

Mobile device safety tips:

- Regularly update the operating system and apps. New vulnerabilities are always discovered, and vendors work to quickly patch their applications and software. For the users, updating is essential for keeping mobile devices as secure as possible.
- Download apps from trusted sources. According to a 2016 Android Security Review by Google, Potentially Harmful Apps (PHA) are still the biggest threat to Android users. Certain third-party app stores have proven to be more likely carriers of malicious apps, so always download from trusted sources. Users should also do their due diligence and check reviews or comments on the app page to make sure it is legitimate.
- Know the risks of rooting. Manufacturers place security restrictions and safeguards on their devices to safeguard users. Rooting (jailbreaking) removes these limitations, leaving the system more vulnerable to malware and other threats.
- Avoid connecting to unsecured Wi-Fi. Turn off the automatic Wi-Fi connection feature on mobile devices. Public hotspots are not secure, and connecting to them can expose the device to a multitude of risks. If connecting is necessary, avoid logging into key accounts or financial services. Setting up a VPN is also a good way to secure data sent and received online.
- Be wary of unsolicited calls or messages. Attackers use a variety of methods to get users to download malware or reveal personal information. Any messages, calls, or emails from unknown senders should be scanned or well-vetted.
- Back up your files. Protect important data from ransomware threats by regularly backing up files. There are many different ways to store mobile device data—from syncing with paired PCs to cloud services or even apps. Efficient programs can automatically back up mobile device data on a set timeline, which is convenient for the user.

And here are good privacy tips that can help protect personal information on mobile devices:

- Set automatic locks on mobile devices. Ensure that the mobile device locks automatically, and has a strong passcode—a simple pattern or swipe password isn't much of a deterrent. If a device is lost or stolen, a strong password prevents anyone from quickly peeking at personal information.
- Limit the personal information given to apps and websites. When signing up for a new service or downloading a new app, registration often requires personal information. Be wary of revealing too much, and research on how secure the application or site is before logging on.
- Manage what is shared online. Make sure to use privacy settings on social media apps and sites. Some sites can broadcast location, email, phone numbers, or more to the public by default.

- Be aware of the scope of app permissions. Apps sometimes require more than the basic default permissions. Make sure the installed apps only have access to features they need.

Users should also invest in multilayered mobile security solutions that can protect devices against online threats, malicious applications, and even data loss.