Office of the Information Commissioner
Queensland

Information Sheet

Information Privacy Act 2009

Privacy and using public wi-fi hotspots

This information sheet will help you understand the risks and simple steps you can take to protect your personal information when using a public wi-fi hotspot.

Overview

A 'wi-fi hotspot' is a location where a wireless access point provides shared Internet access for wi-fi enabled devices such as smartphones, tablets and laptops.

Public wi-fi provides a convenient and often free[1] means of accessing the Internet. Government agencies are increasingly providing public wi-fi access in government buildings such as libraries, in public spaces such as parks and pedestrian malls, and for special events such as conferences and festivals. However, although the wi-fi hotspot is provided by a reputable organisation, such as a local government, the security of your personal information might still be at risk.

Public wi-fi access, by its very nature, is an unsecured network. Once your device is connected, the personal information on it and any information you send using the wi-fi connection (eg, your username and password) can be vulnerable to interception and access.

Regardless of whether it is a government-provided public wi-fi service, you are responsible for ensuring the privacy of your personal information while using a wi-fi hotspot.

Practical tips for protecting your personal information when using a public wi-fi hotspot[2]

- **Check the network name** - It is a common ploy of hackers to set up their own wi-fi hotspot with a name very similar to that of the legitimate wi-fi hotspot. Don't let your device automatically connect to the first wireless network in the list. Instead, manually select the name of the wi-fi hotspot you wish to connect to. Some providers of public wi-fi will provide the exact name of the network in a notice posted near the hotspot or provide a note with details of the wi-fi hotspot name. If in doubt, ask the provider to confirm the name of their wi-fi hotspot.

[1] Some providers of public wi-fi access may require the user to purchase a product or service as a condition of access.
[2] Please refer to the Australian Government Stay Smart Online website – www.staysmartonline.gov.au - for further advice on online safety and security.

- **Avoid sensitive transactions -** A simple way of protecting your personal information is by not displaying it. Avoiding conducting sensitive transactions - such as online banking, sending a confidential email, entering passwords and shopping using a credit card – when using a public wi-fi hotspot. If you must make sensitive transactions, only use secure websites. If using a smartphone, consider using your mobile phone network (eg, your 3G or 4G network) rather than the wi-fi hotspot.

- **Look for the lock -** Wherever possible, use websites that are secured with encryption as this will protect information you send to, and receive from that website. An easy way to identify a secured website is to look at the web address. A secured website will show https:// instead of http:// (the 's' is for secure). Make sure to look for https on every page you visit, not just on the webpage that you use to sign in. A locked padlock or key in the browser window also shows that the website is secure.

- **Dig yourself a tunnel -** If you are a regular user of public wi-fi, consider using a Virtual Private Network (**VPN**). A VPN enables you to create a secure connection (or 'tunnel') through which you can send all your web traffic and gives you the security of a private network even though you're on a public one. You can get a personal VPN account from a VPN service provider.

- **Use the built-in security tools -** To begin with, check that the firewall on your device has been enabled. Always set your network type as public when you connect to a public Wi-Fi hotspot as this will block certain programs and services from running – such as file sharing. If using a smart phone, change your settings so that your phone asks permission to join a new wireless network. Disable wireless networking when you are not using it.

  If you are not sure how to enable any of these settings, try searching online to see whether the maker of your device provides an online support centre. It is likely that these are commonly asked questions for which advice is already available.

- **Keep your software up to date -** Keep your antivirus software and operating system up-to-date. Ensuring that you have the most recent updates and patches installed will fix security vulnerabilities and other problems that have been identified by the software vendor. If using a smartphone, you could look into available mobile apps which provide a package of security tools such as virus protection and remote lock or wipe.

- **Watch your back -** While it is important to keep the risks of using a public wi-fi hotspot in mind, you shouldn't forget about theft the old fashioned way – someone looking over your shoulder. It can be easy to get so absorbed in online activity that you may not notice someone taking note of information that is on your screen. If you can read the magazine of the person sitting nearby, they can probably read the screen on your laptop. An inexpensive solution is to buy a privacy filter, which is a film that adheres to the screen of your mobile device to block the sight from anyone viewing it from the side.

For additional information and assistance please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This information sheet is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to enquiries@oic.qld.gov.au.

Published 2 December 2014 and Last Updated 2 December 2014

Changes to legislation after the update date are not included in this document