

# Watch out there's a Wi Fi Thief about **How vulnerable are you?**

## **The report, by WEB, the WiFi Education Bureau, entitled "Watch out, there's a Wi Fi Thief About", estimates that thousands of businesses in Wales are open to sabotage by kerbside snoopers.**

Similarly a high proportion of home users are unprotected from neighbourhood snoopers who can view all their documents and spy on their online activity.

Commissioned by Cardiff-based software and security company Aytel Systems, the survey took a snapshot view of Wi Fi access points in Cardiff, revealing the alarming extent of network vulnerability.

The survey comes at a time when Wi Fi sales are rocketing. Research from analyst firm GfK revealed that some 380,000 Wi Fi units were sold in the first quarter of 2006.

Without entering any networks, researchers took a car trip in the city, using a normal Wi Fi enabled laptop to identify countless unprotected computer systems and home pcs in the city.

Within one minute of the start-point an unsecured wireless connection was flagged up. Using a default password, this system could have been infiltrated say the survey's authors.

After 1 hour and 2 miles, 550 wireless networks were flagged in the business area, 60 of which were unsecured.

A subsequent 1 hour surveillance of a residential area of the city revealed that 320 Wi Fi sources were visible, 60% of which were unsecured.

WEB has called for an urgent public information campaign to immediately alert businesses and the public to secure their Wi Fi broadband connections at home in the office.

In the interim a free guide has been posted by WEB on [www.wifieducationbureau.org](http://www.wifieducationbureau.org) to show people how to prevent their networks and home pcs from being snooped.

Pete Patel, MD of Aytel Systems, the main sponsor of WEB, said: "Unsecured wireless connections leave both businesses and residential properties open to hackers, who are potentially able to use Internet connections and access personal documents without being traced. This is another potential source of identity theft.

Part of the problem is that routers are supplied as 'plug and play' and people do not realise the security aspects of this. Many routers are therefore left without password protection and can be accessed even on a palm top.

Our advice to home users is to immediately shut down their home Wi Fi and consult their router manual in order to protect their system from outside access."

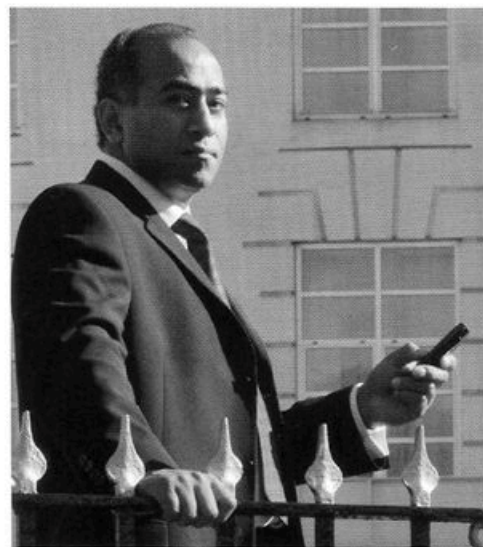
WEB warns that once kerbside hackers enter Wi Fi networks they can change passwords rendering users unable to access their own computer systems.

Hackers can also download information using the unsecured network. IP addresses can be scanned and admission gained into shared networks. People can even be locked out of their own servers.

Companies are advised to contact their IT specialists immediately to ensure their networks are secure, so that only authorised personnel are able to access Internet connections and shared networks.

**For further information contact  
[www.wifieducationbureau.org](http://www.wifieducationbureau.org)  
Tel: 029 20 655 655**

Note: No computer network or home pc system was infiltrated during the compilation of the survey ■



**Talk of the Town:**  
Pete Patel of Aytel Systems says  
Wi Fi systems are vulnerable to attack