INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 5.828 (SJIF 2022)

STUDY OF PUBLIC WI-FI SECURITY CHALLENGES AND SOLUTIONS

Miss. Dipali Vishnu Shinde

Assistant Professor,
Department of Computer Science,
Smt. K. R. P. Kanya Mahavidyalaya, Islampur (Maharashtra, India)
E-mail: dipalishinde18@gmail.com

DOI No. 03.2021-11278686 **DOI Link ::** https://doi-ds.org/doilink/04.2022-72393449/IRJHISIC2203054

Abstract:

Internet is a global communication system that links together thousands of individual networks. It allows exchange of information between two or more computers on a network. Wide Area Network is connecting two or more LANs together, generally across a wide geographical area. Ina constantly connected world, free Wi-Fi can seem like an oasis in the desert, allowing you to ration your data and safeguarding you from eye-watering overage fees. Unfortunately, public Wi-Fi is inherently less safe than personal, private networks such as your home internet or the office network. While using public Wi-Fi there are some security problems.

In this I discussing about security problems of using public Wi-Fi as well as solutions for that problem.

KEYWORDS: *Public Wi-Fi, Cyber Security Attack*

I. INTRODUCTION:

Wireless, or Wi-Fi, as the name suggests, does not use telephone lines or cables to connect to the internet. Instead, it uses radio frequency. Wireless is also an always on connection and it can be accessed from just about anywhere. Speeds will vary, and the range is between 5 Mbps to 20 Mbps. Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants,and hotels — and it allows you to access the Internet for free.

The problem with public Wi-Fi is that there are a tremendous number of risks that go along with these networks. While business owners may believe they're providing a valuable service to their customers, chances are the security on these networks is lax or nonexistent.

Most users working on public Wi-Fi have a lot of important and possibly sensitive information on their devices, some of which could cause serious harm if a hacker gets a hold of it.

Unfortunately, the majority of public Wi-Fi users likely don't realize the threats they face.

II. PUBLIC WI-FI:

Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants, and hotels and it allows you to access the Internet for free. These "hotspots" are so widespread and common that people frequently connect to them without thinking twice. Although it sounds harmless to log on and check your social media account or browse some news articles, everyday activities that require a login like reading e-mail or checking your bank account could be risky business on public Wi-Fi.

III. RISKS OF USING PUBLIC WI-FI:

If you want to stay safe while using public Wi-Fi, you need to know what the potential threats are. To provide you with the tools to work as safely and securely as possible in public spaces, we developed a list to help you identify 7 dangers of public Wi-Fi

1. Theft of Personal Information:

One of the most serious and common threats concerns theft of personal information. These types of threats are:

i) Identity theft:

Identity theft is a cybercrime with the primary goal of illegally obtaining someone's data. Most commonly, cybercriminals use public Wi-Fi hotspots to steal people's credit card information and commit financial fraud. With enough information about an individual, cybercriminals can apply for loans, withdraw money, make purchases and commit other crimes all in their name.

ii) Data breach:

Using public Wi-Fi safely is essential to avoid a data breach, which happens when hackers illegally access private information. Whereas identity theft mainly involves financial information, data breaches can affect any kind of information you store on your device. If you don't know how to safely use public Wi-Fi, cybercriminals can steal your photos, videos, documents, and contacts among others.

2. Cyber Attacks on Businesses:

Business travelers and others who are on the road throughout the day may connect to public Wi- Fi to check their emails, download files, review customers' information, and perform various other tasks that require a network connection.

For instance, you never know what the Wi-Fi provider might track. A lot of public connections are free to use but that does not mean there is not a cost involved. The Wi-Fi provider might be tracking everything you do on the Wi-Fi connection and sell your data to advertisers.

3. **Man-In-The-Middle Attacks:**

One of the most common threats on these networks is called a Man-in-the-Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and "read" them.

For example, say you are staying in a SleepTight hotel for the night. The hotel offers free Wi-Fi to its guests so you power up your laptop, turn on Wi-Fi and see a network called "SleepTyte". If you are not paying close enough attention, you might miss the slight misspelling. When you connect to it, the Internet works as expected so you would not think twice. But in reality, everything you do while on that connection goes through the hacker's computer. Those "man-in- the-middle" could have access to all your login information, passwords and anything else you do while on that Wi-Fi connection.

4. **Unencrypted Connections:**

When you connect to a website that supports encryption, the data that goes back and forth gets encrypted using a secure key. If someone were to intercept that data without the possession ofthe key, they wouldn't be able to read it - the data would look like unreadable computer code.

Not all websites offer encryption though. You can tell by the HTTP prefix stated before the domain name. If it starts with HTTPS, it is an encrypted site. If the web address just contains HTTP, it is not encrypted. When you are connected to a public Wi-Fi network, anyone within range of your computer can intercept everything you send or receive. If you are connected to an unencrypted website, it will all be fully readable.

5. **Packet Sniffing / Eavesdropping:**

Anyone connected to the same Wi-Fi network as you can eavesdrop on what you send and receive using a tool called a packet analyzer or packet sniffer. These tools provide the possibility to view everything transmitted over the Wi-Fi network, provided it is not encrypted.

These tools are not inherently bad. Like many tools, you can use them for good or bad purposes. Packet sniffers let network administrators troubleshoot connection problems and other performance issues with their wireless networks (good). On the other hand, they also let hackers intercept other users' information and steal anything of any value (bad).

For example, your business partner might receive your message after it has been altered by cybercriminals.

6. Malware Distribution:

Another threat that can occur while using public Wi-Fi, is the implementation of malware on your device. Malware exists in many forms:

- Viruses
- Worms
- Trojan horses
- Adware

If someone on the same public Wi-Fi as you has bad intentions, they could plant malware on your computer if it is not protected properly. A suspect Wi-Fi provider could use the hotspot itself to infect your computer with one or more of these threats.

It could be as simple as using the Wi-Fi network to place ads on every website you visit. Thewebsite itself does not run ads, but the Wi-Fi service can overlay them on top of other websites. In that case, the ads would normally disappear once you disconnect from the Wi-Fi and go backto your home or office connection.

7. Session Hijacking:

Session hijacking is another public Wi-Fi security threat. In this case, an attacker intercepts information about your computer and its connection to websites or other services. Once the attacker has that information, he can configure his own computer to match yours and hijack the connection.

For example, hackers could hijack your connection to your bank's website after you log in. From the bank's end of the connection, it would look like your computer and since you are already logged in, the attacker would have access to everything in your account.

IV. GOALS OF NETWORK SECURITY:

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure. The primary goal of network security is Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as CIA triangle.

- **Confidentiality** − The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.
- **Integrity** − This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

- **Availability –** The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

V. SECUIRITY SOLUTION:

If you need to use public Wi-Fi, there are several things you can do to help protect yourself from these threats. If you have taken steps to protect yourself, they will more than likely move on to an easier target.

1) **Don't Share Anything Private:**

Firstly, if you have to connect to a public Wi-Fi network with no protection measurements in place, make sure not to share anything private or log into any sensitive websites. Keep your browsing to a minimum, do not check your email or any other messaging services, and disconnect from the public Wi-Fi immediately once you find the information you need.

2) **Use a VPN Service:**

A virtual private network, or VPN, service encrypts everything you send and receive over a WiFi network. It gets encrypted regardless of whether the Wi-Fi network or website you are accessing supports encryption. With a VPN, you connect to the VPN server over an encrypted connection and everything you do gets routed through that server. Anybody trying to eavesdrop or intercept that information will not be able to read it anyway.

3) **Use 2-Factor Authentication:**

Many websites that deal with sensitive information use a security feature called two- factor authentication (2FA). This is a secondary authentication method working alongside your password. It uses either a specialized app on your smart phone, such as Google Authenticator, or text messaging to send you a unique code after you enter your usernameand password. If a hacker manages to steal your login information, they still cannot log inwithout that 2FA code.

4) **Use Cellular Data or a Mobile Hotspot:**

The safest way to avoid public Wi-Fi security threats is to avoid it in the first place. Instead of connecting to public Wi-Fi, we recommend using a cellular data connection. You can establish this with a digital eSIM solution, a physical international travel SIM card or a mobile hotspot.

5) **Antivirus and Anti-Malware Software:**

Hackers can use stolen credit card information to place orders from anywhere in the world. Antivirus or anti-fraud software can help you with this serious ecommerce issue. They use sophisticated algorithms to flag any malicious transactions to help you can take further action. They provide a fraud risk score which can help proprietors determine if a certain transaction is legitimate.

6) Use Firewalls:

Another effective ecommerce recommendation is to use firewall software and plugins that are pocket-friendly yet effective. They keep untrusted networks at bay and regulate traffic that enters and leaves your site. It offers selective permeability and only allows trusted traffic in.

7) Don't access your personal or financial information: Always assume a public Wi-Fi network isn't secure.

Log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted (meaning that the URL starts with https) — from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.

8) Don't stay permanently signed in to accounts. When you've finished using an account, log out.

9) Don't use the same password on different websites. It could give someone who gains access to **one** of your accounts access to many of your accounts.

10) Pay attention to warnings. Many web browsers alert you before you visit a scammy website or download malicious programs. Don't ignore those warnings. Also keep your browser and security software up to date.

11) Change your device's settings so it doesn't automatically connect to nearby Wi- Fi. That way, you have more control over when and how you use public Wi-Fi.

VI. CONCLUSION:

While using public Wi-Fi there are many issues about security. WLAN security is neither straightforward nor easy, and it is constantly changing. Even WLANs increase client's productivity; they expose the network to a new group of hackers because WLAN works on OTA.In this we have discussed all security issues and solution to those issues so that a protected from various types of attacks.

VII. REFERENCES:

1) https://goodspeed.io/blog/7-dangers-of-public-wifi.html

2) https://clario.co/blog/public-wi-fi-security-risks/

3) E-Commerce: An Indian Perspective –P. T. Joseph. S .J.

4) https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

5) https://www.consumer.ftc.gov/articles/how-safely-use-public-wi-fi-networks