

Exploring the Internet: Good Practices

In this day and age of more and more people having high-speed Internet access it is more important than ever to safe-guard your PC against viruses, spyware and hackers. It is not a matter of whether or not to have virus protection, it is which package you choose to use – it's just that simple. Failing to protect your computer from the dangers that are out there will almost guarantee future trouble.

The world of high-speed Internet is a wonderful and exciting place and we here at Thames Valley Communications want you to enjoy it to its fullest without suffering the pitfalls that most certainly exist. With that in mind, we have put together this list of good Internet practices for you to follow. Follow these guidelines and your PC will thank you for it later by running more efficiently and secure.

1) Purchase and subscribe to a computer virus protection program.

There is a trade-off going from dial-up to high-speed Internet access. With your computer potentially on-line 24 hours a day at a high speed you are much more susceptible to viruses and hackers. A virus is a manmade program that causes an unexpected, usually negative, event on your computer. A bad virus can render your PC non-functional. Virus protection is a must, not an option. Some of the most popular virus protection programs currently are McAfee VirusScan, Norton Antivirus, ZoneAlarm with Antivirus and Trend Micro PC-cillin. Go to these sites to download the program and/or for more information on the products.

McAfee VirusScan	www.mcafee.com - click Home & Home Office
Norton Antivirus	www.symantec.com - click on Shop Home & Home Office
ZoneAlarm	www.zonelabs.com
Trend Micro	www.trendmicro.com - click on Personal
AVG	www.dowbload.com - Search 'AVG'

Additionally you can use Trend Micro's 'House Call' to run a free internet-based scan on your pc by going to housecall.trendmicro.com.

Another way to get these programs is to download one from a site such as www.download.com for a 30-day trial, then get an annual subscription and configure it to update automatically every day. Then your likelihood of being hacked or infected with a virus drops significantly.

Microsoft has a link on their site that guides you through the fundamentals of protecting your PC
<http://www.microsoft.com/security/default.msp>

2) Use a Personal Firewall.

A firewall is a program or hardware device that block unwanted access to and from the Internet so that you have more of a say in what Internet traffic gets to your PC. Many programs have a legitimate reason to attach to the Internet – an audio player such as Windows Media Player gets album and song titles for instance. But without a firewall you are taking a chance that your computer may be attacked by a hacker.

Fortunately getting and setting up firewall software isn't as complicated as it sounds. All of the companies mentioned above also offer firewalls, often packaged together for better pricing. Below are these combined products as of 12/21/2004:

McAfee Internet Security Suite
Norton Internet Security 2005
ZoneAlarm Security Suite
Trend Micro PC-cillin

These are the best buys and are the surest bet to keep you safe on the internet, as long as you keep up with your subscription and schedule them to update daily.

There are also some freeware (free!) personal firewall packages available for use. Though not as time-tested as the others, you can try them out and see how they do. Here is a list of some:

Sygate Personal Firewall smb.sygate.com/ (click 'Need a Free Solution?')
Kerio Personal Firewall www.kerio.com (click 'Products' and 'Download')

Routers with built-in firewalls are another excellent way to keep your computer safe. If you are going to use a router always change the factory username and password to access your router. Depending on the type of router you have, there could be additional security settings within the router that you may want to change. On wireless routers, at the very least, you want to change the router password, enable WEP encryption and MAC filtering.

****Beware of blocking too much – certain programs on your PC need to interact with the Internet and if you block them your program will not function correctly.**

3) Beware Spyware

Most people are familiar with freeware, shareware, cookies, media players, interactive content, and file sharing. What they may not realize is that some of the aforementioned may contain code or components that allow the developers of these applications and tools to actually collect and disseminate information about those using them.

They can track your surfing habits, abuse your Internet connection by sending this data to a third party, profile your shopping preferences, hijack your browser start page or pages, alter important system files, and can do this without your knowledge or permission. Get

enough spyware and your PC slow to a crawl and access to your favorite program may become impossible.

Fortunately some of the best Anti-Spyware programs are absolutely free. Here is a list of the best ones:

Ad-Aware	www.lavasoft.com (highly recommended)
Spybot	www.safer-networking.org
SpywareBlaster	www.javacoolsoftware.com (prevents spyware install)
Windows AntiSpyware	www.microsoft.com (listed under 'popular downloads')

4) Be Careful, Cautious and Concerned

Much of the dangers can be avoided by being careful. These tips will help you avoid getting viruses, hacked or spammed:

- **Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
- **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a friend or someone you know. Some viruses can replicate themselves and spread through email and pretend to be someone you know. Better to be safe than sorry and confirm that they really sent it.
- **Do not open** any files attached to an email if the subject line is questionable or unexpected.
- **Delete chain emails and junk email.** Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site.
- **Update your anti-virus software regularly.** Over 500 viruses are discovered each month, so you will want to be protected.
- **Back up your files on a regular basis.** If a virus destroys your files, at least you can replace them with your back-up copy. Burning a CD of your files every so often is a very good idea.
- **Passwords:**
 - Do not store your passwords in a file on your PC. If you get hacked and they get to that file, you will be in for big-time trouble.
 - Create more difficult passwords. Be creative. Avoid using easy to guess things like your name, birthday and child's name. Passwords are harder to break if they contain both numbers and letters.
 - Avoid using the same username and password for everything. Mix it up as much as possible.
 - Change your password as often as is practical.
- **Beware surfing to questionable websites** – it can lead to unsavory after-effects.
- **Purchase items on-line only at reputable, well-known stores** – and make sure you are actually on their website (check the address line)

- **Macs and Linux boxes get viruses too.** Don't think that these things only happen to Windows users.

5) Avoiding Spam

If you use your e-mail for anything at all, you probably get a lot of spam and junk mail that you would like to be rid of. There is no way of accurately getting rid of all spam. Even if everyone's definition of spam was the same, spammers themselves will always be trying new tricks to bypass your "spam filters." But you can do a pretty good job of getting rid of the most egregious spam. Most spam can be avoided if you are careful about who you give your @tvconnect.net e-mail address to. Only give out your address to trusted sites. Never allow your address to be published on a website. When you sign up for services on-line, make sure to read ALL the fine print and make sure they do not have checkboxes checked off subscribing you to newsletters and volunteering your address to be distributed to 'trusted' affiliates.

Separate Email Accounts - Set up an extra email account for yourself to be used for all online activity. Most Internet service providers allow you several free email addresses. You can also set one up at one of the free email sites such as yahoo, google or hotmail. Use one email account for friends, family and business (the emails that you really care about). Use the other account for all other activity such as registering your computer, software registration, subscriptions to forums and online purchases. Each time you submit your email address online, you have the potential of it getting on some spam list. This can help you keep the flood of email somewhat organized and worse case, if it gets completely out of control, you can delete the account and start over without the hassle of changing your main account.

Email Settings

Depending on what email program you are using, you can change the way email is handled to reduce the likelihood of contracting a virus.

1. **Receiving Attachments** - You can change the settings to prevent attachments that may contain viruses from downloading. This can be a problem if you regularly receive attachments because you may not be able to open them.
2. **Opening Attachments** - The majority of problems come from opening attachments. Do not open any attachments unless you know the sender and even then I would not open them unless you were expecting it.
3. **Displaying Email** - Avoid preview panes. Change the settings to not show you the contents of an email until you double click on them.
4. **Downloading Pictures** - You can also choose to be prompted before downloading pictures within emails instead of displaying them automatically.
5. **Junk Mail** - Explore the options for filtering spam so that you can automatically move them to a spam or junk mail folder. If you wish, you can have them deleted, or brief through them to check for the few real emails that may be misdirected.

6) Windows Updates

Just as important as having a virus protection package is keeping your PCs operating system up to date. Hackers are constantly finding security holes in operating systems so Microsoft and Apple come out with security patches to fix these problems. It is very important to keep up with these patches or you risk someone attacking your PC.

There are a couple of ways to update a Microsoft Windows operating system. Depending on which operating system you are using there will be a **Windows Update** shortcut in your **Start** button somewhere: **XP** keeps it in the Programs folder; in **Windows 2000** it's right in the initial Start button menu towards the top. Regardless of which operating system you run you can always go to www.windowsupdate.com. Windows update will then allow you to scan your PC for updates and give you a list of Critical Updates that need to be installed. You can also schedule updates to automatically install by finding the Windows Update Control Panel and configuring it appropriately.

Macintosh OSX: Click on the Apple Menu and click on Software update. You then will be presented with a choice of items to install.

7) Safeguard your Family

The Internet is a wonderful and informative place, but there may be certain sites that you do not want your entire family, especially your kids, to go to. Fortunately there are several **Internet Filtering** programs that help you in this area. PC Magazine highly recommends Cybersitter, which is available at www.cybersitter.com. Here are a few others:

Cybersitter	www.cybersitter.com
CyberPatrol	www.cyberpatrol.com
IProtectYou Pro Web Filter	www.softforyou.com
Net Nanny	www.netnanny.com
Norton Internet Security	www.symantec.com

8) Credit Card Transactions

1. **Protected Accounts** - If you plan to purchase goods and services online, we would recommend setting up a special online account such as PayPal.
2. **Using a Single Card** - If you prefer to use one of your current credit cards, set aside a single credit card for all online purchases. Don't use that card for any other transactions except online. It will be a lot easier to spot errors and fraudulent charges if it is not filled with normal everyday charges.
3. **Fraud Protection** - Use a credit card that comes with some form of fraud or online purchase protection. (check your credit agreement).
4. **Low Credit Limit** - Select a credit card with a lower credit limit. Having a credit line of only a few thousand dollars opposed to \$18,000 can reduce your potential liability.
5. **Purchase From Know Companies** – Purchase only from known companies or ones that have been recommended to you.
6. **Do not Respond** – Do not give your credit card information to any unsolicited websites (pop-up ads or email solicitations).

7. **Avoid Following Links** - If you want to go to Borders to purchase a book, type their web address in directly, instead of following an unknown link contained within an email. It could take you to a fictitious site that looks just like the original.

8. **Spelling Errors** - When typing in the address to a website, **double check your spelling**. Some fraudulent websites take advantage of common misspellings and may look just like the real thing.

9) **Personal Information**

1. **Never give out personal information** - Never give your social security number to anyone. The same goes for account numbers and passwords.

2. **Be very careful of bank inquires** – Be very wary of answering bank inquiries online. Verify that you do indeed have an account with that inquiring bank before replying to or answering any questions!