



A Beginners Guide to Safer Computing

Part 2

Written by Oliver Koriath

In part one of this series I explained how you can use the built in tools provided by Windows XP to be more secure. If you haven't read it yet I suggest you start there first, and then come back to this article. Unfortunately in this day and age, just following those steps in part 1 is still not enough to keep out the bad guys. The strategy we will be employing here is called 'defense in depth', meaning that we will secure the computer in many layers of protection thus making it harder for the bad guys to get in.

Additional Software

The first thing I am going to tell you before we talk about anything else is, forget Internet Explorer 6. Yes, I want you stop using it. Internet Explorer in its current form, version 6 service pack 1, is probably the worst offender when it comes to security holes in Microsoft products. They have just released version 7 and it has some significant improvements, but for now my money is on another browser. I'll get into why you should do this a little bit later on.

Alternative Web Browser Software

There are a several different kinds of browsers out there and the best part is they are all free. It's just a matter of preference really, so go ahead and download some, or all, and try them out.

Mozilla Firefox

My personal preference is to use the open source browser Firefox. You can get it from here:

<http://www.getfirefox.com>

On the site there is a link to download the program, click on that and Internet Explorer will prompt asking what to do with the file, run or save. Choose save and select the location where you want to save the install program, anywhere is fine as long as you know where to find it again! The default is on your desktop.

Once downloaded, double click the setup file just downloaded and follow the instructions, it's very straight forward. Once finished you should see a new icon on the desktop and start menu. Finished! Happy browsing.

What does open source mean? Open source basically means that this particular software is developed by a community of coders who volunteer their talents towards improving the product. There is no company involved except for the non profit Mozilla Foundation.

Anyone is welcome to contribute code or provide assistance with some other aspect of the project. Microsoft, just as an example, is a closed source software producer. People cannot just take Microsoft programs and modify them unless they actually work for the firm or are licensed to do so. Even then Microsoft still would have final say for what can go into the product.

Now back to why I prefer Firefox. Its robust, loads pages faster, you can add all kinds of extensions to it, it has something called tabbed browsing (which will be in IE 7 now as well), and it is inherently more secure than its cousin from Redmond Washington. If a bug or a problem is found, the programmer community quickly puts out an updated browser to plug the holes. In fact it will periodically check for new versions and download and install the updates for you.

Now because Firefox is open source, there are several offshoot specialty browsers that are currently in various stages of development. Since they are not ready for prime time yet, I would avoid using those for now (of course one can download them and check them out if you wish). Here is one:

Flock

Billed as a social browser because it can integrate with several social networking sites such as Flickr.com and Technorati.com. Pretty neat if you're into that sort of thing like blogs and myspace.com.

<http://www.flock.com>

Netscape

Remember them? The granddaddy of the browser is still around. Yes, kind of ironic isn't it. The original web browser that everyone thought was dead is still alive, and now it's based off Firefox. Funny considering that Firefox is based on Netscape, and now Netscape is built from Firefox. Confusing I know.

<http://browser.netscape.com/ns8/>

Opera

Not related to Firefox in any way, bringing up the rear in terms of market penetration for the Windows platform is the proprietary browser Opera 9. I've briefly played with this browser and was impressed with some features, but I just got so used to Firefox I went back. They used to charge money for this browser, but in the last year or so came to their

senses and made it free of charge. You may have heard about this product because they are in heavy use on the mobile phone market segment.

<http://www.opera.com>

Antivirus Software

For your next, and most likely final, line of defense in securing your computer is the use of an antivirus program. In this day and age, it would be foolish to run a computer on the Internet, dial up or broadband, without some kind of protection from the myriad worms, viruses and other nasties that float around on the net. It is not a question of if, but when you will be infected, or an attempt at least to infect will happen.

Viruses and worms

I'll try and not get too technical here but these programs can spread either by email, embedding into macro files, copying from a floppy or other storage device, and even spreading by actively scanning for vulnerable machines on a network. Tests have been done in the past by placing an unprotected machine on the net and within 10 minutes it became infected. Yes it can happen that fast.

What does Antivirus do?

According to Wikipedia.org (a great resource), Antivirus software “consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software ([link](#)).” In a nutshell, this is the hallway monitor on your computer. It constantly scans files in the background looking for any naughty things that may try to get on your machine. Be aware these programs, as of yet, typically do not detect adware and spyware infections but the line is quickly blurring in this regard. I will go over that more in depth in a bit. But the most important thing to remember about this software is that it is only as good as the latest definition files, and new viruses are discovered in the wild almost daily. It is important that this software remains up to date. You should consult your respective software manual or vendor online support page on how to do this.

I am not going to give any specific vendor recommendations, there are many options. It is up to you to decide which one is best for you. You can either buy it off the shelf or online via a download if you have high speed internet. One thing I will say is that your mileage may vary depending on which vendor you go with, so it pays to do some product research before investing a modest amount of money on a program suite. Many vendors provide free trial versions of their products so you can see how it will operate on your computer. I would encourage you to go download these to see how they work on your system.

Adware and Spyware

The Scourge of the Internet

Viruses and worms are a fairly nasty bunch, but in the last six years or so another phenomenon has taken the limelight away from these baddies. Meet adware and spyware, the ugly cousins in the malicious software family, not as potentially destructive to your computer, but they sure are annoying and hazardous in other ways. Typically these two are lumped together but they behave differently.

Adware

Adware is simply a program that will latch itself onto your computer, without you giving it permission (or in some cases giving it without knowingly doing so) for the purpose of throwing up advertising pop ups while either surfing the net or installing shareware programs downloaded from web sites. You may see new icons on your desktop one day, or an odd new tool bar in Internet Explorer, or a constant barrage of ads in pop up windows, these are signs your computer has been infected. Most annoying, but a fairly easy fix as long as it is caught quickly and removed which I will show you how to do in a moment.

Spyware

The other cousin, spyware (also known as malware), is a variant of the first one but with more nefarious purposes. Its method of infection is the same as with adware, but these little buggers are what give computer users the most grief. They tend to be harder to get rid of, and they love to reinstall themselves. Some become so embedded in the Windows operating system that the computer becomes too unstable, necessitating a complete reinstall. This software is designed typically to track your surfing habits, or worse tries to capture some of your personal data (passwords, credit cards, etc.) without your knowledge, and then transmit this information back to the creator.

How do these guys get on your computer in the first place? Easy, if you visit web sites of a dubious reputation, like a site that offers free online games for example, these programs simply install themselves as soon as you pull up the page. Adware and spyware exploit the relative insecurity of Internet Explorer 6, which allows these components in by default. Hence the reason to not use this browser as I outlined earlier in this article.

Removing This Junk

Thankfully, there are several utilities out there to help in this war for control of your computer, and best of all they are free. These programs are similar in function to antivirus software, they are most effective when using the latest definition files. Basically one downloads the program and installs it, runs the definition update and then scans the computer for these bugs. When it finds something it will flag it, and then later allow you to remove it when it is done scanning. A very simple process and I have found it be quite successful in cleaning many infested computers.

Please be aware there are plenty of imitators out there, I have been using only two programs with great success in the past few years. Namely;

Ad-Ware Personal

<http://www.lavasoftusa.com/software/adaware/>

and SpyBot Search and Destroy

<http://www.safer-networking.org/en/download/>

Ad-aware has a commercial version now, but I have found the free version still works just as well and is really simple to use. Spybot could have a slightly steeper learning curve, but the wizards will guide you through the process which should be straightforward enough. Installing both of these at the same time may seem like overkill, but using them together will catch the most bugs.

In Summary

So hopefully the preceding advice on how to secure your computer is clear, and that you have begun to undertake some of these steps to protect yourself from the bad guys. Download yourself a new browser, install an anti virus package, plus adware detection software and get in the habit of scanning your computer regularly. Doing this in conjunction with following the steps in Part 1 should lead to a happier and safer computing experience, hopefully with a minimum amount of problems further down the road. Have a safe journey!

Oliver Koriath

okoriath@kortechservices.com