Why You Need To Lock Your Phone Number Today

Clark Howard | August 7th, 2025

I read the financial press every day and stay on top of the latest threats to your money. Recently, I came across an article written for a corporate audience, and it was a real eye-opener. It was all about the problems companies are having because of a sneaky crime called "SIM swapping," and how they're all playing this hot potato game of who is going to be left holding the bag.

So, what is a SIM swap, and why is it such a problem?

Why SIM Card Swapping Is a Dangerous Scam

It's a form of identity theft where a criminal impersonates you and convinces your cell phone provider to transfer your phone number to a new SIM card. Sometimes, this happens with the help of an insider at the cell phone company, but often, it's just an outsider who is really good at faking your identity.

The criminal's goal is simple: They want to steal your phone number. Once they convince your cell phone carrier that they are you, they can port your number out and put it on their own phone.

You might be thinking, "What's the big deal? It's just my phone number." But this is a key tool in a criminal's toolbox. For years, companies have lulled themselves into a false sense of security, believing they're protecting your accounts with two-factor authentication. You know, when they send you a one-time use code to your phone to log in?

Well, criminals adapt. They figured out how easy it was to steal your number, and with it, they get the two-factor authentication codes. They normally strike overnight when you're sleeping and not using your phone. Suddenly, your phone service goes dead, and you don't realize it. But on their end, your number is now active on their phone.

The two-factor authentication code for your bank, brokerage, or retirement account now goes directly to them. They use that code to log in, verify they are "you," and before you know it, all your money is gone.

This is exactly what that corporate article was about. Corporate America is in a panic, asking themselves, "What are we going to do? Are we going to give people their money back, taking a hit to our profits, because our security system failed? Or are we going to refuse to give them their money back and make it their problem?"

Right now, SIM swapping is a key tool for criminals, but you have the power to shut them down. And it's so easy.

How To Protect Yourself From SIM Swap Scams

Every cell phone provider has a different procedure, but **you need to put a SIM lock in place.** For my provider, Google Fi, I can do it right in my account. I have my number locked so that if somebody tries to move my service somewhere else, they can't. And when they can't steal my number, they just move on to the next person.

I'm willing to bet that nearly zero people have a SIM lock in place with their cell phone provider. You need to sign in to your account or use your cell phone provider's app, and there will be a procedure to lock your service.

Now, there is a minor hassle to this. If you decide to switch carriers, you have to go through the procedure to take off your SIM protection first. But that small inconvenience is nothing compared to having your money stolen.

Remember this: There is probably not a single person in this country who has not been a part of a data breach. We get those inane letters from corporations or governments or colleges all the time telling us our information has been compromised. The criminals have this data. They know your current and prior addresses, your date of birth, and your Social Security number. When they decide it's your turn to be a victim, they will try to steal your money.

One of the key tools that will shut them down cold is having that SIM lock in place. **If you do nothing else today, I want you to make sure you have your SIM locked down with your cell phone carrier.** I don't want the money you've worked hard to save to suddenly vanish from your life.