



THE INTERNET

It is estimated that over half of Canadians have access to the Internet and its library of thousands and thousands of servers.

Just like everything in life there is good and bad that goes with this new technology. The good is that there is so much information available on virtually every subject, the bad is there is so much information available on virtually every subject.

While useful, the computer in your house can act very much like the Trojan Horse of ancient history. While looking like one thing, it can harbour a multitude of potential problems.



Viruses and Worms

These are programs that execute without your permission and can cause a lot of headaches, problems and potentially damage your data.

Solution: Get anti-virus software and keep it updated (daily if you are a heavy user). I have had good success with the new Norton 2002 and McAfee Anti-Virus Software.

By the way, viruses infect your computer; worms infect your computer and try to infect everything on the network.

Intruders

This is a problem for “always on” connections like xDSL, Cable etc. Hackers try to break into your system. If there isn’t anything valuable they can use your computer to attack other computers without you being aware that your system has been compromised.

Solution: Get a firewall. There are two kinds of firewalls, software and hardware. Some, like “Zone Alarm” are free. Other software firewalls are available from the Anti-Virus vendors or hardware firewalls like a simple Linksys router can provide adequate protection from invasion.

The second line of defence is good passwords. If you can find the word in your dictionary, it’s not good enough. Good passwords are a mix of Uppercase, lowercase, numbers and symbols. (iou\$54LD) You’d remember this as a phrase. “I owe you five dollars for long distance.”

Invited Guests

What if someone wearing a paper bag over their head came to your door and asked to visit with your 14 year old daughter in her bedroom for an hour or so. What would you say?

The Internet can connect you with millions of people all over the world. Problem is along with the ordinary people come the con artists, criminals, pedophiles and ideologies and material that you might not want brought into your house.

The Internet is a great medium for these people to operate. It is unregulated, crosses national borders and it is virtually impossible for law enforcement to police. This means that the responsibility for protecting yourself is yours.

Fraud has and always did have one rule. If it sounds too good to be true it probably is. Counterfeit information on Fraud sites or through email looks professional but Due Diligence and research is your responsibility to make sure it is professional. The proceeds of crime from these scams is estimated in the billions of dollars worldwide.

Virus myths and Urban Legends abound on the net. Two great resources to check are <http://www.vmyths.com> and <http://urbanlegends.about.com> to check out whether the latest “Warning” you’ve received is genuine or fake.

A child on the net is a big concern. Generally they do not have the experience and this naivety lends itself to problems of security and safety. While it is recognized that privacy for a child is an eventual right, where safety and security are concerned – privacy becomes a victim.

If the rule is to knock on the door before you enter, that rule gets tossed out the door if you believe the child is in danger. Safety and security override privacy.

The Internet, by its construction, is not private, it is a shared resource. If you remember what a “party line” was like in rural Alberta, or you’ve ever sent a postcard, you have a good idea about how private the Internet is.

Ideally the computer should be placed in a common area in the house with the screen facing outwards. The system should be locked down with a “system” password so that it cannot be accessed unless an adult is present. Programs like “Mousetrap” (<http://www.ryanware.com/mousetrap.html>) lock the computer’s functions even if it has been rebooted.

Pre-teens and younger children can benefit from the use of filtering programs like *Net Nanny* and *Cyber Patrol*; there are also ISPs who provide content filtering with configurable options.

Monitoring software can be used on systems either overtly or covertly. One of the better ones we have tested is “**Spector**” from <http://www.spectorsoft.com> which takes pictures of what is going on including chat and email sessions. It does this by taking hundreds of screen shots an hour. It can be combined with another program called **e-blast**, which sends an email to you at work so you can monitor what is happening remotely.

There is an increasing trend for schools, government and work to monitor the activities of their users on the net. Being monitored is an activity that many people see as a “necessary evil” in today’s connected world.

Name

Address

Section 6.2 Quiz

1. What dangers are there on the Internet?

2. Give other examples of the 4Ds that could prevent this fraud

3. How is your behaviour going to change now that you have this new information?
