How to Tell if Your Phone Has Been Cloned

by Natasha Stokes on March 30, 2020

Article Courtesy of: https://www.techlicious.com/tip/how-to-tell-if-your-phone-has-been-cloned/

Techlicious editors independently review products. To help support our mission, we may earn affiliate commissions from links contained on this page.

Our phones are the key to our digital identity, so it's no wonder that mobiles have become increasingly attractive targets for cybercriminals, who have at their disposal a fair number of ways to hack a smartphone, some of which require more access and technical savvy than others.

Phone cloning – or the copying of the identification credentials a phone uses to connect to cellular networks – is one method that usually requires the perpetrator to have direct access to a device. That makes it less prevalent than, say, hacking an operating system vulnerability that hasn't been updated, but the consequences are equal to that of most phone hacks – your personal data is exposed, with potential financial consequences or identity fraud.

What is phone cloning?

It's worth distinguishing between "cloning" a phone's data – which spy apps semi-legally offer as a way to spy on the photos, texts and calls of another device – and totally illegal phone cloning, which refers to the copying of a phone's complete cellular identity and using it in another device.

In cloning a phone's cellular identity, a criminal would steal the IMEI number (the unique identifier for every mobile device) from the SIM cards, or the ESN or MEID serial numbers. These identifying numbers are then used to reprogram phones or SIM cards with the stolen phone number.

Then there's also the emerging threat of SIM hijacking, where hackers who have access to stolen phone numbers call up carriers and impersonate account holders to get a new SIM the hacker controls. This method, which relies on social engineering tactics to find out personal information that carriers use to authenticate customer accounts, differs from the highly technical method for SIM (or phone) cloning, but the end result is the same – to gain control over someone's phone service.

Once the perpetrator has control of the phone line, they can send messages and make calls that appear to be from that phone number, with the bill footed by the victim. If a cloned phone and the original are near the same broadcast tower, it could even allow the perp to listen in on any calls made by the victim – though that's probably not the main driver for phone cloning.

The bigger danger is that text messages and calls intended for the rightful owner of the line can also be intercepted – including two-factor authentication codes that allow snoops to get access to critical accounts like email, social media and even banking. (The vulnerability of text messages is one reason why experts recommend other methods of two-factor authentication.)

Phone cloners might also target political figures for surveillance: in February this year, South African state security ministers were reported to have had their cellphones cloned, the crime was detected when several people reported receiving text messages from a minister who hadn't sent them.

Or, cloned phones might be used to generate revenue, sold to people who aren't aware they've purchased a fraudulent handset with stolen credentials.

How phones get cloned

Most phones have SIM cards whose IMEI numbers are protected by secret codes that prevent over-the-air interception. But if someone is able to remove the SIM card and place it in a SIM reader for a few minutes, they can copy all its identifying credentials to load onto a blank SIM. (This technically includes anyone who might get time alone with your device – but as with phone spying, you're likely to have an inkling if there's anyone who might want to do such a thing.)

Researchers have also found a vulnerability in the existing protocol that is used for over-the-air carrier updates. Though rarely used, this flaw could in theory allow hackers to remotely clone a SIM.

Some older phones are more vulnerable to remote attacks. Those running on 2G or 3G CDMA frequencies, which are used only by the Sprint and US Cellular networks (Verizon retired its CDMA network at the end of 2019), broadcast to the operator in a way that would allow special equipment – like a femtocell – to eavesdrop on the connection and intercept handset ESN or MEID serials.

That means older CDMA phones, such as flip phones or 3G-only regular and smartphones, that are locked to either Sprint or US Cellular may be at a slightly elevated risk of remote phone cloning. All that said, however, phone cloning is not as common as it was in the early days of mobile phone use, when the radio frequencies in use were much easier to eavesdrop on.

6 Signs that your phone might have been cloned

If you think your phone might have been cloned, check for these signs which can indicate someone else is using your cellular service, such as:

1. Receiving an unexpected text requesting you to restart your device

This may be the first sign that your phone or SIM has been compromised – restarting your device gives the attacker a window in which your device is off and they can load their phone with your cloned credentials.

2. Calls or texts on your cellphone bill that you don't recognize

Any outgoing texts and calls made on the cloned device will seem to be coming from your phone number – and land on your bill. Even if you don't have an itemized bill, international calls will show up here, so keep an eye on your monthly payments and double-check when you pay more than usual.

3. You stop receiving calls and texts

If someone else has control of your phone number, calls and SMSes may be diverted to their cloned device, or your cellular connection stopped entirely. Check this by having a friend or your partner call you to see if the call rings and if it comes through to your phone.

4. You see your device in a different location on Find My Phone

Logging into Find My iPhone or Google's Find My Device can be a way to check on the integrity of your SIM. If your phone's on your desk, but on the map appears to be somewhere else, someone else may be using your cell service. (Chances are, phone hackers would disable this setting, however.)

5. You get a message from your carrier saying your SIM has been updated

If your credentials have been activated on a new device, your network provider will probably send a message confirming your details have been updated – a major red flag if you haven't done anything. This can also be the point at which you find your device no longer has cellular service.

6. You're mysteriously locked out of your accounts

You might even find someone has commandeered your email accounts and social media handles – as in a spat of Instagram hacks based on stolen phone numbers (in these cases, however, the SIMs were hijacked by attackers who had gleaned enough personal information online to fool carriers into switching over the SIM cards). Either way, someone having control over your phone service means they can do things like trigger a forgotten password, receive a two-factor authentication code to the

phone number they now have access to, then change the password and access any account they know your login name for.

If the worst has happened and your phone has been cloned, you need to call your cellular provider. They should be able to detect and block the cloned device, because each handset has a unique radio fingerprint independent of that serial number that originally belonged to you.

Can you prevent phone cloning?

You can help protect your phone from this type of cloning by observing the same cybersecurity practices that keeps your online life safe:

- Check that carrier texts are coming from legitimate numbers – for example, do they show up in the same message thread as previous carrier texts?
- Train a skeptical eye on any text that requests you do something – are they worded in the way you would expect? What do Google search results have to say about the sender's number?
- Finally, treat your phone's IMEI, ESN or MEID number like any other password - never send it to anyone or give it to any website you don't trust.

Cloning isn't the only way your phone can be compromised. If you have concerns about the security of your device, read our story on how to tell if your phone has been hacked.