Communiqué de presse

GARE AU SKIMMING !
www.stop-skimming.ch

LES MESURES CONTRE LE SKIMMING FONCTIONNENT, LE PHISHING AUGMENTE

L'évolution des délits de skimming en Suisse est positive : les cas de skimming sont en net recul. Ceci peut être dû, d'une part, aux différentes mesures des instituts financiers et d'autre part, aux mesures de précaution plus élevées du côté des titulaires de cartes. Cependant, un déplacement des délits sur le World Wide Web se fait sentir : les cas de phishing ont fortement augmenté. Les coupables obtiennent les données d'accès des comptes par le biais de faux e-mails, SMS, sites Web ou appels téléphoniques.

Berne, le 28 janvier 2014 – Le nombre de délits de skimming a considérablement diminué en 2013. Il y a eu 114 cas au total (année précédente 369). Plus de 12'874 cartes ont été bloquées de manière préventive (année précédente 29'000).

Normes de sécurité élevées des distributeurs de billets
Ceci est le résultat de mesures de sécurité et de précaution importantes, du côté des instituts financiers. En Suisse, la norme de sécurité des distributeurs de billets est très élevée par rapport au niveau international. À cela s'ajoute le fait que la plupart des instituts financiers attirent l'attention des clientes et clients sur le skimming, directement au niveau des distributeurs de billets et montrent comment s'en protéger. D'autres mesures, telles que le nouveau Card Control (géoblocage/contrôle des limites ou géocontrôle) et une vaste campagne de prévention (www.stop-skimming.ch), menée avec la police, ont contribué à renforcer la sensibilisation de la population.

D'autres distributeurs de billets s'équipent
L'année dernière déjà, on a pu constater un déplacement des délits de skimming des distributeurs de billets vers les terminaux de paiement, automates à billets et à essence. Actuellement, les fournisseurs équipent également ces appareils. « Naturellement, comme pour tous les délits, la sécurité totale n'existe pas. Les skimmers cherchent toujours de nouveaux points faibles. L'expérience montre que la meilleure protection contre le skimming reste toujours le masquage de la saisie du code NIP. Les titulaires de cartes peuvent donc eux-mêmes contribuer à la poursuite de la baisse des cas de skimming », d'après Urs Widmer, chef de service de la division d'enquête sur la criminalité économique de la police cantonale de Zurich.

Un net décalage vers le phishing
En Suisse, force est de constater un net décalage vers les cas de phishing. Dans ce type de fraude, les données d'accès pour les opérations bancaires en ligne, les confirmations de transactions de cartes de crédit (3-D Secure, SecureCode), les systèmes de paiement (par exemple PayPal), les plates-formes commerciales (eBay, Ricardo et autres) ou les fournisseurs en ligne sont récupérées afin de piller les comptes ou d'effectuer des transactions.

Généralement, les fraudeurs par phishing envoient des e-mails ou des SMS trompeurs, de la part d'un expéditeur faussé d'un institut financier et indiquent à leurs victimes que les données d'accès à un compte particulier ne sont plus sûres ou qu'une transaction frauduleuse est soupçonnée. Il est demandé aux victimes de saisir leurs données d'accès sous le lien indiqué. Cependant, ce lien ne mène pas au site Internet de l'institut financier, mais à un site Web des malfaiteurs, qui ressemble à s'y méprendre au site Web officiel de l'institut financier. La victime y indique son nom d'utilisateur, mot de passe et autres données sensibles.

Cependant, les fraudeurs par phishing contactent de plus en plus souvent leurs victimes par téléphone (le Voice Phishing ou Vishing). Les malfaiteurs se font par exemple passer pour des collaborateurs du service client d'un institut financier. Dans des circonstances semblables au phishing traditionnel, ils convainquent leurs victimes d'indiquer leurs données d'accès personnelles ou même de confirmer sans le savoir des transactions frauduleuses.

Appel à la responsabilité
En général, les fraudeurs par phishing sont très adroits. Ils savent tromper leurs victimes. « Pour éviter le phishing, comme dans la prévention du skimming, nous faisons fortement appel à la responsabilité de chacun. Un institut financier ne demande jamais les données d'accès, que ce soit par e-mail, téléphone ou un autre moyen de communication. Quiconque donne volontairement ses données se conduit de manière imprudente et ouvre la porte aux abus », d'après Urs Widmer, chef de service de la division d'enquête sur la criminalité économique de la police cantonale de Zurich. C'est pourquoi la police et les instituts financiers déconseillent vivement de donner les données d'accès aux comptes à des tiers. Une méfiance saine et la protection de ses propres données de compte et de carte sont essentielles pour éviter ce genre de délits.

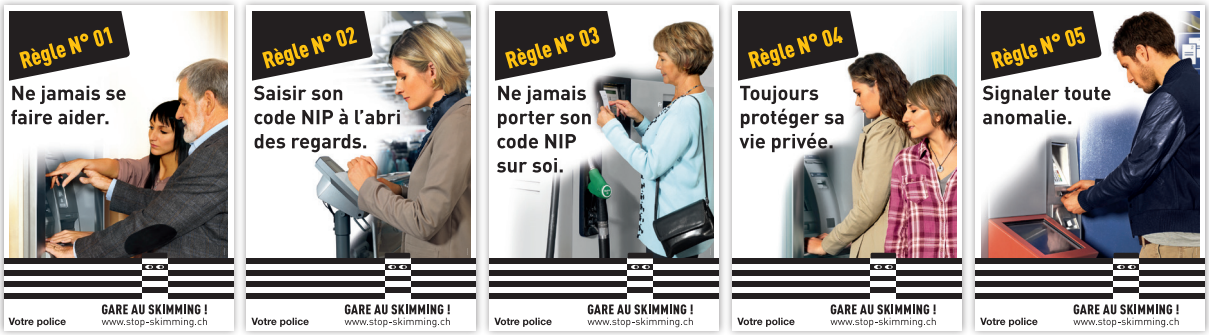
A propos de la campagne

La campagne nationale « Stop skimming » a débuté le 5 mars 2012. La campagne est signée « Votre police ».

Le logo de la campagne montre un voleur en habit de bagnard / de piste magnétique. Ainsi, le skimming est explicitement associé à un vol.

GARE AU SKIMMING !
www.stop-skimming.ch

Le cœur de la campagne est constitué de cinq règles simples qui contribuent à éviter le skimming de manière significative.



La campagne comprend les mesures suivantes :

- Affichage national sur 1600 emplacements
- 11'000 emplacements supplémentaires dans les corps de police
- Site internet
- Dépliants
- Informations sur l'écran d'accueil des bancomats
- Bannières sur les sites internet des banques et des corps de police

Qu'est-ce que le skimming ?

Le terme skimming vient de l'anglais « to skim », écrémer.

Le skimming consiste à manipuler les automates (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 ou sur les automates, qui copie les données contenues sur la piste magnétique de la carte bancaire, de débit ou de crédit et espionne la saisie du code NIP. Les malfaiteurs agissent généralement en bandes organisées.

En Suisse, le retrait d'espèces n'est pas possible avec les cartes PostFinance Card Direct et Maestro si elles ne sont pas munies de leur puce inviolable. Mais dans plusieurs pays en dehors de l'Europe, les données de la piste magnétique et le code NIP d'une carte suffisent pour retirer de l'argent. C'est pourquoi, dans les cas de skimming, l'argent est toujours retiré à l'étranger. La plupart des victimes ne constatent la fraude que lorsqu'elles reçoivent leur relevé de compte.

Quelques mesures de précaution suffisent pour vous protéger du skimming. Pour en savoir plus, cliquez sur www.stop-skimming.ch.

Contacts

Martin Boess
Directeur de la Prévention Suisse de la Criminalité (PSC)
E-mail: mb@skppsc.ch
Tél.: 031 320 29 50

Rolf Nägeli
Chef du commissariat à la prévention et la communication, police municipale de Zurich
E-mail: rolf.naegeli@stp.stzh.ch
Service de presse de la police municipale Tél: 044 411 91 11

Urs Widmer
Chef de service DE criminalité économique, délits économiques, police cantonale de Zurich
E-mail : wid@kapo.zh.ch
Service de presse de la police cantonale Tél: 044 247 36 36

Sindy Schmiegel
Association suisse des banquiers (ASB)
E-mail: sindy.schmiegel@sba.ch
Tél.: 061 295 93 93

Pour les chiffres actuels relatifs aux cas de skimming, veuillez contacter:
SIX Management AG
Media Relations
Selnaustrasse 30
8001 Zurich
E-mail: pressoffice@six-group.com
Tél: 058 399 2227

Communiqué de presse et images

Le communiqué de presse complet est disponible au format PDF et sous http://www.stop-skimming.ch/fr/a_propos_de_cette_campagne/medias/.

Des images sont disponibles sous ce lien:
www.stop-skimming.ch/fr/a_propos_de_cette_campagne/medias/.