

16.02.2026

Fraud – what to do if you were affected?

Despite being cautious and taking security measures, it can sometimes still happen... you fall victim to fraud. Credentials have been disclosed or a payment made. One thing most important in situations like these: Act quickly and do the right thing. A quick response can limit any damage and increase your chances of recovery.

Stay calm and act straight away

If you notice or suspect that you have fallen victim to a scam, don't hesitate! Every minute counts – in particular when e-banking or if credit cards or mobile payments facilities are concerned.

The most important immediate measures:

- Contact your bank or payment service provider immediately and notify them of the incident.
- If necessary, block accounts or have them blocked.
- Change your passwords as soon as possible; also for any services with the same credentials.

Financial institutions and payment providers might be able to stop any suspicious transactions or prevent any future debits if they are notified early.

Secure credentials and check your devices

If your credentials have been disclosed or you scanned a QR code, there is a risk that other accounts might be affected.

We recommend the following steps:

- Change all affected passwords immediately.
- Activate two-factor authentication (2FA) if you have not already done so.
- Remove any apps or software installed unintentionally.
- Check your smartphone (Android) and computer using up-to-date antivirus software.

This way, you can prevent scammers accessing your accounts over and over again.

Document and notify scams

It is important to carefully document any scams, as this will not just help your own bank, but also law enforcement agencies. Amongst others, this includes screenshots of e-mails, texts or websites, payment confirmations and bank statements as well as details of date, time and the exact way the incident happened.

In Switzerland, you should notify the police of any cases of fraud.

Can you retrieve your money?

Whether you can reverse any damage suffered depends on a variety of factors:

- How quickly a scam was reported.
- What type of payment method was used.
- Whether an amount has already been forwarded on.

The earlier you react, the greater your chances that payments can be stopped or reimbursed. Yet there is no guarantee for this.

Learn from an incident

Even if fraud can be very stressful, it still offers a chance to improve your own digital security sustainably. Consciously dealing with such incidents will help you better recognise and understand common scams. It will also encourage you to reflect on your own security habits and to handle links, QR codes and unexpected messages even more carefully in future.

Conclusion

Fraud does not mean you failed personally. Cybercriminals are becoming increasingly professional in their approach. The crucial thing is to react quickly, to limit the damage and to take consistent measures. If you are prepared, you will be able to take confident action should the worst happen, and to sustainably strengthen your digital security.