



## Q & R

### **Qu'est-ce que Card Security ?**

Card Security est une initiative nationale de prévention organisée par la police et consacrée aux fraudes à la carte bancaire (cartes de débit et de crédit). Actuellement, l'accent est mis sur la prévention du phishing. Card Security s'adresse au grand public par le biais d'un site Internet et de différentes campagnes. Cette plateforme permet également aux spécialistes des corps de police et des établissements financiers d'approfondir leurs connaissances sur le sujet.

### **En quoi Card Security est-elle nécessaire ?**

Les délits commis avec des cartes de crédit ou de débit augmentent chaque année de 10 à 20 %. Card Security est l'interlocuteur privilégié de la police pour toutes les questions relatives à l'utilisation frauduleuse des cartes de débit et de crédit. En effet, Card Security fédère les expertises présentes au sein des corps de police, des établissements financiers et des émetteurs de cartes. Sur le site Internet [card-security.ch](http://card-security.ch), les titulaires de cartes bancaires ainsi que les membres de la police et le personnel des banques peuvent trouver des informations détaillées sur les derniers types de fraudes à la carte bancaire et sur les mesures de prévention à adopter.

Card Security s'adresse également aux professionnels. Sur le site [card-security.ch](http://card-security.ch), les membres des corps de police et des banques peuvent prendre connaissance des campagnes en cours, du matériel pédagogique et de toutes les informations utiles.

Grâce à ses campagnes de prévention, Card Security a touché près de 30 millions de personnes en Suisse..

### **Qui est à l'origine de Card Security ?**

Card Security est une initiative de la police sur le thème de la sécurité des cartes bancaires. Card Security sensibilise la population au sujet de la fraude à la carte bancaire par le biais d'un site Internet et de campagnes nationales. Tous les documents sont publiés en quatre langues : allemand, français, italien et anglais.

### **Que signifie #gaffetoi?**

Le hashtag #gaffetoi a été lancé par Card Security dans ses campagnes et son site Internet pour sensibiliser aux dangers des fraudes à la carte bancaire.

### **À qui s'adresse Card Security ?**

Au grand public, en particulier aux titulaires de cartes de débit et de crédit. La plate-forme offre également de nombreuses informations utiles aux professionnels de la police et des établissements financiers.

### **Les fraudes à la carte bancaire ont-elles augmenté ces dernières années ?**

Auparavant, les fraudes à la carte bancaire concernaient surtout les terminaux de paiement ainsi que les bancomats. Ces cas dits de skimming ont fortement diminué. Aujourd'hui, les délits se produisent principalement sur Internet. Les fraudes à la carte bancaire augmentent de 10 à 20 % par an.

### **Quelles fraudes à la carte bancaires sont-elles les plus courantes sur Internet ?**

La plupart des fraudes en ligne commencent par de l'hameçonnage (phishing). Les escrocs envoient des SMS ou des e-mails à leurs cibles. Le message invite ces dernières à cliquer sur un lien qui les mène à une page piratée. Là, les malfaiteurs tentent d'obtenir un maximum d'informations personnelles : nom, date de naissance, numéro de carte de crédit, date d'expiration. Avec ces données, ils parviennent ensuite à dérober l'argent de leurs victimes.

### **Comment prouver qu'il n' y a pas eu d'hameçonnage au préalable ?**

C'est difficile. Souvent, les victimes ne se souviennent pas avoir reçu un e-mail d'hameçonnage et avoir laissé leurs coordonnées. En effet, il s'écoule généralement beaucoup de temps entre la collecte des données et les transactions frauduleuses.

### **Pourquoi les banques n'assument-elles pas la responsabilité des fraudes ou ne sont-elles pas plus conciliantes ?**

La responsabilité est stipulée dans les contrats conclus entre la banque et ses clients. En cas de litige, la question de la responsabilité doit être clarifiée au cas par cas par un tribunal. On peut toutefois partir du principe que la responsabilité de la banque n'est pas engagée si le client a manqué à son devoir de diligence.

### **Est-il judicieux de porter plainte contre inconnu ?**

Oui. Les cyber-escrocs laissent des traces qui peuvent être suivies. Selon leur méthode de dissimulation, il peut toutefois être difficile de remonter jusqu'aux auteurs de l'infraction. C'est pourquoi le dépôt de plainte est important pour la police. C'est le seul moyen dont elle dispose pour obtenir des informations clés et pour pouvoir évaluer l'ampleur de la menace.

À partir du moment où la police (en tant que poursuivant) a connaissance de la situation globale, elle est en capacité de prendre des mesures transfrontalières. Ainsi, des observations supplémentaires peuvent être collectées, contribuant à renforcer la démarche préventive.

Selon le mode opératoire des malfaiteurs, il peut s'avérer difficile de savoir où l'argent est passé. Ceux-ci font souvent appel à des "mules" (blanchisseurs d'argent) qui opèrent dans des pays posant de grands défis à la police ou qui utilisent des services anonymes pour brouiller les pistes.

## **L'argent liquide n'est-il pas plus sûr finalement ?**

L'argent liquide perd de plus en plus de terrain. Souvent, il n'est même plus possible de payer en espèces. Il est donc d'autant plus important que les titulaires de cartes se protègent le mieux possible lorsqu'ils utilisent leurs cartes de crédit ou de débit et qu'ils adoptent les bons gestes.

La majorité des fraudes à la carte bancaire peuvent être évitées grâce à quelques conseils de prévention, à retrouver sur la plate-forme de prévention <https://www.card-security.ch/fr/protéger-sa-carte/>

## **Que puis-je faire pour me protéger contre les fraudes à la carte bancaire ?**

- Informez-vous sur [card-security.ch](https://www.card-security.ch), la plateforme de la police contre la fraude à la carte bancaire.
- Ignorez les e-mails qui vous demandent de cliquer sur des liens pour fournir des mots de passe et des données personnelles.
- Ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes des e-mails suspects.
- Ne communiquez jamais vos codes SMS à des tiers.
- N'entrez vos identifiants de connexion que sur le site officiel d'un fournisseur (jamais via un e-mail ou un SMS).
- Ne communiquez jamais vos identifiants de connexion ou les données de votre carte si vous n'avez pas procédé au préalable à un examen attentif du site marchand.
- Faites bloquer votre carte si vous en avez divulgué les données.
- Activez les notifications automatiques de paiement par carte via SMS.
- Désactivez temporairement votre carte si vous ne l'utilisez pas.
- Désactivez certaines fonctionnalités de la carte (commerce électronique).
- Déposez une plainte auprès de la police si de l'argent vous a été dérobé.
- Vérifiez vos décomptes de cartes et signalez toute anomalie.

## **Contact**

Card Security

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

T: 043 243 65 50