Scientific Journal of Impact Factor (SJIF): 7.37

E-ISSN (O): 2348-4470
P-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 13,Issue 11,November 2026

Cybersecurity Research on Public Wi-Fi Risk Awareness and Security Behavior Among Internet Users.

Victoria Imafidor[1]*, Maria Valentin[1], Asaduzzaman[1], Sawad Sani[1]

[1] *Department of Mathematics and Computer Science, Southwest Minnesota State University, Marshall, Minnesota, United States*

**Corresponding author: Victoria Imafidor (victoria.imafidor@my.smsu.edu)*

Abstract —*Public Wi-Fi is available in many everyday places, including coffee shops, airports, libraries, malls, and universities, making it easy and convenient to get online. However, many users do not fully understand the security risks that come with connecting to these networks. Some people believe that public Wi-Fi is safe as long as they avoid activities like online banking, but even simple actions such as checking emails can expose personal information on an unsecured network. This gap between what users know about Wi-Fi security and how they behave is a growing concern, especially as attackers use methods such as Man-in-the-Middle attacks and fake Wi-Fi networks to take advantage of users. This study examines the relationship between users' awareness of public Wi-Fi security risks and their actual online behavior on these networks. Data were collected through an online survey of 100 participants, measuring both self-reported awareness of security risks and self-reported behaviors while using public Wi-Fi, such as checking emails, shopping, or logging into personal accounts. Results showed that 85% of participants recognized at least some degree of cybersecurity risk, yet 73% reported having accessed an important account while using public Wi-Fi. These findings suggest that awareness alone is not enough to prevent risky behavior, and that users may need clearer, more practical advice on how to stay safe while using public Wi-Fi.*

Keywords—*Public Wi-Fi, Cybersecurity awareness, Security behavior, Virtual private network (VPN), Cybersecurity education*

I. INTRODUCTION

Today, public Wi-Fi is available in many places, including coffee shops, airports, libraries, and universities. It makes getting online easy and convenient, but many users may not think about the security risks that come with using these networks. Some people believe that public Wi-Fi is safe as long as they avoid activities such as online banking or entering other sensitive information. However, an unsecured or poorly protected network can still put users' information at risk.

One of the main concerns is the difference between what people know about Wi-Fi security and how they behave. Even if users know that public Wi-Fi may not be secure, they often continue to use it because of its convenience. Attackers can take advantage of this through methods such as Man-in-the-Middle (MitM) attacks, fake Wi-Fi networks, and packet interception. Users may also check their email, shop online, or log into personal accounts without checking whether the network is trustworthy or paying attention to browser security warnings. These actions can increase the risk of personal information or login details being exposed. This study looks at the relationship between users' awareness of public Wi-Fi security and their actual online behavior. By comparing what users believe they know about security with the activities they perform while using public networks, this research has a goal to identify common risky behaviors. Understanding these behaviors can help show where users need more practical security information and encourage safer habits when using public Wi-Fi.

II. MATERIALS AND METHODS

This study surveyed 100 participants to examine the relationship between awareness of public Wi-Fi security risks and actual online behavior on public networks. Participants were recruited through in-person outreach on campus, including posters, tabling events, and direct conversations with students, faculty, and staff, as well as a survey link distributed university-wide through the school's app. Eligibility was limited to individuals 18 years of age or older who consented to participate anonymously.

Of the 100 participants, 84% were current students, 13% were employed full-time, and 3% were employed part-time. Participants' ages ranged from 18 to 64, and education levels ranged from completed high school or equivalent to doctorate degree. The sample was predominantly composed of current college students, representing a population with regular exposure to digital devices and online platforms. Data were collected using a survey created and distributed through Google Forms. Participants first completed a consent and eligibility section confirming they were 18 or older and agreeing to participate anonymously. Participation was voluntary, no personally identifiable information was collected, and participants could exit at any time by closing their browser.

@IJAERD-2026, All rights Reserved

The survey measured two main areas. The first was awareness, defined as participants' self-reported understanding of public Wi-Fi as a cybersecurity risk. The second was behavior, defined as participants' self-reported actions while connected to public Wi-Fi, including how often they use public networks, whether they log into important accounts on them, whether they adjust their behavior based on perceived risk, and which activities they consider acceptable to perform while connected. Comparing these two measures allowed the study to assess whether awareness of risk corresponds to safer behavior, or whether a gap exists between what users know and what they do. All participants provided informed consent before beginning the survey, and no identifying information was collected at any point, ensuring participant anonymity throughout.

III. RESULTS AND DISCUSSION

The results indicate that public Wi-Fi is a regular source of internet access among respondents. Of the 100 participants, 37 (37%) reported using free public Wi-Fi daily, 13 (13%) used it a few times a week, and 20 (20%) used it a few times a month. Together, 70 respondents (70%) used public Wi-Fi at least monthly. An additional 27 (27%) reported rarely using public Wi-Fi, while only 3 (3%) indicated that they never used it. These results establish that public Wi-Fi exposure is common within the study population rather than being limited to occasional use.

The continued use of public Wi-Fi can partly be understood through its accessibility and convenience. Maimon et al. describe public Wi-Fi as providing a “convenient, cost-effective way for accessing the Internet” [1]. The same study recognizes that public Wi-Fi presents security concerns, stating that “accessing public Wi-Fi networks can be as dangerous as it is convenient” [1]. Potnuru similarly observes the expanding availability of wireless access, noting that “more wireless access points, known as ‘hotspots,’ are becoming readily available” [2]. The frequency identified in the present survey therefore supports examining protective practices rather than assuming that users can simply avoid public Wi-Fi.

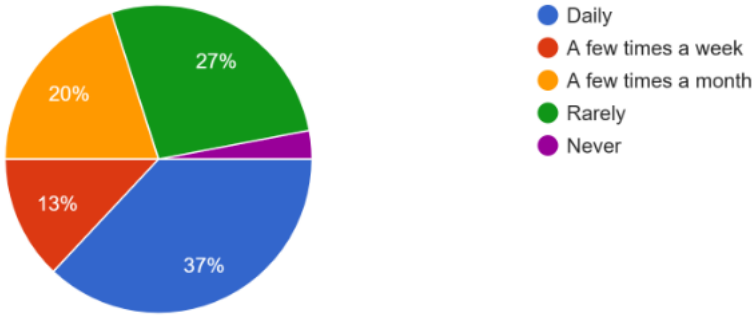


Figure 1. Frequency of Public Wi-Fi Use

Respondents demonstrated substantial awareness that public Wi-Fi can present cybersecurity risks. Of the 100 participants, 21 (21%) considered public Wi-Fi a major risk and 46 (46%) considered it a moderate risk. Therefore, 67 respondents (67%) classified public Wi-Fi as either a major or moderate cybersecurity risk. Another 18 (18%) considered it a small risk, meaning that 85 of 100 respondents (85%) recognized at least some degree of cybersecurity risk. Thirteen respondents (13%) were unsure, while only 2 (2%) stated that they did not consider public Wi-Fi a risk.

These findings indicate that a general lack of risk recognition may not be the primary issue among this sample. Existing literature nevertheless demonstrates why this recognition is warranted. Potnuru states that unsecured Wi-Fi can expose communications to “the dangers of ‘packet sniffing,’ a technique used for eavesdropping on a network” [2]. Maimon et al. similarly explain that open public networks can make “users vulnerable to privacy and security attacks” [1]. More importantly for the present study, the authors report that “a significant amount of users continue to put their security at risk” despite continuing awareness efforts [1]. This distinction between recognizing risk and responding to risk becomes important when the remaining survey findings are considered.

@IJAERD-2026, All rights Reserved

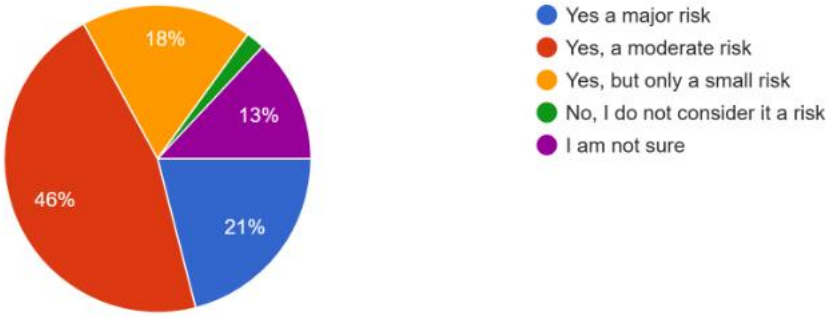


Figure 2. Perceived Cybersecurity Risk of Public Wi-Fi

Despite widespread recognition of public Wi-Fi risk, accessing important accounts while connected to these networks was common among respondents. Fifteen participants (15%) reported doing so frequently, 25 (25%) occasionally, and 33 (33%) rarely. Collectively, 73 of 100 respondents (73%) reported having accessed an important account through public Wi-Fi to some degree. Only 21 respondents (21%) reported that they had not done so, while 6 (6%) were unsure. This result is notable when considered alongside the finding that 67% classified public Wi-Fi as a moderate or major cybersecurity risk. Previous research identifies accessing personal information as an important component of public Wi-Fi security behavior. Maimon et al. found that people who were more situationally aware were "less likely to access personal accounts on public Wi-Fi" [1]. The authors further identify protective online practices including "using remote VPN or avoiding accessing personal information while on the network" [1]. Potnuru also notes that packet sniffing can potentially expose "personal passwords, financial records, and other sensitive information" [2]. The present findings therefore suggest that awareness of general public Wi-Fi risk does not necessarily correspond with complete avoidance of important account access.

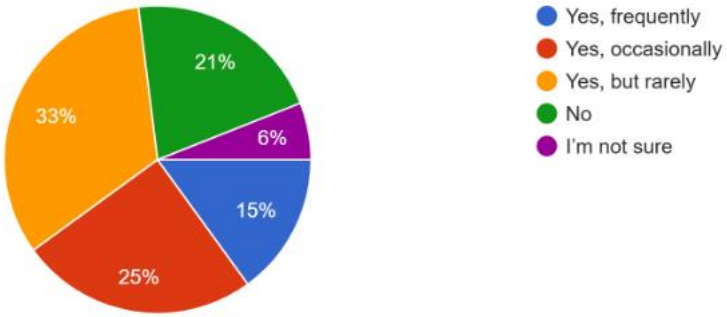


Figure 3. Important Account Access on Public Wi-Fi

Participants reported different levels of behavioral adjustment when connected to public Wi-Fi. Twenty respondents (20%) stated that they always changed their online behavior, while 23 (23%) did so most of the time. Twenty-five (25%) reported changing their behavior sometimes, 14 (14%) rarely changed their behavior, and 18 (18%) never did. Consequently, fewer than half of respondents, 43 of 100 (43%), reported consistently changing their behavior either always or most of the time. In contrast, 57 respondents (57%) changed their behavior only sometimes, rarely, or never. This finding provides further evidence that cybersecurity awareness and protective behavior should be examined separately. Maimon et al. state that "self-protection is effective at preventing victimization" [1]. Their study also describes situational awareness as involving "being mindful of the surroundings and identifying potential threats and dangerous situations" [1]. Practical recommendations reported in the literature include "use encrypted Wi-Fi networks," "use Virtual Private Network (VPN) connections," and avoid transmitting personally identifiable information on unsecured networks [1]. Since most respondents already recognize some level of risk, the findings support cybersecurity education that emphasizes practical protective actions users can employ when they choose to connect, rather than relying exclusively on messages stating that public Wi-Fi is risky.

@IJAERD-2026, All rights Reserved

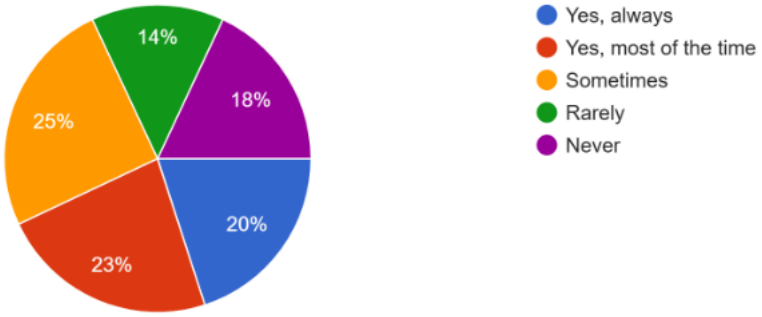


Figure 4. Changes in Online Behavior on Public Wi-Fi

The activity responses provide further insight into how participants perceive public Wi-Fi risk. Social media was selected by 73 respondents (73%), making it the most commonly accepted activity, followed by general web browsing at 67 (67%). School or work accounts were selected by 47 respondents (47%), email by 44 (44%), and online shopping by 40 (40%). In comparison, only 10 respondents (10%) were comfortable conducting banking activities, while 4 (4%) selected none. Because participants could select multiple responses, percentages do not total 100%.

The difference between banking and other account-based activities suggests that respondents distinguish among online activities when assessing risk. The low acceptance of banking indicates caution toward financial information, while substantially greater acceptance of social media suggests that social networking may be perceived as comparatively less sensitive. This distinction warrants attention because public Wi-Fi risks are not restricted to financial transactions. Maimon et al. state that users are advised to avoid transmitting "financial information, usernames, and passwords" on public Wi-Fi [1]. Potnuru describes packet sniffing as technology capable of "intercepting and decoding network communications" [2]. Therefore, the results suggest that public-Wi-Fi education should address the protection of multiple forms of online activity rather than focusing primarily on financial transactions.

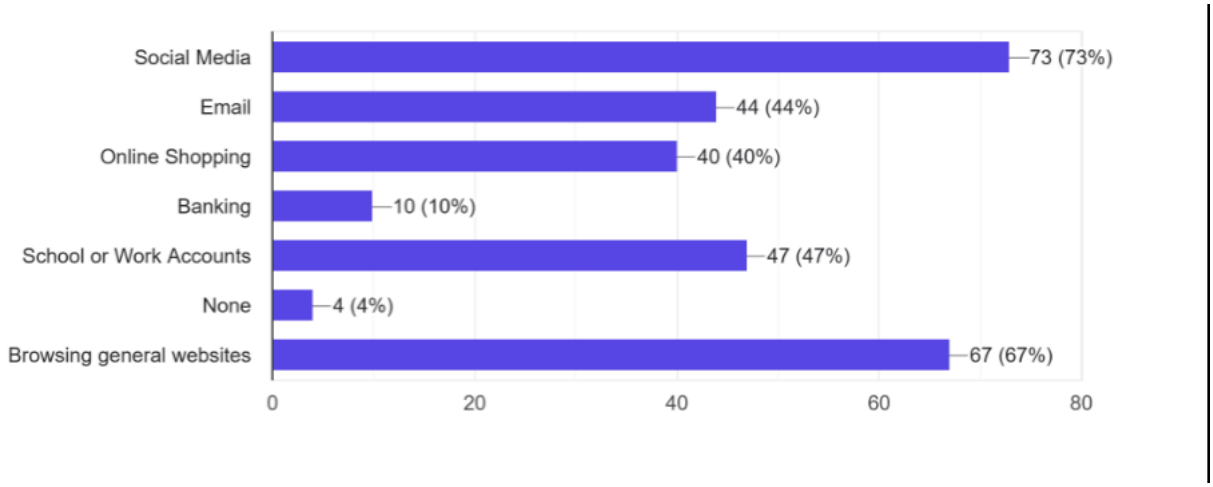


Figure 5. Activities Considered Acceptable on Public Wi-Fi

The combined study shows that most public Wi-Fi users are aware of the dangers involved with using public Wi-Fi and will change their behavior when connected to public Wi-Fi. that users will limit use on financial and banking. The results showed that users were likely to limit financial and banking activities but not social media use. This creates the need for public Wi-Fi security tools and VPN education for the public instead of public Wi-Fi risk awareness. Education should focus on how to safely use VPN and what precautions to take while connected to public Wi-Fi because users will still connect to public Wi-Fi even when aware of the risks. The difference between social media use and banking further suggests that users apply different levels of caution depending on the activity. This supports a practical direction for cybersecurity education focused on helping users protect themselves during public Wi-Fi use. As Maimon et al. conclude, "getting users to reduce their risk online by protecting themselves and their data while using public Wi-Fi networks is a key element of reducing vulnerability to cybercrime" [1].

The central problem this study identifies is not a lack of awareness but a gap between awareness and action. Among the 100 respondents, 67 (67%) rated public Wi-Fi as a major or moderate cybersecurity risk, and 85 (85%) recognized at least some degree of risk, yet 73 of 100 (73%) reported having accessed an important account through a

@IJAERD-2026, All rights Reserved

public network, and only 43 (43%) reported consistently changing their behavior. Because users will continue to connect to public Wi-Fi even when they recognize its risks, solutions should move away from repeating risk warnings and toward building practical protective capability. The literature supports this shift. Sombatruang et al. argue that a "more practical strategy is to urge the public to use a reliable virtual private network not just for sensitive transactions but making a habit of using it whenever they use public Wi-Fi" [3]. Similarly, Mahyoub et al. recommend that users avoid public Wi-Fi where possible and, when no alternative exists, use a VPN to establish an encrypted connection for their traffic (Mahyoub et al., 2025 [reference not supplied]). The present results therefore suggest that cybersecurity education for internet users should prioritize how to use protective tools, not merely why public Wi-Fi is dangerous.

Practical VPN education is an important target because adoption and understanding both lag behind awareness. According to the 2017 Norton Wi-Fi Risk Report cited by Sombatruang et al., only 25% of 15,532 survey respondents across 15 countries reported using a VPN, even though three fourths of participants were placing their data at risk, and 80% admitted using public Wi-Fi for email and online banking [4]. Ramesh et al. further show that users hold incomplete and sometimes flawed mental models of what a VPN provides, what data it can collect, and which threats it addresses, and conclude that user education campaigns concerning VPNs must be prioritized [5]. Education therefore needs to address not only whether users can install a VPN, but whether they understand what protection it offers and when to activate it. Solutions extend beyond the individual users, Sombatruang et al. noted that providers themselves bear responsibility, pointing to Germany's requirement of authentication on all public Wi-Fi hotspots as an example of shifting focus "from fixing the users to other more fixable elements" by encouraging providers to implement secured connections [3]. Complementary behavioral research indicates that situational awareness is associated with safer choices: people who are more situationally aware are less likely to access personal accounts on public Wi-Fi and more likely to cover their screen to prevent others from viewing personal information [1]. Interventions that build this kind of mindfulness may be more effective than abstract warnings. Where structured training is feasible, Nguu and Musuva demonstrate that cybersecurity awareness programs can significantly shape WiFi security behavior through perceived behavioral control, subjective norms, attitude, and behavioral intention, and they present a validated framework for improving employee WiFi security behavior in an organizational setting [6]. Social media was the activity most commonly regarded as acceptable on public Wi-Fi (73 respondents, 73%), far ahead of banking (10 respondents, 10%), and Potnuru describes packet sniffing as a technique capable of "intercepting and decoding network communications" [2] a risk that is not limited to financial transactions. Maimon et al. advise users to avoid transmitting "financial information, usernames, and passwords" on public networks, treating self protection as an effective means of preventing victimization [1]. Education should therefore correct the assumption that social media activity is low risk and teach precautions that apply across all forms of online activity, including the use of encrypted networks, VPN connections, and caution when transmitting personally identifiable information.

IV. CONCLUSION

This study examined the relationship between internet users' awareness of public Wi-Fi security risks and their actual online behavior on those networks. The findings show that awareness is widespread but does not reliably translate into protective action. A majority of respondents recognized public Wi-Fi as a cybersecurity risk, and most reported adjusting their behavior at least sometimes, yet nearly three quarters had accessed an important account while connected to a public network, and fewer than half reported consistently changing their behavior. Social media emerged as the activity users were most willing to conduct on public Wi-Fi, while banking was treated with far greater caution. Together, these results confirm the study's central thesis: internet users are aware that public Wi-Fi is risky and many will modify their behavior while connected, but most still use social media through public Wi-Fi, suggesting that risk recognition alone does not produce consistent self protection.

The main conclusion of the survey is that the problem of connecting or not connecting to public Wifi is behavioral rather than informational. Users are not simply uninformed about public Wi-Fi risk, so continued emphasis on awareness messaging is unlikely to close the gap on its own. What emerges instead is a need to educate internet users on how to protect their browsing activity while connected, with education focused on practical, usable precautions. Prior work supports this direction. Sombatruang et al. found that people can misjudge risky situations and make decisions inconsistent with expected utility, sometimes trading security for convenience or data savings [7], while Swanson et al. describe users as engaging in a form of "naïve security," making choices based on mistaken analogies to the physical world despite increasing awareness of vulnerability [8]. The present findings align with these observations and reinforce that knowledge alone is an insufficient lever for behavior change. Several contributions follow this study. First, it provides empirical evidence of an awareness behavior gap specific to public Wi-Fi use, distinguishing between what users know and what they do. Second, it identifies social media as a distinct area of underestimation, since users appear to treat social networking as comparatively low risk even though the underlying exposure to packet interception is not activity specific [2]. Third, it points toward a practical educational direction centered on VPN use, encrypted connections, and appropriate caution when transmitting personal information, consistent with recommendations in the literature (3; Mahyoub et al., 2025 [reference not supplied]).

@IJAERD-2026, All rights Reserved

One Limitation of this research is that the sample was drawn largely from a university population and relied on self reported behavior, which may not represent the wider public or capture actual online activity. The findings should therefore be interpreted as an indication of patterns in a digitally familiar population rather than as a generalizable measure of national behavior. Future research could extend the survey to more diverse participants, observe behavior directly rather than through self report, and evaluate whether targeted VPN and protective practice education produces measurable changes in what users do on public networks. Such work would help determine how best to convert the awareness users already possess into the protective habits they currently lack.

ACKNOWLEDGEMENT

The authors would like to thank all participants that completed the survey.

V. CONFLICT OF INTEREST

The authors declare no conflict of interests.

REFERENCES

[1] Maimon, D., Howell, C. J., Jacques, S., & Perkins, R. C. (2022). Situational awareness and public Wi-Fi users' self-protective behaviors. Security Journal, 35, 154–174. DOI: 10.1057/s41284-020-00270-2

[2] Potnuru, M. (2012). Limits of the Federal Wiretap Act's ability to protect against Wi-Fi sniffing. Michigan Law Review, 111(1), 1–30. DOI: Not available

[3] Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 1–11. DOI: 10.1109/PST.2018.8514208

[4] Sombatruang, N., Omiya, T., Miyamoto, D., Sasse, M. A., Kadobayashi, Y., & Baddeley, M. (2020). Attributes affecting user decision to adopt a virtual private network (VPN) app. In Information and Communications Security: 22nd International Conference, ICICS 2020 (pp. 223–242). Springer. DOI: 10.1007/978-3-030-61078-4_13

[5] Ramesh, R., Vyas, A., & Ensafi, R. (2022). "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. arXiv. DOI: Not available

[6] Nguu, J. M., & Musuva, P. M. W. (2024). Determining the efficacy of cybersecurity awareness programs on enhancing WiFi security behaviour. 2024 IST-Africa Conference (IST-Africa), 1–8. DOI: 10.23919/IST-Africa63983.2024.10569622

[7] Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions. Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (STAST '16), 61–72. DOI: 10.1145/3046055.3046058

[8] Swanson, C., Urner, R., & Lank, E. (2010). Naïve security in a Wi-Fi world. In Trust Management IV (pp. 32–47). Springer. DOI: 10.1007/978-3-642-13446-3_3

[9] Ali, S., Osman, T., Mannan, M., & Youssef, A. (2019). On privacy risks of public WiFi captive portals. arXiv. DOI: 10.1007/978-3-030-22479-0_6

[10] Noh, J., Kim, J., & Cho, S. (2018). Secure authentication and four-way handshake scheme for protected individual communication in public Wi-Fi networks. IEEE Access, 6, 16539–16548. DOI: 10.1109/ACCESS.2018.2809614

[11] Vondráček, M., Pluskal, J., & Ryšavý, O. (2018). Automated man-in-the-middle attack against Wi-Fi networks. Journal of Digital Forensics, Security and Law, 13(1), 59–80. DOI: 10.15394/jdfsl.2018.1516

@IJAERD-2026, All rights Reserved