Malware is everywhere so watch out for the fake healers

May 13 2014, by Andrew Smith

You could hire an army to protect yourself. Or just do your research. Credit: Michael Li, CC BY-NC

There is nothing worse than having a fake healer offer a cure that does absolutely nothing. History is full of tales of frauds and quacks offering a cure for all, which eventually turn out to be nothing more than a bitter tasting facsimile of the real thing.

Google has recently removed an Android fake anti-malware application called Virus Shield, fearing that it did the exact opposite. Based on the reports, this app was fortunately benign and did not appear to infect the smartphones or tablets of its users. But it could have been worse, potentially opening up their devices to many undesirable exploits.

The problem is widespread and has been for some time. Cybercrime isn't just about exploiting technology, some of the most successful scams are those that exploit your trust.

Malware is a term used to cover a wide range of attacks. A virus is one amongst many styles of attack, as it is the oldest and best understood by the majority of computer users. Others include Trojans, where an application you download has hidden code designed to reach out to a remote party; worms, which spread via email or insecure networks; and zombies, which are used by cybercriminals to exploit your computers resources.

There is a chance that you could fall for pop ups and operating system windows that look like the real deal or download a fake anti-malware application, which itself turns out to be malware.

Popular anti-malware applications like AVG and Sophos are mimicked when you visit websites. These look like applications that could help you but are fakes. The riskiest sites are those associated with illegal software downloads, pirate copies of movies and pornography. Cybercriminals trade on the notion that you are unlikely to admit to what you were doing at the time you made the mistake of clicking on the pop-up and had their download compromise your system.

Or, as is often the case, they trade on our desire for a good deal. If a deal seems too good to be true, it often is. This is no different with anti-malware applications. The price is often right, you like the promises

made and the name of the application may even sound genuine. Checking the source of an application is equally as important as checking if it is the right product.

Discovering a fake app in its store is embarrassing for Google. But the reality is that it is your responsibility to double check the credibility of anything you download. In the case of anti-malware applications, checking to see if the creators are well-known is essential. There are many credible anti-malware software houses around the world.

New start-ups are welcomed by the industry but if you are unsure, then you are best advised to do some research before installation, such as by looking at different review sites.

Cyber-criminals do understand human nature even if considerable efforts are made by developers to secure systems. The weakest link is always the human part of the chain, this is known as social engineering. For you and I, it pays to be vigilant, and we have to be cautious when being offered a good deal to secure our device.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Malware is everywhere so watch out for the fake healers (2014, May 13) retrieved 24 April 2024 from https://phys.org/news/2014-05-malware-fake-healers.html