CONCEALED CYBER RISKS: NAVIGATING THE PERILS OF PUBLIC WI-FI

Apurva P
Sambhram University Jizzax

Annotation. This paper aimed to assess trends in public Wi-Fi usage, the level of awareness regarding the associated risks, and the presence of self-imposed safety measures. To achieve this, a survey was conducted with a convenience sample of 80 participants. The findings revealed a high frequency of public Wi-Fi use among individuals for activities like checking emails, logging into social media, and general browsing. However, there was a significantly lower engagement with public Wi-Fi for financial and banking purposes. This indicates that while users might recognize the risks, there is a pressing need for enhanced education to empower individuals to adopt necessary precautions, as well as to foster collaboration among stakeholders to protect public Wi-Fi networks. Consequently, this study highlights a relatively limited understanding of the dangers associated with public Wi-Fi usage, despite an increasing demand for its installation and use, raising concerns amid our growing dependence on digital technologies.

Keywords: Public Wi-Fi, Cybersecurity, style, styling, insert (key words*)*

I. Introduction

A. Society today is marked by an increasing demand for convenience alongside a fast-paced lifestyle. This has led to trends like remote work and e-learning, largely driven by the rise of the digital era and the resulting shifts in our environments. Consequently, many venues such as coffee shops, airports, libraries, and public transit systems now provide free public Wi-Fi for their customers. For many of these establishments, offering public Wi-Fi serves primarily as a marketing strategy, often neglecting proper network configuration, which increases cybersecurity risks. This is particularly true for networks that require no authentication and lack traffic encryption. While public Wi-Fi provides easy and often free connectivity, it is susceptible to cyberattacks, becoming a prime avenue for attackers to gain access to sensitive information. Thus, public Wi-Fi not only faces security threats but also jeopardizes users' online privacy.

B. Justification

Public Wi-Fi is increasing across establishments with the increased virtualization of routine activities such as working and learning. However, it is emerging as a key source of security and privacy risks due to its both configuration and usage patterns. From a configuration stance, some networks use older encryption standards and with the increased complexity and scope of cyber-attacks, this makes them weak and susceptible to being hacked. Also, because of the increased utility of public Wi-Fi, another risk related to configuration is that one is at risk of connecting to a fake or malicious hotspot (Johansen, 2021). That is, an attacker can create a fake hotspot to intercept traffic from unsuspecting victims. This way, it is possible to capture valuable information, which can be used as a platform to launch other attacks or allow for lateral movement. With regards to the role of usage patterns, Flockett [2] outlines that for most people the security of the public Wi-Fi is not a key priority to consider, instead, more focus is on the utility of a network. As such, most users' select Wi-Fi networks based on its strength, appropriateness of its name, or they will indiscriminately connect to the available free network. Therefore, with public Wi-Fi increasingly becoming a standard for most establishments, there is a foreseeable increase in cybersecurity risks. However, because of their utility in present-day society,there is a need to determine the best practices when using public Wi-Fi.

C. Research aim and objectives

This study will concentrate on identifying trends in public Wi-Fi usage, including the level of awareness regarding existing risks and the protective measures individuals take on their own. To this end, it will aim to address the following research objectives.

- To determine the degree of awareness on the risk associated with public Wi-Fi use.
- To establish the prevalence of public Wi-Fi.

II. Literature review

A. Prevalence of public Wi-Fi

Public hotspots are rising exponentially both within a state and across the globe. This is

being driven by the increased penetration and utilization of the internet, smartphones, and smartphones. As such, connectivity is emerging as an ideal that should be promoted especially in light of the prevalent realities such as e-learning, increased social media use, and remote working. As such, this is resulting in a unique confluence of self-reinforcing factors. That is, the increased number of devices with internet connectivity is increasing the need for ubiquitous connectivity. In turn, establishments are responding by installing public Wi-Fi to appeal to the market due to the latent need for connectivity. Also, this increased availability of public Wi-Fi is in turn stimulating both the adoption of connectivity-enabled devices such as smartphones, which in turn conflates the demand for public Wi-Fi. In line with this, it is estimated that in 2017 there were 50 million hotspots across the US, and with the significant continued increase in public Wi-Fis, it is estimated that 340 million hotspots would translate to 1 hotspot for every twenty people globally [8]. Similarly, while 61 percent of households in the US had Wi-Fi installed in their homes, 64 percent of this population will also use public Wi-Fi on their smartphones whenever they leave their houses. This way, it can be outlined that the population is opening itself up to both security and privacy risks because of the increase in accessible hotspots, increase in connectivity enabled devices and their utilization rates (especially laptops and smartphones), and the increased utility of public Wi-Fi to the populace.

With the increased dependence on information technology, cyberattacks are increasing in both incidence and severity. Also, the increased mediatization of routine activities is contributing to the increased dependence on information technology solutions and computer networks. With regards to the increased adoption of public Wi-Fi, it is important to contextualize this growth within the link between increased internet interconnections and cybersecurity incidents [4]. This way, as more public Wi-Fis are installed across organizations, this is contributing to the rise of a new vector of attack for cybercriminals. This is outlining the need for targeted interventions attending to different groups of users and also the implementation of security mechanisms to not only bolster confidence levels but also promote privacy protection [4]. Therefore, it is foreseeable that with the increased mediatization of society, public Wi-Fi implementation and utilization are poised to rise. In turn, this will increase both the severity and incidence of cyber-attacks if effective protections are not put in place.

H1: The increased utilization of computing devices (laptops and smartphones) is stimulating both public Wi-Fi use and installations.

B. Risk factors associated with risky public Wi-Fi use

Increased dependence on computer networks and information solutions is linked to increased cyber security risks and financial burdens. Due to the attractiveness of cyber-attacks, it is expected that there will be an increase in the number and scope of cyber-attacks. When contextualized with public Wi-Fi use, it is important to evaluate the risk within the fact that cyber criminality is fundamentally grounded on having internet connectivity and a computer [4]. Therefore, while public Wi-Fi is rated as having great utility for most of the members of the public, there is little understanding of the underlying security and privacy risks. Also, in line with the observation by Johansen

[5] that some public Wi-Fis use older encryption standards which increase the susceptibility of a network to an attack, Gregory et al. [3] note that businesses are still lagging with regards to the development and implementation of procedures and protocols that relate to the use public Wi-Fi. Like users, businesses also have an inadequate understanding of the privacy and security risks associated with public Wi-Fi. As such, this points to some degree of disconnect between the promotion of utility and safeguarding users with the core user groups being significantly unaware of the underlying risks associated with public Wi-Fi use.

With awareness having been established as a key approach to promoting effective public Wi-Fi use, it is important to note that there is a need to empower the population to adopt cyber-security sound behaviors in their use of public Wi-Fi. As outlined by Bencie [1], even for those with an understanding of the underlying risks of using public and unsecured networks most people will still use the networks. Hence, this shows that the increased awareness of the associated

concerns without taking any remediation step is a risk in itself. To this Bencie [1] posit that for members of the public it is common to think that cybersecurity concerns are mainly prevalent in corporations. In line with this, Sombatruang et al. [6] note that people will transmit sensitive data through public Wi-Fi even when they areaware of the inherent risks. In turn, this presents the need to understand the relationship between risk awareness and risk behavior whereby the utilization of public Wi-Fi is not purely a decision of maximizing utility although saving data plans is a key contributing factor to public Wi-Fi use. As such, this shows that the decision to use public Wi-Fi is significantly a form of resource preservation method and less of a well-thought-out evaluation of costs and benefits. Similarly, Bencie [1] posits that while most people are cautious about public Wi-Fi, they will tend to use non-secure networks. This goes to show that increasing awareness is not enough to promote effective behavioral changes, hence, this shows that utilization of public Wi-Fi isnot entirely a logical decision, which points to the need for intensive approaches.

H2: Increased awareness of the risks posed by public Wi-Fi use does not translate to the adoption of protectivebehaviors.

III. METHODOLOGY

To evaluate a number of factors, a convenience sample of 80 participants was given a quantitative survey questionnaire. This approach was deemed successful since a survey questionnaire is thought to be a dependable and simple research tool, and quantitative methods are excellent for spotting trends and patterns. Statistical techniques were used to quantify and illustrate the trends and patterns pertaining to public Wi-Fi usage in the analysis of the responses that were gathered. Insights from the literature review were also contrasted with the results of this analysis.

IV. Results and analysis

A. Utilization of computing devices and public Wi-Fi usagetrends

Today, most establishments such as coffee shops, airports, libraries, public transit among others are now offering free public Wi-Fi for their clientele as a marketing strategy Johansen and Pehar [5,6]. This study draws from this to determine the magnitude of utilization of public Wi-Fi and the knowledge of the associated cybersecurity risks across society. The results of the analysis are as follows: when accessing public Wi-Fi. As such, this research study supports the hypotheses generated from the review of the literature:

Question	Agree	Disagree
Are you likely to go to a location because of free Wi-Fi	56 (70%)	24 (30%)
Are you likely to stay longer in a location because of Wi-Fi	59 (74%)	21 (26%)
Are you likely to spend moremoney in a location because of Wi-Fi	53 (66%)	27 (34%)
Are you likely to do your banking on public Wi-Fi	15 (19%)	65 (81%)
Are you likely to check your emails on public Wi-Fi	61 (76%)	19 (24%)
Are you likely to update your social profiles on public Wi-Fi	64 (80%)	16 (20%)
Are you likely to browse theweb using public Wi-Fi	55 (69%)	25 (31%)
Are you likely to use public Wi-Fi for work purposes	22 (28%)	58 (72%)

Table 1: Use of public Wi-Fi

H1:The increased utilization of computing devices (laptops and smartphones) is stimulating both public Wi-Fi use and installations.

H2: Increased awareness of the risks posed by public Wi-Fi use does not translate to the adoption of protectivebehaviors.

From the table 1 above and using some verbal

Discussion

According to the Commonwealth Department ofCommunications, majority of the society members have little awareness of the cybersecurity issues and concerns. A similar trend can be inferred from the results of the study, which in turn establishes the need for public awareness

campaigns on cyber safety. As such, while the aim is not to demonize public Wi-Fi usage, there is an inherent need to promote the degree to which the society is informed so they can take the necessary precautions, or be informed of the consequences of indiscriminate public Wi-Fi use (Reed, 2020). To this, it is outlined that the main attack orchestrated on public Wi-Fi is the man in the middle attack where a cybercriminal places themselves between a user and the services they are utilizing. This is critical because the cybercriminal is not only in a position to see a user's activity, but they can also make changes to requests by a user to a system or the replies sent by a system to the user.

While the government bears the central mandate to responses, the research established that the use of Wi-Fi in public places is significantly high as 75% of the respondents use public Wi-Fi and more 79% consider public spaces based on the availability and utility of public Wi-Fi. In line with this, the research established that 70% of the respondents actively look for locations or go to a location because of the free Wi-Fi being offered there. To make it even more interesting is that 66% of the public would opt to even spend more in a location because of the provision of free Wi-Fi. It was also established that 74% of the respondents tend to always find themselves staying longer in a venue because of the utilization of free Wi-Fi.

Some worrying trends are that, 19% of the respondents agree that they can or they perform their banking transactions while on the unsecured free public Wi- Fi. When it comes to checking emails, 76% of them always try to find updates on their emails when on public Wi-Fi. Social media, which is common, is at 80% chance of being accessed on free public Wi-Fi. Also, 69% browse the web most times while connected to public Wi-Fi. Another worrying trend is that a good number, 28% of the respondents use free public Wi-Fi for work-related purposes. Looking at the usage durations, we discovered that 52% of people use public Wi-Fi at least once every week and 17% use it at least once every month.

With the increased indiscriminate utilization of public Wi-Fi, it is plausible that either people lack the knowledge of how to safely use it or they are ignorant of the risks. Similarly, Flockett [2] asserts that most people are not concerned about cybersecurity risks but with the utility of the network. For instance, how strong the network is, how available and if it is entirely free. We can therefore make a conclusion that best practices need to be imposed on people promote public sensitization campaigns, there is also a need for a multi stake holder approach. From the research this is established by the high demand and preference for establishments with public Wi-Fi connections. For instance, financial institutions can be actively involved by sensitizing their customers to not making transactions over public Wi- Fi either through mobile or ecommerce platforms. Similarly, the establishments themselves also have a role to play by informing the clientele the risks associated with public Wi- Fi use and the steps they have taken if any, and also how the customers can further protect themselves from falling victim [6]. Finally, since remote working is a key contributor to the increased rate of public Wi-Fi usage, employers also have a role to play by setting up public Wi-Fi usage protocols in addition to training their workforce on the risks and how to safeguard themselves and the organization's network and information assets. Also, it should be standard practice that employers should provide their workforce with a VPN they can use when using public Wi-Fi to reduce the risks posed by human factors such as ignorance or forgetfulness [1,7]. Therefore, with the relative increase in public Wi-Fi usage, there is a need for a holistic approach to empower the population whilst also building the necessary technological capacity to secure users when they are using public Wi-Fi connections.

V. Conclusion

Public Wi-Fi installation, demand, and utilization are on the rise. While they are source of significant benefits for majority of the population, there is a need to evaluate the cybersecurity risks associated with its usage to safeguard users and to ensure cyber secure trends and patterns due to the increased incidence of cybersecurity attacks. This is especially critical because of the noticeable indiscriminate public Wi-Fi usage where people are mainly focused on the utility metrics and not the cybersecurity implications. However, there is some degree of awareness of the associated risks due to the noticeable low self-reported rate of public Wi-Fi to connect to

finance or banking services. To this, there is a foreseeable approach to promote cybersecure trends, that is, quantifying the risk to an individual. This is especially because there is a high utilization of public Wi-Fi to access emails and social networking sites, which also has privacy and confidentiality concerns, coupled with a preference for locations with public Wi-Fi. Therefore, while it is impossible and defeatist to challenge the rising prevalence of public Wi-Fi, it ispossible to empower users and organizations to institute the right measures and procedures to mitigate the prevalent and emergent cybersecurity risks.

REFERENCES

[1] L. Bencie, "Why You Really Need to Stop Using PublicWi-Fi," *Harvard Business Review*, 2017. [Online]. Available: https://hbr.org/2017/05/why-you-really- need-to-stop-using-public-wi-fi. [Accessed: 13- Jan- 2022].

[2] A. Flockett, "Hidden dangers of public WiFi and how toavoid them," *Electronic Specifier*, 2019. [Online]. Available:https://www.electronicspecifier.com/products/cyber-security/hidden-dangers-of-public-wifi-and-how-to- avoid-them. [Accessed: 13- Jan- 2022].

[3] M. Gregory, I. McShane, and C. Wilson, *practicing safepublic Wi-Fi - Assessing and managing data-security risks*. Melbourne: Centre for Urban Research (CUR), 2016.

[4] J. Jang-Jaccard and S. Nepal, "A survey of emergingthreats in cybersecurity", *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014. Available: 10.1016/j.jcss.2014.02.005.

[5] A. Johansen, "Public Wi-Fi security: Why public Wi-Fi is vulnerable to attack", *Norton*, 2021. [Online]. Available: 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. [Accessed: 13- Jan- 2022].

[6] D. Pehar, "Cybersecurity and Public Wi-Fi," *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2020/ 08/06/cybersecurity-and-public-wi-fi/?sh=1fc996e311f7. [Accessed: 13- Jan- 2022].

[7] D. Reed, "Why WiFi is a Security Risk for Your Business's Wireless Network," *Advanced Network Service*, 2020. [Online]. Available: https://www.anscorporate.com/blog/why-wifi-is-a- security-risk-for-your-businesss-wireless-network.[Accessed: 13- Jan- 2022].

[8] E. Shahin, *Is WiFi Worth It: The Hidden Dangers ofPublic WiFi*. 2017.

[9] U.M.Yarlakabov Didactic Ways of Forming Students' Technical Thinking.- Eastern European Scientific Journal, 2018 - journale.auris-verlag.de

[10] Sharipov Sanjar. Vocational orientation through the development of mathematical competences in the students of technical higher education institutions. CURRENT RESEARCH JOURNAL OF PEDAGOGICS. 3. No. 06 (2022). 58-64. https://doi.org/10.37547/pedagogics-crjp-03-06-10

[11] Nadirova-Kazan, H. (2023, November). EXPLORING THE CONTENT OF MEDIA LITERACY: A COMPREHENSIVE REVIEW. In International Scientific and Current Research Conferences (pp. 107-110).

[12] Mahkamov, S., Aynakulov, T., & Baratov, J. (2024). ANDROIDDA MODEL VIEW PRESENTER (MVP) ARXITEKTURASI. International Journal of scientific and Applied Research, 1(3), 199-202.

[13] Ikrom Kulanov, Sneha Latha, Azizbek Uzakboyev, Shakhzoda Burkhanova. Effect of gyrotactic microorganisms on electrically conducting carreau nanofluid flow along an exponentially stretching surface in the presence of chemical reaction. Problems in the textile and light industry in the context of integration of science and industry and ways to solve them: ptlicisiws-2.4–5 may 2023.Namangan, Uzbekistan.AIP Conf. Proc. 3045, 030066 (2024). https://doi.org/10.1063/5.0197498

[14] Sanjar Sobirovich Sharipov. IMPLEMENTATION OF SPECIAL AND GENERAL PROFESSIONAL INTEGRATION AS A PEDAGOGICAL PROBLEM Scientific Bulletin of Namangan State University.2020. 2-8. 364-370-p.