International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Public Networks: A Threat or Shield to Personal Data

Shriya Chandel

B.B.A. LL.B. Student, New law College, Bharati Vidyapeeth (Deemed to be University)

Abstract

The increase in development of technologies made networking an integral part of everyone's life. From initial wired technology to the change in wireless technology today, everything has become so convenient that it is difficult to live in this society without access to such benefits. Public network is one of them. Along with convenience, such network also has potential security and privacy risks. However, most users keep neglecting the privacy threats being unaware of the preventive measures to shield their data. The aim of this research paper is to analyze whether the public networks are only a threat to personal data or if it can be shield to protect user's personal and sensitive data from getting revealed. The public networks have its own set of pros and cons which on one hand, supports the networks as most preferred connection because of its easy accessibility, availability, cost-efficiency etc. while on the other hand, proves to be a paradise of hackers, home to viruses and malwares etc. After collection of all the information, related articles, etc., it is brought to notice that there are several kinds of threats and malwares attached to this type of network which is unthinkable for the general public. Although there are various preventive measures as well to protect the personal data but it is unaware to the general public. The research paper gives details on the working of public networks, advantages and limitations of these networks, various malicious attacks, articles on major security risk at public places on free Wi-Fi, cyber-crime risk on free Wi-Fi and Bluetooth as well as free Wi-Fi being the most potent tools for cyber crooks, along with the preventive measures to shield personal data from any such above mentioned threats..

Keywords: Public Network, Public Wi-Fi, Threat, Privacy, Encryption, Hacking, Malicious

1. Introduction

Network is a connection between two or more computers that are linked to each other for the purpose of sharing information, resources such as transferring or exchanging files, communication and other services. Usage of hardware and software technologies allows communication between various devices easier whether they are located in the same physical location or are geographically dispersed. Along with the evolution of technologies, networking emerged as an integral part in everyone's life. From initial wired network technology, it developed into wireless network technology that we have today. Now, the world revolves around this wireless network technology called internet which is nothing but a network that connects billions of devices across the world at the same time. It is one of the biggest examples of public network. Public Network, in general refers to a network that is easily accessible and open to the general public that is to each and every citizen such as the public Wi-Fi connections at airports, hotels, malls, shops etc. These networks are said to be typically unsecured which means that they don't require

a password or any kind of authorization to connect to it. Since, these networks are easily accessible to everyone, the users from all across the world can connect and use the online facilities available to them. These networks are preferred by both public as well as the service provider because it reduces the individual's cost for using it. Also, the set up and maintenance of public networks are cheaper in comparison to a private network which is way more costly due to its additional requirements even after initial investment. These networks are mainly established and operated by a third-party telecommunications provider for the purpose of providing data transmission services to the public. Mobile networks are also a subset of the public networks and generally uses the same technologies like mobile phones. Public networks can be a threat or even be a shield to your personal data. As the one operating the public network is not known, so there are risks of man-in-the-middle attacks, hacking, malware etc. but it is also a great approach to access the internet without having to worry about privacy. It can be accessed at libraries, universities and other such public places which require to log in with credentials. There are some secure public networks as well which can be accessed without credentials and they use encryption to protect personal information from third party's eyes. 4 In this time and era, protecting personal data is tough. A slight mistake and personal information are leaked and misused for various malicious purpose which are beyond the imagination of a common man. Public Wi-Fi connections, if lacking security, may be used as a medium by the hacker to inject devices with malwares and viruses. This case makes it a threatening situation for users. Despite having risks, there are various preventive measures that must be taken at all cost to not get involved in any malicious attacks.

2. How does a public Wi-Fi works?

The public Wi-Fi hotspots have a separate public access networks that use a Wi-Fi access point connected to a special router to distribute internet services to the users through portable devices connected by those Wi-Fi technology in the access point's vicinity. The public Wi-Fi networks are found at airports, hotels, offices, universities, libraries, cabs and many other places. In certain cases, users may have unrestricted access and in other cases the user needs to pass through encrypted security process by logging in with email address and password..

3. Advantages of Public Network

- **Accessibility:** The foremost advantage of a public network is its accessibility. It is accessible to each and every one across the world. A large number of people can access it at the same time without any kind of restrictions. Therefore, these networks are widely approached.
- **Cost-efficient:** One of the reasons why this type of network is widely approached is because it is affordable. This network is available at extremely low-cost levels. The set-up and maintenance of this network is way cheaper as compared to private networks.
- **Availability:** The public networks allow its users to connect to the internet at any available place till the time there is a connectivity device with the user such as mobile phones, laptops, tabs, etc. even in case of emergency, or sudden loss of private network, the public network can be immediately accessed.
- **Scalability:** The public networks are designed in such a way that it can easily handle a large number of users. In case of private network, the service provider has to upgrade the infrastructure to let more users enter but, in 5 public network, there is no requirement for extra spending on upgradation of infrastructure as it is already capable of managing the increase in traffic.

- **No Entry Barriers:** There is no need for setups, dedicated infrastructure or specific protocols in case of public network. It eliminated the difficult path of going through setups and long processes. It ensures that individuals with limited resources can also benefit from this network.

4. Limitations of Public Network

- **Speed:** The public networks tend to be slower than private networks as is handles huge user traffic at the same time. The unpredictable number of users on this network often leads to congestion and hence, it is better to perform lighter activities only such as browsing data, e-mailing, messaging, searching etc. and time taking activities should be avoided.
- **Limited Security Protocols:** Public networks may lack upgraded and advanced security protocols unlike private networks which has powerful security measures. Such lack may become the reason for man-in-the-middle attacks, phishing attacks, malware attacks etc.
- **Vulnerable to Attacks:** The unprotected public networks that is those without encryption or password protection are often at higher risk of cyberattacks. They become potential targets of data theft, data breach etc.
- **Lack of Privacy:** Since, the public network is available and accessible to everyone, users lack privacy. Therefore, activities performed on such networks can be easily eavesdropped by the cybercriminals and sold to third parties by unethical network providers.
- **Bandwidth Limitations:** The public networks in airports, malls, etc. often have limited bandwidth due to the huge traffic of users in that connection. This causes insufficient internet speed, inefficient browsing experience, longer download times.

5. Is Public Network Safe?

The public networks found in places like airports, shopping malls, hotels, etc. aren't considered safe for sharing personal and sensitive data. There are various reasons to it. Those networks prove to be a target of malicious attacks, such that is not even heard or known common public. The reasons are:

- **Man-in-the-Middle Attacks[1] :** In this type of cyber-attack, the attacker secretly positions himself in a conversation between a user and an application either to eavesdrop or to impersonate one of those parties to steal personal data such as credentials, passwords, account details etc. by making it seem like a normal exchange of information. Attainment of such information can further lead to malicious intents like identity theft, fund transfers without approval, automatic password change etc. Creating malicious Wi-Fi hotspots available to public are the simplest way of such attacks. These aren't password protected and when the user connects to this network, the path for cybercriminals opens.
- **Evil Twin Attack:** This type of cyber-attack is similar to Man-in-the-Middle Attack. Here, the attackers set up malicious Wi-Fi- hotspots with names that seems trustworthy and once the user connects to that network, they intercept the personal data.
- **Packet Sniffing Attack[2] :** In this type of cyber-attack, the hackers maliciously capture the data that was sent across a secured Wi-Fi. Then from there the attackers unpack that data and extract an individual's login credentials or financial information.

[1] Private Network vs Public Network: A Detailed Breakdown, Red Switches, (https://www.redswitches.com/blog/public-vs-private-networks/)
[2] The Dangers of Public Wi-Fi, Aura, (https://www.aura.com/learn/dangers-of-public-wi-fi)

- **Eavesdropping:** In this type of cyber-attack, the attackers maliciously use packet sniffing tools on a public network to capture the data of user transmitted over that particular network.
- **Rogue Hotspot:** In this type of cyber-attack, the attacker maliciously set ups a rogue Wi-Fi hotspot with a seemingly genuine name to that of an actual public Wi-Fi network to deceive the users and potentially accessing their personal and sensitive data.
- **Password Cracking Attack:** In this type of cyber-attack, the scammers use software that automatically tries a huge number of usernames and passwords with malicious intentions to unlock a router's management interface.
- **Malware Distribution:** One more kind of cyber-attack can be malware distribution, where, if the user is connected to an unsecured Wi-Fi network then the malware can be easily sent to their devices which will further destroy the important data on those devices.
- **Un-encrypted Networks:** There are various un-encrypted public Wi-Fi networks which makes it easier for the cyber attackers to intercept data.
- **Security Vulnerabilities:** There are times when some default router settings allow cyber criminals to log in as an administrator or he can simply plant malicious software on user's devices.

6. Free Wi-Fi in Public Places: A Major Security Risk

According to an article in Economic Times[3], a researcher armed with mere $100 device confirmed fears of security risks associated with offering free Wi-Fi at public places in Bengaluru airport. He was successfully able to hack into the computers of hundreds of users who were connected to the airport's complementary Wi-Fi at that time. He also got access to the user's personal data such as WhatsApp conversations, credit card numbers and encrypted user names and passwords as well. This incident casted a dark shadow over the government's plan to offer free Wi-Fi in 2,500 cities and towns across the country.

According to the exercise conducted at Bengaluru airport by the chief scientist of Appknox, Shubho Halder, such free Wi-Fi spots and airports in India are hacker's paradise owing a lack of proactive security.

The Cisco Systems, an American networking equipment maker, has tools to identify fake Wi-Fi hotspots and even locate the user, but hackers still have their way around it. Further, in many cases, even if those tools have ability to prevent such misuse, they often don't activate it. Also, those tools can only talk about the happenings, the authority to take actions still depend upon the security teams.

According to Symantec Corporation, to avoid MITM attacks, users must use VPN to carry out sensitive activities or limit their usage on web browsing over public networks.

7. Cyber Crime Risk- Free Public Wi-Fi

According to the article in India Today[4], during the announcement of go-ahead of free Wi-Fi scheme, the Chief Minister Arvind Kejriwal said that with 11,000 hotspots, the project will be the biggest initiative of its kind not just in India but the world.

Cyber-crime expert Amit Dubey said that the scale of the hotspots has the potential fodder to cyber criminals unless the government comes up with a foolproof monitoring and regulation mechanism.

The article also mentions how the series of threat of unsecured Wi-Fi network started to appear since its

[3] Varun Aggarwal, Wi-fi Offered Free in Public Places Poses a Major Security Risk, ECONOMIC TIMES, May 20, 2015
[4] Ankit Yadav & Chayyanika Nigam, Cybercrime Risk in Free Public Wi-fi, INDIA TODAY, August 11, 2019

first recognition in 2008, then in 2015 and further in 2016. It also mentions the working of this system and politics over Wi-Fi.

8. Bluetooth & Free Public Wi-Fi: Most Potent Tools for Cyber crooks

According to an article in Times of India[5], the cyber expert Vivek Nanoti said that cyberattacks can be attributed to improper and immature use of Bluetooth and free Wi-Fi and if it is not handled properly, these two modes give easy access to the mobile to hackers to use various means to loot you.

The cyber-attack called Bluesnarfing was also mention in this article. This attack gives the hackers access to a Bluetooth device's stored information such as contacts, text messages, etc.

According to the cyber expert, 86% of all cyberattacks are for monetary gain, rest 14% comprises of security, revenge porn or any other motive. The four basic reasons that lead to hacking are lack of research-awareness, unsecured server, no firewalls and no or less frequent security audit.

9. Preventive Measures to Shield personal Data

- **Use of VPN[6]:** One of the best ways to minimize the risk from public network and shielding personal data is to use a Virtual Private Network (VPN). Using a VPN on public Wi-Fi creates a VPN secure tunnel through which accessing information becomes private with an addition of extra layer of security to the connection. With this method users can shield their sensitive information from potential eavesdroppers and cyber-attackers.
- **Only Browse HTTPS websites:** Being on the public Wi-Fi the user must be careful and browse only those websites that include an SSL (Secure Sockets Layer) certificate. To identify, these websites always start with "HTTPS". They are encrypted websites which makes the browsing more secure. If websites starting with HTTP are browsed on public network, it may create a threat to the device as well as user's personal data.
- **Use Two-Factor Authentication:** While being on public network, one of the best ways to enhance protection is by enabling the two-factor authentication on any service that offers it. This gives an assurance that even if an attacker gains access to passwords while the device is using public network, they still won't be able to access accounts. There will be a second log in step, may be a call or code on the device that will be used to log in that account.
- **Operating System should be Up to Date:** The operating system, with every update, often includes important security patches that can further protect the device from Wi-Fi threats. It is a very crucial step to update operating system as it ensures safe browsing experience.
- **Use of Antivirus Software:** Installing antivirus software in the device is another method to protect from threat of personal data leakage. If this software is installed, it protects from threats such as computer viruses and spyware.
- **Always Log Out:** Once the website browsing is completed, it is a must to log out from the services being used. It should be made sure that the settings of "forget the network" is applied. If not then it may automatically again reconnect to that network without permission once the device comes within the range. This will help in minimizing the time a device was connected to a particular public network.

[5] Samaresh Acharya, Bluetooth, free public wi-fi most potent tools for cybercrooks, TOI, November 21, 2023
[6] VPN, Tech Target, (https://www.techtarget.com/searchnetworking/definition/virtual-private-network)

- **Turn off File Sharing:** File sharing must be turned off before accessing public Wi-Fi. If that setting is on, the folders may be accessible to anyone connected to the same public network creating a threat to personal information.
- **Adjust Connection Settings:** Configuration of wireless setting on the device to not automatically connect to available public hotspots. Doing this will prevent the device from broadcasting that it is trying to connect to available hotspots and will save them from attacker's eyes.
- **Use Browser Extensions:** Consider the installation of an extension like "HTTPS Everywhere", which will force all the websites visited to connect using HTTPS. This is a Firefox, Chrome, and Opera extension which reduces the risk of ending up on an unsafe website.

Conclusion

The question remains unchanged. Whether Public Network is a threat or shield to personal data. In this era of continuous changes in technologies, networking is an integral part of life which cannot be ignored. Public Network as discussed is an accessible, affordable, barrier free and easily available network surrounded with various threats. Accessing to this network can result in threats of malwares, viruses, data theft, identity theft, fraud, etc. However, everything has pros and cons. If public networks are easily accessible to everyone it is also surrounded with threats. And if this network is constituted with threats, it also has its own shield for protection. Therefore, whether public network is a threat or shield to personal data depends on the user. If the user is careless and makes even a slightest mistake during his connectivity to public network, he will risk his own personal information. Hence, the preventive measures should be kept in mind and followed at all times to shield one's own personal data. Nonetheless, public network is both a threat as well as a shield to an individual's personal data.