MOBILE PHONES AND DEVICES TARGET OF SIM CARD SWAPPING SCAM

Cellphones and mobile devices today are more than a means of communication. They are portable computers that conveniently fit in our pockets and store a wealth of significant, personal data. The phone number itself is often used as a means to verify your identity, linked to your bank accounts, email, social media accounts and more. As a result, bad actors can help themselves to the data stored on your device through SIM-card swapping without physically having possession of your phone.

WHAT IS A SIM CARD?

A subscriber identity module, or SIM card, is a small plastic chip inside your cellphone or mobile device that stores information or data, including which cellular network your cellphone connects to and the phone number assigned. In addition, the stored information may include your contacts; billing information; passwords; biometric information used to authenticate you, such as your thumbprint; and other sensitive information.

PHONE PORTING VS. SIM SWAPPING

Phone porting is a legitimate service that enables a mobile device user to switch cellphone carriers while retaining the same phone number. When the user switches cellular services and keeps the same phone number, the information stored on the SIM card is transferred to the new carrier. This is called "porting" and is required under current U.S. laws.

In addition, a legitimate mobile device user may transfer the data stored on their current SIM card, including the phone number, to a new SIM card with the same cellular network. This is called SIM swapping and is often initiated by the user when upgrading to a new or different mobile device.

WHAT IS A SIM SWAP SCAM?

Malicious SIM swapping and phone porting, also known as "SIM hijacking" or "SIMjacking," is a type of account takeover. Using data that's often exposed in prior data breaches or information you may publicly share on social networks, the attacker poses as you to trick your cellphone carrier into switching the SIM card linked to your phone number and replaces it with a SIM card in their possession.

Once the SIM card has been transferred, your phone completely loses service; you can't send or receive text messages or phone calls. **If your device loses service unexpectedly or presents a warning indicating no active SIM card, contact your phone service provider as soon as possible.** You may receive a text message stating that the SIM card for your number has been changed and to call customer service if you didn't make the change. However, with your SIM card no longer active, you cannot use it to call your carrier and will need to use a different device.

WHY DOES IT MATTER?

Malicious SIM swapping allows attackers to impersonate the targeted user and access one-time passcodes sent via text message to the targeted user's mobile number. These authentication codes can be used to access email addresses, bank accounts, online banking credentials, cryptocurrency wallets and other accounts. Once the attacker has access, they can change your username and passwords, and are just a few clicks away from logging into your email, bank or social media accounts.

HOW TO PROTECT YOURSELF

MULTIFACTOR AUTHENTICATION

U.S. mobile carriers offer limited protection against malicious SIM swapping. Most companies offer multifactor authentication to authorize the swapping or porting of a phone number. Users should take advantage of these options, if available, and request such options, if not available.

ONLINE BEHAVIOR

Beware of phishing emails and other ways attackers may try to access your personal data that may help them convince your cellphone carrier that they are you.

NO-PORT OPTION

Some carriers offer this as an additional layer of protection against SIM swapping, although phone companies typically require a customer to call and inquire about the no-port feature.

ADDITIONAL ACCOUNT SECURITY

Always talk with your PNC representative about the latest security features offered specific to your bank accounts.

PROTECT YOUR DEVICE

While working with employees in a carrier's retail store, make sure your phone and SIM card are always in your sight.

CON PDF 0520-057

PNC BANK