Caltha Tech
Cybersécurité

Programme pédagogique : sensibilisation des utilisateurs aux nouveaux risques digitaux

A l'issue de cette formation, le stagiaire sera capable de comprendre et d'appréhender le SI de son entreprise, de détecter une attaque informatique et d'y réagir.

MODULE : SENSI-1

DURÉE : 3.00 HEURES

LIEU : Chez le client

PROFIL DES STAGIAIRES : Aucun profil particulier

PRÉREQUIS : Aucun

Objectifs pédagogiques

Cette formation apporte des connaissances aux stagiaires leur permettant de sécuriser leur utilisation de l'outil informatique (smartphone, tablette, ordinateur) et ainsi de limiter les risques cyber associés.
Les participants apprendront à adopter les bonnes pratiques au quotidien, à détecter une attaque et à y faire.

Contenu de la formation

- **Comprendre et appréhender le système d'information (SI) de l'entreprise**

Explication de ce qu'est un système d'information pour que le stagiaire en comprenne les enjeux et pourquoi il doit s'impliquer dans la sécurité.
Présentation des risques techniques, humains et juridiques.

- **Présentation des programmes malveillants et leurs objectifs**

Nous présentons les programmes malveillants les plus courants pour que les utilisateurs sachent reconnaître une menace.

- **Présentation des attaques par messagerie et leurs objectifs**
  - Le **pourriel** (spam)
  - Le **canular** (hoax)
  - Le **SCAM**
  - **L'hameçonnage** (phishing)

- Le **logiciel de rançon** (ransomware ou rancongiciel)

- **Identifier un e-mail frauduleux**

Présentation de méthodes simples d'analyse d'e-mail : analyse du contenu du message, analyse de l'en-tête, analyse de l'expéditeur.

- **Apprendre à détecter une attaque**

Présentation des symptômes qui peuvent laisser penser qu'un périphérique (ordinateur, tablette, smartphone) est contaminé ou attaqué.

- **Etude des logiciels de rançon (ransomwares) et comment réagir si l'entreprise est menacée**

Les logiciels de rançon font partie des plus grosses menaces à l'heure actuelle pour les entreprises. Nous expliquons le fonctionnement et présentons un cas concret d'une très grosse entreprise française qui a été attaquée.
Présentation de différentes stratégies à adopter en fonction du type d'attaque.

- **Savoir réagir en cas de suspicion d'attaque ou d'attaque**

Nous présentons les gestes à adopter et les organismes à contacter qui peuvent venir en aide.

- **Adopter les bons gestes au quotidien**

Nous donnons des conseils aux stagiaires pour travailler en sécurité quelque soit leur environnement :

- Gestion de mot de passe
- Navigation sur internet
- Gestion de boîtes e-mail
- Connexion aux réseaux
- Politique de sauvegarde
- Gestion des données
- …

- **Nos conseils pour des usages au quotidien**

Organisation de la formation

Equipe pédagogique

La formation est menée par Nicolas BESSIN, policier en disponibilité, issu du Service des technologies et des systèmes d'information de la sécurité intérieure (5 ans), ex-formateur dans un cabinet de formation/audit/conseil en sécurité/sûreté (2 ans) créé par un ancien commandant de Police, négociateur du RAID. Nicolas dirige sa propre entreprise depuis juin 2015.

Moyens pédagogiques et techniques

- Accueil des stagiaires dans une salle dédiée à la formation
- Documents supports de formation projetés.
- Exposés théoriques
- Etude de cas concrets / Exercices
- Partage d'expérience
- Envoi par e-mail d'un support pédagogique numérique aux participants à l'issue de la session

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Feuilles de présence.
- Questions orales ou écrites (QCM).
- Formulaires d'évaluation de la formation.

Accessibilité handicap

Handicap moteur : à définir en fonction du lieu de formation
Autre handicap : nous consulter en fonction du Handicap.