Security an increasingly vital issue for wi-fi users

Wireless networks, or wi-fi, have become very popular.

But a big issue is security. Where once we could rely on the doors and locks to control access to our buildings and it's internal networks, we are now at the mercy of anyone within wireless networking range of the wireless access points (Waps).

If the wi-fi network is not secured, any person within range of the Wap will be able to connect to the network and view traffic as though they were plugged into the network.

In 2007, Rits carried out a review of the security configuration of Waps in the greater Dublin area. This review covered Dublin 2, the IFSC, Citywest, Parkwest, Sandyford and Leopardstown. More than 2,700Waps were assessed in this review, and 29 per cent of these had no security of any type configured.

To ensure relevance of results, wireless hot-spots in cafés have been excluded from the results.

Rits repeated this review earlier this year and this time around, there were more than 4,000Waps included, with an increase to 32 per cent of unsecured Waps. This is very disappointing, particularly given the focus on the Make IT Secure week, and the coverage that the Eircom WEP issues got last year.

It was also disappointing to note the slow pace of migration from WEP to WPA on the installed base of Dublin Waps.

The two main risks to the network from wi-fi installations are unauthorised users getting access to the internal, private network and information assets, and intercepting and accessing information f lowing between wi-fi devices and the Wap.

Passwords can be recorded, information passing on the network analysed - accessing data such as credit cards, VoIP phone calls recorded etc. If the malicious user wishes to use the internet connection for nefarious purposes, it will be investigated as though it came from the owner of the internet connection.

The latter one is a common risk and there are many pieces of anecdotal evidence of people having huge internet connection traffic loads when they are light users themselves.

This is a particular risk in built-up areas, as there are often multiple unsecured wi-fi connections for the internet available.

The accessing of a wi-fi Wap without the consent of the owner and using it to gain access to other services has been outlawed in Britain, and there are prosecutions pending.

In Berwick-upon-Tweed, two men were arrested for illegally using a Wap for accessing e-mail. Networking giant Cisco released a recent survey showing 11 per cent of remote workers admitted to using someone else's internet connection without permission, a rise from 6 per cent from their previous survey.

If you have a Wap installed for business or home use, connected to your internal

network or the internet, make sure that security is enabled on the device.WPA2 is recommended.

It is the responsibility of any organisation deploying or selling wireless networking technologies to explain the risks to their customers, and to assist them in implementing appropriate controls.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com