Random Thoughts
from William Blinn Communications
TECHNOLOGY • MARKETING • COMMUNICATIONS
April 2010

Plague. Pestilence. Infestations.

Your computer is infected! The message claims to be from Microsoft and urges me to run the attached file to patch the system. Microsoft doesn't send messages such as this, but it's easy to forge a return address on an e-mail message. As a result, some people will run the attached file and – sure enough – now the computer will be infected even if it wasn't before.

Other similar scare tactics guide you to a website that infects your computer. Still others entice the victim to download what appears to be a legitimate application, a video file, or something else that's attractive.

No matter how careful you are, it's easy to make a mistake that results in an infection. Although it's best to avoid these infestations, it's important to know what you can do if something bad happens. Eliminating the problem might be as easy as running ComboFix or Malwarebytes' Anti-Malware, or you may find that you need to format the hard drive and reinstall everything. That's just one reason why it's so much better to avoid this stuff rather than to recover from it.

On May 5, 2000, I was one of the first victims of the first widespread computer worm.

What if ...?

The Red Cross teaches emergency workers that the first part of solving a problem is to avoid making the problem worse. Act without thinking and you may be injured or killed, the trainers say. With computers, a good first step, if you think there's a problem, is to disconnect your computer from the LAN. Even if you're not on a LAN, pull the plug on the Intenet until you can examine the situation. If the malware is sending your personal or financial information to someone, you want that to stop. Now.

On May 5, 2000, I was one of the first victims of the first widespread computer worm. Recognizing that something bad was happening, I pulled the plug on the network connection and immediately called my supervisor. Because of that and even though this worm attempted to spread via the network, the infection was limited to my computer.

Don't even think of using your computer to search the Internet looking for a cure. Any search for malware removal tools is likely to produce several hits for organizations that will actually install malware on your computer. Instead, try a trusted site such as Bleeping Computer, where you'll find tutorials for removing specific threats. A visit to Bleeping Computer is a good second step if the quick-and-easy solution I'll describe next doesn't work.

The Quick-and-Easy Solution

Two applications can be combined to remove many threats: ComboFix and Malwarebytes' Anti-Malware.

ComboFix is so good that fraudsters have set up sites that claim to offer the application for download. These will simply make the matter worse. The one and only place to obtain ComboFix is from the Bleeping Computer site: www.bleepingcomputer.com/combofix/.

There is no installation; you just download ComboFix and run it. But understand that this is powerful medicine. It could render your computer non-functional. That said, it's also your best chance to return the computer to normal operation without having to format the drive.

Download ComboFix to your computer's desktop. Also download Malwarebytes Anti-Malware (www.malwarebytes.org), but don't try to install it. Then disconnect the computer from the Internet and either turn off or uninstall any antivirus application.

Bleeping Computer has detailed instructions on how to use ComboFix. Read them. Print them. And follow them step by step. Take care not to interrupt ComboFix. Bleeping Computer points this out several times and it is critically important.

When ComboFix is finished, install Malwarebytes' Anti-Malware. Choose the full scan. Because your computer isn't connected to the Internet, you won't have the latest definition files. That's OK. Malwarebytes Anti-Malware will explain that that there are two versions of the program, one paid and one free. The free version omits real-time monitoring. This is OK; you won't need it now. Depending on the speed of your computer, the size of the disk drives, and how many applications are on the computer, the scan may take just a few minutes or it might continue for several hours.

Random Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.785.9359. On the Web at www.Blinn.com.

Law of Cat Acceleration: A cat will accelerate at a constant rate until he gets good and ready to stop.

What you want to see, when the process ends, is a screen that shows no infections, but you may see one or more items in a list of problem files. The Anti-Malware application can remove these, but stop for a moment and read the list. Automated processes aren't always correct and you want to avoid removing something that you need.

Once you've decided which files to remove, simply instruct the application to remove the ones you've selected. You'll probably be instructed to restart the computer at the end of the process. When the computer is running again, it's important to run the scan again to confirm that the problems have been resolved.

Is Everything OK Now?

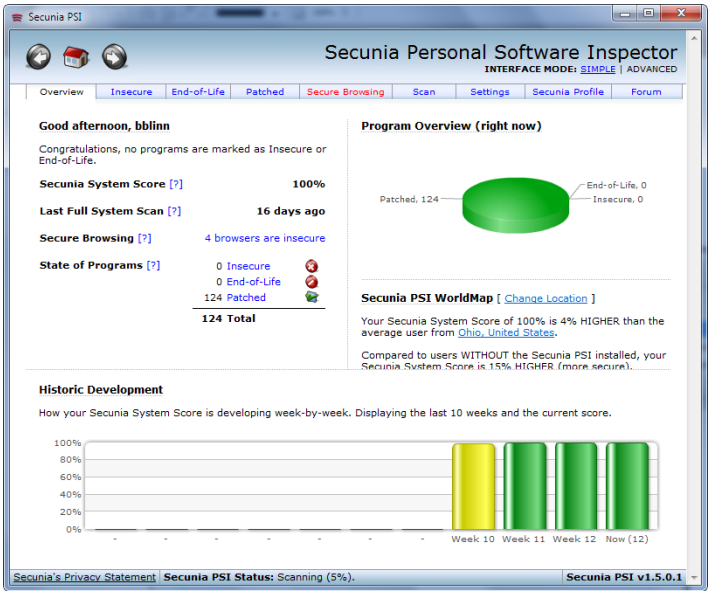
If the computer is now clean, you should reinstall your antivirus program and then connect to the Internet to obtain the latest antivirus updates.

If not, you have several options: You could format the drive and reinstall everything, or you could visit Bleeping Computer and discuss the problem on one of the forums, or you could take your computer to a technician for repair.

If all of this sounds like a lot of work and a lot of bother, it is. That's why it's so very important to avoid infections in the first place. I've found Symantec's Norton Internet Security 2010 to be helpful in this regard.

Keep Applications Up To Date

All software has bugs. Some are benign, but others open serious security holes. When publishers find a security problem, they usually issue a patch to fix it. Microsoft does a good job of patching its own applications via the Windows Update service and other publishers such as Adobe routinely have their applications check for updates. But what about your other programs?



Secunia, a Danish company that was founded in 2002, offers fee-based security applications for companies, but it also offers a Personal Software Inspector. Unlike Microsoft's Baseline Security Analyzer, Secunia's Personal Software Inspector examines software from all publishers and advises you when updates are avaialable.

When Secunia PSI finds a program with known security flaws, it will offer a link directly from the scanner to the publisher's website so that you can download and install the patch. It doesn't get much easier than this.

I have old applications (some go back to DOS days) stored on the computer. These applications have security flaws, but I'm keeping them only for historical reference so there's no danger. Secunia PSI allows users to specify directories that will not be examined for just this reason.

When you run Secunia PSI, you'll probably find that every browser on your computer has security problems and that some of these have no known solution. This is distressing, but at least it levels the playing field a bit and you will know about some of the potential threats. ß

Microsoft is 35

In November of 1980, a 5-year-old company named Micro-soft agreed to license a personal-computer operating system that it hadn't written and didn't own to IBM. IBM hadn't announced its personal computer yet; that would come in 1981.

Bill Gates and company worked with a small software company in Seattle, offering them what seemed like a large cash price for a rewrite of an operating system patterned after Digital Research's CP/M operating system. What Microsoft neglected to mention to Seattle Computer was that it intended to license the software to IBM.

That's the operating system that became MS-DOS (when Microsoft sold it) and PC-DOS (when IBM sold it).

Along the way, the company changed its name to MicroSoft and then to Microsoft. Bill Gates became for a while the richest person in the world. The company spawned many millionaires.

Where will Microsoft be in another 35 years? Given the challenges it faces, Microsoft might become another DEC. Another Digital Research. Another Ashton-Tate. Or it could be another IBM.

Only time will tell. ß