QUE FAIRE EN CAS DE SKIMMING ?

Vous avez de fortes présomptions de piratage sur un automate ou vous pensez avoir été victime de skimming ? Adopter les comportements suivants vous sera utile :

- N'utilisez aucun automate qui vous paraît suspect. Si votre carte n'est pas restituée sans raison valable, le mieux est de rester devant l'appareil jusqu'à ce que la situation se règle ou de faire bloquer immédiatement votre carte. Contactez l'opérateur de l'automate ou l'établissement financier compétent et, en dehors des heures d'ouverture, la police via le numéro d'urgence 117. Suivez les instructions de la police et ne touchez à rien jusqu'à son arrivée.
- N'acceptez pas l'aide de tierces personnes. Il peut s'agir d'escrocs ou de leurs complices.
- Faites bloquer votre carte si vous soupçonnez une utilisation frauduleuse. Agissez de même en cas de perte ou de vol de votre carte, ou encore si votre carte n'est pas restituée sans raison valable par l'automate.

FAIRE BLOQUER SA CARTE

Afin de bloquer immédiatement votre carte, ayez toujours sur vous votre numéro de carte et le numéro de téléphone du service client de votre fournisseur de carte. Protégez-vous contre le skimming !

Pour en savoir plus : www.stop-skimming.ch

« Stop skimming » – une campagne menée par votre police

Attention à vos cartes

Votre police

GARE AU SKIMMING !
www.stop-skimming.ch

FAITES ATTENTION À VOTRE ARGENT !

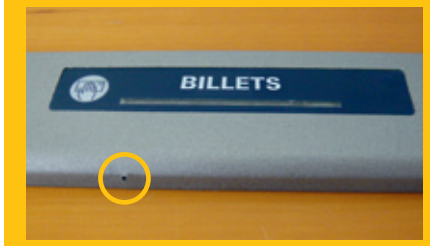
Une fraude sophistiquée consiste à voler votre argent directement sur votre compte. Pour cela, les fraudeurs se procurent illégalement des informations sur vos cartes bancaires, de débit et de crédit puis retirent de l'argent à votre insu. Cette escroquerie est appelée skimming.

Le nombre de vols par skimming en Suisse a fortement augmenté ces derniers temps. Dans de nombreux cas, les malfaiteurs profitent du manque de méfiance de leurs victimes.

Quelques précautions suffisent pour vous protéger de ces retraits frauduleux. Retrouvez toutes les informations utiles dans ce dépliant.

QU'EST-CE QUE LE SKIMMING ?

Le skimming consiste à manipuler les automates et terminaux de paiement (bancomats, distributeurs de billets et terminaux de paiement dans les commerces, les stations-service, la restauration, etc.). Pour ce faire, les escrocs se servent d'un équipement spécial introduit dans les automates ou à proximité, qui copie les données contenues sur la piste magnétique de la carte bancaire, de débit ou de crédit et enregistre le code NIP. Les malfaiteurs agissent généralement en bandes organisées.



Caméra miniature (exemple)
Filme la saisie non protégée du code NIP.

Dispositif pirate placé sur la fente d'introduction de la carte (exemple)
Copie les données de la piste magnétique.

CONSEILS DE SÉCURITÉ

PROTECTION CONTRE LE SKIMMING

Les conseils suivants vous seront utiles pour vous protéger contre le skimming et les autres fraudes à la carte bancaire.

Confidentialité du code NIP
Votre code NIP est strictement confidentiel et ne doit en aucun cas être divulgué à des tiers, conservé avec la carte ou noté sur la carte. N'entrez jamais votre code NIP au niveau de l'ouvre-porte.

Saisir son code NIP à l'abri des regards
Quel que soit l'automate, composez toujours votre code NIP à l'abri des regards. Pour ce faire, cachez le clavier avec votre main ou avec votre portefeuille lorsque vous composez votre code confidentiel. Ne laissez personne voir le code NIP que vous entrez. Demandez aux personnes qui s'approchent de trop près de garder leurs distances.

Faire part de ses soupçons
Si vous découvrez qu'un automate a été piraté ou si vous avez de fortes présomptions, avertissez immédiatement l'opérateur de l'appareil ou l'établissement financier compétent. En dehors des heures de bureau, contactez la police via le numéro d'urgence 117. Vous contribuerez ainsi à éviter d'autres préjudices.

Contrôler ses comptes
Vérifiez régulièrement vos relevés de compte et contactez immédiatement votre établissement financier si vous constatez des anomalies.

« Stop skimming » – une campagne menée par votre police