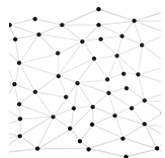


09 déc.

16 oct.

31 mai



Mise à jour nov. 2023

# Former et sensibiliser les utilisateurs à la sécurité informatique

**Durée** 1 jour (7 heures)

« Délai d'accès maximum 1 mois »

Nantes / Rennes : 580 € HT

Brest / Le Mans : 580 € HT

Certification : NON

## OBJECTIFS PROFESSIONNELS

- 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

## PRE-REQUIS

- Pas de prérequis spécifique

## MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- 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.

## MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- 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,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

## MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

## MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone 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-Entreprise 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. Nous préconisons 4 personnes maximum par action de formation en classe à distance

## ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

## 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.

## A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- 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.

## Programme de formation

### La sécurité et l'entreprise (01h00)

- 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 (00h45)

- 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 (01h00)

- 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 (00h45)

- 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 (01h15)

- (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 (00h45)

- 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 (00h45)

- 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 (00h15)

- Synthèse des points abordés
- Savoir évaluer les risques

### Règles de bonnes conduites (00h00)