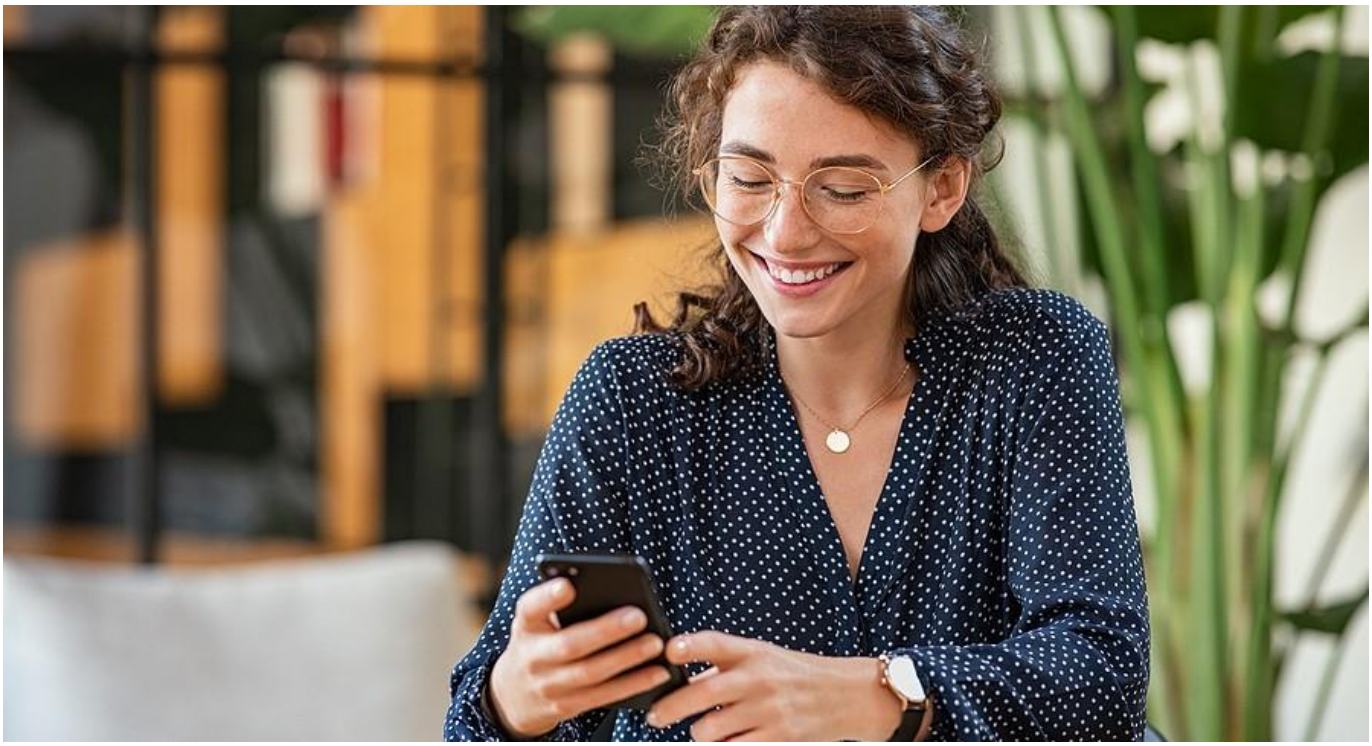
7 Best Practices to Protect Your Phone from Hackers



The phone in your pocket can prove both one of your biggest assets and one of your biggest liabilities. Think of the worlds a thief can enter through your mobile phone. They can access your finances, your precise location, your contacts, sensitive business and health documents, and much more. The following tips will help you protect your phone from hackers.

Hackers can access your phone directly or through iCloud. Or, using minimal, easily discovered, personal information, they can monitor your communications and location or even hijack your phone. By using a combination of technology and common sense, users can keep most hackers at bay.

1. First Step to Protect Your Phone from Hackers: Check Those Apps

According to experts, 70 percent of fraud on mobile devices begins with malicious apps. To secure your device from these threats, begin by choosing your apps carefully. Download only from reputable sources, such as the App Store. And before you install an app, research the publisher and check user reviews. Be sure to turn on auto updates to get security patches.

Additionally, take careful note of the permissions requested during app installation. If the app requests access to more features than reasonable, disallow the access. You can, and should, also check the permissions of apps already installed. Do this through Settings>Privacy or Permission Manager.

2. Browse Safely

Public Wi-Fi provides an ideal atmosphere for snooping on unencrypted data. VPNs offer a safe way to browse the internet away from the office or home. The VPN runs in the background while you browse, encrypting your data and hiding your activity from any lurkers.

3. Smarten Up Your Authentication

All too often, smartphone users neglect to fully implement the most common security features included with their devices. Always set a passcode for phone access. When available, also use biometric authentication, such as facial recognition or fingerprint scanning.

To further strengthen your security posture, set passwords for individual apps and enable login notifications. Use two-factor authentication for key accounts. But instead of using your primary phone or email for the second authenticator, use an authenticator app such as Microsoft Authenticator.

4. Turn Off Wi-Fi and Bluetooth When Not Using

Hackers can connect to your phone with relative ease using Wi-Fi or Bluetooth. Consequently, you should always turn off Wi-Fi and Bluetooth when not in use. Similarly, if you must use a hotspot in public, check your settings to ensure you have tightened security.

5. Increase Mobile Security Measures

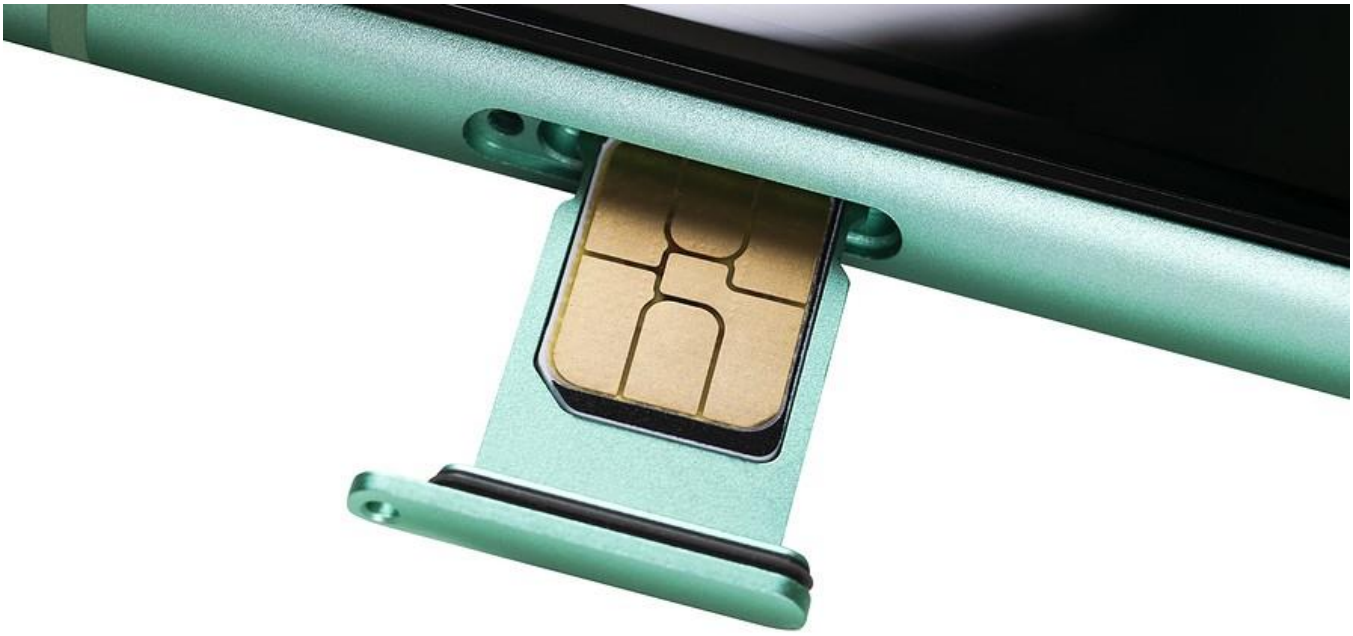
Beyond the basic security that comes with your phone, take time to implement additional mobile security. For instance, IT departments use DNS security systems to protect personal computers from

phishing, malware, or other harmful content. The same service can also protect mobile devices. And be sure to implement antivirus and anti-malware software.

Businesses with a mobile workforce also need to update their mobile security policies and procedures. A mobile device management (MDM) service such as Microsoft Intune proves helpful here. These services allow organizations to enforce password policies, define whitelists or blacklists and remotely wipe a lost or stolen device.

6. Enable Phone Tracking and Remote Locking

Most phone providers offer a Find My Device app, and that app typically includes remote lock and/or wipe functionality. If the app does not come pre-installed, be sure to install it and turn it on. This allows you to find a lost phone. It also provides you the ability to lock your phone from a distance or wipe the phone if you assume someone has stolen it, thus protecting your data.



7. Lock Your SIM Card

With a limited amount of personal information, hackers can hijack your SIM card. For instance, with just your phone number and the last four digits of your Social Security number, they can call your service provider to request a replacement SIM. This allows them to intercept text messages, including one-time passcodes (OTP) used for authentication.

Guard against this threat by adding a passcode to your SIM card. On an iPhone, for example, simply go into Settings>Cellular>SIM PIN. Turn on the SIM, adding a unique PIN.

Secure Both Your Personal Identity and Your Business

Beginning with these mobile security best practices, individuals and businesses can safeguard sensitive data from attack. The cybersecurity team at Messaging Architects stands ready to assist organizations in implementing a comprehensive security strategy. For instance, we can help you implement DNS security, set up MDM and tighten up your security policies.