



Communiqué de presse

## **La police lance une campagne de mise en garde contre les délits de phishing liés aux cartes bancaires**

**Avec la popularité grandissante des achats en ligne, l'activité des cyber-escrocs est en augmentation. Chaque année, les fraudes à la carte bancaire augmentent de 10 à 20 %. Le phishing (hameçonnage) reste l'arnaque la plus courante, exploitant la crédulité et l'ignorance des victimes. La police intensifie ses efforts pour protéger les titulaires de cartes, qui peuvent se prémunir efficacement contre ces vols grâce à de simples mesures de précaution.**

**Zurich, le 29 mai 2024** – Ces dernières années, les paiements sans espèces ont considérablement augmenté. C'est un moyen de paiement simple, pratique et très sécurisé, à condition toutefois que les titulaires de cartes respectent quelques précautions. Or c'est justement là que le bât blesse. « Force est de constater que les titulaires de cartes agissent souvent avec une grande imprudence. Certain(e)s ignorent même qu'il ne faut jamais divulguer des données confidentielles comme leurs codes de sécurité ou leurs codes CVV. De même, avant de confirmer une transaction par SMS, il est essentiel de s'assurer de sa légitimité et de l'identité de l'expéditeur » explique Bernard Vonlanthen de l'unité communication et prévention à la police cantonale Fribourg. « Il est tout à fait indispensable que les forces de police continuent à sensibiliser régulièrement la population aux quelques mesures de précaution à prendre. »

### **Qui est concerné par la fraude à la carte bancaire ?**

Les fraudes à la carte touchent des personnes de tout âge et de tout sexe avec des montants allant de petites sommes à des préjudices très élevés. En Suisse, les fraudes à la carte ne sont pas systématiquement comptabilisées mais selon une extrapolation, elles s'élèveraient à près de 90 millions de francs pour l'année 2023. Cette estimation repose sur les valeurs de référence de quelques établissements financiers et sur les données de la Banque nationale suisse. Elle comprend aussi bien les transactions par carte dans les magasins et sur Internet que les retraits aux bancomats en Suisse et à l'étranger. Selon les indications des corps de police, si le montant moyen des délits se situe entre 1000 et 2000 francs, celui-ci peut être beaucoup plus élevé et, dans certains cas, atteindre le plafond de retrait fixé.

« Nous recommandons de fixer les plafonds de retrait des cartes au niveau réellement nécessaire » précise Bernard Vonlanthen. « Il est tout à fait essentiel que les victimes portent plainte, ce qui est malheureusement rarement le cas. Celles qui ont perdu de petites sommes ou qui se sentent responsables préfèrent endosser les pertes financières sans les signaler à la police. » Une situation qui n'arrange rien. En effet, les dénonciations contribuent à mieux comprendre le mode opératoire des cyber-escrocs et à identifier les liens de cause à effet, augmentant ainsi considérablement les chances de succès dans le travail d'enquête de la police.

## **Des professionnel(le)s à l'œuvre**

Une chose est sûre : les cyber-criminel(le)s agissent de manière de plus en plus professionnelle. La plupart des arnaques commencent par du phishing (hameçonnage). Les cibles sont contactées par e-mail, SMS ou chat par des tierces personnes qui les dirigent sous un prétexte quelconque vers un site web frauduleux. Les cyber-escrocs vont alors « à la pêche » aux informations confidentielles. Les victimes sont invitées à saisir leur identité ou leurs données de carte pour que la marchandise commandée puisse enfin leur être livrée ou qu'un abonnement prétendument bloqué soit réactivé. Une négligence qui peut coûter cher.

Les attaques de phishing diffèrent par leur teneur et leur présentation, mais le principe reste le même.

## **Comment se prémunir contre le phishing ?**

Voici quelques mesures de précaution pour se protéger efficacement :

- # Se méfier des messages provenant d'expéditeurs inconnus. Vérifier systématiquement l'e-mail de l'expéditeur et l'URL.
- # Ne cliquer sur aucun lien, n'ouvrir aucune pièce jointe ; se connecter exclusivement à partir de sites officiels.
- # Se méfier de tout message urgent exigeant une action immédiate.
- # S'assurer que le paiement soit sécurisé avant de saisir les données de sa carte.
- # Lire attentivement le SMS de validation et s'assurer que tout est en ordre avant d'appuyer sur « ok »
- # Utiliser des mots de passe robustes et l'authentification à deux facteurs (2FA) ou à plusieurs facteurs (MFA).
- # Activer les notifications de paiement afin de recevoir un message sur son smartphone avant chaque transaction.
- # Vérifier régulièrement les transactions et les relevés de compte. Signaler immédiatement tout mouvement suspect à son établissement financier.
- # Fixer un plafond de retrait bas. Activer exclusivement les fonctionnalités nécessaires.
- # Porter plainte en cas de fraude.

## **Campagne nationale de prévention de la police**

Depuis plusieurs années, la police mène des campagnes nationales pour sensibiliser le public au problème des fraudes à la carte bancaire. « Cette année, le phishing est au cœur de la campagne Card-Security » explique Bernard Vonlanthen. « Notre objectif est de continuer à ancrer s comportements sécurisés au sein de la population. »

La campagne 2024 sera déployée en deux vagues : au printemps (du 29 mai au 26 juin 2024) et à l'automne (du 28 août au 25 septembre 2024). Elle reposera principalement sur les médias en ligne et sur la communication relayée par les corps de police.

Pour en savoir plus sur les nouveaux types de fraude et les mesures de précaution à prendre, les titulaires de cartes peuvent se rendre sur le site [www.card-security.ch](http://www.card-security.ch) et tester leurs connaissances grâce à un nouveau quiz.

## **Contact**

Bernard Vonlanthen, unité communication et prévention à la police cantonale Fribourg

Téléphone : +41 26 305 16 28

E-Mail : [bernard.vonlanthen@fr.ch](mailto:bernard.vonlanthen@fr.ch)

Pour commander des visuels supplémentaires, veuillez envoyer un e-mail à :

[info@card-security.ch](mailto:info@card-security.ch)

## Visuels



# gaffetoi

**La pêche miraculeuse,  
ça n'existe pas !**

card-security.ch

card security  Votre Police



# gaffetoi

**Il y a anguille  
sous roche !**

card-security.ch

card security  Votre Police



# gaffetoi

**Je ne tomberai pas  
dans tes filets !**

card-security.ch

card security  Votre Police



# gaffetoi

**Ça pue  
le phishing !**

card-security.ch

card security  Votre Police