Assignment Report January 17, 2021

Final Survey Report

Attitude Towards Public Wi-Fi Threat

Yuyao Duan
Fredric Eriksson

Table of Contents

1 Introduction

Wi-Fi networks have become more and more common in various public places which could bring the customers a convenient experience. Companies and business organizations value this add-value service since it could increase customer loyalty, repeat business, and create an outstanding brand image. The previous research has clearly depicted the growing trend of public "Wi-Fi hotspots" from 22.7 million in 2014 to 289.3 million in 2018 [1]. This, however, on the other hand, may lead to a series of potential threats behind this popular trend [1].

As we know that there are many kinds of Wi-Fi hotspots in public places which some of them do not require any password to access i.e. using no encryption while others may need either social network accounts or online registrations to log in [1]. Users should be extremely cautious since even a simple packet sniffer is capable of picking up login information when the user's device is accessing sensitive websites in the hotspot environment [1]. Moreover, evolving Wi-Fi hacking toolkits lead to the barriers to intercept data on public hotspots becoming very low even in the encrypted hotspots environment [1].

Based on the above understanding, we are interested in investigating people's attitudes towards using public Wi-Fi hotspots in their everyday life. The main purpose of this investigation is to find out if people really know the potential security threats when using public hotspots. We want to explore the reasons behind the choices and the relationship regarding demographic patterns and decisions.

1.1 Survey background

This survey aims to investigate people's security consciousness when using public Wi-Fi. The survey is conducted by the following logic:

First of all, this survey will collect information in terms of the respondents' age and educational background; after this, a series of self-assessment questions related to IT/computer science, smart devices, internet, and public Wi-Fi will be conducted in order to test the relations between respondents' background and self-awareness; moreover, attitude questions related to using public Wi-Fi and security awareness of public Wi-Fi will be asked. In the end, a question list related to various well-known cyber-attacks is given to recheck the respondents' knowledge about cybersecurity.

1.2 Survey aims

The aim of this study is to investigate the potential correlation between people's security awareness and attitudes of using public Wi-Fi and the personal background in terms of age and educational background.

1.3 Survey method

The survey was conducted by using Google Forms as the main tool to collect respondents' answers. Social networks including Slack, Discard, Facebook, WhatsApp,

Reddit are used for getting responses from people with various backgrounds, which will help achieve reliability for this research. An overview of the survey's questions can be found in the "Applied survey questionnaire" section.

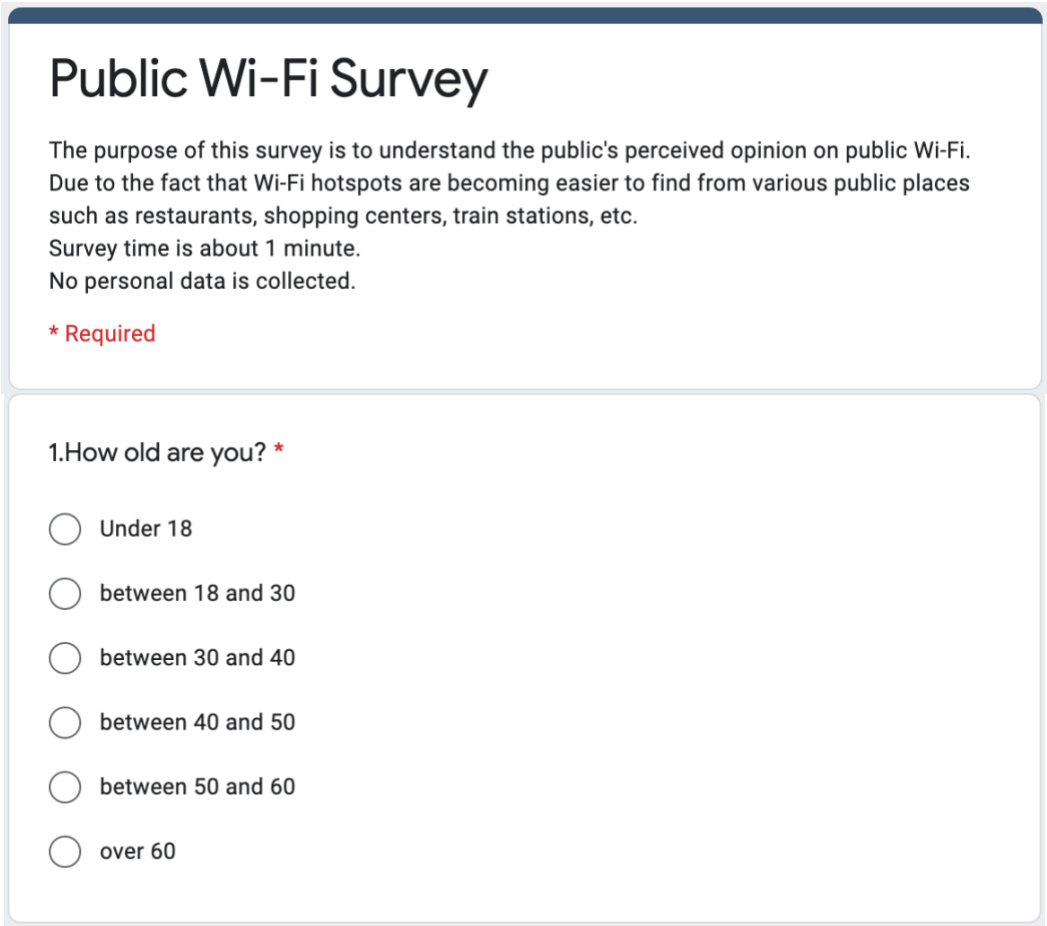
2 Hypothesis

The expected outcome of this research is that older adults may tend to overlook the security threats of public Wi-Fi, and therefore, they are more likely to use it. By comparison, younger people have better security awareness regarding public Wi-Fi hotspots and they tend to refrain from using it in everyday life.

In addition, individuals with higher educational background may also have better knowledge to protect themselves, thus, they also tend to stay away from using public hotspot services.

3 Applied survey questionnaire

This survey contains ten questions: the first two questions closely related to the personal background – age and educational background. Question 3 to 6 are used to test the respondents' personal knowledge in terms of general knowledge about IT/computer science, smart devices, the internet, and Wi-Fi. Question 7 to 9 are used to find the respondents' attitudes towards public Wi-Fi, using public Wi-Fi, and if individuals implement strategies to overcome public Wi-Fi threats. Question 10 is an extra question to identify the respondent's personal knowledge regarding cybersecurity aiming to recheck the correspondence between the previous selections and personal knowledge.



Public Wi-Fi Survey

The purpose of this survey is to understand the public's perceived opinion on public Wi-Fi. Due to the fact that Wi-Fi hotspots are becoming easier to find from various public places such as restaurants, shopping centers, train stations, etc.
Survey time is about 1 minute.
No personal data is collected.

* Required

1.How old are you? *

- Under 18
- between 18 and 30
- between 30 and 40
- between 40 and 50
- between 50 and 60
- over 60

2.What is your educational background? *

- ◯ Primary school
- ◯ middle school (or the same)
- ◯ high-school (or the same)
- ◯ undergraduate (bachelor degree)
- ◯ graduate (master degree)
- ◯ PhD/Doctor
- ◯ Other: _____

3.How familiar are you with computer science / IT field? *

	1	2	3	4	5	6	7	8	9	10	
Not much	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Very much

4.How familiar are you with smart electronics (laptops, smartphones, etc.)? *

	1	2	3	4	5	6	7	8	9	10	
Not much	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Very much

5.How familiar are you with the internet and Wi-Fi? *

	1	2	3	4	5	6	7	8	9	10	
Almost never use them	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Use them daily

6.Do you know what a public Wi-Fi is? *

- ◯ Yes
- ◯ No

7.How dangerous do you think using a public Wi-Fi is? *

	1	2	3	4	5	6	7	8	9	10	
Very safe	○	○	○	○	○	○	○	○	○	○	Very dangerous

8.When you go to the public places that provide free Wi-Fi services, to what extent do you tend to use them? *

	1	2	3	4	5	6	7	8	9	10	
Never	○	○	○	○	○	○	○	○	○	○	Always

9.Do you use a VPN (Virtual Private Network) or other encryption tools to protect your internet connections when you use public Wi-Fi? *

- ○ Yes
- ○ No
- ○ Sometimes

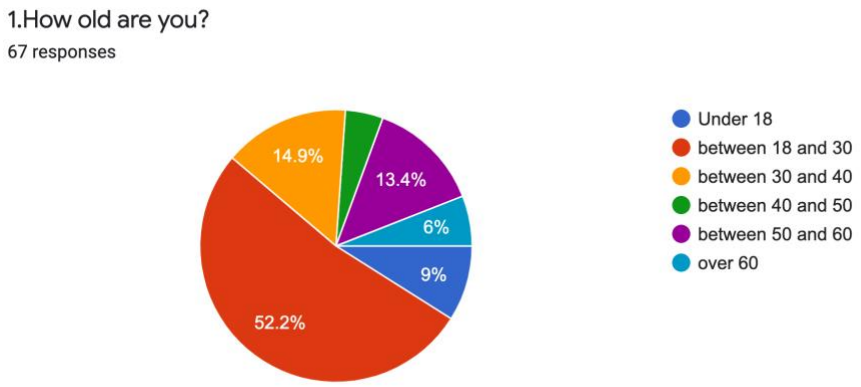
10.Have you ever heard about the following cyber-attacks?

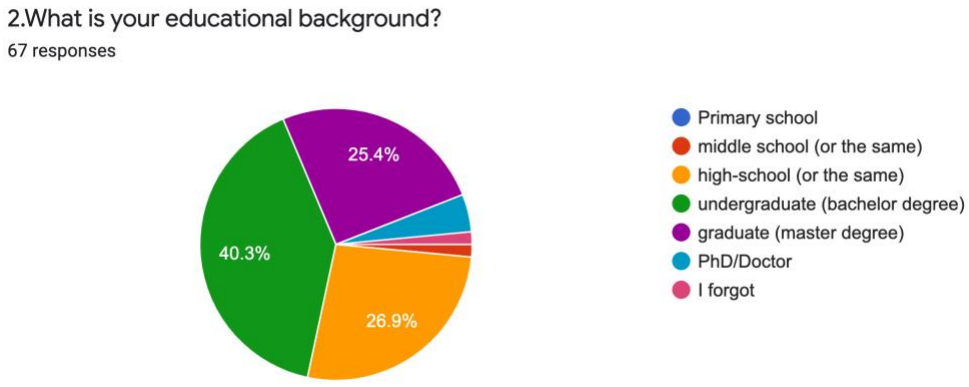
- ☐ Man-In-The-Middle Attack
- ☐ Evil Twin / Rogue Wi-Fi Networks
- ☐ AirCrack-NG
- ☐ Malware Injections
- ☐ Passive Sniffing / Packet Analyzers
- ☐ Ad Hocs
- ☐ Worms
- ☐ Cowpathy

4 Result

In total, there are 67 responses collected in this survey. The response summary of each question is presented as follows in order to give an overview of the participants' backgrounds and attitudes towards the public-Wi-Fi-related questions.

4.1 Respondents' background

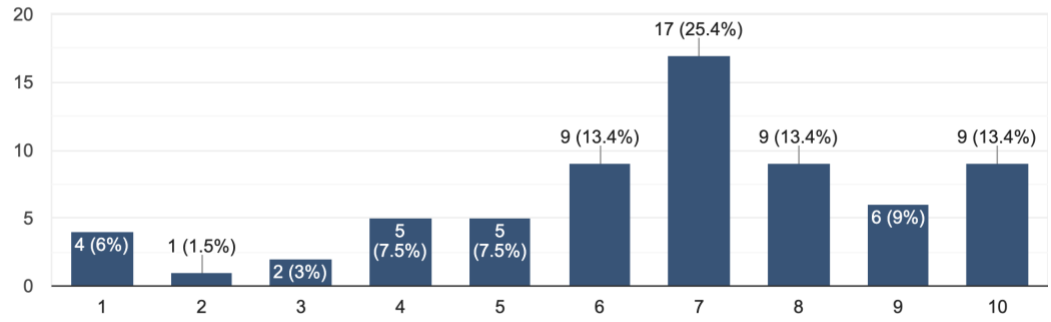




4.2 Respondents' personal knowledge

3.How familiar are you with computer science / IT field?

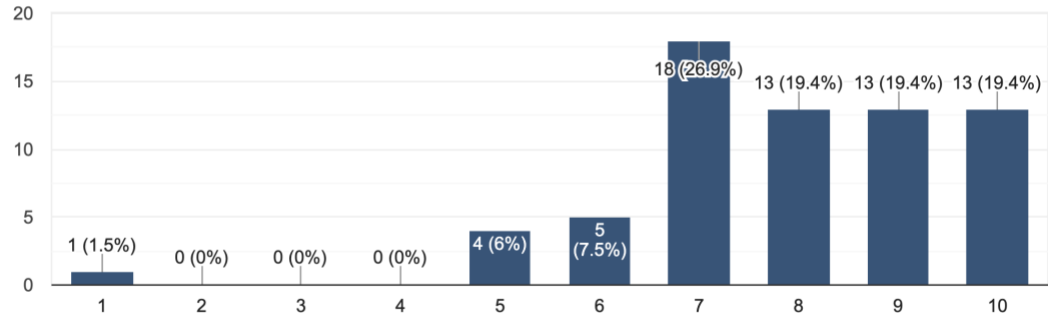
67 responses



Not Much Very Much

4.How familiar are you with smart electronics (laptops, smartphones, etc.)?

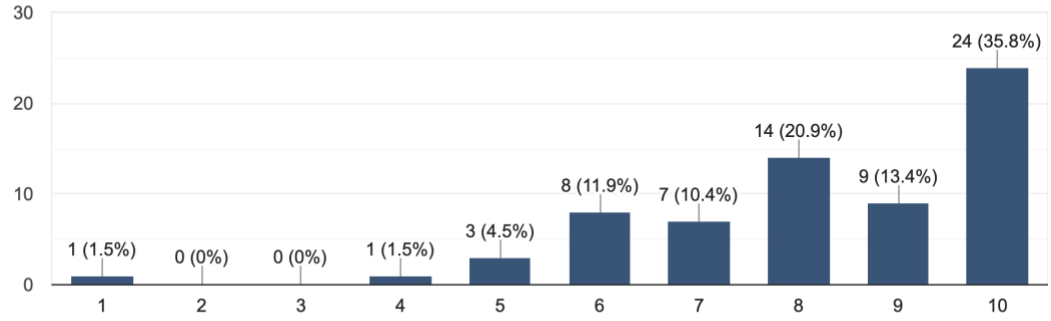
67 responses



Not Much Very Much

5.How familiar are you with the internet and Wi-Fi?

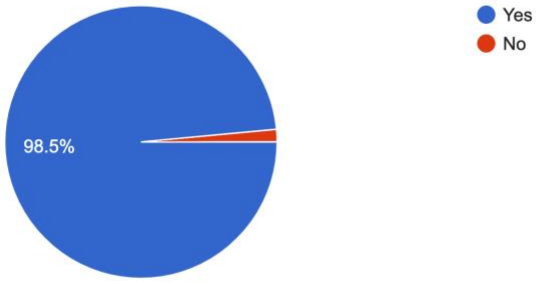
67 responses



Almost never use them Use them daily

6.Do you know what a public Wi-Fi is?

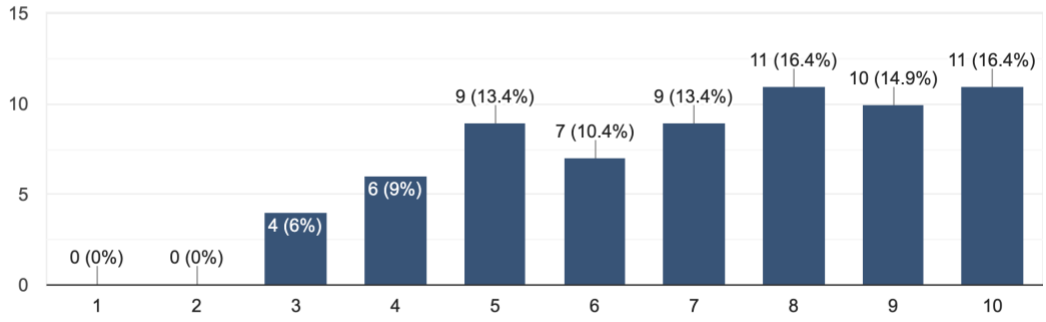
67 responses



4.3 Respondents' attitudes towards public Wi-Fi

7.How dangerous do you think using a public Wi-Fi is?

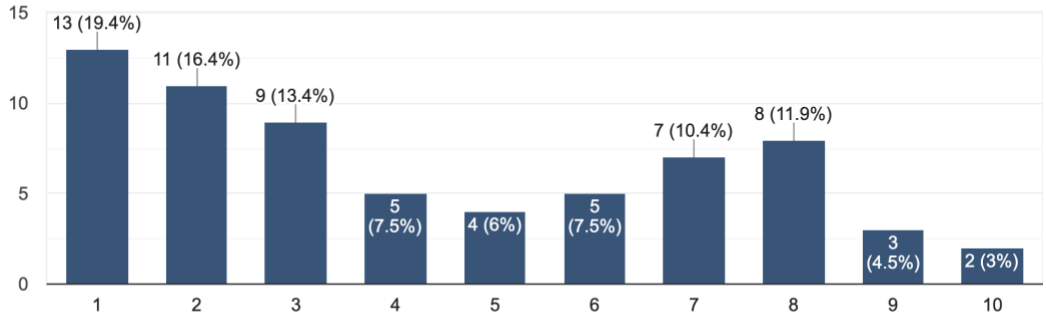
67 responses



Very safe Very dangerous

8.When you go to the public places that provide free Wi-Fi services, to what extent do you tend to use them?

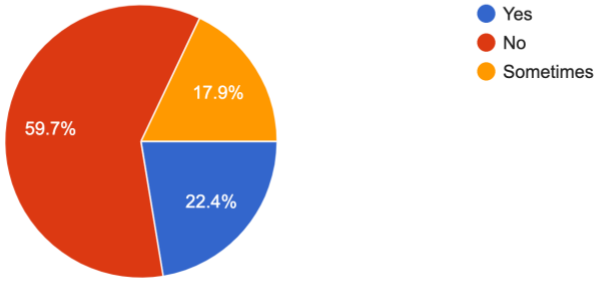
67 responses



Never Always

9.Do you use a VPN (Virtual Private Network) or other encryption tools to protect your internet connections when you use public Wi-Fi?

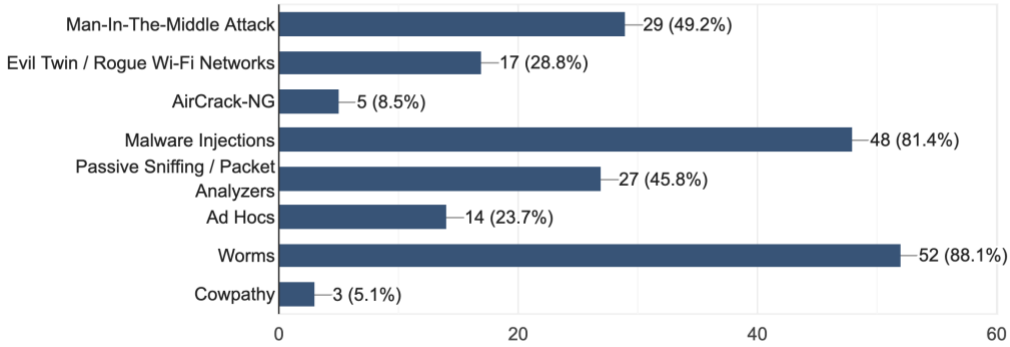
67 responses



4.4 Respondents' knowledge regarding cyber-attacks

10.Have you ever heard about the following cyber-attacks?

59 responses



5 Analysis

This section contains two main parts: the overall analysis is based on the summary data from the four different aspects viz respondents background analysis, respondents' self-assessment analysis, respondents' attitudes towards using public Wi-Fi, and respondents' knowledge about cyber-attacks; the hypothesis analysis aims to investigate if the statistical results can deduce the hypothesis of this research.

5.1 Overall analysis

Based on the above statistical diagrams, the following section will present the analysis from the summary information in order to provide an overview about the survey results of the respondents.

5.1.1 Respondents background analysis

In this survey, we define that participants who are from the first and second group – "Under 18" and "between 18 and 30" are considered as young people while respondents who are older than 30 are classified as the relatively older adults' group. From the pie chart of Question 1, we can see that young people consist of 52.2% (35) and 9% (6) respectively in total. By contrast, older adults account for 38.8% (28) of this survey. The reason behind this phenomenon can relate to the data collection approaches since the majority of the responses are collected from the online community "Reddit" that the main active population is young people. We tried to overcome this limitation by using personal contacts via Facebook and WhatsApp for more elderly people which eventually contributed to 28 respondents that was only 13 less than the young group.

Regarding the educational background, the three main participant groups are "undergraduate" (27), "high school" (18), and "graduate" (17) which represent 40.3%, 26.9%, and 25.4% respectively. Furthermore, there are three Ph.D./Doctor participants and one middle school student in this survey who make up 4.5% and 1.5% individually. Only one participant claimed "I forgot (my educational background)" in this study.

5.1.2 Respondents' self-assessment analysis

From Question 3 to 6, we can identify the main trend of these questions: 74.6% of respondents rate their familiarity with computer science/IT greater or equal to 6 points out of 10; 85.1% of respondents grade their familiarity with smart electronics greater or equal to 7 points; 92.4% of respondents estimate their familiarity with the internet and Wi-Fi greater or equal to 6 points; 66 out of 67 (98.5%) participants know what is public Wi-Fi. In general, we can find that people are familiar with IT, smart electronics, the internet, and public Wi-Fi regardless of age groups.

5.1.3 Respondents' attitudes towards using public Wi-Fi

From Question 7 to 9, we can find the main trend of respondents' attitudes regarding using public Wi-Fi: 71.5% of respondents believe that public Wi-Fi is not safe and grade the points tending to dangerous (points greater or equal to 6); 58.2% of participants

consider they will try to avoid using public hotspots services (points lower or equal to 5). Though most respondents have the security awareness of public Wi-Fi, 59.7% of respondents do not use the virtual private network (VPN) or any other encryption tool while they connect to public Wi-Fi. By comparison, only 22.4% of respondents always use encrypted communication methods connecting to public hotspots.

5.1.4 Respondents' knowledge about cyber-attack

According to the statistics, 59 participants out of 67 know at least one type of cyber-attack in the list which informs that most people nowadays have knowledge about cyber-threats.

5.2 Hypothesis analysis

In order to infer the hypothesis, all the responses will be analyzed in detail and presented in this section. To do this, each question will be examined based on the statistical results. The starting point of analyzing the hypothesis is the age and educational background of the respondents.

5.2.1 Age analysis

Table 1 Statistics results of Question 3 – 8

	Question 3	Question 4	Question 5	Question 6	Question 7	Question 8
Young group average score	7.00	8.73	8.54	41 out of 41 say "Yes"	7.34	4.29
Older adult group average score	6.12	7.12	7.69	25 out of 26 say "Yes"	6.65	7.69

** The data is extracted from the proof material "Attitude towards Wi-Fi threats statistical table"*

As we can see from Table 1, the young people rate higher scores than the older adults in terms of familiarity with IT, smart devices, and the internet and Wi-Fi which proves that young people have better knowledge in these aspects. With respect to Question 6, all young participants know what is public Wi-Fi while there is one candidate of the older adult group who claims "don't know about public Wi-Fi". Furthermore, the average scores of dangerous awareness towards public Wi-Fi hotspots which is assessed by the young group (7.34) is obviously higher than the older group (6.65) that echo the older adults tend to overlook the security threats of the hypothesis. Following the results of Question7, the differences in the attitudes towards using public Wi-Fi between the different age groups is further proved by Question 8 which young people consider that

they are less likely to use public Wi-Fi (4.29) compared to the result of the older adults (7.69) which eventually verifies the hypothesis regarding age differences.

Table 2 Statistics results of Question 9 – 10

	Question 9	Question 10
Young group	23 out of 41 **never** use encryption tools (56.10%)	6 out of 41 **do not** know at least one cyber-attack method (14.63%)
Older adult group	17 out of 26 **never** use encryption tools (65.38%)	2 out of 26 **do not** know at least one cyber-attack method (7.69%)

**The data is extracted from the proof material "Attitude towards Wi-Fi threats statistical table"*

From Table 2 we can find that the young group has a lower percentage (56.10%) of "never use encryption tools" compared to the older group (65.38%) which sheds light on that young people have higher security awareness to encrypt their communication when they use public Wi-Fi awareness than the older adults. Interestingly, the survey's results point out that the older respondents have better knowledge about cyber-attack (7.69% do not know at least one cyber-attack method) than the younger group (14.63%). The possible reason for this phenomenon is because older people have better life experiences than younger people with the knowledge about cyber-attacks which can be learned from news, media, and other approaches.

5.2.2 Educational background analysis

Table 3 Statistics result of Question 3 – 8

	Question 3	Question 4	Question 5	Question 6	Question 7	Question 8
Under bachelor degree average scores	5.95	7.60	8.15	19 out of 20 say "Yes"	6.50	5.15
Bachelor degree average scores	6.74	8.00	8.37	17 out of 17 say "Yes"	7.74	3.48
Above bachelor degree	7.25	8.00	8.05	18 out of 18 say "Yes"	6.75	4.75

average scores						

**The data is extracted from the proof material "Attitude towards Wi-Fi threats statistical table"*

In this educational background analysis, all education levels are classified as the above three dimensions – "under bachelor degree" (Primary school, middle school (or the same), high-school (or the same)), "bachelor degree" (undergraduate), and "above bachelor degree" (graduate (master degree), Ph.D./Doctor). As we can see from Table 3, the differences between "under bachelor degree" and "bachelor degree" are apparent which verifies the hypothesis. From Question 3 to Question 8, the performance of participants with bachelor degrees shows that they have better knowledge in IT (Question 3), smart devices (Question 4), the internet (Question 5), and security awareness (Question 7 and 8) when using public Wi-Fi than the candidates who have a lower educational background. However, the statistical results show that the difference between "bachelor degree" and "above bachelor degree" is insignificant, which some of the performance of the respondents of "above bachelor degree" is even less than undergraduate candidates (Question 5, 7, and 8). Participants from "above bachelor degree" only show that they have better knowledge in IT/computer science (7.25) than the bachelor degree holders (6.74). In terms of security awareness of public Wi-Fi, the people who are graduates or Ph.D./Doctors show that they are less likely to believe the threats of public Wi-Fi and more likely to use public Wi-Fi than the undergraduate respondents.

Table 4 Statistics results of Question 9 – 10

	Question 9	Question 10
Under bachelor degree	10 out of 20 **never** use encryption tools (50.00%)	2 out of 20 **do not** know at least one cyber-attack method (10.00%)
Bachelor degree	18 out of 27 **never** use encryption tools (66.67%)	3 out of 27 **do not** know at least one cyber-attack method (11.11%)
Above bachelor degree	12 out of 20 **never** use encryption tools (60.00%)	3 out of 20 **do not** know at least one cyber-attack method (15.00%)

**The data is extracted from proof material "Attitude towards Wi-Fi threats statistical table"*

From Question 9 to 10, we can see the statistical results showing that respondents with lower educational backgrounds are more likely to use encryption tools and have more knowledge about cyber-attacks which are kind of in conflict with results of Question 3 – 8. The possible reason behind this situation may relate to the number of samples, in which the contradictions could be solved if more meticulous data is collected.

6 Discussion and conclusion

In this section, the research results will be discussed in order to provide a deeper understanding regarding individuals with different personal backgrounds reacting to the threats of public Wi-Fi. The conclusion of this research will be followed and the limitations of this research will be reviewed.

6.1 Discussion

The hypothesis regarding people's attitudes towards using public Wi-Fi hotspots has been explored in this survey. Ten survey questions embedded with the potential logic are given in order to deduce the hypothesis. A total of 67 responses based on the intention of gathering data at different ages and educational backgrounds are collected in this research. Moreover, all the answers of the questionnaire are carefully analyzed from both the overview and in detail.

Overall, this research provides a clearer overview of people's attitudes towards using public Wi-Fi services. No matter the respondents from which background, the statistical results show that the majority of people are familiar with computer science, smart devices, the internet, and public Wi-Fi. Though 71.5% of participants believe that public Wi-Fi hotspots are not safe and 58.2% respondents consider they will try to avoid using public Wi-Fi services while the majority of participants (59.7%) do not use any encrypted communication tool when they go out using public hotspots even 88.06% (59 out of 67) responses show that people have knowledge about cyber-attacks approaches. This can be explained by individuals nowadays having more access to information, however, people lack a deep understanding of the related knowledge eventually leading to the absence of effective actions.

6.2 Conclusion

Analyzing from the age dimension validates the initial hypothesis that young people have better knowledge about IT/computer science, smart devices, the internet, and Wi-Fi hotspots. Furthermore, the performance of the young group shows that young people have a higher security awareness and are more likely to use encryption tools to protect their wireless communication when they use public Wi-Fi services. By contrast, the statistical results show that the performance of the older adults is inferior to the young participants in all aspects. With respect to the educational backgrounds, the collected data partially proved the hypothesis that the participants with bachelor degrees show better performances in all perspectives than the respondents from the "under bachelor degree" group. Statistics show that the interviewees who are educated above undergraduate do not perform better than undergraduates. According to the data, the actual boundary of distinction remains between people who are educated under bachelor degree and those who have received undergraduate education. No significant differences between the undergraduates and the participants who are educated higher than bachelor study have been found in this research.

Although this research intends to provide a comprehensive view of people's

attitudes towards using public Wi-Fi hotspots, the actual practice shows that there still remain a few limitations in this survey. Better data collection approaches should be considered in order to gather more refined data in terms of ages and educational background. Moreover, this study ignores the potential cultural influence since one survey participant from Reddit pointed out that a Wi-Fi user may hold totally different attitudes towards using public Wi-Fi services when he or she stays in different countries. However, due to COVID-19 epidemic, applying online surveys makes it more difficult to control cultural factors compared to the traditional methods. Furthermore, the time limitation is another important factor which restricts the availability of larger amounts of data. As we can find from Table 4, the conflict results can be compromised when more responses can be obtained from the survey.

Bibliography

[1] WatchGuard Technologies, “Navigating the Challenges with Wireless Security”, [2016-01]