Comunicato stampa

ATTENZIONE ALLO SKIMMING!
www.stop-skimming.ch

LE MISURE ANTISKIMMING FUNZIONANO, ORA DILAGA IL PHISHING

Per fortuna, in Svizzera i reati di skimming stanno diminuendo. Merito, da un lato, delle misure di sicurezza adottate dagli istituti finanziari e, dall'altro, della maggiore prudenza dimostrata dai possessori di carte. Purtroppo, però, ora è il web a catalizzare l'attenzione dei truffatori e si moltiplicano i casi di phishing. I phisher sono coloro che tentano di ottenere i dati di login delle loro vittime attraverso e-mail, SMS e siti Internet fasulli o addirittura per telefono.

Berna, 28 gennaio 2014 – Nel 2013 il numero dei reati di skimming è drasticamente diminuito. Complessivamente sono stati registrati 114 casi (369 nell'anno precedente) e in via precauzionale sono state bloccate più di 12 874 carte (29 000 nell'anno precedente).

Standard di sicurezza al top presso gli sportelli Bancomat
Questo risultato è stato raggiunto grazie alle misure precauzionali e di sicurezza adottate dagli istituti finanziari. Oggigiorno in Svizzera lo standard di sicurezza degli sportelli Bancomat è uno dei più elevati a livello internazionale. Inoltre, la maggior parte degli istituti finanziari mette in guardia i propri clienti dal rischio skimming direttamente agli sportelli Bancomat, spiegando loro come tutelarsi. Alla maggiore sensibilizzazione della popolazione, tuttavia, hanno contribuito anche altre misure come la recente introduzione del Card Control (geoblocking, geocontrol o riduzione dei limiti di prelevamento all'estero) e una campagna di prevenzione su vasta scala (www.stop-skimming.ch) condotta in collaborazione con la Polizia.

Anche gli altri distributori automatici si attrezzano
Già lo scorso anno gli skimmer avevano allentato la presa sugli sportelli Bancomat per prendere di mira i terminali di pagamento, i distributori automatici di biglietti e le colonnine self-service delle stazioni di servizio. Ora anche i fornitori di questi apparecchi si stanno attrezzando contro lo skimming. Urs Widmer, Capo del reparto investigativo criminalità economica della Polizia cantonale di Zurigo sostiene: «Naturalmente, come per qualsiasi reato, non si può mai essere sicuri al cento per cento. Gli skimmer sono alla continua ricerca di punti deboli da colpire. L'esperienza insegna che il modo migliore per tutelarsi contro lo skimming è digitare il codice PIN al riparo da occhi indiscreti, coprendo i movimenti delle dita sulla tastiera. I possessori di carta, quindi, possono fare molto per arginare ulteriormente il fenomeno dello skimming».

Si moltiplicano i casi di phishing
In Svizzera lo skimming sta rapidamente lasciando il posto al cosiddetto phishing, una truffa che consiste nel cercare di ottenere le credenziali d'accesso a conti online, sistemi di protezione antifrode per le transazioni con carta di credito (come 3D Secure, SecureCode), sistemi di pagamento (ad es. PayPal), piattaforme di e-commerce (eBay, Ricardo, ecc.) o case di vendita online allo scopo di prosciugare i conti degli ignari malcapitati o di eseguire transazioni illecite.

Normalmente i phisher inviano e-mail o SMS con falso mittente: fingendosi un istituto finanziario, informano le proprie vittime che i loro dati d'accesso a un determinato conto non sono più sicuri o dicono di sospettare una frode ai loro danni. Dopo di che, le invitano a inserire i loro dati d'accesso in una pagina che si apre cliccando su un determinato link. Quest'ultimo però non indirizza alla pagina Internet di un istituto finanziario, bensì a un sito web apparentemente identico creato ad arte dai truffatori. In buona fede, l'ignara vittima digita il proprio nome utente, la propria password e dati simili.

Sempre più spesso, però, i phisher operano anche per telefono. In questo caso la truffa prende il nome di voice phishing o vishing. I visher si fingono operatori del customer support di un istituto finanziario e, come i colleghi phisher, cercano di carpire alle malcapitate vittime i loro dati d'accesso personali o addirittura di convincerle a confermare una transazione illecita.

Appello al senso di responsabilità
Di solito i phisher sono molto abili e sanno come ingannare le loro vittime. «Per non cadere nella trappola del phishing, ci appelliamo, come abbiamo già fatto nella campagna di prevenzione contro lo skimming, vivamente al senso di responsabilità del singolo individuo. Un istituto finanziario non chiederebbe mai i dati di login ai propri clienti con un'e-mail, per telefono o usando altri mezzi di comunicazione. In questi casi, chi rivela volontariamente i propri dati agisce con negligenza e spalanca le porte ai truffatori», spiega Urs Widmer, Capo del reparto investigativo criminalità economica della Polizia cantonale di Zurigo. Polizia e istituti finanziari raccomandano pertanto di non rivelare a nessuno i dati d'accesso al proprio conto. Una sana diffidenza e il mantenimento del più stretto riserbo sulle credenziali d'accesso ai propri conti e alle proprie carte sono fondamentali per impedire che vengano commessi reati di questo tipo.

Sulla campagna

La campagna nazionale «Stop skimming» ha preso il via il 5 marzo 2012 su iniziativa della «vostra polizia».

Il logo rappresenta delle strisce che, oltre a simboleggiare le bande magnetiche, alludono a una divisa da carcerato dietro alla quale si cela un ladro, perché lo skimming è un furto in piena regola.

ATTENZIONE ALLO SKIMMING!
www.stop-skimming.ch

La campagna è incentrata su cinque regole di comportamento molto semplici ma anche molto efficaci nella lotta contro lo skimming.

La campagna prevede le misure seguenti

- Affissione di manifesti in 1600 punti d'affissione su tutto il territorio nazionale
- Affissione di 11 000 manifesti supplementari ad opera della polizia
- Sito web
- Dépliant informativi
- Breve video introduttivo agli sportelli Bancomat
- Banner nei siti web delle banche e dei corpi di polizia

Che cos'è lo skimming?

Il termine skimming deriva dal verbo inglese «to skim» che significa «scremare», «sfiorare».

Per skimming si intende la manomissione dei distributori automatici (sportelli Bancomat, distributori di biglietti e terminali per il pagamento con carta di credito nei negozi, nelle stazioni di servizio, nei ristoranti ecc.). I truffatori si servono di speciali congegni che, applicati ai distributori automatici, sono in grado di copiare i dati contenuti nella banda magnetica delle carte di credito, di debito e di conto e di spiare il PIN mentre viene digitato. Spesso queste truffe sono opera di bande criminali organizzate.

In Svizzera non è possibile prelevare denaro contante con le carte PostFinance Card Direct e Maestro senza il microchip anti-contraffazione. In diversi Paesi extraeuropei, invece, basta aver acquisito i dati della banda magnetica e il codice PIN per poter prelevare denaro contante. È per questo motivo che i prelevamenti illeciti vengono sempre effettuati all'estero. Quasi sempre le vittime dello skimming si accorgono del furto solo dopo aver esaminato l'estratto conto.

Per difendersi dallo skimming basta adottare alcune semplici precauzioni. Per saperne di più, visitate il sito www.stop-skimming.ch.

Contatto

Martin Boess
Direttore della Prevenzione Svizzera della Criminalità (PSC)
E-mail: mb@skppsc.ch
Tel.: 031 320 29 50

Rolf Nägeli
Capo del Commissariato Prevenzione e Comunicazione, Polizia municipale di Zurigo
E-mail: rolf.naegeli@stp.stzh.ch
Ufficio stampa della Polizia municipale, tel.: 044 411 91 11

Urs Widmer
Capo del reparto investigativo criminalità economica e reati economici,
Polizia cantonale di Zurigo
E-mail: wid@kapo.zh.ch
Ufficio stampa della Polizia cantonale, tel.: 044 247 36 36

Sindy Schmiegel
Associazione Svizzera dei Banchieri (ASB)
E-mail: sindy.schmiegel@sba.ch
Tel.: 061 295 93 93

Per avere cifre aggiornate sui casi di skimming rivolgersi a:
SIX Management AG
Media Relations
Selnaustrasse 30
8001 Zurigo
E-mail: pressoffice@six-group.com
Tel: 058 399 2227

Comunicato stampa e materiale grafico

La versione integrale del comunicato stampa è disponibile in formato PDF al link http://www.stop-skimming.ch/it/sulla_campagna/media/.

A questo link trovate il materiale grafico:
www.stop-skimming.ch/it/sulla_campagna/media.