation

---

Mode d'organisation : Présentiel ou distanciel

Durée : 1 jour(s) · 7 heures

### Contenu pédagogique

---



#### Type

Action de formation



#### Public visé

Toute personne concernée par une démarche sécurité au sein de l'entreprise  
Cette formation est accessible aux publics en situation de handicap et aux personnes à mobilité réduite. Des aménagements peuvent être prévus en fonction des profils. Nous contacter pour plus d'information.

#### Prérequis

Pas de prérequis spécifiques



#### 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



#### Description

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



## Modalités pédagogiques

Réflexion de groupe et apports théoriques du formateur – Travail d'échange avec les participants sous forme de discussion – Utilisation de cas concrets issus de l'expérience

professionnelle – Exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique – Remise d'un support de cours complet pour référence ultérieure



## Moyens et supports pédagogiques

Accueil des apprenants dans une salle dédiée à la formation. Chaque participant disposera d'un ordinateur (si besoin), d'un support de cours, d'un bloc-notes et d'un stylo. La formation se déroulera avec l'appui d'un vidéoprojecteur et d'un tableau blanc.



## Modalités d'évaluation

### Avant la formation :

Nous mettons en place une évaluation de chaque participant via un questionnaire d'évaluation des besoins et de niveau.

Un audit complémentaire peut-être proposé pour parfaire cette évaluation

### Pendant la formation :

Des exercices pratiques (études de cas, jeux de rôle, questionnaires, quiz, mises en situation, ...) sont proposés pour vérifier le niveau de compréhension et d'intégration du contenu pédagogique.

### À la fin de la formation :

Le participant auto-évalue son niveau d'atteinte des objectifs de la formation qu'il vient de suivre.

Le formateur remplit une synthèse dans laquelle il indique le niveau d'acquisition pour chaque apprenant : « connaissances maîtrisées, en cours d'acquisition ou non acquises ». Il évalue ce niveau en se basant sur les exercices et tests réalisés tout au long de la formation.

Le participant remplit également un questionnaire de satisfaction dans lequel il évalue la qualité de la session.

À la demande du stagiaire, le niveau peut aussi être évalué par le passage d'une certification TOSA pour les outils bureautiques, CLOE pour les langues.



## Admission

L'admission à ce module se fait sous réserve d'analyse du questionnaire de positionnement et de validation du niveau et des besoins de l'apprenant par notre équipe pédagogique.

Le délai d'accès maximum à cette formation est d'un mois, en nous contactant au 04.72.77.53.54 ou par mail à [contact@abellis-formation.com](mailto:contact@abellis-formation.com)

L'inscription sera validée par retour du devis signé. L'apprenant et/ou le responsable formation recevra, à sa réception, la convention, une invitation et notre plan d'accès (si la formation se déroule en nos locaux).

Référent administratif : Amandine GARAMPON

Référent pédagogique : Marylou MOTTA



## Modalités de suivi

Emargement réalisé par 1/2 journée – Certificat de réalisation remis à l'employeur à l'issue de la formation – Assistance par téléphone et messagerie – Support de cours remis à chaque participant à l'issue de sa formation – Suivi de la progression 2 mois après la formation

