Q & R

Card Security : c'est quoi exactement et qui est derrière cette initiative ?
Card Security est une initiative nationale de prévention qui œuvre pour la protection contre les délits liés aux cartes de débit et de crédit. Elle vise à sensibiliser le grand public à travers des campagnes ciblées sur les réseaux sociaux, des reportages dans les médias et la diffusion d'informations aussi bien sur ses réseaux partenaires que sur son site internet card-security.ch. Son action préventive consiste essentiellement à alerter la population sur les arnaques en cours et à diffuser les bonnes pratiques pour une utilisation des cartes de débit et de crédit en toute sécurité. La plateforme sert également de ressource approfondie pour les professionnel(le)s des corps de police et des institutions financières.

L'initiative Card Security, qui émane des corps de police, est portée par l'association du même nom, dont le comité directeur réunit des représentant(e)s des sociétés émettrices de cartes et des forces de l'ordre. Elle bénéficie d'un large soutien institutionnel, notamment de la police, des sociétés émettrices de cartes et des établissements bancaires.

En quoi Card Security est-elle indispensable ?
Les infractions liées aux cartes de débit et de crédit connaissent une progression annuelle de 10 à 20 %. Card Security s'impose comme la plateforme de référence de la police pour toutes les questions relatives à l'utilisation frauduleuse des cartes de paiement. Card Security fédère en effet les expertises issues des corps de police, des établissements bancaires et des émetteurs de cartes. Le site internet card-security.ch met à disposition des titulaires de cartes, des agents de police et du personnel bancaire un ensemble d'informations détaillées sur les stratégies frauduleuses émergentes et sur les mesures préventives recommandées.

Card Security cible également un public professionnel. Via la plateforme card-security.ch, les personnels des corps de police et des institutions financières peuvent accéder aux campagnes en cours, aux ressources pédagogiques et à un ensemble complet d'informations spécialisées.

« LINDA te protège du phishing ! » - qu'est-ce que cela signifie ?
La campagne Card Security 2026 s'articule autour du slogan « LINDA te protège du phishing ! ». LINDA, représentée par une pêcheuse, incarne un acronyme dont chaque lettre constitue une règle mnémotechnique pour déjouer les tentatives d'hameçonnage (phishing) :

L = Liens et annexes : à évaluer
I = Informations : à vérifier
N = Neutralité de l'entête : à analyser
D = Délais urgents : à suspecter
A = Adresse expéditeur : à authentifier

L'acronyme LINDA constitue ainsi un aide-mémoire efficace permettant aux titulaires de cartes de débit et de crédit de mémoriser les bonnes pratiques et de déjouer les tentatives d'hameçonnage.

À qui s'adresse Card Security ?
Principalement aux titulaires de cartes de débit et de crédit. La plateforme constitue également une ressource précieuse pour les professionnel(le)s des corps de police et des institutions financières.

Les fraudes à la carte ont-elles augmenté ces dernières années ?
Le phénomène a évolué : autrefois concentrées sur les terminaux de paiement et les bancomats, les fraudes par « skimming » ont considérablement diminué. En revanche, les délits se sont massivement déplacés vers la sphère numérique, avec une progression annuelle de 10 à 20 %.

Quelles sont les fraudes à la carte les plus fréquentes en ligne ?
La majorité des vols commence par du phishing (hameçonnage). En manipulant leurs cibles, les cyber-escrocs les amènent à divulguer des données sensibles : codes PIN, codes de confirmation reçus par SMS, numéros CVC/CVV ou mots de passe. Pour ce faire, ils recourent à des sites ou à des QR codes contrefaits, des liens inclus dans des e-mails, des appels ou des messages (SMS, WhatsApp, Messenger, etc.). Une fois ces informations collectées, ils dépouillent leurs victimes.

Comment prouver que la compromission des données ne provient pas d'une attaque d'hameçonnage ?
C'est difficile. Entre le moment où les données sont dérobées et celui où elles sont utilisées, il s'écoule souvent plusieurs mois. Ce délai rend difficile, pour les victimes, le souvenir précis d'avoir cliqué sur un lien suspect ou d'avoir répondu à un message frauduleux.

Pourquoi les banques n'assument-elles pas la responsabilité en cas de fraude ou ne font-elles pas preuve de plus de souplesse ?
Les clauses contractuelles définissent précisément la répartition des responsabilités entre chaque établissement financier et ses client(e)s. En cas de litige, seule l'autorité judiciaire peut statuer sur chaque cas spécifique. Néanmoins, le principe généralement admis décharge la responsabilité de l'établissement lorsque le client a enfreint son devoir de diligence.

Est-il pertinent de porter plainte contre inconnu ?
Absolument. Les cyber-escrocs laissent des traces numériques, même si leurs stratégies d'anonymisation ne permettent pas toujours de remonter jusqu'aux auteur(e)s de l'infraction. Le dépôt de plainte fournit aux autorités des renseignements essentiels pour mesurer l'ampleur réelle du phénomène.

Cette compréhension approfondie permet aux forces de police d'orchestrer des opérations transfrontalières et d'affiner leur démarche préventive. Toutefois, le recouvrement des fonds subtilisés demeure complexe face au recours à des « mules financières » (intermédiaires servant au blanchiment) qui opèrent depuis des pays posant de grands défis à la police ou utilisant des services garantissant l'anonymat.

L'argent liquide n'est-il pas plus sûr finalement ?
Les espèces perdent progressivement du terrain, certaines transactions étant désormais exclusivement électroniques. Il devient donc impératif pour les titulaires de cartes de débit et de crédit d'adopter des comportements sécuritaires.

La majorité des fraudes à la carte peuvent être déjouées en appliquant quelques mesures de prévention simples, détaillées sur la plateforme card-security.ch/fr/proteger-sa-carte/

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

LINDA te protège du phishing !

L = Liens et annexes : à évaluer
I = Informations : à vérifier
N = Neutralité de l'entête : à analyser
D = Délais urgents : à suspecter
A = Adresse expéditeur : à authentifier