Medienmitteilung

VORSICHT SKIMMING!
www.stop-skimming.ch

SKIMMING-MASSNAHMEN GREIFEN, PHISHING NIMMT ZU

Die Entwicklung der Skimming-Delikte in der Schweiz zeigt ein erfreuliches Bild: Skimming-Fälle sind deutlich rückläufig. Dies kann einerseits auf verschiedene Massnahmen seitens der Finanzinstitute, andererseits aber auch auf höhere Vorsichtsmassnahmen auf Seiten der Kartenbesitzer zurückgeführt werden. Zu spüren ist jedoch eine Verlagerung der Delikte ins World Wide Web: Phishing-Fälle haben stark zugenommen. Die Täter gelangen dabei via gefälschte E-Mails, SMS, Webseiten oder Telefonanrufe an die Login-Daten von Kontobesitzern.

Bern, 28. Januar 2014 – Die Zahl der Skimming-Delikte hat 2013 massiv abgenommen. Insgesamt gab es 114 Fälle (Vorjahr 369). Über 12 874 Karten wurden präventiv gesperrt (Vorjahr 29 000).

Hohe Sicherheitsstandards bei Geldautomaten
Dies ist das Resultat konsequenter Sicherheits- und Vorsichtsmassnahmen seitens der Finanzinstitute. In der Schweiz ist der Sicherheitsstandard der Geldautomaten auf einem im internationalen Vergleich sehr hohen Niveau. Hinzu kommt, dass die meisten Finanzinstitute Kundinnen und Kunden direkt an den Geldautomaten auf Skimming aufmerksam machen und auch zeigen, wie man sich davor schützen kann. Weitere Massnahmen wie das neu eingeführte Card Control (Geoblocking/Limiten- resp. Geocontrol) und eine breit angelegte Präventionskampagne (www.stop-skimming.ch), die zusammen mit der Polizei durchgeführt wurde, haben zur verstärkten Sensibilisierung der Bevölkerung beigetragen.

Andere Kartenautomaten rüsten nach
Bereits im Vorjahr war eine Verlagerung der Skimming-Delikte weg von den Geldautomaten hin zu den Zahlterminals, Billet- und Tankomaten festzustellen. Auch bei diesen Geräten rüsten die Anbieter derzeit nach. «Selbstverständlich gibt es wie bei jedem Delikt nie eine hundertprozentige Sicherheit. Skimming-Täter suchen immer wieder nach neuen Schwachstellen. Die Erfahrung zeigt, dass der beste Schutz vor Skimming nach wie vor das Abdecken der PIN-Code-Eingabe ist. Die Kartenbesitzer können also selber viel dazu beitragen, dass die Skimming-Fälle weiter abnehmen», so Urs Widmer, Dienstchef in der Ermittlungsabteilung Wirtschaftskriminalität der Kantonspolizei Zürich.

Deutliche Verlagerung in Richtung Phishing
Auffallend ist, dass in der Schweiz eine deutliche Verlagerung hin zu Phishing-Vorfällen stattfindet. Bei dieser Betrugsart werden die Zugangsdaten für Online-Banking, Kreditkarten-Transaktionsbestätigungen (etwa 3-D Secure, SecureCode), Bezahlsysteme (zum Beispiel PayPal), Handelsplattformen (eBay, Ricardo und andere) oder Online-Versandanbieter in Erfahrung gebracht, um damit die Konten zu plündern oder Transaktionen zu tätigen.

In der Regel verschicken die Phisher betrügerische E-Mails oder SMS mit gefälschtem Absender eines Finanzinstituts und informieren darüber ihre Opfer, dass die Zugangsdaten zu einem bestimmten Konto nicht mehr sicher sind oder eine betrügerische Transaktion vermutet wird. Die Opfer werden aufgefordert, ihre Zugangsdaten unter einem angegebenen Web-Link einzutragen. Dieser Link führt jedoch nicht auf die Internetseite des Finanzinstituts, sondern auf eine Webseite der Täter, die der offiziellen Webseite des Finanzinstituts zum verwechseln ähnlich sieht. Das Opfer gibt dort gutgläubig Benutzernamen, Passwörter und ähnliche Angaben ein.

Immer häufiger treten die Phisher allerdings auch per Telefon in den Dialog mit ihren Opfern (sogenanntes Voice Phishing, oder Vishing). Die Täter geben sich dabei zum Beispiel als Mitarbeitende des Kundensupports eines Finanzinstituts aus. Unter ähnlichen Vorwänden wie beim traditionellen Phishing überreden sie ihre Opfer wiederum, persönliche Zugangsdaten preiszugeben oder sogar unwissentlich betrügerische Transaktionen zu bestätigen.

Appell an Eigenverantwortung
Phisher gehen in der Regel sehr geschickt vor. Sie verstehen es, ihre Opfer zu täuschen. «Zur Verhinderung von Phishing appellieren wir ebenso wie bei der Prävention gegen Skimming sehr stark an die Eigenverantwortung jedes Einzelnen. Ein Finanzinstitut fragt nie von sich aus nach Login-Daten, egal ob per E-Mail, Telefon oder mit einem anderen Kommunikationsmittel. Wer diese Daten freiwillig herausgibt, geht fahrlässig vor und öffnet dem Missbrauch Tür und Tor», so Urs Widmer, Dienstchef in der Ermittlungsabteilung Wirtschaftskriminalität der Kantonspolizei Zürich. Polizei und Finanzinstitute warnen deshalb dringend davor, Zugangsdaten zu Konten an Dritte herauszugeben. Ein gesundes Misstrauen und das Schützen der eigenen Konto- und Kartenangaben sind zentral, um solche Delikte zu verhindern.

Zur Kampagne

Die nationale Kampagne «Stop Skimming» startete am 5. März 2012. Absender der Kampagne ist «Ihre Polizei».

Das Kampagnen-Logo zeigt einen Dieb im Sträflings- bzw. Magnetstreifen-Anzug. Damit wird verdeutlicht, dass es sich bei Skimming um Diebstahl handelt.

VORSICHT SKIMMING!
www.stop-skimming.ch

Im Zentrum der Kampagne stehen fünf einfache Verhaltensregeln, die massgeblich dazu beitragen, Skimming zu vermeiden.

Die Kampagne umfasst folgende Massnahmen

- Nationale Plakatierung mit 1600 Plakatstellen
- 11 000 zusätzliche Plakate durch Polizeikorps ausgehängt
- Website
- Informationsflyer
- Intros an Geldautomaten
- Banner auf Websites von Banken und Polizeikorps

Was ist Skimming?

Der Begriff Skimming wird vom englischen Wort «to skim» abgeleitet, was so viel bedeutet wie «abheben», «abschöpfen».

Als Skimming bezeichnet man das Manipulieren von Kartenautomaten (Geldautomaten, Billettautomaten und Zahlterminals im Detailhandel, an Tankstellen, in der Gastronomie usw.). Dabei bringen die Täter spezielle Apparaturen am oder im Automaten an, die die Magnetstreifendaten von Konto-, Debit- und Kreditkarten kopieren und den PIN-Code ausspähen. Bei der Täterschaft handelt es sich häufig um organisierte Gruppen.

In der Schweiz ist es nicht möglich, mit PostFinance Card Direct und Maestro-Karten Bargeld ohne den fälschungssicheren Chip zu beziehen. In verschiedenen aussereuropäischen Ländern genügen jedoch Magnetstreifendaten und PIN-Code, um Geld abzuheben. Aus diesem Grund wird bei Skimming das Geld immer im Ausland abgehoben. Die meisten Opfer bemerken die Tat erst, wenn sie ihren Kontoauszug prüfen.

Vor Skimming kann man sich bereits mit wenigen Vorsichtsmassnahmen schützen. Erfahren Sie mehr unter www.stop-skimming.ch.

Kontakt

Martin Boess
Geschäftsleiter Schweizerische Kriminalprävention (SKP)
E-Mail: mb@skppsc.ch
Tel: 031 320 29 50

Rolf Nägeli
Chef Kommissariat Prävention und Kommunikation, Stadtpolizei Zürich
E-Mail: rolf.naegeli@stp.stzh.ch
Medienstelle Stadtpolizei Tel: 044 411 91 11

Urs Widmer
Dienstchef EA Wirtschaftskriminalität, Wirtschaftsdelikte, Kantonspolizei Zürich
E-Mail: wid@kapo.zh.ch
Medienstelle Kantonspolizei Tel: 044 247 36 36

Sindy Schmiegel
Schweizerische Bankiervereinigung (SBVg)
E-Mail: sindy.schmiegel@sba.ch
Tel: 061 295 93 93

Für aktuelle Zahlen zu Skimming-Fällen wenden Sie sich bitte an:
SIX Management AG
Media Relations
Selnaustrasse 30
8001 Zurich
E-Mail: pressoffice@six-group.com
Tel: 058 399 2227

Medienmitteilung und Bildmaterial

Die vollständige Medienmitteilung finden Sie im PDF sowie unter
http://www.stop-skimming.ch/de/ueber_die_kampagne/medien/.

Unter diesem Link steht Bildmaterial zur Verfügung:
www.stop-skimming.ch/de/ueber_die_kampagne/medien.