Perth commuters face cyber threat via free wi-fi

May 13 2015, by Chris Marr

"The problem with WPA is that you need a password, and on a bus or train it's probably going to be an open hotspot which means not having any security," Prof Woodward says. Credit: Nicolas Nova

In light of the proposal to introduce free wi-fi throughout Perth's public transport network be aware that there are increased cyber security risks, warns ECU computer security expert Professor Andrew Woodward.

Wi-fi is a local area network that uses radio signals instead of hard wires

to send and receive information, as such it is much easier to eavesdrop on a wi-fi network than a wired network.

Using generally available technology and software, it is possible to intercept and capture the traffic on somebody else's session when you are sharing the same wi-fi hotspot.

"In a confined environment such as a bus or train, you are more susceptible to someone trying to do something malicious because you're not mobile," Prof Woodward says.

"So if you're doing anything where you're entering passwords or logging on, in theory, somebody could capture all of that and get access to your accounts.

"It's kind of like me writing my bank password on a post card and sending it through the mail, while it's unlikely anybody would read it, why take the risk?"

While travelling, a thief has plenty of time to record what you are doing and gain all the data they would need to later access your personal information.

Wi-fi risks higher on public transport

The same risks apply to other wi-fi hotspots such as hotels, airport lounges and restaurants but these risks are increased in a crowded and confined space like a bus or train where people are together for longer.

"It's a matter of being aware that anything you do in that environment, somebody could be eavesdropping," Prof Woodward says.

Wi-fi Protected Access, or WPA, offers password protected access and/or encryption (scrambling) of the data being sent or received.

But WPA is something that the host puts in place, not something that the user can choose to install.

"The problem with WPA is that you need a password, and on a bus or train it's probably going to be an open hotspot which means not having any security," Prof Woodward says.

Prof Woodward says that to ensure the bus or train company carries no responsibility for any malicious acts, each compartment would need to have a disclaimer in public view warning of the risks.

Wi-fi hotspots are already available in many transport systems throughout Australia and no security issues have yet been reported.

The London cabs which were introduced to Perth in 2013 offers free wi-fi through Perth-based internet service provider iiNet.

Provided by Science Network WA