Payment Services

Prévention anti-skimming pour terminaux intérieurs et extérieurs

Empêchez le piratage des données de cartes («skimming»)[1] dans le périmètre intérieur et extérieur de votre point de vente! Détectez le plus tôt possible d'éventuelles manipulations opérées à votre insu sur votre terminal de paiement et prenez les mesures qui s'imposent. En votre qualité de commerçant, vous et vos collaborateurs jouez un rôle crucial dans la prévention ou la réduction des dommages financiers susceptibles de survenir dans ce genre de fraudes.

Préparation: photographiez le terminal de paiement/l'automate dans son état original.

⚠ Tirez deux photos de chaque terminal de paiement utilisé:
- une vue de la fente d'introduction des cartes;
- une vue du clavier sur lequel le numéro secret d'identification personnel (NIP) est composé.

Ces photos servent de référence lorsque vous effectuez des comparaisons au cours des contrôles quotidiens recommandés. Elles vous permettent de déceler si des dispositifs frauduleux de prélèvement des données de cartes («skimming») ont été installés à votre insu.

Conseils pour les contrôles

⚠ Le matin, à midi et le soir, lorsque vous arrivez ou quittez votre lieu de travail, vérifiez si les modules suivants ont fait l'objet de manipulations.

A cet effet, comparez les photos originales susmentionnées avec ces éléments:
- le clavier et la fente d'introduction des cartes du terminal de paiement;
- toutes les zones du point de vente et de son périmètre extérieur susceptibles d'être équipées d'une caméra miniature dont le champ visuel couvrirait le clavier.

Même si ce sont les automates situés à l'extérieur qui sont les plus menacés, nous recommandons de contrôler aussi les terminaux de paiement se trouvant à l'intérieur du point de vente.

Si vous suspectez une manipulation, voici comment procéder:

1. N'autorisez plus d'opérations de paiement sur le terminal concerné.
2. Ne démontez **aucun** dispositif de prélèvement frauduleux des données de cartes («skimming») installé à votre insu (p. ex. des modules près de la fente d'introduction des cartes, des caméras miniatures, etc.).
3. Si la manipulation concerne un automate/un terminal de paiement situé à l'extérieur, éloignez-vous car le malfaiteur se trouve peut-être encore dans les parages, en observation.
4. Informez immédiatement la police.
5. Remplissez le «Formulaire en cas de manipulations d'un ATM ou d'un autre terminal» et retournez-le au plus vite (veuillez observer les indications figurant sur le formulaire!). Vous trouverez ce formulaire sous www.six-payment-services.com/skimming

[1] Skimming = terme anglais signifiant «écrémer». Lors du skimming, le terminal de paiement est modifié de telle manière que l'auteur de cette manipulation puisse prendre connaissance des données contenues sur la piste magnétique de la carte et du numéro secret d'identification personnel (NIP) du titulaire de la carte. Le prélèvement frauduleux des données est réalisé par le malfaiteur qui place un dispositif comportant une tête de lecture de piste magnétique devant le lecteur de cartes ainsi qu'une caméra miniature ou un faux élément de clavier.

110.0011.03 INT_FR/02.2016

Les coordonnées de votre interlocuteur local sont disponibles sous: www.six-payment-services.com/contacts

SIX Payment Services SA
Hardturmstrasse 201
Case postale
CH-8021 Zurich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Vienne
Autriche