Beware of card fraud: How you can protect yourself!

Shopping on the internet is fundamentally safe. Card processors and banks invest heavily in their security systems. Nevertheless, fraudsters succeed again and again in stealing money from their victims. In the latest scam, victims unknowingly activate a mobile payment system. Marcel Drescher, Head of Fraud Services at the UBS Card Center, explains how fraudsters go about digital wallet fraud and how you can protect yourself against it.

What are digital payment systems?

With these systems, electronic payment information is stored on a digital medium for use instead of a plastic card. This can be in the form of a digital wallet on smartphones or smartwatches, for instance. Thus, the corresponding device can be used as a credit or debit card for payments.

What are the most common types of fraud in online shopping?

Often, personal card information that you legitimately use for a payment in retail shops is stolen at a later date due to a data leak and used for fraudulent purposes.

Another common type of fraud is the obtaining of personal card information and the corresponding electronic access by sending phishing emails. In such emails, the scammers make you believe, for example, that a small fee is still outstanding for the delivery of a parcel. You are prompted to make this payment via a link sent in the email. However, the link leads to a fake website. If you enter your personal card details there and then also disclose the access code that you received separately via SMS or notification, the fraudsters can take your money.

What is digital wallet fraud?

With this type of fraud, scammers attempt to improperly register a third party's data in their own wallet app so that they can subsequently use their device to make fraudulent payments in shops, restaurants or online.

Fraudsters often obtain the data they need by sending a phishing email.

How do fraudsters go about this type of fraud?

Fraudsters often obtain the data they need by sending a phishing email. Victims disclose their details under the assumption that they are complying with the request for payment in the phishing email. In addition, they also pass on the access code for confirming wallet registration, sent to them separately via SMS to their registered mobile phone numbers. This is done by entering the code on the fake website. With this information, fraudsters now have all the information they need to register successfully.

Where can I learn more about phishing emails and how do I recognise them?

You can find the most important information at www.card-security.ch, www.cybercrimepolice.ch or the relevant pages of your bank or card issuer.

What do I have to do if I have passed on my card data and electronic access details?

Have the card frozen immediately and notify the relevant party that you have given out personal card data or access codes. You can also freeze your card directly and quickly via the card issuers' web services. Once the card has been frozen, it is protected against further misuse. Unfortunately, fraudulent transactions that took place before freezing can no longer be reversed.

How can I protect myself from attacks on my debit and credit cards?

The best protection is ensured if you read the messages from the card issuer that you receive via SMS or other notifications completely and exactly. If a payment is made via a small fee, but the SMS states that this is the confirmation code for registering credit card XY for a digital payment solution, then the code must not be passed on under any circumstances.

Furthermore, it is highly recommended to activate a notification service for your card payments as soon as transactions have been made with a card. This allows you to keep track of everything at all times and prevents multiple fraudulent transactions from taking place within a very short period of time. If you receive such a message about an unknown transaction, you should have the card frozen immediately and contact the card issuer.

Also contact the card issuer if you have any doubts about a payment request. They can help you and possibly save you from data misuse.

Am I liable for financial losses caused by card fraud?

This is a matter of due diligence: If the customer have complied with the obligations they've accepted in accordance with the General Terms and Conditions, they will be compensated for their losses. This is the case, for example, if their personal data was stolen via a data leak.

On the other hand, the customer do not receive any compensation if they pass on their personal card data via a link from a phishing email. The customer is responsible for losses up to the point in time when they or the card issuer freeze the card. Therefore, it is important to check exactly what the approval code is for before passing it on. Pay close attention to what you approve, the amount and the retailer.

Marcel Drescher, Head of Fraud Services at the UBS Card Center

Marcel Drescher and his team handle credit and debit card fraud cases for the bank UBS and other Swiss card issuers.