SEI New ways. New answers.®

SIM Swap Fraud: How it Works, How to Protect Yourself

Your cellphone could provide a way for cybercriminals to access your financial accounts. How? Through your mobile number.

In this form of fraud, scammers call your mobile carrier, impersonating you and claiming to have lost or damaged their (your) phone's SIM card. They then ask to activate a new SIM card that they own. This ports your telephone number to the fraudster's device.

Once the criminals control your phone number, they can access your phone communications with banks and other organizations with the end goal of defrauding you.

Here are three signs you may be a victim of SIM swapping:

- **You can't place calls or texts.** This likely means fraudsters have deactivated your SIM and are using your phone number.
- **You're notified of activity elsewhere.** You'll know you're a victim if your phone provider notifies you that your SIM card or phone number has been activated on another device.
- **You're unable to access accounts.** If your login credentials no longer work for finance-related accounts, you likely have been taken over. Contact your bank and other organizations immediately.

And here are ways you can help protect yourself:

- **Online behavior.** Beware of phishing emails and other ways attackers may try to access your personal data.
- **Account security.** Boost your cellphone's account security with a unique, strong password and strong questions-and-answers that only you know.
- **PINs.** If your carrier allows you to set a separate passcode or PIN for your communications or changes to your account, consider doing it.
- **IDs.** Don't build your security and identity authentication solely around your phone number.
- **Behavioral analysis technology.** Banks can use technology that analyzes customer behavior to discover compromised devices, warning them not to send SMS passwords.
- **Callbacks.** Some organizations call customers back to make sure they are who they say they are—and to catch identity thieves.