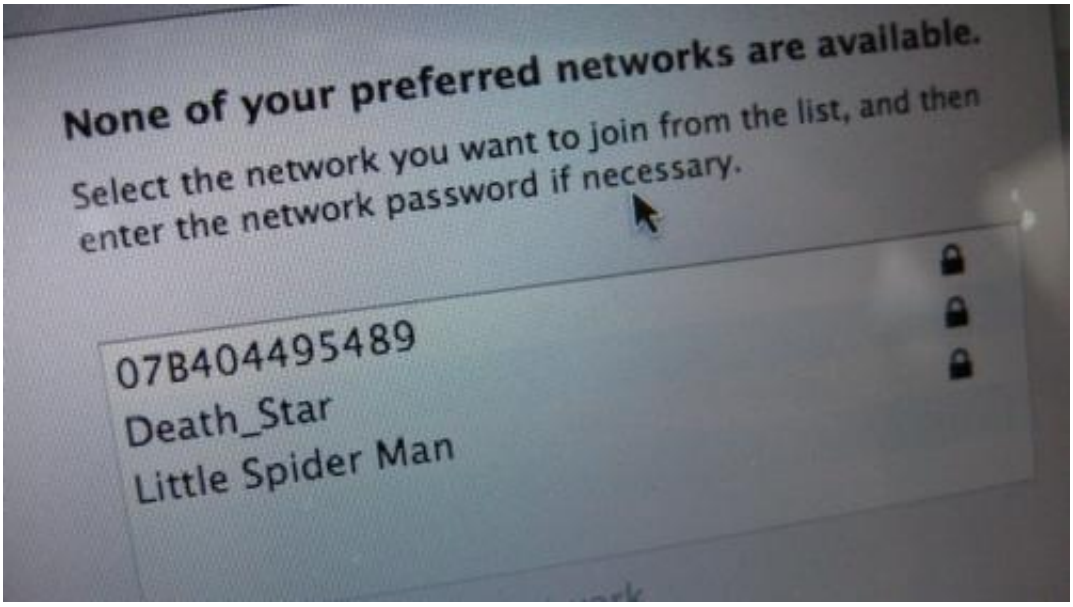
Explainer: Is your Wi-Fi secure?

May 21 2014, by Andrew Smith



You can trust some but not others. williamhartz, Credit: CC BY-NC-SA

James Lyne from IT security firm Sophos recently carried out a two-day public awareness exercise as part of the InfoSec 2014 conference.

In a low-emission variation of war driving, Lyne cycled around the streets of central London with a Raspberry Pi strapped to his bike. As he rode, he collected all the security details from wireless networks that had been left publicly visible by their owners.

During this two-day cycle ride, Lyne revealed that around 23% of the 81,743 wireless networks he identified were still insecure.

Lyne has done the same in San Fransisco as part of Project Warbike, eliciting similar results. Others, such as the Queensland Police, have done it too. All aim to show just how easy it is to access Wi-Fi networks if those running them don't take simple steps to secure them.

How the crooks get in

There are lots of naughty people out there, and while it's unlikely that your wireless network would be specifically targeted by cybercriminals, the likelihood exists that someone could see your exposed system and take advantage in one way or another.

If a wireless network is not secure, someone with more malevolent intentions than James Lyne can use a free network scanner to access it and redirect its traffic. That enables them to collect all manner of data which, in time, could easily reveal confidential information about you. Some network scanners are able to collect all network traffic from a target computer. Which means they could reassemble the web pages you visit and possibly even your Skype calls.

Basically, it's the online equivalent of leaving your keys in your front door for days or weeks on end.

If your wireless network is using WEP or WPA, please stop now. These are older methods of ensuring your wireless network offers a secure connection. The encryption behind these security protocols has long been compromised. They are the proverbial red rag to a bull for wannabe hackers, who know the weaknesses and exactly how to exploit them.

Sadly these protocols are still being used. Individuals and organisations installed WEP and WPA wireless access points back when they were secure but haven't updated their security, even though the ability of cybercriminals to compromise systems has advanced.

Currently the best wireless security option is WPA2, where the strength of the encryption has been increased above that of WEP and WPA.

Depending on your own model of home wireless access point, you should be able to change the settings via your web browser. This will force you to change the wireless key on your access point as well as all devices, so avoid doing it when a loved one is watching Netflix.

There has been advice on hiding your wireless network, which will discourage the prying eyes of amateur hackers. This works by entering a blank network name in the wireless network device settings or selecting the hidden option if one is available. Still, most decent wireless network scanners, will easily find a hidden wireless network.

Beware the public hotspot

Public hotspots are a great thing and I often wish there were more of them. Many cafes, restaurants and shops offer them so you can continue to go about your online business on their premises. It's something I often make use of when writing for The Conversation.

But, there is always a price to pay for free internet access. Just because your favourite coffee chain is giving it to you doesn't mean you should be complacent. I could easily scan that wireless network and see what you are doing, which means that these are not places to complete important financial transactions or share your secrets.

An excellent example of public wireless insecurity, is firesheep developed by Codebutler in 2012. This web browser plugin would capture any publicly broadcast cookies from a login session and give you illicit access to other people's accounts.

You can easily check how secure a wireless network is from your

computer or smartphone. When you join the network, the system will announce the type of security you need to use to gain access. There are many helpful guides, that can offer insight into how you could do more to protect your system.

Or you could use some of the network scanners freely available on the internet. But be warned, you are using the same tool that others could use to compromise your system. When you are using public wireless, you should consider what you are doing. Opening your browser to access your online banking details may not be the wisest move.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: Explainer: Is your Wi-Fi secure? (2014, May 21) retrieved 2 May 2024 from https://phys.org/news/2014-05-wi-fi.html