Comunicato stampa

Milano, settembre 2022

Carte di pagamento: i consigli per tutelarsi dai raggiri

Le frodi ai danni di possessori di carte di pagamento si moltiplicano e al tempo stesso si fanno sempre più sofisticate e tecnologiche. Per non farci trovare impreparati è importante seguire alcuni accorgimenti. Ecco quali sono a oggi le più frequenti truffe e i suggerimenti degli esperti di SOStariffe.it per prevenirle e correre ai ripari nel caso i malintenzionati abbiano già agito.

Può accadere con un prelievo all'ATM o a causa di un acquisto online su un sito poco sicuro. Le truffe ai danni dei proprietari di carte di pagamento sono sempre più frequenti. Le modalità per sottrarre denaro da una card sono molteplici e sempre più ingegnose: dal phishing alla clonazione della carta, passando per la sottrazione del codice pin. **SOStariffe.it** ha fatto il punto sulle che sono **le truffe più frequenti** relative alle **carte di pagamento** (carte di credito, di debito o prepagate). Ecco alcuni utili consigli pratici per prevenire i raggiri o far fronte a una frode già avvenuta, limitando i danni.

Il phishing: cos'è e come starne alla larga

Si tratta della tipica truffa telematica messa in atto per estorcere i dati della carta o del conto corrente collegato. **I malintenzionati si fingono membri di un'organizzazione affidabile.** Ad esempio, potrebbero simulare di far parte di una compagnia assicurativa, telefonica o della stessa banca che ha emesso la carta di pagamento. A quel punto**, inviando e-mail o sms al malcapitato possessore della tessera elettronica, proveranno a estorcere i dati di accesso invitandolo a comunicarli di sua volontà, con una richiesta pretestuosa.** I dati saranno quindi utilizzati per sottrarre denaro dal conto corrente o dalla carta.

Come possiamo proteggerci da questo tipo di frode? Anzitutto **evitiamo di fornire i dati della nostra carta di pagamento a seguito di richieste pervenute via e-mail o sms da parte di soggetti non meglio identificati che si spacciano per aziende note o per la nostra banca.** Se ci arriva una richiesta simile, leggiamo con attenzione la comunicazione per comprendere se si tratti di una richiesta legittima o meno.

Evitiamo di agire d'impulso. Contattiamo subito il servizio clienti del nostro istituto bancario o dell'azienda mittente della comunicazione per accertarci che ci abbiano effettivamente inviato quella richiesta. In generale, nessuna banca chiederà mai ad un suo cliente i dati di una carta di pagamento via mail o SMS. Comunicazioni di questo tipo sono, quindi, da bollare immediatamente come sospette. È importante non agire mai di fretta e prendersi sempre tutto il tempo per analizzare la richiesta.

Sottrazione del pin della card: si previene così

Le carte di pagamento sono solitamente dotate di un codice pin. Si tratta di un sistema di protezione numerico fondamentale in caso di furto della carta. Viene da sé che un malintenzionato che entri in possesso sia della carta che del codice pin potrà servirsene liberamente, prelevando da uno sportello ATM anche l'intero importo del nostro conto corrente, prima che la carta venga bloccata in seguito a segnalazione alla banca emittente.

È perciò buona norma non comunicare mai a nessuno il pin della nostra carta di pagamento. Si tratta di un dato strettamente personale da tenere a mente. Evitare di annotarlo su appunti cartacei o digitali da portare con sé, insieme alla carta stessa.

Clonazione della carta di pagamento: proteggiamoci con gli alert

Tutte le carte di pagamento, di debito e di credito, possono essere clonate tramite vari stratagemmi. Una volta duplicate possono essere usate all'oscuro del titolare. **Possiamo accorgerci della clonazione della nostra card se notiamo ammanchi sospetti di denaro, non collegati ad alcuna transazione che abbiamo effettuato.** Naturalmente una carta clonata può essere usata senza l'autorizzazione del titolare.

Come facciamo a scoprire subito se stanno tentando di utilizzare il duplicato della nostra carta? **Possiamo attivare i sistemi di alert previsti dalla nostra banca (come e-mail, sms o notifica via app) che ci avvisano di ogni tentativo di utilizzo dello strumento, dunque anche quelli fraudolenti.**

Inoltre, è possibile attivare i sistemi di sicurezza per verificare l'identità di chi esegue le transazioni online, come ad esempio l'autorizzazione a due o più fattori, che accerta se siamo effettivamente noi che stiamo usando la card tramite l'invio di codici via SMS e l'inserimento di una password statica.

Truffe dell'ATM: occhio agli sportelli manomessi

Quando ci avviciniamo agli sportelli ATM per effettuare un prelievo prestiamo grande attenzione al suo aspetto. Potrebbe infatti essere stato manomesso per effettuare truffe. Ad esempio, **dovremmo insospettirci se notiamo una finta fessura del bancomat, al di sopra di quella effettiva.** Si tratta di un'apparecchiatura di solito denominata "skimmer", che serve a clonare le carte di pagamento.

Lo skimmer contiene un ulteriore lettore di banda magnetica per copiare i dati memorizzati sulla carta. In genere una piccola telecamera, montata in modo da passare inosservata sullo sportello, registra l'introduzione del PIN e la trasmette al truffatore senza che l'utente del bancomat si accorga di nulla.

Quando effettuiamo un prelievo controlliamo perciò con attenzione che l'ATM non sia stato manomesso, con l'applicazione di altre mostrine al di sopra della fessura del bancomat e nascondigli segreti per la telecamera. Al termine dell'operazione verifichiamo che l'importo prelevato sia stato correttamente addebitato.

In caso contrario procediamo subito con il blocco della carta**.**

Gli sportelli ATM più evoluti consentono di prelevare senza inserire la carta, in modalità cosiddetta "cardless". Potrebbe essere una buona idea affidarsi a questo sistema quando presente.

Truffa del POS: controllare sempre l'importo della transazione

Entriamo in un supermercato, facciamo la spesa al termine paghiamo col nostro bancomat tramite POS. Anche in questo caso ci stiamo esponendo a rischi. Perché ad esempio il negoziante se in malafede potrebbe eseguire più operazioni consecutive di addebito dalla nostra carta oppure impostare un importo più alto rispetto a quello pattuito.

Perciò quando paghiamo con la card verifichiamo con attenzione l'importo della transazione inserito sul POS prima di avvicinare la tessera. Consultiamo subito dopo la ricevuta e la notifica di pagamento sullo smartphone. Diffidiamo degli esercenti che chiedono la carta senza mostrarci il POS con l'importo inserito.

Truffe sugli acquisti online: comprare solo su store affidabili

Anche i siti di e-commerce possono riservare spiacevoli sorprese. Se acquistiamo su un portale inaffidabile con una carta di pagamento rischiamo di perdere somme di denaro senza venire in possesso di alcuna merce. **Quando si fanno acquisti online e si effettua un pagamento digitale con card è opportuno sempre verificare se il portale rispetti gli standard minimi di sicurezza.**

Utilizziamo perciò una carta prepagata anche virtuale o un servizio terzo di affidabilità garantita come ad esempio PayPal che eseguirà la transazione senza comunicare i dati della carta al venditore. **In generale meglio inserire i dati solo su siti estremamente affidabili e noti.**

Frode del finto bancario: come smascherarla

È una versione più tradizionale e meno tecnologica del phishing: un truffatore contatta l'utente via telefono o porta a porta fingendosi un rappresentante della banca che ha emesso la carta e con una scusa tenta di entrare in possesso della card, dei dati e del codice pin.

Stiamo in guardia da qualsiasi richiesta di questo tipo. **Nessuna banca chiama o scrive ai propri clienti per richiedere i dati della carta: si tratta sempre di truffe.** Mettiamoci in contatto, immediatamente, con il servizio clienti dell'istituto di credito per effettuare le opportune verifiche. **Diffidiamo sempre da chi richiede i dati della tessera senza motivo**, ad esempio fingendo di dover effettuare un ipotetico controllo.

Per individuare la carta di pagamento più adatta alle nostre esigenze di spesa possiamo usare lo strumento di

comparazione di SOStariffe.it (https://www.sostariffe.it/confronto-carte/) che permette di confrontare tutte le offerte disponibili sul mercato italiano al momento. Inoltre, grazie all'app per dispositivi mobili è possibile analizzare le condizioni di ciascuna card in pochi clic.

Per maggiori informazioni:
Alessandro Voci
Tel+39.340.53.96.208
E-mail: ufficiostampa@sostariffe.it
Skype: sostariffe