Unit 9 Network Security

**Corey Crooks**

**Purdue University Global**

**IT190 – Marjorie Furay**

**February 12, 2021**

**Risks to the Network**

1. Is my network safe with password protection?

Generally speaking, it is a very good idea to always use passwords to add a layer of security to your network. Passwords can not only help you maintain the proper amount of traffic within your network, but also aide to keep out unsavory characters that may be hunting for precious data developed by the devices connected. Just because you have a password on your Wi-Fi doesn’t mean you are completely safe from attacks, however, so additional tools are available to help your devices and documents sleep safe and sound through the nights to come.

2. Can the websites I visit compromise my network

They can. There are a great many tools that individuals looking to hijack your network can use to do so. One of those tools that has become quite popular is through malware installed on your computer through ads, pop-ups, or even just visiting a specific URL. This can trigger a download of the program they can use, and if not handled especially carefully, this can lead to great harm for not only your system, but also everyone connected to the network your system is on.

3. Isn’t my ISP like comcast supposed to handle security?

For a certain degree, they do. Internet Service Providers handle a widescale version of security to make sure that one network infected with malware cannot hop to another network within their services. Unfortunately, it is up to you to not get the malware in the first place. There are many tools you can use to have safe practice on the internet, and your ISP may bundle such software like antivirus with your internet subscription. More on specific programs later.

4. What if I have a 2.4 GHz network that no one else is connected to as free Wi-Fi for everyone?

Generally speaking, it is a bad practice to give out free Wi-Fi if it is unprotected. Commonly, routers will have multiple channels such as 2.4 GHz, and then another at 5 GHz to aide in bandwidth. You could be forgiven for thinking that these are separate networks entirely, and thus if they were compromised, the other network would remain in-tact. Unfortunately, this is not the case. These different channels are simply just different speeds. For this reason, having a free Wi-Fi that is not password protected is akin to inviting danger into your home.

**Risks to computers connected to the network**

5. Are my documents safe from people physically outside my home?

They are not. Simply because your documents are stored locally on your computer, doesn’t mean they can only be accessed locally. You may have needed tech support in the past, and during this session you may have given the agent access to your computer so that they could use your device remotely—moving the mouse cursor, opening files, downloading programs, and much more. Well, this technology isn’t just limited to tech support agents. All it takes is for you to navigate to the wrong section of the web, and click the wrong button then suddenly your entire system is being remote-controlled by someone across the globe.

6. Do I have to be careful about programs I download?

It is essential that you thoroughly vet and look carefully at each and every program you download. As described above, the consequence for downloading a malicious program isn’t just that your default browser changes to Yahoo. Downloading and running a malicious program can have any number of effects on your system depending on the Operating System. It could delete essential files to turn your computer into an expensive paperweight. It could put all of your files onto their server, and subsequently give them immense bargaining power against you for blackmail. It could even hijack the hardware of your machine and use it for cryptocurrency mining. There is no guaranteed outcome, but there is guaranteed frustration.

7. Are my credentials safe with a compromised network?

They are not. Some programs today have a number of ways to grab your information without you even knowing. For example, a keystroke recorder will record each letter you type on your keyboard and relay that information back to anyone trying to gain access to your accounts and files. This information can be processed to accurately determine what login credentials you use for any number of websites, and thus grant the user access to all of your precious accounts.

8. Is my hardware safe with a compromised network?

Absolutely not. One thing many people hold for granted is the hardware in their machine. Often times it is overlooked in a system, and too much of the focus in security is put on software and data. But one of the things commonly targeted in cyberattacks is actually the hardware. Malicious attacks can do a great many things to your hardware to get you to pay a ransom. They could limit your CPU clocks to make your computer run so slow that work on the machine is practically undoable, or my personal favorite, they could cause heat-generating components like the graphics card to run gradually faster and faster until your components literally catch fire and melt. There is quite a lot of damage that could be done to an unprotected machine, and for the hackers out there, the digisky is the limit.

**Ways to protect the network**

9. What is a firewall? Do I need to keep flammable materials like paper and cloth away while using it?

Firewalls are one of the incredibly common techniques used by antivirus applications to block certain ports, signals, or applications from communicating via the internet on your device. Firewalls are an essential first step to securing your internet activity, and by extension, your device. Firewalls are commonly integrated into most antivirus such as the default program included with your operating system like Windows Defender, or even premium antivirus like McAfee or Norton, though the feature set of the latter programs is much more robust and available to customize.

10. What are safe practices regarding network security?

There are millions of practices available to keep your hardware and software secure, but many people have practices in common. After all, many hackers find that smaller targets are usually easier to infiltrate when compared to targets like big companies and corporations (Johansen, 2019). For starters, look carefully at any online activity you do. This includes everything from browsing the web to downloading and installing applications. If you don’t know it, you don’t need it. Additionally, you can employ the help of antivirus and malware protective tools. After all, you are human and likely make mistakes here and there. Antivirus can help mitigate the effects of those.

11. How can Network Scanners and Antivirus like Norton help?

There are a great many ways these programs can help you. Firstly, as described before, nearly every program out there dealing in this matter has some sort of Firewall protection system. These help to limit the traffic that is being used over the internet, and block potentially threatening signals from reaching your computer. These usually also double as an antivirus suite to help pinpoint threatening applications and remove them from your computer if necessary. Antivirus can pinpoint even down to specific files to scan for anomalies that may harm your computer. Take Norton Antivirus for example. Norton has at the front end a rich firewall with many different tuners in case of signals the user knows is safe, but may not have the reputation to pass Norton’s scans. It also has a scanning tool to scan your entire hard drive(s) for potential out-of-character files to pinpoint viruses as they originate. It also has a network scanning option that not only gives pointers on reputations of specific websites, but also checks for suspicious activity over the web.

12. Do only business professionals need to worry about strict network security?

Security is important for everyone. It is true that business have a lot more valuable data than the average computer user, but that doesn’t mean that you are safe from hijackings and attacks. In fact, in 2018 there were over 30 million cyber-attacks per year (PurpleSec, 2021). With cybercrime as rampant as ever, it would be foolish to think that a certain population is virus-free (Yes. Even Macs get viruses and malware). As long as you are safe on the internet and keep your computer secure, then you should make it out just fine.

**Ways to protect individual computers**

13. What are VPN’s?

A Virtual Private Network is a service that can mask your initial connection signal and provide a means of anonymity on the web. There are many ways this can be useful, but most commonly it is a means of providing additional security. While using a VPN as a sort of proxy it makes your connection very difficult to trace to your real-world position therefor extremely limiting the data an individual can collect on you, and making you less susceptible to attacks.

14. What is a specific VPN, and how can it help me?

VPN services like NordVPN help computers and users keep their privacy on the internet. This can severely limit the trackers companies and individuals use as well as hinder their abilities to collect information on you and your system. In turn, this makes you much less susceptible to things like targeted attacks, and information-driven blackmail. With cyberattacks against devices increasing by 600% between 2016 and 2017 (Comcast, 2019), it is more important than ever to look into security. This leads to a happier system and a happier you, free to browse that Reddit thread to your hearts content without having to worry about who is watching you do it.

15.What are decent Antivirus applications, and how do they help?

As far as antivirus goes, there are many different choices out there. Already discussed is both Norton and Windows Defender. If you have a windows system, and don’t want to do a whole lot of fiddling with permissions then Windows Defender may actually work quite well for you. Alternatively, if you find yourself needing the extra kick, and you want to get into the nitty-gritty of security, then upgrading to programs like Norton and McAfee may suit you well. Norton does very well with Security on your system, and managing threats as they appear. McAfee can be built straight into your browser in order to further inform you on the websites you visit, and how to stay safe on them.

# **References**

Comcast. (2019, January 8). *Comcast Launches Digital Security Service To Protect WiFi Connected Devices In The Home*. Retrieved from Comcast.net: https://corporate.comcast.com/press/releases/comcast-launches-digital-security-to-protect-wifi-devices

Johansen, A. G. (2019, April 9). *10 cybersecurity best practices that every employee should know*. Retrieved from Norton: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

PurpleSec. (2021, February 12). *2020 Cyber Security Statistics*. Retrieved from PURPLESEC: https://purplesec.us/resources/cyber-security-statistics/#:~:text=In%202018%20there%20were%2080%2C000,30%20million%20attacks%20per%20year.&text=Ransomware%20attacks%20are%20growing%20more,businesses%20with%20under%201%2C000%20employees.