BANGKO SENTRAL NG PILIPINAS

BEWARE OF SIM CARD FRAUD ATTACKS!

The Bangko Sentral ng Pilipinas cautions the public against SIM card fraud and scams.

What is a SIM card?

SIM stands for **subscriber identity module** or **subscriber identification module** which stores the subscriber identity number used to identify and authenticate subscribers on a mobile network. It also corresponds to the mobile phone number of the subscriber.

Why do fraudsters want to take control of your SIM card?

Majority of the banks and other financial institutions require multifactor authentication (MFA) in online financial transactions. This entails requiring customers to key in a one-time PIN or password received via their registered mobile phone number before online transactions such as funds transfers can be completed. Fraudsters are therefore interested in this piece of information for them to carry out unauthorized funds transfers.

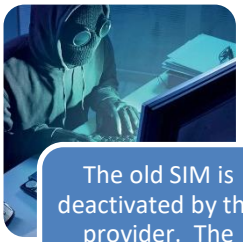
How do SIM card fraud attacks work?

Fraudsters can carry out their SIM fraud in two distinct ways:

Attack Type 1: SIM Swap Fraud Attack

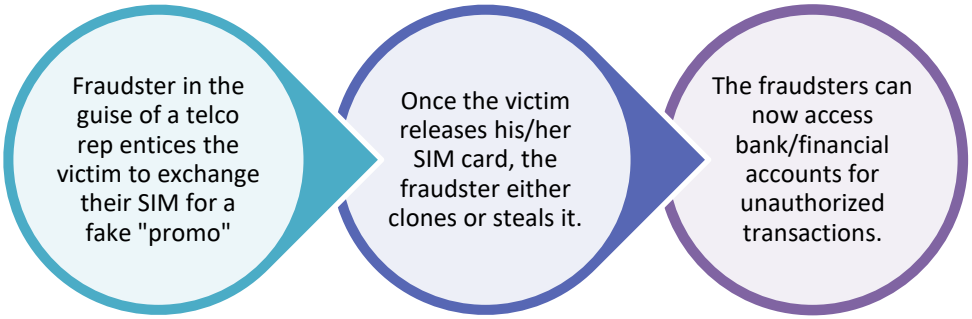
Fraudsters obtain personal banking details through phishing and other tactics.

Once sufficient information are obtained, they request the mobile phone provider for a SIM replacement.



The old SIM is deactivated by the provider. The fraudster is now free to access bank accounts of the victim.

Attack Type 2: Direct SIM Scam



How can you protect yourself from SIM fraud attacks?

- ✓ Never give out personal information and SIM card details in response to unsolicited calls/texts from unknown individuals.
- ✓ Always check SMS and email alerts for unusual transactions and/or activities involving your bank/e-money accounts.
- ✓ In case you've already provided your SIM and other personal details, contact your bank/mobile phone provider immediately.