Cybersécurité – Sensibiliser ses collaborateurs

« La question n’est pas de savoir si vous serez attaqué, mais quand ! »

Cette phrase clé est largement diffusée par l’ANSSI (Agence Nationale de la sécurité des systèmes d’information) pour faire prendre conscience de l’enjeu de la « cybersécurité ».

A une époque où l’informatique se développe dans toute structure, les surfaces d’attaques sont multiples, les scénarios s’affinent… Et, pour un pirate, vous n’êtes jamais trop petit pour être intéressant…

Cette formation aborde les principes de la cyber-hygiène et des réactions à tenir.
Elle n’aborde pas la cybersécurité d’un point de vue développement logiciel ou matériel.

Durée

7 heures

Objectifs

- Comprendre le fonctionnement physique du web, du cloud, des différents outils et technologies utilisées.
- Prendre conscience du risque cyber dans son entreprise
- Identifier les principaux scénarios liés déployés par les pirates
- Mettre en place une cyber-hygiène dans son entreprise : authentification, mots de passe, sauvegarde et cryptage des données, gestion des périphériques, emails, ect.
- Anticiper une attaque et mettre en place des scénarios clés pour savoir y réagir
- Identifier les principaux acteurs de la cybersécurité et les outils associés.

Programme de formation

Digitalisation des entreprises et augmentation de la surface d'attaque

- La cybersécurité pour les entreprises
- Comprendre les motivations des pirates
- Les principaux scénarios de cyberattaques

Adopter une bonne cyber-hygiène au quotidien

1 – Sécuriser à minima son poste de travail

2 – Les enjeux de l'authentification

- Mot de passe, gestionnaire, double authentification et techniques avancées

3 – La gestion des données

- Hébergement, sauvegarde et lisibilité
- La responsabilité liée à vos données

4 – Sécurité des mails, SMS, whatsapp

- Les bonnes pratiques pour éviter de tomber dans le phishing
- Drives et données associés aux mails

5 – Sécurité des sites et des applis

- Détectez les sites frauduleux des sites fiables
- Agissez correctement sur le web et évitez de vous faire piéger
- Apprenez à lire les URL et les liens de téléchargement

6 – Les enjeux du nomadisme

- Le BYOD (Bring Your own Device) et ses limites : risque de pertes de support, mélange d'infos, etc.
- Le travail en nomadisme : VPN et Wifi Public

7 – Votre communication au public : Les risques du « social engineering »

- Quelles sont les informations publiques connues de l'entreprise ? De ses salariés ?

8 – Les transactions en ligne

- Bonnes pratiques pour sécuriser ses transactions en ligne

9 – Cryptographie

- Fonctionnement théorique

Réagir face à une cyberattaque

1 – Minimiser l'impact d'une cyberattaque :

- Mesures à prendre en interne,
- Scénarios et démarches types à construire
- Actions à mener : dépôt de plainte, notification à vos clients, à la CNIL, au public,...

2 – Se faire épauler par des acteurs de la cybersécurité :

- Cybermalveillance,
- ANSSI,
- CNIL,
- Gendarmerie, etc

Public visé

- Toute personne intéressée par la cybersécurité
- Entreprises souhaitant sensibiliser ses collaborateurs à la cybersécurité.

Prérequis

- Être au minimum à l'aise dans l'informatique

Modalités de suivis

- Il est demandé aux stagiaires à chaque début de demi-journée la signature d'une feuille de présence
- Durant la formation, le formateur veille à la bonne compréhension et acquisition de l'information au travers de questions posées aux stagiaires

Moyens pédagogiques

- La formation alternera méthodes expositives, démonstratives et actives
- Mise en pratique
- Les séquences de théories seront le plus souvent accompagnées de séquences pratiques ou de démonstration d'outils ou de méthodes de travail
- Mindmap retraçant toute la présentation
- Support pdf synthétisant la formation et ressources en ligne.

Accessibilité

Alençon, Saint-Lô : Locaux accessibles aux personnes à mobilité réduite

Caen – locaux partiellement accessibles aux personnes à mobilité réduite

Modalités d'évaluation

- Différents exercices pratiques permettent de vérifier l'acquisition des compétences
- Une auto-évaluation est demandée à l'apprenant à la fin de la formation
- Le formateur valide ou non les acquis de l'apprenant