

Security Warning

We've all seen it. A dialog box pops up, informing us in urgent words that a virus has been found on our hard disk, and that by clicking OK, we can run a protection program to disinfect the disk. As we freak out, the temptation to click OK is almost irresistible.

According to a recent white paper "[Report on Rogue Security Software](#)," from [legitimate] security firm Symantec, that's the doing of a new set of cyber-criminals. These companies peddle bogus security software to unsuspecting end users by scaring them into a knee-jerk response. The programs have such legitimate sounding names as SpywareGuard, AntiVirus 2009, and SpywareSecure.



To download the program, the end user submits a credit card number for payments up to \$100. The actual program may be utterly useless, or it might be harmful, allowing hackers access to your computer for data theft or malicious destruction.

The Symantec report says that the company has found some 250 separate fake programs being sold through almost 200,000 web sites.

Maybe you are too sophisticated to be fooled, but there are people in your organization (and among your family and friends) that might not be quite so wary.

Here are a few pointers in keeping them from being ripped off -- or worse:

1. Stick with legitimate, well-regarded security software from well-known and reviewed companies like Symantec, McAfee, Sophos, Trend Micro and others (check online for reviews from PC Magazine or PC World). One of these programs should be bought through legitimate channels (like a well-known online store of a major electronics/computer chain) or installed by the manufacturer.
2. Be aware what software is installed and make sure that updates are regularly downloaded. In larger companies, this will be monitored by the IT department.
3. If you see a pop-up box warning against a virus, calm down. Run or let IT run the legitimate virus software already installed if you have real reason to be worried about a virus.
4. In general, stay away from marginal websites. Be every careful when an email links to unknown websites. Google is pretty reliable about confirming the legitimacy of Web sites when you search.
5. Be careful about viewing, opening and especially running email attachments unless you are 100% sure they're legitimate and come from a known source.
6. If you are asked to download any software, stop and think. Make sure you understand exactly what you're downloading, and if you have any doubt, click Cancel.
7. Don't use a credit card to download security software interactively unless you 100% sure it is legit.