



Wi-Fi (Internet) Leeching

We have all seen adverts in the free English Language Publications offering Internet access with a one off payment and no monthly fees.

At first sight these offers appear to be too good to be true and unfortunately for takers of this service they are.

Anyone who uses these services normally receives an antenna, which generally costs no more than £100, which is then connected to an existing neighbouring wireless network.

This practice is known as Wi-Fi Leeching.

"So I use a neighbour's Internet Access Point, what is the problem?"

Wi-Fi leeches attach to non-secured wireless networks without the owner's knowledge or permission. The "Leech" then uses this connection to access the Internet. In many countries this form of unauthorised Internet access is illegal and in some cases prosecution has been brought against the offenders.

"But I haven't stolen anything?"

Most suppliers of this "leeching" service defend this practice by saying that the owners should have secured their access point and "how can it be stealing if you're not taking anything". However just because the data being stolen is not a solid 3 dimensional object it is still classed as stealing.

If you were passing a neighbour's house and their front door was open it does not give you the right to walk in. And should you take something then it's a crime.

An unsecured access point is like an open front door.

"But they don't have to pay extra for me using their connection?"

Somebody is paying for the bandwidth, typically the owner of the access point or his or her Internet Service Provider (ISP).

The owner will also be liable to a download limit, which normally if they exceed, they have to pay for.

By “leeching” the Internet connection you will be taking some of this download limit and not contributing to the cost of the Internet connection. i.e. stealing from the authorised owner of the access point.

“But they don’t know who I am?”

Should somebody suspect that their Internet access point is been “Leeched” it is not difficult to find who is connected to their connection.

All access points have a utility to display who is connected wirelessly to the access point. This utility displays the IP Address, Mac address and normally their computer name.

The Mac Address is unique to every network card and once tracked down it is a 100% accurate way to prove which computer made the connection.

“But what if they can’t trace me?”

If the owner of the access point suspects that their connection is or has been leached they can simply enable wireless security.

This prevents connection to the access point unless the correct encryption code, or password, is known.

Therefore the too good to be true Internet offer turns out to be.... just that!