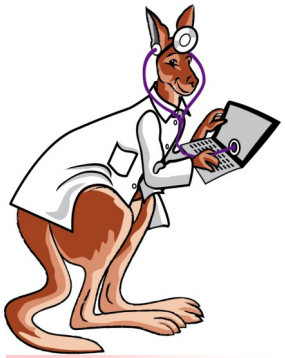
Aussie Mobile PC Doctor

How Safe IS Your Wi-Fi?

Volume 5, Issue 2

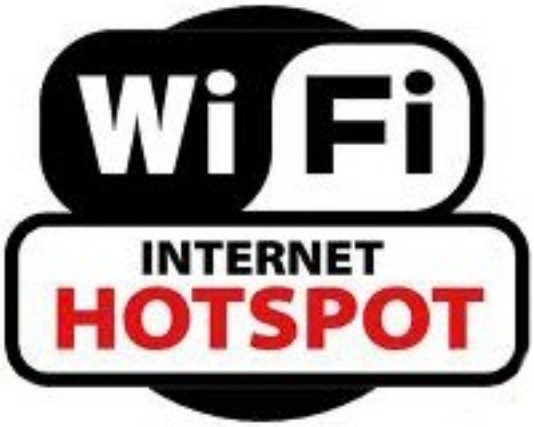
Whats Hot

- A second cross-platform Trojan downloader has been discovered that detects if you're running Windows, Mac OS X, or Linux, and then downloads the corresponding malware for your platform. Unlike the first one, which supported PowerPC Macs, this one does Intel x86 Macs. ." Just like last time, the Trojan downloader checks your operating system so it can pick which malware to download onto your computer. The Web-based social engineering attack relies on a malicious Java applet to install backdoors on Windows, Mac, and Linux computers. When you first visit such a compromised site, you are prompted to install the Java applet, which unsurprisingly hasn't been signed with a certificate. If you do so, the applet checks which operating system you have (Windows, Mac OS X, or Linux) and then drops a corresponding Trojan for your platform.



10 Tips for Working Securely from Wireless Hot Spots

The advantages of Wi-Fi hotspots are obvious. The use of wireless internet access is set to reach a total of 120 billion connections in 2015, due to growing support from major broadband internet service providers (ISPs). Wi-Fi hotspots have become a service which is used by businesses as a competitive differentiator to attract customers to other product offerings, layered on top of core offerings. Notebook PCs account for most connections, but the rate of smartphone and tablet access is increasing rapidly. But beware: "public hotspots" have been called that for a reason. They are open networks and therefore vulnerable to security breaches. They cannot guarantee your safety. When you connect to an unsecured Wi-Fi network, anyone on the same network potentially has access to your computer and to all your internet activities. They can snoop around in your emails and see what you've been doing on the internet, without needing your password. This applies to all hotspots – even to those that require pay-per-hour or monthly subscription fees. These are almost always unencrypted, so all your emails, passwords, security codes and other information can be visible to hackers lurking on the same



1. Disable your Wi-Fi adapter

When you're not at home or at work, it's a good idea to turn off your laptop or notebook's Wi-Fi capability when you're not using it. Otherwise your computer might connect to a malicious hot spot without your realizing it. Many laptops now have a Wi -Fi hardware button you can use to disable your Wi-Fi adapter. If yours doesn't, you can disable your Wi-Fi adapter using your operating system.

2. Try to choose more secure connections

Use a virtual private network (VPN)

It's not always possible to choose your connection type, but Internet security is critical. When you can, opt for wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, and encryption can help protect your computer from unauthorized access. For example, instead of using a public hot spot with no encryption, use a virtual private network (VPN). If your business does not have its own VPN, you can download and install free VPN software. The secu-

rity features of the different available networks appear along with the network name as your PC discovers them.

3. Protect your email with https

One way to protect your email messages in public is to select the https

or other secure connection option in your email account settings (if your email provider supplies one). This option may be called always use https, more secure connection, or something similar. Even if the email provider you use has a secure network, after you log on to your account on a public network, your information is no longer encrypted unless you use a more secure connection. An https connection, for example, which includes encryption, is more secure than an http connection

4. Make sure your firewall is activated

A firewall helps protect your PC by preventing unauthorized users from gaining access to your computer through the Internet or a network. It acts as a barrier that checks all incoming information and then either blocks the information or allows it to come through. All Windows operating systems come with a firewall, and you can make sure it's turned on.

5. Monitor your access points

Chances are that there are multiple wireless networks anywhere you're trying to connect. These connections are all access points, because they link into the wired system that gives you Internet access. So how do you make sure you're connecting to the right one? Simple—by configuring your PC to let you approve access points *before* you connect.

6. Disable file and printer sharing

File and printer sharing is a feature that enables other computers on a network to access resources on your computer. When you are using your mobile PC in a hot spot, it's best to disable file and printer sharing—when it's enabled, it leaves your computer vulnerable to hackers. Remember, though, to turn this feature back on when you return to the office.

7. Make your folders private

When the folders on your mobile PC are private, it's more difficult for hackers to access your files.

8. Encrypt your files

You can protect your files further by encrypting them, which requires a password to open or modify them. Because you must perform this procedure on one file at a time, consider password-protecting only the files that you plan to use while working in a public place.

9. Consider removing sensitive data from your portable computer

If you're working with extremely sensitive data, it might be worth taking it off your portable computer altogether. Instead, save it on a corporate network share or on a password-protected site, such as Windows Live SkyDrive, and access it only when necessary. This way, you have multiple safeguards in place. A few simple precautions can help make working in public places more secure. By selecting the best wireless Internet connections and adjusting settings, you can enjoy more productive and safer work sessions—no matter where you are.

10. Use your common sense

Avoid transactions that require a lot of personal information, for example shopping and banking.

Avoid giving credit card, insurance or social security numbers

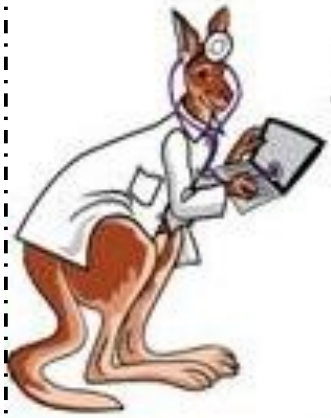
Create different usernames and passwords for different accounts so if one is hacked the others stay safe

Cookies remember usernames and passwords, making data breaches easier. So before you connect to a public Wi-Fi hotspot, delete your

browsing history and your cookies

Log out of websites when you've finished with them

If you follow these simple steps, you can help ensure that using Wi-Fi stays the huge benefit it's intended to be, making you more mobile, more independent and more efficient. And if you don't? Let's just say: "better safe than sorry".



Aussie *Mobile* PC DOCTOR

we come to you

IT SPECIALIST

- ✓ Over 30 yrs Experience
- ✓ No Call-Out Fees
- ✓ Door to Door Service
- ✓ Data Backup & Recovery
- ✓ Secure Wireless Networks
- ✓ Virus & Spyware Removal
- ✓ PC & Laptop Repairs
- ✓ Wireless Printer Set UP
- ✓ 48 HR Turnaround
- ✓ Private Tuition &

For All Your PC Needs

0497 872 847

20% Discount with this flyer