

# Staying private in public

## a guide to using shared computers and wifi connections

11/2011



**Although convenient, surfing the 'net on a public computer or over a public wireless network (WiFi) can make you more vulnerable to theft, fraud and hardware infections.**

**While browsing at a library, café, hotel or airport, it's important to take some extra care and limit the amount of personal information you transmit. These handy hints will help you keep your private bits private when you're out and about.**

### Think before you submit and cover your tracks

Be mindful of the sites you visit when using a computer or device that's not part of your secure home network.

- When logging onto a website or checking email, untick the box that saves your personal information like usernames and passwords. This simple step means your details won't be visible to the next person that uses the computer.
- Delete browsing history before logging off. Browsers store information about the sites you visit, so it's a good idea you clear your browsing and download history, cookies and cache.
- Limit the amount of personal banking and online shopping you do when using public computers or WiFi. Stick to general browsing where your private details and passwords are not required.

### Watch your back

Be aware of your surroundings when using an Internet café.

- If possible, choose a computer with a screen that faces a wall or has unattended computers around it.
- Shoulder surfing is when someone snoops over your shoulder to read what you're typing. Just like when you're using an ATM, make sure no one is watching what you're doing and what you're typing.
- If you leave the computer for any reason, even to grab a quick coffee, log out so that your computer can't be accessed by a passer-by.

### Some like it HOT

When you connect to a public wireless access point, or hotspot, it's likely the connection is not secure making it possible for others using the same network to monitor your activity.

- Avoid hotspots that are run by people or organisations you don't know. The not so nice out there can set up rogue networks and access your private information.

- Upon connection, if you're prompted to select a network type, always select "public" when connecting to a WiFi network outside of your home. This gives you increased security so you can rest a little easier.
- If you keep personal files on your PC consider making them unreadable to others (also known as encrypting) so they're protected from snooping outsiders that might be using the same public network.

### Practice safe surfing

As the saying goes, it's better to be safe than sorry. These final precautions provide peace of mind and are best practiced whenever you're using a public computer or connection.

- When you're done, disable your device's wireless and Bluetooth. It can save your security from being compromised and, as a bonus, it will save your battery life.
- Avoid using your USB memory stick in public computers because malicious software can transfer from an infected computer to your home PC. If you must transfer documents via USB, make sure your virus scanner vets the stick before you use it again.
- Make sure your security settings are always up-to-date. This means activating virus definitions, firewalls, and anti spyware.

Pick up more hints and tips from **iiNet's Online Safety Series** from [iinet.net.au/safety](http://iinet.net.au/safety).

