Ecco com’è possibile tutelarsi.

» Diffidare da messaggi provenienti da mittenti sconosciuti.

» Mai cliccare sui link e non aprire gli allegati.

» Verificare sempre l’indirizzo e-mail e l’URL del mittente.

» Loggarsi solo su siti web ufficiali (e non tramite link).

» Tenere sempre aggiornati il browser web e il sistema operativo.

» Mai trasmettere i propri dati di login o delle carte di pagamento.

» Utilizzare password forti e l’autenticazione a due fattori.

» Attivare un servizio di notifica dei pagamenti con carte.

» Verificare le transazioni e i pagamenti.

Testa le tue conoscenze!

Cos’altro posso ancora fare?

» Informati presso la tua banca o la società emittente la tua carta di pagamento in merito alle funzioni di sicurezza della carta.

» Attiva solo le funzioni della carta che utilizzi davvero ogni giorno.

» Sporgi denuncia in caso di furto.

Per maggiori informazioni:
www.card-security.ch

SKPPSC Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

#faiattenzione

Occhio al phishing!

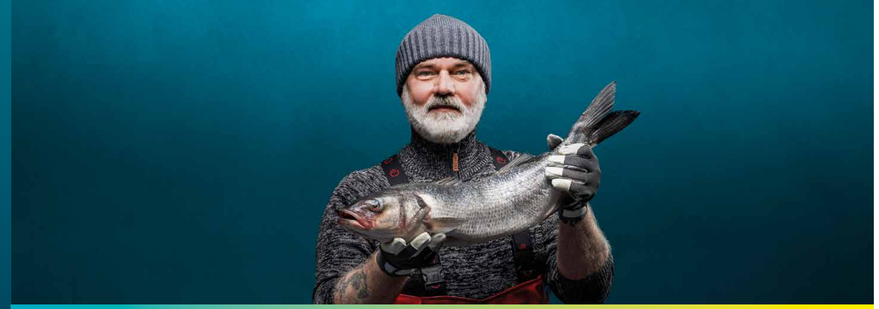
Tutelati dall’abuso delle tue carte di pagamento.

card security

La vostra Polizia

#faiattenzione a questi tipi di FRODE

Le carte di credito e di debito sono mezzi di pagamento molto sicuri e popolari, usate spesso e volentieri per fare shopping online. Ciò attrae anche i truffatori, che tentano di rubare denaro alle loro vittime adottando metodi di frode sempre nuovi. La maggior parte delle frodi con carte di pagamento può essere evitata se i titolari di tali carte si attengono a poche regole di base.



Phishing

Gli attacchi di phishing si distinguono spesso per aspetto e tono, ma il principio su cui si basano è sempre lo stesso. Le potenziali vittime ricevono via e-mail, cellulare o social media messaggi che sembrano provenire da una banca, dalla società emittente la carta di pagamento o da un servizio di consegne. Con un pretesto le vittime vengono invitate a seguire il link contenuto nel messaggio. Chi fa clic sul link finisce su un sito web contraffatto dove viene invitato a fornire informazioni personali. A questo punto, chi non sta attento, rischia di perdere tanto denaro.

Pharming

Il pharming è imparentato con il phishing. Le potenziali vittime inseriscono un indirizzo web corretto e vengono dirottate a loro insaputa su un sito contraffatto. Ciò avviene con l'aiuto di un virus o di un trojan (cavallo di Troia). Come nel caso del phishing, le vittime vengono poi invitate a inserire i loro dati personali e le informazioni relative alla carta di pagamento. Con queste informazioni i malviventi possono infine rubare facilmente il denaro. Questo tipo di frode è denominato «pharming» perché spesso in background vengono gestite intere server farm con siti web contraffatti.

Carding

Nel caso del carding, i truffatori si servono di informazioni relative a carte di pagamento rubate o contraffatte per effettuare acquisti online o per prelevare denaro ai bancomat. Preferiscono carte o shop online scarsamente protetti. I dati necessari per perpetrare le frodi sono stati previamente raccolti illegalmente mediante attacchi di phishing, violazioni alle normative vigenti in materia di protezione dei dati o skimming e venduti nella darknet. Le vittime si accorgono della truffa solo dopo che è già stato sottratto loro denaro. Tra il furto di dati e la truffa vera e propria possono spesso intercorrere mesi.

Scamming

Nel caso dello scamming, invece, i truffatori cercano di attirare le loro potenziali vittime con offerte allettanti. Tutte queste offerte, tuttavia, mirano a convincere con un pretesto le vittime ad anticipare denaro. Lo scamming ha molti volti: truffa affettiva (romance scam), truffa su investimenti finanziari (investment scam), truffa con false offerte locative (flatmate scam), truffa con lavori facili e ideali (employment scam) o promesse di vincite alla lotteria (lottery scam).