'Evil twin' fear for wireless net

People using wireless high-speed net (wi-fi) are being warned about fake hotspots, or access points.

The latest threat, nicknamed evil twins, pose as real hotspots but are actually unauthorised base stations, say Cranfield University experts. Once logged onto an Evil Twin, sensitive data can be intercepted. Wi-fi is becoming popular as more devices come with wireless capability. London leads the global wi-fi hotspots league, with more than 1,000. The number of hotspots is expected to reach 200,000 by 2008, according to analysts. "Users need to be wary of using their wi-fi enabled laptops or other portable devices in order to conduct financial transactions or anything that is of a sensitive or personal nature," said Professor Brian Collins, head of information systems at Cranfield University.

"Users can also protect themselves by ensuring that their wi-fi device has its security measures activated," he added. BT Openzone, which operates a vast proportion of public hotspots in the UK, told the BBC News website that it made every effort to make its wi-fi secure. "Naturally, people may have security concerns," said Chris Clark, chief executive for BT's wireless broadband.

"But wi-fi networks are no more or less vulnerable than any other means of accessing the internet, like broadband or dial-up." He said BT Openzone, as well as others, have sophisticated encryption from the start of the login process to the service at a hotspot. "This means that users' personal information and data, logon usernames and passwords are protected and secure," said Mr Clark.

In the vast majority of cases, base stations straight out of the box from the manufacturers are automatically set up with the least secure mode possible, said Dr Nobles. Cybercriminals who try to glean personal information using the scam, jam connections to a legitimate base station by sending

a stronger signal near to the wireless client. Anyone with the right gear can find a real hotspot and substitute it with an evil twin. "Cybercriminals don't have to be that clever to carry out such an attack," said Dr Phil Nobles, a wireless net and cybercrime expert at Cranfield. "Because wireless networks are based on radio signals they can be easily detected by unauthorised users tuning into the same frequency."

Although wi-fi is increasing in popularity as more people want to use high-speed net on the move, there have been fears over how secure it is. Some companies have been reluctant to use them in large numbers because of fears about security. A wireless network that is not protected can provide a backdoor into a company's computer system. Public wi-fi hotspots offered by companies like BT Openzone and The Cloud, are accessible after users sign up and pay for use. But many home and company wi-fi networks are left unprotected and can be "sniffed out" and hi-jacked by anyone with the correct equipment. "BT advises that customers should change all default settings, make sure that their security settings on all equipment are configured correctly," said Mr Clark. "We also advocate the use of personal firewalls to ensure that only authorised users can have access and that data cannot be intercepted." Dr Nobles is due to speak about wireless cybercrime at the Science Museum's Dana Centre in London on Thursday.