

Beware The Anti Virus Scanner Scam!

There are many reputable anti virus software companies out there. Some are well known brands that you can see both online and off. Their software is considered among the best. Then there are those who are not so widely known that are just as good, but only available online, and in some cases, only available as freeware. Others offer a scanner, but not the cleaner in a demo mode. Then there are the total scammers. These are among the prolific of thieves online. Their scam often catches the unwary, the illiterate, the easily panicked. Some of these so called virus scanners have been nothing more than clever frauds. Still others have been clever attempts at identity theft as they scan the victim's computer for financial information or user names and password information. Then there are still others that start as a trojan that mislead the victims into "purchasing" the scammer's software to get rid of the virus. In one sense, this spells double trouble. How? The victim buys a fake software that can be more dangerous as it can lead to the victim's identity theft. It may get rid of the virus or just the message, but plants others in its place. It should also be noted that this scam is growing very fast. Scammers and would be thieves are using this type of scam more often than one would believe. One of the more recent versions of this scam (called the MonaRonaDona scam) uses a different approach. The victim's computer is infected by a trojan. This trojan can be from a website, an e-mail, or a pop up. The trojan pops up a message that notifies the user of its existence. The user may research it and find a number of blogs, message board, or stories ,etc. on this. All of these fake entries direct the use to fake anti virus software to get rid of the trojan. The software may in fact turn off the message (thereby "cleaning the victim's computer") but it may also be scanning for information or planting more of the viruses it is supposed to be cleaning. Anti virus experts have also found a link to a registry cleaner program that itself was found to be a fraud. Where this one becomes different is how the scam is being promoted. That promotion is being done on social networking and video sharing sites. The bogus blog entries, etc. are set up on these sites as a type of waning. The result is that a large number of people have fallen victim to this fraud. To avoid scams like this, here are a few tips: Purchase a good anti virus and anti spyware software. One that offers a firewall would be even more preferable. Once you install it keep it updated. A good idea is to set it to auto update. It is also a good idea to manually update your software once in a while to ensure that it is working properly. Do not click on any popup that advertises anti virus or anti spyware software. Many viruses often come from popups. A good tip here is to install a good pop up blocker. You should also avoid any sites that are questionable, especially ones that promise the world. Another reason to avoid questionable sites is that they are often filled with malicious codes. Sometimes these malicious codes are auto downloaded. A final note is that you should never download any freeware software unless you are certain it is from a reputable company. Many of these freeware programs are nothing more than viruses in disguise.

About the Author

Ryan Smith is the author of the hot, new, blog "The 10 Commandments of ID Theft Protection" Learn more at <http://www.e-profitsubmissions.com/wordpress>

Source: <http://americanahost.com>