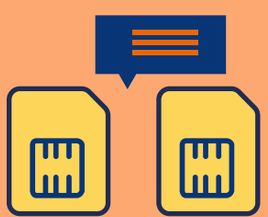
SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.

HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.

With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession



The fraudster can now receive incoming calls and text messages, including access to the victim's online banking

The victim will notice the mobile phone lost service, and eventually will discover they cannot login to their bank account

WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Restrict information and show caution with regard to social media.
- Never open suspicious links or attachments received by email or text message.
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- Update your passwords regularly.
- Buy from trusted sources. Check the ratings of individual sellers.
- Download apps only from official providers and always read the apps permissions.
- When possible, do not associate your phone number with sensitive online accounts.
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.
- Frequently check your financial statements.

ARE YOU A VICTIM?

- If your mobile phone loses reception for no reason, report it immediately to your service provider.
- If your service provider confirms that your SIM has been swapped, report it to the police.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | enisa European Union Agency for Cybersecurity | European Cyber Security Month

#CyberScams