

A Prescription for Prevention

How to Protect Your Home Computer from Malware

Charles Bennett - MBA, Principal Consultant, Triella

A lot has changed over the past year in the area of home computing. Most homes have a computer in order to allow the kids and family access to the Internet, do online banking and access the other resources such as word processing and spreadsheets. But, more importantly, many use their home computer for accessing documents and email located at their place of business.

Yet the threat to home users has never been so great and yet, at the same time, so hidden. In fact, if you use high speed Internet access, the probability that your computer is currently infected by malware is almost 100%. Sure, you use antivirus software and possibly antispyware software - but there is a lot more than that required to keep your computer out of harms way.

Malware Threatens Your Computing Experience

What is malware? It is malicious software, software that generally does something inappropriate on your computer without your knowledge. Spyware, a form of malware, has now taken over as the leading cause of computer infections. It is far less likely that your computer will be infected by a virus than it is that it will be infected by spyware. Spyware is software that resides on your computer waiting for a hacker to activate it to participate in an attack or to convey confidential information. It is also software that can track and report upon your on line activity, keystrokes and actions over the internet to the spyware purveyor. Adware, a kind of spyware, can also track and report upon your on line activity to customize a wide range of pop up ads that will appear when you browse the Internet.

Today, many infections come directly from the web sites that are visited by your computer - drive by infections if you will. Selecting a link provided by a Google search can launch a plethora of pop up windows, each with the potential to infect your system. Internet Explorer can now be compromised through browser hijackers, another form of malware, that do everything from resetting the home page to monitoring search requests that you enter and redirecting the browser to a site of their choosing. Hijackers can also prevent access to the very sites that could help you in the event of a problem.

Prepare for the Worst

There are many steps required to clean and protect your computer from infection. A heavily infected computer may need to be reformatted and built from scratch as there are some infections, such as rootkits, that even the best commercially available programs cannot repair.

Collect all of your original software CD's and installation disks and keep them in one place. If you have received upgrades, put them in the same place also. If you have downloaded upgrades to your software, burn those upgrades onto a CD and keep them with your original software.

Document all of your passwords and access points for email, logging on, Quicken, specific web sites - everything that you use that requires a password. Store that documentation with your original CD's.

Finally, back up your data. The quickest way to do this is to burn it to one or more CD ROMs. Back up only the data, you do not need to backup your programs since they can be installed from the original disks. If you are still not convinced, know that backing up and restoring your programs will not cause them to work properly because of the many changes that are completed with an installation that are not done with a restoration.

In the event that your computer must be rebuilt, you will have the tools needed to allow it to be restored effectively.

Take Steps to See if Your Computer is Infected

Many of the steps listed here are both diagnostic as well as preventative. Due to space constraints, step by step instructions are not provided here. However, using a combination of Google searches and Start>Help you should be able to perform the instructions yourself. You may wish to engage the services of someone more technical than yourself to help with these processes.

Run Microsoft's Malicious Software Removal Tool

This tool will remove most of the known and dangerous threats from your computer system. You can find it at: <http://www.microsoft.com/security/malwareremove/default.msp>. Just run the software right from your Web browser.

Install an Anti Virus Program

If you are using a free antivirus program, get rid of it. That is not to say that there may not be a free product worthy of protecting your system out there but as the old adage goes, 'you get what you pay for'. If you are using an antivirus program produced by a company whose business involves more than just virus, spyware and malware protection, get rid of it. Software conglomerates have good products, but you need a great product to protect your computer today.

Our recommendation is to use Trend Micro's PC Cillin Internet Security 2005. This software provides virus, spam and limited spyware protection for your computer. You can download and pay for this software directly from www.trend.com under the Home & Home Office tab. For now, download the trial version until you can determine that your computer is free of spyware.

Be sure to uninstall any antivirus software that you have running before installing Trend. Only one antivirus software program can operate on your computer at a time.

Install an Anti Spyware Program

Unlike virus programs, with anti spyware, more is better. Even though PC Cillin provides some spyware protection, it is not sufficient to deal with the scale of the threat. We recommend using the products in addition to PC Cillin:

Microsoft Antispyware

Adaware Personal SE

Spybot Search and Destroy

Each product is free and scans for and removes spyware from your computer. In addition, both Microsoft Antispyware and Spybot provide future protection (or immunization) against future infections.

For optimal results, purchase Trends Antispyware or Webroots Spysweeper, available at <http://www.webroot.com/>.

The Registry

Even after doing everything stated above, you may find that certain pieces of malware continue to infect your system. If this is the case, call an expert who can review and remove entries in the registry that malware uses to reinfect your system.

The Hosts File

The HOSTS file can control access to certain web sites and is used by malware to cause your computer to be directed to spoofed sites or sites containing additional malware. Spoofed sites look exactly like the real sites but with one major difference - they are under the control of hackers.

It is best for you to have a qualified person look at the Hosts file on your computer in the event that there are entries required for communicating with your business.

Maintain the Integrity of Your Computer

The following steps help to reduce the likelihood that your system will be infected by protecting the perimeter of your network.

Purchase a Hardware Based Firewall

Firewalls are embedded into most routers on the market today. The benefit of a hardware based firewall is that it cannot be defeated through software. It forms the first line of defence for your systems.

Routers come in wired and wireless versions and can usually be obtained for less than \$100.00. They allow you to share one Internet connection with several computers in your home. Their embedded firewalls protect each connected computer. No home should be without one.

Routers from Linksys and NetGear are recommended. You can purchase these at any local computer store.

Use Wireless Encryption

If you purchase a wireless router but do not have any wireless devices at home, then turn off the wireless functionality on the router. In addition, you should change the default IP address and the default password for the router. These steps simply make your computer a harder target than someone who does not employ the same protection methods.

If you do purchase a wireless router, set up wireless encryption such that a passphrase (password) is required to connect to your wireless network. This will prevent the person next door or at the street corner from hitching a free ride on your network.

Keep Your Windows Up-to-date

If you are not using Windows XP, consider upgrading to it. This software is more secure than previous operating systems. At the same time, it is also the target of most current malware attempts. Regardless of your operating system, you should keep it current with Windows Updates. You can access Windows Updates using Start>All Programs>Windows Update.

In particular, for Windows XP users, be sure to load SP2 and to turn on automatic updates so that your computer stays protected. The majority of malware exploits known vulnerabilities in Windows for which there are fixes.

Enhance Your Browser

Most users use Internet Explorer. As a result, it is the most popular target for malware. Some fine tuning (done under Tools>Options) will enhance your browsing experience:

1. Reduce the size of your cached internet files to about 100MB.
2. Delete all offline content.
3. Delete all cookies. (Note: this will result in some web sites not remembering who you are when you return to them.)
4. Turn off the option to remember passwords for Web sites. (This information can be farmed by spyware and used for identity theft.)

In addition, we recommend downloading an alternate browser - in this case Mozilla's Firefox. You can obtain this free browser from www.firefox.com. While Firefox is not free of the potential vulnerabilities, it is less likely to be compromised by the vulnerabilities that can render Internet Explorer inoperable. Should you find your browser hijacked, you can use Firefox to download the tools needed to correct the problem.

In addition, when visiting questionable sites, such as on line gaming, pornography or sites suggested by a Google search use the Firefox browser. When visiting known sites and secure sites such as online banking, continue to use Internet Explorer.

Use Outlook, not Outlook Express

If you have Outlook on your computer, use it instead of Outlook Express. Outlook will automatically convert all of your data from Outlook Express when you first run it. Outlook provides many feature enhancements over Outlook Express but more importantly, since it has a corporate rather than personal focus, is more secure and is less susceptible to corrupting your data.

Be Cautious in the Future

Once your system is cleaned, you should change your computing habits to be more alert to potential attacks. You are the best defence against malware. Here are some extra things to keep in mind:

1. When installing free software from the Internet, read the license agreements. If they make mention of 3rd party software, cancel the installation and do some research to see if the package is known to contain spyware.
2. If a pop-up window appears when browsing a web site, ignore any buttons or options presented, just hit Alt+F4 which is the Windows command to close the pop-up window. Buttons can say anything and can be programmed to do anything so don't trust them in a pop-up window.
3. Install the Google Toolbar. You can find it at <http://toolbar.google.com>. The toolbar includes a pop-up blocker and many productivity enhancing features that make Internet use easier.

Avoid Instant Messaging (IM) Programs

If possible, avoid the use of these programs as they can be transport mechanisms for malware. Recent malware software has been known to target IM programs such as MSN Messenger, Yahoo Messenger and AOL Messenger.

Avoid Links to Greeting Card Sites

Malware can also take advantage of the way in which people behave. You have likely received a greeting card from someone in the past with a link to a Web

site where you can pick up the card. The links are usually quite complex and it would be difficult for anyone to determine beforehand whether you were being directed to a genuine site or to a spoofed site containing malware that could infect your system. It is best to check with the sender to see if they sent you a card before opening it. Remember, email addresses can be forged too so send them a separate message rather than replying to or forwarding the one that you received.

Implement a Daily Backup System

Be sure to backup your data daily. You can back up to CD if you have a CD Burner or use one of the many Internet based backup systems.

Turn on System Restore

If you are using Windows XP, be certain that the System Restore feature is turned on. Should your system be infected, you can restore your system to a previous point in time thereby thwarting the malware.

Conclusion

Your computer is under constant attack while it is connected to the Internet. Taking the time to introduce preventative measures will save you down time and the cost of hiring a technician to fix problems beyond your technical ability. In short, an ounce of prevention is worth a pound of cure! Don't wait until you realize you are infected to take action. By then it is too late.

Charles Bennett is the President of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. He can be reached at cbennett@triella.com or 416.269.4368. For additional articles, go to www.triella.com.

© 2005, by Triella. All rights reserved. Reproduction without permission is prohibited.