24.11.2021

E-Mail fraud attempts are constantly improving

Until a few years ago, awful English and faulty representation served to expose fraudulent e-mails. Today, these look increasingly authentic. But you can expose them still.

Using specific responses to e-mails actually sent, criminals are currently trying to tempt company employees into opening infected file attachments. The particularly perfidious thing: Such response mails seem to actually originate from the original addressee (source: www.cybercrimepolice.ch (http://www.cybercrimepolice.ch)).

For a few years now, we have been experiencing an increasing professionalisation of fraud attempts on the Internet generally. Accordingly, phishing (https://www.ebas.ch/en/phishing/) messages received by e-mail, SMS or WhatsApp look very authentic, making it hard to distinguish them from the real thing both visually and content-wise. And criminals are hardly deterred by anything nowadays to deceive unsuspecting consumers.

The good news: With the help of just a little prior knowledge, it is relatively easy to debunk just about all fraud attempts via e-mail, SMS or messenger service. Follow our recommendations to protect yourself and your device:

- Fraudulent messages usually contain a dangerous link or an infected file attachment. If possible, you should therefore never use any link provided in any e-mail, SMS or messenger notification, but always enter the Internet address required (for instance that of your bank) manually into the address line of your browser.
- Don't open any attachments you didn't expect to receive, or if you are unable to verify the authenticity of a message received.
- Only use confidential information, such as access data for your e-banking facility, for the intended purpose. Never pass them on to anyone else, not even (purported) employees of your bank or a renowned company such as Microsoft or Apple.
- Always apply a healthy dose of suspicion on the Internet. If a message, website or service looks strange to you, you should use a secure channel, for instance your telephone, to contact your bank or the respective provider involved via the familiar direct dial number of your customer consultant.

Further information and tips regarding fraud attempts can be found in our article on "Phishing (https://www.ebas.ch/en/phishing/)".