

BEWARE OF FAKE ANTIVIRUS PROGRAMS

**Beginners' Kaffee Klatch
Presented by Bill Wilkinson
June 5, 2010**

Con men have always known that the easiest way to deceive a mark is to offer what he wants most. People are not skeptical of what they want to believe in. So it is no surprise that cyber crooks are offering false protection against dangerous viruses and other malware. That free antivirus program you were so glad to discover and install may be a virus in disguise! You may even have paid money to let this fox into your chicken coop.

A sudden injection of fear is a very useful tool for getting people to do what you want. You may be surfing the Web when suddenly a yellow "hazard" triangle pops up with an alarm: "Your computer is infected by a virus! Download this antivirus program now!" or words to that effect. A lot of people do so without an instant's hesitation. Then they're in trouble.

These rogue antivirus programs look busy running reports, and tell you they've deleted viruses. But in reality, they may have sniffed out your bank account data, user names and passwords for your credit cards, passwords to other sensitive sites, your Social Security Number, and other things used for identity theft.

Sometimes fake antivirus programs secretly install robot software, enslaving your computer to a remote mastermind who will use it while you're away from your computer to distribute spam or malware to other unsuspecting marks. If your ISP determines that malware is being distributed from your computer you may lose your Internet account.

How to Detect Fake Antivirus Programs

For starters, watch out for well-known rogue products with names such as Antivirus 2010, Win AntiSpyware, and Antivirus 360. Unfortunately, those are just the tip of the iceberg. According to *Network World*, fake antivirus programs are proliferating so fast, they could soon outpace the ability of legitimate security tools to detect them.

So aside from the names, how can you recognize fake antivirus programs before it's too late? There are several tell-tale signs:

High levels of alarm: those yellow triangles, jittering popup windows, lots of exclamation points, the word "alert" repeated six times per second -- all these things are done to induce alarm and cause you to act without thinking first.

A phony free virus scan "performed" without your permission is another tipoff. Real antivirus vendors ask if you want them to scan your computer, fake ones often tell you they have done so and found malware the instant you land on their site. A full virus scan takes many minutes, not a split second.

"Buy it right now" pitches. Every legitimate antivirus program lets you download a trial version before you buy.

No links to reviews of the product in recognized publications. Don't be fooled by "testimonials" that were written by the malware maker himself.

If you encounter a popup window alerting you that your computer is infected, **DON'T close the popup window** with a click of your mouse! That often triggers the secret downloading of a malware program onto your computer. Instead, **close your entire browser and restart it without restoring the previous tabs** that were open.

Perhaps the best way to avoid fake antivirus software is to have REAL security protection in place. And fortunately, there are some excellent Free ANTI-VIRUS and ANTI-SPYWARE tools you can download and install on your computer. These tools will not only scan your hard drive for existing malware, but they'll also block them from being downloaded in the future. (See the Beginner's Kaffee Klatch file, *Protection from the Nasties*, for recommendations that have been vetted by the professionals.) <http://scscc.com/bkk/ProtectionfromtheNasties.pdf>