The Dangers of SIM swapping

SIM swapping, also called SIM jacking or SIM hijacking, is a form of **identity theft where a criminal steals your mobile phone number by assigning it to a new SIM card.** They can then **insert the new SIM into a different phone to access your other accounts and do real damage.**

What is a SIM?

SIM stands for **subscriber identity module**, and it's commonly known as that small, removable chip card used in a mobile phone. Each SIM card is unique, and yours is associated with your mobile account. You can pop it out of your phone and put it in another, and your phone number and account data travels along.

How does SIM swapping happen?

The SIM swapping scam starts with a person impersonating you as they contact your mobile carrier. They will claim that they have a new SIM card to activate for your account. They might say the original phone and SIM card were lost, destroyed or sold with the SIM card left in accidentally.

The mobile carrier will most likely request some identity verification, such as the account PIN or security questions that you set up, or the last four digits of your social security number. More on this later. Once the criminal has persuaded the mobile carrier's customer service representative that they're legit, **they're able to get your phone number reassigned to their SIM**. The criminal has essentially disconnected your phone number from your phone and assigned it to their SIM card, which they've popped into their device. With that, they can go about **resetting account passwords and taking control of any two-factor authentication that goes to your phone via text message.** They can start accessing a multitude of accounts, email, digital payment systems, social media, shopping, and so on.

Let's get back to that detail about your **account PIN and last four digits of your social security number**. How would someone know this information? This is where things get interesting and show the direction that modern cyber criminals are taking.

Welcome to the world of data breaches

Over the years, thousands of data breaches have occurred with billions of records stolen, including the April 2021 Facebook data leak that impacted 533 million accounts. These numbers are so large, you might be numb to them now. Perhaps nothing bad has ever happened to you personally, and you've been able to change your passwords on breached accounts, so you're safe, right? Not exactly.
Our research shows that while people are gravely concerned about their bank account and social security information showing up in a data breach, they are **less concerned about their name, email address or their birth date.** And yet when put together, **this is exactly the kind of information that is risky to account security** for things like your bank, your medical records, your mobile carrier and any online account.
Here's why.
As the amount of breached data grows, cybercriminals have gotten organized, connecting the various data dumps together to create more full pictures of each individual so they can use it later. Consider the following scenario:

- **January 2019: Big Breach A**
  Includes your name, email address, password and phone number. You changed your password on that account and moved on.
- **November 2020: Big Breach B**
  Includes your email address, social security number, physical address and date of birth. This was alarming, so you changed your password just to be safe.
- **April 2021: Data Scrape C**
  Includes your name, email address, phone number and gender identity. You never heard about this one

because it wasn't a data breach at all. This information was pulled from information you made public through your social media accounts.

Here's a simple table view of what they've collected:

	Big Breach A	Big Breach B	Data Scrape C
Name	x		x
Email address	x	x	x
Password	x (since changed)	x (since changed)	
Phone number			x
Social security number		x	
Physical address		x	
Date of birth		x	
Gender identity			x

Cyber criminals could now connect these breach records via your email address, which was common in all three, giving them a more complete information picture about you.
Let's talk about your mobile account PIN. Do you remember it? According to security researchers, there's a high probability that your PIN is something easy to remember, like your birthday, birth year, street address or ZIP code. Looking at the above table, **the cyber criminal now has that data, and it's associated with your phone number.** They can make a few educated guesses about your PIN to gain access to your account.
If that doesn't work, they could simply tell the mobile customer service rep Wow, I set that PIN so long ago, and I have no idea what it is. Very believable! No problem, **the customer service rep says, just tell me the last four digits of your social security number**. BINGO, the criminal impersonator also has that data at their fingertips. **The SIM transfer takes a few minutes. When it's done, you're kicked out of your phone's account.**

How do you know if you've been SIM swapped?

On your end, **your phone might start behaving strangely**. **Texting and calling may not work**. If you're on WiFi, you might start getting emails about account changes. Friends might tell you that your social media accounts have been hacked. Even worse, unauthorized bank activity could start happening.

What should I do if I've been SIM swapped?

If any of this happens, **get in touch with your mobile carrier immediately for help**.

How can I prevent SIM swapping?

There's not an easy answer to this question, but there are a few things you can start doing right away.

- **Reset the PIN** on your mobile account. Select a strong, complex PIN that only you will know. Don't use things like your address, birthdays or social security number — information that could show up in a data breach.
- Set your online profiles to be more private. In the recent Facebook data leak, no passwords or logins were stolen, rather the information collected was scraped from public profiles. Consider doing this for all social accounts — Facebook, Twitter, Instagram, LinkedIn, TikTok, SnapChat to name a few. Then move onto all your online accounts that have social aspects, like event invitation sites, workout accounts, chats, etc. Set your information as private or viewable only by trusted friends wherever you can.

Contact your mobile carrier and ask them what they're doing to protect you from SIM swapping. Your carrier may already have solid protections in place. If not, the more consumers ask service providers for security protections, the more likely they are to happen.

Don't wait for a data breach to get smart about your security

Being alert to security issues like data breaches and SIM swapping is part of modern internet citizenship as we do more with our devices and live online. Here are some more tips:

- **Use Firefox Monitor**. Check to see if your email address has been part of a previous data breach and get alerted to future ones.
- Choose strong, unique passwords. Firefox Password Manager can suggest strong, unique passwords, save them, and help you manage them whenever you're logged into your account.
- **Use Firefox Relay**. Use Relay's email aliases to break the email address connection between your data in different data breaches.
- **Make your social media accounts more private.** Part of what makes social media fun is that people share personal stories and info. But that doesn't mean your account needs to share personal data publicly like your phone number, address, location and birthday (to name just a few things) with anyone who looks for it.

Consider using a 2-factor authentication device or app that doesn't use SMS or texting.