



Comunicato stampa

La polizia mette in guardia con la campagna dai reati di phishing legati alle carte di debito e di credito

Lo shopping online è molto diffuso. Ciò attrae anche truffatori e malintenzionati. I reati legati a carte di pagamento aumentano ogni anno del 10-20 per cento. Il phishing è il tipo di frode più frequente, con il quale i truffatori approfittano della buona fede e dell'ignoranza delle proprie vittime. È proprio su questo aspetto che punta la polizia con la sua campagna. Bastano poche precauzioni da parte dei titolari di carte di pagamento per evitare di essere derubati.

Zurigo, 29 maggio 2024 – Negli ultimi anni il pagamento senza contanti è sensibilmente aumentato. Perché è pratico, comodo e anche molto sicuro purché i titolari delle carte si attengano ad alcune regole di base. Ma proprio questo aspetto è anche la sfida più grande. «Continuiamo a rilevare che i titolari delle carte agiscono con molta imprudenza. Spesso non sono per niente consapevoli di non dovere mai comunicare a terzi dati confidenziali come i codici di sicurezza o i numeri CVV. Anche in caso di un SMS di conferma si dovrebbe premere okay solo se si è davvero sicuri dell'identità del mittente e di chi ha dato l'ordine», spiega Renato Pizolli, ufficiale responsabile del servizio comunicazione, media e prevenzione presso la Polizia Cantonale del Canton Ticino. «Perciò è importante che la polizia informi periodicamente la popolazione sulle poche precauzioni che si possono prendere», continua Pizolli.

Chi rimane vittima di un reato legato a carte di pagamento?

I reati legati a carte di pagamento interessano persone di ogni età e sesso. Può trattarsi di somme esigue oppure anche molto importanti. In Svizzera i reati legati a carte di pagamento non sono rilevati sistematicamente. Una proiezione ipotizza che il danno causato da tali reati ammonti a circa 90 milioni di franchi svizzeri per il 2023. Questa ipotesi si basa sui valori empirici raccolti da singoli istituti finanziari e sulle cifre fornite dalla Banca Nazionale Svizzera in merito ai prelievi effettuati con carte di pagamento nei negozi, in Internet e ai bancomat in Svizzera e all'estero. La somma di reato media oscilla tra circa 1000 e 2000 franchi. Secondo i dati forniti dai corpi di polizia, queste cifre possono risultare anche molto superiori e in singoli casi raggiungono persino l'importo dell'intero limite di prelievo.

«Consigliamo di impostare i limiti di prelievo delle carte solo nella misura effettivamente necessaria», spiega Renato Pizolli. «Per noi è inoltre importante che le vittime sporgano denuncia», prosegue Pizolli. «Purtroppo ciò non avviene sempre. Chi perde solo pochi soldi o si accorge di avere sbagliato, si assume il danno senza denunciare la frode alla polizia». Questo non è un modo di agire ottimale, perché le denunce contribuiscono a comprendere meglio il modus operandi dei truffatori e a riconoscere i nessi. Tutto ciò aumenta notevolmente le possibilità di successo delle indagini svolte dalla polizia.

Professionisti all'opera

Emerge soprattutto un fatto: i truffatori agiscono in modo sempre più professionale. La maggior parte dei reati legati a carte di pagamento iniziano con il phishing. Le potenziali vittime vengono contattate via e-mail, SMS o chat da sconosciuti e attirati con un pretesto su un sito web contraffatto, dove i malfattori «pescano» informazioni riservate. Le vittime sono invitate a inserire sul sito web informazioni personali come le proprie generalità o i dati relativi alla carta di pagamento per poter finalmente vedersi recapitare la merce ordinata o per riattivare un presunto abbonamento bloccato. Chi non sta attento rischia di perdere tanti soldi.

Gli attacchi di phishing si distinguono spesso per aspetto e tono, ma il principio su cui si basano è sempre lo stesso.

Com'è possibile proteggersi dal phishing?

I seguenti accorgimenti aiutano a proteggersi in modo efficace:

- # Diffidare da messaggi provenienti da mittenti sconosciuti. Verificare sempre l'indirizzo e-mail e l'URL del mittente.
- # Non cliccare mai sui link e non aprire gli allegati; loggarsi solo su siti web ufficiali.
- # Insospettirsi se viene chiesto di agire immediatamente.
- # Fornire i dati relativi alla carta di pagamento solo se si è sicuri del processo di pagamento.
- # Leggere attentamente l'SMS di conferma e premere «Okay» solo se si è assolutamente sicuri.
- # Utilizzare password forti e possibilità per l'autenticazione a due fattori (2FA) oppure l'autenticazione a più fattori (MFA).
- # Attivare un servizio di notifica dei pagamenti con carte sul proprio smartphone.
- # Controllare periodicamente le transazioni e gli estratti conto. Notificare immediatamente all'istituto finanziario eventuali irregolarità riscontrate.
- # Ridurre il limite di prelievo. Attivare solo le funzioni della carta che si utilizzano davvero.
- # Sporgere denuncia in caso di frode.

Campagna di prevenzione nazionale della polizia

Già negli anni precedenti la polizia ha agito in modo proattivo lanciando campagne nazionali sul tema delle frodi con carte di pagamento. «La campagna Card Security di quest'anno è focalizzata sul phishing», spiega Renato Pizolli. «Il nostro obiettivo è di consolidare ulteriormente le principali regole comportamentali in vaste fasce della popolazione».

La campagna di quest'anno sarà lanciata in due ondate in primavera (dal 29 maggio al 26 giugno 2024) e in autunno (dal 28 agosto al 25 settembre 2024). La campagna sarà incentrata principalmente sui media online e sulla diffusione da parte dei corpi di polizia.

Sul sito web www.card-security.ch i titolari di carte di pagamento possono costantemente informarsi sui tipi di frode più in voga al momento e sulle precauzioni del caso. Inoltre possono rinfrescare le proprie conoscenze partecipando a un nuovo quiz.

Contatto

Renato Pizolli, ufficiale responsabile del servizio comunicazione, media e prevenzione presso la Polizia Cantonale del Canton Ticino

Telefono: +41 91 814 67 42

E-mail: renato.pizolli@polca.ti.ch

Per richiedere ulteriore materiale fotografico, si prega di inviare un'e-mail a:

info@card-security.ch

Materiale fotografico

