5 CONSEILS POUR DÉJOUER LES TENTATIVES D'ARNAQUE AUX PAIEMENTS

1. Prenez le temps avant de cliquer

Les fraudeurs cherchent souvent à faire réagir rapidement : compte bloqué, paiement immédiat, offre limitée, problème de sécurité…

Avant de cliquer, de scanner un QR code, de répondre ou de confirmer une opération, prenez du recul. En cas de doute, ouvrez vous-même le site ou l'application officiels concernés, sans passer par le lien reçu.

2. Vérifiez qui vous contacte réellement

Les messages frauduleux peuvent sembler très crédibles : logo connu, ton familier, lien presque identique à l'original.

Soyez attentif aux signaux d'alerte : fautes d'orthographe, numéro inconnu, adresse d'expéditeur inhabituelle, URL modifiée ou demande urgente.

Le cadenas et le "https://" ne suffisent pas : vérifiez toujours l'adresse complète du site.

3. Ne partagez jamais vos codes ou données sensibles

Une banque, une application de paiement ou une organisation légitime ne vous demandera jamais de communiquer votre code PIN, mot de passe, code de vérification ou vos données bancaires par e-mail, SMS, téléphone ou chat.

Méfiez-vous des demandes de "confirmation d'identité", de "sécurisation de compte" ou de transfert vers un "compte sécurisé". Toute action sensible doit se faire dans l'application bancaire officielle ou sur une plateforme de confiance

4. Protégez vos comptes et appareils

Utilisez des mots de passe forts et différents pour vos comptes importants : e-mail, banque, paiement, e-commerce.

Activez l'authentification à deux facteurs, gardez vos appareils et vos applications à jour, téléchargez uniquement depuis les stores officiels et vérifiez régulièrement vos comptes pour repérer toute activité suspecte.

5. Restez dans les environnements de paiement fiables

Les arnaques surviennent souvent lorsqu'on vous pousse à sortir du processus normal : lien de paiement séparé, QR code externe, autre site ou méthode de paiement inhabituelle.

Sur les plateformes de seconde main ou marketplaces, restez dans le système prévu, vérifiez le profil du vendeur, le montant et le bénéficiaire avant toute confirmation. Pour les opérations sensibles, évitez le Wi-Fi public et privilégiez une connexion privée et de confiance ou un réseau mobile, comme la 4G ou la 5G.

En cas de suspicion de fraude, agissez rapidement :

1. Bloquez votre carte via Card Stop : +32 78 170 170.
2. Signalez la fraude via Fraudstop, accessible au même numéro que Card Stop.
3. Signalez les messages suspects à l'adresse suspect@safeonweb.be.
4. Déposez plainte auprès du commissariat de police le plus proche.

Pour en savoir plus sur la fraude aux paiements et les bons réflexes de sécurité, consultez la page dédiée : bancontact.com/fr/consommateur/cybersecurite.