# Votre banque vous écrit ? Attention aux fausses lettres !

**De faux courriers ressemblant à s'y méprendre à ceux d'établissements financiers connus atterrissent régulièrement dans nos boîtes aux lettres. Voici comment les reconnaître.**

**Principales informations à connaître :**

- Lorsque vous vous connectez à votre compte d'e-banking, faites-le toujours depuis le site officiel ou l'application de banque mobile de votre établissement bancaire.
- Vérifiez l'authenticité du courrier que vous recevez par la poste de la même manière que pour vos messages électroniques et signalez les lettres suspectes à votre banque.
- Vérifiez l'adresse Internet des codes QR lus avec l'appareil photo de votre dispositif avant de suivre le lien.

Les escrocs se donnent beaucoup de mal pour faire en sorte que leurs fausses lettres se rapprochent le plus possible des vraies et n'hésitent pas à reproduire les logos et la mise en page habituelle de ce genre de courrier. Leur but est bien entendu d'obtenir de leurs victimes des informations confidentielles ou des identifiants de connexion pour accéder par exemple à leur compte d'e-banking.

Un scénario typique consiste à inciter les clients d'une banque à flasher le code QR présent sur la lettre, pour les conduire sur une page Internet ressemblant parfaitement à la page de connexion de votre e-banking. Il vous suffit que la victime saisisse ses identifiants dans les champs correspondants pour que les criminels obtiennent ainsi l'accès à son compte.

Ce procédé est le même que pour le phishing (https://www.ebas.ch/phishing) (ou hameçonnage) classique, à la différence près que le message reçu n'est pas électronique (email, SMS ou Messenger), mais bien physique. Les criminels n'hésitent pas à faire pression sur leurs victimes, en les menaçant de bloquer leur compte s'ils n'exécutent pas l'action requise dans le faux courrier.

Le recours aux codes QR présente un avantage intéressant pour les escrocs, dans la mesure où l'adresse Internet qui renvoie au site frauduleux n'est pas immédiatement lisible car encodée dans la mosaïque. Si l'adresse apparaissait directement sur le papier, un coup d'œil suffirait pour s'apercevoir de la supercherie.

Mais pour comprendre s'il y a arnaque ou pas, il est possible de vérifier l'adresse Internet qui s'affiche sur le téléphone avant d'être redirigé vers le site web correspondant, juste après avoir flashé le code QR. La méthode imparable reste néanmoins d'accéder aux services de votre banque en tapant à la main l'adresse Internet du site dans la barre d'adresse de votre navigateur, ou en utilisant l'application de banque mobile officielle.

*Des escrocs parviennent à imiter de manière très crédible les documents écrits, et notamment des lettres commerciales d'entreprises reconnues comme sérieuses, comme des établissements bancaires par exemple. Ces lettres frauduleuses invitent les clients à exécuter certaines actions liées à la sécurité, le but étant bien entendu d'obtenir*

*des informations confidentielles, voire les identifiants de connexion des personnes.*