



## Wi-Fi

July 2007

**Do you want to extend your company network, but have run out of connection points - or want your staff to have Internet /email access whilst travelling? Wi-Fi might provide the solutions.**

**Our E-Business Advisers discuss this no-wires connection option:**

### 1. What is Wi-Fi - Wireless Fidelity?

Wireless Fidelity (Wi-Fi) is the standard that ensures straightforward inter-connection of different vendors' equipment in an easy-to-use, high-speed Wireless Local Area Network (WLAN).

Wi-Fi can liberate users; no plugs and no wires are needed.

Wi-Fi comprises an access point and a wireless card for your PC, laptop, or any other device which can be networked. Many devices are starting to be built with this Wi-Fi card in-built.

As long as you're within 100m indoors or 300m outdoors, then information can be transmitted between them.

Wi-Fi transmits and receives information through walls and ceilings, and eliminates the need to network cable your business.

You can also use Wi-Fi when travelling - Wi-Fi networks (known as "Hot Spots") are also found in public places such as hotels, airport lounges, railway stations and other locations where numbers of travellers gather.

This is one of the fastest-growing segments of Wi-Fi service.

More and more business travellers and mobile professionals need fast and secure Internet access wherever they are.

To cater for this demand, Wi-Fi "Hot Spot" networks are increasingly being found in many locations (such as pubs and coffee houses) in urban areas, or in hotels for their business traveller guests.

A user simply buys a voucher that then allows them to use the Wi-Fi Hot Spot.

Another huge growth area is in home computer networks.

A recent US report says that 59% of US homes with a network - for example, 2 or 3 PC's sharing a broadband connection - use a Wi-Fi network to achieve this.

The big advantage in a home setting is obviously the lack of cables. (Source: CNET news.com)

### 2. The technical bit.....

Wi-Fi is a play on the 1950s term Hi-Fi, ("High Fidelity"), used as a description of the then-best in sound reproduction.

"Wi-Fi" was introduced as a trademarked alternative to the previous technical label - IEEE 802.11, which was based on the name of the networking standards committee.

The term Wi-Fi was coined in 1999 by the organisation now known as the Wi-Fi Alliance.

This organisation oversees the technical performance of products which utilise W-Fi



# Fact Sheet

technology. Products which pass the Alliance tests are given the registered trademark Wi-Fi.

Since 1999, there have been improvements in the standards - mostly related to connection speed.

Wi-Fi is developing fast, which means there are a number of standards in use, with very similar names, not all of which are compatible with each other.

We've had the 802.11 "a" standard, the 802.11 "b" standard, and we are currently on the 802.11 "g" standard.

'a' and 'b' aren't compatible - they use different frequencies to transmit their signals. Wi-Fi 802.11 'g' is an advance on 'b', and is also compatible with it. Many existing Hot Spots, for example, use 'b'.

Although this sounds confusing, a Wi-Fi "g" standard laptop will connect to a "b" standard Hot Spot - but will only work at the lower speed that exists within the "b" standard - 11Mbps compared to the "g" connection speed of 54Mbps.

However, many new pieces of equipment will allow connection at a, b or g standards - look for this logo on the equipment:



### 3. How about security?

When you buy Wi-Fi equipment, it is likely that you will find the security settings switched off.

This default allows maximum access to Wi-Fi wireless networking, but it also allows unauthorised access to your network!

Recently, the BBC reported on how an empty can of "Pringle" crisps could be made to help snoopers spot Wi-Fi networks open to attack.

A security company helped demonstrate that a directional antenna, made with a "Pringles" can, significantly improves the chances of finding the Wi-Fi wireless computer networks being used by firms in London's financial district.

The exercise, conducted using this homemade antenna, found that over two-thirds of computer networks were doing nothing to protect themselves - they were open to all to spy on.

All the firms could easily have stopped hackers by making a few simple changes to the set-up of their wireless networks.

The simple solution is to ensure security settings - such as WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) are switched on before you begin using the network.

Additionally, because Wi-Fi is seen as a key technology by key market leaders such as Microsoft and Intel, a great deal of effort is going into creating even more secure arrangements.

(For example, Intel released a range of microchips - Centrino - particularly suitable for notebook computers, with an integrated WLAN Wi-Fi capability).

### 4. Where are Hot Spots?

There are literally thousands of Hot Spots in the UK and abroad - with an increasing number day by day.



# Fact Sheet

Best estimates for the UK range around the 40,000+ mark, with well over 100,000 in the USA

## 5. Useful Links

[www.wi-fi.org](http://www.wi-fi.org) -  
Web site of the Wi-Fi Alliance

[www.bt.com/openzone](http://www.bt.com/openzone) -  
Web site for the BT Openzone Wi-Fi offering

*Disclaimer: we have no commercial links with this company or its products, and its appearance in this fact sheet is not an endorsement.*