Article Side

# How to spot fake virus warnings and get proper protection by Sean Burke

Article published on April 30th 2012 | Technology

Antivirus software doesnâ€™t just provide active protection from online threats and malware. It can also give computer users valuable peace of mind, so they know that if they should inadvertently happen to catch a virus or worm, theyâ€™ve already taken protective measures. Unfortunately, some suspicious companies and websites take advantage of this trust in antivirus and propagate fake virus warnings in order to frighten users into downloading bogus software, sometimes known as â€œscarewareâ€•. So how can you spot fake virus warnings, and where can you get proper protection?

Fake virus warnings can often be difficult to distinguish from real ones. Thatâ€™s because their creators often take the time to make these warnings look legitimate â€“ for instance, by designing a logo thatâ€™s similar to a well-known antivirus brand, or creating online adverts that look and feel authoritative. They may also be worded to scare you into thinking your computer is in imminent danger of catching a computer virus, unless you download their â€œsoftwareâ€• immediately. So itâ€™s no wonder so many people fall prey to these fake security scams.

Once youâ€™ve clicked on a rogue security software download, there are many ways it can affect you adversely. For example, the bogus programme might ask you to pay for the software or for updates in the future. This is an easy way of luring users into a fraudulent transaction and taking money from them. Scareware may also slow down your computer, initiate frequent pop-ups that disrupt your workflow and prevent any legitimate antivirus software you have downloaded from working properly. More sinister variations may also install malware on your computer that can steal your data or permanently corrupt your files.

With such damaging consequences, knowing how to spot a fake antivirus warning is a valuable skill that computer users should cultivate. One tip in avoiding rogue security software is never to download a programme that youâ€™ve not heard of, not researched or did not seek out yourself. If you visit a website and a pop-up window tells you that you need to download antivirus software, simply note down the name of the software and close the window. Itâ€™s advisable to exit the webpage which initiated the pop-up in the first place as well. Then simply make an internet search for the antivirus brand and see if itâ€™s legitimate.

Many users may also be tempted by the words free anti virus download. However, avoid clicking on such adverts until youâ€™ve done your research. Many legitimate internet security options are free of charge, while others usually offer their users a free trial. So, itâ€™s a myth that protecting your computer from malware is always expensive. Before downloading anything, read up on which antivirus software offers the best protection and the best value, and donâ€™t forget that you should also protect all your computing devices â€“ including your smartphone and tablet â€“ before connecting to the internet.

Article Source:
http://www.articleside.com/technology-articles/how-to-spot-fake-virus-warnings-and-get-proper-protection.htm - Article Side

Sean Burke - About Author:

Sean Burke writes for a digital marketing agency.  This article on a free antivirus download has been commissioned by a client of said agency.  This article is not designed to promote, but should be considered professional content.

Article Keywords:
Free antivirus download, internet security, fake virus warnings, scareware, rogue security software, malware, antivirus software

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!