'Evil twin' hotspots are a new menace for Wi-Fi Internet users

January 20 2005

'Evil Twin' hotspots: the latest security threat to web users, according to wireless internet and cyber crime experts at Cranfield University, academic partner of the Defence Academy of the UK.
"So-called ‘Evil Twin’ hotspots present a hidden danger for web users," explained Dr Nobles.
In essence, users think they’ve logged on to a wireless hotspot connection when, in fact, they’ve been tricked to connect to the attacker’s unauthorised base station. The latter jams the connection to a legitimate base station by sending a stronger signal within close proximity to the wireless client – thereby turning itself into an ‘Evil Twin’.

Once the user is connected to the ‘Evil Twin’, the cyber criminal can

intercept data being transmitted, such as bank details or personal information. “Cyber criminals don’t have to be that clever to carry out such an attack,” added Dr Nobles. “Because wireless networks are based on radio signals, they can be easily detected by unauthorised users tuning into the same frequency."

Dr Phil Nobles, wireless internet and cyber-crime expert at the university, will be speaking at the wireless crime event at the Science Museum’s Dana Centre – the UK’s only venue for adults to discuss controversial science – on Thursday 20 January 2005 from 19.00-20.30. He will explain the latest security threats to internet users and will also discuss wireless computing vulnerabilities that exist at present.

Unwitting web users are invited to log in to the attacker’s server with bogus login prompts and can pass sensitive data such as user names and passwords which can then be used by unauthorised third parties. This type of cyber crime goes largely undetected because users are unaware that this is taking place until well after the incident has occurred.

Attacks can also take the form of degrading the performance of the client network or a complete denial of service. The attacker can get the victim’s network to collude in the attack so that the degradation in network performance is less likely to be detected.

Professor Brian Collins, Head of Information Systems Department at Cranfield University, said: “Web users who use wi-fi networks should be on their guard against this type of cyber crime.

“Given the spread and popularity of wireless internet networks – which, according to data research company IDC, is predicted to increase from 7,800 to nearly 22,000 by 2008 – users need to be wary of using their wi-fi enabled laptops or other portable devices to conduct financial transactions or anything of a sensitive or personal nature, for fear of

disclosing this information to an unauthorised third party."

Professor Collins continued: "Users can also protect themselves by ensuring that their wi-fi device has its security measures activated. In the vast majority of cases, base stations taken out of the box direct from the manufacturer are configured in the least secure mode possible."

Cranfield University acknowledges that this is a new area of cyber crime where more research is required.

Lisa Jamieson, Head of Programmes at the Dana Centre, added: "Half of all business wireless networks in this country have inadequate security controls in place, making their information vulnerable to attack. At the Dana Centre we have in place a hardened firewall which protects the public using our wireless network from electronic attack.

"Through this event, the audience will be more aware of the potential risks and can find out how to ensure that they don't become another cyber victim statistic."