

## Fraude à la carte bancaire

# La police s'attaque au piratage des bancomats

Près de 180 cartes de paiement falsifiées ont été retrouvées par la police genevoise à la mi-mars. Les polices cantonales ont lancé une campagne de prévention contre le «skimming»



Les escrocs se servent d'un dispositif introduit dans ou sur les automates, comme une microcaméra ou un faux clavier, qui copie les données contenues sur la piste magnétique de la carte bancaire, et espionne la saisie du code NIP. Ils peuvent alors fabriquer une fausse carte. DR

## L'essentiel

● **Fraude** Le skimming, consistant à pirater les distributeurs pour réaliser une copie des cartes bancaires, a explosé en 2011.

● **Prévention** Les polices cantonales lancent une campagne de lutte contre ce phénomène, qui touche notamment Genève.

● **Conseils** Quelques précautions permettent de réduire les risques de se faire pirater sa carte.

Sophie Simon

**S**top skimming. C'est le nom de la campagne nationale de prévention contre la fraude à la carte bancaire lancée début mars. Une initiative de toutes les forces de police suisses, notamment celle de Zurich, soutenue par l'Association suisse des banquiers et la Prévention suisse de la criminalité. Le tout financé par les institutions financières.

Le «skimming» consiste à pirater des automates et terminaux de paiement pour obtenir les numéros des cartes bancaires et les codes secrets des utilisateurs, dans le but de réaliser des copies de ces cartes. Si le phénomène existe depuis des années en Suisse, il s'est répandu largement dès 2010 et a explosé en 2011 (*lire l'infographie ci-dessous*). Pour 2012, les chiffres manquent encore pour tirer une conclusion nette. Bernhard Wenger, porte-parole de Six Group (infrastructure de trafic des paiements), estime que la tendance est à la baisse: «Le nombre de cas de skimming est passé de 3 ou 4 par jour au début de l'année 2011 à 3 ou 4 par semaine actuellement. Les banques ont investi pour sécuriser leurs appareils, et les clients sont plus attentifs à protéger leur code NIP.»

A Genève, il est difficile d'obtenir des chiffres précis. On connaît seulement le nombre de cas relevant de l'article 147 du

Code pénal sur «d'utilisation frauduleuse d'un ordinateur», qui sanctionne l'ensemble des détournements de fonds réalisables avec un ordinateur. Selon ces chiffres, 154 cas ont été dénoncés en 2011, dont une part indéterminée relève du skimming. Pour le premier trimestre 2012, il y a déjà une quarantaine de cas.

### Coup de filet à Genève

Huit «skimmeurs» ont été arrêtés en mars à Genève, indique Jean-Philippe Brandt, porte-parole de la police cantonale. Parmi lesquels six Chinois pour une seule et même affaire: des membres de la filière ont essayé d'acheter deux montres pour une valeur de 27 000 francs, mais la bijouterie concernée a eu des doutes. La police a réussi à retrouver l'hôtel où les individus logeaient, et a procédé aux arrestations au fur et à mesure des avancées de l'enquête. Les fraudeurs possédaient au total près de 180 cartes skimmées! «En imaginant que chaque carte a une limite de 5000 francs, je vous laisse faire le calcul», commente Jean-Philippe Brandt. Le calcul est fait: un potentiel de 900 000 francs à retirer frauduleusement. Le Ministère public n'a pas souhaité communiquer sur cette affaire, l'enquête étant en cours.

Y a-t-il un profil de skimmeurs? Toujours selon la police genevoise, il y aurait deux groupes distincts. Les skimmeurs de cartes de retrait, qui piègent les bancomats dans le but d'obtenir de l'argent cash, sont plutôt originaires de Roumanie. Et les skimmeurs de cartes de crédit étrangères, utilisées pour effectuer des achats ici, qui sont généralement originaires d'Extrême-Orient (Malaisie, Hongkong, Singapour...) Il s'agit là d'un skimming «de haut rendement à l'échelle internationale».

Selon Rebeca Garcia, responsable communication de l'Association suisse des banquiers, «la hausse des cas de skim-

ming est due au fait que les criminels ont élargi leur réseau: en dehors des bancomats, d'autres compagnies qui acceptent les cartes de débit et crédit (La Poste, les CFF, le commerce de détail) sont victimes d'attaques.»

Vérification faite du côté des Chemins de Fer Fédéraux, Frédéric Revaz, porte-parole, affirme que «cinq cas de skimming ont touché les gares genevoises en 2011 dont deux cas en novembre à Genève aéroport. Ensuite, aucun cas n'a été rapporté jusqu'en mars 2012, où trois appareils piratés ont été signalés à l'intérieur de Cornavin.»

Quant à La Poste, Marc Andrey, porte-parole de PostFinance, explique qu'«il n'y a jamais eu de cas de skimming sur les postomats. Par contre des Postcards ont été skimmées sur des distributeurs d'autres banques.»

Les quelques stations-service genevoises que nous avons contactées ne semblent pas avoir connu de problèmes.

### 14 millions dérobés

En 2011, plus 14 millions de francs ont été dérobés grâce au skimming. Les banques jouent-elles le jeu en matière de remboursement des clients? Oui, selon Christian Guex, ombudsman des banques pour la Suisse romande: aucune réclamation de

client n'a été enregistrée en 2011 ni en 2012. Il faut cependant que le cas de skimming soit établi, donc que le client soit encore en possession de sa carte. Rebeca Garcia estime que dans la plupart des cas le remboursement est possible, si les conditions générales de la carte de paiement ont été respectées. Par exemple il ne faut pas avoir communiqué le code à un tiers ou l'avoir conservé avec la carte.



Retrouvez la campagne «Stop skimming» sur: [www.stop-skimming.ch](http://www.stop-skimming.ch)

## Cas de «skimming» dans les bancomats en Suisse

Ces données concernent uniquement les cartes Maestro			
	2009	2010	2011
Nombre de cartes bloquées à la suite d'un «skimming»	Environ 6200	Environ 5500	<b>Environ 34 000</b>
Nombre de transactions effectuées	11 991	11 617	<b>29 818</b>
Sommes dérobées en francs	3,6 millions	4,7 millions	<b>14,2 millions</b>
Nombre de bancomats piratés	32	135	<b>489</b>

\* Chiffres convertis du dollar américain

O. CHIACCHIARI SOURCE: SIX GROUP

## Conseils pratiques de la campagne

### Recommandations adressées aux titulaires de cartes:

**Saisir son code NIP** à l'abri des regards, c'est-à-dire en le masquant avec la main pour éviter qu'il ne puisse être filmé.

**Ne jamais se faire** aider pendant un retrait, ne pas se laisser distraire.

**Signaler toute anomalie** sur un automate: pièces desserrées, détériorations, rayures, traces de colle.

**Vérifier régulièrement** ses relevés de compte et contacter immédiatement l'établissement financier si vous constatez des irrégularités.

**Le code NIP** ne doit pas être conservé avec la carte.

**Ne jamais communiquer** son code ou donner sa carte à des tiers.

### Recommandations adressées aux commerçants:

**Les skimmers** veulent acheter vite et cher. La rapidité de l'acte d'achat est un indice.

**Ils ne connaissent** pas les limites d'achat des cartes fraudées.

Il arrive donc qu'ils paient avec plusieurs cartes, ou qu'ils changent de carte en cours d'achat.

**Les derniers chiffres** qui apparaissent sur une carte skimmée sont aléatoires: donc le numéro qui apparaît en relief sur la carte physique ne correspond pas au numéro inscrit sur le ticket.

**Les escrocs se font souvent** passer pour des techniciens. N'autorisez l'accès qu'aux techniciens que vous employez. **S.S.**