**To go, or not to go, wireless with your DSL connection**

Going wireless with Internet connections these days is turning into a trend, and one that many of us are starting to enjoy. The convenience of being able to stay connected at any spot, or two feet, or ten feet away from 'any spot', is delightful, we must admit. However, another buzz that has come out of wireless popularity is the security problem that joins it. Though security features are gradually advancing, it can't be assumed that having a password is sufficient to guard personal and confidential information on your computer when using a wireless router.

In short, it is safest not to go wireless with your business. There are too many ways for outsiders to hack in and it may not be worth taking the chances. To give an example, anyone with a laptop can sit outside your office building and use a 'packet sniffer' to read all the 'airborne' information that is travelling between your computer and the wireless router. In other words, it's not even necessary for a hacker to access your computer directly anymore to find information. Of course, there are also software programs that can continuously dig to find out passwords, so those don't always help either. Hackers are everywhere, and their life purpose is often just to figure out how things work, and see if they can win against a system. Often they succeed, and when they do, IT companies know that it's time to change course and find another way of 'ensuring' security. With a hard wire, the physical connection makes it almost impossible for a hacker to gain access – unless digging up your underground phone line is an option.

On that note, be aware that it is also unsafe to be free riding on other people's wireless connections. Some of them are honey traps, designed specifically to get your attention so that you will go online to say, do your banking, thus allowing the perpetrator to abuse your financial information. Sometimes this could be one of your neighbors, who you trust, but who also unknowingly have made their open wireless connections the perfect bate for hackers to secretly install monitoring software. If you ride on their waves, you run all the same risks of having your own computer spied on.

There are some cases, however, where providing wireless access is unavoidable. Let's say your company operates on an office campus, meaning that Internet needs to be available throughout your large property, or perhaps you own a café and need wireless access to draw customers. In such circumstances, keep in line with these security forces that will at least be a help to you, and constantly do scans to see who has been gaining access, or trying to gain access to your network:

**Have two Internet connections.** That's right, two, even if it costs more. Keep the wired-only connection for the really top-secret operations (e.g. company trades, products in development, banking passwords and numbers, etc.). Allow wireless connections for general purpose use to your employees or customers but don't allow the two connections to communicate with each other. In other words, a wireless connection should not give access to the company's server where network files are stored.

**Use a MAC address filter** to determine who is allowed access to your network. A MAC address is somewhat like a serial number that is found in computer hardware and acts as an identity card to a router. If the router sees that the user is registered in its list of allowable clients, it will give access. If not, then it will deny access. This method can also be susceptible to hacking by those who know how to

disguise themselves, or steal MAC address identities, but at least it puts more of a barrier up. Also, this scenario probably wouldn't work well in the café scenario, since a store clerk might have to configure the router's client list every time a customer wants wireless access to the Internet.

**Set up a loooong password**, as long as possible. It just makes it all the more harder for a hacker's software to figure out, kind of like a long equation. If you use security that allows for 26 characters, use them all, and mix them up. Again, hard to do in the café, but hey, at least you can ensure people are actually buying from you to use the connection by giving out the password on receipts every time someone orders a coffee. Change the password often if you do this to avoid the numbers getting passed around too much.

**Change the SSID.** This is the name of the wireless connection people see when they are searching for a network to join. Manufacturers of routers send out their equipment with the name already in place, and it usually takes the brand name of the company or something similar. These names are seen as an easy target by hackers because they appear insecure. After all, if you didn't change the SSID, you probably didn't change the security encryption either.

**Use Firewalls**. That's plural. Make sure there is one running on the wireless connection and also one running on the computers since, after all, the devices are communicating with each other during an entire Internet session.