AGENTIC ARMOR

Lock Your Number

A plain guide to stopping SIM swap fraud: the three moves, in order, carrier locks first because they are free.

Your phone number is the master key to your digital life, and most people do not know it can be stolen without anyone touching your phone.

What is a SIM swap?

A SIM swap is when a criminal convinces your phone carrier to move your number to a phone they control. Sometimes they port the number to another carrier. Sometimes they swap it onto a new SIM card. Either way, your calls and text messages start going to them instead of you.

That is dangerous because of what your texts carry. Banks, email accounts, and shopping sites send sign-in codes by text message. If your number moves, those codes go to the thief. With your codes in hand, they can reset your passwords, empty accounts, and lock you out of your own life, often in under an hour. Carriers have gotten better at checking identity, but the attack still works often enough that the fix is worth an evening of your time.

There are three moves that stop it. Do them in this order. The order matters.

This guide is the how. Its companion editorial, The Carrier Lock, is the why: the argument for why a free protection that ships turned off cannot wait. The two were written to be read together.

The first move: lock your number at the carrier. This one is free.

Every major carrier in the United States is required to offer you two locks, free of charge: one that blocks changes to your SIM, and one that blocks your number from being ported to another carrier. Most accounts have both locks turned off. Turning them on takes about twenty minutes.

Call your carrier or open their app, and ask for the SIM change lock and the port-out lock, by those names. If the person helping you does not recognize the names, ask for the free account locks that prevent a SIM change or a number transfer until you personally turn them off. While you are there, set an account PIN that is not used anywhere else in your life, and turn on alerts so you are notified if anyone requests a change. Do this for every number you rely on, including a second line if you have one.

This move lives at the carrier, not in your phone, so it is identical for everyone: iPhone and Android owners take exactly the same steps, because the lock guards the number itself, not the device in your hand.

One warning: your carrier may offer to generate a transfer PIN for you. You do not need one unless you are actually moving your number to a new carrier that day. The locks are the protection. Leave the transfer PIN alone.

And one safety rule that rides with everything in this guide: your carrier will never call, text, or email you to ask for your account PIN or a transfer PIN. Anyone who asks for one is running the very fraud this guide defends against. Hang up, and call the carrier yourself, at the number on your bill.

The second move: put hardware keys on your most important accounts.

A hardware security key is a small device, about the size of a house key fob, that plugs into your phone or computer or taps against it. Your most important accounts can require it at sign-in. No key, no entry, and there is no code for a thief to intercept, because nothing is texted anywhere.

Put keys on the accounts that guard everything else: your main email, your Google, Microsoft, or Apple account, your password manager, and your bank and investment accounts where they are supported. Buy two keys, not one, and enroll both. One lives with you. The second lives somewhere safe at home. Keys cost roughly thirty to sixty

dollars each, and the major brands work with all of the big accounts. Some accounts, including Apple, require two keys to turn the feature on at all, which is the market quietly telling you the same thing this guide is.

On an iPhone, a key usually works by tapping it against the back of the phone, which is called NFC; newer iPhones can also take a key plugged into their charging port. Either way takes a second, and it works the same at sign-in as it does on any other phone or computer.

The third move: move your texted-code accounts to an authenticator app or a key.

Go through your accounts one at a time, starting with money: banks, investments, payment apps, and crypto if you hold it. Then your email and social accounts. Then everything else. At each account, open the security settings and look for the option to use an authenticator app or a security key instead of texted codes. Turn it on, prove the new method works by signing in with it, and only then turn the texted codes off.

Two things to expect. Most services will not move an existing authenticator setup for you; you enroll the new method fresh at each account, which is why this move goes one account at a time. And a few services, often smaller banks and utilities, still offer texted codes and nothing else. For those, the first two moves are your protection, plus turning on every transaction alert the account offers.

iPhone owners have one convenience worth knowing here: the Passwords app built into the iPhone can itself hold sign-in codes for accounts, so it can serve as the authenticator this move asks for, with the codes living on the phone rather than arriving by text. The enrollment at each account works exactly the same way.

Why this order

The carrier locks come first because they are free, they take minutes, and they protect every account that still depends on texted codes, including the ones you have not gotten to yet. The keys come second because they take the most valuable accounts off the phone network entirely. The account-by-account move comes last because it takes the longest, and it is safe to do slowly once the first two moves are holding.

We made the first of these moves ourselves, tonight, and it took minutes. The second and third moves are the road we are on, in the order this guide gives them, and we wrote it so you can make all three. Your number is worth locking. It holds more of your life than the phone in your pocket does.

- END OF DOCUMENT -