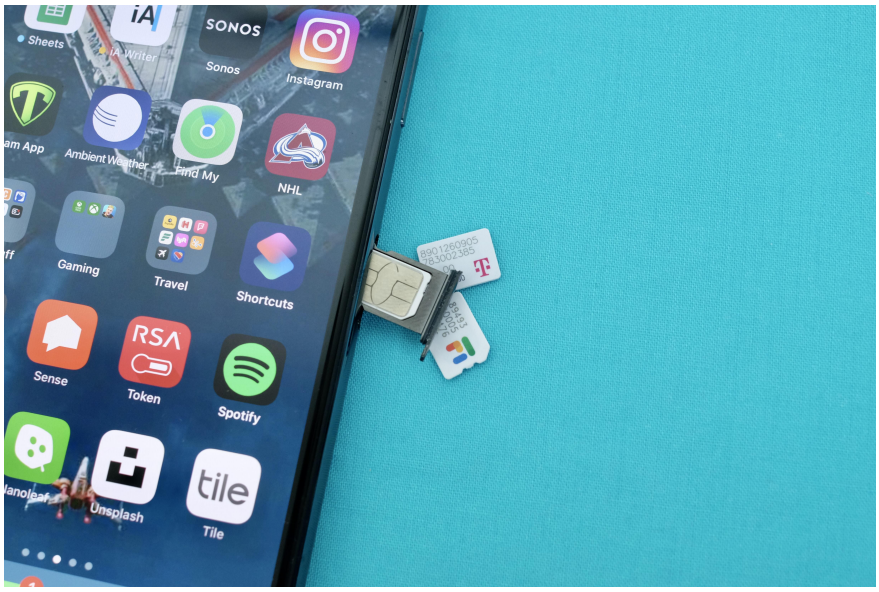
# SIM swap fraud: What it is, why you should care and how to prevent it

Phone number theft is something you need to be aware of -- it's all too easy to give hackers the keys to your online accounts.

Scams related to the coronavirus pandemic are on the rise. Phone calls and text messages claim to offer a cure or test kits, but what the scammers are really after is your personal information. With that information, hackers and scammers can do all sorts of things, like take control of your phone number and then access your online accounts.




In January, a published study revealed how incredibly easy it to do, potentially leading to thousands of dollars in fraud -- that's *your* money on the line. The practice of SIM swapping is becoming increasingly common, and despite carriers putting safeguards in place, researchers were able to demonstrate taking over your phone number quickly and with ease.

The SIM card inside your phone is a small plastic chip that tells your device which cellular network to connect to, and which phone number to use. We rarely ever think about SIM cards, except maybe when we get a new phone.

SIM swapping occurs when someone contacts your wireless carrier and is able to convince the call center employee that they are, in fact, *you*, using your personal data.

They do this by using data that's often exposed in hacks, data breaches, or information you publicly share on social networks to trick the call center employ into switching the SIM card linked to your phone number, and replace it with a SIM card in their possession.

Once your phone number is assigned to a new card, all of your incoming calls and text messages will be routed to whatever phone the new SIM card is in.

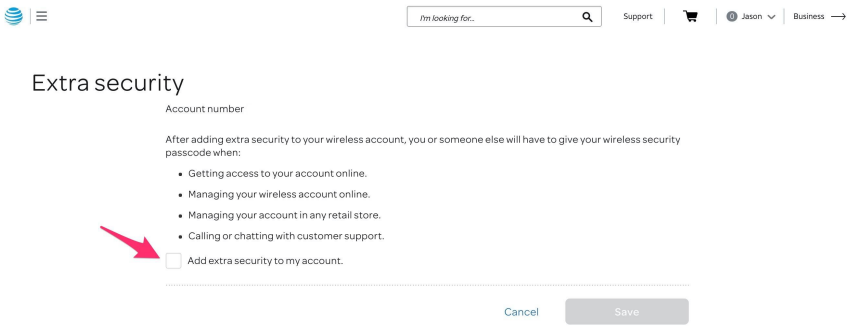
At first glance, it seems somewhat harmless. But when you consider that most of us have our phone numbers linked to our bank, email and social media accounts, you quickly begin to see how easy it would be for someone with access to your phone number can take over your entire online presence.

Matthew Miller, a contributor to CNET sister site ZDNet, fell victim to a SIM swap scam last year, and he's still experiencing the repercussions of the fallout. Whoever took over Miller's phone number gained access to his Gmail account, and promptly changed his password, then erased every email, deleted every file in his Google Drive account, and eventually deleted his Gmail account altogether.

Miller later discovered he was targeted because he had a Coinbase account and his bank account was linked to it. Miller's phone received his Coinbase account's two-factor authentication codes, so the hackers were able to log into his cryptocurrency trading account and buy $25,000 worth of Bitcoin. Miller had to call his bank and report the transaction as fraud. That's on top of the immense vulnerability he felt.

One ill-gotten gain for someone who takes over your phone number is the instant access to any two-factor authentication codes you receive through text messages, the pin that an institution texts you to verify that you are who you say. That means if they have your password, they're just a few clicks away from logging into your email, bank or social media accounts.

And if someone gains access to your email account, they can change passwords and search through your email archive to build a list of your entire online presence. Take the time to move away from SMS 2FA codes and use app-based codes instead. Seriously.




# What can you do to prevent SIM swapping on your account?

You can decrease your chances of someone gaining access to and taking over your phone number by adding a PIN code or password to your wireless account. T-Mobile, Verizon, Sprint and AT&T all offer the ability to add a PIN code.

Some companies, like Sprint, require you to set up a PIN code when you sign up for service. However, if you're unsure if you have a PIN code or need to set one up, here's what you need to do for each of the four major US carriers.

1. **Sprint customers**: Log in to your account on Sprint.com then go to **My Sprint** > **Profile and security** > **Security information** and update the PIN or security questions then click **Save**.

1. **AT&T subscribers**: Go to your account profile, sign in, and then click Sign-in info. Select your wireless account if you have multiple AT&T accounts, then go to **Manage extra security** under the **Wireless passcode** section. Make your changes, then enter your password when prompted to save.

1. **T-Mobile users**: Set up a PIN or passcode the first time you sign in to your My T-Mobile account. Pick **Text messages** or **Security question** and follow the prompts.

1. **Verizon Wireless customers**: Call *611 and ask for a Port Freeze on your account, and visit this webpage to learn more about enabling Enhanced Authentication on your account.

If you have service through a different carrier, call their customer service number to ask how you can protect your account. Most likely, you'll be asked to create a PIN or passcode.

When creating a PIN or passcode, keep in mind that if someone has enough information to fake that they're actually you, using a birthday, anniversary, or address as the PIN code isn't going to cut it. Instead, create a unique passcode for your carrier and then store it in your password manager.

## How do you know if you've been affected?

The easiest way to tell if your SIM card is no longer active is if you completely lose service on your phone. You may receive a text message stating the SIM card for your number has been changed, and to call customer service if you didn't make the change. But with your SIM card no longer active, you won't be able to place a call from your phone -- not even to customer service (more on this below).

In short, the quickest way to tell if you've been affected is if your phone completely loses service and you can't send or receive text messages or phone calls.

## What should you do if you find yourself a victim of SIM swap fraud?

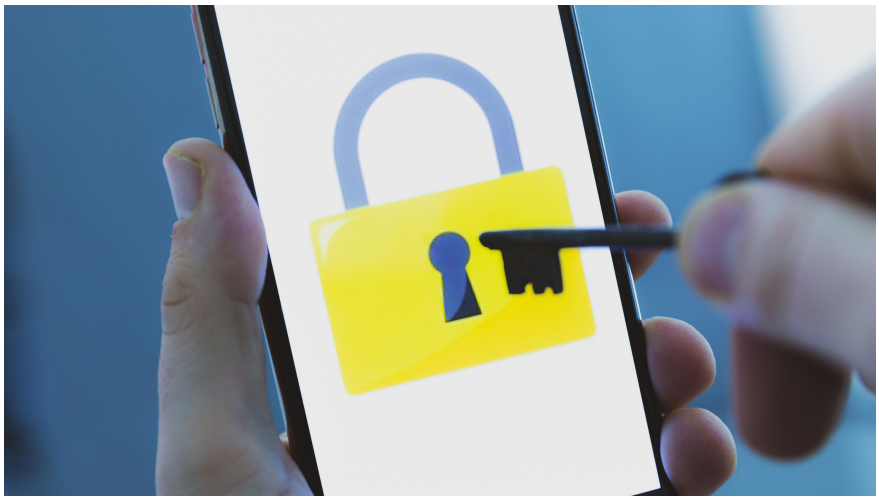
The truth is, if someone wants access to your phone number bad enough, they will do all they can to trick your carrier's support representative. What we've outlined above are best practices, but they're not foolproof.

Researchers were able to pose as account holders who had forgotten their PIN or passcodes, oftentimes providing the recent numbers called by the account holder. How do they know those numbers? They either tricked the account holder into calling a couple of numbers -- or even scarier, phone numbers for incoming calls to the account they want to take over, meaning the bad guy simply needed to call the target's phone number themselves.

Once you realize you've lost service on your mobile device, call your carrier immediately and let them know you didn't make the changes. The carrier will help you recover access to your phone number. I can't emphasize this enough -- *do not wait to call*. The longer someone has access to your phone number, the more damage they can do.

Here are the customer service numbers for each major carrier. Put your carrier's number in your phone as a contact:

1. **Sprint**: 1-888-211-4727
2. **AT&T:** 1-800-331-0500
3. **T-Mobile:** 1-800-937-8997
4. **Verizon:** 1-800-922-0204



With your SIM card deactivated, you won't be able to call from your phone, but at least you'll have the number handy to use on someone else's device.

You'll also want to reach out to your bank(s), credit card company, and double-check all of your online accounts to make sure that the perpetrator hasn't changed your passwords or made any fraudulent transactions. If you find transactions that aren't yours, call your bank or visit a branch right away and explain the situation.

Remember, no matter how many PIN codes or passwords we add to our online accounts, there's still a chance that someone will find a way to break in. But at least by setting a passcode for your account, and knowing what to do if you find yourself a victim of SIM swapping, you're prepared.

Another critical aspect of strong online security is to use a password manager to create and store unique passwords on your behalf. Additionally, enable two-factor authentication on every account that offers it.