univlearn.
COACHING & FORMATIONS IT

FORMATION EN PRESENTIEL ET/OU EN DISTANCIEL (SELON LE THEME)

SENSIBILISATION À LA CYBERSÉCURITÉ

Dernière mise à jour le 14/03/2023.

OBJECTIF

Etre sensibilisé aux risques en matière de cybersécurité

COMPÉTENCES DÉVELOPPÉES

- Comprendre les principes de sécurité en informatique
- Comprendre les menaces et les attaques
- Connaitre le risque
- Acquérir les bonnes pratiques professionnelles et personnelles de protection
- Etre en mesure de réagir

Tarif	**690** € HT par participant
Réf.	**SenCyb**
Contact	0465260114 nathalie.husson@univlearn.fr https://univlearn.fr/

PUBLIC CONCERNÉ

Toute personne souhaitant comprendre les principes de la cybersécurité

PRÉ-REQUIS

- Aucun prérequis

MODALITÉS D'ACCÈS

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint. Si la formation est financée via un OPCO, vous devez au préalable avoir obtenu un accord de ce dernier.

ACCESSIBILITÉ AUX PERSONNES EN SITUATION DE HANDICAP

Nos locaux sont accessibles aux Personnes à Mobilité Réduite PMR. De plus, nos conseillers sont disponibles pour vous accompagner dans vos démarches à travers nos partenaires. Nous sommes en mesure de mobiliser les expertises, les outils nécessaires pour vous accueillir, vous accompagner et vous former.

MODALITÉS DE DÉROULEMENT DE L'ACTION DE FORMATION

Formation présentielle dispensée par un formateur expert en cybersécurité. La formation alterne des exposés théoriques, des démonstrations et la mise en pratique au travers d'exercices et de cas concrets.

Niveau	Modalité	Effectif par session	Durée
Autres formations professionnelles continues	**Présentiel**	**2 mini > 6 maxi**	**7 heures / 1 jour(s)**

PROGRAMME

Module 1 : Introduction

- Définitions et bref historique
- Les principaux éléments de langage
- Les principales composantes du monde numérique
- Le principe de « sécurité » en informatique
- Les principaux acteurs du monde numérique

Module 2 : Les menaces

- Les principales menaces et leurs motivations
- Les principales formes d'attaques
- Le panorama des menaces, passé, présent et à venir

Module 3 : Le risque

- La notion de risque
- Les actifs matériels, professionnels et personnels, le cas du BYOD
- Les actifs immatériels, le cas des médias sociaux
- Les types de risques
- Les différents types d'impact
- Les aspects juridiques : les infractions et les responsabilités
- Les principales méthodes d'évaluation des risques

Module 4 : Les protections

- La limitation de la « surface d'attaque »
- L'optimisation de l'objectif de sécurité
- Les outils de protection des données, des systèmes et des communications
- Le principe du chiffrement et de la signature numérique
- Les bonnes pratiques professionnelles et personnelles de protection

Module 5 : Réagir

- L'utilisation de la preuve numérique
- La procédure pénale, commerciale et civile
- Les acteurs de la réaction, les cas de l'atteinte à l'image, de l'usurpation

Module 6 : Conclusion

- Les thèmes complémentaires
- Bibliographie
- QCM
- Questions-réponses

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Consultant formateur expert en cybersécurité (10 ans d'expérience)	Evaluation de fin de formation afin d'évaluer l'atteinte des objectifs, Questions posées par le formateur tout au long de la formation à l'oral ou à travers un QCM	Attestation individuelle de formation