

How-To Geek

How Criminals Order Phones in Your Name (and How to Stop Them)



JOSH HENDRICKSON [@canterrain](#)

JULY 12, 2019, 6:40AM EDT



Cunaplus/Shutterstock

A new type of phone theft is on the rise. Instead of stealing phones directly from you, thieves impersonate you to get brand new smartphones from your cellular carrier and stick you with the bill. Here's what's going on.

ADVERTISEMENT

What Is Account Hijacking?

Outright smartphone theft is getting harder to pull off and less lucrative. We're more careful with our phones than we used to be and—starting with the iPhone—more smartphones offer encryption and lost phone tools out of the box. So, some criminals have adopted a new tactic. Instead of messing with stolen phones and worrying

about activation problems, they pose as you and order new phones on your account.

The scam works well for a variety of reasons. The criminal gets to take advantage of any phone deals your account is eligible for, paying as little as possible up-front (perhaps, even nothing at all), and you may not notice until it's too late. Upgrading your existing lines is the more noticeable method because your phones stop working, so some criminals add new lines, instead. With that route, you may not realize what's happened until the next bill comes. And, if you have your phone bill set up for automatic payment, you could miss it for longer than that.

In some cases, the point isn't to steal phones. Criminals may upgrade your lines as a means to take your number through SIM swapping. Your phone number is [transferred to a phone they have](#), which they can then use to hijack any accounts that rely on your phone number as a recovery option.

How Criminals Hijack Cell Phone Accounts



Borka Kiss/Shutterstock

At this point, you might wonder how a criminal can buy smartphones with someone else's account. Unfortunately, we've discovered more than one answer to that question.

Sometimes, the perpetrator steals your identity, creates a fake ID with your name and his photo, and then goes to a retail store to buy the phones. You might think that method could only occur close to where you are but, as [Lorrie Cranor](#), a former chief technologist for the FTC found out, that's not the case at all. She discovered her phones turned off after someone posing as her, multiple states away, upgraded her lines to new iPhones. You can find similar complaints on [phone carriers' forums](#) as well.

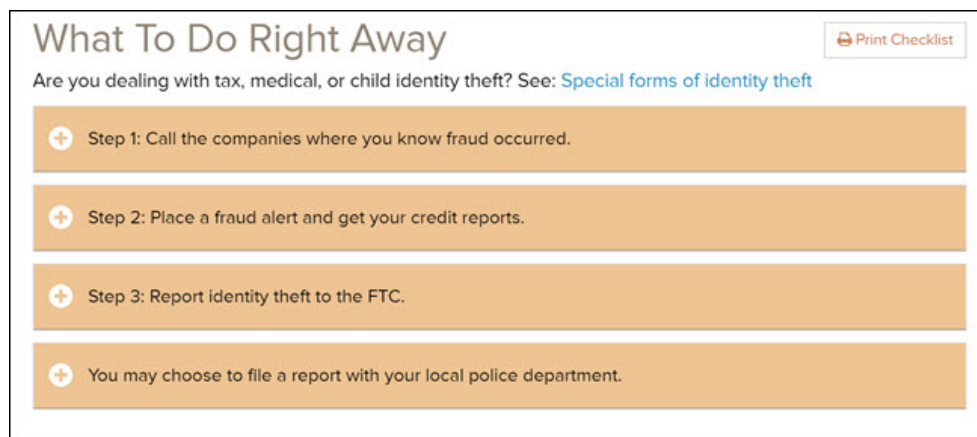
In 2017, [Cleveland police arrested three men](#) after linking them to \$65,000 worth of cell phone theft, mostly through the use of fake IDs.

In other cases, simple phishing tactics are at play. In early 2019, Verizon customers in Florida started receiving calls about suspected fraud. The representative told the victims they needed to verify their identity and, to do so, Verizon would send a PIN. They would then need to read the PIN to the person on the phone.

But the person on the phone [wasn't an employee from Verizon](#). It was the fraudster the victim had just been warned about. In this case, the thief generated an actual Verizon PIN, most likely by using the account recovery process. When the victim received the PIN and handed it over, they gave the criminal the very details they needed to get into the account and order new smartphones. Thankfully, Verizon employees noticed other red flags and called the police, but that doesn't always happen.

In late 2018, [twelve people were accused](#) of hacking into people's online accounts, adding or upgrading lines, and then shipping the new hardware elsewhere. Before police caught up with them, it's believed the perpetrators managed to obtain over \$1 million worth of devices. They used information purchased on the dark web from data breaches or, in some cases, sent phishing messages to steal account info.

What to Do if Your Account Is Hijacked



What To Do Right Away [Print Checklist](#)

Are you dealing with tax, medical, or child identity theft? See: [Special forms of identity theft](#)

- + Step 1: Call the companies where you know fraud occurred.
- + Step 2: Place a fraud alert and get your credit reports.
- + Step 3: Report identity theft to the FTC.
- + You may choose to file a report with your local police department.

identitytheft.gov

If you're the victim of account hijacking, it may feel like there's nothing you can do, but that's not true. You shouldn't have to pay for a service you didn't want, and phones you don't have. Get a pen and paper and take notes on the process. Write down which companies you called, the date and time, and the name of any person you spoke with. Take notes on what the company representatives say—especially if they promise to take action or ask you to follow up with more information or paperwork. The FTC put together a [helpful checklist](#) to follow, and we'll be covering some of those steps as well.

First, call your phone carrier and explain the situation. Ask if they have a fraud department. If they do, ask to be transferred. Explain the situation and ask for help solving the problem. Find out precisely what proof they need from you and write everything down. You should also ask if your account can be frozen and if you can add a PIN validation (or other security measures) to prevent anyone from adding more lines to your account.

Next, place a [fraud alert](#) on all your credit accounts. You might also consider [freezing your credit](#). A credit freeze should prevent anyone from opening an entirely new account in your name but, unfortunately, it might not prevent upgrade and add-a-line fraud. Many phone carriers bypass a credit check in favor of checking billing history for existing customers. Still, a credit freeze could prevent other kinds of fraud, so it's worth it.

With a credit freeze in place, it's time to report the fraud to your local police department. Call or visit them and ask how to report the

situation. Be sure to have any proof on hand, like bills from the added lines. Explain what happened and get a copy of all the paperwork.

Now, contact your phone carrier again with any paperwork they requested (including the police report) and ask how to reverse all charges if it hasn't already been done.

Be prepared for this process to take some time—sometimes, days or weeks. Keep a log of everyone you contact and every step you take. This prevents you from repeating unnecessary steps and gives you a semblance of control over the process.

How to Prevent Account Hijacking

You can take steps to prevent account hijacking from occurring in the first place (or again). Considering how easy identity theft is, the primary goal is to put additional barriers in place. Thankfully, the four major carriers do have options. Unfortunately, while Sprint and Verizon make that extra security a requirement for all new customers, AT&T and T-Mobile do not.

If you're a Verizon customer, you should have set up a four-digit account PIN when you started the service. If you didn't, or you forgot your PIN, go to the company's [PIN FAQ page](#), and click on the "Change Account PIN" link. Log in with your Verizon account when prompted.

Sprint also [requires a PIN](#) as part of a customer's account setup, so if you're with Sprint, you should already have one. Sprint also requires a security question as a backup and lets you pick from a list. Try to pick a question that can't easily be found in a Google search. If you forgot your PIN, you can sign in to your online account and change it in the Security & Preferences section.

AT&T customers [aren't required to set a PIN](#), but you should. You'll need to log into AT&T's online portal. Look for two options: Get a new passcode and Manage extra security. You should go through both of these processes. Manage extra security simply tells AT&T to ask for your passcode in more situations, like managing your account in a retail store.

By default, T-Mobile asks [account verification questions](#) to determine identity. You can set up a PIN to use instead, but the only way to do so is to call them. From a T-Mobile phone, you can use 611. T-Mobile has two options: an account security PIN and a [port out PIN](#). They protect different things, so you might want to set both.

If you're using a service other than the four major carriers, you should check its support site or call customer service to find out what security options you can set up, and how to add them.

Once you have your PINs set, it wouldn't hurt to call back in a day or two and verify that they ask for it. The process is straightforward, and you probably won't run into any issues. Peace of mind and a little practice using your new PIN is worth the time spent—especially if you discover something did go wrong, and your carrier didn't set your PIN correctly.

READ NEXT

- › [How to Stream UFC Fight Night 155 de Randamie vs. Ladd Online](#)
- › [How to Speed Up Your Internet Connection](#)
- › [How to Add Alexa to Your Smart Mirror](#)
- › [How to Encrypt and Decrypt Files With GPG on Linux](#)
- › [Windows 7's July 2019 Security Patch Includes Telemetry](#)



JOSH HENDRICKSON

Josh Hendrickson has worked in IT for nearly a decade, including four years spent repairing and servicing computers for Microsoft. He's also a smarthome enthusiast who built his own smart mirror with just a frame, some electronics, a Raspberry Pi, and open-source code. [READ FULL BIO »](#)

How-To Geek is where you turn when you want experts to explain technology. Created in 2006, our articles have been read more than 1 billion times. [Want to know more?](#)