Programme de formation

Cyber sécurité : Mieux comprendre les risques sur internet afin d'assurer la protection de ses usages numériques

5 jours, soit 35 heures

Public visé

Tous publics

Pré-requis

Aucun

Objectifs pédagogiques

- comprendre les concepts clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles et de protéger leur vie privée,
- protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants (malware) et les accès non-autorisés,
- connaître les différents types de réseaux, de connexions et les composants spécifiques tels que le pare-feu (firewall) qui peuvent poser problème lors des connexions,
- naviguer sur le World Wide Web et communiquer en toute sécurité sur Internet,
- comprendre les problèmes de sécurité liés à la communication, notamment en matière de courrier électronique et de messagerie instantanée (MI – IM/Instant messaging),
- sauvegarder et restaurer des données de manière appropriée et sécurisée, entreposer ses données et ses dispositifs numériques mobiles en toute sécurité.

Description/Contenu

Concepts de sécurité

Menaces sur les données

- Comprendre la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)

Valeur de l'information

- Identifier les mesures à prendre pour empêcher les accès non- autorisés aux données
- Comprendre les caractéristiques de base de la sécurisation de l'information
- Identifier les principales règles de protection, de conservation et de contrôle des données

Sécurité personnelle

- Identifier les méthodes employées pour l'ingénierie sociale comme les appels téléphoniques, l'hameçonnage, l'espionnage par-dessus l'épaule (shoulder surfing)
- Identifier les méthodes de vol d'identité

Sécurité des fichiers

- Comprendre les effets de l'activation / la désactivation des macros dans les options de sécurité des applications
- Utiliser un mot de passe pour les fichiers£
- Comprendre les avantages et les limites du cryptage des données

Logiciels malveillants

Définition et fonctionnement

Types

- Reconnaître les différentes techniques adoptées par les logiciels malveillants
- Reconnaître les différents types d'infections
- Reconnaître les types de vols de données

Protection

- Comprendre comment fonctionne un logiciel anti-virus et identifier ses limites
- Planifier lesanalyses en utilisant un logiciel anti- virus
- Comprendre l'importance de télécharger et d'installer régulièrement les mises-à-jour des logiciels anti-virus

Sécurité réseau

Réseaux

- Comprendre le rôle de l'administrateur réseau dans la gestion des comptes utilisateurs, des droits d'accès, des autorisations et des espaces disques alloués aux utilisateurs
- Comprendre l'utilité et les limites d'un pare-feu (firewall)

Connexions réseaux

- Comprendre que le fait de se connecter à un réseau peut entraîner des problèmes de sécurité

Sécurité en environnement sans fil

- Connaître l'importance d'imposer la saisie d'un mot de passe
- Connaître les différents types de sécurisation d'un réseau sans fil

Contrôle d'accès

- Connaître les bonnes pratiques en matière de mot de passe
- Connaître les principales possibilités de contrôle d'accès biométrique

Utilisation sécurisée du Web

Navigation Web

- Reconnaître un site Web sécurisé
- Mettre en fonction un certificat numérique
- Choisir les réglages appropriés pour autoriser, bloquer les mouchards électroniques
- Comprendre le but, la fonction et les types de logiciels de contrôle de contenus

Réseaux sociaux

- Comprendre les risques potentiels lors de l'utilisation des réseaux sociaux
- L'importance d'appliquer les bons réglages de confidentialité pour les comptes de réseaux sociaux

Communications

Email

- Comprendre le terme : hameçonnage (phishing). Identifier les principales caractéristiques d'hameçonnage comme : utiliser le nom d'entreprises connues, de personnes connues, proposer des liens Internet falsifiés

Messagerie instantanée

- Comprendre les failles de sécurité liées aux messageries instantanées
- Connaître les méthodes pour assurer la confidentialité

Gestion de la sécurité des données

Sécuriser et sauvegarder les données

- Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles
- Identifier les paramètres d'une procédure de sauvegarde

Destruction sécurisée

Modalités pédagogiques

Chacune de nos formations en présentiel est basée sur une pédagogie essentiellement active, se composant d'exposés théoriques et pratiques, de temps d'échanges, d'études de cas, dans des exercices individuels ou en groupe, permettant à chacun d'être acteur dans son apprentissage.

Nos formateurs sont formés aux **sciences cognitives,** ils sont à la fois experts dans leur domaine et pédagogues. Les exercices sont, dans la mesure du possible, extraites de votre quotidien professionnel et permettent ainsi d'appliquer et transférer rapidement les compétences acquises.

Moyens et supports pédagogiques

Afin de créer des conditions les plus favorables pour nos formations, nous mettons à disposition des stagiaires :

- Des supports de cours (format papier ou multimédia) pour la partie en présentiel et FOAD de la formation
- Pour les formations en présentiel : Notre salle de cours est équipée de tableaux blancs, d'imprimante, d'une connexion WiFi, et d'un ordinateur portable par stagiaire avec les logiciels et applications appropriés.

Modalités d'évaluation et de suivi

Pédagogie active basée sur une évaluation tout au long de la formation, des quiz, des travaux pratiques, des exercices ou des mises en application.

Évaluations avec transmission au formateur pour analyse et dans un but d'évolution continue :

- à chaud en fin de formation
- à froid effectuée auprès du stagiaire après 3 mois

Accessibilité

Le délai d'accès à la formation est inférieur à 2 mois à réception du devis signé.

Le centre de formation est accessible aux personnes en situation de handicap. Si vous avez des besoins en compensation pour suivre une formation, contactez notre référente handicap.

La référente handicap chez Voyelle est : Yolande Louvet 06 71 75 62 77