Three security issues to consider when using public Wi-Fi

By Aaron Thornton

20 Apr 2015

Public Wi-Fi is almost everywhere nowadays. Coffee shops, libraries and even airports have installed hot spots to feed the growing demand for ubiquitous Wi-Fi. While convenient to use, there are hidden security risks you should know about.

Packet sniffing

Remember, the Wi-Fi you're connecting to is shared with others, which substantially increases your risk of becoming a victim.

Shared connections allow others to read your data and track your online activity. Sensitive information, such as your username and password, can be captured in the process. Since most people use the same username and password for multiple accounts, the risk is magnified. An attacker could steal your credentials and compromise far more than your Twitter or Facebook account. They may even gain access to your financial records or other private information.

You might think that an expert would be needed to carry out such an attack. However, that's far from the case. Free plug-ins simply list out the URLs you are visiting, compromising your privacy and possibly your security.

Consider the following Amazon URL: www.amazon.com/gp/aw/s/ref=is_box_?k=nail+polish. Amazon uses similar URLs for every part of your shopping experience. The result is that the attacker can see your browsing history. If you pass cookies unencrypted or log in to websites that don't use HTTPS, the attacker can start to see a pattern and use such unencrypted data to log in to your accounts.

Man-in-the-middle attacks

Man in the middle isn't a new type of schoolyard game. Instead, it's a class of attack made possible when the communications of an unsuspecting user are intercepted and modified by an attacker. In the case of a Wi-Fi hot spot, the attack would typically be implemented by the owner and would revolve around mirror-like copies of popular websites such as Twitter and Facebook.

To you, it appears like you're interacting with the actual website. However, the attacker has presented you with their own malicious copy of the website to trick you into passing sensitive information such as a username and password. Such information would then be used to log in wherever possible in an attempt to gradually escalate access to financial records and other valuable private information.

Malicious Wi-Fi hot spots

Wi-Fi hot spots can be named anything the owner would like. How do you know that the StarbucksWi-Fi free access point is the official one?

Any malicious attacker can set up a clandestine hot spot and name it whatever they want. As you browse your traffic is recorded and later analysed for any sensitive information that may prove useful in compromising your accounts. Instead of just connecting to an arbitrary Wi-Fi access point, check with establishment to ensure that you're connecting to the official Wi-Fi and not a malicious hot spot.

Free Wi-Fi is tempting, but remember to protect yourself from data theft. Avoid public Wi-Fi when possible. Use SSL and VPNs when you have no other choice and always make sure to confirm the authenticity of the hot spot before you connect.

ABOUT AARON THORNTON

Managing Director at Dial a Nerd

- #BizTrends2020: SME technology in 2020 - a path to efficiency - 6 Jan 2020
- Are you leaving the front door open for cyber criminals? - 16 Oct 2019
- Why tough times call for technology-led innovation - 10 Sep 2019
- What every business owner should know about migrating to the cloud - 3 Aug 2018
- Three security issues to consider when using public Wi-Fi - 20 Apr 2015

View my profile and articles...