ESCROQUERIES

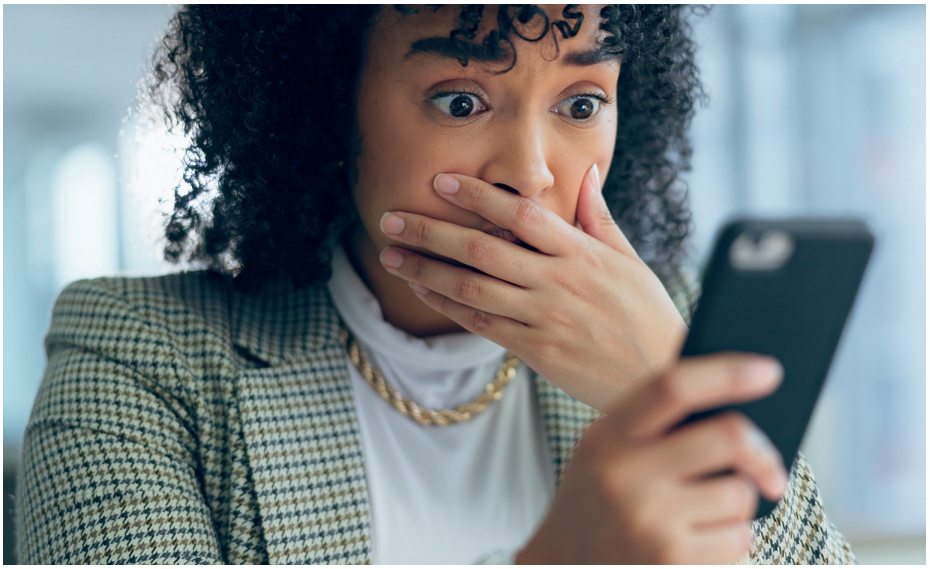
LUC LEESCO, EXPERT-COMPTABLE,
PARTENAIRE DE FNI COMPTA

Fraudes aux moyens de paiement : recommandations

Qui n'a jamais été confronté à une fraude ou une arnaque sur Internet ? Nous avons tous autour de nous des amis ou connaissances ayant subi ces désagréables expériences. Certains ne s'en vantent d'ailleurs pas, honteux d'avoir été abusés. Sont-elles une fatalité, quelles sont les conséquences ? Faisons-le point.

Internet, ce beau terrain de jeu

Il n'a pas fallu attendre l'Internet pour que sévissent des escrocs en tout genre. Savez-vous qu'en 1925, Victor Lustig (un nom pareil, ça ne s'invente pas), avait même vendu… la tour Eiffel. Avec la généralisation des transactions en ligne, les escrocs de tout poil ont gagné là un magnifique terrain de jeu. Investissements financiers trop avantageux, faux sites de vente, phishing…leur ingéniosité n'a pas de limite. Si le risque zéro n'existe pas, quelques règles de bon sens peuvent limiter l'exposition à ces personnes qui en veulent à votre argent. Nous examinerons quelques exemples.



Si le risque zéro n'existe pas, quelques règles de bon sens peuvent limiter l'exposition aux escrocs qui en veulent à votre argent.

Le législateur contre-attaque

La fraude aux moyens de paiement risquant de saper la confiance dans l'économie moderne, le législateur et les différents acteurs concernés (banques, fintech…) ont pris des mesures de protection du consommateur. C'est ainsi qu'est née la directive européenne DSP2 et plus précisément l'authentification forte ou double authentification, instaurant des normes de sécurité plus strictes. La Banque de France a émis une série de recommandations et en particulier précise que les financiers doivent rembourser les victimes en cas de doute sur le consentement donné aux opérations, hormis le cas de "négligence grave".

La double authentification

La double authentification, dite aussi en deux étapes (2FA), fonctionne de la manière suivante. Pour prouver son identité, l'utilisateur saisit son mot de passe et reçoit un code provisoire par SMS ou par courriel ou une notification dans une application pour valider l'opération. Une sécurité bien difficile à "hacker" qui donne du fil à retordre aux fraudeurs.

Ingénierie de la manipulation

Les escrocs les plus aguerris ne sont pas restés inactifs devant ces portes devenues inviolables ou presque. Ils ont vite compris que la faille dans la sécurité, c'était la future victime elle-même. Aussi se sont-ils concentrés sur la manipulation de celle-ci pour la faire participer à sa propre escroquerie. Mais avant de voir l'ingénierie de la manipulation à l'œuvre, examinons la classique escroquerie à la carte bancaire (CB).

Fraude à la carte bancaire

Le vol classique : un escroc récupère votre code confidentiel lors d'un achat (restaurant, magasin, location de voiture etc.) ou retrait (DAB). Son complice dérobe ensuite votre CB. Il ne lui reste plus qu'à effectuer des retraits en espèces avant que vous ne vous en rendiez compte.

Plus subtil : la fraude sans présentation de la carte bancaire (CNP) concerne les cas où la CB n'est pas nécessaire pour effectuer une transaction.

Exemple. Emma dispose d'une CB professionnelle à débit différé. Très occupée, elle est peu attentive à l'état de ses comptes. Alors, lorsque son expert-comptable l'interroge sur certaines dépenses effectuées il y a quelques mois, elle découvre des achats qu'elle n'a jamais réalisés. Elle fait immédiatement opposition et réclame le remboursement à sa banque qui s'étonne de cette découverte tardive.

Analyse. Comment a-t-il été possible pour un escroc de faire des emplettes à sa place alors que sa CB n'a jamais quitté son portefeuille ? Il suffisait de posséder le numéro de carte, la date d'expiration et le cryptogramme au verso de la carte. Pour certains types d'achat, il n'est pas obligatoire de disposer du code confidentiel. Les fraudeurs se procurent les données de CB sur le Darknet par hameçonnage (phishing), auprès d'employés indélicats qui, sous un prétexte quelconque, ont éloigné la carte de votre vue et en ont pris une photo recto verso (loueur de voitures, restaurant, hôtel, boutique etc.).

<u>Ce qu'il faut faire.</u>

- Éviter le débit différé afin de disposer d'un état en temps réel de ses transactions.
- Vérifier son compte bancaire toutes les semaines.
- Ne jamais laisser un commerçant s'éloigner avec sa CB.
- Si l'on veut être très prudent, régler ses achats sur les sites incertains avec des CB à usage unique.
- Demander le remboursement immédiat à sa banque (article 133-18 du Code monétaire et financier).

Usurpation d'identité (spoofing)

Le spoofing est une usurpation d'identité (faux conseiller : bancaire, Ameli, France Travail, Netflix etc.), qui permet de manipuler la victime et lui faire commettre l'escroquerie par elle-même sans s'en apercevoir (manipulation).

Exemple. Jennifer reçoit un appel d'un faux agent du service antifraude de sa banque qui l'informe d'un piratage en cours sur sa CB. Paniquée, elle suit sans discuter ses instructions et lui communique les codes de validation reçus par SMS pour authentifier sa transaction. Grave erreur, sans le savoir, elle valide les acquisitions de l'escroc qui a réalisé pour 9 000 € d'achat.

Analyse.

- Le fraudeur a récupéré les informations de la CB par hameçonnage, sur le Darknet ou par clonage de la CB.
- Il effectue des achats coûteux en ligne.
- Comme il ne peut pas valider la transaction par lui-même en raison de la double authentification, il va les faire valider par la victime elle-même, qui est sous le coup de l'émotion.
- Il est crédible car il dispose d'informations sur la banque et la victime.
- Il accentue la panique de la victime en appelant hors des heures d'ouverture de la banque.
- Le stress pousse la victime à suivre les instructions du faux agent.
- Elle valide ainsi toutes les opérations en attente : le tour est joué !

<u>Ce qu'il faut faire.</u>

- En cas de doute, toujours rappeler le service interbancaire 0 892 705 705 (Tarif : 0,34 € la minute – ouvert 24h/24, 7j/7).
- Transmettre ses informations confidentielles seulement à des personnes bien identifiées.
- Ne jamais valider des opérations dont vous n'êtes pas à l'origine ; elles sont par définition suspectes.

Faux RIB

Un individu malveillant pirate la messagerie d'une entreprise et envoie des factures à ses clients comprenant un faux RIB. Certains d'entre eux n'y prennent pas garde et payent la facture en toute confiance, enrichissant l'escroc !

Exemple. Un matin, en consultant ses courriels professionnels, Adèle, Idel expérimentée, tombe sur la facture d'un fournisseur habituel en matériel médical. Cette dernière semble tout à fait normale, à l'exception d'un détail : le RIB indiqué pour le virement est différent de celui qu'elle connaît. Intriguée, elle appelle son fournisseur qui lui affirme ne jamais avoir envoyé cette facture. Sans ce réflexe de vérification, Adèle aurait été victime d'une arnaque au faux RIB.

Analyse.

- L'escroc a piraté le compte de messagerie du fournisseur.
- Il envoie de fausses factures à tous ses clients, modifiant le RIB pour recevoir les paiements sur son propre compte.
- Sur le volume, certains clients effectuent mécaniquement les virements…

<u>Ce qu'il faut faire.</u>

- Toujours s'assurer que le RIB correspond bien au RIB connu.
- Demander immédiatement à sa banque d'annuler le virement ("call back").

Négligences graves ?

Comme nous l'avons vu plus haut, l'organisme financier est tenu de vous rembourser à la condition que vous n'ayez commis aucune négligence grave. Il est donc de votre intérêt de suivre les conseils suivants :

- au moindre doute, appelez votre banque ou le service opposition ;
- vérifiez régulièrement vos relevés bancaires pour pointer toute opération suspecte ;
- évitez le débit différé qui peut masquer les opérations quotidiennes ;
- soyez vigilant envers les courriels ou SMS non sollicités ;
- ne faites aucune confiance à un site que vous ne connaissez pas ;
- attention aux offres mirifiques, etc.

Soyez diligent !

Les banques ont développé un arsenal de techniques en vue de sécuriser les paiements mais des failles demeurent. Le suivi de vos relevés de comptes est l'une des meilleures parades pour repérer les fraudes éventuelles lorsqu'elles ont eu lieu malgré votre vigilance. C'est l'une des raisons pour laquelle l'application Vite Ma Compta vous propose de vérifier l'état de vos comptes chaque semaine. Les utilisateurs apprécient cette fonctionnalité car ils conservent ainsi un meilleur contrôle sur leurs dépenses et, cerise sur le gâteau, maîtrisent mieux leurs finances. De quoi ravir leur comptable ! ●