6 things to know about used or refurbished Android phone

If your Android phone isn't running the latest software, your security and privacy might be in jeopardy.

With flagship phones like the Samsung Galaxy S20 Ultra and iPhone 11 Pro costing over $1,000, it's more tempting than ever to pick up a bargain, refurbished phone. But while you can pick up a used Samsung Galaxy, Sony or HTC phone that's of good quality for a very low price, is it actually safe to use these phones?

Phones released years ago run outdated versions of Android. That may well mean that they don't have critical security updates that can keep you -- and your data -- safe from prying eyes. If you're concerned about security and privacy on your previously owned phone, here are some things you should consider.

What is a security patch for a phone OS?

Whenever hackers discover a new hole in your phone's software to exploit, phone-makers usually get it fixed, and that fix is sent out to your phone to make sure that nobody can take advantage of it. That's a security patch. You'll likely have received plenty of them over time as cybercriminals are always trying to find new ways to circumvent the security on your phone. It's a continual cycle of identifying threats, solving them, then finding the next one.

Most of the time, you'll never know about it, but it's the thing that's keeping your phone up to date and protected against known threats.

Why do manufacturers stop sending out security patches?

Manufacturers such as Samsung, Sony, Google and HTC only provide support to a phone for so long. Each new handset that's released and each new version of Android require new threat assessment and patching. That's a lot of work, and it means that finding and patching those holes for every single handset spanning years and years just becomes unfeasible.

As a result, Google and the phone-makers eventually have to cut off support for older handsets, usually once a device gets to be two or three years old. Those handsets then will no longer receive security updates, meaning that when a threat is detected on that phone, it simply won't be fixed.

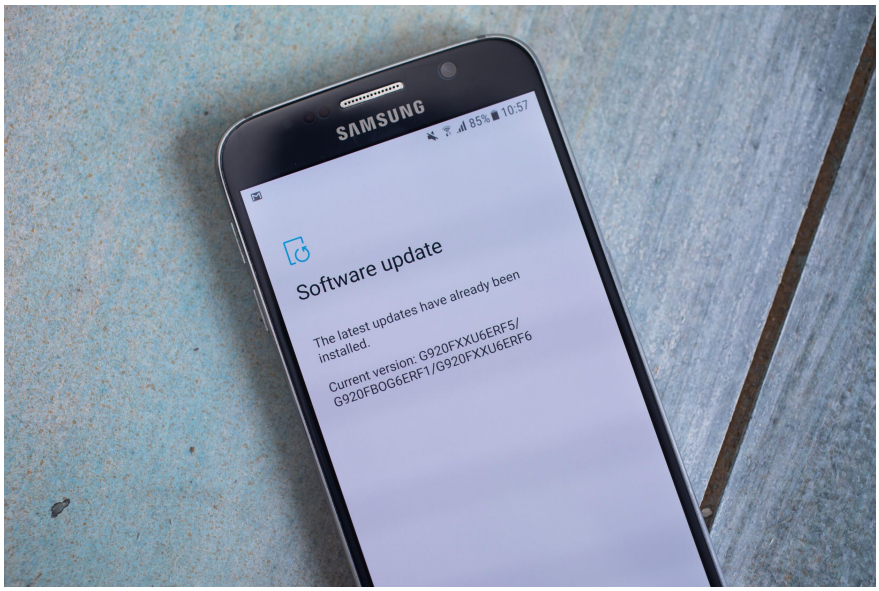
So is using an out-of-date phone safe?

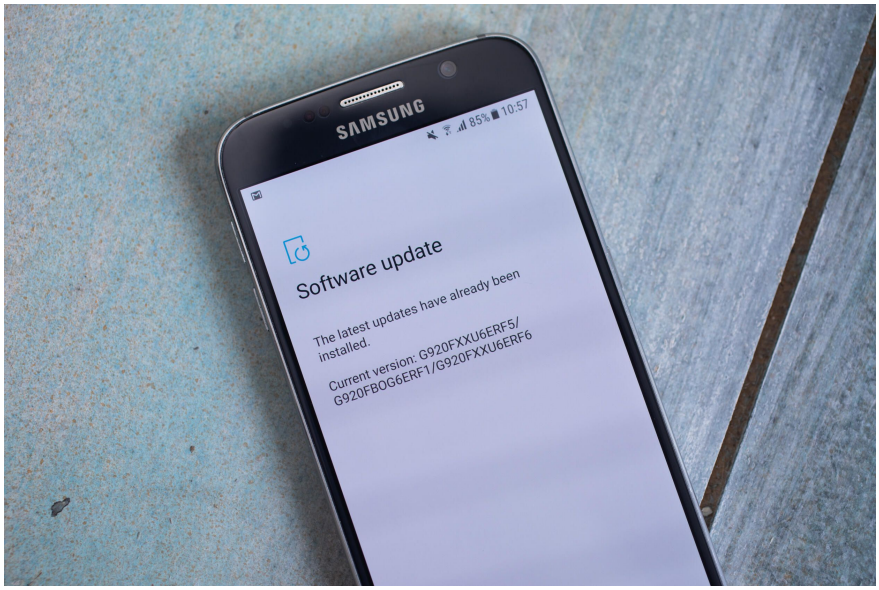
As Christoph Hebeisen, director of security intelligence company Lookout, explains, "We do not consider it safe to run a device that does not receive security patches. Critical security vulnerabilities become public knowledge every few weeks, or months, and once a system is out of support, then users who continue to run it become susceptible to exploitation of known vulnerabilities."

According to Hebeisen, a vulnerable phone could allow full access to everything that's on your phone, including your personal and company emails, contact information, your banking details or audio of your phone calls. A hacker could continue to have access to this information for as long as you continue using the compromised handset.

Paul Ducklin, principal research scientist at security company Sophos, agrees, saying, "If your phone has a software vulnerability that crooks already know how to exploit, for example to steal data or implant malware, then that vulnerability is going to be with you forever."

Read more: Best portable chargers and power banks to buy for Android in 2020



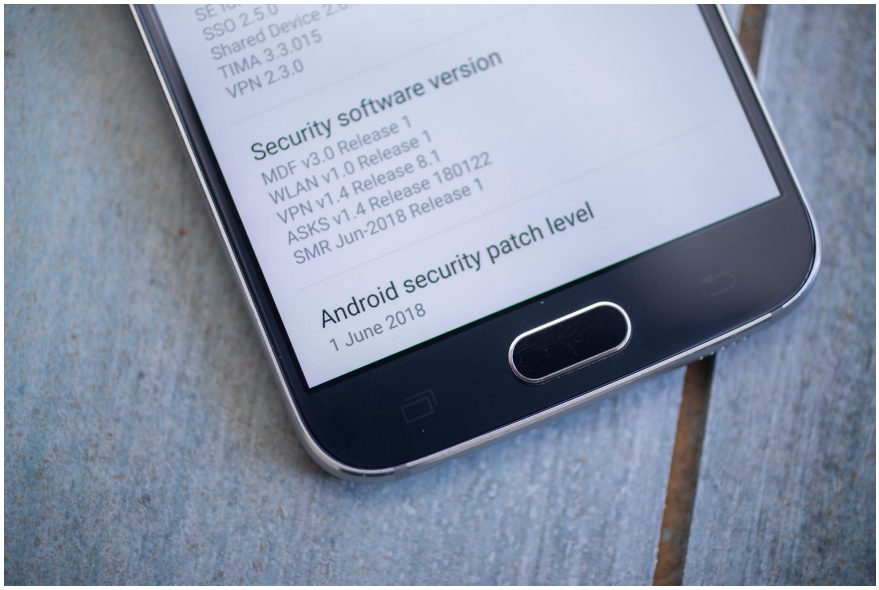


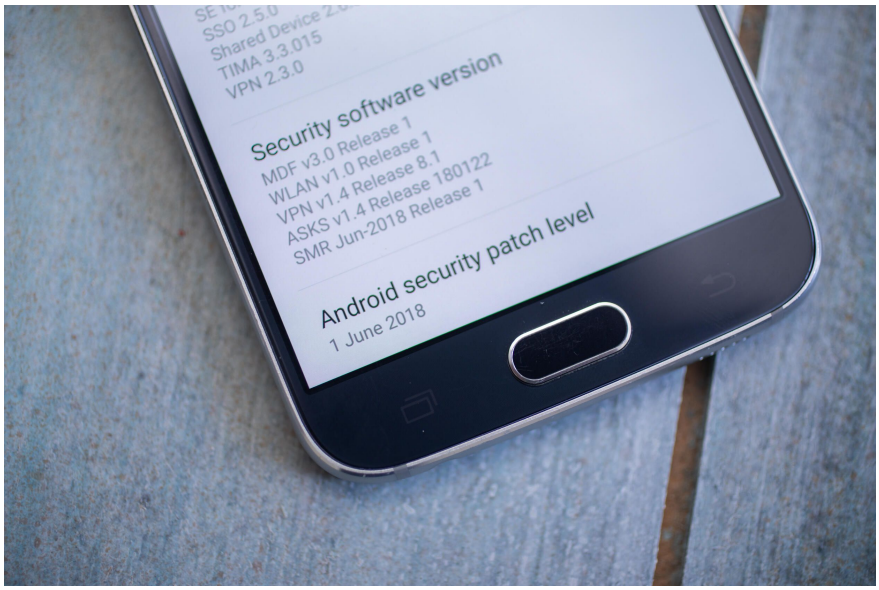
How do I know if my phone is out of date?

Finding out if your phone is still supported and receiving security patches often isn't straightforward. To start, go into Settings and check your software updates. Install the latest version. Usually it'll give you some indication of when the phone was last updated. If your phone says it has the latest OS software, but that latest version was installed many months or years ago, it's bad news. Your phone is probably no longer supported.

Sadly, manufacturers don't give you a big warning that tells you when they've dropped support for a phone, so you either find out through a rude awakening like I mentioned above or figure it out yourself through some other means.

A good rule of thumb is that a phone will no longer be supported if it's two to three years old. This varies from company to company, however. Google, for example, states that it makes security updates available for Android versions 8.0, 8.1, 9.0 and 10. Its Pixel phones get security updates for "at least three years" from when they went on sale and Google also mandates that manufacturers must provide at least two years of updates for devices. Apple, by comparison, still provides software updates for phones going back five years, because it has relatively few models to manage. The latest iOS 13 can be installed on 2015's iPhone 6S ($450 at Sprint).





Finding out if your Android phone is supported will involve some digging. I found Nokia's tool for seeing updates of its phones after going through a series of support pages on its website. Samsung sent me its list after I contacted its PR team, and it's available online here. Google has a page that clearly tells you when your Pixel or Nexus phone will lose security support. (Spoiler alert: All Nexus phones and the first-gen Pixel are out of support, with the Pixel 2 ($600 at Amazon) losing support this October.) Your best place to start is with the support pages on your phone manufacturer's website.

You might not notice immediately if your phone is out of date. The most obvious sign you're on old software might be when you look for new apps to download. Many apps will simply be incompatible due to the software and hardware limitations on your phone and you won't be able to install them.

How can I tell if my phone has been hacked?

Whether you'd ever notice if your phone's security was compromised is difficult to say. Cybercriminals don't exactly make it known they've accessed your device, so you'll need to look for signs. Popups that might appear on the phone are a big giveaway, as are any apps that suddenly appear that you didn't download.

Look out for unexplained high data usage too, as it could be that malicious apps are using a lot of data in the background. Other indicators can also include unusually high battery usage and sluggish performance, but both of these can also be attributed to using older hardware that degrades over time.

How can I keep myself safe if I have an old phone?

As Hebeisen says, the best way to keep yourself safe is simply to not use a phone that's no longer supported. If you're short on money, can't afford to upgrade just yet or you're using an older phone temporarily for whatever reason, there are a couple of things you can do that could help.

First, you should make sure the phone has the latest software installed. If you bought it used, make sure to fully factory-reset the phone. Ensure that you only download apps from the Google Play Store (rather than from third-party or unofficial app stores) and certainly avoid installing apps by downloading the APK file from a website. This can often be a way that malicious software weasels its way into a phone.

You can help protect your personal information by simply not giving too much away in the first place. Don't do any banking on the phone, don't sync your company email accounts and don't send sexy pictures or have sexy video chats until you're back on a protected device. (Even over a phone, it's important to practice safe sex.) According to Hebeisen, if you don't take such precautions, "this might enable an attacker to observe and manipulate almost everything happening on the device." That's a cold shower, right there.