Les fondamentaux de la cybersécurité : Ensemble, construisons un monde plus sûr !

Nous vivons dans un monde hyperconnecté où désormais tout est possible ou presque. Le revers de la médaille, les pirates informatiques sont passés d'amateurs à des groupes industriels : leur cible … tout le monde, sans distinction. Tous ensemble, adoptons les bons réflexes pour limiter les impacts d'une cyberattaque.

Objectifs pédagogiques :

- **Sensibiliser** les participants sur les risques et les menaces liés à la cybercriminalité.
- **Informer** les participants sur l'état de la menace et les acteurs clés à connaître.
- **Identifier** les différentes menaces susceptibles d'impacter son activité.
- **Intégrer** les bonnes pratiques dans son activité pour anticiper les menaces.

Public visé :

Cette formation s'adresse à toute personne souhaitant se sensibiliser à la cybersécurité.

Prérequis :

- Aucune connaissance particulière n'est nécessaire.
- Un téléphone ou un ordinateur pouvant se connecter à Internet.

Modalité de la formation :

- Durée : 1 jour - 7 heures
- Format : 100% présentiel
- Formation certifiante : non
- Lieu : selon la session de formation
- Coût de la formation : 350 € HT / participant
- Nombre de participants (recommandé) : 3 à 5

Contacts :

- Contact : Nicolas PEIFFER - contact@alveelia.fr - 05.18.22.02.17
- Référent handicap : Nicolas PEIFFER - contact@alveelia.fr - 05.18.22.02.17

Déroulement de la formation – jour 1 :

Module 1 : Introduction à la cybersécurité

- L'état de la menace
- Les acteurs
- Témoignages

Module 2 : Identification des menaces courantes

- Le piratage de compte
- Le phishing
- Le ransomware

Module 3 : Panorama des menaces et bonnes pratiques

- Identifier les attaques
- Les bonnes pratiques

Module 4 : Intégrer des outils pour se protéger

- Protéger ses mots de passe

Module 5 : Réagir face à un incident de cybersécurité

- Subir et gérer une attaque
- La gestion de crise

Module 6 : Intégration dans la culture de l'entreprise

- Inventaire et analyse de risques
- La protection des données
- Etablir un plan d'actions

Evaluation finale

- Validation des acquis

Conclusion

- Bilan et débrief

A l'issue de la formation :

Le bénéficiaire sera capable d'anticiper les menaces en appliquant des bonnes pratiques pour participer à la sécurité du système d'informations de son organisation.

Modalités évaluation :

- **Evaluation formative :** en complément des échanges et des interactions avec le formateur, les participants effectueront des exercices pratiques en fonction des différents modules.
- **Évaluation sommative :** en fin de formation, un quizz sera effectué par chacun des participants afin de mesurer l'acquisition des compétences.

Méthodes pédagogiques :

- **Méthode expositive :** utilisation de supports visuels (diaporamas, vidéos, …).
- **Méthode participative :** les participants réaliseront des activités afin de favoriser les échanges.
- **Méthode expérientielle :** les participants effectueront des cas pratiques ou des mises en situation.

Moyens pédagogiques :

- Supports visuels : diaporamas, vidéos, fiches pratiques, fiches mémo, …
- Utilisation de jeux immersifs et interactifs : cyber@hack - phish&click

Délais d'accès :

Nous nous engageons à donner une réponse sous 24 heures.
La date d'entrée en formation sera conforme à la date inscrite sur le contrat ou la convention de formation.
Celle-ci respectant le délai légal de rétractation.

Modalités d'accès aux personnes en situation de handicap :

Tous les moyens sont mis en œuvre pour permettre aux personnes en situation de handicap de suivre la formation dans des conditions optimales.

Formateur(s) :

Nicolas PEIFFER

- Formation : master en informatique
- Expérience professionnelle :
    - Plus de 17 ans d'expérience dans le domaine du numérique
    - Gestion de projets / Responsable R&D / Encadrement d'équipe