Asia-Pacific Journal of Information Technology and Multimedia 12(1) 2023: 111 – 124
https://doi.org/10.17576/apjitm-2023-1201-06

Anatomy of Network Security Execution through Utilizing SPSS to Evaluate Public Wi-Fi

Anatomi Pelaksanaan Keselamatan Rangkaian melalui Penggunaan SPSS untuk Menilai Wi-Fi Awam

Amani Balqis binti Johal[1], Aws A. Abdulsahib[2]

[1]Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor
[2]The Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Putrajaya Campus, Jalan Kajang - Puchong, 43000 Kajang, Selangor

**Corresponding author: amanibalqis118@gmail.com*

Received 2 February 2023
Accepted 23 February 2023, Available online 1 June 2023

ABSTRACT

The increasing number of internet users has had a significant influence on the functions of Wi-Fi. Due to its extensive availability and free service, Wi-Fi has become an indispensable instrument for communication, especially among students. The continuous expansion of Wi-Fi provides an opportunity for malevolent attackers to undertake cyberattacks using public Wi-Fi as a route. Therefore, a full grasp of Wi-Fi dangers is required, which brought to this study that attempts to discuss the usage and awareness of public Wi-Fi among students. It is to study the human behaviour of students by doing the sampling of research, which involves distributing the survey questions to primary and secondary students at Alnoor International School to assess whether they are alert to the implications of using public Wi-Fi. To determine the findings of the study, chart forms are used. It showed that most students are aware of how dangerous public Wi-Fi can be, but they don't know enough about security to know how to protect themselves from potential dangers and threats from hackers.

Keywords: HTTPS protocol, Network Security, Public Wi-Fi, User awareness, VPN Usage.

ABSTRAK

Jumlah pengguna internet yang semakin meningkat telah memberikan pengaruh yang signifikan terhadap fungsi Wi-Fi. Oleh kerana ketersediaan yang meluas dan perkhidmatan percuma, Wi-Fi

telah menjadi alat yang tidak boleh dipisahkan untuk berkomunikasi, terutamanya dalam kalangan pelajar. Perluasan berterusan Wi-Fi memberikan peluang kepada penyerang yang berniat jahat untuk melancarkan serangan siber dengan menggunakan Wi-Fi awam sebagai laluan. Oleh itu, pemahaman sepenuhnya tentang bahaya Wi-Fi diperlukan, yang membawa kepada kajian ini yang cuba membincangkan penggunaan dan kesedaran tentang Wi-Fi awam dalam kalangan pelajar. Kajian ini bertujuan untuk mengkaji tingkah laku manusia pelajar dengan melakukan persampelan penyelidikan, yang melibatkan soal selidik kepada pelajar sekolah rendah dan menengah di Alnoor International School untuk menilai sama ada mereka peka terhadap implikasi menggunakan Wi-Fi awam. Untuk menentukan hasil kajian, bentuk carta digunakan. Ini menunjukkan bahawa kebanyakan pelajar sedar tentang betapa bahayanya Wi-Fi awam, tetapi mereka kurang pengetahuan tentang keselamatan untuk melindungi diri daripada bahaya dan potensi ancaman daripada penggodam.

Katakunci: Wi-Fi awam, protokol HTTPS, kesedaran pengguna, Keselamatan Rangkaian, Penggunaan VPN.

INTRODUCTION

According to the growing number of internet users, internet usage has increased. Therefore, needless to say, Wi-Fi has notably become essential for people to keep themselves connected to the internet. Therefore, individuals have a tendency to do whatever it takes to remain connected to the internet. Unfortunately, public Wi-Fi is vulnerable to cyber threats and cybercrime, and it jeopardies cyber security (Maimon et al. 2017).

Public Wi-Fi is remarkably accessible in the majority of public locations, for example, coffee shops, hotels, shopping malls, and airports. Furthermore, with the implementation of the work-from-home policy due to the ongoing global pandemic of the coronavirus disease that has hit worldwide, it has significantly impacted society's lifestyle, especially people’s working lifestyle. Workers, particularly those who do not have access to an internet connection at home, typically complete their work outside, primarily on their laptop by accessing public Wi-Fi, which is more convenient for them than mobile devices, which can easily connect to the internet via mobile data (Aborujilah et al. 2022).

Moreover, most people connect to public Wi-Fi regularly owing to its free service and availability since it is nearly everywhere. Typically, a user's personal information, such as name, email address, phone number, etc., must be entered prior to gaining access to a Wi-Fi network. Then only the user is able to access their desired website (Ali et al. 2019). Without taking precautions while connecting to the internet, such as using a virtual private network (VPN) and installing anti-virus software (Poojary 2021), it can consequently pose a security risk such as DNS spoofing, Wi-Fi password cracking, the man in the middle, and the evil twin (Susanto et al. 2021). Therefore, this research paper focuses on human behaviour by surveying their awareness and knowledge of the implications of connecting to public Wi-Fi.

LITERATURE REVIEW

Numerous publications have been published throughout the years concerning the risk of using public Wi-Fi. This chapter summarises several related works from the last four years, from 2019 to 2022. This chapter will provide the necessary background for this study. A summary of the literature review is presented in Table 1.

The study by Susanto et al. (2021) discusses the risk that using public Wi-Fi networks poses to user data. In this experiment, they used HTTPS and the HTTP protocol to conduct a man-in-the-middle (MITM) attack on the user's data, involving data modification. The results show that the platforms used to simulate public Wi-Fi networks have been subjected to MITM attacks such as SSL stripping, ARP poisoning, and session hijacking. Passwords and MAC addresses are among the information that ARP poisoning attacks collect from their targets. Without providing user authentication, the HTTP session hijacking technique generates a session id. On the HTTPS protocol, neither the SSL stripping attack nor the session hijacking attack were effective. However, there is a limitation in this study, which is that the method they are using is limited to one website application with deficient physical hardware, which does not reflect the deployment of actual public areas.

In the work that had been done by Hammad and Ati (2020), the focus was on public Wi-Fi security on mobile devices. To determine the threat, the researchers used honeypot procedures on Android devices. Moreover, HosTaGe has been verified to help detect the attack by performing the honeypot and displaying the infected Wi-Fi location, attack type, and attack percentage. The gathered attack information will be sent to the HosTaGe user so the user will be aware of the network not being used. However, the proposed method does not guarantee the network's security since the malicious attacker will continue to launch different attacks.

As for Al Neyadi et al. (2020), they discussed the execution of public Wi-Fi vulnerabilities that can be exploited by performing DNS spoofing, Wi-Fi password cracking, Man in the Middle, and Evil Twin to identify the vulnerabilities. The author focused on the implementation on Raspberry Pi and Kali Linux to test the security of public Wi-Fi by conducting DNS spoofing, Wi-Fi password cracking, Man in the Middle, and Evil Twin attacks. Nonetheless, there are some weaknesses regarding the study, namely that the solution presented should only be treated as a precaution to some extent and that it is best to refrain from making sensitive transactions or viewing sensitive data when using a public Wi-Fi network.

Ali et al. (2019) examined the personal information leaking through the use of a third-party captive portal. The studies' main approach is that data and traffic are gathered when a user accesses a captive portal, where the user must fill out information before an internet connection is provided. Specifically, through Chrome and Windows on a public hotspot. In addition to the research findings, they come from the analysis of data collection, privacy breaches, web trackers, HTTP cookies, fingerprinting, the performance of two anti-tracking extensions, and private browsing mode. Nevertheless, there is a limitation to the studies: the use of a VPN and visiting HTTPS, which is recommended, will still put you at risk in terms of privacy and security.

Furthermore, the studies presented by Karaymeh et al. (2019) provide research regarding security protection strategies when using public Wi-Fi. The way they carry out the study is by creating intermediate devices that can operate over a wireless connection that is connected to the user's device and to public Wi-Fi. From the research executed, there are three stages of vulnerability scans performed at the access point using Wireshark in this study. In the first stage, a scan is executed at the access point and user device. Next, for the second stage, the scan is carried out at the access point that is connected to their device solution. For the third stage, the scan at the access point will be done with the device solution as well as the VPN. In stages one and two, the wireshark is able to see the traffic sent and received outside the access point. On the other hand, nothing could be seen being transferred by Wireshark in the third stage. Despite the study being meant to be simple to use by non-technical people, the solutions presented still require some knowledge in order to operate them.

TABLE 1. Summary of the Literature Review

Author	Domain	Method/Approach they are using	Result	Limitation
Susanto et al. (2021)	The usage of public Wi-Fi network places carries the danger of user data threat.	Utilising HTTPS and HTTP protocol to conduct a Man in the middle (MITM) attack on user's data involving data modification.	The platforms used to simulate public Wi-Fi networks have been subjected to MITM attacks such as SSL Stripping, ARP Poisoning, and Session Hijacking. Passwords and MAC addresses are among the information that ARP poisoning attacks collect from their targets. Without providing user authentication, the HTTP Session Hijacking technique generates a session id. On the HTTPS protocol, neither the SSL Striping attack nor the Session Hijacking attack were effective.	The method they are using is only to one website application with deficient physical hardware which does not reflect the deployment of actual public areas.
Hammad and Ati (2020)	Public Wi-Fi security on mobile devices	Deploying the honeypot procedures on android devices to determine the threat.	HosTaGe has been verified to help detect the attack by performing the honeypot and displaying the infected Wi-Fi location, attack type and attack percentage, the gathered attack information will be sent to the HosTaGe user so the user will be aware of the network not used.	The proposed method does not guarantee the network's security since the malicious attacker will continue to launch with different attacks.
Al Neyadi	Public Wi-	Performing DNS	The author focused on the	The solution presented

et al. (2020)	Fi vulnerabilities that can be exploited.	Spoofing, Wi-Fi password Cracking, Man in the Middle and Evil Twin to identify the vulnerabilities.	implementation on raspberry bi and kali Linux to test the security of public Wi-Fi by conducting DNS Spoofing, Wi-Fi password Cracking, Man in the Middle and Evil Twin.	should only be treated as precaution to some extent best to refrain from making sensitive transactions or viewing sensitive data when using a public Wi-Fi network. .
Ali et al. (2019)	Personal information leaking through the usage of a third-party captive portal.	The data and traffic is gathered when a user is accessing a captive portal, in which the user would have to fill in information before an internet connection is provided. Specifically, through Chrome and Windows in a public hotspot.	The analysis on data collection, privacy breaches, web trackers, HTTP cookies, fingerprinting, the performance of two anti-tracking extensions, and private browsing mode are the findings of the study.	The use of VPN and visiting HTTPS that is recommended will still put you at risk in terms of privacy and security.
Karaymeh et al. (2019)	Security protection strategies when using Public Wi-Fi.	Creating intermediate devices that can operate in a wireless connection which is connected to the user's device and to public Wi-Fi.	There are three stages of vulnerability scans performed at the access point using Wireshark in this study. For the first stage, a scan that is executed in the access point and user device. Next, for the second stage the scan is carried out at the access point that is connected with their device solution. And for the third stage, the scan at the access point with the device solution as well as the VPN. In stage one and two, the Wireshark is able to see the traffic sent and received outside the access point. On the other hand, nothing could be seen being transferred by Wireshark in the third stage.	The proposed solution is meant to be simple to use by non-technical people. However, the solution presented still requires some knowledge in order to operate them.

RESEARCH METHODOLOGY

This section provides the research methodology for implementing this, which is on the security risk of public Wi-Fi. A measurement tool was used in this study by conducting a survey on 46 students, consisting of primary and secondary students at Alnoor International School. There are six stages performed in this research, which are planning, information gathering, scanning, analysis, progress, and lastly, reporting. The research process is shown in Figure 1.

FIGURE 1. Research process flowchart

The first stage is planning. Planning research is carried out by selecting a clear topic on which research will be conducted. Then, examine the other research journals or literature works with related research topics. This is to get the foundation of the research from the related work so that it can be used to construct research ideas. The problem statement, research objective, methodology, and research limitations are identified by reviewing related work on a similar topic. This is intended to outline the requirements for conducting an investigation.

Next, the second stage is information gathering. Descriptive research was selected as the qualitative approach in executing the study, which is also known as survey research, because it proved to provide an accurate depiction, such as opinion, belief, and knowledge, of the specific group or circumstance. The survey is distributed to the 26 primary students and 20 secondary students at Alnoor International School. The survey used is in the form of a Google Form questionnaire. So, the student has to answer the survey in the school's computer lab, where the question is already set up on the computer.

In the third stage, scanning is implemented using the information gathered from the survey questions that have been distributed. Scanning is the process of checking, or, in other words, cleaning, data before it can be transferred to the SPSS (Statistical Package for Social Science) tools to be analysed. This is specifically to increase the accuracy of the data once it is analysed. Any different data for the same value is equalized, especially in the question in which typing the input

is required. For instance, the school name and class name Also, for the question that needs only numeric answers, like age, need to change it to only be in the number form.

Furthermore, the fourth stage, which is analysis, is vital to obtaining the results of the research. The data collected is analysed using SPSS (Statistical Package for Social Science) to generate the graph based on the survey question administered. In other words, SPSS is used to assess the observed probability among students based on the data collected.
The fifth stage is the progress stage. The progress stage is where it is time to interpret the analysis acquired from the survey and use inferential statistics to draw conclusions from our data about more general situations and describe the occurrence of the data result.

The final stage is the report. The report provides in-depth analysis, explanation, and argumentation of the research conducted. It explains the whole study's findings, which will be divided into various sections, which are the summary, introduction, literature review, methodology, results based on analysis, and conclusion.

RESULT

This section will give the results of the survey administered to 46 primary and secondary students of Alnoor International School on June 22 and 23, 2022. The data are analyzed using SPSS. There were 14 female and 12 male respondents at the primary level, and 5 female and 15 female respondents at the secondary level. The purpose of this survey is to assess students' awareness and understanding of public Wi-Fi security. Two distinct analyses will be conducted on the data. One segment for primary students and another for secondary students. Table 2 shows the summary of respondent details.

TABLE 2: The respondent details

Grade						Gender			
Secondary			Primary			Secondary		Primary	
S1	S2	S3	P6	P5	P2	Male	Female	Male	Female
45% (9)	25% (5)	30% (6)	46.2% (12)	19.2% (5)	34.6% (9)	75% (15)	25%(5)	46.2% (12)	53.8%(14)

According to Table 3, 34.62% of primary students have never used public Wi-Fi, whereas 10% of secondary students have never used public Wi-Fi. This is expected due to secondary students having more internet access because they usually have their own mobile phones or devices. Thus, continuous internet access is needed to use the mobile device. Unlike primary students, who are mostly still kids, they are still fully under their parents' supervision. As a result, some parents are less likely to encourage their child to use a mobile device, and in some cases, children borrow their parents' phones. As a result, the use of public Wi-Fi is unaffected.

TABLE 3: The frequency of student using public Wi-Fi

Oftenness	Primary Student (%)	Secondary Student (%)
Every day	11.54	5.00
Frequent	11.54	15.00
Never	34.61	10.00
Rarely	42.31	70.00

Primary

According to the result of the question "Have you ever heard of security risks regarding public Wi-Fi?" as shown in Figure 2, it indicates that 46.15% of the students, which is the largest percentage, are not sure of the security risk that might happen to them when they are accessing public Wi-Fi, while 30.77% of the respondents have never heard of public Wi-Fi security. The next lowest percentage, 23.08 percent, of the respondents have heard of the public Wi-Fi security risk.

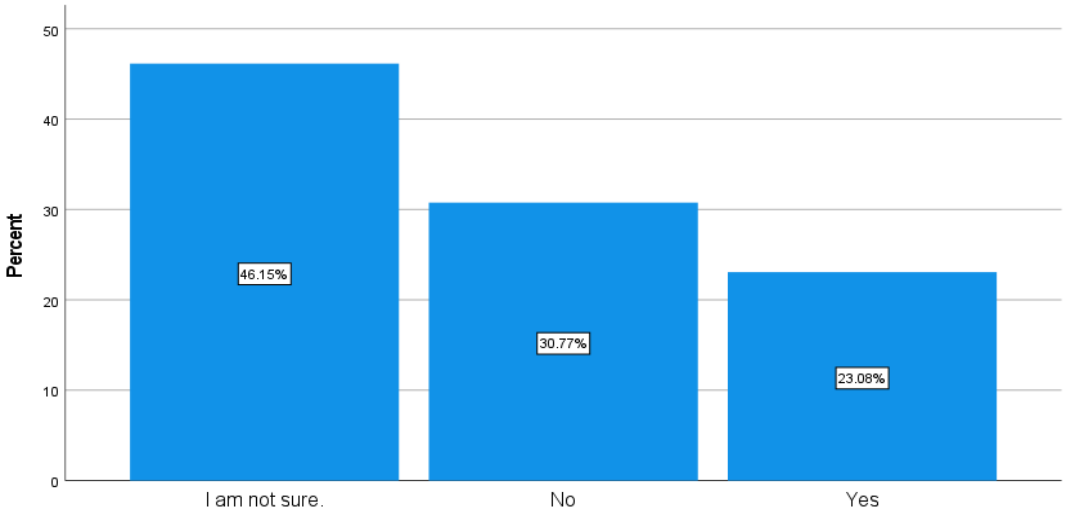

FIGURE 2. Student's knowledge about public Wi-Fi security risk

Figure 3 shows the graph in relation to the students' concerns about public Wi-Fi among primary students. From the graph shown, it can be observed that more than 76% of the primary students have shown little concern for public Wi-Fi security. This is alarming due to the biggest percentage of the graph being contributed by the "a little/kind of" percentage. Furthermore, 17.6% of primary students responded, "very concerned," which is the second-highest percentage, while 5.88% of students lack concern about public Wi-Fi security.

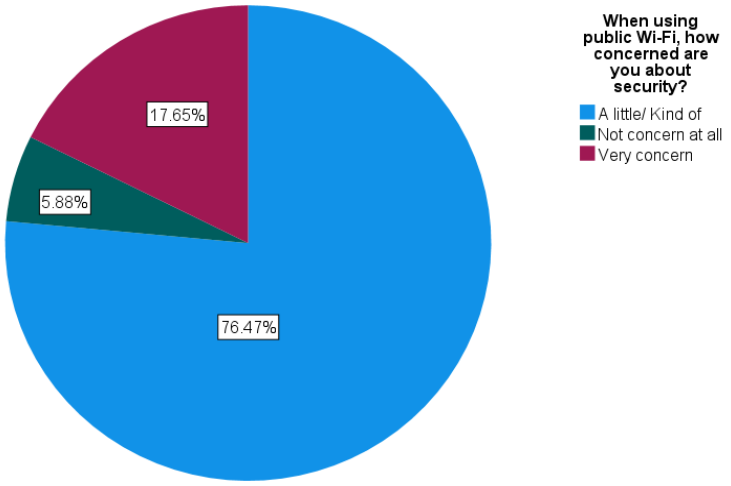

FIGURE 3. Student's concern about public Wi-Fi security.

Figure 4 presents the student awareness regarding the dangers of public Wi-Fi. The graph depicts that 42.31% of respondents among primary students are aware of the dangers of public Wi-Fi. However, 38.46% of students are not sure if the public Wi-Fi is unsafe, and the remaining 19.23% are not aware of the risk of public Wi-Fi that can possibly cause grave harm to them if they do not handle it properly.

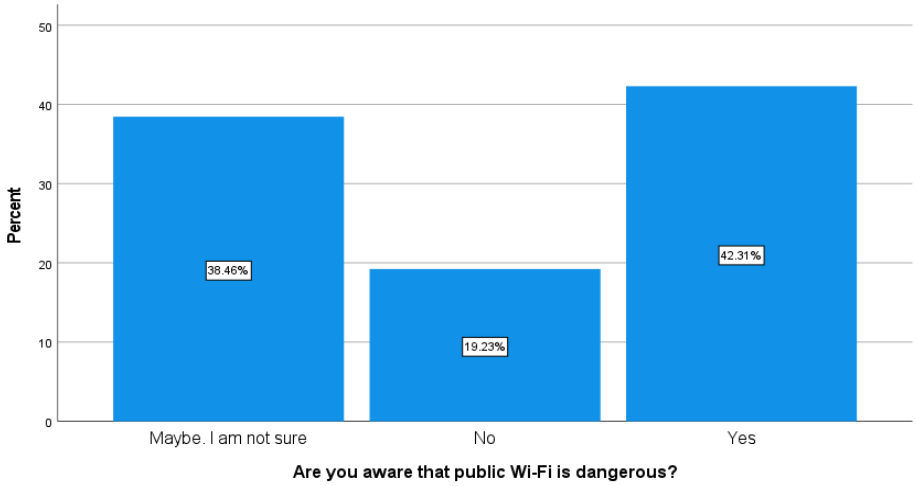

FIGURE 4. The awareness of the public Wi-Fi danger among primary students

Figure 5 is the graph regarding the students' opinion of using public Wi-Fi if they know the negative impact of it. It is clear that a large majority (46.15%) of the students choose "Maybe" as their answer because they do not know whether they're going to use the public Wi-Fi if they know the negative impact that might occur to them. Next, 42.31% of the students will use the public Wi-Fi once they recognize the negative impact. The next percentage is 11.54% of students who decide to still use the public Wi-Fi even though they acknowledge the risk.

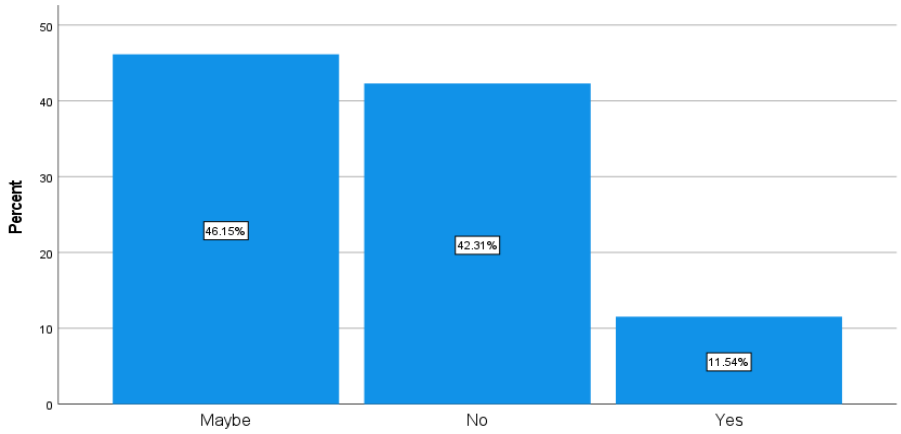

FIGURE 5. Primary student opinion of public Wi-Fi usage on the knowledge about negative impact of using public Wi-Fi.

Secondary

Figure 6 shows whether or not the student uses the same email address and password for all of their online platform accounts. The graph proves that 80% of students use a different email address and password for their account, and the other 20% use the same email address and password combinations for all of their accounts. This question is intended to determine whether the student is aware that a malicious attacker can gain unauthorized access to any of their accounts if they use the same email address and password for all of their accounts across all of their online platforms.

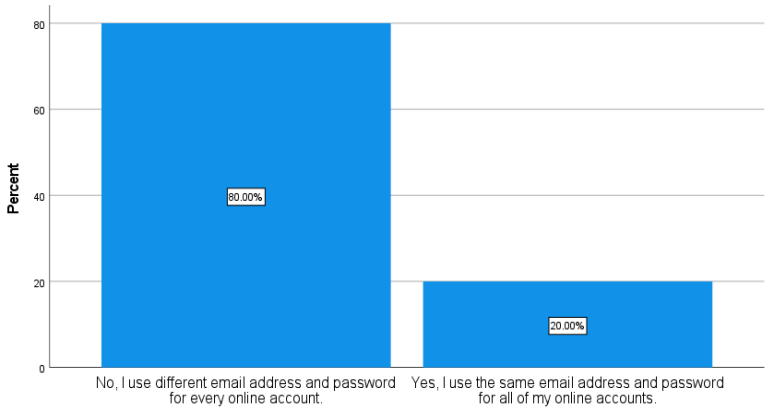

FIGURE 6. Secondary student usage of the same email address and password for online accounts

Figure 7 shows how much the student knows about the padlock and HTTPS symbols in an address bar. This question is to determine if the student is concerned enough to acknowledge the importance of HTTPS and padlock symbols in the address bar. Although this is not directly about public Wi-Fi, they are very crucial, especially in terms of privacy, due to the fact that they signify whether the webpage they are going to is safe or not. Therefore, the result shows 65% of the students check every time they browse any website. 25% of the students are not sure if they check them or not, while the other 10% do not check the existence of the HTTPS and padlock symbols in the address bar.

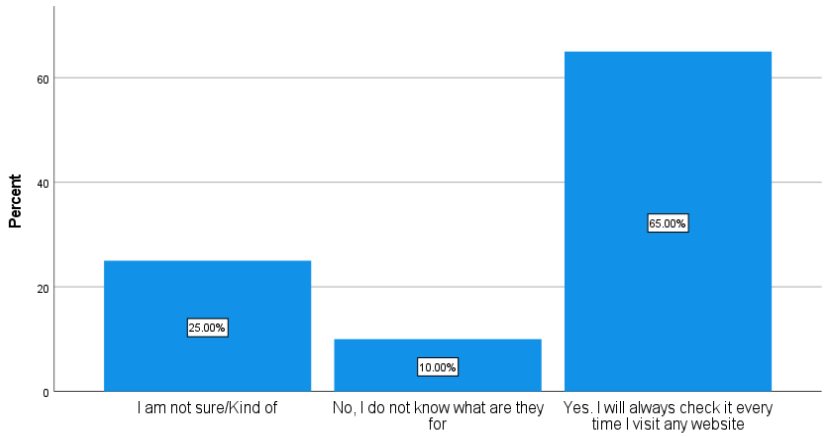

FIGURE 7. Secondary student's knowledge about the HTTPS and padlock symbol in an address bar

Figure 8 is a graph about how worried high school students are about using public Wi-Fi. More than 55% of the secondary students are a little concerned about the public Wi-Fi security risk. Furthermore, 22.2% of secondary students answered "very concerned" tied with the students who are not concerned at all when connecting over public Wi-Fi.

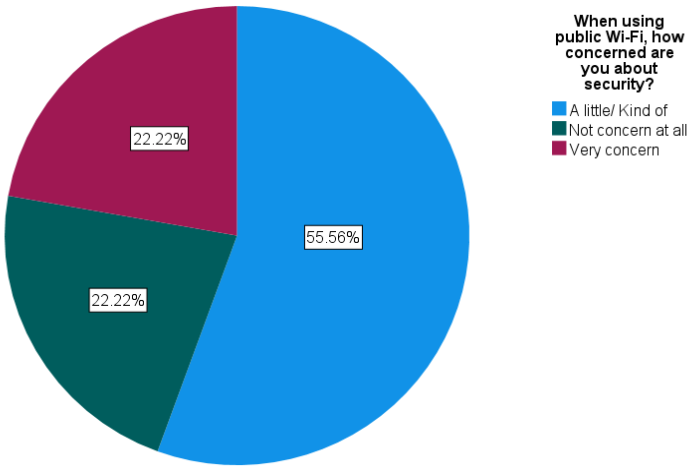

FIGURE 8. The concern of utilization public Wi-Fi among secondary students

Figure 9 presents the result of the question in regards to the awareness of the public Wi-Fi security risk among secondary students. As can be seen from Figure 9, the majority of the students (85%) are aware of the public Wi-Fi risk, while the remaining percentage of the students (15%) responded that they did not know of any public Wi-Fi security risk. This is a good sign, as the result indicates the student acknowledges that public Wi-Fi has its own risks when accessing it.

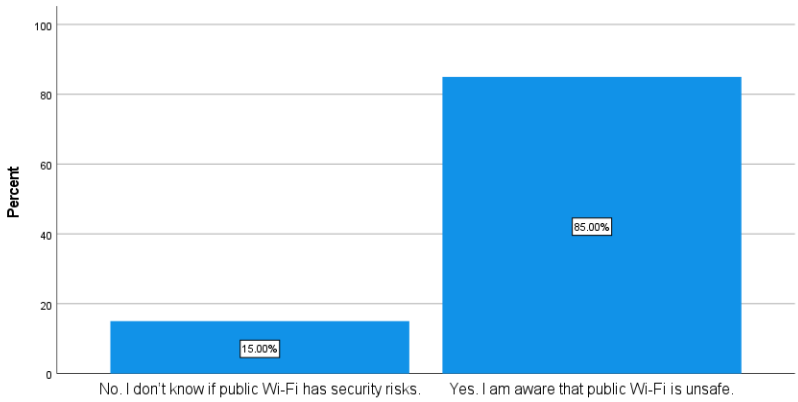

FIGURE 9. The Awareness of Public Wi-Fi Connection among Secondary Students

Figure 10 depicts secondary students' attitudes towards public Wi-Fi usage if they are aware of the negative consequences of using public Wi-Fi. 45% of the students choose "Maybe" as they possibly do not know the negative impact mentioned exactly. So, they cannot really decide if they will use it in the future, even after acknowledging the dangers of public Wi-Fi. Next, 35% of the students decided not to use the public Wi-Fi if they knew the negative impact that would happen to them. However, 20% of the students respond that they will most likely use public Wi-Fi. It seems that this student is not concerned about the negative impact that could harm them, probably because they think the data they handle is not that sensitive to be concerned about.

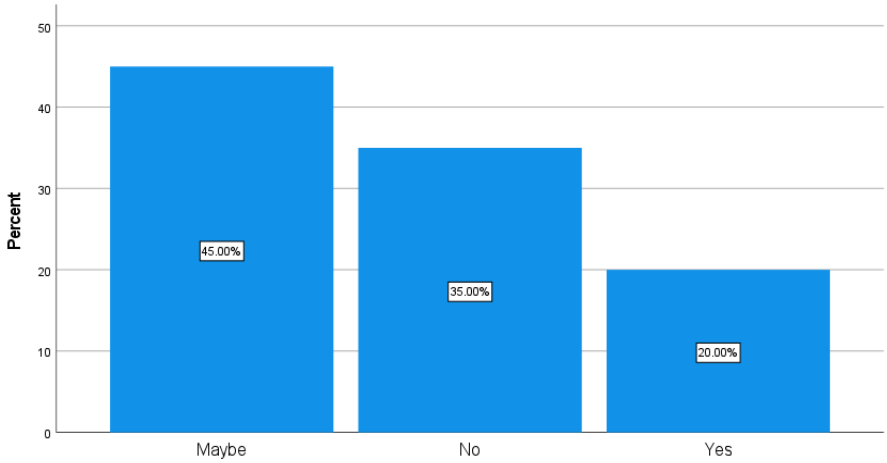

FIGURE 10. Secondary student opinion of public Wi-Fi usage on the knowledge about the negative impact of using public Wi-Fi.

DISCUSSION

In Figure 4, the result illustrates the graph of student awareness regarding the dangers of public Wi-Fi. It can be seen that the majority of students are not sure of the exact danger of public Wi-Fi. The second-largest percentage of students are aware of the risk that could happen to them when accessing public Wi-Fi. However, in the graph of Figure 2, it can be observed that most of the students are not sure if they have heard of a security risk coming from public Wi-Fi, and the second

biggest percentage of the students have never heard of the public Wi-Fi risk. It can be proven that although the students are aware of how dangerous public Wi-Fi is, they still lack the necessary security knowledge of potential threats and attacks.

As can be seen in Figures 6 and 7 for secondary students, most of them use different email addresses and passwords for their online accounts, and most of them check the HTTPS and padlock symbols in the address bar. This suggests that secondary students already take precautions against the possible risks that could happen and care about the security of their online accounts.

To observe the students' concern about the public Wi-Fi's security from both groups of students, which are primary and secondary, according to the graph in Figure 3 and Figure 8, the result shows the majority of the students have a concern about the public Wi-Fi's security. This can be explained by the fact that the student knew of the danger, but they did not know how likely or how threatening it could be when the hacker could potentially exploit their privacy or security.
Furthermore, from the graphs in Figure 4 and Figure 9, it can be deduced that all students, primary and secondary, are very well aware of the potential threat of public Wi-Fi and the fact that it is unsafe. The graph in Figure 5 for primary students and Figure 10 for secondary students, on the other hand, shows the expected contrast between primary and secondary students in Figures 4 and 9. Most of the students answered "maybe" despite their awareness of attacks and threats that could potentially harm them. The lack of security awareness could be due to inadequate public education on Wi-Fi security.

CONCLUSION

The rising use of public Wi-Fi has prompted worries about the security of devices and the user's privacy, which may be compromised if the user is unaware of the repercussions of using public Wi-Fi. According to the results of the study, most students know that there are risks to using public Wi-Fi. However, they lack awareness of the public Wi-Fi consequences, which leads them to choose to use public Wi-Fi since they do not know the likelihood of encountering a public Wi-Fi danger. Hence, public education on Wi-Fi security is needed to provide the necessary Wi-Fi security knowledge so that people can utilise it without any worries and safely. From this study, it can be deduced that student awareness is in a critical state.

In future research, the sampling of the research, which is a distributed survey, should have been larger than the number of students in the current study to increase the accuracy of the results obtained. Furthermore, future studies ought to use more complex graphs, such as histograms, so that the curve of the graph can be seen and, from there, a forecast can be made. Moreover, this study is focused on student behaviour regarding public Wi-Fi risk. It is encouraged to do more study in this area that is more in-depth and oriented towards more specific subjects pertaining to public Wi-Fi.

REFERENCES

Aborujilah, A., Al-Othmani, A. Z., Hussien, N. S., Mokhtar, S. A., Long, Z. A., & Nizam, M. (2022, March). Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study. *In 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE)* (pp. 440-450). IEEE.

Ali, Suzan & Osman, Tousif & Mannan, Mohammad & Youssef, Amr. 2019. On Privacy Risks of Public Wi-Fi Captive Portals.

Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Mohammad, Q. H., & Alrabaee, S. 2020. Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux. *In 2020 12th Annual Undergraduate Research Conference on Applied Computing* (URC) (pp. 1-4). IEEE.

Angaswamy, Selvaraja & P, Asha & Jayakumara, Dr. 2014. Use Of Wi-Fi Connection by The Research Scholars of University of Mysore, Karnataka: A Study. *International Journal of Academic Library and Information Science.* 2. 150-157. 10.14662/IJALIS2014.041.

Chigada, J., & Madzinga, R. 2021. Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, 23(1), 1-11.

Hammad, L. A., & Ati, M. 2020. Assessing Security Health of Public Wi-Fi Environments in the UAE. *In 2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1-6). IEEE.

Haque, Md & Raj, Nidhi & Singh, N. 2020. Wi-Fi Adoption and Security Survey. 10.9790/1676-1204016774.

Karaymeh, A., Ababneh, M., Qasaimeh, M., & Al-Fayoumi, M. 2019. Enhancing data protection provided by VPN connections over open Wi-Fi networks. *In 2019 2nd International Conference on New Trends in Computing Sciences* (ICTCS).

Maimon, D., Becker, M., Patil, S., & Katz, J. 2017. {Self-Protective} Behaviors Over Public {Wi-Fi} Networks. In The LASER Workshop: Learning from Authoritative Security Experiment Results (*LASER 2017*) (pp. 69-76).

Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y., & Ruan, N. 2019. Revealing your mobile password via Wi-Fi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*, 19(2), 432-449.

Poojary, P. S. Safety Measures to be Maintained while Using Public Wi-Fi. Journal homepage: www.ijrpr.com ISSN, 2582, 7421.

Susanto, A., & Raharja, W. K. 2021. Simulation and Analysis of Network Security Performance Using Attack Vector Method for Public Wi-Fi Communication. *The IJICS (International Journal of Informatics and Computer Science)*, 5(1), 7-15.

Sciences (ICETAS) (pp. 1-6). IEEE.

Yu, L., Luo, B., Ma, J., Zhou, Z., & Liu, Q. 2020. You Are What You Broadcast: Identification of Mobile and {IoT} Devices from (Public){Wi-Fi}. *In 29th USENIX Security Symposium (USENIX Security 20)* pp. 55-72.

Zhang, J., Tang, Z., Li, M., Fang, D., Chen, X., & Wang, Z. 2019. Find me a safe zone: A countermeasure for channel state information-based attacks. *Computers & Security*, 80, 273-290.