Cybersécurité: crimes financiers et fraudes à l'ère numérique

OBJECTIFS

Protégez-vous et votre organisation contre les cyber-menaces grâce à cette formation engageant et axée sur la pratique sur les crimes financiers à l'ère numérique. Cette e-learning interactive est conçue pour améliorer vos connaissances et les mettre en pratique. De plus, elle développe votre capacité de réflexion critique, votre sens des responsabilités et votre compréhension de l'ingénierie sociale. L'e-learning est conçu comme un reportage dans lequel deux pirates informatiques vous dévoilent leur fonctionnement, leurs techniques et leurs tactiques.

Cette formation vous permettra de :

- Acquérir une compréhension approfondie de l'ingénierie sociale et reconnaître les tactiques manipulatrices utilisées par les cybercriminels ;
- Comprendre et identifier différentes cyberattaques telles que le phishing, les deep fakes et les logiciels falsifiés ;
- Appliquer vos nouvelles connaissances dans des scénarios réalistes à l'aide de vidéos et d'exercices interactifs ;
- Renforcer vos compétences pour identifier les mots de passe faibles et utiliser des mots de passe forts ;
- Analyser et évaluer la fiabilité des sites Web, des e-mails et des profils sur les médias sociaux ;
- Reconnaître et éviter les dangers des réseaux Wi-Fi non sécurisés ;
- Détecter les activités suspectes ;
- Reconnaître les tactiques d'ingénierie sociale ;
- Signaler les cyberattaques.

Cliquez ici pour voir la bande-annonce.

RESUME

Catégorie:

- Compliance & audit

Niveau:

Avancé

Type de formation:

E-learning

Prix:

- Membre: € 160.00
- Non-membre: € 180.00
- Partner BZB: € 160.00
- Partner Cevora: € 120.00
- Incompany: sur mesure, prix à la demande

Heures de recyclage:

- Banque: **2h** général
- Assurances: **2h** général
- Crédits à la consommation: **2h** général
- Crédits hypothécaires: **2h** général

- Compliance: **2h**

PUBLIC

Cette formation s'adresse aux professionnels souhaitant approfondir leurs connaissances et se protéger contre la menace croissante de la cybercriminalité :

- Les employés travaillant quotidiennement en ligne ;
- Les gestionnaires responsables de la sécurité des informations sensibles ;
- Toute personne désireuse d'améliorer sa sécurité numérique.

CONNAISSANCE PRÉ-REQUIS

Formation de niveau avancé : cette formation requiert une connaissance générale de base du sujet.

PROGRAMME

CONTENU

- Introduction à la cybercriminalité
- Ingénierie sociale
  - Apprenez ce que signifie l'ingénierie sociale et comment elle est utilisée pour manipuler les gens
  - Identifiez les techniques et stratégies psychologiques derrière l'ingénierie sociale
  - Renforcez votre résilience face à ce type d'attaques cybernétiques et apprenez à appliquer des mécanismes de défense efficaces
- Les armes des cybercriminels
  - Explorez les différents outils et techniques utilisés par les cybercriminels pour accéder aux systèmes et aux données
  - Informez-vous sur les risques des deep fakes, des logiciels falsifiés et autres méthodes d'attaque avancées
  - Comprenez comment les cybercriminels exploitent les vulnérabilités des personnes et des systèmes, ainsi que les mesures que vous pouvez prendre pour vous protéger
- Les attaques des cybercriminels
  - Plongez dans les différents types d'attaques cybernétiques, comme le phishing, le ransomware et les macros
  - Apprenez à reconnaître, prévenir et limiter ces attaques
  - Adoptez une attitude proactive envers la cybersécurité
- Mesures de sécurité et gestion des incidents
  - Apprenez à appliquer des mesures de sécurité essentielles pour vous protéger, vous et votre environnement numérique
  - Comprenez les principes fondamentaux de la gestion des incidents et apprenez à réagir rapidement et efficacement en cas de cyberattaque
  - Découvrez comment minimiser votre empreinte numérique et garantir la confidentialité dans un monde numérique

INFORMATIONS PRATIQUES

- **Durée :** 2 heures
- **Matériel didactique:** module interactif
- **Heures de recyclage :** Chaque module comprend un test en ligne composé de questions à choix multiples. Les heures de recyclage ne sont accordées que si vous réussissez ce test. Si vous l'échouez (résultat inférieur à 60 %), les heures de recyclage ne seront pas accordées pour ce module. Nous vous recommandons donc de ne passer le test que lorsque vous êtes sûr de maîtriser la matière.

MÉTHODOLOGIE

Un « **E-learning** » est un auto-apprentissage à 100 %. Vous vous connectez individuellement à la plateforme d'apprentissage MyFA et

traitez à votre rythme le contenu d'apprentissage qui vous est proposé via une présentation interactive. Vous pouvez suivre cette formation en ligne où, quand et aussi souvent que vous le souhaitez. Le matériel didactique se compose d'un format numérique avec texte, vidéo, images, animations, questions de test et/ou références à des documents et/ou sites web pertinents.