

## **Protecting yourself while online**

The internet is filled with a vast array of useful, fun and interesting information. Unfortunately it is also a hostile environment, which can have detrimental effects on the people who use it. Insecure use of the internet/email can cause troublesome effects such as virus infections, identity theft, loss of privacy, spyware/malware problems and data loss. This edition of PSO Power Tools will give you the top 7 ways you can protect yourself while online.

### **1. Install, use, and keep your anti-virus software updated:**

- Virus writers and antivirus software manufacturers play a game of “cat and mouse.” When a new virus is discovered, the antivirus organizations update their software “patterns” or “definitions” to catch the newly discovered virus. The virus writer then adjusts or creates a new virus to circumvent the antivirus company’s efforts. Then the antivirus company updates its patterns, so the virus writer updates his virus...and the antivirus company updates its patterns...etc.
- Your virus protection is only as good as its last update. If you are not updating your virus software regularly you are not protecting yourself from the latest virii. Remember, your antivirus program can only protect you from what it knows about.
- There are many commercial antivirus products available. The “big three” are Symantec (<http://www.symantec.com>), McAfee (<http://www.mcafee.com>), and Trend Micro ([www.trend.com](http://www.trend.com)). There are also a few free antivirus scanners available. The most popular is AVG Free edition, which can be downloaded here: <http://www.grisoft.com/doc/40/Ing/ww>. As with most things, you traditionally “get what you pay for” and if you can afford the commercial costs (approx \$40/year) you will be better served by a purchased product.

### **2. Keep your operating system and programs patched:**

- In addition to using and updating your antivirus software, you must also keep your operating system (Windows 98, Windows XP, etc) up to date. Virus writers author their programs to exploit weaknesses in the operating system to infect your PC. Keeping your operating system updated reduces the risk of this occurring.
- The Microsoft Operating System update site can be accessed here: <http://windowsupdate.microsoft.com>. This site will scan your PC for the available updates and give you the opportunity to install them. You may have to reboot your PC and visit the site a few times to become fully updated the first time.
- The Microsoft Office update can be accessed at <http://officeupdate.microsoft.com> and provides a similar service to the Operating System update system.
- Windows 2000 and Windows XP both contain features, which allow them to be updated automatically. Use this if you have an “always on” internet connection such as MTS DSL or Shaw broadband.

### **3. Be cautious when downloading files or reading email which contains attachments:**

- Never open attachments contained in an email from someone you don’t know.
- Never open unsolicited email attachments without confirming that the sender actually meant to send them. Many viruses send themselves out from an unsuspecting user’s

computer in an attempt to fool their contacts into opening the attachments and infecting themselves.

- Do not pay attention to email “virus warnings” as the vast majority of them are hoaxes designed to entice you to delete critical system files. Forwarding these messages to others increases the problem. Do not send these types of messages to others.

#### 4. Be concerned about your privacy:

- Never use an “unsubscribe” link in a spam email that you have received. Most times, this only “confirms” the validity of your email address and you will commonly receive even MORE spam after “responding” to the initial spam email. The correct way to deal with spam is to simply delete it. If you are an experienced user you may analyze the message headers and report the offending person to their internet provider.
- Do not select the “save passwords” option when using your internet browser. Should someone gain access to your PC (remotely or otherwise) they may be able to impersonate you and make transactions on your behalf.
- Never perform financial transactions on public or shared computers that you may find in internet café’s.
- Recognize that identity theft is real, and a growing problem. Regularly verify your credit card and bank statements for any signs of misuse. It is also good policy to periodically check your personal credit rating for anything out of the ordinary. Usually your bank manager can assist in the process.
- Never write down your account usernames or passwords. Do not share this information with others.

#### 5. Backup your data consistently:

- A good rule of thumb is that you backup what you would be angry if you lost. Imagine coming into your office one morning and your entire computer is gone. What files/data would you miss? Those are the things that should be backed up on a regular basis.
- Files can be “burned” to CD’s, DVD’s or stored on a network server (if you have one available). Keep backup copies in a different location from your computer. If your office was to burn down, you couldn’t recover your files if they burned up as well. Consider keeping data copies of your home PC in your office, and your office files in a secure location away from the office.

#### 6. Avoid and detect “spyware:”

- Spyware is a program, which installs on a target computer usually without the operator’s knowledge or understanding. Spyware can perform keystroke logging (password stealing), screen shots (see what you are doing on your PC), data theft, send spam, host illegal servers/sites on your PC, and degrade your computer’s performance. More and more of it is being used to steal your personal information to commit identity theft.
- Spyware is commonly installed by “free” programs such as “email smilies,” free games, or free screensavers. A lot of ‘spyware removal’ tools are actually spyware themselves! Do not install/download files from “free” sites or by responding to ads received as “popups” when using the internet or sites contained in a “spam” email.
- Regularly run a spyware detection program such as LavaSoft’s AdAware which is free for non commercial use at <http://www.lavasoftusa.com/> On the lower right hand portion of your screen, select the “download.com” icon which looks like this:



## **7. Protect your PDA (personal data assistant), Laptop and Cellular telephone:**

- The FBI statistics state that 1 out of every 10 laptops are stolen within the first 12 months of ownership. 30% of PDA's (Palm Pilots, portable organizers) are lost every year. Less than 10% of lost or stolen devices are ever recovered intact.
- Lock up your laptop using a specialized laptop cable to your desk. Never leave your laptop in your vehicle, or let it out of your site.
- Many cellular phones can function as PDA's storing names, phone numbers and important documents. If you must keep this type of information on a portable device, consider using encryption and passwords to protect the contents should the devices become lost or stolen.
- Keep a record (away from the device) of the serial number, model type and configuration of any portable device. Report loss of theft to the police immediately. If you had any "password lists" or other information which could be used to access other computing systems or confidential information, advise your system manager immediately so he/she can take appropriate action to protect corporate data.

## **8. Use common sense when conversing via the internet:**

- Consider email like a postcard. Don't assume the intended recipients will only read it. Never use free email services such as "hotmail" when transmitting confidential information.
- Be aware the "Internet remembers forever." Anything you post to a mailing list, chat room, blog or any other public forum can be archived, indexed and made available to everyone – forever. Think twice before posting angry, inflammatory or potentially untruthful messages in a public forum. Those words may come back to haunt you decades down the road, long after your emotions on the subject have subsided.
- Know whom you are chatting with. It's trivial to assume someone's identity in a chat room or instant messenger conversation on the internet. Perceived anonymity makes it easy for someone to describe themselves in ways completely different from what they are really like. Even worse, you may encounter some sort of predatory person. Never reveal personal information that would enable someone to learn more about you, such as your phone number or address.

By following the above tips, you should be able to have a safe and enjoyable experience using the internet, without jeopardizing your security, privacy or personal information.

I hope you enjoyed this edition of the PSO Power Tools.

**The PSO Unit would like to thank Mike Shaver, Sport Manitoba Information Technology Manager for writing this edition of PSO Power Tools. If you have any questions about the content, please feel free to contact Mike directly at [mike@sport.mb.ca](mailto:mike@sport.mb.ca). Thanks again Mike for the important information.**

### **Publication of the PSO Unit**

Contacts: Janet McMahon    [mcmahon@sport.mb.ca](mailto:mcmahon@sport.mb.ca)    Fred Schneider    [schneider@sport.mb.ca](mailto:schneider@sport.mb.ca)  
Brenda Wiwcharyk    [wiwchar@sport.mb.ca](mailto:wiwchar@sport.mb.ca)    Kristin Albo    [albo@sport.mb.ca](mailto:albo@sport.mb.ca)

For further information, please contact a member of the PSO Unit.