23.10.2020

The latest attempts at phishing fraud

Phishing messages sent out via e-mail or SMS have once again started to markedly increase since late summer. In the process, these fraud attempts are becoming ever more sophisticated. Don't be deceived!

Internet criminals don't just demonstrate a technological understanding, but time and again also prove to be very resourceful. While during lockdown, it was Corona-related phishing messages which were predominant, since August, fraudsters have been coming up with ever new scams to hoodwink credulous users. Alleged blocks on accounts and cards, undelivered parcels, vouchers won and telecom company refunds are currently the most popular phishing traps employed.

These faked messages usually reach users by e-mail or SMS – and are becoming increasingly plausible. Attackers write in flawless German. Often, victims are addressed via their own e-mail address or even their name. The sender's address is also quite often faked, and the linked phishing website frequently displays a HTTPS address and a domain name regularly considered trustworthy by laypersons. Fraudsters sometimes also use malicious e-mail attachments instead of links to mislead even experienced recipients.

Caution is advised – but please don't panic. There are a few simple rules of conduct to protect you against all such fraud attempt:

- Never use any links you receive by e-mail, SMS or messenger services, and never scan in any such QR codes to log into your financial institution facility.
- Never fill in any forms received by e-mail and asking you to enter log-in information.
- Treat e-mail and SMS attachments with great caution.
- Never disclose any confidential information, such as passwords, during telephone calls.
- Always enter the address for your online service provider or financial institution's log-in page manually via the browser address line.
- Check there is an SSL connection (https://, lock symbol) when calling up a log-in page, and verify that the Internet address shown in the address bar of your browser actually indicates that you have reached the correct page.
- Contact your financial institution if you are not quite sure or something is not completely clear.

Additional information can also be found in our article on Phishing (https://www.ebas.ch/phishing).