Pakistan Telecommunication Authority
Headquarters, Islamabad

PTA Cyber Security Advisory No.: 156 **24-08-2022**

Name: SIM Swapping

Threat Classification: SIM Swap Fraud

Summary:

SIM swapping is a kind of fraud where a fraudster contacts victim's mobile phone's carrier and trick them into activating a SIM card that the fraudsters have. Once this happens, the fraudster has control over victim's phone number. Anyone calling or texting victim's number will contact the fraudster's device, not victim's smartphone.

To successfully commit this type of fraud, bad actors need additional information about the victim, like his/her email, home address, and phone number. This information may even be available online, either through a search engine or social media. Once the fraudster has this information, they may call victim's carrier and pretend to be him/her in order to transfer his/her phone number to a new SIM card and device.

Recommendations:

1. Beware of **phishing emails** and other ways attackers may try to access your personal data to help them convince your bank or cell phone carrier that they are you. Don't click on links in email messages from people you don't know.
2. Boost your cellphone's account security with a unique, strong password and strong security questions and answers that only you know.
3. If your phone carrier allows you to set a separate passcode or PIN for your communications, consider doing it. It could provide an additional layer of protection.
4. If possible, avoid posting your full name, address, or phone number on public sites. An identity thief could find that information and use it to answer the security questions required to verify your identity and log in to your accounts.
5. If you stop receiving any calls or texts, and you don't know why, contact your wireless provider immediately. Even if you don't use your mobile device often, you should check regularly for provider and account alerts