

Guide to High-Speed Internet Use for the Inexperienced

Since high-speed internet was made available in LeFlore county in the last couple of years, my phone rings off the hook from people who's computers have literally choked themselves to death because they have inadequate virus, firewall and spyware protection and a lack of plain-old common sense.

They ask me "What can I do?" and when I start to explain in the simplest of terms, they say "I don't understand a word you are saying."

So as a result, I shall do my duty as an Information Technology professional and publish my thoughts on the subject and call it "Guide to High-Speed Internet Use for the Inexperienced"

I will break this down into two parts. The first is for the person whose computer has now literally clogged itself up so bad it will no longer function or is now so slow it is unusable. The second is for people just buying a new computer or just restoring your old computer like it came from the factory and starting over.

Part I: The Polluted Computer. If you've been riding your new high-speed connection a while and have noticed that your connection is now really slow, or you're getting so many pop-ups that you can't keep them shut down, or your computer won't let you connect to the internet, or it keeps throwing up sexually-explicit websites, you might qualify to be called polluted.

What causes this? Viruses, advertisement software, key loggers, browser hijackers and re-directors, Trojan horse programs, etc. How do you clean it off and put it back to normal? Good luck. Some people in the area are experienced enough to do this, but their time is expensive. My suggestion? Copy all of the files you wish to keep to a CD-R or CD-RW disc or Jump drive and re-load your computer from scratch using the restoration CDs that came with it, and follow the instructions in Part II. If all else fails, you're only recourse is to take your unit to a professional, or buy a new one!

Part II: Clean Slate. So you've just brought that new computer home from the store and you are ready to set it up and get it connected to the Internet. You un-pack it, set it up, turn it on and install the software necessary to get your connection up and running. You're safe now, right? It's a new computer and it will have everything I need to keep myself safe? NOT HARDLY.

Most new off-the-shelf computers come with a trail version of an anti-virus package, maybe some other trial versions of Internet Security software of some sorts, but none come ready to protect, no not one.

What do you need to be protected? In order of importance in today's world, you need five things: A GOOD anti-virus package, either a personal software or hardware firewall, some anti-spyware software, a temporary files sweeper and an decent amount of common sense.

The cost to home users for this software? Nothing. Not one dime for the home user. Why? Because several people in this world understand that home users are naïve and won't pay for adequate protection and they have taken pity on these people by offering "free to home user" version of their products.

These versions are not completely full-featured, but do offer a more than adequate measure of protection against the elements that cause your computer to clog up. Could I give recommendations for such software? Here's my list of top contenders for safety:

Anti-Virus

AVG - <http://free.grisoft.com/freeweb.php/doc/2/> - Publisher: Grisoft

Avast - http://www.avast.com/eng/down_home.html - Publisher: Alwil Software

Firewall *

ZoneAlarm -

<http://www.zonelabs.com/store/content/company/products/zna/m/freeDownload.jsp> - Publisher: Zone Labs Inc. Free version works great, but some technical knowledge is necessary to interpret the messages. Upgrading to ZoneAlarm Pro for a small one-time fee is recommended to cut down the number of messages you will receive.)

* Windows XP Home or Professional comes with a built-in firewall package. Installation of XP Service Pack 2 will automatically turn this feature on. All users of Windows XP should up grade to Service Pack 2.

Spyware Removal

Ad-Aware - <http://www.lavasoftusa.com/support/download/> - Publisher: Lavasoft Inc.

Spybot Search & Destroy - <http://www.spybot.info/en/download/index.html> - Publisher: Safer Networking Limited

Microsoft Anti-Spyware – (Beta version is free until July, 2006, but may be extended beyond that while in Beta testing phase – valid only for Windows XP and 2000)

<http://www.microsoft.com/athome/security/spyware/software/default.mspx>

Publisher: Microsoft

Spysweeper – <http://www.spysweeper.com> - Publisher: WebRoot, Inc. (Free Trial, \$29.95 to buy)

Temporary File Sweeper (Cleans unnecessary files from your computer)

CCleaner – <http://www.ccleaner.com/ccdownload.asp> - Publisher: CCleaner.com

The sites will either will ask you to give them donations to help keep them alive, or they will encourage you to upgrade to their “full or professional versions” with more than the basic features. If you find the products you have installed useful down the road, I encourage you to give a small donation if you can do so.

In addition to downloading and installing your choice of these wonderful pieces of software, you need to realize that each of these packages need to be updated frequently and executed on a scheduled basis to keep your computer clean and tidy.

Windows Updates: As long as your computer has Microsoft Windows Version 98 Second Edition or higher, you can keep the Windows operating system updated via Microsoft’s Windows Update Website <http://windowsupdate.microsoft.com>

There is a link in Internet Explorer under the Tools menu for this site as well as a link on most computers when you click on the START button. All “Critical” updates should be installed. You may also wish to install some of the other suggested software updates or hardware driver updates, but they are not necessary for the safekeeping of your computer.

Common Sense: Enough cannot be said for having a little bit of common sense when you use the internet.

The first and foremost thing to understand is that if a piece of software is offered as free, usually it’s not completely free. Many games are included in this category. When you agree to the License Agreement included with the installation of the software you have just downloaded, you need to read the fine print of that agreement before proceeding. Often you will find that third-party tracking and reporting software (spyware) will be installed along with it.

Second, understand that you don’t have to open e-mail attachments from anyone. There is no law that says you have to even open up a message if you aren’t completely sure you know who it’s from.

More viruses are spread by opening e-mail attachments than any other way. A good way of keeping down SPAM from your e-mail inbox is to change your e-mail address every couple of years and then give it only to those people that are important to you.

Third, don’t be the goober that forwards every cute, warm, funny, amazing e-mail message you get, thus perpetuating the flow of useless crud to others. Forget the chain letters that threaten you with bad luck down the road if you don’t and the Gap jeans e-mail that will get you a gift certificate worth \$245 if you forward it to 20 friends. It’s all

a bunch of baloney. It doesn't work. E-mails can't be tracked past the person you send it to, much less around the world.

Fourth, make passwords for accounts hard to guess. For instance, most people use their favorite pet, child, spouse or college team as their password. Or they use a date that is important. A "strong" password is one that can't be guessed easily, or cracked by a password generator in a short period of time.

Ideally, a password should be a minimum of six characters, numbers or special symbols. Seven or eight is even better since it takes an exponential number of tries for a password generator to crack it.

Good password examples: k00ki3\$ ba6b0yz! W0lfM3a+

Bad password examples: spot 091101 steph spot

Fifth, NEVER, and I mean NEVER, click on a link in an e-mail that asks you to update your account information because of this or that reason (social engineering), or asks you for an account name and password. If you have a question about your account, call the company using the phone or go to their website by typing in the web address into your browser or clicking on an already existing favorite or bookmark, so you know for sure you are dealing with that entity and not a fake.

Most e-mails from financial institutions or retail or internet-based stores or auctions that ask you to update your account information are fake (phishing) and they wait on you to give them your personal information, then they re-direct you to the real site to continue on with your business. Then they become you with that information (identity-theft).

I hope this helps some of you to be better prepared for life in the world of high-speed access to the internet. Happy surfing.

Ralph Perdue Jr.

Computer/Technology Manager

Oklahoma Department of Career and Technology Education

Skills Centers Division