Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

February 08, 2022

Alert Number
I-020822-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public

The Federal Bureau of Investigation is issuing this announcement to inform mobile carriers and the public of the increasing use of Subscriber Identity Module (SIM) swapping by criminals to steal money from fiat and virtual currency accounts. From January 2018 to December 2020, the FBI Internet Crime Complaint Center (IC3) received 320 complaints related to SIM swapping incidents with adjusted losses of approximately $12 million. In 2021, IC3 received 1,611 SIM swapping complaints with adjusted losses of more than $68 million.

How a SIM Swap Scheme Works

SIM swapping is a malicious technique where criminal actors target mobile carriers to gain access to victims' bank accounts, virtual currency accounts, and other sensitive information. Criminal actors primarily conduct SIM swap schemes using social engineering, insider threat, or phishing techniques. Social engineering involves a criminal actor impersonating a victim and tricking the mobile carrier into switching the victim's mobile number to a SIM card in the criminal's possession. Criminal actors using insider threat to conduct SIM swap schemes pay off a mobile carrier employee to switch a victim's mobile number to a SIM card in the criminal's possession. Criminal actors often use phishing techniques to deceive employees into downloading malware used to hack mobile carrier systems that carry out SIM swaps.

Once the SIM is swapped, the victim's calls, texts, and other data are diverted to the criminal's device. This access allows criminals to send 'Forgot Password' or 'Account Recovery' requests to the victim's email and other online accounts associated with the victim's mobile telephone number. Using SMS-based two-factor authentication, mobile application providers send a link or one-time passcode via text to the victim's number, now owned by the criminal, to access accounts. The criminal uses the codes to login and reset passwords, gaining control of online accounts associated with the victim's phone profile.

Tips on How to Protect Yourself

The FBI recommends individuals take the following precautions:

- Do not advertise information about financial assets, including ownership or investment of cryptocurrency, on social media websites and forums.

- Do not provide your mobile number account information over the phone to representatives that request your account password or pin. Verify the call by dialing the customer service line of your mobile carrier.
- Avoid posting personal information online, such as mobile phone number, address, or other personal identifying information.
- Use a variation of unique passwords to access online accounts.
- Be aware of any changes in SMS-based connectivity.
- Use strong multi-factor authentication methods such as biometrics, physical security tokens, or standalone authentication applications to access online accounts.
- Do not store passwords, usernames, or other information for easy login on mobile device applications.

The FBI recommends mobile carriers take the following precautions:

- Educate employees and conduct training sessions on SIM swapping.
- Carefully inspect incoming email addresses containing official correspondence for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names.
- Set strict security protocols enabling employees to effectively verify customer credentials before changing their numbers to a new device.
- Authenticate calls from third party authorized retailers requesting customer information.

Victim Reporting and Additional Information

If you suspect that you are a victim of SIM swapping:

- Contact your mobile carrier immediately to regain control of your phone number.
- Access your online accounts and change your passwords.
- Contact your financial institutions to place an alert on your accounts for suspicious login attempts and/or transactions.
- Report information concerning all suspicious activity to your local law enforcement agency or your local FBI field office (contact information can be found at www.fbi.gov/contact-us/field-offices.)
- Report the activity to the FBI's Internet Crime Complaint Center at www.ic3.gov.