WI-FI Security

[Name]

[Institutional Affiliation]

WI-FI Security

According to Morley (2016), Wireless Internet Connections, or WI-FI connections, are becoming increasingly popular for both private and business internet usage. However, this increasing popularity, coupled with a lack of consumer awareness about how these systems work, means that security issues are also on the rise.

Norton, experts in web security and a leading provider of PC security software, explain that "security on these networks is lax or non-existent" (Symantec Corporation, 2018, n.p.). They describe how this leaves information (such as passwords and personal information) vulnerable as it passes from the user's device to the website. There are a number of reasons this might happen. In the first place, many routers – used to provide the WI-FI service – are shipped with encryption capabilities switched off; unless this feature is deliberately enabled by the professional setting up the network, then information transmitted using the WI-FI service will be easy for hackers to access and read. Unsecured WI-FI connections also leave users more vulnerable to middle-man attacks, malware attacks, and "Wi-Fi snooping and sniffing" where cybercriminals use "special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals" (Symantec Corporation, 2018, n.p.). Finally, users who are unaware of the risks of open unsecured connections may also fall victim to "rogue" hotspots, which look legitimate but are in fact unsecured connections giving cybercriminals direct access to a user's information (Symantec Corporation, 2018, n.p.). These are all dangers to which the user in the provided scenario for this assignment might fall victim to in connecting to the open unsecured Wi-Fi connection described in this scenario. In this particular scenario, moreover, the nature of the work might raise further security concerns: if the health-insurance related work

done on the unsecured connection concerned clients' information, this would put not only the user at risk, but also the clients and corporation.

According to Norton, there are a number of ways of increasing security when using an open, unsecured network. Users should avoid auto-connecting to open, unsecured networks, and avoid logging into accounts using apps instead of websites using HTTPS; they should also avoid websites holding sensitive information (such as healthcare or financial information) altogether. Users should also disable file-sharing, use a VPN where possible, and always log out of accounts when finished with them (Symantec Corporation, 2018, n.p.).

One recent example of a breach across an open Wi-Fi connection was journalist Steven Petrow's experience of being hacked in mid-air whilst writing a news-story about a dispute between Apple and the FBI. Using an open unsecured connection on a flight from Dallas, Petrow emailed colleagues and leads about his story, some of which included sensitive information about the case. Petrow was unaware that his connection had been hacked until he was stopped at the gate by a fellow passenger, who revealed that he had hacked the connection and was able to discuss Petrow's communications in detail. As Petrow describes it, "I felt as exposed as if I'd been stark naked" (Petrow, 2016, n.p.). Although the stranger on the plane's actions were intrusive, they were conducted to make a point – that information sent on open, unsecured networks is vulnerable. The hacker succeeded in making his point, and Petrow would go on to write stories raising awareness of this issue.

What both Petrow's story and Norton's publically-offered advice reveal is that user education and awareness are one of the most important defences against security breaches. If users make themselves more aware of the risks pertaining to open, unsecured WI-FI access, as

well as the many security options available to them, security attacks are much less likely to be successful.

References

Symantec Corporation (2018). “The Risks of Public Wi-Fi.” Retrieved from https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html.

Petrow, S. (2016, February 24). “I Got Hacked Mid-Air While Writing an Apple-FBI Story.” Retrieved from https://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720/.

Morley, D. (2016). *Understanding Computers: Today and Tomorrow, Comprehensive, 16th Edition*. Cengage Learning: VitalBook file.