



12 SAFETY TIPS FOR SMARTPHONE SAFETY AND PRIVACY



As mobile phones become smarter, they're more like mini computers that contain lots of personal information about us. Here are 12 easy steps you can take to manage your privacy and safety when using your smartphone.

1. Put a passcode on your phone.

The easiest thing for you to do is to put a passcode on your phone. Having a passcode will make it harder for someone to pick up your phone and scroll through, access your accounts, or install something malicious. In the event that your phone gets stolen or you lose it, it'll make it a bit harder for others to get into your phone. Most phones just ask for a 4-digit passcode, but some phones will allow you to use a more complex passcode or even a thumbprint.

2. Turn off location sharing.

Most phones have a GPS and other location indicators that can pinpoint your general or exact location. With this capability, many applications may collect and share your location information. However, many smartphones give you the option of managing your location sharing under the "settings." You can pick and choose which applications may access your location or you can opt to turn off the location setting altogether. Minimising the location access can also help increase the battery life on your phone. If your phone doesn't offer specific location-sharing settings, choose carefully when downloading new apps so you're not sharing your location unknowingly.

3. Turn off Bluetooth when not using.

Bluetooth allows your phone to communicate with other devices, such as the hands-free option in your car or your printer. If accessed by someone else though, they could misuse it to access your information or intercept your calls. Turn off the Bluetooth on your phone and turn it on only when you need to connect with other devices. Many phones also allow users to set passcodes or additional security levels on their Bluetooth as well. Use all available options to increase your privacy.

4. Check your privacy and security settings.

Most smartphones have settings that will help you manage your privacy and safety. You can find these controls through the settings on your phone or through the settings of a specific app. These settings may allow you to limit an application's access to the data on your phone, including access to your location, pictures, contacts, notes, etc. You may even be able to block cookies and limit what data your mobile browser collects.

5. What online accounts are you automatically logged into?

One of the convenient features of having a smartphone is to quickly access email or social media accounts with just a tap of a finger. However, this also means that you are always connected to accounts that may contain sensitive information. Consider logging out of certain accounts if you can, so that others can't access those accounts if they are using your phone. Keep in mind that depending on the type of phone you have, you might not be able to log out of some accounts, such as email accounts, but may have to remove the entire account from your phone. In this case, make your decision based on your own privacy and safety risk. While it may be inconvenient to access the account through the browser instead, it may be safer.

12 Safety Tips for Smartphones

6. Review the apps you download.

Know the apps that are on your phone, and if you have an unfamiliar app, delete it. Apps are easy to download and easy to forget, but depending on the app, it could be accessing private information or could be a monitoring program that someone installed without your knowledge or consent.

7. Put a password on your mobile account to keep others from accessing your account.

If you're worried that someone might be contacting your mobile phone provider to obtain information about you and your account, you can ask your mobile phone company to put additional security on your account, such as a password. Only someone with this password will be allowed to make changes to your account.

8. Lock down your online phone account.

Keep in mind that even if someone doesn't have access to your phone, it might be possible for them to access your online account. Online accounts can include your mobile phone account, call logs, your email or social media accounts, your Google Play/Apple AppStore, or iCloud account. Update the passwords and security questions for those accounts to ensure someone else can't get access.

9. Use virtual phone numbers (such as Skype or Google Voice) to keep your number private.

To further maximise your privacy, consider using a virtual number, such as Skype or Google Voice or a throw away number, so you don't have to give out your actual phone number. A virtual phone number will also allow you to screen calls and make calls/send texts from the virtual number.

10. Try not to store sensitive information on your phone.

Although it may be tempting to store information such as passwords, account numbers, or personal information on your phone, the less sensitive information you have, the less likely someone else can access it. You might even want to consider deleting sensitive text messages or voicemails so they're not stored on your phone.

11. Use anti-virus and anti-spyware software on your phone.

After years of warnings, we are fairly used to ensuring we have anti-spyware, anti-malware, and anti-virus programs on our computers. This software should also be used on our smartphones as well. Search for programs in the app stores and discuss them with your wireless provider. Some phones come with built-in software that you won't want to override.

12. Take care when using safety apps.

There are many "personal safety apps" available for download that offer to increase the users' personal safety – immediately connecting them with 000 or selected trusted individuals. Several of these apps are designed and marketed specifically to survivors of violence. Before relying on any safety app in an emergency, be sure to test it out with friends and family to be sure that it works correctly for you. Your trusted friend may not receive your location with your emergency call or may not receive your call for help at all. Always know the quickest way to access 000 on your phone in case of an emergency. Many phones have a quick emergency call button that you can even dial without entering the phone's passcode.

For additional technology tip sheets and handouts, visit www.techsafety.org.au