

**Revealed: How a Pringles can cracked the City's most secret networks. Richard Fletcher slid through the cyber defences of dozens of London firms with just a car, a laptop and an empty snack can. 'Companies have opened up an enormous back door into their corporate networks'.**

**The Telegraph, Sunday March 10 2002  
Richard Fletcher**

More than 40 City firms have left their computer networks wide open to "amateur hackers" who can access their systems using just a normal laptop computer and an empty snack carton, an investigation by The Sunday Telegraph can reveal.

Not only are the firms - which include one of the UK's largest technology companies and a leading European investment bank - leaving their networks open to attack, but thousands of amateur hackers are using the shocking security flaw to "piggy back" corporate networks and gain free high-speed access to the internet.

Numerous hackers websites - which can be found using any internet search engine - not only reveal the location of the firms vulnerable to attack, but also provide hackers with the software and detailed instructions necessary to access wireless networks.

Once they gain access they can read confidential e-mails and other secret data including trading records, using code-breaking software to unscramble even the most heavily encrypted files.

Last week The Sunday Telegraph - in conjunction with I-Sec, one of Britain's leading independent security firms - identified more than 60 vulnerable networks during a controlled 45-minute drive around the City of London.

"I hope this exercise raises awareness at board level of the risk that this security flaw poses to confidential information," said Geoff Davies, the managing director of Brighton-based I-Sec.

This shocking breach of commercial security centres on the increasing use of wireless networks, which give employees quick and easy access to a company network when using a laptop computer.

In an increasing number of buildings, employees no longer have to connect their laptop or handheld computer to the system with wires or cables, but can gain access using a wireless network.

For corporate customers and staff - more and more of whom are using laptops - wireless networks not only save staff time, but also generate huge cost savings.

Last year worldwide sales of wireless equipment increased by 80 per cent to more than \$1bn, according to IDC, the IT research consultancy. The networks are also being installed in airports, hotels and coffee shops.

But in the US the security flaws in wireless networks have prompted a number of government departments - led by the Lawrence Livermore National Laboratory (a weapons laboratory) to switch off their wireless networks.

The decision sent shockwaves through the IT sector, yet during a 45-minute drive around the City of London The Sunday Telegraph discovered 42 wireless networks that were completely unprotected. These were companies that had not even bothered to switch on the basic encryption security features on their equipment.

All these networks were identified using Netstumbler, freely available software which can be found in seconds on the internet. The only other equipment necessary was a pounds 60 network card and a converted tube of Pringles crisps, the dimensions of which make it ideal to convert into an antenna.

The 45-minute drive began on the western edge of the City near Spitalfields. Netstumbler identified its first unprotected wireless network before we had even driven off.

As well as revealing the identity of the network, Netstumbler also identifies the manufacturer of the wireless system, the strength of the signal and the channel number or wavelength.

But most importantly the software - which works by constantly sending out a message requesting access to wireless networks and then analysing the responses - can detect whether a network is using WEP, the security system for wireless networks.

After driving 500 metres, Netstumbler had already found seven unprotected networks. We drove on, although a hacker would have been able to access the majority of these networks simply by adjusting the settings on his network card and working in his car.

On Farringdon Street we found an unprotected wireless network bearing the same name as an FTSE250 technology company whose headquarters stood just yards away. Even when a network did not bear the company name, working out its identity was not difficult.

Driving past the London headquarters of a leading European investment bank elsewhere in the City, Netstumbler found a wireless network bearing the name "equities trading desk". Others bore company initials or the name of specific departments, such as "IT projects room" - another unprotected network.

But many of the networks had not even been renamed and still bore the default identities set by the manufacturer.

"The biggest problem is that people are just taking these things out of the box and plugging them in," Davies explains. "The fact that a network still bears the default name suggests that they haven't even changed the basic settings. It is an invitation to hackers. Default settings suggest to a hacker that security is low on the priority list of the system administrator. They know that they will almost certainly get access in seconds and then remain undetected."

As we turned into Cannon Street, Netstumbler found six more networks and by the time we reached Monument, we had found 25 networks, only three of which had any protection.

At no point did The Sunday Telegraph or I-Sec attempt to log onto any of these wireless networks or to download confidential information. But had we done so, in the vast majority of cases the system would have assumed that we were a legitimate employee, says Davies.

Other IT security experts agree and explain that with the help of additional software we would not only have been able to access the internet, but also e-mail and any internal systems, including databases containing confidential client data.

"Companies have opened up an enormous back door into their corporate networks," warns Davies.

**Full article can be found in The Sunday Telegraph, 10<sup>th</sup> march 2002**