Windows The Official Magazine
Home | My Home

BUY STUFF TECH SUPPORT

True tech success stories

Is your wireless network running slow? Does your bandwidth allowance seem used up quicker and quicker each month? If you answered yes Gentle Reader, then you may need these tips on wireless network security.

Have you ever wondered why your wireless network slows down at certain times of the day? Or how you could have hit your quota for the month so early when all you do is surf the net and do some internet banking? You could be a victim along with countless other Australians of having internet bandwidth stolen from right under your nose, a result of an unsecured wireless network.

Having an unsecured wireless network and an internet connection is not only like leaving your front door wide open, its like putting all your things out on the side walk with a 'TAKE ME' sign attached. All over Australia, unsecured wireless networks are being leached by one or more computer users without the account holder's knowledge and it takes no technical skill or knowledge other than clicking a button to join the network.

In most cases leachers will use an unsecured wireless network just to get free internet connectivity. In addition to this, unsecured wireless networks are targeted by people intent on carrying out criminal activity such as hacking, fraud, money laundering and the download and sharing of illegal material such as abusive and denigrating pictures and movies including child pornography.

Having an unsecured wireless network also jeopardises the security of your private information and personal data. By leaving your wireless network unsecured you are allowing anyone access to traffic on your network which often includes personal information about you including emails, user names, passwords and documents.

All this can be to a greater part avoided by enabling wireless security on your wireless router. Wireless security is just like dragging all your possessions back in the house and putting a lock on your front door. As a Geeks2U technician, I come across customers with internet issues linked to unsecured wireless networks all the time. Here are four of the most effective ways a home user can secure their home network:

Geek of the month

Paul Pratley

Paul is an experienced wireless network engineer and has most recently worked as a computer forensic analyst with NSW Police. He has training in the analysis of a wide range of devices including computers, CCTV systems, mobile phones, GPS and other storage and handheld electronic devices and is recognised in Australian courts as an expert in the field of computer forensics.

"Having an unsecured wireless network is like leaving your front door wide open..."

1. Choose the highest level of security possible

There are a number of different types of wireless security and you should choose the highest level which is compatible with all of your devices. WEP encryption is the lowest level and is like having a locked fly screen door, not great but ok. WPA and WPA2 are much stronger forms of security, equivalent to having a nice solid front door with a deadlock. These can eventually be bypassed by someone intent on gaining access, but will keep most away.

2. Choose a strong password

Wireless security for home users relies on passwords for access to the wireless network. No matter what type of security you choose, if you have a weak password it will be easy to break into. Just think if everybody had keys to their front door which were smooth with no grooves how easy it would be to break in! A strong password is more than 8 characters with upper and lower case characters, numbers and symbols.

3. Change the default network name (ESSID)

Wireless routers pretty much all come with a set network name from the manufacturer. The network name indicates to your equipment which network they are joining as opposed to all the other wireless networks near you. This should be changed to something unique. Leaving it as the default name will cause problems with other people's networks near you sharing the same name and will attract people to try and break into it as it will appear to have not been set up properly.

4. Turn off broadcast of the network name (ESSID)

You can't steal what you can't see. Turning off broadcasting of the network name means that it won't appear automatically on other people's computers. Of course that means it won't automatically appear on yours either, but that's ok. You can set that up manually on each of your devices since you are going to know the name of the network, it's yours after all.