Sécurisez vos comptes : Le bouclier anti-fraude indispensable

Renforcez vos accès et identifiants

• Activez systématiquement l'authentification forte (double facteur) sur votre application bancaire pour valider chaque connexion et virement.

• Utilisez des mots de passe robustes et uniques pour votre compte bancaire, distincts de ceux utilisés pour vos réseaux sociaux ou sites marchands.

• Ne communiquez jamais votre code secret, vos mots de passe ou les codes de validation reçus par SMS, même à un conseiller supposé.

Adoptez les bons réflexes de navigation

• Ne cliquez jamais sur les liens contenus dans un e-mail ou SMS ; passez toujours par l'application officielle ou tapez manuellement l'adresse du site.

• Vérifiez systématiquement l'URL du site bancaire dans votre navigateur (présence du 'https://' et du verrou) avant de saisir vos identifiants.

• Refusez toute demande de transfert d'argent vers un prétendu 'compte de sécurité' ou 'compte refuge' : aucun conseiller ne vous demandera cela.

Surveillez vos opérations et vos outils

• Paramétrez des alertes SMS ou des notifications push en temps réel pour chaque débit afin de détecter immédiatement toute opération suspecte.

• Privilégiez l'utilisation de la carte virtuelle (e-card) pour vos achats en ligne afin de générer un numéro éphémère pour chaque transaction.

• Mettez à jour régulièrement le système d'exploitation de votre smartphone et l'application de votre banque pour bénéficier des derniers correctifs de sécurité.

Réagir en cas d'urgence

• En cas de vol ou de perte de votre carte, faites opposition immédiatement via votre application bancaire ou en appelant le numéro d'urgence interbancaire 116 116 (disponible 24h/24).