Cheap smartphones can have serious privacy problems

For years, reports have said that low-cost smartphones are being equipped with spyware and even malware. Unfortunately, that situation remains unchanged.

Here's what to know about cheap smartphones and how you can buy a new device safely.

Why are cheap smartphones bad for privacy?

Simply put, a phone needs minimal production costs, and an incredibly cheap price means you're selling your privacy to save a few hundred thousand more. However, your stolen data is worth much more than a new smartphone.

According to the University of Edinburgh, several brands, including OnePlus, Oppo, Realme and Xiaomi, are said to have collected large amounts of data from Chinese users without their knowledge or permission. Although low-cost phones sold internationally do not use the same data collection features, they come preloaded with third-party apps that can also collect data.

American-made brands are not always better. Blu, a Miami-based smartphone brand, has been embroiled in privacy scandals twice, involving third-party vendors collecting data and sending it to Chinese servers. National, but the negligence involved has put hundreds of thousands of users at risk.

You can pay more for a phone with better privacy. The iPhone is the #1 choice for privacy, capable of protecting users from outside attacks, but installing an Android ROM like CalyxOS or GrapheneOS offers the best privacy overall.

What data do cheap smartphones collect?

Low-cost smartphones collect many types of data. Most of the data is not directly harmful and focuses on data such as IMEI numbers and MAC addresses. However, researchers looking at OnePlus and other brands also found that, in China, phones collect information about each user's phone number, app usage patterns, and performance data. capacity, call and SMS history, GPS coordinates and contact numbers.

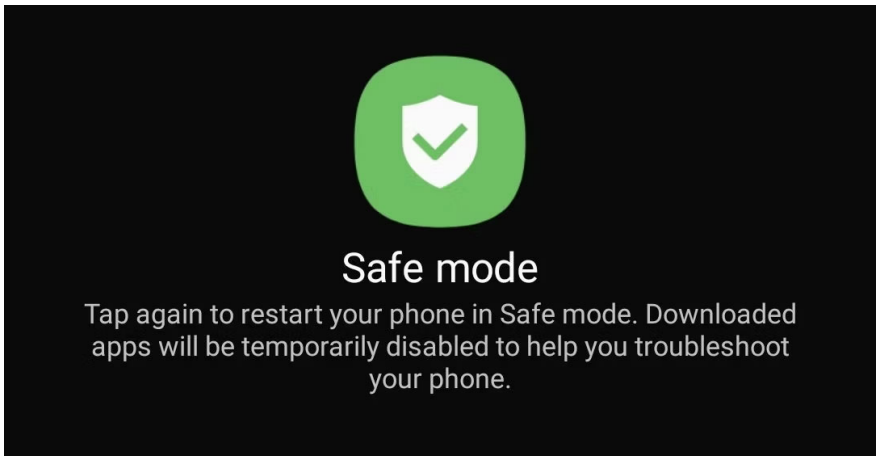
Much of this data is Personally Identifiable Information (PII). It's unclear what these brands plan to use the data for, but it's best to make sure they receive as little data as possible. You never know who might see your data or how they might use it later. For that reason, it's important to be selective about who you buy your phone from and what software you use.

How to check smartphones for spyware

If you're concerned that your phone may not be as private as you think, it's important to check for and remove any spyware on your device. Unfortunately, some cheap phones have suspicious apps that cannot be removed. In some cases, you may need to completely remove the operating system. To remove spyware:

1. Delete any apps you don't recognize.
2. Navigate to **Security and privacy > Other security settings > Device admin apps** to check for apps that have admin rights.
3. Use an anti-malware application to scan for spyware.
4. Watch for symptoms of spyware, like constant battery drain or sluggish performance.
5. Look for strange behavior like random shutdowns or reboots.

If malware scans and manual software searches don't turn up any obvious spyware but you see signs that point to the presence of spyware, activating Safe Mode is your best bet. to check the root cause. Safe Mode prevents third-party apps from running, so if your phone suddenly starts operating in Safe Mode, you'll know that you may have spyware installed.



Safe Mode can be activated by holding the power button until the reboot option appears. These options vary by device, but in general, booting into Safe Mode can be done by pressing and holding **Power Off , then waiting for the Reboot to Safe Mode** option to appear. When an option appears, tap it and allow the phone to reboot.

After the phone restarts, try using the phone and observe if the same symptoms of spyware persist. If so, the phone may be defective or the hardware may not be powerful enough. But if it suddenly works fine again, navigate to your apps in Settings and uninstall anything you don't completely trust. You should also:

1. Check your Downloads folder and App List for any files or applications you don't recognize
2. Run the scan with an anti-malware application again, as some malware may bypass detection outside of Safe Mode

If the performance difference in regular mode and Safe Mode persists but the problem cannot be fixed, then you can only resolve it by factory resetting the device. Normally, you can factory reset your device in Settings by navigating to **System > Reset > Factory reset** .

How to buy a smartphone without spyware?

If you intend to buy and use an off-the-shelf smartphone, you'll never achieve perfect privacy, but there are plenty of great options.

Apple doesn't offer complete privacy, but you can protect yourself from most outside spyware by using your iPhone. Branded Android devices are also unlikely to carry spyware.

However, that doesn't mean companies like Apple and Samsung don't collect some data. If you want perfect privacy, you'll need to install another operating system. CalyxOS and GrapheneOS are both ideal. Investing in a device with a bootloader that you can lock down, such as a Google Pixel, will also ensure that security is not hindered by your efforts to protect your privacy.

And remember that every app you install poses a privacy risk, no matter which smartphone manufacturer you buy from or which operating system you use. If you're not comfortable with Google or Meta, look for alternative apps, because no matter what phone and operating system you use, they will continue to collect any data allowed.

There will always be risks to privacy when you access the Internet and download various applications, but making the right decisions about the type of smartphone you buy and the operating system you use can makes a huge difference.