23.02.2022

Criminals want to get their hands on your SIM card – and then your bank account

Hackers steal or copy SIM cards and abuse them to obtain access to apps and bank details. Such an attack usually starts with a phishing message.

Some US-$ 68 million have been scammed out of victims by fraudsters in the USA, using the so-called SIM swapping trick. In the process, they either steal or copy their victims' SIM cards and abuse it to obtain access to apps and bank details (source: Heise Security, 20 Minuten).

Cases of SIM swapping, even if comparatively few, have also come to light in Switzerland. The initial attack usually involves phishing (https://www.ebas.ch/en/phishing/) mails, texts or Messenger messages containing a link to a fake website run by the attacker. This is where innocent users are asked to enter their mobile provider details and/or access data to a certain online service or their e-banking facility. Sometimes access data obtained via data leaks are also bought en masse (for instance on the Darknet).

Since e-banking portals and other online services increasingly make use of two- or multi-factor authentification (2FA, MFA), attackers will need user name or account number and password on the one hand plus a SIM card either stolen or reordered from the mobile provider, so they can intercept and use the second security factor. Data and SIM cards thus stolen or obtained some other way are then used by fraudsters to obtain illegal access to relevant e-banking portals or online services.

Protect yourself by ...

- never using any links you receive by e-mail, SMS or messenger services or obtained by scanning in a QR codes to log into your financial institution facility or any online service.
- never filling in any forms received by e-mail and asking you to enter log-in information.
- treating e-mail and SMS attachments with great caution.
- never disclosing any confidential information, such as passwords, during telephone calls.
- always entering the address for your online service provider or financial institution's log-in page manually via the browser address line.
- checking there is an SSL connection (https://, lock symbol) when calling up a log-in page, and verifying that the Internet address shown in the address bar of your browser actually indicates that you have reached the correct page.
- never leaving your mobile device out of sight and having a device or SIM card blocked immediately if lost or stolen.
- contacting your financial institution if you are not quite sure or something is not completely clear.