Stealing Your ID by Stealing Your Phone's Account: How to Avoid the SIM Swap Scam

Author : David Gurliacci

Categories : Consumer and Finances, Public Safety

Tagged as : Crime Prevention Advice 2019, Crime Prevention Tips, Crime Prevention Tips 2019, Identity Theft, Identity Theft Scams 2019, SIM Swap Scam

Date : October 26, 2019

If your cell phone is your go-to device for checking your email, paying your bills, or posting to social media, you're not alone.

So imagine that your cell phone suddenly stops working: no data, no text messages, no phone calls.

Then picture getting an unexpected notification from your cellular provider that your SIM card has been activated on a new device. What's going on? These could be signs that a scammer has pulled a SIM card swap to hijack your cell phone number.

— This article *(except for the NPR excerpt in the sidebar) is from the Federal Trade Commission's*

So how do scammers pull off a SIM card swap like this? They may call your cell phone service provider and say your phone was lost or damaged. Then they ask the provider to activate a new SIM card connected to **your** phone number on a new phone — a phone **they** own.

If your provider believes the bogus story and activates the new SIM card, the scammer — not you — will get all your text messages, calls, and data on the new phone.

The scammer — who now has control of your number — could open new cellular accounts in your name or buy new phones using your information.

Or they could log in to your accounts that use text messages as a form of multi-factor authentication. How? Because they'll get a text message with the verification code they need to log in.

- **Multi-factor authentication** (MFA) can provide extra account protection by requiring two or more credentials to log in. Besides your password, you'll need a second credential to verify your identity. That could be **something you have** — like a passcode you get via text message, a security key, or an authentication app. Or **something you are** — like a scan of your fingerprint, your retina, or your face.

Armed with your log in credentials, the scammer could log in to your bank account and steal your money, or take over your email or social media accounts. And they could change the passwords and lock you out of your accounts.

SIDEBAR:

Why This Is Worse Now and Who Gets Targeted More

From ""SIM-Swap' Scams Expose Risks Of Using Phones For Secondary I.D.*," a National Public Radio news segment on Oct. 25:*

- "[S]ometimes it's an inside job, with phone company staffers helping to make the switch, as alleged by federal prosecutors in a case this spring."
- "SIM-swapping has been around for years, but there's never been so much at stake. 'Phone numbers have suddenly become valuable,' says Allison Nixon, director of security research at Flashpoint, a company that tracks cyber crime. She says phone numbers have become an

irresistible target for scammers because so many companies now use the numbers to help confirm customers' identities."

- "As scams go, SIM-swapping is labor-intensive." The thieves do research on targets who are wealthy, because that's where they can get a big payoff. One crypto-currency investor in California says he lost $24 million through a SIM-swap scam last year. But as choice victims wise-up, the scammers could go down market to increasingly less wealthy potential victims.

How to Protect Yourself From This

Here's what you can do to **protect yourself from a SIM card swap attack:**

- **Don't reply to calls, emails, or text messages that request personal information.** These could be phishing attempts by scammers looking to get personal information to access your cellular, bank, credit or other accounts. If you get a request for your account or personal information, contact the company using a phone number or website you know is real.
- **Limit the personal information you share online.** If possible, avoid posting your full name, address, or phone number on public sites. An identity thief could find that information and use it to answer the security questions required to verify your identity and log in to your accounts.
- **Set up a PIN or password on your cellular account.** This could help protect your account from unauthorized changes. Check your provider's website for information on how to do this.
- **Consider using stronger authentication on accounts with sensitive personal or financial information.** If you do use MFA, keep in mind that text message verification may not stop a SIM card swap. If you're concerned about SIM card swapping, use an authentication app or a security key.

If You Think It's Already Happening to You

If you're the target of a SIM swap scam:

- Contact your cellular service provider immediately to take back control of your phone number. After you re-gain access to your phone number, change your account passwords.
- Check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution.

If you think a scammer has your information — like your Social Security, credit card, or bank account number — go to IdentityTheft.gov to see the specific steps to take.

Find out what else you can do to protect the personal information on your phone and how to keep your personal information secure online.