

If you've recently been the victim of fake antivirus software, then you know the frustration of trying to remove it from your computer. The reality is you're not alone - millions of PC users are duped into installing this rogue software. And some unwittingly download it after visiting a dodgy website.

There're many different forms of fake antivirus programs of course. Some are Trojans that spy on your PC activity and report back to their authors. And others are designed to push adverts to your computer and get you to purchase whatever they're selling.

Their main goal however is to make you part with your money and they've designed numerous ways of doing this.

The most common fake antivirus scam is it purports to run a full scan of your PC. And without fail the rogue program displays a warning message saying your PC is infected with viruses; and that the only way to remove these threats is by paying for the full version.

Contrary to what many believe, you can spot fake antivirus software and avoid being a victim again.

How to avoid fake software

1. Genuine Antivirus Software

If you've suffered fake antivirus infection before, it's likely you didn't have genuine software to begin with. Without antivirus software, then there's a strong possibility you'll get it again. And that's especially true if you continue downloading music, software and attachments online. And that also applies to visiting sites that host malware and questionable content.

To prevent Round 2 from happening, then download reputable security software that includes antivirus, antispymware, anti-spam and firewall software. If you're not sure where to begin, then we recommend you read reviews on the leading antivirus software programs.

2. Free Software

Beware of free antivirus programs! The reality is there're very few reputable security software programs that supply free antivirus software. And the one's that do usually do it as a marketing strategy to get you to purchase their full antivirus software programs. These free programs are good of course and will provide basic protection for your PC.

Fake antivirus programs on the other hand, pretend to be all free and claim to remove all threats on your PC. But the truth is they're rogue programs and their job is to spread Trojans and steal your personal details and money.

3. Dodgy Websites

Most malware threats and fake software programs are spread when people visit dangerous websites like porn and illegal sites. Unfortunately, many of these sites are listed in Google and other search engines. And despite the fight that search engines are waging against these sites, they don't seem to be abating.

There are some major steps you can take to avoid visiting these sites. The first and most important one is to have antivirus software that includes URL Advisor and anti-phishing tools. BitDefender Internet Security is one such security product; with the best features and tools to protect you from these sites and fake antivirus software programs. With this software, you'll know instantly if a site is safe or dangerous. And if you accidentally click on it, you'll get a pop-up message warning you not to proceed.

Fake antivirus software is created by cyber criminals who want to steal your money. They are sophisticated programs and you need the best security software to stop them.

[telefon dinleme](#)