

Prévention des fraudes numériques : pratiques et cas concrets - BFFN

Code produit : BFFN

Niveau : Initiation

Modalité : Presentiel

Durée (en heure) : 7.0

Tarif : 0,00 € HT

Eligible DDA : non

Public :

Conseillers en agence,
chargés de clientèle,
gestionnaires middle-office,
responsables conformité,
référents sécurité

Prérequis :

Aucun

Objectif

- Identifier les principales menaces de cyberfraude touchant la banque et ses clients
- Adopter les bons réflexes face aux tentatives de fraude (phishing, virement, ingénierie sociale...)
- Conseiller les clients sur les bonnes pratiques de sécurité numérique
- Réagir rapidement en cas de suspicion de fraude ou d'incident
- Contribuer activement à la prévention des risques dans son périmètre

Programme de la formation

1. Panorama des cybermenaces dans le secteur bancaire
 - État des lieux de la cyberfraude : chiffres clés, tendances actuelles
 - Menaces majeures : phishing, ransomware, malware bancaire, usurpation d'identité, fraude au président
 - Cibles internes et externes : collaborateurs, clients, partenaires
2. Typologies de fraudes numériques
 - Fraude au virement SEPA (manipulation IBAN, ingénierie sociale)
 - Phishing et spear phishing : emails, SMS, sites clones
 - Fraude à l'usurpation d'identité : faux documents, comptes détournés
 - Fraudes via réseaux sociaux et messagerie instantanée
3. Posture du conseiller face à la fraude
 - Rôle du conseiller dans la chaîne de prévention et d'alerte
 - Vigilance comportementale : détection des signaux faibles
 - Réflexes clés à adopter face à un doute ou un client en danger
 - Comment sensibiliser le client sans générer de peur ou de méfiance excessive
4. Dispositifs de sécurité et outils internes
 - Présentation des outils de détection / alerte disponibles dans le SI
 - Procédures internes : escalade, blocage, remontée conformité
 - Interaction avec les référents cybersécurité, RCCI
 - Traces, preuves, signalements : que faire en cas d'incident ?

Moyens d'évaluation

- Evaluation des acquis de la formation par le biais de QCM et/ou d'exercices pratiques
- Questionnaire de satisfaction à chaud complété par chacun à l'issue du stage
- Questionnaire d'évaluation à froid complété par chacun entre 2 et 3 mois après le stage

Méthodes pédagogiques

- Exposés à partir d'un diaporama
- Brise-glace interactif
- Carte mentale collaborative

- Escape Game ou « Cyber Enquête »
- Jeu de rôle inversé
- Mises en situation
- Débriefing collectif
- Serious game narratif
- Echanges d'expériences

AF2A - 64 Rue de Miromesnil, 75008 Paris

Copyright 2024 AF2A. Tous droits réservés.