02 — Faux conseiller bancaire

Interrompre une demande bancaire pressante et rappeler par un canal connu.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Un homme appelle Samira et se présente comme le service antifraude. Il connaît son nom et évoque un achat de 780 €. Le numéro affiché ressemble à celui de sa banque. Pour annuler l'achat, il lui demande de valider une notification et de transférer son épargne sur un « compte sécurisé ». Il propose ensuite qu'un coursier récupère sa carte.

Comprendre le piège

L'escroc utilise la peur de perdre son argent pour faire autoriser un paiement ou un virement. Des informations exactes et un numéro affiché peuvent être usurpés. Une validation dans l'application peut exécuter l'opération dont l'appelant prétend empêcher la réalisation.

Les signes d'alerte

• Une personne demande un code secret ou un code reçu par SMS.

• Elle dicte des validations censées annuler une fraude.

• Elle réclame un virement de sécurité ou la remise de la carte.

• Elle interdit de raccrocher ou de parler à l'agence.

02 — Vérifier et réagir

Le réflexe à retenir

Raccrocher. Rappeler la banque avec le numéro figurant sur la carte, un document habituel ou l'application déjà installée. Ne valider aucune opération dictée par l'appelant.

Que faire si j'ai été victime ?

Des codes ou une validation ont été donnés

Alerter sans attendre la vraie banque et expliquer précisément ce qui a été communiqué ou confirmé.

La carte est compromise

Demander l'opposition immédiatement. Ne remettre ni carte ni code à un coursier.

Un virement est parti

Demander à la banque si elle peut tenter son rappel et contester les opérations concernées. Une récupération ou un remboursement ne sont pas garantis par cette démarche.

Préparer la suite

Garder horaires, numéros, messages et références d'opérations. Changer l'accès bancaire si compromis avec l'aide de la banque ; déposer plainte.

À vous de jouer

À deux, un participant lit le scénario et l'autre formule sa phrase pour mettre fin à l'appel. Il montre ensuite où retrouver le vrai numéro, sans afficher de donnée bancaire personnelle.

Réponses personnelles : .....

.....

02 — Petit quiz

Une seule réponse par question. Choisir puis expliquer sa décision. Les corrections figurent dans le document séparé « Quiz corrigés » et sur la page de la situation.

1. Le numéro affiché suffit-il à reconnaître la banque ?

A. Oui, toujours.

B. Oui, si l'appelant connaît mon nom.

C. Non, il peut être usurpé.

2. On demande de valider pour annuler un achat. Que faire ?

A. Raccrocher puis joindre la banque indépendamment.

B. Valider rapidement.

C. Transmettre le code à un proche de l'appelant.

3. Un coursier vient prendre la carte. Quelle réponse ?

A. La couper puis la lui donner.

B. Refuser et alerter la banque.

C. Lui laisser le code séparément.

4. Une demande de rappel de virement garantit-elle de récupérer l'argent ?

A. Oui, si elle est immédiate.

B. Oui, après une plainte.

C. Non, il faut agir vite sans promesse de résultat.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Faux conseiller bancaire

Service-Public — Arnaque sur Internet et THESEE

Sources vérifiées le 12 novembre 2026. Conditions des services à vérifier lors des démarches.