SIM Swapping

SIM stands for subscriber identity module, and it's commonly known as that small, removable chip card used in a mobile phone. Each SIM card is unique and is associated with your mobile account. SIM-swapping frauds are on the rise. SIM swapping is a type of account takeover scam where fraudsters take control of your phone number to access all kinds of personal information. They can even use it as an attack vector for two-factor authentication and one-time passwords (OTP). It requires only minor tech skills for an attacker to target your cellphone number, which is why it has become popular with younger, less sophisticated fraudsters.

How SIM Swapping Occurs

The SIM swapping scam starts with a person impersonating you as they contact your mobile carrier. They will claim that they have a new SIM card to activate for your account. They might say the original phone and SIM card were lost, destroyed, or sold with the SIM card left in accidentally. The mobile carrier will most likely request some identity verification, such as the account PIN or security questions that you set up, or the last four digits of your social security number. Once the criminal has persuaded the mobile carrier's customer service representative that they're legit, they're able to get your phone number reassigned to their SIM. The fraudster can now intercept all your member's text messages and phone calls – meaning they can interfere with any password resets via call or text. They can also receive two-step verification passcodes for accounts where it is enabled. The criminal has essentially disconnected your phone number from your phone and assigned it to their SIM card

Warning Signs You've Been SIM Swapped

Symptoms occur quickly when a SIM-swapping attack hits. Here are a few warning signs that SIM swapping has occurred:

• Friends might tell you that your social media accounts have been hacked and you see the posts you never made.

• The phone might start behaving strangely. Texting and calling may not work or the phone network will show no signals. In addition, your SIM card will not show your service provider company.

• If you're on Wi-Fi, you might start getting emails about account changes.

• Some wireless carrier services use client email to send notifications. For example, if your email account is not compromised yet, you will receive a notification via email. Now you know that your new SIM card got activated even though you never requested a new SIM card.

• You are no longer the owner of your accounts. It is because your account detail got changed by the attacker.

• Unauthorized bank activity could start happening. Common scams targeting your members

Preventing a SIM - Swapping Attack

• An effective method is to contact their mobile phone carrier to add a PIN or password to the account. If an attacker doesn't extricate this PIN before attempting to hijack the account, it could thwart any attack altogether. Some carriers may even allow their customers to set up isolated PINs for SIM cards inserted in phones.

• To protect your accounts, consider the use of a two-factor authentication device or app that doesn't rely on SMS text messages. Two-factor authentication is a great way to bolster security.

• Some carriers also have features that could potentially stop SIM swapping. For example, Verizon has a feature that can be enabled from their My Verizon app called "Number Lock." This feature enables customers to prevent an unauthorized port out or SIM swap of your mobile number.