CID
ARMY CRIMINAL INVESTIGATION DIVISION

26 January 2024

Cybercrime Prevention Flyer

SIM Swapping

Nearly every person in the U.S. has a cellular device. Meaning each person is digitally connected to the device associated phone number and the information, financial, health, work, social, etc., stored on the device. With a simple SIM swap, sometimes referred as simjacking, simhijacking, or simcard hacking, a cell phone user could be locked out of their number.

A SIM, or Subscriber Identity Module, refers to a small card that users insert into mobile phones and other devices to identify and authenticate them on a mobile network. The SIM card holds information such as the International Mobile Subscriber Identity (IMSI) and the keys for encrypting and decrypting communication between the mobile device and the network. The SIM card plays a crucial role in making calls, sending messages, and accessing a user's mobile data services.

In more recent years, providers have begun to use eSIMs, or embedded SIMs in mobile devices. An eSIM is a digital version of the traditional physical SIM card used in mobile devices. Unlike a physical SIM card, an eSIM is embedded directly into the device's hardware, eliminating the need for a physical card and allows users to switch mobile carriers without changing SIM cards. Unfortunately, having an eSIM does not protect against a SIM swapping attack.

Cybercriminals employ SIM swapping as a technique to perpetrate identity theft against a victim. During SIM swapping, the cybercriminal transfers the victim's cellular service from the SIM card in the victim's possession to a new SIM card under the cybercriminal's control.

To execute this attack, the cybercriminal must impersonate the victim, convincing the victim's mobile carrier to transfer the service to a new SIM card. The attacker typically acquires personal information through social engineering tactics like phishing emails, extensive open-source and social media research, or purchasing information from the dark web.

Once the cybercriminal successfully impersonates the victim to the mobile carrier, the cybercriminal diverts text messages and phone calls to the SIM card they control. Subsequently, the cybercriminal exploits two-factor authentication to gain access to text messages, emails, passwords, social media platforms, photos, cryptocurrency exchange accounts, financial data, bank accounts, and other valuable items.

Detecting SIM swapping in a timely manner can minimize potential negative consequences. SIM swapping warning signs include:

- Change in service notifications.
- Inability to make calls, send text messages, or use mobile data.
- Denied account and mobile application access.
- Identifying unauthorized transactions.

SIM swapping is preventable. Using biometric authentication, two-factor authentication through an authenticator application, or setting up a SIM lock down, SIM PIN, or SIM alert are all prevention methods. Most importantly, limit posted social media information.

Victims of SIM swapping should:

- Contact their mobile service provider and request account access removal for the unknown device. The service provider may require in-person contact for identity verification.
- Contact all financial institutions to secure financial accounts and review recent account activity for unauthorized transactions.
- Change passwords and enhance account security by enabling multi-factor authentication, such as face ID or other biometric authentication features.
- Set up bank and mobile carrier alerts to be notified of any future suspicious activity.
- Lock down and limit access to social media accounts.
- File a police report and report the incident to the Internet Crime Complaint Center.

Additional Resources

Cell Phone Fraud

FBI Tech Tuesday: SIM Swapping

Enhanced Personal Security Guide

Authorized for widest release, without restrictions.

To receive Cyber Directorate Cybercrime Prevention Flyers, send an email to: **CYDIntel@army.mil**

Cyber Directorate Headquarters
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134

REPORT A CRIME
CLICK TO SUBMIT A TIP

CID LOOKOUT
ON POINT FOR THE ARMY

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products, or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.