What is scareware? How to remove Scareware?

Scareware is a malicious computer program designed to deceive users into thinking that it is a legitimate application and requires you to buy something for nothing. Scareware's most popular camouflage is antivirus software. You will be notified that your computer has been infected.

Scareware is a malicious computer program designed to deceive users into thinking that it is a legitimate application and requires you to buy something for nothing. Scareware's most popular camouflage is antivirus software. You will be notified that your computer has been infected.

1. What is Scareware?

Scareware is a malicious computer program designed to deceive users into thinking that it is a legitimate application and requires you to buy something for nothing.

Scareware's most popular camouflage is antivirus software. You will be notified that your computer has been infected. Hackers will suggest downloading antivirus programs to remove viruses on your computer. When you try to remove the virus through this software, it will ask you to buy the full version before it can clean the system for you.

Most free and legitimate antivirus software will not require you to purchase the full version to remove the virus. If a software requires an upgrade, then you can think of it as a Scareware application.

2. How does Scareware work?

Hackers create Scareware for the purpose of clicking on the popup window to install their program. Once these phishing software has access to your device, they will notify you that your computer is infected with the virus and ask you to purchase the full version of the antivirus program before it can. Can clean the system for you.

When you buy these software and the results are:

- It looks like your device is being protected in the wrong way: although you buy software to protect your device, it doesn't seem like that, even if your device is in danger.

- Credit card information: when you enter credit card information to purchase the program, then your credit card information is also in an "unsafe" state.

3. What to do if a Scareware popup window appears?

To protect your computer from Scareware, you can apply some of the following solutions:

- Never click on the popup window: Instead of clicking **Cance** l or clicking **X** to close the popup window, right-click the window icon on the Taskbar, then select **Close** to close the window popup again without clicking anywhere on that popup window.

- Install popup blocker programs: When a network attack occurs, your system is always a victim. Therefore it is best to install popup blockers to block popup windows that hackers use to cheat.

- Be wary of "free" anti-virus software: Free antivirus software has dozens on the Internet, but among them there are malicious software and programs that users are not good at. know. If you accidentally click to download and install a malicious program, then you cannot predict what will happen. So the best way is to download and buy antivirus software from trusted software developers.

- Also most free and legitimate antivirus software will not require you to buy the full version to remove the virus. If a software requires an upgrade, then you can think of it as a Scareware application and stay away from the software.

Refer to some of the following articles:

1. Use the CMD command to remove viruses on Windows computers

1. Troll friends by creating "fake" virus on Notepad

1. No need to use an antivirus program, this is how to get rid of the virus on your computer

Wish you have moments of fun!