

## BBC NEWS / TECHNOLOGY

[Graphics Version](#) | [Change to International Version](#) | [BBC Sport Home](#)

[News Front Page](#) | [World](#) | [UK](#) | [England](#) | [Northern Ireland](#) | [Scotland](#) | [Wales](#) | [Business](#) | [Politics](#) | [Health](#) | [Education](#) | [Science/Nature](#) | **[Technology](#)** | [Entertainment](#) | [Video and Audio](#) | [Programmes](#) | [Have Your Say](#) | [Magazine](#) |

Friday, 27 April 2007, 11:53 GMT 12:53 UK

### How to keep your wi-fi network safe

By Paul Rubens



**With growing numbers using wi-fi in their homes, Paul Rubens looks at how good security is on these networks.**

In less than two minutes hackers can defeat the security measures protecting many home wireless internet connections.

Defeating these measures could let them capture passwords, steal confidential information or download illegal pornographic material using the connection.

Many home internet users rely on an encryption system called Wired Equivalent Protection (WEP) to stop others using their wi-fi link, even though WEP has long been known to be flawed.

In early April three cryptographic researchers at the Darmstadt Technical University in Germany revealed a method of exploiting the flaws far more effectively.

Before now it took at least 20 minutes of monitoring the airwaves before it was possible to break in to a wireless network protected by WEP.

Now, armed with a program written by the researchers, it is possible to break in to the same network far faster.

"Breaking in to a WEP protected network is now very easy to do," said Erik Tews, one of the researchers.

"Doing it in 60 seconds is realistic, or five minutes in the very worst case. We think now that WEP is really dead and we recommend that no-one should use it."

In its place he recommends an encryption system called Wi-fi Protected Access (WPA),

introduced four years ago to replace WEP. "We have had a very close look at WPA and we can't find anything to exploit," he said.

The only known way to defeat WPA encryption - and WPA2, a newer version - is to use what is known as a brute force dictionary attack.

This involves trying millions of different words or combinations of words from in the hope of stumbling upon the correct password.

### Legal fears

There are good reasons for ensuring a home internet connection is as secure as possible, said Struan Robertson, a technology lawyer at legal firm Pinsent Masons.



"Although home internet users are not responsible for illegal activities carried out by hackers hijacking their internet connection, they do risk having their computer equipment seized by the police," he said.

"If your internet connection is used by a hacker to download illegal pornography, the problem is that the police are likely to come knocking on your door.

"There's a good chance that you will lose your computer while they take it away for forensic analysis and you will then have to go through the painful process of clearing your name with the police who are investigating," he said.

And the consequences could be far more serious for anyone using their home internet connection for business purposes, said Simon Halberstam, head of e-commerce law at Sprecher Grier Halberstam.

*"WEP is broken"*

**Amit Sinha**

"If you fail to take appropriate technical measures to protect personal data by using a flawed encryption system like WEP you could be breaking the Data Protection Act, and face a fine or even imprisonment," he said.

Yet net providers like BT - one of Britain's largest - continue to put customers at risk by supplying wireless routers pre-configured to use WEP rather than WPA.

"The reason we have gone with WEP is that it will work straight out of the box. Not all laptops or other wireless devices can or do use WPA," said a BT spokesperson.

"There is a small risk from a determined and skilled hacker, but it requires considerable skill and knowledge to break WEP. It is extremely unlikely that you would encounter such a hacker."

### Tool time

This may have been true five years ago but cracking a WEP-protected network is now trivial with easy-to-use tools available on the internet.

There are software suites which enable script kiddies - unskilled wannabe hackers - to break in to neighbours' networks without leaving their bedrooms.

The majority of routers are sold without any encryption pre-configured at all, and although buyers can activate WPA encryption themselves, many do not.



"There is a lot of fear about switching on encryption," said Rob Falconer, sales and marketing manager at router manufacturer Belkin, which supplies its wireless devices without encryption.

"But we always recommend using WPA or WEP as a bare minimum and we try to make it as easy as possible."

Although customer security is important, financial considerations come first, he said.

"If we shipped them with WPA encryption turned on and unique passwords, our costs would go up dramatically. At the moment we can't see a cost-effective way of doing that."

So what is the best way to protect a home wireless network?

Amit Sinha, a wireless security expert at security consultants AirDefense, dismisses many of the security features - such as MAC address filtering and hiding the name of a home wireless network - offered by wireless routers, because these can be circumvented in seconds by anyone using tools such as Aircrack-ng.

He says home users should always change the password on their router, but concludes that effective encryption is the best solution.

"WEP is broken, so I recommend turning on WPA with a non-dictionary password," he said.

"If you use one which is long enough - at least 20 characters - then it becomes unfeasible for a hacker to mount a brute force attack, because finding your password would take longer than the entire history of the universe," said Mr Sinha.

---

[E-mail this to a friend](#)

---

#### **Related to this story:**

[Switch on for Square Mile wi-fi](#) (23 Apr 07 | Technology )

[Teachers want wi-fi risk research](#) (23 Apr 07 | Education )

[Two cautioned over wi-fi 'theft'](#) (17 Apr 07 | Hereford/Worcs )

[Belfast firms 'ignore wi-fi risk'](#) (24 Mar 05 | Northern Ireland )

[Wireless users 'do more online'](#) (26 Feb 07 | Technology )

[Q&A: Wi-fi explained](#) (08 Mar 06 | Technology )

## RELATED INTERNET LINKS

[Air Defense](#)

[Wi-fi Protected Access](#)

[Darmstadt attack on WEP](#)

The BBC is not responsible for the content of external internet sites

---

SEARCH BBC NEWS:

search

---

[News Front Page](#) | [World](#) | [UK](#) | [England](#) | [Northern Ireland](#) | [Scotland](#) | [Wales](#) | [Business](#) | [Politics](#) | [Health](#) | [Education](#) | [Science/Nature](#) | **[Technology](#)** | [Entertainment](#) | [Video and Audio](#) | [Programmes](#) | [Have Your Say](#) | [Magazine](#) |

---

[NewsWatch](#) | [Notes](#) | [Contact us](#) | [About BBC News](#) | [Profiles](#) | [History](#)

[^ Back to top](#) | [BBC Sport Home](#) | [BBC Homepage](#) | [Contact us](#) | [Help](#) | [©](#)