Formation sensibilisation à la cybersécurité

Durée :	1.0 jour(s)
Objectifs :	• Comprendre les attaques • Comprendre les enjeux pour l'entreprise • Comprendre comment se défendre en profondeur • Appréhender les attaques
Public :	• Tout public
Prérequis :	• Utilisation d'internet
Modalités et moyens pédagogiques	• **Modalités et délais d'accès** : L'inscription comprend : demande d'inscription, étude du dossier et positionnement, validation et contractualisation. L'accès à la formation est effectif après validation administrative et pédagogique. Un délai de rétractation de 14 jours s'applique pour les formations financées à titre individuel. Les délais d'accès peuvent varier selon les modalités et les financements. • **Accessibilité handicap :** La formation est accessible aux personnes en situation de handicap. Des adaptations peuvent être proposées après étude des besoins. Merci de signaler toute situation dès l'inscription. • **Sanction de la formation :** Attestation de fin de formation remise au participant/ Evaluation de la satisfaction réalisée en fin de parcours. • **Moyens pédagogiques :** Démonstrations visuelles et pratiques à travers des exercices d'application et/ou des cas concrets des stagiaires. Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran. Portail web : maformation.vaelia.fr
Modalités d'évaluation	Auto-évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
Moyens d'encadrement	Un formateur expert spécialisé en ingénierie Informatique dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.

Satisfaction globale :	/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Environnement de la sécurité utilisateur

- Origine et évolution des systèmes d'information
- Un monde numérique de plus en plus connecté
- Le Cloud et la dématérialisation
- Un environnement à risques élevés
- Les quatre grands types de risques pour l'utilisateur

Comprendre les attaques

- Les différents types de hackers
- Motifs et organisation des attaques
- Types d'attaques
- Motivations des pirates
- Principaux enjeux et conséquences des attaques

Comprendre les enjeux pour l'entreprise

- Enjeux pour l'utilisateur et l'entreprise
- Conséquences principales :
- Perte financière, Atteinte à l'image, Exigences légales (RGPD)

Comment se défendre en profondeur

- Défense en profondeur et bonnes pratiques
- Authentification et gestion des mots de passe
- Conseils pour les mots de passe
- Les malwares et leurs types
- Se prémunir contre les malwares
- Bonnes pratiques de sécurité

Appréhender les attaques

- Explication et identification des spams, e-mails de Phishing, Spear-Phishing, identifier les bons liens, les bonnes pièces jointes…
- Atelier reconnaissance des mails douteux sur une boite mail : simulation d'identification de mail douteux - Reconnaissance de SMS d'hameçonnage sur Android

Savoir comment se défendre

- Comment réagir ?
- Comment se protéger ?
- Connaître les bonnes pratiques utilisateurs.
- Comprendre ce qu'est MailInblack Protect