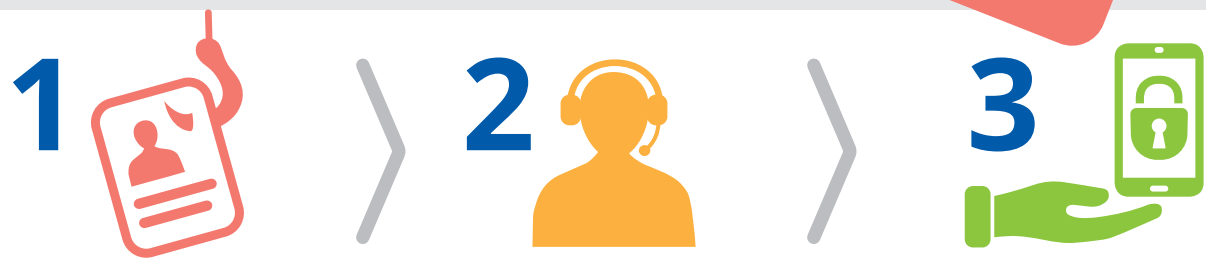
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

How to avoid MOBILE SIM SWAPPING?

WHAT IS A SIM SWAPPING ATTACK?

In a SIM swapping attack, an attacker takes over your mobile phone number by asking the mobile telecom provider to link your number to a SIM card under the attacker's control.



1 Collect victim's personal data
Via phishing, data breaches, social media searches, malware

2 Carry out the fraudulent SIM swap
In-store, contacting company's representative over the phone or online through the provider's app or portal

3 Exploit the swapped SIM
The fraudster receives calls or messages addressed to the legitimate user to make bank transactions and accessing email accounts, sites and social media

WHAT ARE THE WARNING SIGNS?

- **Before the attack:** You receive strange phone calls asking you to share codes or SMS messages that you have received from your mobile telecom provider.
- **During the attack:** Your phone loses network connection for a longer period, and you are not able to make or receive phone calls.
- **After the attack:** You may see suspicious transactions in your banking accounts, or lose access to your social media or email accounts, or see other activity you do not recognize.

WHAT TO DO IF YOU ARE A VICTIM?

If you experience any of the above signs, ccontact your telecom provider as soon as possible.

If it confirms the SIM swap, immediately contact your bank and change the passwords to your online accounts. Furthermore, report the fraudulent activity to the police.

HOW TO PREVENT THE ATTACK?

- Avoid providing any personal information to someone pretending to be representative of the telecom provider.
- Never communicate, over the phone, the one-time passwords you receive from your mobile operator.
- Choose app-based 2-factor authentication, instead of two-factor via mobile phone or SMS.
- Be cautious with the personal information that you share on websites and social media.
- Do not open suspicious hyperlinks or attachments received through email or SMS

European Union Agency for Cybersecurity
www.enisa.europa.eu