

6 Recommended iOS security when using iPhone

Whether you are an individual or a representative for a business, securing data privacy on your personal devices (phones, computers ...) is a must.

Most people depend on smartphones these days, and that's why we should learn to better secure devices. Today, I will introduce to you some simple tips to help prevent hacking when using iPhone.

1. Recommended security on iOS 14

Starting with iOS 14, Apple has added a range of features related to security and privacy.

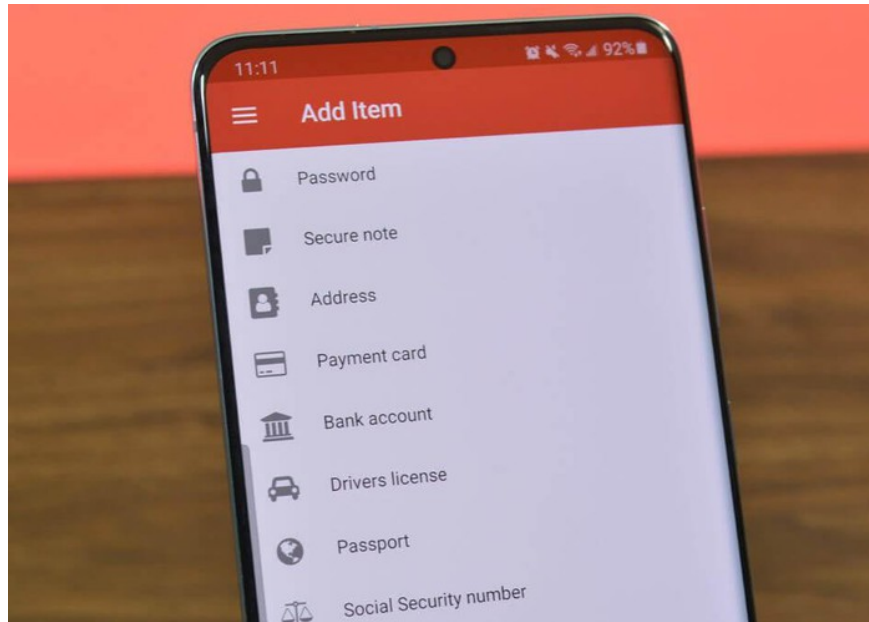
When you store your credentials on your iPhone, the device will automatically check and display a warning if it detects a leaked password.

If you want to actively check, users can access Settings (settings) - Password (password), enter the password when requested. When you're done, you'll see all your previously saved accounts (arranged alphabetically by site name).

If it detects a weak or leaked password, Apple will display a Security Recommendations message. At this point, you just need to follow the instructions to change your password.

2. Set a strong password

A strong password will usually have a minimum of 8 characters, which includes lowercase letters, uppercase letters, numbers and special characters. If you have too many accounts to manage, it's best to use specialized password managers like LastPass or 1Password.



3. Enable the Private Address feature

Starting with iOS 14, Apple has added a new option that allows users to use a private WiFi address for each connection.

To activate, go to Settings - WiFi, click on the 'i' icon and turn on the Private Address option (secure address). This way, it will be difficult for businesses and hackers to track your activity.

4. Jailbreak restrictions

Basically, jailbreak is almost similar to rooting on Android devices, allowing users to interfere more deeply with features on the system. However, the jailbreak also unintentionally opens a 'back door' for malware to easily penetrate.

5. Use a VPN

Using a VPN (Virtual Private Network also known as a virtual private network) will help encrypt all data sent / received between the iPhone and the server, limiting the theft of important data.

When using public WiFi in cafes, shopping centers . you should enable additional VPN software before making important transactions. Besides, VPN also allows users to easily access restricted websites (geographical location, IP .).

6. Turn off previews on the lock screen

A common security error that most users are making is allowing the display of the content of notifications, messages . right on the lock screen. Therefore, if important information is sent, everyone around you can completely peek at the content.

To disable previews on the lock screen, go to Settings - Notifications - Show previews - When unlocked.

You finished reading the article "**6 Recommended iOS security when using iPhone**" 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.
