BITS 3353 Network Security Administration and Management

ASSIGNMENT (15%)

Chosen Topic:

PUBLIC WIRELESS ACCESS/HOTSPOTS

Group 17 Members:

1- Muhammad Izham Bin Norhamadi (B032020039)

2- Ahmad Sha Herizam Bin Tahir (B032020009)

Lecturer:

Dr. Nur Fadzilah Binti Othman

Table of Contents

Introduction of Public Wireless

In this modern era, public wireless network can be found everywhere either from restaurant or even in a library. Every layer of people can access these networks or internet as easy as ABC in just one click and automatically every information that reside in the so-called sacred place called internet in just at the tip of our finger. For example, the most popular wireless network that everyone uses around the world is WI-FI. This WI-FI can be divided into public and private which different in term of security risks. Private WI-FI do not have a lot of risks to worry about since it handles only in small organizations and have a security measure to protect it but for public WI-FI, it is different story. To make sure everyone can enjoy this network fairly, most public WI-FI do not have any password required or the least security measure it have is only have one layer of security which is only have a password authentication. Also, the password used is so simple and can be guessed easily. This is clearly seeing that any public wireless access of network is vulnerable to various kinds of network attacks compared to private wireless network.

Day by day, technology advancing in rapid speed. A lot of recent technology has been migrating to more wireless approaches since from millennium society's eyes, having a wireless devices or technology can make quality of life much easier than wired one. This is 100% true since having a wireless device, someone can access everything at everywhere they go. But from security perspective, wireless approaches can be so vulnerable at point where attackers also can wirelessly attack wireless device easily. Compared to wired device, to access the network we need to physically have the cable connection. So having a secure physical place for the network cable makes wired devices much more secure than the wireless one. That is why wireless networks have more security risk that need to get attention to when using it.

Overall, every individual either expert in technology or not, must have a decent knowledge of how to make sure to use public wireless networks access properly and always have an appropriate security measure when dealing or using the public wireless access. Every day, new networks attacks has been recognized and some of it hard to counter or solve. So, having an extensive and correct way to prevent any security issue related to public wireless access is heavily recommended to minimize any damage from network attack and completely block off all malicious or dangerous network exploits as much as possible to have a better public network environment.

Security and Privacy Issues

Since public Wi-Fi is convenient and free, most people are not aware of how exposed their data are on their devices, which ranges from important documents at a job to sensitive information like banking credentials. Public Wi-Fi is the prime spot for cyber criminals to steal user data and confidential information. Just like how you should care for your privacy in public, should you care for what your device sent over public Wi-Fi.

Devices that are connected to public Wi-Fi hotspots are at risk of Man-in-the-middle attacks. Data that was sent over a public Wi-Fi is often unencrypted, making it easy for cyber criminals to intercepts your data travelling between your device and the Wi-Fi router. This can lead to theft of personal information such as login credentials, financial information, personal data, and pictures. This information can damage a person's finances and reputation.

Cyber criminals also often set up a Wi-Fi point without password called rogue hotspot. These hotspots are meant to mimic a legitimate hotspot provided businesses, such as restaurants and cyber cafes. Any device that is connected to these Wi-Fi network will be eavesdropped and monitored by the cyber-criminal using packet sniffing tool to steal the user's confidential data. Besides spying on your internet activity, they can also hijack your session where an attacker

intercepts information about your computer and its connection to websites or other services. Once the cyber-criminal has this information, he can configure his own computer to match your device and hijack the connection.

Lastly, devices that are connected to public Wi-Fi are at risk of getting malware, such as viruses and worms in their system. A cyber-criminal that is connected to the same Wi-Fi hotspots as you can plant a malware to your device if it is not protected properly. One of the methods of getting your device infected by malware is by placing ads on websites you visit. This can be possible by using the Wi-Fi service to overlay the ads on top of other websites. By clicking these ads, your device can be vulnerable to virus installation that may persist if you are using the device.

Prevention Strategies

Using a VPN

The main reason to use VPN when surfing the internet using any public wireless network or hotspot is to hide users' IP addresses by redirecting the network to remote server that specified by VPN host. This means that only a VPN server is providing a source of internet information. Automatically, Internet Service Provider (ISP) and other third party cannot gain information about what website we visit or data that travel between us and internet. By having VPN, any potential information breach by hacker can be overcome due to these hackers cannot reveal our true IP address since IP address has a lot of ports which hacker can try out force connect with our device to steal confidential information such as credit card information.

Use SSL connection

Having an SSL connection on top of VPN can give an extra layer of protection when surfing the internet. SSL is for authentication and encryption of connection over the network. This means

that we need to always use HTTPS connection when visiting frequent websites or websites that require any credential input. This is because we might use the same password credential for some normal websites such as forums or discussion groups. Without HTTPS connection, hackers can gain credential information and can have access to our other important website such as bank.

Make sure to protect our data

When we connect to public wireless network or hotspot, obviously our data has a risk of leaking to public attention if not secure properly. Besides having a VPN, users need to take extreme precautions on their data flow back and forth in this public network. That's mean is whenever we need to input whatever data to the internet using the public Wi-Fi such as email address or password, make sure we use email address that is the primary one and prevent from using password that we use all across our social platform. Having a 2FA security also is recommended. This is because if any hacker wants to attempt to login by using our password, they need to have access physically to our phone since 2FA requires users to give confirmation to their smartphone.

Update Software or Application regularly

One of the biggest reasons that our data is vulnerable to hackers is that our software is still not up to date with the latest version. As we know most updates of software always have a latest security measure to deal with the newest type of attack whether it is malware attack or phishing. So having updated software will make sure to keep a layer of protection when surfing using the public network. In this modern world, a lot of new types of cybersecurity attacks occur every day. Day by day new malware keeps being introduced in the cyber world. That's why new security measure for a software must have in every software nowadays to counter all the cybersecurity attack especially when users using public network or hotspot that has a lot of security risk if not have proper version of a software of application.

Conclusion

Wi-Fi hotspots are becoming more common in business premises now as the internet became more and more prominent as the source of entertainment, communication and work and creating these hotspots may potentially attract customers to premises. However, the same features that make free Wi-Fi hotspots desirable for consumers also make them desirable for hackers; namely, that it requires no authentication to establish a network connection. Its biggest threat being the ability for hackers to position themselves between unsecured device and the connection point, collecting your information. Through this way, a hacker has access to every piece of information that you're sending out on the internet such as login credentials and credit card information. Thus, we as a Wi-Fi hotspot user should be aware of what we're about to send through the network, or we can secure our connection using VPN so that a hacker would not be able to glean through our information. It is understandable that there's going to come a time when an unsecured, free, public Wi-Fi hotspot is the only connection available when it is needed. Understanding public Wi-Fi risks and using security solutions will ensure your private data is safe and secured while browsing internet.

References

1. Aberdeen Cybersecurity, Wired vs Wireless Networking, https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking/
2. University of Strathclyde Glasgow, Public Wi-Fi Hotspots, https://www.strath.ac.uk/is/cybersecurity/publicwi-fihotspots/
3. GOODSPEED, 7 Danger of Public WiFi, https://goodspeed.io/blog/7-dangers-of-public-wifi.html
4. Check Point Blog, Rogue WiFi Hotspots, https://blog.checkpoint.com/2014/05/06/rogue-wifi-hotspots-getting-coffee-putting-enterprise-risk-social-engineering-ep-4/#:~:text=A%20rogue%20hotspot%20is%20a,Fi%20access%20to%20its%20patrons.
5. Kaspersky, How to Avoid Public WiFi Security Risks, https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
6. What is VPN? How It Works, Types of VPN, https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn
7. Does a VPN protect you from hackers?, https://thehackernews.com/2021/08/does-vpn-protect-you-from-hackers.html
8. Public Wi-Fi security: Why public Wi-Fi is vulnerable to attack, https://us.norton.com/internetsecurity-wifi-public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-to-attack-and-how-to-stay-safe.html