Discussion 10D

Would you connect to an Unsecured Wireless Network? For this discussion address these concerns: Would you use your neighbor's unsecured wireless home network? Why or why not?

You’re sitting on a bench at your college’s campus, waiting for a friend to get out of class. To use time effectively, you pull out your laptop and begin to work on the weekly CIS discussion question. Unfortunately, the only accessible internet connection at the time is the school’s public, unsecured student network. You soon discover that your need for the internet outweighs the risks… it was only a matter of time. Defeated and out of options, you give-in and connect. This is a somewhat silly and dramatized scenario, however, it’s a true story which is presently taking place as I write this post. Beyond a realization of how much I depend upon the internet for daily tasks is the affirmation that I am willing to connect to unsecured wireless networks.

Unsecured wireless networks, often advertised as “Free WIFI”, are becoming more popular, largely in response to mobile smartphones. Most budget cellphone users are all too aware that cellular network connections and data transfers can quickly become expensive. Free WIFI is often the remedy, whether it be at college campuses, libraries, airports, or even some box stores like Home Depot. As several phone users, including myself, fall into this category, it’s important to understand the risks and ethics of unsecured wireless connections. Easily accessible tools exist which can “sniff” or intercept and analyze data transferred on a network. Unencrypted user names and passwords would be of specific interest to malicious users. To better protect against this, network users should always opt to use encrypted protocols such as https. Users should be cautious when connecting to any network, open or secured. Ensure that the network is sponsored by a safe, reliable source. Ofttimes a malicious network known as a “honeypot” may exist, disguised under a friendly and believable network name. An open network doesn’t grant anyone within connection range an open invitation to use it. Taking advantage of a neighbors unencrypted wireless network should be looked down upon as petty theft and simply unwise. While this crime is often overlooked and gone unpunished, it is prohibited by most Internet Service Providers (ISPs). There have been a few instances where a network-theft perpetrator has been fined.

Resources:

1. [www.lifewire.com/is-it-safe-to-use-an-open-wireless-network-2378210](http://www.lifewire.com/is-it-safe-to-use-an-open-wireless-network-2378210)

2. <https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html>

3. <https://www.finjanmobile.com/the-dangers-of-using-unsecured-wi-fi/>

4. <https://www.nolo.com/legal-encyclopedia/stealing-wi-fi-your-neighbor-a-victimless-crime.html>

