a little CRC...

Northcliffe Community Resource Centre

Tel: 9776 7330
Fax: 9776 7338
PO Box 133, Northcliffe
ncrc@northcliffe.org.au

Invasion of the Computer Snatchers

The range of computer threats is constantly growing. Computer users need to take them seriously. A degree of paranoia pays...

Identity theft, password theft, account hacking...
These could result in someone getting access to your online accounts or finances. Choose secure passwords (not just easily remembered ones). Write them on paper in case you forget them (hackers will have a hard time getting hold of your paper password list).

Viruses, Worms, Trojans, Spyware, Keyloggers, Botnets...
These can stop your computer from functioning, steal your login details and destroy your documents and files. *Botnets* cause your computer to start 'attacking' other computers without your knowledge. Telstra says that 5.4% of it's users' computers are infected with botnets, and in the USA the infection rate is 15%.

If you suspect any type of infection take action, make backups and stop using your machine for internet banking and online purchases.

Nigerian Prince SPAM, Phishing and Online scams...
Have you ever been warned that someone you know is stranded in a foreign country and needs financial assistance? It's a scam!!!

SPAM is unwanted, unasked for email and is the starting point for most scams: marriage scams, inheritance scams, investment scams, lottery scams and more. If you know someone likely to fall for an internet scam please try to educate them. A WA man recently lost $3m through an online scam.

'It's Microsoft calling. There's a problem with the computer...'
Hang up. I doubt Microsoft will ever call you. Alternatively the caller might claim to be from Telstra, Iinet,'the computer service department' or elsewhere. Most computer users have now wised up...

Electronic Blackmail and Ransomware
Ransomware takes control of your computer and files and asks you to pay a fee so the problems can be 'fixed'. Often the company offering the 'fix' is the originator of the problem. Recently a US Police Department admitted to paying an electronic blackmailer who took control of their files. Even pros can become victims. Backup your files and store the backup away from your computer.

Online Reputation Blackmail
...A business owner will be alerted to an unjustified negative review of their business on the internet by an 'online reputation service' (who made the review) offering to delete it... for a fee...

Cyber-stalking and Online Bullying
Having witnessed physical bullying, the risks of online bullying seem overstated to me. However cyber-stalking takes it a step further. A cyber stalker may hack your accounts, impersonate you to discredit you, and install malware and spyware onto your computer. If you're a victim it's time to educate yourself about computer security.

Spyware, Snooping and Hacking for the Man
Spyware can track your internet usage, expose your emails and documents to third parties, or spy on you using your microphone or webcam. Laptops are more vulnerable as these tools are built into the machine. Online spying is an unavoidable fact of modern life. Governments around the world hire scores of hackers for spying on citizens, businesses, organisations and even themselves. Blackmailers, cyberstalkers, 'hacktivists', or your business competitors are also potential snoopers. If you think you are a potential target then you will need expert advice. One simple privacy measure individuals can take is to put removable tape over their web-cam (try a Post-it).

Productive Paranoia
Don't let anyone tell you computer security is easy. Even experts are challenged to not open the wrong email or download and install the wrong program. There was never 100% safe. Now there isn't even 99% safe. We are all potential victims.

However those with good knowledge, and who look for the clues, have a significantly better chance of staying safe.

Understanding that you are at risk provides the basis for action: make backups, stay offline when necessary, take precautions...

Don't Rely on A Wish and a Prayer
Recent studies have shown that a computer without virus protection, surfing the internet, will become infected on average within 20 minutes. If you use Windows XP, Vista or Windows 7, **you need anti-virus software**. It also needs to be up to date. I recommend the free product 'Microsoft Security Essentials' since it keeps itself up to date without the need for maintenance payments.

Other essential measures include performing Windows updates, Java updates, Adobe Reader, Flash and other software updates.

Where are you getting your software from?
If you get your GIMP download from gimp.com rather than gimp.org, or your media player from freedownloads.com then you are putting yourself and your computer at risk. When you install software you give it wide open access to your entire computer. Malware can arrive on the coat tails of legitimate programs.

Do some research and find out the **official download source** for the program you want. Make sure this source has a good reputation. Try not to accidentally click on the advert which is disguised as the 'download' link. This is a difficult job for computer beginners!

"Do/n't expect something for nothing"
Many internet scams rely on 'suckers' believing that someone, somewhere, has money or favours to offer them. A friend of mine puts it this way 'You can never con an honest man.' Unfortunately, on the internet, this is far from true.

The internet is, in many respects, a gigantic treasure trove of free stuff. Scammers just play on the expectations this has produced.

In fact **paying** for things on the internet is where many scams begin - including theft of credit card and personal information.

Many of the rules of computer security are not absolute. If you are concerned about any of these issues come and see us at the Northcliffe CRC and we will do our best to provide useful advice.

Graham Evans