

11 Essential Tips to Keep Your Android Phone Safe

Let's face it: Our phones know more about us than we think - storing everything from personal messages to banking details!

Let's face it: Our phones know more about us than we think – storing everything from personal messages to banking details! That's why keeping your Android phone secure should be a top priority for everyone.

1. Avoid connecting to unsafe networks

While public Wi-Fi networks — like those at coffee shops or airports — are often free and convenient, they're often unencrypted, making it easier for hackers to steal data.

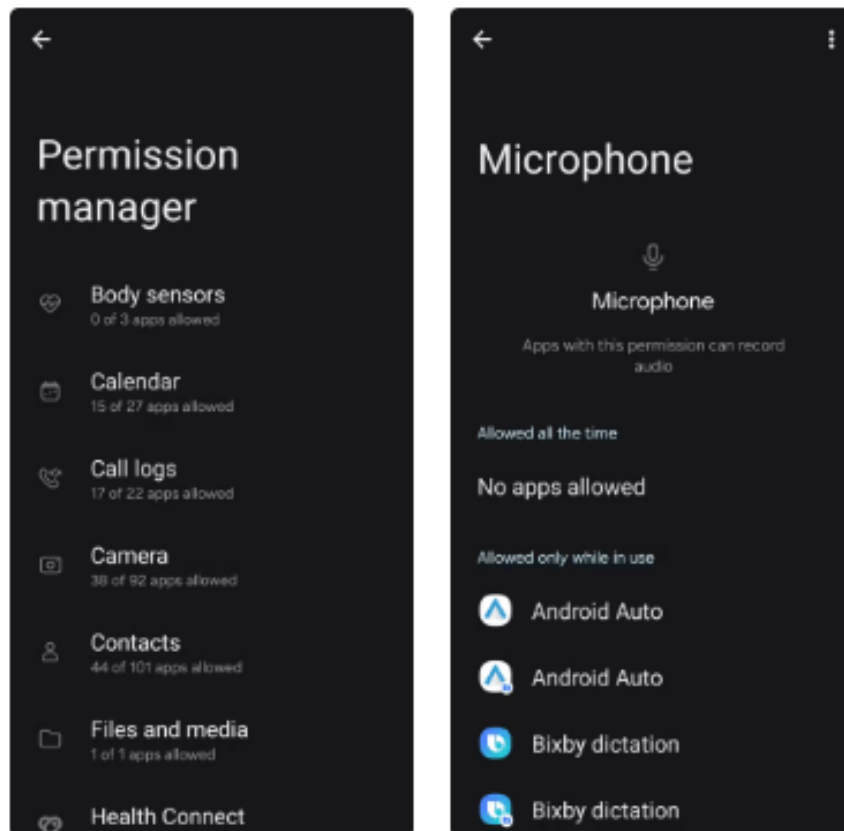
That's why it's best to avoid them as much as possible. If you need to access the Internet on the go, use mobile data, even if you have to pay for it.

However, for those times when you must use public WiFi, rely on a VPN to encrypt your connection. It adds an extra layer of security by hiding your IP address and encrypting your data, thus minimizing the risk.

2. Regularly review and manage app permissions

When setting up apps and games for the first time, people sometimes rush to grant permissions to apps without thinking too much.

With so many apps installed on your phone, it's easy to forget what permissions you've granted. So be sure to periodically review your app permissions.



For example, regularly review which apps have access to your location, camera, or microphone. Keeping a close eye on permissions will prevent unwanted apps from collecting more data than they need and help protect your privacy.

3. Turn on Find My Device

Find My Device is one of the most important features on Android as it allows you to track the location of your device on a map and call it to find it easily.

In the unfortunate event that your phone is stolen, you can even remotely lock your phone and wipe the data to ensure your personal information remains safe and secure.

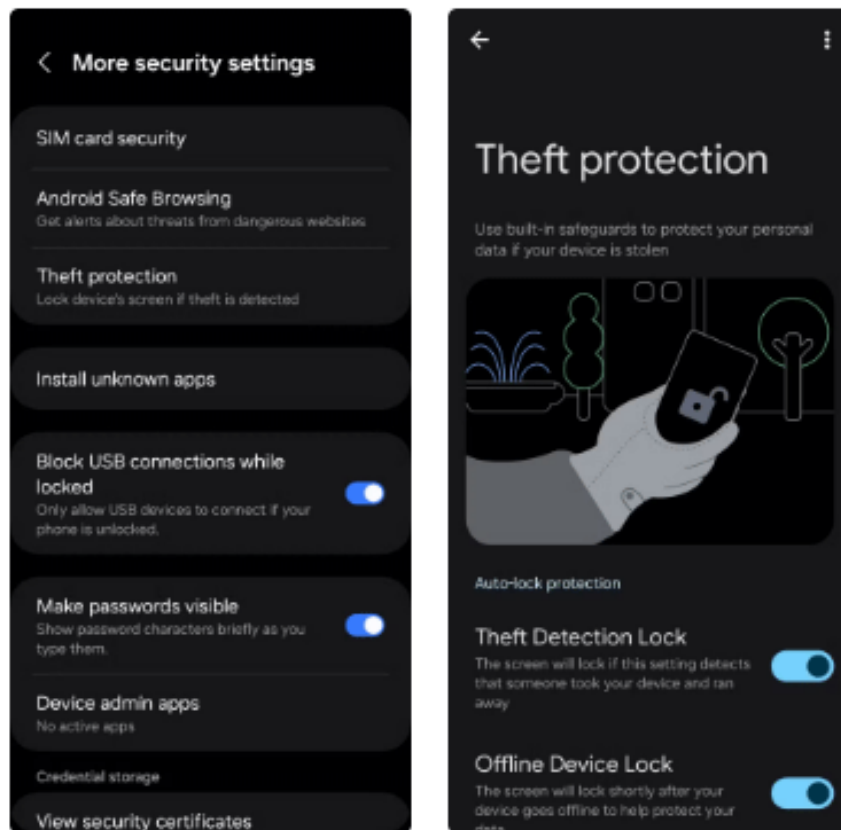
While your phone is protected by a strong screen lock passcode, Find My Device gives you peace of mind that your data is secure no matter what happens to your device.

4. Turn on Theft Detection Lock and Offline Locking

One of the biggest fears when traveling to new cities or unfamiliar neighborhoods is having your phone stolen. Luckily, Google's Theft Detection Lock helps address this concern.

When enabled, the feature uses sensors and AI to detect motion that suggests someone might be snatching your phone and running away. If it detects any such activity, it will lock the device immediately.

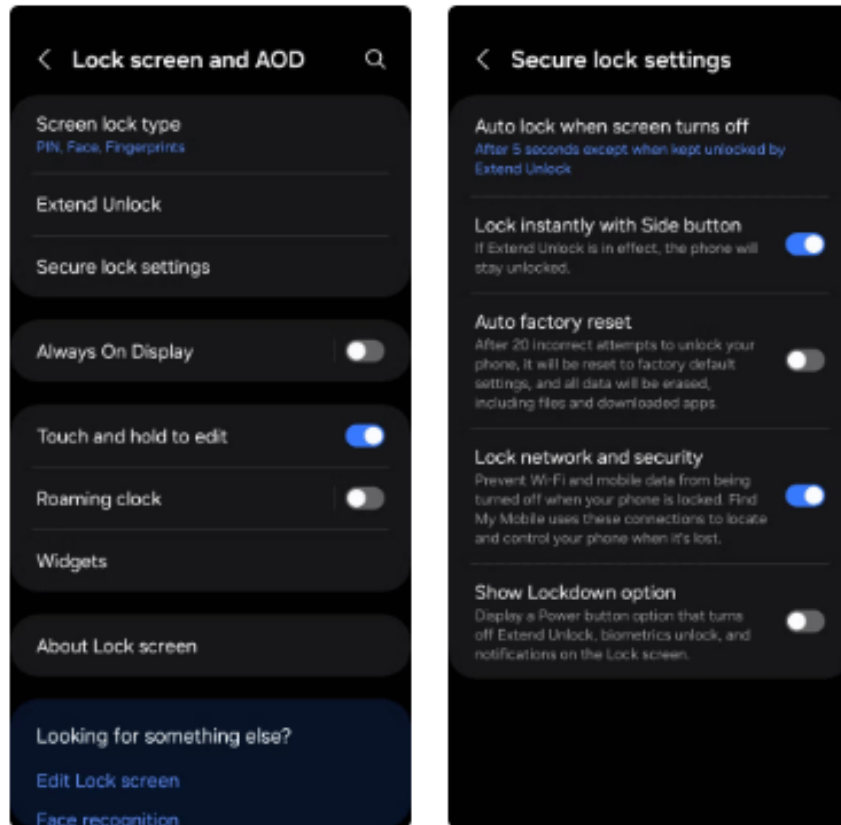
Also, turn on "Offline Locking." This feature detects signs like prolonged loss of internet connection or multiple failed attempts to unlock your phone. If it detects any of these unusual patterns, it will automatically lock your device to protect your data.



5. Disable Quick Settings access on the lock screen

Another thing you can do to keep your phone secure is to disable Quick Settings access on the lock screen. This way, you can ensure that no one can tamper with essential features, like putting your phone in airplane mode or turning off mobile data and location services, even if they get your device.

This is especially important in case you accidentally lose your phone and it falls into the wrong hands.

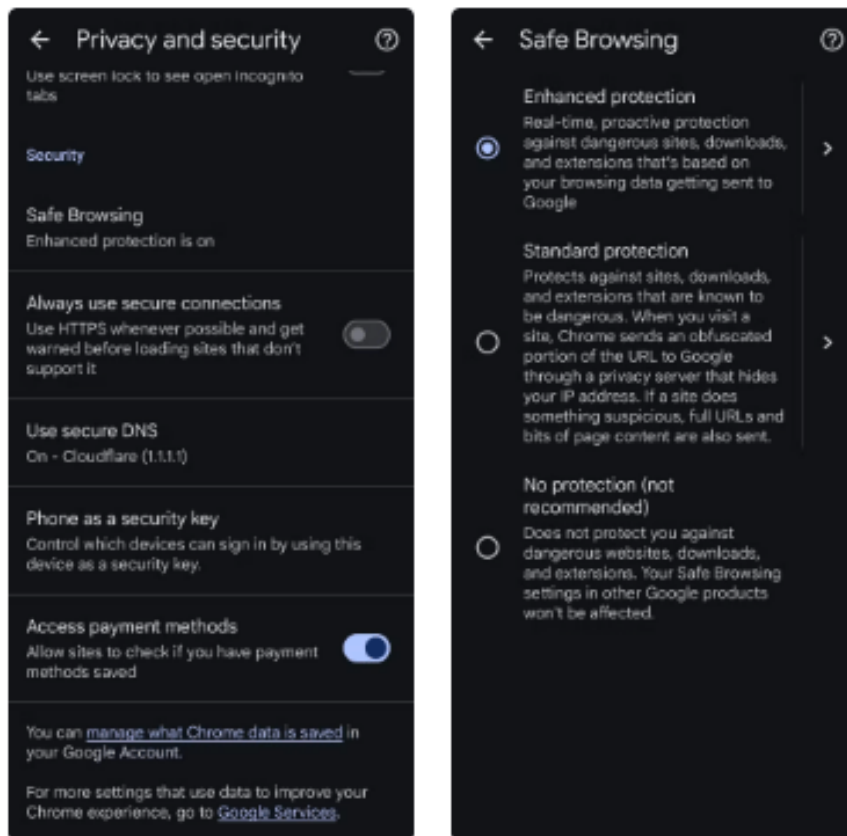


6. Always use Safe Browsing mode

In their spare time, many people often spend time reading articles and browsing the web in general on their favorite browser - Google Chrome.

To protect your Android phone from malicious websites and downloads, always turn on Safe Browsing. This feature protects you from phishing attempts and harmful websites that could compromise your device.

By default, Chrome's Safe Browsing feature is set to **Standard protection** . However, it's recommended to keep it on **Enhanced protection** for maximum protection.



7. Stay away from suspicious links and attachments

The simple habit of not clicking suspicious links and opening random attachments will save you from countless potentially harmful situations.

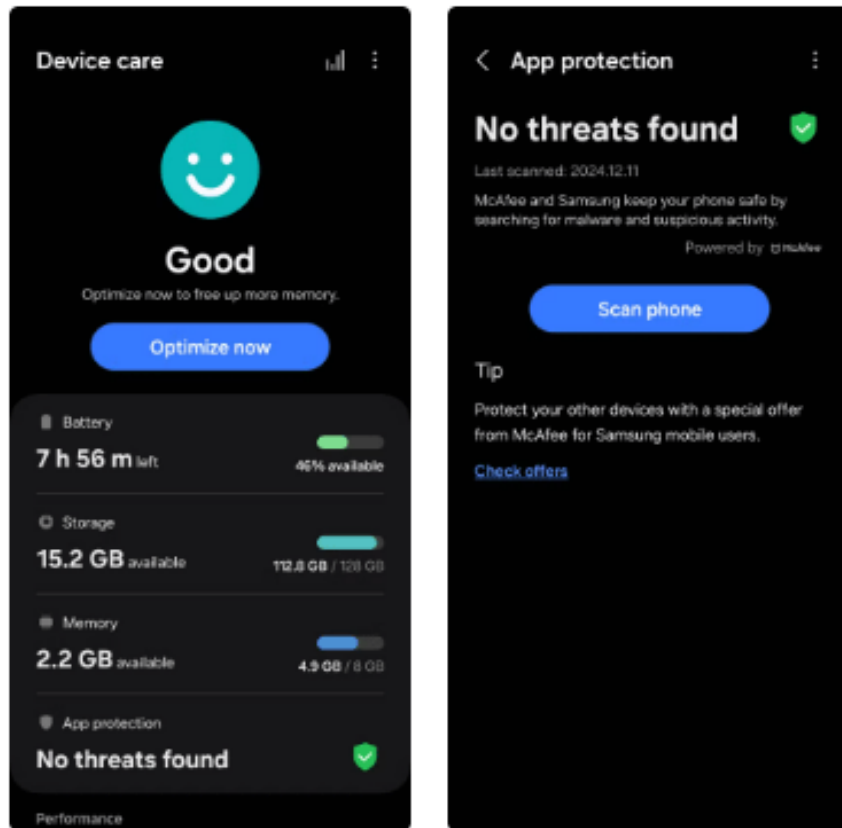
Whether it's an email, text message, or even a social media post, always be cautious before clicking on anything unfamiliar. Pay close attention to the sender's details and look for warning signs, such as misspelled words or suspicious URLs. These errors often signal phishing or fraud attempts.

As the saying goes, if something seems too good to be true, be wary. For this reason, always avoid suspicious attachments and links unless you are absolutely sure of their origin.

8. Scan your phone regularly for malware

No matter how careful you are about what you download, there's always a chance something could slip through. That's why you should regularly scan your Android phone, just like you would your PC.

These scans help detect hidden threats or apps that may not immediately give you obvious warning signs. This proactive approach not only helps you spot potential issues early, but also helps keep your phone running smoothly and securely.



9. Use secure NFC with device unlock request

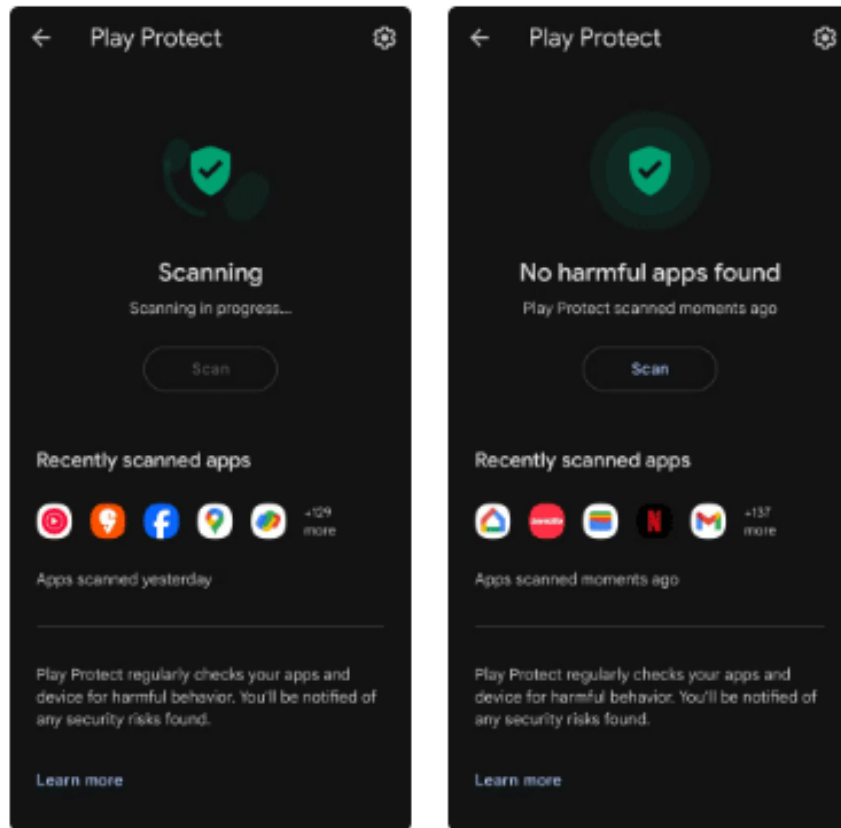
NFC has brought a lot of convenience to our daily life by allowing you to make quick payments, even without unlocking your phone. However, to be safe, always enable the **Require device unlock for NFC** option on your Android phone.

This ensures that no one can access NFC features without unlocking the device first.

10. Only download apps from the Play Store and use Google Play Protect

Unlike the iPhone, Android makes it easy to download apps. While you may be tempted to try apps from third-party sources, the risk is usually not worth it. Instead, use the Play Store, where Google carefully vets all apps for security and compliance.

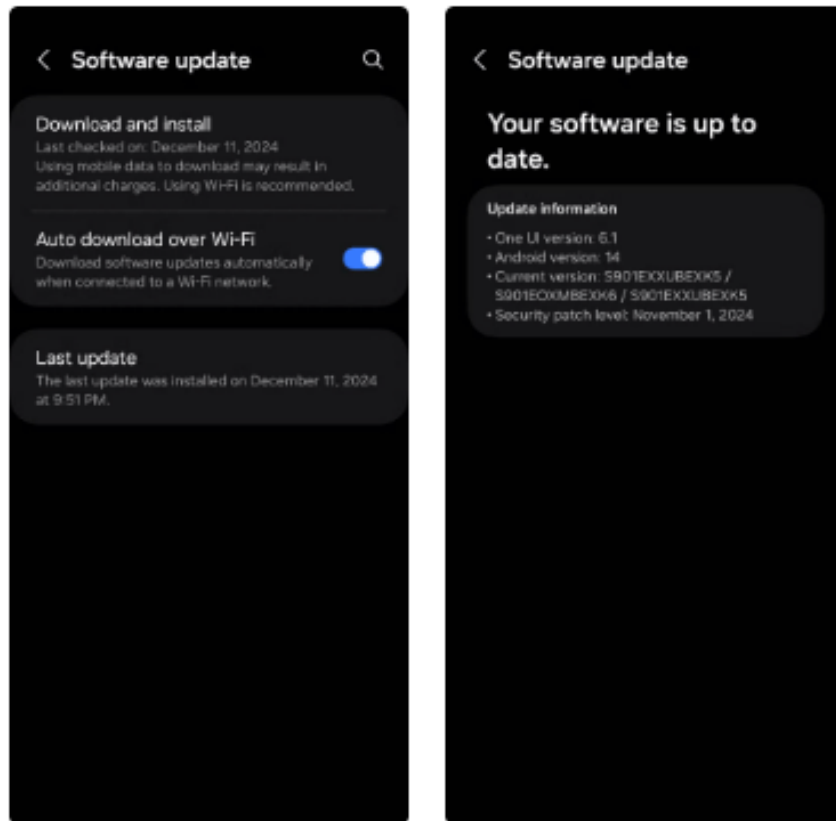
Also, keep Google Play Protect enabled on your phone. This security feature regularly scans installed apps and devices for any malicious behavior. If it detects any security risks, it will notify you immediately so you can take action.



11. Keep your device software up to date

Android updates, whether system updates or security patches, often include important fixes for vulnerabilities that can be exploited by hackers or malware.

So, whenever you get a notification about a new software update, make it a priority to install it as soon as possible.



This also applies to app updates. Turn on automatic updates for your Android apps so you can benefit from bug fixes, performance improvements, and security patches without having to think about it. This habit of keeping your apps and devices up to date goes a long way toward keeping them secure.

Overall, keeping your Android phone safe is a combination of conscious practices and taking advantage of built-in features. From enabling Safe Browsing and using trusted app sources to keeping your software up to date, every little step goes a long way toward protecting your device from potential threats.

You finished reading the article "**11 Essential Tips to Keep Your Android Phone Safe**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.