27.10.2022

Smishing: Swiss bank customers also targeted

Stay alert – even where text messages are concerned! That's because the names of renowned Swiss companies are a favourite for fraudsters to use in malicious schemes.

Remain sceptical when you receive SMS, MMS, WhatsApp or Messenger messages asking you to click a link, in particular if these are supposed to come from a renowned parcel service or financial service provider.

As can be seen from a report this week by the Zürcher Kantonspolizei (https://www.cybercrimepolice.ch/de/fall/sms-zkb-access-app-voruebergehend-eingeschraenkt-ist-ein-perfider-phishingversuch/) , Smishing remains as popular a means as ever for criminals to cheat Swiss citizens out of their money.

Never click on any links included in text messages, but manually enter the website address of your financial institution which you are familiar with into your browser. Then check there is a secure connection (https://, lock symbol, target address). In case of uncertainty or ambiguity, please contact your financial institution to confirm they actually sent that text.

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