

From the TechnoManor

My wife quipped, "I will not load software on my computer without first checking with Dave!"

The reason for the remark: I told her I have to buy Windows Vista to install on a client's computer. Because...

My client's computer became infected using a very sneaky form of "social engineering." Despite trying tools that claimed (on the Web) to cure this infection, they didn't. Unfortunately he discovered he didn't have the original operating system CD. Ooops.

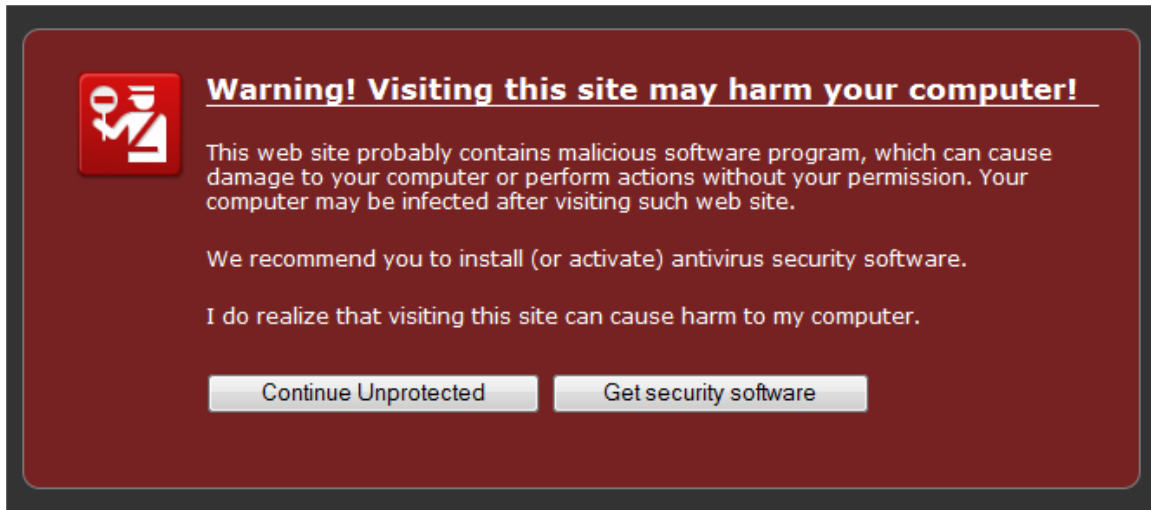
That's why I'm off to Fry's to buy a copy of Windows Vista. On Friday, I'll be erasing the hard drive, installing Windows Vista, reinstalling all the programs, and all the data.

What is *social engineering*? It's a phrase used to describe the activity, typically by phone or the Internet, to fool you into doing something you wouldn't normally do: like give out your Social Security Number, credit card number(s), or other vital information. Or to download software that proves damaging to you or your computer.

The key words are "fooled" and "normally do." The techniques used in social engineering look or sound so authentic and legitimate, that you believe no harm will come to you.

So, what was this sneaky form of social engineering that my client encountered? That's what I want to tell you about today. I really don't want you to be "bitten" by this, too.

If you're visiting a Web site and you suddenly see the following page:



Write down (on paper) the Web address you visited. Then click the red **X** in the upper right of your Web browser and close the browser.

DO NOT CLICK ANY BUTTONS OR LINKS ON THAT WEB PAGE!

This warning Web page is a trick. If you click the **Get security software** button, an infection masquerading as “Personal Antivirus” will be legitimately downloaded and installed on your computer. You have opened your door and allowed an intruder to enter.

Clicking **Continue Unprotected** is supposed to do nothing. However, I don't want to test that theory.

Ok, you may be wondering a couple of things.

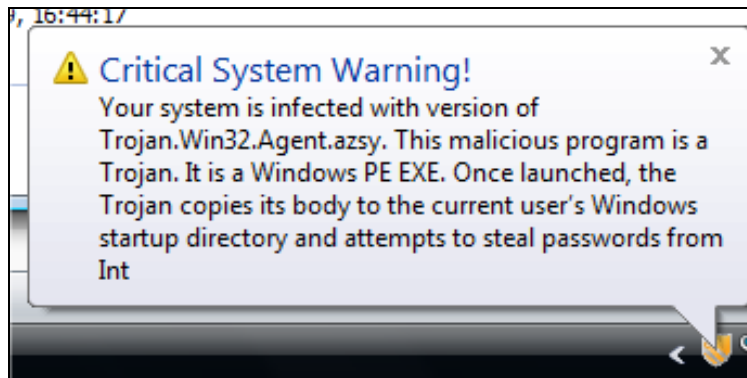
1. How where did that warning Web page come from and why are you seeing it?
2. Why did I have you write down the Web address you visited?

Answer 1. The Web site you visited has been compromised. A Web site runs on a computer, much like your own. Security software (your “aunties” from my 10/2/2008 article) and up-to-date software are just as important on computers serving Web pages. Major Web sites (like Google, eBay, Apple, Microsoft, and so on) are diligent about keeping their Web sites secure. But many other Web sites are not. They can become infected, just like your computer can.

You are seeing their infected Web site.

Answer 2. You want to remember where you encountered the warning Web page, and not go back! Or perhaps try to contact their webmaster to tell them they have a problem.

So, what happens if you have been fooled and clicked **Get security software**? Well, you will start seeing troubling pop-ups from the lower right looking like the following:



If you click on this warning balloon, or others like it, you may see what looks like a legitimate antivirus program window. Here's where the deception continues. The bogus Personal Antivirus looks remarkably like the legitimate AVG Anti-Virus window. I happen to use AVG and am pleased with it. Take a look at the following illustrations:

Bogus – Personal Antivirus



Legitimate – AVG Anti-Virus (Free)



I saw the screen on the left on my client's computer and stared at it for a few minutes. It looked so convincing. Then I realized, "wait a minute, *who* is this *Personal Antivirus*? Most security software vendors proudly display their brand and company names. I don't see that anywhere."

There was a link to view a license on the bogus Personal Antivirus. I skimmed it and saw no mention of a company. The agreement looked legitimate but said absolutely nothing.

Then I realized this was bogus software. On further inspection of the computer I discovered the following:

- The Windows Security Center had been disabled. I couldn't tell at a glance the state of the security software. Not good.
- The Windows Firewall was turned off. Uh oh, the barn door has been left open.
- System Restore was turned on. However, all of the restore points had been removed. So, there was no way to restore Windows to a date before the infection.
- Add or Remove Programs did not list a Personal Antivirus (or PAV). So, this program was not using sanctioned installation methods. That means you couldn't uninstall it by legitimate means.
- Norton Antivirus was blissfully running and reported everything was ok! This isn't surprising. Most sophisticated infections know how to side-step the major security software programs. And since Personal Antivirus was legitimately downloaded and looked benign, Norton didn't object.

If you've seen these things, sadly, your computer has been infected.

My understanding from the Web is that Personal Antivirus (or PAV) only tries to extort money from you to "buy" this software by getting a credit card. However, it can bring along other malware, or open the door to allow other malware to enter. By the time you realize what happened, it's too late.

I tried some of the suggested software that is supposed to remove this problem. I even tried my old favorite, Spybot. None of them totally eradicated the infection. I suppose if I had a few days to devote to the problem, I might have been successful.

However, the only sure thing is to erase the hard drive and reload everything. It is time-consuming, but can be completed in my lifetime.

What I've shown above is simply today's rogue software. There are others, and more will follow. Each one looks so believable. In many cases, your security software may not be aware that it's being tricked. So, what can you do?

Here's what I do:

- Be skeptical. I have a modest set of regular Web sites I visit. I'm fairly confident they're ok. However, if I suddenly see something odd (like a warning message), I bail out. For new Web sites, I'm very tentative about clicking links and I always decline ActiveX or other add-ons.
- Know my computer. I'm familiar with the names and providers of the software on my computer. I know the names of the Web browser, antivirus software, firewall, and so on that I'm using. No, you don't need to know the mechanics or settings of all. But many times it's the simple things (like misspellings or a missing brand name) that catches my eye and makes me go, "something is wrong here."
- Keep it simple. More is Less. If some Web site claims I'm unprotected, why is that happening? Succumbing to fear and downloading more security software isn't the answer. Checking my existing security software is the solution.

And finally, only my wife can turn to me and ask, "Should I download this software?" I don't want to be deluged with phone calls. Assume my answer will be, "why do you need it?!?"

Thanks To: I used material from the Web site **malwarecrawler.com**. It provided some of the images and was quite useful in giving background to the PAV problem. I plan to visit it in the future to help debunk social engineering issues.

Because of last week's storm damage at church, I've delayed ending my "From the TechnoManor" articles by one week. My final article in *The Link* will be on June 25th. Last call for questions! Send 'em to:

frenchygrey@gmail.com

Dave Gillen