SIM SWAPPING AND MOBILE PHONE HIJACKING

As your trusted financial partner, S&T Bank continually works to ensure that you have a safe and secure banking experience. We also want to make you aware of emerging fraud risks so that you can better protect your personal information from potential compromise.

What is a SIM Card?

A SIM (Subscriber Identity Module) card is a piece of plastic with a silicon chip containing unique data on it, similar to the chips found on credit cards. These cards link a mobile device to the owner's account and make it possible to route communications for individuals to the right device on networks maintained by various mobile carriers.

What is SIM Swapping?

SIM swapping is a technique used by attackers to gain unauthorized access to a victim's mobile phone number and associated accounts. The process typically involves the attacker gaining the victim's personal information through social engineering, then contacting the mobile carrier posing as the legitimate account owner, typically claiming to have lost their phone and requesting a new SIM card or SIM swap. Once the carrier approves the request, the attacker's SIM becomes associated with the victim's mobile phone number. The victim losses service and the attacker gains control over all activities associated with the victim's old phone (incoming calls, text messages, authentication codes, etc.).

SIM swapping and mobile phone hijacking attacks can have a devastating impact on the victim, leading to possible identity theft and enabling fraud. By following the preventative measures identified below, you can reduce the risk of these attacks and protect your personal information and privacy:

Preventative Measures

Confirm a Passphrase or PIN is Setup on Your Account

Most carriers provide an extra layer of security to your account by allowing you to setup a PIN or passphrase that is required before any changes can be made to your account. Contact your carrier if you're unsure whether this feature is already enabled for you. (Some carriers even support enabling a PIN for your SIM card within your device. Enabling a SIM PIN can help prevent unauthorized SIM swapping).

Avoid Sharing Personal Information

Be cautious about sharing personal information online and on other social media platforms. Information can be harvested to impersonate you or answer security questions. Attackers use various social engineering tactics in an attempt to gain trust and trick their victims.

Use Two-Factor Authentication (2FA)

Consider implementing 2FA on your accounts where possible, avoid using SMS messaging as the second factor where able.

Remain Cautious of Phishing Attempts and Suspicious Messages

Attackers are looking to trick you into revealing personal information and login credentials. Always take a moment to verify authenticity of communications, especially when personal information is requested from an unknown source.

Monitor Your Accounts

Regularly monitor your accounts for any suspicious activity. Most carries provide the ability to enable alerts for account changes and login activity.

Use Strong Passwords

Use complex passwords and avoid reusing the same password across multiple accounts.

Regularly Update Software

Keep your mobile device updated with current application and operating system patches to help prevent vulnerability exploitation.

Beware of Public Wi-Fi

Avoid connecting to public Wi-Fi, especially those that are not secured. It is rather simple for an attacker to intercept your data and possibly even gain access to your device.

Encrypt Your Data

Ensure your device is setup with encryption enabled to prevent unauthorized access in the event your device is lost or stolen.

Review Permissions on Your Apps

Avoid installing applications requesting unnecessary permissions, revoke permissions that could compromise your privacy and security.

Please visit stbank.com often to stay abreast of rising fraudulent scams and the best ways to mitigate potential risks.