SIM CARD SWAPPING
Is Your Cell Phone Safe?

I am sure you consider yourself a responsible person when it comes to taking care of your possessions. You may say you have never left your wallet in a taxi or lost an expensive ring down the drain. Most of us don't let our smartphones out of our sight, yet one day you notice it's acting oddly. Did you know that your device can fall into cybercriminals' hands without ever leaving yours? SIM swapping is a method that allows criminals to take control of your smartphone and break into your online accounts. Here are a few easy steps you can take to safeguard your smartphone from prying eyes and hackers.

The SIM (subscriber identity module) is a memory chip that makes your phone truly yours. It stores your phone plan and phone number, and can also store your photos, texts, contacts, and apps. In most cases, putting your SIM card from an old phone into a new one will transfer your personal data as well. If criminals gain access to your SIM, they can access your two-factor authentication codes sent via text messages and email to secure your personal online accounts such as banking, social media and emails. They can use the information they obtain to impersonate you and even scam your contacts.

What is SIM card swapping?

Unlike what the name suggests, SIM swapping doesn't need a cybercriminal to get access to your physical phone and steal your SIM card. Swapping can be remote. Cybercriminals, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can access your phone's data and change your account passwords to lock you out of your online banking profile, email, and more. Swapping is especially relevant right after a large mobile provider's data breach. Cybercriminals can steal millions of phone numbers and user associated personal details. They can ther use these details to SIM swap, allowing them to receive users' text or email two-factor authentication codes to gain access to personal accounts.

How Can You Tell If You've Been SIM Swapped?

The most glaring sign that your phone number was reassigned to a new SIM card is that your current phone no longer connects to the cell network. That means you won't be able to make calls, send texts, or surf the internet when you're not connected to Wi-Fi. Since most people use their smartphones every day, you'll likely find out quickly that your phone isn't functioning as it should.

Additionally, when a SIM card is no longer active, the carrier will often send a notification text. You may also receive a text asking you to restart your device. This is usually a message sent by the hacker. Restarting your device gives them a chance while your phone is off to steal your SIM details. Never click on any links to verify. If you receive one of these texts but didn't deactivate your SIM card, use someone else's phone or landline to contact your wireless provider.

If you are using something like Find My iPhone for iOS or Google's, find my device for Android, then this can be a good way to check for SIM problems. If your phone is appearing in a different location, this is a sure-fire sign that your SIM card has been compromised and is being used by a hacker

TIPS ON HOW TO PREVENT SIM SWAPPING

Set up two-factor authentication using authentication apps. Two-factor authentication is always a great idea; however, in the case of SIM swapping, the most secure way to access authentication codes is through authentication apps, versus emailed or texted codes. It's also a great idea to add additional security measures to authentication apps, such as protecting them with a PIN code, fingerprint, or face ID. Choose pin codes that are not associated with birthdays, anniversaries, or addresses, opt for a random assortment of numbers.

Watch for phishing attempts. Cybercriminals often gain information for their identity-thieving attempts through phishing. This is the method they use to fish for sensitive personal information that they can use to impersonate you or gain access to your financial accounts. Phishing emails, texts, and phone calls often use fear, excitement, or urgency to trick people into giving up valuable details, such as Social Insurance Numbers, birthdays, passwords, and PINs. Be wary of messages from people and organizations you don't know. Even if the sender looks familiar, there could be typos in the sender's name, logo, and throughout the message that are a good tipoff that you should delete the message immediately. Never click on links in suspicious messages.

Use a password manager. Your internet browser likely asks you if you'd like the sites you visit to remember your password. Always say no! While password best practices can make it difficult to remember all your unique, long, and complex passwords and passphrases, do not set up autofill as a shortcut. Instead, entrust your passwords and phrases to a secure password manager, such as True Key. A secure password manager makes it, so you only have to remember one password. The rest of them are encrypted and protected by two-factor authentication. A password manager makes it very difficult for a cybercriminal to gain entry to your accounts, thus keeping them safe.

Boost Your Smartphone Confidence

With just a few simple steps, you can feel better about the security of your smartphone, cellphone number, and online accounts. There are identity theft protection companies out there that will detect suspicious activity on your devices for a cost of course. Time is of the essence in cases of SIM swapping and other identity theft schemes. If you suspect sim swapping has occurred, take immediate action to secure your bank accounts and change passwords.