

Computer Tips

Brought to you by

Michael's Computer Services

Using Your Internet Safely

There are perhaps dozens of reasons for using the Internet, yet I'm sure everyone who uses the Net is interested in one common issue—privacy. Using the Internet often requires sensitive information, such as providing your name, location, and email address. Even your financial information must be provided when using an online checkout, or when using Internet banking. Using your password or PIN is also common on secure and many government websites. Other information about you is made available when you are browsing the Net, such as your IP (internet provider) address, your type of browser, and the version of Windows you use. Keeping this personal and usually sensitive information private and out of undesirable hands is possible, provided you follow a few simple tips for safe surfing.

1) Install an Antivirus program. Better still, also use a firewall and antispyware program. We use and recommend AVG 7.5 Free, Spybot Search & Destroy 1.5, and the firewall built-in with SP2 for Windows XP.

2) Whatever antivirus/antispyware program you use, make it is UP-TO-DATE. Just having a program installed will not protect you. Most protection programs have a built-in easy method of downloading and installing program updates.

3) Do not reply to any email that you do not recognize. There are currently several emails circulating the Internet which claim to be from your bank, stating your account details are out of date. The email then provides a link to supposedly update your details. These emails are nothing more than a FRAUD. If you click the link, your details will go to another site, where your details are collected and used to access your bank accounts.

4) Be very careful what software you download from the Internet. As a rule, if the software pops up in your browser uninvited, then don't download it. Most of these downloads contain Spyware, a group of software that are designed to detect your personal information and Internet habits, and report back to their creators. Chat program add-ons, PC system cleaners, screensavers, and online casino games are common ones to avoid.

5) Never, ever, send your credit card details, bank account password, or other online passwords via email. Email is the least secure way to send sensitive details.

6) Make sure you are using the latest version of your browser. Your browser is the main interface to the Internet, and it is therefore necessary that it has the latest protection. All current Internet browsers have some basic protection built-in, such as popup blockers, anti-phishing (detects websites posing as another site), ActiveX script protection, and cookie security.

7) Check that you are using reputable toolbars in your browser. These toolbars are typically a line of search shortcuts near the top. Google, Ninemsn, and Yahoo are common and safe. Others such as Hotbar, Dashbar, Starware, and MyWebSearch are all spyware and should be removed.

Michael's Computer Services

85 Chester Street, Nanango

- ADSL & Internet Setup
- New & Used Computers
- System Upgrades
- Software Sales & Installation
- Ink & Toner Cartridges
- Website Design & Hosting
- Virus Removal & Prevention
- Printers & Scanners
- Hardware Sales & Installation
- Laptops & Projectors
- Networking
- Local In-Home Service



Call Michael or Naomi on:

4171 0981

or Mob. 0419 790 071

www.mcsyarraman.com.au