Degree project

Why do people use public Wi-Fi? An investigation of risk-taking behaviour and factors lead to decisions

Bachelor Degree Project in Informatics

First Cycle 30 credits

Spring term 2023

Mohamad Abdulkader

Supervisor: Dennis Modig

Examiner: Ali Padyab

Acknowledgements

The Wireless Networks course has been a source of inspiration for my thesis, significantly influencing the trajectory and focus of my research. I am sincerely grateful to my supervisor, Dennis Modig, for providing invaluable guidance and constructive feedback throughout the process. I also like to express my deepest appreciation to Ali Padyab, my examiner, for his unwavering support and invaluable insights. His expertise and guidance have played an instrumental role in refining the academic rigour of my research. Furthermore, I extend my heartfelt gratitude to my family for their unwavering support and understanding throughout my academic journey.

ABSTRACT

The usage of public Wi-Fi and hotspots has witnessed a substantial increase in recent times, providing convenient connectivity in various public areas. Public wireless networks are now widely accessible, especially in smart cities. However, utilising public Wi-Fi exposes individuals to potential threats to their privacy and security. Hackers can exploit vulnerabilities present in public Wi-Fi networks, such as the "Evil Twin" attack, to deceive users and unlawfully obtain their personal information. The main objective of the research was to investigate people's awareness of the security risks associated with public Wi-Fi usage and to identify the factors that contribute to their willingness to take such risks. The research adopted a qualitative approach, utilising semi-structured interviews with 14 participants to gain valuable insights into their understanding and knowledge of the risks connected with public Wi-Fi. The majority of respondents employed public Wi-Fi for educational purposes, browsing the Internet, and engaging with social media platforms. Additionally, the findings of the study explored the motivations and influences that lead individuals to take risks when using public Wi-Fi. Factors such as convenience, cost-effectiveness, saving mobile data usage, limited mobile network coverage, and a lack of awareness concerning privacy and security risks emerged as the most significant reasons and influences behind the utilisation of public Wi-Fi.

Keywords: public Wi-Fi, hotspots, wireless networks, privacy, security, awareness, attitude, knowledge, risks, factor.

Table of Contents

1 Introduction

The popularity of Wi-Fi and public hotspots has risen in recent years. Nowadays, public Wi-Fi is available in most places, such as public squares, shopping centres, transportation and cafes, especially in smart cities. Many of these networks are open and accessible, and some require authentication. Many companies believe that providing public wireless networks is helpful, and these networks provide individuals with a convenient way to communicate (Sombatruang et al., 2016). Despite public wireless networks providing easy connectivity, security risks can be encountered in such an environment (Sombatruang et al., 2016). The use of public Wi-Fi exposes users to potential privacy and security threats. In addition, the transmission of wireless signals extends beyond the boundaries of the building housing the access points (AP), making it possible for hackers to capture these signals from nearby areas (Maimon et al., 2022). One of these risks is the "Evil Twin" attack, which can hijack the connection between the node and the Wi-Fi hotspot. The risk can be done by installing a rogue device that deceives the user by naming the network with the same identifier as the original network. This attack can steal the private data of the user when the user is associated with this network (Choi et al., 2022). Usually, on social media websites and apps, the user is asked for personal data such as name, age, and other personal data. Such information can be transmitted via these services without encryption. Although the login process for most of the major web-based email services is encrypted, the contents of email messages are not. This leaves users vulnerable to privacy and security threats as any person along the way from the user to the access point can intercept this information (Klasnja et al., 2009).

People are advised to limit the type of web-based information they access on public Wi-Fi to confidential information. For example, the Federal Trade Commission (FTC) encourages individuals to be vigilant and take specific measures to protect their information (Maimon et al., 2022). They recommend using encrypted Wi-Fi networks, entering personal information only on secure networks, using Virtual Private Network (VPN) connections, and sending emails with confidential information should be avoided (Maimon et al., 2022).

Many people continue to use potentially unsafe public Wi-Fi despite mounting evidence of these risk concerns. Mobile data access becomes quicker and less expensive. Understanding the rationale behind such choices is essential to develop effective risk-reduction tactics. Various factors have been the subject of prior studies, with varying results (Sombatruang et al., 2019). Users are unaware of the risks associated with accessing unprotected public Wi-Fi (Klasnja et al., 2009). However, Sombatruang et al. (2019) found that some users were aware of the risks but still exhibited optimism bias, believing they were less likely to experience negative outcomes than others. The perceived risks did not significantly affect users' choices. Instead, their desire to conserve mobile data was the primary motivator for using unsecured Wi-Fi, despite the associated risks (Sombatruang et al., 2019). A study conducted in Japan indicates that many applications still transmit personal information in an unencrypted manner, and still, many individuals use public Wi-Fi for sensitive transactions (Sombatruang et al., 2018). Based on a previous study, many individuals were aware of the dangers of using public Wi-Fi and prioritised personal comfort over privacy (Choi et al., 2022). It becomes puzzling when a person realises the risks and continues to behave indifferently, and this behaviour can have potentially harmful consequences (Choi et al., 2022).

The current topic is chosen to conduct the study, which is necessary to explore the reasons that drive users to use public Wi-Fi in Sweden and consider the behaviours of users and the factors that cause them to use public wireless networks. Sweden is a developed country, and infrastructures are developed, including its public Wi-Fi network. This widespread availability of public Wi-Fi has made it easy for people to stay connected and work remotely. In addition, this thesis will focus on the potential risk associated with public hotspots and existing security breaches in such networks that lead to the targeting of privacy and sensitive information. Understanding the reasons and influences that

drive people to use public wireless networks is essential to reduce those risks and finding ways and methodologies to mitigate those risks (Sombatruang et al., 2018).

The study structure is as follows: In section two, introduce the background, and in section three, introduce the problem definition. Section four is dedicated to presenting the methodology, and section five outlines the results of the study. Section six presents the discussion, and finally, the conclusion is presented in section seven.

2 Background

This section presents to the reader the important background information to give an overview of the study context and to let the reader recognise and understand the problem of the study.

2.1 What is Wi-Fi?

Public Wi-Fi is a type of wireless Internet that can be accessed in public places such as airports, libraries, cafes, or parks. It is usually provided by businesses or organisations for free or at a cost, allowing the public to connect to the Internet (al Neyadi et al., 2020). Wi-Fi is a technology that allows a person to access the Internet via a mobile device without a physical connection. The Institute of Electrical and Electronics Engineers (IEEE) defines the Wi-Fi standard as part of the 802 networking specifications (al Neyadi et al., 2020). To create a Wi-Fi network, a user needs hardware components like wireless access points or routers and user devices like smartphones, tablets, laptops, etc., that are equipped with Wi-Fi adapters. The wireless router is connected through a physical connection, such as fibre, and then sends and receives data through radio waves to and from connected devices (al Neyadi et al., 2020). Over the years, the growth in Internet traffic has led to an increase in bandwidth and speed for end-users. From 1995 to 2016, Internet users increased from 16 million to over 3 billion (al Neyadi et al., 2020).

2.2 Security and privacy risk of unsecured public hotspots

Prior research that looked at the security of public Wi-Fi covered it from a technical and behavioural perspective. According to Sombatruang et al. (2016), data security and privacy can be at risk on public Wi-Fi networks. Data transfer via the air exposes networks vulnerable to many dangers (Ahadi et al., 2020), where public Wi-Fi usually lacks encryption, leaving information vulnerable and susceptible to being captured by hackers (Watts, 2016). According to Choi et al. (2022), Wi-Fi security measures, especially encryption, authentication, and confidentiality, are insufficient to stop harmful attacks. Many public Wi-Fi networks lack appropriate security protections, and outdated encryption algorithms are still used in some areas. As a result, users accessing Internet-based services through public Wi-Fi networks face potential threats and risks to their privacy and security (Choi et al., 2022). Sombatruang et al. (2018) point out that they obtained different types of credentials information in their research. Initially, the researchers discovered an unencrypted password in one of the emails they intercepted, which allowed them to access an encrypted file. In addition, an authentication token was being transmitted via HTTP basic authentication for one of the servers. Cheng et al. (2013) conducted a study that reviewed 20 airport datasets from four countries and found that privacy breaches can reach up to 68%. Thus, travellers accessing the Internet at airports unknowingly expose their private information. This is a cause for concern as users have limited means to determine the security of their communications and identify who can access them (Klasnja et al., 2009). According to Fang et al. (2020), bus hotspots collect detailed usage records, which can be shared with third parties such as advertisers or researchers. However, the open nature of the bus environment and the possibility of device theft or vandalism raise the potential for privacy breaches. Attackers could use leaked information to uniquely re-identify users in bus Wi-Fi systems and potentially exploit their personal information (Fang et al., 2020).

According to Klasnja et al. (2009), the primary and most common apprehension, and in some cases, was the possibility of exposing sensitive personal data such as financial information or personally identifiable data during connecting to public Wi-Fi. Credit card information, bank account data, and social security numbers are the key components of this dataset. The city of London police alerted the public that criminals can target credit card information by establishing fake Wi-Fi networks (Evil Twin) or carrying out Man-in-the-Middle (MITM) attacks on public Wi-Fi (Sombatruang et al., 2016). This

section will explain the most critical attacks and risks using public hotspots. Section 2.2.1 presents phishing and Evil Twin, and section 2.2.2 introduces a man-in-the-middle.

2.2.1 Phishing and Evil Twin

Phishing refers to attempting to steal personal or confidential information through electronic means, usually by disguising the fraudulent communication to look like it is coming from a reputable source (Kindberg et al., 2008). This is often achieved by making the phishing email or message appear similar to legitimate communications from trusted online companies, such as banks or financial services, in terms of branding and appearance (Kindberg et al., 2008). Conducting a Wi-Fi phishing attack is simple for an attacker who has a laptop and can carry it around discreetly. The attacker can deceive a user into connecting to a false hotspot and then, like a phishing website, collect data from the user and provide fake responses that contain malware (Kindberg et al., 2008).

An Evil Twin exploit is a well-known attack that has been around for 20 years. The attacker deceives the user into connecting to a false AP while the person is unaware of it and instead connects to the hacker's AP by seeming to be a legitimate access point (Ahadi et al., 2020). According to Hossain et al. (2019), the impact of an Evil Twin attack can be classified into three distinct categories. Firstly, in category A, the attacker can eavesdrop on and manipulate network traffic. Secondly, category B involves the theft of social credentials. Finally, in category C, the attacker can identify individual users. It is important to note that successful Evil Twin attacks not only facilitate credential theft and unauthorized account access but can also lead to denial of service (DoS) incidents by blocking users' Internet access (Hossain et al., 2019). Sometimes, an Evil Twin attack is used to gather client information, which is a form of phishing (Ahadi et al., 2020). As soon as the customer connects to this fraudulent AP, the confidential information of the user can be deleted or changed. Similar to when a client tries to connect to a certain network, the user sends a query request to the desired network in the Wi-Fi network connection list, which is displayed in the client network preference list of the wireless network connection window (Ahadi et al., 2020). The hacker interrupts this probe transmission and sets up an Evil Twin attack. The hacker can then steal the client's personal data, including credit card numbers and passwords (Ahadi et al., 2020). According to Li et al. (2016), the attacker intercepts the Wi-Fi traffic to identify vulnerable areas and selectively examines the channel state information (CSI) to deduce keystroke details and hack the password of the victim. This approach offers two advantages to the hacker: they gain control over the cloned network, granting them unrestricted access to shared information while also avoiding legal consequences associated with breaching an established network (Watts, 2016).

Setting up free hotspots requires minimal effort and can be easily replicated (Watts, 2016). One common technique used by hackers involves cloning networks (Watts, 2016; Li et al., 2016). According to Chen et al. (2021), an attacker can set up a phishing AP near a hotel or café. They will configure a laptop with analysis software to build a wireless AP with the same name, channel, and encryption as a legitimate AP. Then, they will wait for a legitimate user to connect to the phishing AP. Once the user connects to the phishing AP, the attacker can intercept the user's sensitive information, such as their account and password, by launching a man-in-the-middle attack. The attacker can also use an active attack by sending a false connection cancellation request frame to the attack target, causing the target device to break the connection with the real AP and connect to the phishing AP instead (Chen et al., 2021). The user would have no idea that such an attack is taking place. Phishing is the most commonly performed attack on Wi-Fi networks, and it is believed to result in a loss of about $3.2 billion each year (Sudar et al., 2017).

2.2.2 Man-in-the-middle (MITM)

A man-in-the-middle attack is a frequently employed method in various networks (Noh et al., 2018). A MITM attack happens when an attacker intercepts communication between two parties and can modify or change the exchange (Al Neyadi et al., 2020; Trewin et al., 2016). At the same time, the victims believe they communicate directly with each other (al Neyadi et al., 2020). Conducting a MITM attack is easier on a wireless network compared to a wired one (Kindberg et al., 2008). The MITM attack requires the prior implementation of ARP spoofing. This involves the attacker deliberately sending messages using manipulated address information, causing the intended recipients to direct

their messages to the attacker. As a result, the attacker positions themselves between the AP and the target station, enabling them to intercept and monitor all traffic transmitted between the two (Noh et al., 2018). The attacker can intercept all unencrypted data sent to or from the user and even grab encrypted data using Transport Layer Security (TLS) or Secure Socket Layer (SSL) if the user does not verify certificates. Determining the origin and verifying the authenticity of a wireless service is not easy to check. Therefore, users still need to have a certain level of trust regarding the authenticity of a specific Wi-Fi service (Kindberg et al., 2008).

2.3 Previous Research

This section will delve into the literature regarding the usage intent of public Wi-Fi, the reasons and factors for using public Wi-Fi, users' awareness of the associated risks when utilising public Wi-Fi, and the security and privacy risks involved. Each topic will be addressed individually.

2.3.1 Usage intent of public Wi-Fi

Studies have shown that people use public Wi-Fi for a variety of online activities. A study conducted in Australia by Lambert et al. (2014) found that people utilised public Wi-Fi for communicating with friends and family through emails and social media, as well as for leisure activities such as browsing the Internet to pass the time. Students also use public Wi-Fi to complete educational activities such as school assignments (Lambert et al., 2014). A study done in Seattle and Boston by Hampton and Gupta (2008) found that individuals use public Wi-Fi for sending browsing the Internet, emails and instant messaging with friends. According to Hossain et al. (2019) found in their research, the majority of users who connected to fake access points primarily engage with social networking sites such as Facebook, Gmail, Instagram, and WhatsApp, while none of them visits online transaction-related websites like Amazon or Bikroy.com. Breitinger et al. (2020) reported that 35.8% of users limit their usage to browsing without sharing sensitive information, such as banking applications. However, the information was gathered through self-reported methods such as surveys and interviews rather than observation (Sombatruang et al., 2016).

The study conducted in the UK by Sombatruang et al. (2016) found that participants engaged in various activities while using the experimental Wi-Fi. The most widely used platforms were Google, Facebook, Apple iTunes, WhatsApp, Snapchat, and Instagram, accounting for almost 50% of the total usage. Additionally, the researchers noticed traffic to websites outside the UK. The increasing number of people in the UK who have data plans and do not have to rely on public Wi-Fi for Internet access may lead to a decrease in the usage of public Wi-Fi. However, the continued increase in the number of public Wi-Fi offerings suggests that there is still demand for these services, despite the availability of alternative options (Sombatruang et al., 2016).

2.3.2 Reasons and factors for using public Wi-Fi

Many users utilise public Wi-Fi because it provides convenience (Sombatruang et al., 2016). Public Wi-Fi has become the most convenient and economically feasible means of facilitating access to the Internet and corporate networks (Sudar et al., 2017). A widely recognised risk bias is overconfidence (Sombatruang et al., 2018). In contrast, Swanson et al. (2010) found that people often do not believe these dangers will come to fruition despite being aware of potential hazards. Users of public Wi-Fi are confident that their devices' security measures will keep them safe (Klasnja et al., 2009). People use public Wi-Fi because it is free (Sombatruang et al., 2016). In contrast, Sombatruang et al. (2018) reported that, particularly among people with tiny monthly data allowances, the desire to save mobile data limit was connected to risk-taking behaviour and the use of unprotected public Wi-Fi. Sombatruang et al. (2019) reported that recent research has shown that users' desire to save mobile data encouraged them to utilise unprotected Wi-Fi rather than perceived risks having an impact on their decision-making about using public Wi-Fi. Additionally, the preservation of mobile battery, age, education, and income level influence users' decisions to utilise unsecured Wi-Fi networks (Sombatruang et al., 2019). It is common for individuals to use public Wi-Fi networks instead of 3G/4G

cellular networks as Wi-Fi is usually quicker and less costly (Cheng et al., 2013).

2.3.3 Users' awareness of the risks associated with utilising public Wi-Fi

Previous literature has explored users' awareness of the risks of utilising public Wi-Fi. In their study, Breitinger et al. (2020) surveyed participants and discovered that a majority of them lacked the necessary knowledge about security precautions when connecting to public Wi-Fi networks. Despite ongoing endeavours to enhance the awareness of potential risks and necessary security measures among users of public Wi-Fi, a considerable number of individuals keep risking their security by transmitting sensitive information in public wireless networks (Maimon et al., 2022). Klasnja et al. (2009) found that participants had a lack of awareness about the associated risks and rarely considered privacy and security concerns while using Wi-Fi. Fang et al. (2020) stated that open public Wi-Fi in buses has led to an increasing worry regarding potential privacy breaches for users. Despite expressing concerns in general, participants felt secure and fearless when using Wi-Fi due to their routine practices and beliefs, coupled with a limited understanding of the actual risks involved (Klasnja et al., 2009). Lotfy et al. (2021) mentioned in their paper that people lack an adequate understanding of the risks associated with using public Wi-Fi and mistakenly believe they are safe. Previous studies have demonstrated that many people are unaware of the potential dangers of using public Wi-Fi (Consolvo et al., 2010). In a study conducted by Klasnja et al. (2009) in the United States, it was discovered that users in a technologically advanced region lacked awareness of the potential hazards associated with Wi-Fi usage. Despite residing in an advanced technological environment, there was a lack of consciousness regarding the visibility of transmitted data through Wi-Fi to others. However, the protective measures they had implemented gave them a false sense of security. Upon receiving comprehensive information about the associated risks, the users are willing to adapt their behaviours in order to reduce the potential threat. Breitinger et al. (2020) reported a lack of people's awareness regarding security measures, where only 7.2% employed additional security measures like VPN software while using public Wi-Fi. Notably, users with a stronger background in cybersecurity are more inclined to utilize VPNs or entirely avoid public Wi-Fi networks.

2.3.4 Security and privacy risks of utilising public Wi-Fi

Previous studies have covered the security and privacy risks associated with using public hotspots. Sombatruang et al. (2016) identified significant security and privacy risks. They found that certain applications and websites, such as Instagram, Channel 4, and Bumble, leaked cookies that could compromise data privacy. These leaked cookies contained sensitive information such as video links, TV shows viewed, photos accessed, and even private information from online dating profiles. The researchers could access this information without requiring user authentication, indicating a potential security breach. Cheng et al. (2013) reported discovering leaked sensitive personal information of users while using public Wi-Fi networks in airports. Sombatruang et al. (2018) analysed Wi-Fi packets and found sensitive data transmitted without encryption on public Wi-Fi networks. Their finding included unencrypted images from an online dating app, search history, clear-text emails and documents, and various forms of unencrypted credentials.

Klasnja et al. (2009) conducted a study on Wi-Fi users' privacy concerns. The primary concern identified was the potential theft of financial or sensitive personally identifiable information, such as credit card numbers and social security numbers. Participants expressed fear of identity theft and financial damage. Cheng et al. (2013) investigated the privacy and security risks of public Wi-Fi networks during travel. They discovered that users' personal information, such as device names, gender, age, and location, can be used to profile individuals. Additionally, user identification is possible by matching this information with social network platforms. The researchers provided an example of identifying a user by analysing Domain Name System (DNS) queries, MAC addresses, and device names to infer the user's country of origin, find the user's name, and narrow down potential candidates on social websites. In their research, Lotfy et al. (2021) analysed data obtained from users who utilised a public Wi-Fi network for their experiment. The study reveals instances of privacy breaches, with certain users having their personal information, such as email addresses, phone numbers, user IDs, and device names matching their names, exposed to potential risks. Fang et al. (2020) findings

demonstrate a significant privacy risk associated with public Wi-Fi in the bus, wherein as little as two randomly selected records of a user's connection history and location can lead to the unique re-identification of approximately 98.1% of the users by potential attackers.

3 Problem Definition

In this chapter, an overview of the broader problem domain is presented. The first subsection provides a rationale for why this particular area is the focus of the thesis. The study's primary aim and purpose are explained in the second subchapter. The third subsection outlines any constraints that may be relevant to the project.

The public Wi-Fi demand arises when many people use public wireless access points networks via mobile devices such as smartphones or other devices because of the increased social media apps or e-learning. Many tasks can be solved by using the Internet. Public hotspots are available in most public areas, and now it is much easier to stay online in many places such as airports, transport stations, coffee shops and other public places. However, many public Wi-Fi is unsecured (Sombatruang et al., 2016), meaning the data are not encrypted. Sometimes, the network uses low security, such as Wired Equivalent Privacy (WEP). According to Sebbar et al. (2016), roughly one-quarter of public Wi-Fi in London and Dubai continue to utilise an outdated encryption algorithm called WEP, which can be easily cracked (Choi et al., 2022). As a result, people who utilise public Wi-Fi networks to connect to Internet-based services like email, social media platforms, and online shopping face potential risks (Klasnja et al., 2009). Connecting to unsecured hotspots presents a valuable opportunity for hackers to gain unrestricted access to unsecured devices on the network (Sombatruang et al., 2019). Furthermore, connecting puts users at risk of security and privacy breaches as many people use public Wi-Fi for different purposes, including bank transmission and sensitive information, whether users are aware of it or not (Choi et al., 2022).

To summarise the research problem, public networks undoubtedly provide Internet connectivity for many people. However, the problem addressed in the research revolves around the users' awareness of the risks and their intentions with utilising public Wi-Fi networks. Many users need more knowledge regarding the risks associated with connecting to such networks. In addition, it is to determine whether people know the security risks when connecting to public networks and the reasons and factors that drive people to use public hotspots.

3.1 Motivation

Over time, there will be a growing number of public Wi-Fi networks. However, this comes with a significant risk, as the number of attackers and network attacks is expected to rise in tandem with the expansion of these networks. Hence, users must be conscious of the potential risk linked with public Wi-Fi.

The study will be conducted almost similarly to that undertaken in the UK by Sombatruang et al. (2016). The article is titled "Why do people use unsecured public Wi-Fi? An investigation of behavior and factors that drive decisions". However, there will be some differences. Firstly, the research will be conducted in Sweden to explore people's awareness of the security risks of using public Wi-Fi in the country. Secondly, since the UK study was conducted in 2016, several factors have changed, including technological advancements that have likely improved the speed and reliability of these networks, making them more appealing to users. Finally, with the growing media coverage of cyber-attacks and online security breaches, people may now be more cautious when using public Wi-Fi and take extra measures to protect themselves.

The main advantage of this thesis is to investigate public Wi-Fi users' attitudes towards the risks associated with its usage and the measures they take to ensure their safety. The study can provide valuable insights into how people perceive the risk of public Wi-Fi and the strategies they use to protect themselves.

3.2 Aim

This research purpose is to comprehend the factors that motivate individuals to use public hotspots and pinpoint the factors that contribute to risky behaviour. This study aims to determine if people are aware of the potential security risks while connecting to public wireless networks and, if so, why they decided to take those risks if they know about them.

Additionally, the research will use a qualitative approach to explore the factors that influence risky behaviour among Swedish individuals who use unsecured public Wi-Fi. Through in-depth interviews with 14 participants, the study will investigate the participants' knowledge and awareness of the prevalent hazards associated with using open public Wi-Fi.

The research questions for this thesis are:

RQ1: Why do people use public Wi-Fi in Sweden?

RQ2: How do people reason about the costs and benefits of using hotspots in Sweden?

3.3 Delimitations

The thesis will focus on user awareness and perceptions of security risks associated with connecting to public Wi-Fi. The study will not focus on the technical details of specific attacks or vulnerabilities, despite technical factors influencing user behaviour. However, this study explores the subjective factors that motivate individuals to use public Wi-Fi and the decision-making processes that lead to risky behaviour. Therefore, the study will not provide a comprehensive analysis of the technical aspects of public Wi-Fi security, and its findings should not be construed as technical advice or recommendations.

4 Methodology

Berndtsson et al. (2008) suggest that in order to accomplish the aim of the research, it is necessary to set sub-goals and select appropriate methods for each sub-goal. The methods chosen could impact the research's quality and conclusions. Therefore, it is important to consider the study's objective and anticipated outcomes before selecting a method to answer research questions and achieve the main purpose of the research.

This chapter covers the method used to carry out this study and is divided into eight sections. The first section explains how the study goal is broken down into sub-goals, while the second section provides information about the strategies used to answer the research questions. The third section discusses why the qualitative approach is the most appropriate for this thesis. Section four covers the qualitative interview, and section five provides information about collecting data. Section six explains how the interview questions are created. Section seven examines the validity and reliability considerations of the study, ensuring the accuracy and consistency of the data. Finally, section eight explores the process of thematic analysis, which is employed as the data analysis method in this study.

4.1 Sub-goals

The objectives of the research are accomplished via several sub-goals that have been established. The sub-goals are addressed using specific techniques to attain the aim of this thesis. The steps to achieve these objectives are outlined and explained below in the sequence in which they will be accomplished.

a) Literature review of the subject
b) Analyse previous research
c) Create interview questions
d) Interview conducting
e) Analysis of interview data
f) Assemble a checklist
g) Discuss the study's findings and its conclusion.

The steps mentioned above have been illustrated through a process model (Figure 4.1.1).

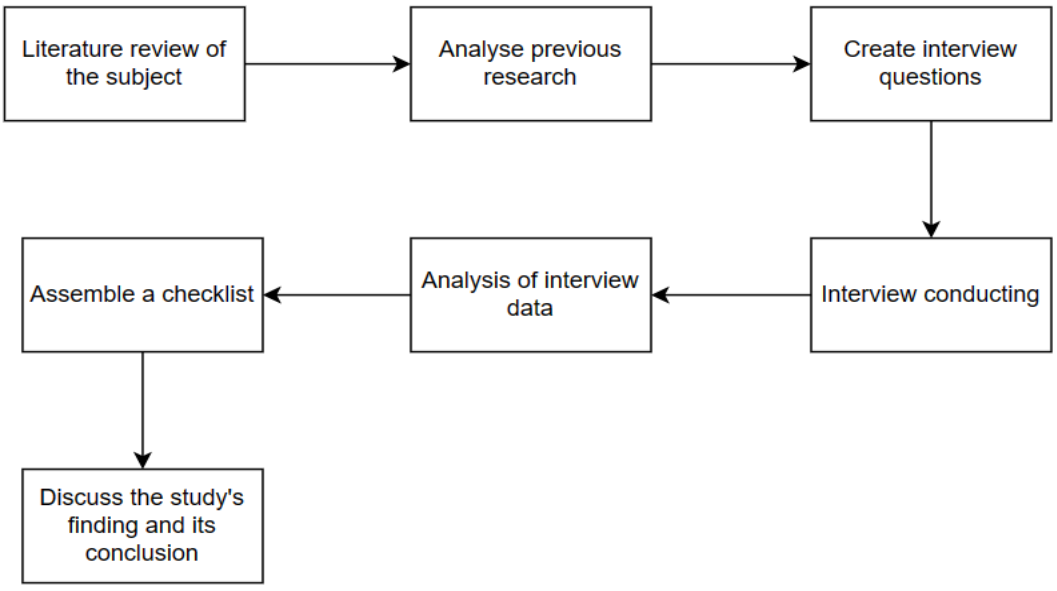

Figure 4.1.1. The process model of handling the study

4.2 General Strategy

The study aims to detect people's awareness regarding the security risk while using public Wi-Fi and investigate the factors that led to the risky behaviour. The research was conducted by interviewing 14 participants with limited geographic scope, focusing only on Sweden. A qualitative approach is used to answer the research questions and achieve the purpose of the study. The data collection will rely on semi-structured interview questions, and the information gathered will be analysed using thematic analysis.

4.3 Qualitative Approach

The qualitative approach stems from the social sciences, and its objective is to enhance comprehension of a particular field rather than explain it (Berndtsson et al., 2008). This thesis seeks to answer the research questions: "Why the people use public Wi-Fi in Sweden?"; "How do people reason about the costs and benefits of using hotspots in Sweden?"

A richer and deeper understanding of a subject can be obtained using a qualitative approach than is likely to be possible with quantitative techniques (Skinner et al., 2000). According to Shelton et al. (2014), gaining comprehension of the motivations and behaviours of individuals is crucial for progress and systematic. Well-planned qualitative research can produce valuable data and significant perspectives; this research is based on understanding why people use unsecured public networks. Qualitative research techniques are a set of approaches crafted to facilitate researchers in comprehending phenomena as they occur naturally in their environment. However, unlike most quantitative research techniques, the qualitative approach involves the researcher predefining their procedures (Shelton et al., 2014).

When a qualitative research approach is applied, the researcher becomes a part of the issue scenario because a topic is frequently investigated in a unique setting where the researcher analyses from a position near the subject being studied. A qualitative technique is used to investigate problems by looking for linkages and studying human elements in regard to technology (Berndtsson et al., 2008).

Qualitative research highlights how people experience and interpret the events and structures of their everyday social setting. Qualitative research sheds light on how people experience and interpret the events and structures of their daily social surroundings (Skinner et al., 2000). This thesis sheds light on people's experience with public wireless networks and explains the reasons for bearing the potential risks resulting from connecting to such networks. Consequently, qualitative data gathering concentrates on the routine and unexceptional events that happen naturally in natural settings to better grasp the issue (Skinner et al., 2000).

The method in this thesis is limited to interviews. Data was collected through the interview of the participants instead of using the survey method or focus group. According to Qu and Dumay (2011), focus group interviews involve a group of people being interviewed together in a flexible and exploratory discussion format where the interviewer acts as a moderator to facilitate the discussion. Thus, the main advantages of focus groups are convenience and time savings for both the interviewer and interviewees. However, focus groups may not always be suitable for studying and discussing sensitive topics. Therefore, people may disclose implicit answers publicly, as it could affect the validity of the study result.

Compared to the survey, interviews are more effective at extracting detailed personal stories and perspectives from individuals, providing researchers with a more comprehensive understanding of their views (Alshenqeeti, 2014). Interviewing helps explore how people create and interpret meanings within their natural environment. The value of interviewing stems not only from its ability to provide a complete overview and analyse language but also from allowing interviewees to express themselves in their own words, thoughts, and emotions (Alshenqeeti, 2014).

4.4 Qualitative Interviews

The qualitative research approach is based on interviews to portray and clarify how individuals live, understand, endure, perceive, and attain their experiences, which is accomplished by exploring the viewpoints and insights of people (Schultze & Avital, 2011). The conducted interview method jewels the current aim of the research as each person has different behaviour when choosing to connect to the public hotspot.

Qualitative interviews are more flexible and can yield information that may be missed in a quantitative interview. Qualitative questions are usually open-ended and allow participants to answer in their own words. The interview method is popular in scientific research because participants find it natural to talk and carry on the discussion (Griffee, 2005).

The interview method allows conducting of face-to-face (FTF). In essence, conducting interviews in person, or FTF has several advantages compared to other methods (Schober, 2018).

According to Alshenqeeti (2014), an interview is a conversation between two parties that can be expanded to gather detailed information on a specific topic or phenomenon. The purpose of the interview is to interpret the subject based on the perspectives and meanings shared by the interviewees (Alshenqeeti, 2014).

Interviewing is valuable not only for creating a comprehensive overview, analysing data, and presenting detailed perspectives of participants but also because it allows them to use their own voices and communicate their personal thoughts and emotions (Alshenqeeti, 2014).

4.5 Data Collection

The primary objectives of the interview are to comprehend why the participant utilises unsecured public Wi-Fi (Sombatruang et al., 2016). Various interview methods can be utilised to collect informative data from a qualitative research approach (Alshenqeeti, 2014).

The semi-structured interview is used in this thesis. According to Alshenqeeti (2014), the semi-structured interview offers greater flexibility than a structured interview, enabling interviewers to probe and elaborate on the interviewee's responses, leading to a more thorough investigation of the subject matter.

According to Qu and Dumay (2011), a semi-structured interview is popular due to its flexibility, ease of use, and clarity. The greatest advantage is its ability to reveal significant and frequently undisclosed human and organisational behaviour aspects. It is often the optimal and most practical method for collecting information. The semi-structured interview, rooted in human dialogue, permits a proficient interviewer to adjust the approach, speed, and sequence of inquiries to elicit complete answers from the interviewee. The crucial benefit of this method is that it empowers interviewees to provide explanations using their vocabulary and linguistic style to align with their thinking (Qu & Dumay, 2011).

The interview involved open-ended questions that had been prepared, but they not be asked in the exact order they were listed (Wohlin et al., 2012). After obtaining the participant's consent, each participant's conversation is recorded to ensure that the questions and answers are the main focus. Thus, this is necessary because capturing all the information exchanged during the interview can be challenging. According to Wohlin et al. (2012), interviews can be conducted with both groups of people and individuals. However, this particular study will only involve interviewing individuals. This decision was made because group dynamics can influence participants' answers, which may not accurately reflect their personal opinions. In addition, not all group members may have the opportunity to express their views.

On-site or via Zoom session, interviews were conducted with 14 participants from different demographic backgrounds (Table 4.5.1). Before the interviews, the participants are given an information sheet about the study and their consent is obtained. In addition, the identity of the participants will not be disclosed, nor their names are published in this thesis.

Interview subject	Code	Age	Gender	Education level
1	P1	18-24	Female	Bachelor's
2	P2	18-24	Male	Bachelor's
3	P3	25-34	Female	Bachelor's
4	P4	25-34	Male	Bachelor's
5	P5	18-24	Female	Bachelor's
6	P6	18-24	Female	Bachelor's
7	P7	35-44	Male	Bachelor's
8	P8	18-24	Female	Bachelor's
9	P9	18-24	Male	Bachelor's
10	P10	25-34	Male	Bachelor's
11	P11	18-24	Male	Bachelor's
12	P12	25-34	Male	Bachelor's
13	P13	18-24	Male	Bachelor's
14	P14	35-44	Female	High school

Table 4.5.1. Demographic of participants

4.6 Interview Questions

The questions in the interview are related to the research questions, although they may not be worded the same way. The questions can be either open-ended, meaning they permit a wide range of answers and topics from the interviewee or closed, which provides limited potential answers (Wohlin et al., 2012).

In order to design and write the research questions, the previous literature relevant to the study's aim is reviewed. This review focused on examining previous studies related to the usage of public Wi-Fi, the reasons and benefits of using public Wi-Fi and people's awareness of the risks associated with the use of public hotspots. By reviewing the existing literature, valuable insights into the field were gained, which helped inform the design of the interview questions. The literature review aimed to identify gaps in the current knowledge and understand the existing findings in relation to people's behaviours and perceptions regarding public Wi-Fi usage. This process ensured that the interview questions were tailored to address the research objectives effectively.

The design of the interview questions was inspired by previous research on public Wi-Fi networks (Sombatruang et al., 2016), which explored participants' perceptions and experiences when using open public hotspots, their perception of risks and security associated with public Wi-Fi, and the rationale behind their decision to connect or not to public Wi-Fi. The research conducted by Sombatruang et al. (2016) served as a reference point for the design of the interview questions in the present study. However, the specific interview questions used in the present study were not explicitly mentioned in the research conducted by Sombatruang et al. (2016). The interview questions were created and developed independently to address the research questions, "Why do people use public Wi-Fi in Sweden?" and "How do people reason about the costs and benefits of using hotspots in Sweden?". The questions are focused on gathering information about participants' motivations for using public Wi-Fi and the activities and applications used. The factors that lead participants to use public Wi-Fi and the perceived benefits of using it. The interview questions also covered the participants' awareness and understanding of risks associated with public Wi-Fi, including specific security risks and the measures

taken to protect personal information when using public Wi-Fi. For more details on the interview questions employed in the present study, please refer to Appendix A.

4.7 Validity and Reliability

According to Noble and Smith (2015), validity concerns the soundness and appropriateness of the methods used and the accuracy with which the results reflect the data. Whilst reliability pertains to the consistency of the analytical procedures utilised. Lincoln and Guba (1988) suggest alternative standards to demonstrate rigour in qualitative research, which include truth value and consistency; the truth value house aspect to reflexivity and applicability to the phenomenon.

4.7.1 Truth value

Noble and Smith (2015) acknowledge the existence of diverse perspectives; the researchers describe their personal experiences and opinions that could have led to bias in the methodology; presents the participants' viewpoint clearly and precisely. This section will present the reflexivity and representativeness of the findings concerning the phenomena (Noble & Smith, 2015).

4.7.2 Reflexivity

According to Noble and Smith (2015), personal biases may have affected the results. In this thesis, personal biases are considered to avoid influencing the finding. The interview questions are formulated in a manner far from the directive way. The questions are written in an appropriate way to be able to get the answer from the participant with more information to get accurate findings. Furthermore, the interview questions are discussed with the supervisor and the examiner to avoid personal biases. In addition, no assumption is taken before the interviews are conducted, such as that people who use insecure public Wi-Fi are unaware of the risks or are careless with their personal information.

Peer debriefing is a collaborative process that aids researchers in identifying and uncovering any biases or assumptions they may have unknowingly incorporated into their work (Noble & Smith, 2015). Engaging in discussion with an impartial peer, such as a researcher focusing on a different research area, can assist the researcher in refining their understanding of the data and pinpointing potential biases (Hadi & José Closs, 2016). The thesis underwent a rigorous academic peer review process and received valuable feedback from two students and the examiner. This peer debriefing was facilitated through opportunities such as presenting and discussing the research at the university. During these presentations, the students and examiner actively engaged in questioning and providing critical feedback on the thesis. This comprehensive evaluation by peers and the examiner ensured the thorough examination of the study's methodology, findings, and potential limitations. The incorporation of their feedback enhanced the academic integrity and quality of the research.

4.7.3 The results' applicability to the phenomenon

Sampling bias is avoided when there is a possibility of a biased selection of study participants or data sources, leading to an incomplete or inaccurate portrayal of the population or phenomenon under investigation. Acknowledging such biases requires recognising the constraints of the sample and examining their potential impact on the analysis and findings (Noble & Smith, 2015). Sampling bias is avoided in this study. All 14 samples selected for the interview used public Wi-Fi, and this approach would help to avoid biased results. In addition, the samples had diversity in age groups and genders selected to provide a more comprehensive understanding of the factors that influence the use of public Wi-Fi in Sweden.

In addition, it maintains meticulous records, provides a rational decision path and ensures data interpretations are consistent and transparent (Noble & Smith, 2015). The voice recording of the interviews are kept, and the transcript into text format.

Respondent validation engages participants in providing feedback on the transcribed and whether the

concluding themes and concepts developed appropriately reflect the phenomena under investigation (Noble & Smith, 2015). This study could engage four participants to ensure the right reflection on the issue and get more accurate findings.

Furthermore, to support the findings, the research incorporates detailed and verbatim descriptions of participants' accounts. These detailed and thick descriptions provide a deep understanding of the participants' experiences, perspectives, and narratives, offering substantial evidence to support the conclusions drawn in the study (Noble & Smith, 2015). This thesis includes the incorporation of thick verbatim descriptions derived from participants' voice recordings played a crucial role in supporting and robustness of the findings.

According to Noble and Smith (2015), one of the strategies to ensure the truth value is data triangulation which is the process through which multiple approaches and viewpoints work together to provide a complete collection of findings. This thesis cannot follow data triangulation since just one approach is used, and the data was collected via only the interview method.

4.7.4 Consistency

According to Noble and Smith (2015), consistency is a clear and comprehensible account of the research process provided, starting from the preliminary outline and then moving on to the creation of methods and the presentation of results. The thesis has explained all steps of the methodology process, starting with sub-goals, specifying the approach and method used to collect the data and explaining the analysed method used to get the finding. Furthermore, the process is controlled by the supervisor.

4.8 Thematic Analysis

The thematic analysis method is used to analyse the data obtained from the interviews. Thematic analysis is an analytical framework that strives to identify, analyse, and report recurring patterns or themes that emerge from primary research. At its most fundamental level, it involves a rigorous data organisation, presentation, and interpretation process that aims to uncover various dimensions of the research topic (Wohlin et al., 2012). According to Braun and Clarke (2006), the thematic analysis involves a nuanced and comprehensive categorisation and explanation of the data set while minimising any potential inadequacies in the description. The thematic analysis method is adopted because data have been collected through interviews with individuals of different levels of education, age, gender and the extent of their use of public networks. Detailed, meaningful data will be collected to understand participants' behaviour and rationale for using insecure public hotspots.

The study used a thematic analysis approach that follows the guidelines of Braun and Clarke (2006), which outlines six distinct phases for conducting thematic analysis, as shown in Table 4.9.1. However, Maguire and Delahunt (2017) suggest that the stages do not have to occur in a specific order. Sometimes the person might need to go back and forth between them, potentially multiple times, especially when working with a large amount of detailed information.

1	Acquiring familiarity with the data
2	Creating initial codes
3	Scanning for themes
4	Reviewing themes
5	Defining and naming themes
6	Reporting the findings

Table 4.9.1. Thematic analysis phases

The process of analysis utilised in this study was founded on Braun and Clarke (2006) guide to thematic analysis. All of the interview recordings were transcribed before the analysis process started. The transcriptions were reviewed several times to enhance the overall comprehension of the findings.

Once this step was completed, the gathered materials were coded related to the research questions to enhance their comprehensibility and comparability, see Figure 4.9.2. Open coding was utilised to arrange the materials in a deliberate and methodical manner. Through the process of coding, the material was condensed to include only the relevant portions pertaining to the study and research questions. Open coding is more adaptable than inductive coding and permits the development and modification of keywords during the analysis process (Braun & Clarke, 2006).

Excerpt	**Codes**
"Well, actually, like sometimes surfing the Internet, I use Google for browsing and checking the news, and I use social media like WhatsApp to talk with my family, YouTube, Netflix, Facebook and Instagram. Also, I use it for education purposes, like in school or on the train, once I feel that I have time."- Participant 4.	Internet browsing. Communication with family. Social media services. Education purposes.
"Public Wi-Fi is convenient because it allows me to connect multiple devices at the same time. I can work on my laptop and watch videos on my phone at the same. Because it is free also, so I do not have to pay money. I use public Wi-Fi to save my mobile data because I have a limited subscription of 8GB."– Participant 14.	Multi-device connectivity. Free. Limited mobile data usage.
"I know it is risky, but I have just general information about the risk, like someone can track me on public Wi-Fi and collect some information about me. But actually, I have no idea about fake access points, man-in-the-middle and phishing. This is the first time I have heard about it."– Participant 9.	Awareness of public Wi-Fi risks. Risk perception of public Wi-Fi. Lack of knowledge about fake access points, man-in-the-middle attacks and phishing.

Figure 4.9.2. Show an example of coding

In the next phase of the analysis process, codes are integrated together to create and develop various themes and form a themes map. In the next phase, which involves reviewing the theme, each theme is carefully analysed to determine if there is sufficient data to support it. The themes need to be internally coherent. In the next phase, the themes are identified and given specific definitions and names. Braun and Clarke (2006) note that a theme is not defined by specific guidelines but rather by its significance regarding the research questions. Finally, in the last phase, producing the report, the data is used to provide further arguments in relation to the research questions.

5 Results

The results analysed provide insights into the motivations and factors that influence participants' use of public Wi-Fi, as well as their awareness of the associated risks. Table 5.1 presents the comprehensive list of codes, sub-themes, and the main theme. The subsequent sections present the main themes and present the findings accordingly.

Codes	**Sub-theme**	**Main theme**
Social media services. Communication with Family.	Social media	Usage intent of public Wi-Fi
Internet browsing. Education purposes. Occasional reliance on public Wi-Fi while travelling. Transportation information. Broad usage intent.	Finding information	
Multi-device connectivity. Faster Internet speeds. Access to Wi-Fi in public places. Available in public places. Quick access to the Internet.	Convenience	Reasons and benefits of using public Wi-Fi
Cost-saving. Free.	Cost-effective	
Limited mobile data usage. Saving costs associated with mobile data.	Save mobile data	
Train/bus Wi-Fi for stability. Poor mobile coverage in buildings. Poor mobile coverage in remote areas. Use of public Wi-Fi in response to poor mobile coverage.	Poor mobile coverage	
Awareness of public Wi-Fi risks. Limited knowledge of risks. Trust in specific public Wi-Fi networks. Risk perception of public Wi-Fi. Lack of knowledge about fake	Security risks associated with public Wi-Fi usage	Privacy and security concerns of using public hotspots

access points, man-in-the-middle attacks and phishing.		
Knowledge of data collection and potential misuse. Concerns about personal information exposure. Lack of consideration and limited awareness. Perceived safety based on experience. Perception of personal information security.	Personal information and personal information aggregation	
Sensitivity of financial transactions. Potential for unauthorised access. Risk perception and personal experience. Limited awareness and lack of consideration.	Exposure of financial details	
No tool to protect. Limited awareness of safety measures.	Lack of knowledge regarding protection measures.	Public Wi-Fi protection
VPN as a protection strategy. Using public Wi-Fi without encryption in some cases.	Protection to stay safe on public Wi-Fi	

Table 5.1. Codes, sub-theme and the main theme

5.1 Usage intent of public Wi-Fi

The usage intent of public Wi-Fi varied among participants in this study. However, the majority of them indicated using public Wi-Fi for browsing the Internet and engaging in social media services activities and activities related to education, such as school assignments or university tasks. This thesis identifies two themes that underscore the usage intent of public hotspots. First, social media is presented in 5.1.1, and the second theme of finding information is presented in 5.1.2

5.1.1 Social media

In this study, the participants stated the use of social media services such as Facebook, Instagram, Twitter, Netflix, YouTube and WhatsApp while connecting to public Wi-Fi. Many participants used social media applications to communicate with family and friends or watch movies. Participant 1 stated the use of public Wi-Fi primarily for accessing social media apps, as well as to communicate with friends and family. This response highlights the usage intent of public Wi-Fi as a means of accessing social media and staying connected with others.

"I mainly use public Wi-Fi for accessing social media apps like Facebook, Instagram, and Twitter. I also use WhatsApp to talk with my friends and family."- Participant 1

Participant 10 stated that he uses public Wi-Fi for various purposes, including communicating with

friends and family through social media apps like Facebook, Snapchat, and Instagram.

"As a student, I use public Wi-Fi to access my online courses and study materials and surf the Internet and also watch videos. I also use it to communicate with my friends through social media apps; for example, I use Facebook, Snapchat and Instagram."- Participant 10

5.1.2 Finding information

The majority of participants mentioned utilising public Wi-Fi for various purposes, such as educational activities and browsing the Internet to seek information or access services like locating places or arranging transportation. Additionally, many participants mentioned using public Wi-Fi for online shopping.

Participant 3's response shows that public Wi-Fi is an essential resource for accessing a broad range of services and activities, from educational purposes, entertainment and communication to shopping and banking. Public Wi-Fi allows the participant to engage in these activities without having to worry about data usage or limited connectivity.

"I use public Wi-Fi for everything, from browsing the web to streaming music, videos and use it to do my assignments. I also use it to shop online, check my email, and stay connected with my friends on social media platforms. I also use public Wi-Fi to pay my bills."- Participant 3

However, participant 9 stated that he does not rely on public Wi-Fi much but uses it sometimes while travelling. The participant used public Wi-Fi to access location information, book a taxi, and check transportation information.

"Actually, I do not rely on public Wi-Fi much, but sometimes, for example, when I am travelling. So, I need Wi-Fi to know a place location or to book a taxi and check, for example, transportation information."- Participant 9

5.2 Reasons, benefits and factors of using public Wi-Fi

The interviews with participants revealed several factors driving people to use public Wi-Fi, one of which is the desire to conserve their mobile phone's battery. Some respondents noted that using mobile cellular data consumes more battery power compared to using Wi-Fi. Moreover, participants highlighted that public Wi-Fi is often the only option available for Internet connectivity while travelling, especially in airports. Participant 9 specifically acknowledged the limited choices for accessing the Internet, particularly in airports where public Wi-Fi is typically the only available choice.
"When I travel, especially in airports, public Wi-Fi is usually the only option available for me to connect to the Internet [...]. - Participant 9

Additionally, this study identifies several themes that underscore the reasons, benefits, and factors associated with the utilisation of public Wi-Fi. The first theme, presented in section 5.2.1, focuses on the convenience provided by public Wi-Fi. The second theme, discussed in section 5.2.2, highlights the cost-effectiveness of utilising public Wi-Fi compared to using cellular data. Furthermore, section 5.2.3 delves into the theme of how public Wi-Fi helps save mobile data usage and finally, poor mobile coverage is presented under section 5.2.4.

5.2.1 Convenience

Convenience is one of the reasons and benefits of using public Wi-Fi. Most of the participants point out the use of public Wi-Fi mainly because of its convenience.

Participant 5 mentioned that she prefers using public Wi-Fi because it is faster than her mobile data connection. The participant also mentioned that she could easily stream videos and download large files without any issues. Additionally, public Wi-Fi is available in many public places, making it very convenient for her to stay connected wherever she is.

"I prefer using public Wi-Fi because it is much faster than my mobile data connection. I can easily stream

videos and download large files without any issues. Plus, it is available in many public places, which makes it very convenient for me to stay connected wherever I am outside."- Participant 5

Responder 3 mentioned that public Wi-Fi is provided higher speed than mobile data connection and saves time.

“Public Wi-Fi is convenient because it provides faster download and upload speeds compared to my mobile data connection, and it saves my time.”- Participant 3

Participant 14 pointed out that public Wi-Fi is used for multiple devices and various use.

“Public Wi-Fi is convenient because it allows me to connect multiple devices at the same time. I can work on my laptop and watch videos on my phone at the same.”- Participant 14

Participant 8 mentioned that she prefers public Wi-Fi because she does not need to use her personal hotspot (mobile hotspot using cellular data), making connecting her devices to the Internet more convenient.

"Whenever I need to use the Internet on my laptop, I prefer using public Wi-Fi instead of my personal hotspot. It is just more convenient and does not drain my phone's battery."- "Participant 8

Overall, participants prefer using public Wi-Fi mainly because of its convenience, which includes faster speeds, availability in public places, and the ability to connect multiple devices simultaneously. It also saves time and eliminates the need to use personal hotspots, making it more convenient for users to stay connected to the Internet.

5.2.2 Cost-effective

All participants in the study reported the importance of the cost-free nature of public Wi-Fi as a primary motive for its utilisation. The participants highlighted that they could easily access the Internet and use various services without paying fees in various locations, such as schools, train stations, airports, shopping malls, and other public places.

According to some participants, one of the advantages of using public Wi-Fi is that it is accessible without any additional charge. This cost-effectiveness is especially beneficial while travelling, as it allows participants to carry out various tasks from different locations without incurring any extra expenses. For instance, they can use public Wi-Fi to check maps and navigate unfamiliar areas, as well as stay connected with friends and family, all without the need for additional payments. The availability of free public Wi-Fi, therefore, provides a cost-effective solution for fulfilling their Internet requirements while on the go, eliminating the need to pay for data roaming or other additional charges associated with Internet access during travel.

"Public Wi-Fi is a great option for me when I am travelling because it is free. I can check maps, find information about the area, and stay connected with friends and family without paying anything extra."- Participant 12

Many participants shared their perspectives on the cost-effectiveness of public Wi-Fi, underling the financial benefits it brings. According to them, using public Wi-Fi eliminates the need to spend money on an Internet connection while being away from home. The participants found this particularly advantageous when working remotely, as they can access the Internet without incurring any additional charges. By utilizing public Wi-Fi, they can stay connected, manage their tasks, and even attend online meetings without worrying about costs.

"Public Wi-Fi is such a money-saver for me, especially when I am outside the home. The best part is that it is completely free! When I am, for example, working remotely, I rely on public Wi-Fi to stay connected without having to spend money."- Participant 13

5.2.3 Save mobile data

Save mobile data is one of the reasons and factors that drive people to use public Wi-Fi. Most of the participants are using public Wi-Fi to save mobile data allowance, and many participants report that

they have a limited mobile subscription plan. Public Wi-Fi helps the responders to use their mobile data connection efficiently. Many responders explicitly indicated that they use public Wi-Fi to conserve their mobile data usage and reduce costs by opting for more affordable mobile data plans.

"Public Wi-Fi helps me save money by choosing a lower mobile phone plan. I use public Wi-Fi as much as it is available to conserve my mobile data."- Participant 7

Participant 2 explained that he lives in an area without a wireless network, which drives the participant to use his mobile subscription for Internet access. The participant stated that he has a limited monthly mobile data plan of 25 gigabytes, and he connects to public Wi-Fi whenever it is possible to save his mobile subscription, which he uses at home.

"I think that I want to save my own 4g because I have just 25 gigabytes every month. But I am leaving a place that does not have so good Wi-Fi, and usually, at the end of the month, I have like one or two gigabytes of 25 gigabytes. So that is why when I am outside, I try to use public Wi-Fi, if possible."- Participant 2

5.2.4 Poor mobile coverage

Many responders point out that poor mobile coverage data is a key factor and a common issue that drives them to use public Wi-Fi in different locations, especially in remote or indoor areas. Public Wi-Fi can provide a more stable Internet connection in locations with weak mobile network coverage.

Participant 14 uses public Wi-Fi because it is a more stable and reliable Internet connection when the mobile network is poor while on the train or the bus in some places.

"Sometimes the mobile network is weak in a different location when I am using the train or the bus. So, I prefer to connect to the train or the bus Wi-Fi, which is more stable." – Participant 14

Participant 5 mentioned that one of the reasons and motives for using public wireless networks is when a person is in a building with poor mobile phone coverage, such as the basement or underground garage.

"When I am in a building with poor mobile coverage, I usually try to connect to public Wi-Fi. This happens a lot in basements or underground parking garages. I rely on public Wi-Fi because the mobile network is weak or not available at all."- Participant 5

Participant 12 reported using public Wi-Fi in a remote area or travelling through areas with poor mobile coverage, such as camping. The participant found that public Wi-Fi can provide a more reliable connection in such situations.

"I love camping, but the mobile coverage can be pretty poor in remote areas far from the city. That is why I always try to find public Wi-Fi when I am out there."- Participant 12

5.3 Privacy and security concerns of using public hotspots

The interviews with the participants showed that their concerns and awareness regarding Wi-Fi use fell under three themes. First, security risks associated with public Wi-Fi usage are presented under 5.3.1. Second, personal information and personal information aggregation are presented under 5.3.2. Finally, the exposure of financial details is presented under 5.3.3.

5.3.1 Security risks associated with public Wi-Fi usage

Despite the spread of public Wi-Fi, many participants in this study were unaware of the potential risks associated with its use. Specifically, 12 out of 14 participants did not know about the risks of fake access points, man-in-the-middle attacks, and phishing. These participants had little understanding of how these risks could be exploited to compromise the security of their data.

Participant 6 demonstrated some basic understanding of the risks of fake access points and phishing

but remained uninformed about man-in-the-middle attacks.

“I know it exists, and I know that it can happen as such. I do not really know the details of how it is done. So just try to be generally careful and also try not to go into Wi-Fi [...] I know it is a risk because it is not like devices can recognise each other within the same network.”- Participant 6

However, this lack of awareness is concerning, as it suggests that many users may unknowingly put themselves at risk when using public Wi-Fi. Participants 2 and 13 clearly stated that they had no knowledge previously regarding the potential risks associated with public Wi-Fi.

“I have never been told that it can be risky if you use public Wi-Fi.”- Participant 2

"I had no idea about fake access points or man-in-the-middle attacks until now. As for phishing, I have heard of it, but I never thought it could happen through public Wi-Fi."- Participant 13

5.3.2 Personal information and personal information aggregation

Most of the participants demonstrated a level of understanding of the issue of information aggregation and the vulnerability of personal information when connected to public Wi-Fi networks. These participants were aware of the risks involved in sharing their personal data and expressed concerns about third-party entities accessing and collating their information, creating comprehensive profiles that could potentially compromise their privacy. They highlighted the potential for cybercriminals to exploit this information for malicious purposes. One participant recognised the inherent risk in data collection and acknowledged the potential for misuse by unauthorised individuals.

"Well, I know that it is a risk because all networks gather data, and there is a risk involved with this, and those who receive the information could potentially use it against me."- Participant 11

Some participants have expressed doubt regarding using their personal information when accessing public Wi-Fi. Participant 2 was apprehensive about the possibility of others accessing his name, phone number, and address, and he was unsure about how this information could be exploited. This participant highlighted his uncertainty about the potential consequences of accessing his personal information and the extent to which it could be exploited.

"I do not know how they could like to use my personal information, my name. They can check up, and they know my name and my phone number and my address, what I have, and things like that. I do not think that they can come any closer than that."- Participant 2

However, another participant exhibited a limited awareness of the security risks pertaining to personal information and its aggregation when utilising public Wi-Fi. The participant displayed a sense of indifference and undermined the potential dangers that unauthorised access to her personal data could pose. The participant's perception of minimal risk indicated a lack of understanding concerning the potential ramifications associated with divulging personal information over public Wi-Fi networks.

"I never really thought about it. I mean, I always use public Wi-Fi and never have any issues. I do not think anyone would be interested in my personal information anyway." - Participant 5

5.3.3 Exposure of financial details

Several participants in the study expressed concerns about the security risks associated with using public Wi-Fi, particularly in relation to the exposure to financial information. The participants demonstrated a reluctance to use applications or engage in financial transactions while connected to public wireless networks. However, two participants were unaware of the risk of leaked financial information while using public Wi-Fi, and they used the public hotspot to do bank transactions or shop from different websites.

Participant 11 expressed concerns about the safety of entering his bank card's Card Verification Code (CVC) when making online purchases. The participant believed that if someone else had access to the router or the ability to intercept data packets, where could potentially view sensitive card information, including the card number, validation date, and CVC code. The participant showed a level of awareness of the potential risks associated with entering financial information over public Wi-Fi networks. In

addition, the participant recognised the possibility of unauthorised individuals intercepting and accessing his card details.

"Yes, because while buying things on the Internet, I will need to enter my CVC code on the bank card. I think it is unsafe because other people can see the data package if they have access to the router or if they have accessed and see my card number, the validation date, and my CVC or CV code. So that could be a huge problem."- Participant 11

In another instance, participant 2 demonstrated a complete lack of knowledge regarding the potential leakage of financial details when using public Wi-Fi. Oblivious to the risks involved, the participant openly accessed his bank application while connected to public networks, regardless of location, be it a crowded train or any other public place.

"I never really thought about it. I use public Wi-Fi all the time, in places like trains or cafes, and I log into my bank account, or sometimes I do some shopping. I have never had any issues so far, so I assume it is safe."- Participant 2

5.4 Public Wi-Fi protection

The study's findings are varied concerning the protection measures employed when connecting to public Wi-Fi, which can be categorised into two sub-themes. The first sub-theme, discussed in section 5.4.1, highlights the participants' lack of knowledge regarding protection measures. The second sub-theme, presented in section 5.4.2, focuses on the measures taken to ensure safety while using public Wi-Fi.

5.4.1 Lack of knowledge regarding protection measures.

Many participants expressed a limited understanding of the necessary precautions to take while using public Wi-Fi. The participants explicitly stated the use of public Wi-Fi without any protection measures and exhibited a tendency to trust the security of public Wi-Fi without implementing additional protective measures such as using virtual private networks or ensuring encrypted connections.

Participant 14 expressed that she had not considered the security implications before but had complete trust in public Wi-Fi, using it in a similar manner to her home Wi-Fi. The participant stated that she connected to public Wi-Fi without any protection and was unaware of the need for software to ensure her safety while using public hotspots.

“I did not think about it before, but I trust it and use public Wi-Fi as normal and similar when I use my Wi-Fi at home. […] To be honest, I used to connect to public Wi-Fi without any protection. I do not know that I should use any software to be on the safe side during the use of the public hotspot.”- Participant 14

While some of the participants showed complete trust in the security and expressed high confidence in the security of public wireless networks and used public Wi-Fi for all purposes as they usually do without the use of any protection tool. However, the participants justified that they did not experience any problems during their connection to public networks. Participants explicitly explained the use of public networks to carry out many tasks, including banking transactions.

Participant 3 expressed her trust in the security of public Wi-Fi and claimed not to be too concerned about it. The participant utilises public Wi-Fi for a wide range of purposes, including financial transactions, and has never encountered any problems. The participant stated the use of public Wi-Fi without any protection way.

"I trust the security of public Wi-Fi. I am not too worried about it, to be honest. I use public Wi-Fi for pretty much everything, including financial stuff, and I have never had any issues. […] I have not used any protection strategies while using public hotspots"- Participant 3

Participant 2 stated that he uses public Wi-Fi whenever it is available, and he trusts its reliability. The participant mentioned that he conducted various activities, including shopping, banking, and accessing social media apps via public Wi-Fi, without encountering any issues.

"Actually, I use public Wi-Fi in different places whenever it is available because I trust it. I used to do everything while connecting public Wi-Fi, like shopping and banking, and I used social media apps without experiencing any issues."- Participant 2

5.4.2 Protections to stay safe on public Wi-Fi

The study found that some participants used VPN technology to secure their online activities and avoid transmitting financial details while using public Wi-Fi. Two participants used antivirus software as a protective measure while accessing public Wi-Fi. In addition, many participants showed low trust in the security of public Wi-Fi and reported refraining from using financial information over public Wi-Fi.

Participant 6 highlighted the adoption of VPN technology and avoiding banking activities as primary safety measures while using public Wi-Fi.

“Well, I try to use a VPN. I tried not to log into things like the bank app or website or use my bank ID while I connected to public Wi-Fi. I think that is the main one.”- Participant 6

Additionally, participant 11 noted that in urgent situations, the participant might use public Wi-Fi without encryption. Still, the participant prefers to use VPN technology to safeguard his data whenever he has time.

“I know that using public Wi-Fi without encryption is not secure, but sometimes I have no other choice because sometimes I need to use public Wi-Fi in an urgent way. But if I have more time, I will use a VPN to protect my data.”- Participant 11

Participant 5 mentioned her use of antivirus protection for her devices. The participant has Norton antivirus installed on her mobile phone and used AdBlock on the laptop as a means of protection against viruses and hackers.

“Yes, I use antivirus protection. I have Norton antivirus installed on my mobile phone, and I use AdBlock on my laptop. That is what I know or consider as protection against viruses or hackers.”- Participant 5

6 Discussion

The results of the study are discussed in this section, and various aspects are discussed in this chapter. First, the limitation is presented under 6.1. Ethical aspects are explored in section 6.2, which presents the ethical considerations of the study. Finally, section 6.3 discusses societal aspects.

The findings of this study indicated that people use and connect to public Wi-Fi while outside the home, such as in school, shopping malls or other public places. In addition, this study indicates that public Wi-Fi is primarily used for different purposes, such as browsing the Internet and engaging in social media activities. The participants in the study reported using popular applications such as YouTube, Facebook, Instagram, and Snapchat while connected to public Wi-Fi networks. This finding is consistent with the research conducted by Sombatruang et al. (2016) and Choi et al. (2022), which found that users use public hotspots for online media services in different public places. The consistency of these findings suggests a general trend in public Wi-Fi usage across different contexts.

Furthermore, this thesis found several main reasons, benefits and factors for using public Wi-Fi. Most participants stated that convenience was one of the significant reasons to use public hotspots, where public hotspots are easy to use and provide faster speed compared to their mobile data connection. All participants used public Wi-Fi because it is free and easily accessible in schools, train stations, airports, shopping malls, and other public places. This finding is consistent with previous research that has identified cost-effectiveness as a significant factor motivating individuals to use public Wi-Fi (Sombatruang et al., 2016).

Additionally, most of the participants use public Wi-Fi to save their mobile data connections because they have limited mobile subscription plans. Using public Wi-Fi helps them use their mobile data efficiently and reduces costs. Sombatruang et al. (2018) found that people use public Wi-Fi to conserve mobile data allowance.

This study contributes to the previous literature by uncovering a new factor that influences the participants to use public Wi-Fi, which had not been explored in previous studies, within the specific context of Sweden, with its vast geographic landscape and varying levels of network infrastructure. Poor mobile coverage was another factor that drove participants to use public Wi-Fi, especially in remote or indoor areas with weak mobile network coverage. Public Wi-Fi provided a more stable Internet connection in such locations, enabling participants to stay connected. This study's finding expands our understanding of the motivations behind public Wi-Fi usage and underscores the importance of network coverage as a contributing factor.

The similarities between this study's findings and previous research highlight the consistency in users' preferences and motivations for public Wi-Fi usage. Factors such as convenience, cost-effectiveness, efficient use of limited mobile data, and the influence of network coverage emerge as common themes. These collective findings contribute to a comprehensive understanding of users' motivations for connecting to public Wi-Fi networks, emphasizing the significance of these networks in meeting connectivity needs and reducing data-related expenses, particularly in locations with inadequate mobile network coverage.

Regarding the level of awareness of the potential security risks of using public Wi-Fi, the study found that most of the participants basically were unaware of rogue access points, man-in-the-middle attacks and phishing attempts. The participants show a limited understanding of the risks. This finding is consistent with other research, which found the participant had no knowledge related to rogue access points (Klasnja et al., 2009). However, when the participants were queried regarding the potential risks associated with connecting to public Wi-Fi networks, specifically with regard to the leakage of sensitive financial or personal information, it was observed that the participants exhibited a level of knowledge that could possibly occur. The participants in the study expressed concerns about the potential for third-party entities to access and misuse their personal data, particularly in the context of unsecured public Wi-Fi networks.

Many participants were also apprehensive about the possibility of financial information being compromised. However, despite this awareness, the majority of the participants reported that they

continued to use public Wi-Fi networks frequently. This aligns with other research, which found many individuals may still use public Wi-Fi even though it poses a risk to their security. (Sombatruang et al., 2018). It is worth noting that this contradiction in behaviour highlights the complex nature of users' decision-making when it comes to public Wi-Fi usage and their risk tolerance levels.

The study found that some participants took proactive measures to enhance their safety while using public Wi-Fi. They reported using VPN technology to secure their online activities and avoid transmitting sensitive information. Additionally, a few participants mentioned using antivirus software as a protective measure. Furthermore, many participants expressed low trust in the security of public Wi-Fi and refrained from conducting financial transactions or sharing sensitive information over these networks. On the other hand, the study's findings on public Wi-Fi protection measures reveal a significant gap in the participants' understanding of necessary precautions. Many participants displayed a tendency to trust the security of public Wi-Fi without implementing additional protective measures such as VPNs or encrypted connections. This lack of knowledge was evident in their usage patterns, where they connected to public Wi-Fi networks without any form of protection. These findings are consistent with previous studies on trust in Wi-Fi hotspots (Kindberg et al., 2008) and privacy concerns in everyday Wi-Fi use (Klasnja et al., 2009). Kindberg et al. (2008) highlighted the existence of trust among Wi-Fi hotspot users, leading to a lack of precautionary measures. Similarly, Klasnja et al. (2009) found that individuals tend to be fearless when using Wi-Fi networks, indicating a lack of concern for privacy and security. The participants in the current study demonstrated similar patterns of behaviour, exhibiting high levels of trust in the security of APs and a lack of knowledge regarding protection measures. The results underline the need for increased awareness and education regarding public Wi-Fi security and suggest potential strategies to promote safer usage of these networks.

6.1 Limitations

The study used a qualitative approach to collect data through interviews with 14 participants. The data were analysed through thematic analysis. The selected method was effective in providing an in-depth understanding of the experiences of participants and the factors that motivate them to use public Wi-Fi. However, a larger sample size would have provided more detailed insights into the motivations and risk-taking behaviours of individuals using public Wi-Fi.

The outcomes can have varying interpretations based on the setting and the demographic under examination. For instance, the results of this investigation may not have universal applicability beyond Sweden. Moreover, the study did not differentiate between different types of public Wi-Fi networks, such as free Wi-Fi offered by establishments or those that require a code obtained through purchase, such as coffee shops. This lack of differentiation may overlook potential variations in security practices and user behaviours between these types of networks, which could impact the findings. Additionally, one limitation of the study is that it relied on self-reporting from participants regarding their usage of public Wi-Fi, which may introduce response bias and inaccuracies. Conducting on-site interviews or providing a more representative sample and deeper insights into users' behaviours and perceptions. Finally, the study relied on participants' self-reported use of antivirus software or VPN technology as a measure of security. However, the study did not verify whether participants were actually using these measures or if they were using them correctly, which could affect the accuracy of the findings.

6.2 Ethical Aspects

The study's findings shed light on numerous ethical implications linked to the utilisation of public Wi-Fi. These implications revolve around concerns such as the potential misuse of information by malicious actors, the responsible treatment of user data by companies, and the risks posed by rogue access points that threaten individuals' privacy and have broader societal ramifications.

One notable ethical concern revolves around protecting users' personal information and online security. The study exposed a lack of awareness among many participants regarding protective measures while using public Wi-Fi, rendering them susceptible to privacy breaches. Unsecured public

wireless networks can be exploited by hackers to intercept sensitive data, leading to identity theft, financial fraud, and other detrimental consequences.

Furthermore, the research underscored the potential abuse of user information by companies that offer public Wi-Fi services. Participants engaged in activities involving confidential data while connected to public Wi-Fi, potentially exposing their personal and financial information to service providers. Ethical considerations arise when companies utilise or sell this data without proper consent, compromising users' privacy and autonomy.

Another ethical aspect pertains to the installation of deceptive access points, which are unauthorised Wi-Fi networks designed to deceive unsuspecting users. These rogue networks trick individuals into connecting, thereby granting hackers access to collect personal data for malicious purposes. Such practices pose substantial security risks and contribute to various forms of cybercrime, ultimately impacting individuals and society in adverse ways.

6.3 Societal Aspects

This research explores the societal implications stemming from the limited information accessible to individuals and the lack of accurate understanding of the risks associated with utilising public wireless networks. The findings highlight that the majority do not know about the main risks nor how to take the necessary measures to protect their data and personal information while connecting to public open wireless networks. Initiating educational and awareness campaigns could prove beneficial in shaping public perceptions concerning the usage of public Wi-Fi networks. By conducting public campaigns and implementing educational programs, community awareness of the potential risks associated with utilising public networks can be heightened, thereby influencing behaviours and decision-making.

When examining the utilisation of public Wi-Fi networks, an important factor to consider is the role of infrastructure and accessibility. Specifically, the availability and quality of mobile network coverage exhibit notable variations across various locations throughout Sweden. This variability in network coverage may impact individuals' reliance on public Wi-Fi networks to access the Internet. The deployment of 5G technology emerges as a promising solution to alleviate the coverage issue. The implementation of 5G networks can provide enhanced connectivity, improved network speeds, and increased capacity, which can help address the limitations of existing mobile network coverage. By leveraging 5G technology, individuals in areas with limited coverage can potentially access high-speed and reliable Internet connections, reducing their dependence on public Wi-Fi networks. Therefore, the integration of 5G technology presents an excellent opportunity to mitigate the coverage issue and enhance the accessibility of Internet services for users across various locations in Sweden.

7 Conclusion

This research aimed to investigate the factors that motivate individuals to use public Wi-Fi networks, identify the factors that contribute to risky behaviour, and evaluate the level of knowledge among the users regarding the risks associated with using unsecured public Wi-Fi. Through qualitative interviews with 14 participants in Sweden, the research sought to answer two research questions. By addressing the research questions, valuable insights have been obtained, shedding light on the factors that drive individuals to use public Wi-Fi and their perceptions regarding its cost and benefits.

Research question 1: Why the people use public Wi-Fi in Sweden?

The study revealed that participants had varying intentions when using public Wi-Fi, including Internet browsing, social media engagement, finding information, and activities related to education. The findings of this study explored several key motivations for using public Wi-Fi among participants in Sweden. Convenience emerged as a significant factor, with participants emphasising the ease of use and faster speeds offered by public hotspots compared to their mobile data connections. The widespread availability of public Wi-Fi in different public locations contributed to its popularity and cost-effectiveness compared to cellular data, particularly for individuals with limited data plans. Insufficient mobile coverage in certain areas also drove people to rely on public Wi-Fi networks.

Research question 2: How do people reason about the costs and benefits of using hotspots in Sweden?

Despite the benefits, participants were aware of the security risks associated with unsecured public wireless networks. They acknowledged the potential interception of personal data by hackers and malicious actors for fraudulent activities. Nevertheless, some participants still chose to use public Wi-Fi, suggesting that convenience and cost may outweigh the perceived security concerns.

Moreover, the study revealed that participants had limited awareness of more sophisticated cyber-attacks such as fake access points, man-in-the-middle attacks, and phishing attempts. This lack of awareness increases vulnerability to cyber-attacks on public Wi-Fi networks. Therefore, individuals using public Wi-Fi should educate themselves about the associated risks and implement measures to protect their personal information.

It is important to highlight that this study specifically focused on the Swedish participants and cannot be generalised to other contexts. Care must be taken when interpreting the results beyond the boundaries of this study, as they may not accurately reflect the views and behaviours of individuals in other countries or regions. The study sheds light on individuals' motivations and decision-making processes using public Wi-Fi networks, where convenience and cost are primary drivers, while security concerns also influence their choices. Therefore, individuals must be aware of the potential risks linked to public Wi-Fi and take necessary precautions to safeguard their personal information while using such networks.

7.1 Future Work

Future research could expand on the current study's findings by exploring the various factors, impacts, and motivations that cause people to use public Wi-Fi networks. Researchers can use quantitative survey methodology to investigate these reasons over a larger sample and more diversified demography. This method would provide an evaluation of the generalizability of the variables found in the study.

Using a survey-based approach, researchers can gather data from a broader range of participants, facilitating a more comprehension of the rationales for the risky behaviour of using public Wi-Fi. This method would entail designing a structured questionnaire that incorporates questions pertaining to motivations, fears, and patterns of public Wi-Fi use.

Overall, conducting a quantitative survey study represents a valuable avenue for future research endeavours aimed at further investigating the reasons, factors, and motivations behind public Wi-Fi usage. Such an approach would enhance our understanding of these variables within a broader

population, ultimately contributing to the development of targeted interventions and policies designed to bolster the security and privacy of individuals accessing public Wi-Fi networks.

References

Ahadi, S. A. A., Rakesh, N., & Varshney, S. (2020). Overview on Public Wi-Fi Security Threat Evil Twin Attack Detection. *Proceedings of IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation, ICATMRI 2020*. https://doi.org/10.1109/ICATMRI51801.2020.9398377

Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Qbea'H, M., & Alrabaee, S. (2020). Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux. *Proceedings - 2020 12th Annual Undergraduate Research Conference on Applied Computing, URC 2020*. https://doi.org/10.1109/URC49805.2020.9099187

Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, *3*(1). https://doi.org/10.5430/elr.v3n1p39

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). Thesis projects: A guide for students in computer science and information systems: Second edition. In *Thesis Projects: A Guide for Students in Computer Science and Information Systems: Second Edition*. https://doi.org/10.1007/978-1-84800-009-4

Braun, V., & Clarke, V. (2006). Qualitative Research in Psychology Using thematic analysis in psychology Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2).

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers and Security*, *88*. https://doi.org/10.1016/j.cose.2019.101647

Chen, T., Kong, D., & Hong, Y. (2021). Development and Implementation of Anti Phishing Wi-Fi and Information Security Protection APP based on Android. *IOP Conference Series: Earth and Environmental Science*, *1802*(3). https://doi.org/10.1088/1742-6596/1802/3/032109

Cheng, N., Oscar Wang, X., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013). Characterizing privacy leakage of public WiFi networks for users on travel. *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2013.6567086

Choi, H. S., Carpenter, D., & Ko, M. S. (2022). Risk Taking Behaviors Using Public Wi-Fi™. *Information Systems Frontiers*, *24*(3). https://doi.org/10.1007/s10796-021-10119-7

Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010). The Wi-Fi privacy ticker: Improving awareness & control of personal information exposure on Wi-Fi. *UbiComp'10 - Proceedings of the 2010 ACM Conference on Ubiquitous Computing*. https://doi.org/10.1145/1864349.1864398

Fang, Z., Fu, B., Qin, Z., Zhang, F., & Zhang, D. (2020). PrivateBus: Privacy identification and protection in large-scale bus wifi systems. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *4*(1). https://doi.org/10.1145/3380990

Griffee, D. (2005). Research tips: Interview data collection. *Journal of Developmental Education*.

Hadi, M. A., & José Closs, S. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38*(3). https://doi.org/10.1007/s11096-015-0237-6

Hampton, K. N., & Gupta, N. (2008). Community and social interaction in the wireless city: Wi-fi use in public and semi-public spaces. *New Media and Society*, *10*(6). https://doi.org/10.1177/1461444808096247

Hossain, I., Hasan, M. M., Faisal Hasan, S., & Karim, M. R. (2019). A study of security awareness in Dhaka city using a portable WiFi pentesting device. *ICIET 2019 - 2nd International Conference on Innovation in Engineering and Technology*. https://doi.org/10.1109/ICIET48527.2019.9290589

Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Fraser, D. S., & Jay, T. (2008). Measuring Trust in Wi-Fi hotspots. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/1357054.1357084

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). When i am on wi-fi, i am fearless: Privacy concerns & practices in everyday wi-fi use. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/1518701.1519004

Lambert, A., McQuire, S., & Papastergiardis, N. (2014). Public Wi-Fi: Space, sociality and the social good. *Australian Journal of Telecommunications and the Digital Economy*, *2*(3). https://doi.org/10.7790/ajtde.v2n3.45

Li, M., Meng, Y., Liu, J., Zhu, H., Liang, X., Liu, Y., & Ruan, N. (2016). When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-October-2016*. https://doi.org/10.1145/2976749.2978397

Lincoln, Y., & Guba, E. G. (1988). Criteria for Assessing Naturalistic Inquiries as Reports. *American Educational Research Association*.

Lotfy, A. Y., Zaki, A. M., Abd-El-Hafeez, T., & Mahmoud, T. M. (2021). *Privacy Issues of Public Wi-Fi Networks*. https://doi.org/10.1007/978-3-030-76346-6_58

Maguire, M., & Delahunt, B. (2017). Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars. All Ireland Journal of Teaching and Learning in Higher Education. *All Ireland Journal of Teaching and Learning in Higher Education n (AISHE-J)*, *8*(3).

Maimon, D., Howell, C. J., Jacques, S., & Perkins, R. C. (2022). Situational awareness and public Wi-Fi users' self-protective behaviors. *Security Journal*, *35*(1). https://doi.org/10.1057/s41284-020-00270-2

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. In *Evidence-Based Nursing* (Vol. 18, Issue 2). https://doi.org/10.1136/eb-2015-102054

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*. https://doi.org/10.1109/ACCESS.2018.2809614

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. In *Qualitative Research in Accounting and Management* (Vol. 8, Issue 3). https://doi.org/10.1108/11766091111162070

Schober, M. F. (2018). The future of face-to-face interviewing. *Quality Assurance in Education*, *26*(2). https://doi.org/10.1108/QAE-06-2017-0033

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1). https://doi.org/10.1016/j.infoandorg.2010.11.001

Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016). An empirical study of WIFI security and performance in Morocco-wardriving in Rabat. *Proceedings of 2016 International Conference on Electrical and Information Technologies, ICEIT 2016*. https://doi.org/10.1109/EITech.2016.7519621

Shelton, C. L., Smith, A. F., & Mort, M. (2014). Opening up the black box: An introduction to qualitative research methods in anaesthesia. In *Anaesthesia* (Vol. 69, Issue 3). https://doi.org/10.1111/anae.12517

Skinner, D., Tagg, C., & Holloway, J. (2000). Managers and Research: The Pros and Cons of Qualitative Approaches. *Management Learning*, *31*(2). https://doi.org/10.1177/1350507600312002

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 2018. https://doi.org/10.1109/PST.2018.8514208

Sombatruang, N., Onwuzurike, L., Sasse, M. A., & Baddeley, M. (2019). Factors influencing users to use unsecured wi-fi networks: Evidence in the wild. *WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks*. https://doi.org/10.1145/3317549.3323412

Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions. *ACM International Conference Proceeding Series*, *Part F130652*. https://doi.org/10.1145/3046055.3046058

Sudar, C., Arjun, S. K., & Deepthi, L. R. (2017). Time-based one-time password for Wi-Fi authentication and security. *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, *2017-January*. https://doi.org/10.1109/ICACCI.2017.8126007

Swanson, C., Urner, R., & Lank, E. (2010). Naïve security in a Wi-Fi world. *IFIP Advances in Information and Communication Technology*, *321*. https://doi.org/10.1007/978-3-642-13446-3_3

Trewin, S., Swart, C., Koved, L., & Singh, K. (2016). Perceptions of Risk in Mobile Transaction. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*. https://doi.org/10.1109/SPW.2016.37

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud and Security*, *2016*(1). https://doi.org/10.1016/S1361-3723(16)30009-4

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in software engineering. In *Experimentation in Software Engineering* (Vol. 9783642290442). https://doi.org/10.1007/978-3-642-29044-2

Appendix A - Questions of interview

1. Can you tell me your age and education level?
2. Can you describe why you use public Wi-Fi?
3. Which activities and applications do you use on open public Wi-Fi?
4. Can you describe your experience using public wireless networks?
5. Which factors drive you to use public Wi-Fi?
6. How often do you use public Wi-Fi?
7. What benefits can you get when you use public Wi-Fi? Can you give me an example?
8. How about other benefits such as being connected all the time, saving mobile data, or because most public Wi-Fi is free, so you can save money?
9. Do you know anything about the risks of connecting to open public Wi-Fi??
10. How much trust do you have in the security of public wireless networks?
11. What do you know about these risks, “fake access point”, “man-in-the-middle”, and “phishing”?
12. In addition, there are also security risks while using public Wi-Fi, such as leaks of personal information and personal information aggregation; what do you know about them?
13. Do you think financial details such as card numbers and account numbers can be leaked on public Wi-Fi?
    - 13.1. If yes, can you explain how?
    - 13.2. If no, can you explain why you do not think so?
14. How do you protect your personal information when using open public Wi-Fi?
15. At the end of our discussion, will you use public Wi-Fi without protection?
16. Is there anything you want to share or find relevant that I have not asked you?