Beating Adware, The Sneakiest Software

Promoters of adware, software that shows advertising on a user's computer, use some cunning tricks to get you to install their software on your machine. Here's what to look out for.

Adware is, by definition, something reasonable people don't want on their computers. That's why malware can't just come out and ask people to install it. Often, the computer owner is completely unaware of it being installed. But not always.

When adware doesn't want to sneak in through an open window, it will try to trick you into letting it in through the front door. Don't think you could be tricked? Don't be so sure until you've checked out these most common ways people have been tricked into allowing malware to be installed on their machines.

Adware Installation Trick 1: Piggybacking

• How it works: malware may come bundled with a legitimate piece of software the user actually wants, such as a game or emoticon. The malware is merely labeled "companion software," without any indication of what it will do.

• How to fight it: be very suspicious of any software that comes bundled with other software. Don't installed software that comes bundled with other software unless you know everything that the bundled software does. After all, if the bundled program has anything to do with the program you actually want, why couldn't the software developer just get both programs' functionalities into a single piece of software? Software developers are now very sensitive to malware concerns and will provide a lengthy explanation of just why the bundled software is necessary, in the cases when they actually do need to use bundled software.

Adware Installation Trick 2: Bait and Switch

• How it works: since people are getting more and more suspicious of bundled software, the malware's developers may simply label it as valuable software, for instance, a browser plugin that supposedly accelerates web browsing (but in reality only shows ads).

• How to fight it: again, a suspicious mind is useful in avoiding malware. Ask yourself some questions:

o What will this software actually do? Malware often comes with very fuzzy claims attached. Sure, it says it will improve your browsing experience, but how? Often, this improved browsing experience just means a browsing experience with more advertising.

o If the software is so great, why is it being given away free? Most commonly, software is only given out free in two cases: if it's OpenSource (designed by a community of developers and not proprietary--OpenSource software is always clearly labeled as such); or simply a come-on for a fuller-featured version of the software. If neither case is true, there's a real chance the software is financed by adware.

Adware Installation Trick 3: Outright Lying

• How it works: malware may even be labeled as something else entirely, such as a well-known piece of software or a crucial component of the computer operating system.

• How to fight it: this is the trickiest malware of all, and requires extreme caution. You don't want to start deleting any of your program files, much less your system registry entries, unless you're absolutely sure it's malware. Plenty of overzealous parasite hunters have shot their own machines to bits this way. This is one case where you want to be using an anti-spyware program, and preferably a second anti-spyware program to provide a second opinion.

Getting Rid of Adware

Adware is so tricky that trying to uninstall it by yourself could be like a trip into the Matrix. Luckily, there are good

anti-spyware programs that tackle adware as well--after all many adware programs are also spyware since they monitor your internet usage.

True, it may feel like adding insult to injury to have to install more software to get rid of software you never meant to install in the first place. But sometimes you just have to fight fire with fire.
