

Phishing, Smishing & Vishing : reconnaître et prévenir la cyberfraude dans le secteur financier

OBJECTIFS

Cette formation propose une approche pratique pour reconnaître et prévenir la cyberfraude dans les contacts clients et les processus internes. Les participants apprendront à agir rapidement et en toute sécurité, à suivre les procédures internes et à informer correctement les clients.

Les objectifs de cette formation sont :

- distinguer les différentes formes de phishing, smishing et vishing ;
- reconnaître les tactiques les plus récentes (audio deepfake, spoofing, fraude au CEO, ingénierie sociale) ;
- identifier les signaux d'alerte dans les e-mails, SMS, appels téléphoniques et réseaux sociaux ;
- réagir correctement et suivre les procédures internes (IT-security, fraude, conformité) ;
- appliquer des mesures préventives : hygiène numérique, politique de mots de passe, MFA ;
- comprendre comment la cyberfraude cible spécifiquement les institutions financières.

RESUME

Catégorie:

- Retail banking
- Compliance & audit

Niveau:

Basique

Type de formation:

Formation en classe

Prix:

- Membre: € 310.00
- Non-membre: € 340.00
- Partner BZB: € 310.00
- Incompany: sur mesure, prix à la demande

Heures de recyclage:

- Banque: **3h** général
- Assurances: **3h** général
- Compliance: **3h**

PUBLIC

Le cours de formation peut être suivi par différents groupes cibles :

- les collaborateurs du secteur financier : employés de banque, conseillers en crédit et assurance, profils compliance, front- et back-office, call center, accueil ;
- les équipes responsables de la sécurité client, de la compliance et de la détection des fraudes.

CONNAISSANCE PRÉ-REQUIS

Formation de niveau de base : cette formation ne requiert aucune connaissance préalable et couvre la base du sujet.

PROGRAMME

CONTENU

- **Introduction**
 - Panorama des menaces cyber dans le secteur financier
 - Tendances récentes dans les banques et assurances
 - Impact sur la satisfaction client, la réputation et les obligations légales
 - Comment les cybercriminels manipulent les employés financiers
- **Phishing en détail**
 - Reconnaître les e-mails frauduleux
 - Techniques : spoofing, QR-phishing, vol d'identifiants, malware
 - Analyse d'exemples réels (banques belges)
 - Exercice pratique : « Vrai ou faux ? »
- **Smishing & fraude via WhatsApp**
 - Analyse des fraudes par SMS et messagerie
 - Campagnes de smishing liées aux banques
 - Comment les clients sont trompés par un langage urgent / faux liens
 - Exercice pratique : évaluer des SMS et liens suspects
 - Bref : utilisation sécurisée des appareils privés (BYOD)
- **Vishing & ingénierie sociale**
 - Arnaques téléphoniques : faux centres d'appel, faux employés, « fraude helpdesk »
 - Spoofing des numéros de téléphone
 - Voix deepfake et manipulation par IA
 - Jeu de rôle : gérer des appels inattendus
 - Définir les limites : quelles infos ne jamais partager ?
- **Prévention, procédures & bonnes pratiques**
 - Procédures internes de signalement (IT, fraude, management)
 - Comment réagir correctement en cas d'incident
 - Conseils de prévention pour collaborateurs, équipes et clients
 - Mots de passe, authentification multi-facteurs, sécurité des appareils
 - Checklist : hygiène cyber quotidienne pour les employés financiers

INFORMATIONS PRATIQUES

- **Durée :** ½ journée de formation (3 heures de formation)
- **Heures :** 13:30 à 17:00
- **Lieu :** Febelfin Academy : Phoenix building, Boulevard du Roi Albert II 19, 1210 Bruxelles

MÉTHODOLOGIE

Une « **Formation en classe** » se suit en présentiel en groupe. Vous êtes présent avec les autres participants et le professeur à un moment convenu dans la même salle de cours. Il existe des possibilités d'interaction et de feed-back, tant des participants à l'enseignant qu'inversement. Le matériel didactique se compose comme base d'une présentation via la plateforme d'apprentissage MyFA, complétée de supports divers tels que syllabus numérique, présentation, extraits audiovisuels...

Matériel didactique :

- Présentation PowerPoint ;
- Cas réels de fraude