International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Safety Measures to be Maintained while Using Public Wi-Fi

Pallavi Suresh Poojary

Student ,Depatment of Msc-IT Keraleeya Samajham Model College, Dombivli , India

ABSTRACT

Now a days internet connectivity has become one of the major important need, due to which people always look for an access to internet. With shops , cafes , malls etc providing free access to wifi has become a convenient way to keep a check on social sites , email etc .When people are out it is convenient for them to get free access to the public wi-fi . But getting access to the public wifi has always risk of compromising the device's security. These are networks which are used my millions of people on daily basis . among which some of them can be hackers as well. Data sent through public wifi can be easily hacked by the attackers , also if the device is not protected by anti-malware then they are more prone to attack. The purpose of this paper is to investigate which are the techniques which can help the user to keep their device safe from an attacker , while using public wifi .By collecting and studying various research paper , journal , and websites , the techniques and methods for prevention of attack on device while using public wifi.

Keywords: Data Privacy, Prevention, Techniques, User, Public Wifi

1. Introduction

We live in an era where most of the people own a laptop , mobile phones etc. which most of the times need an internet connection , and it gets convenient for the user if they get free access to internet when they are outdoor.

Using an unsecured network can always risk the users device's security . The device which doesn't have anti malware security makes it more prone to attack.

The public wifi makes it easier for the attacker to hack the user's data and misuse it later. So to avoid such attack it is necessary to users to follow some techniques for keeping their device from attack while using public wifi.

2. Background/Literature Review

A recent study made by Kaspersky , Hackers can also use an unsecured Wi-Fi connection to distribute malware. If user's allow file-sharing across a network, the hacker can easily plant infected software on user's computer. They also found "that about 80% owners of tablet and 43% of mobile phone users use free public WiFi networks . A table report indicated that 45 % of all mobile devices were used to access free wifi.

Some attackers have also managed to hack the connection point itself, which causes a pop-up window to appear during the connection process offering an upgrade to a software . By just clicking the window , it installs the malware. According to study made by internet and society on 09 December, 2016With hackers finding it easy to access personal information of the data subjects, data can be hacked by unauthorized internet access by spoofing the MAC and IP addresses of the user's device or by use of default settings (saved passwords or IPs). Crucial data like social sites , password of social account , bank account information etc , are at risk

* *Corresponding author.*

E-mail address: pallavipoojary9@gmail.com

3. Method and Materials

- Journals , Newspaper, Case studies and Research papers all related to security while using public wifi are been collected analyzed and compared to study what are the attacks which may happen while using Public wifi and what are the methods which can be used for securing the device while using public wifi
- This research is based on Secondary data

4. Data and Results

- After surveying through various Research papers , articles of news paper etc, It has came to light that there are several attacks which might happen if a user access an unsecured public wifi .
- Man in the Middle attack
- Man-in-the-middle (MITM) attacks and rogue hotspots are ways that these cyberattacks happen in these public wfifi network. According to study made by Norton, MITM attacks happen when hackers violate a security vulnerability in the network to intercept data.
- The cybercriminals sniff out information from browsing activities, account log-ins, and eCommerce transactions. Crucial information, such as passwords and financial data are exposed to hackers . Cybercriminals could intercept communications between two systems who believe they're communicating directly with each other, unaware of a snooper in the middle.
- Rogue Wi-Fi Networks
  Here the hackers creates a wifi network which looks legitimate for the user , or perhaps even clones a trusted network. User's may recognize such fake networks because they mention something that makes them look appealing like "Free Access" or "No Password." Avoid these unsecured networks as much as possible. If user's are accessing a public Wi-Fi in a cafe or restaurant, they will have a password in place for users .
- Packet Analyzers
  Packet analyzers, also known as small computer codes which monitors traffic on the given network . They can also intercept some data packages and can provide information about the content . These types of codes are used in a non-malicious way, so that they can gather data about traffic. Some codes capable of installing errors, to test out whether the network is capable of handling the error or not . Rogue Access Points
  Rogue APs differ from rogue networks. Though they are similar in nature, rogue APs are nothing but access points installed in pre existing network. They usually come in the form of wireless routers. Usually they are installed by employees, to give more customers access to the Wi-Fi network. But many times these router may have not been configured properly due to which the attacker gets a chance to exploit the system even though it been secured.
- Evil Twins
  An evil twin is somewhat similar to the rogue AP, but it's much sophisticated interms of masking it's purpose. They are designed to look and act like legitimate networkHackers can clone an AP user's know and trust, and create one that is identical. When user's connect via this AP, user's are actually connecting to the evil twin, which then proceeds to send info to the hacker.These Wi-Fi networks are extremely exposed to these types of attacks.

Security measures to be followed while using Public wifi

After surveying through the news articles , journals and research paper written by a cyber security expert . After comparing through these article , there are few common and important measures mentioned by them which might help the users to protect there device while using public wifi

- Always be careful while using public wifi , avoid transaction crucial data over network.
- Never to connect through unknown wireless access points.
- Install VPN in devices.
- Install an anti virus software.
- Avoid money transaction while using public wifi.
- Always connect with the sites starting with https.
- Avoid entering passwords while using public wifi.
- Always keep the os and apps updated of the systems

5. Discussions

The main purpose of this paper to find out what are the threats and what are the security measures which needs to be followed while using public wifi .
Accessing the public wifi without any security measures may create a doorway for the hackers to attack the device of the user. Sending data through an unsecured network makes it easier for the attacker to hack the data of the victim. Accessing a free public wifi seems to be very convenient , but for the hacker it an easy opportunity to violate the users device. Many internet and cable firms offer complimentary secure hot-spots for their customers due to this concern, with customers logging in using their account profile to access high-speed wi-fi hot-spots, with built in security firmware. When available, make use of this networks

- Users must always be careful while using public wifi , even if using public wifi make sure not to transfer important data through out the network and avoid making transactions at that time .
- Never connect to any unknown wireless access point . Sometimes the cybercriminals create a bogus link that has similar name as the cafe or the shops name , therefore before accessing contact the shop owner and ask for their wifi access point.
- Mostly it's recommended to have VPN installed in the devices while accessing the public wifi . VPN will create a private tunnel which will encrypt all data that passes through the network .
- Always be careful while using public wifi , avoid transaction crucial data over network.

6. Conclusion

First of all people must be made aware of the risks of using public wifi , they must be warned about using an unsecured network for sharing an important data through out that network. Sometimes people access such network in case of emergency and attackers always look forward for opportunity to hack into such vulnerable system and collect important information. Therefore user must always avoid accessing such networks . If accessed then avoid making bank transactions, entering passwords or sending some crucial data in to that network.

Most common attack which happens while using public wifi is Man In The Middle Attack , here if for example if data is sent from person A to person B through unsecured network then attacker can intercept the data being transferred between two systems. To avoid such attacks VPN is mostly suggested for the users to install. What VPN does is that it creates a private network through public internet connection . It masks the ip address of the devices and makes it anonymous . It creates an encrypted and secured connections for the user. Always before accessing a wifi network make sure that the network is legitimate , such networks always have attractive offers like "no password " , "free access ". Avoid such networks Because there is a high chance that it might harm user's device. Another suggestion is to always visits sites which starts with HTTPS . To avoid file sharing while using Public wifi. While using pubic networks always keep the firewall enabled.

Acknowledgements

I would like to express my special thanks of gratitude to all my teachers for their able guidance and support in completing my research. I also like to extend my gratitude to the Principal Sir "**Dr. Ravindra P Bambardekar**" for helping me with all the facility that was required
.

References

- Ni,Qiang,Romdhani,Lamia,and Turletti,Thierry,"A Survey of QoSEnhancements for IEEE 802.11 Wireless LAN",Journal of WirelessCommunication and Mobile computing,Vol.4,No.5,2004,pp547-566
- Mani Subramanium,Network Management-Principles and Practices,2nd Edition,Pearson,2013.
- Gast,Matthew,802.11 Wireless Networks:The Definitive Guide,2nd Edition,O'Reilly Media,Inc.,2005
- Zhao Xin. Global WIFI users has reached 700 million, [j]. The people's post and telecommunications, 2011 (9) 35-36, in Chinese.
- J. WELCH , S. D. LATHROP , A Survey of 802.11a Wireless Security Threats and Security Mechanisms. United States Military Academy West Point , New York, (2003), http://www.itoc.usma.edu/Documents/ ITOC TR-2003-101 (G6).pdf.
- White paper: Testing for Wi-Fi Protected Access (WPA) in WLAN Access Points. Net-O2 Technologies, (2004), http://whitepapers.zdnet.co.uk/0,39025942,60152756p,00.html
- Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010, September). The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In Proceedings of the 12th ACM international conference on Ubiquitous computing (pp. 321-330). ACM
- F-Secure (2014), THE F-SECURE WI-FI EXPERIMENT, www.fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f-secure.pdf
- Florêncio, D., Herley, C., & Coskun, B. (2007). Do strong web passwords accomplish anything? HotSec, 7, 6.
- Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. Psychological bulletin, 125(3), 367.
- Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009, April). When i am on wi-fi, i am fearless: privacy concerns & practices in everyday wi-fi use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1993-2002). ACM