#faiattenzione

Occhio al phishing!

card security

La vostra Polizia

CHE COS'È IL PHISHING?

Il phishing è il tipo di frode attualmente più frequente con carte di credito e di debito. Quasi tutte le frodi con carte di pagamento iniziano con un messaggio di phishing. I malfattori agiscono con grande abilità. Ad esempio, camuffano i loro messaggi sotto forma di comunicazioni da parte di una banca, di una società emittente carte di pagamento o di un servizio di consegne. Contattano i destinatari via SMS, WhatsApp, e-mail ecc. invitandoli a seguire il link contenuto nel messaggio, che li reindirizza su un sito web contraffatto dove le vittime devono poi rivelare informazioni personali.

Non appena i «phisher» sono entrati in possesso dei dati, prelevano denaro o effettuano acquisti online con la carta. Chi non sta attento, perde rapidamente tanti soldi.

Chi reagisce alle mail di phishing e trasmette credenziali di accesso o codici, si espone a un grande pericolo: in caso di violazione dell'obbligo di diligenza, di solito i titolari delle carte di pagamento rispondono personalmente dei danni subiti.

CONSIGLI CONTRO GLI ATTACCHI DI PHISHING

Verificare il mittente.

Se non si è sicuri se si tratti di un messaggio di phishing, è meglio controllare subito l'indirizzo e-mail del mittente. Conosci questa persona? L'indirizzo e-mail è credibile? Chiedi ulteriori informazioni direttamente al mittente ufficiale, ad esempio alla banca o al servizio di consegne.

Cercare eventuali errori.

Verifica se l'e-mail inaspettata è autentica. Presta attenzione a logotipi contraffatti, errori di ortografia o a ragioni sociali fasulle. Vale la pena prestare un occhio di riguardo a questo aspetto.

Non trasmettere credenziali di accesso.

La tua banca o la società emittente la tua carta non ti contatta mai per chiederti informazioni riservate o credenziali di accesso. Inoltre gli istituti finanziari non informano mai via e-mail su insolite transazioni su conti bancari o carte di pagamento. Non rispondere mai a tali richieste.

Non agire mai sotto pressione.

Diffida quando qualcuno ti fa pressione o ti minaccia di pesanti conseguenze. È tipico delle e-mail di phishing fissare termini stretti o ventilare minacce di conseguenze penali.

Verificare i link.

Non aprire link né allegati se non conosci il mittente e non aspetti messaggi. Potrebbe trattarsi di un link che conduce a un sito web contraffatto o di un allegato contenente software dannoso.

Digita sempre personalmente i link a siti web terzi nella riga dell'indirizzo del browser. Verifica se si tratta di un URL ufficiale della società in questione. Dovresti diffidare da link eccessivamente lunghi. Gli indirizzi dei siti web degni di fiducia iniziano con «https://».

Pagare solo se si è sicuri.

Trasmetti informazioni sulla carta e codici di sicurezza solo se vuoi effettuare un pagamento.

Attivare l'app della carta di pagamento.

Attiva l'app della società emittente la tua carta di pagamento. In tal modo riduci il rischio di frode. Puoi verificare ogni pagamento e a volte devi pure riconfermarlo (3-D Secure).

Verificare ogni pagamento.

Controlla attentamente ogni richiesta di pagamento e verifica il destinatario del pagamento. Conferma i pagamenti solo dopo aver controllato l'importo e il nome del commerciante.

Non inoltrare mai a terzi i codici di conferma.

Non inoltrare mai a terzi i codici di conferma. Con un codice di conferma i truffatori possono configurare altri servizi, p. es. un sistema di pagamento mobile come Google Pay, e rubare denaro dal tuo conto.

Verificare gli shop.

Leggi sempre attentamente le condizioni generali di contratto del commerciante pubblicate sul relativo sito web e presta attenzione a sigilli di garanzia come ad esempio «Trusted Shops».

Aggiornare i dispositivi.

Programmi obsoleti installati sul computer o sullo smartphone rappresentano un rischio per la sicurezza. Aggiorna regolarmente i tuoi dispositivi e colma eventuali lacune di sicurezza effettuando i necessari e periodici aggiornamenti. Installa anche software di sicurezza e programmi antivirus.

Sporgere denuncia.

Se sei rimasto vittima di un attacco di phishing, fai bloccare immediatamente la tua carta di credito o di debito e modifica le credenziali di accesso a tutti gli account. Sporgi denuncia alla polizia.

I PAGAMENTI CON CARTE DI CREDITO E DI DEBITO SONO SICURI.

Essendo mezzi di pagamento molto sicuri e popolari, le carte di credito e di debito sono usate spesso e volentieri per fare shopping online. Questo attira anche i truffatori. Gli attacchi di phishing sono in aumento. I truffatori agiscono in modo sempre più raffinato e professionale, per cui le vittime non sospettano di nulla.

La maggior parte dei reati legati a carte di pagamento può essere evitata attendendosi a poche regole di base. Seguile con attenzione!

Vai al test delle conoscenze:
card-security.ch/it/quiz

Maggiori informazioni sul tema della sicurezza delle carte di pagamento:

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