

Tech Tuesday: Building a Digital Defense Against SIM Swaps

March 8, 2022



Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against SIM swaps.

SIM stands for Subscriber Identity Module. Cell phone companies in the U.S. and around the world use SIM cards. It is that card that connects your phone to the provider's network, tells the network where in the world you are, and allows you to make calls and send text messages.

Of course, nothing useful comes without a risk... in this case, cyber criminals are using a technique called SIM swapping to steal money by gaining access to your bank accounts, your virtual currency accounts and/or other sensitive information. In fact, in 2021, the FBI's Internet Crime Complaint Center (www.IC3.gov) received more than 1,600 SIM-swapping complaints with adjusted losses of more than \$68 million.

There are three main ways that bad actors get access to your phone in this way: through social engineering, insider threat, or phishing schemes.

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** techniques pay off a mobile carrier employee to switch a victim's mobile number to a SIM card in the criminal's possession.

Criminal actors also use **phishing techniques** to deceive phone company employees into downloading malware onto their company's systems. That malware then allows the bad guy to do his own 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. The criminal uses the codes to login and reset passwords, gaining control of online accounts associated with the victim's phone profile.

Here's how to protect yourself:

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

If you receive a call or message from someone claiming to work for your cell provider, do not give that person any account information.

Avoid posting personal information online, such as mobile phone number, address, or other personal identifying information.

Use unique passwords for each online account.

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 on mobile device applications.

If you are the victim of an online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.

###

Sources: <https://www.ic3.gov/Media/Y2022/PSA220208>