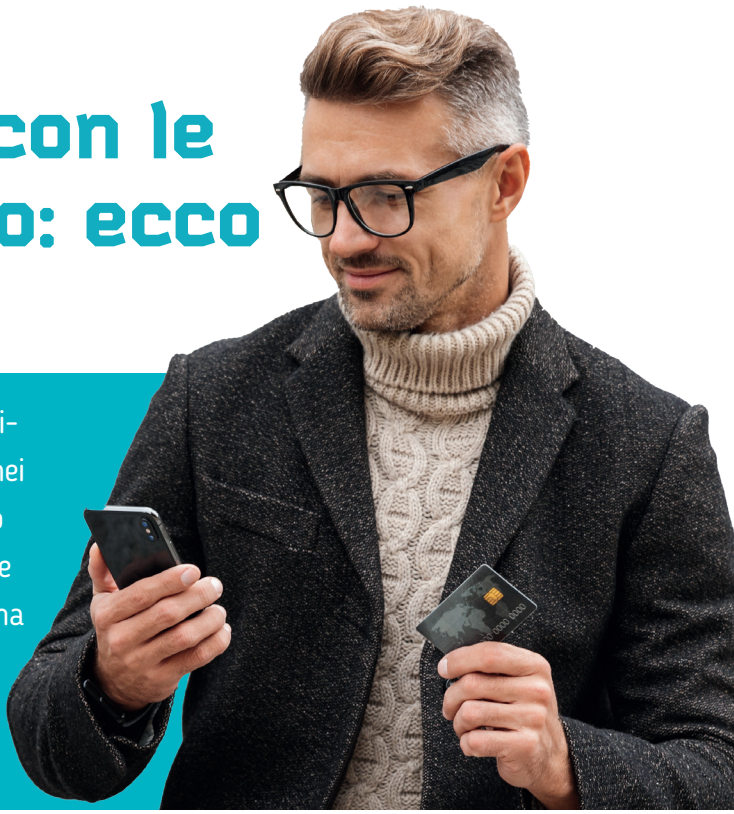
Occhio alle truffe con le carte di pagamento: ecco come proteggervi!



In linea di massima è possibile fare acquisti in rete in tutta sicurezza. Gli elaboratori di carte e le banche investono molto nei propri sistemi di sicurezza. Ciononostante i truffatori riescono talvolta a sottrarre denaro alle proprie vittime. Nel più recente tipo di truffa le vittime attivano inconsapevolmente un sistema di pagamento mobile. Marcel Drescher, Head Fraud Services dell'UBS Card Center, spiega come procedono i malfattori nel digital wallet fraud e come tutelarsene.

Che cosa sono i sistemi di pagamento digitali?

Si tratta di informazioni elettroniche di pagamento che vengono memorizzate per l'utilizzo su un mezzo digitale anziché su una carta di plastica. Ad esempio, sotto forma di un portafoglio digitale, un cosiddetto «wallet», installato su uno smartphone o su uno smartwatch. Di conseguenza, tale dispositivo può essere utilizzato per i pagamenti proprio come una carta di credito o di debito.

Quali sono i tipi di truffa più frequenti nello shopping online?

Spesso le informazioni personali delle carte, utilizzate regolarmente per effettuare pagamenti presso i commercianti online, vengono rubate in un momento successivo in seguito a una fuga di dati e utilizzate a scopi abusivi.

Un altro tipo di truffa molto diffuso è l'appropriamento fraudolento di informazioni personali delle carte e dei relativi mezzi di accesso elettronici tramite l'invio di e-mail di phishing. Con tali e-mail i truffatori richiedono ad esempio alle vittime di versare ancora una piccola tassa prima di poter recapitare un pacco. Chiedono loro di effettuare il pagamento tramite il link indicato nell'e-mail. Il link conduce tuttavia a un sito web contraffatto. Se vi si inseriscono i dati personali della propria carta e si svela anche il codice di accesso ricevuto separatamente via SMS o notifica, i truffatori possono disporre a piacimento del denaro della vittima.

I truffatori si appropriano spesso dei dati necessari inviando un'e-mail di phishing.

Che cos'è un digital wallet fraud?

In questo tipo di frode i truffatori cercano di registrare abusivamente i dati di una terza persona nella propria app wallet, in modo da poter poi effettuare pagamenti abusivi in negozi, ristoranti o online.

Come procedono i malfattori in questo tipo di frode?

I truffatori si appropriano spesso dei dati necessari inviando un'e-mail di phishing. Le vittime svelano i propri dati credendo di rispondere alla richiesta di pagamento relativa all'e-mail di phishing. Inoltre trasmettono anche il codice di accesso per la conferma della registrazione del wallet, inviato separatamente via SMS ai loro numeri di cellulare registrati. Ciò avviene inserendo tale codice sul sito web contraffatto. A questo punto i truffatori dispongono di tutti i dati necessari per effettuare la registrazione con successo.

Dove posso informarmi sulle e-mail di phishing e come le riconosco?

Le principali informazioni si trovano sui siti www.card-security.ch, www.cybercrimepolice.ch o richiamando le relative pagine della banca o della società emittente della carta di pagamento.

Che cosa devo fare se ho già trasmesso i dati della mia carta e il codice di accesso elettronico?

Si deve immediatamente fare bloccare la carta facendo presente di aver trasmesso a terzi i dati personali della carta o i codici di accesso. È possibile fare bloccare in modo rapido e diretto la carta anche tramite i servizi web offerti dalle società emittenti di carte. Dopo il blocco della carta, quest'ultima sarà protetta da ulteriori abusi. Tuttavia, le transazioni abusive effettuate prima del blocco non possono purtroppo più essere annullate.

Come posso tutelarmi da attacchi ai danni delle mie carte di pagamento?

La protezione migliore può essere garantita leggendo attentamente tutte le informazioni ricevute via SMS o altri canali di comunicazione dalla società emittente di carte. Se si effettua il pagamento di un piccolo importo, ma nel relativo SMS è specificato che si tratta del codice di conferma per registrare la carta di credito XY per una soluzione di pagamento digitale, non si deve in nessun caso trasmettere il codice.

Inoltre è caldamente raccomandato di attivare un servizio di notifica dei pagamenti con carte, non appena sono state effettuate transazioni con una carta. In questo modo, è possibile tenere sempre sotto controllo i pagamenti e impedire che varie transazioni abusive possano essere effettuate in un breve lasso di tempo. Se si riceve una tale notifica relativa a una transazione ignota si dovrà fare bloccare subito la carta e contattare la società emittente.

La società emittente della carta andrà contattata anche in caso di dubbio circa una richiesta di pagamento. La società emittente sarà lieta di fornirti ragguagli in merito e potrà forse tutelarti da un abuso dei dati.

Rispondo io dei danni finanziari che mi derivano da una frode di questo tipo?

Si tratta di una questione dell'obbligo di diligenza: se il cliente ha ottemperato ai propri obblighi da lui accettati in conformità delle condizioni generali di contratto, il danno subito gli sarà indennizzato. È il caso, ad esempio, quando i dati personali sono stati rubati per via di una fuga di dati.

Il cliente non viene indennizzato invece se svela i dati personali della propria carta di pagamento attivando un link contenuto in un'e-mail di phishing. Il cliente risponderà del danno subito fino al momento in cui lui o la società emittente avrà fatto bloccare la carta. Per questo è importante verificare con attenzione per che cosa si trasmette il codice di autorizzazione prima di inviarlo, controllando sempre l'importo e il destinatario della transazione.

Marcel Drescher, Head Fraud Services UBS Card Center

Marcel Drescher e il suo team si occupano di casi di frode relativi alle carte di credito e di debito per conto della banca UBS e di altre società svizzere emittenti di carte.