



November 23, 2006

'Evil twin' Wi-Fi hacks target the rich

Hackers after high net worth individuals in wireless scam

By Iain Thomson

Locations popular with high net worth individuals are being targeted by hackers using phoney wireless access points to steal personal information.

So called 'evil twin' attacks involve putting a wireless access point near a commercial hotspot and giving it the same name.

When the unsuspecting user logs-on to the bogus hotspot their traffic is monitored, personal information can be gathered and in some cases the computer can be hacked remotely.

"We are not seeing these in Starbucks much, as there is not much value in a MySpace login," said Richard Rushing, chief science officer at Wi-Fi security firm AirDefense.

"Instead they are targeting the locations where the better-off are hanging out because they have something worth seeing."

Rushing explained that 'evil twins' had recently been found in the first class lounge of an international airport, and in garages that specialise in expensive cars that offered Wi-Fi while you wait. Train station lounges had also been targeted.

This form of attack uses social engineering and hacking, since a key part is lulling the suspect into a false sense of security but mimicking a legitimate service.

It also shows the extent to which hackers are having to deal with information overload from skimming too much information to process effectively.

The attacks are a growing problem for security managers. While corporate Wi-Fi networks are increasingly being locked down on installation, it is the individual user who is now seen as the weakest link.

Also appeared in:

