

How to Prevent Cell Phone Hacking

You discover that intimate conversations, images and messages have been spread online. This is not only an invasion of other people's privacy but also affects your personal life. Although many politicians and celebrities have fallen victim to mobile phone hacking, you now have ways to protect your device. This article will provide information to help you protect yourself and your loved ones from phone-related scandals or becoming victims of privacy invasion by hackers.

Protect Yourself



Have a proactive protection mindset. That doesn't mean being paranoid, but knowing how to accept the fact that someone wants to hack your personal information for bad purposes. For example, an ex or someone who doesn't like what you say/do, friends who don't hang out anymore, etc. You can't predict how quickly relationships can deteriorate so it's always best to be careful. Secure personal information properly.

Use password. Maybe you feel safe because you never gossip. But not sure, if someone wants to hack your account, the password is what stops them. People don't just hack mobile phones because they want to know personal information, maybe they want to see more detailed and secret things in the phone, usually information of family members, friends or acquaintances. This is the information you need to carefully keep confidential besides bank account information and money transfers on messages.

Don't let anyone know your password. When you trust someone and ask for their help, such as a spouse, change your password when you're done.

Don't let anyone outside of society know your password. Set a password when in public places.

Don't program a password into your cell phone.

Don't save private data to your phone for long periods of time. If hackers break into your email account, all data will be lost (usually permanently). Even if you set a new password and log back into your account, you will not be able to access the previous information.



Back up important correspondence, store files or photos on your mobile phone to another device.
Regularly back up personal computers and tablets.



Think, don't assume. Is there a disruption that could leave your information stolen? Imagine the worst case scenario of your cell phone being hacked, then figure out what to do from there. Practice the habit of not using your phone with confidential information, delete important information you have just received after reading it or backing it up to another device. If your phone doesn't contain important information, there's nothing to worry about if it's lost or stolen. Think carefully, don't use your smartphone without thinking.

Set a more secure password



Set a password to protect your voicemail box. The way to ensure that unwitting hunters cannot delete personal voice messages on the system is to set password protection.

Follow the onscreen instructions to set a password for direct voicemail or remote reception. Many systems allow access to your mobile phone's voicemail from another device, making it even more vulnerable if you don't set a password.

Many phones have default voicemail passwords (which are often easy to guess). If you use this feature, please change your password immediately.

Too difficult, right? Lost documents on your phone? Call your distributor or service provider for help.



Choose a password that is difficult to guess. Setting a simple password is easy to remember, but if the password is related to a birthday, phone number or a series of consecutive numbers that others can guess, the risk level is very high.

Avoid setting numeric passwords related to birthdays, anniversaries or consecutive numbers. The first time, hackers can try your birthday password, relatives or pets. At the same time, many people set obvious passwords like '1,2,3,4,5', thinking that hackers will ignore this option because it's too easy. Just like phone users never think that someone hacks their phone.

Do not set a password related to middle names or pet names. Recognizable names and words will be cracked quickly if the person is close to you. Information you provide online (Facebook, LinkedIn, Twitter, forum posts, etc.) should not be included in your password.

Set complex character strings including uppercase letters, numbers, and symbols. The more complex the character string, the higher the security level. Use capital letters in the middle of the string and insert additional symbols to increase complexity. You can refer to instructions on choosing a secure password online.



Don't use one password for your entire phone account. Although using multiple passwords will cause confusion, the most effective way to protect your mobile phone (your information in general) is to set a different password for each account accessed on the phone.



Regularly update your password. Don't forget to change your password regularly to stay safe. Daily updates are not necessary, but it is a good idea to change your password from time to time.

Schedule a new password update. Whether updating weekly, monthly or quarterly, you should strictly follow it. You can write down the password in a notebook every time you update it.

When updating your password, write it down or store it in a safe location *away from* your phone, bag, wallet, or anything related to your phone. You should not leave a list of passwords in your notebook for a long time

because if it is lost or stolen, the person who picked it up or the thief will have all your information. Write down the password on each piece of paper, write 'school' or 'house repair' on the outside, in case the house is burglarized.

Other security methods



If Bluetooth is enabled, 'Discoverable' mode must be turned off. This is a way to limit other devices from detecting Bluetooth in the nearby area. This is the default setting on most new phones.



Install phone security software if the device allows it. Depending on the phone model you are using, you may or may not download it for free. For example, many phone models will lock access after a long period of use. Check to see if your phone has that function or not. If your phone is stolen, this passcode will prevent thieves from accessing personal data.

Contrary to what people think, there are actually no "viruses" on phones. However, there still exist some malicious applications that intentionally steal information on your phone. Security software will check your phone and notify you if it finds a malicious application. Only if you own a jailbroken Android device or iPhone do you really need to use this software. However, you should be careful when downloading it. Only download from reputable sellers or websites and watch out for unexpected problem warning windows.

Find an app that allows you to remotely control your phone in case it's stolen. Some applications give you full control over your phone in case it is stolen, help you track its location or delete all personal data stored on the device.

Remember to protect your security application settings with a separate password if this feature is available.

You finished reading the article "**How to Prevent Cell Phone Hacking**" 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.