5 mobile security risks you need to avoid

Here are the most used mobile attack methods of 2018. Let's find out and see these new digital wave protections.

On March 5, 2019, Kaspersky Lab published an article discussing the top malware attack methods in 2018. They said the total number of attacks was nearly double in a year. See the most used attack methods of 2018 and this new way of protecting against digital threats.

1. Risks from malware and how to prevent it
2. How many types of malware do you know and how to prevent them?
3. Summary of popular network attacks today

1. Trojan Dropper

Trojan Dropper does not harm directly, they disguise themselves as applications or programs for readers to install them and infect malware. Sometimes they download or unzip the malware, install it and then delete it to avoid suspicion. Or it can be hidden further, continue to infect the system even if the user deletes the main malware. Malware developers prefer this method because they can add a layer of protection for malware to distribute.

How to fight Trojan Dropper

The Dropper Trojan sounds complicated but it still follows the same rules as most other malware. It still needs to be downloaded on the system to infect everything. Therefore, you can still apply common malware removal methods.

1. Do not download suspicious files from unspecified websites or emails.
2. Beware of free apps, including apps from official stores.
3. Use reliable antivirus applications for phones. Refer to the article Top best antivirus application for Android phones and Top 5 antivirus software for iPhone.

2. Banking SMS Malware

When setting up two SMS authentication factors, even if the hacker knows the bank account information, it cannot be accessed because they do not have a confirmation code. That's why hackers using malware are able to read SMS messages on their phones.

When hackers log into the victim's bank account, the malware will read the code on the message and send it to their phone. So they have enough information to log in to their bank account. To accomplish this task, malware often falsifies messaging applications like WhatsApp for users to grant access and read SMS messages.

Hackers have upgraded their attacks to take advantage of Android's new accessibility service. This new feature helps people who have problems reading the screen, it can read the two-factor authentication code on SMS for users. Therefore, malware can target this service and read what it sends. When the user receives the authentication code, malware reads the code and sends the information to the malware developer.

Ways against Banking SMS Malware

Be careful with applications that require message access or accessibility services. Bank Malware needs this permission to read SMS messages and reject them to keep your account safe. Only install messaging apps in reliable, legal sources.

3. Malvertising and Adware

Unlike other money-making malware, adware does not target users' bank accounts. Instead it earns profits through interactive advertising in infected applications. Adware developers often trick advertisers into appearing outside of infected apps, making it difficult for them to find which apps are serving ads.

How to fight Malvertising and Adware

1. Be careful with applications installed and only download from official sources.
2. If you see ads appearing on your phone, see recently downloaded apps and delete them as soon as possible.
3. Use antivirus software to clean up everything.

4. Miner Trojan

The Miner Trojan does the work that people call 'cryptojacking', in which a harmful agent takes over the device to exploit virtual money at your expense.

The growing speed of smartphones is the reason malware developers choose the Miner Trojan. The stronger the phone, the more profitable it can be. Fortunately, it's easy to detect active Miner Trojans on your phone because the entire system will slow down.

How to fight Miner Trojan

If you see the phone signal being crawled, it is possible that your phone is being attacked by Miner Trojan, thus running a reliable antivirus tool to remove them.

However, the phone is not always slow due to the Miner Trojan. This may be because you run too many applications, the phone memory is low. If the antivirus application does not show signs of trojans, try removing the application.

See also: Trick to speed up Android phones after a period of use

5. Riskware

Riskware is a strange malware on this list because it is not specifically designed to be malware. This is the name given to applications that perform unsafe operations.

When a user makes an in-app purchase on Android or iOS, the official hosting service will process this payment, from which the user may via Google / Apple to track the transaction that has been performed.

Although this function is very convenient for users, it can make it difficult for developers. Novice developers sometimes use a riskware-based system, sending confirmation SMS to them when the user makes an in-app purchase.

However, this SMS system makes it possible for developers to have full control over purchases, which can refuse to provide content to shoppers even though they have paid and users cannot do anything. Google / Apple also cannot help, because the purchase is not through their system.

How to resist Riskware

1. If an application does not use the official means of payment, ignore it.
2. Always make a purchase through the official channel, requesting proof of purchase.