STUDY ON DATA SECURITY AWARENESS IN MOBILE PHONE USAGE AMONG UNIVERSITY STUDENT USING STATISTICAL ANALYSIS

NURUL IZZATI SYAZWANI BINTI RASHIDI

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: STUDY ON DATA SECURITY AWARENESS IN MOBILE PHONE USAGE AMONG UNIVERSITY STUDENT USING STATISTICAL ANALYSIS

SESI PENGAJIAN: 2022 / 2023

Saya: NURUL IZZATI SYAZWANI BINTI RASHIDI

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

_____ SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____ TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
___✓___ TIDAK TERHAD	

DR. ZAHEERA ZAINAL ABIDIN
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi (FTMK)
Universiti Teknikal Malaysia Melaka (UTeM)

(TANDATANGAN PELAJAR)

Alamat tetap: NO 148, TAMAN MANJUNG POINT SEKSYEN 2, 32040 SERI MANJUNG, PERAK.

Tarikh: 15/9/2023

(TANDATANGAN PENYELIA)

DR. ZAHEERA BINTI ZAINAL ABIDIN

Tarikh: 20/9/2023

STUDY ON DATA SECURITY AWARENESS IN MOBILE PHONE USAGE AMONG UNIVERSITY STUDENT USING STATISTICAL ANALYSIS

NURUL IZZATI SYAZWANI BINTI RASHIDI

This report is submitted in partial fulfilment of the requirements for the Bachelor of [Computer Science (Cyber Security)] with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

STUDY ON DATA SECURITY AWARENESS IN MOBILE PHONE USAGE AMONG UNIVERSITY STUDENT USING STATISTICAL ANALYSIS

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date: 15/9/2023

(NURUL IZZATI SYAZWANI BINTI RASHIDI)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of [Computer Science (Cyber Security)] with Honours.

DR. ZAHEERA ZAINAL ABIDIN
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi (FTMK)
Universiti Teknikal Malaysia Melaka (UTeM)

SUPERVISOR : _____ Date: 20/9/2023

(DR. ZAHEERA BINTI ZAINAL ABIDIN)

DEDICATION

To my beloved family and friends, who have supported me during this entire study effort, I would want to dedicate it. Through the entire process, their constant support and inspiration have been crucial. Their kindness and compassion laid the groundwork for this effort, and I am eternally thankful for them.

My supervisor, Dr. Zaheera binti Zainal Abidin, is also the recipient of my sincere gratitude. She has been an amazing mentor, helping me along the way and offering insightful criticism that has helped to develop this study. Her dedication to quality and her confidence in my abilities have been essential to my success.

I'd want to express my gratitude to the study's participants for agreeing to take part. Their assistance has been priceless and has really aided my understanding of Data Security in Mobile Phone Among University Student.

Finally, I would like to express my gratitude to all of the mentors, colleagues, and other individuals who have helped and inspired me throughout this journey. Reaching this accomplishment has been made possible in large part by your support and belief in my work.

This study effort is a means of acknowledging and expressing gratitude to all persons who have had a significant impact on my life, including those who were previously mentioned as well as the numerous others. I appreciate your contributions on this adventure.

ACKNOWLEDGEMENT

I am incredibly grateful for the completion of this final year project report, all praises to Allah with His Permission and Grace. I would like to take this opportunity to thank the following people, without whom this accomplishment would not have been possible.

I must first express my gratitude to my supervisor, Dr. Zaheera binti Zainal Abidin, for her crucial direction, counsel, encouragement, and encouraging remarks throughout the entire process of finishing this project. Her knowledge and constant support were crucial to the accomplishment of this report.

For their constant encouragement and steadfast support throughout my endeavour, Mr. Rashidi bin Zainal Abidin and Mrs. Nasariah binti Mat Nasib have my undying gratitude. My endurance and commitment have been motivated by their love, compassion, and encouragement.

I also want to express my sincere gratitude to Muhamad Afif bin Nor Hashim, Nurin Izz Natasha binti Hassan, Nur Izzati Husna binti Affrendi, and Nur Amalya binti Mohd Maheran, who are also among my dear friends. Your ongoing reassurance, care, love, and encouragement have been instrumental in giving me the drive I needed to finish this project. I sincerely appreciate you being a source of inspiration and encouragement in my life.

I want to express my sincere appreciation to Allah and the people mentioned above. The extent of my gratitude for your unflagging love, support, and inspiration is beyond words. May Allah grant you all a bountiful blessing for your efforts to my accomplishment.

ABSTRACT

Mobile phone and mobile devices are common tools used by faculty and students on college campuses in various universities. The usage of mobile devices in education is increasing due to quick and easy access for learning materials and submissions of assignments. Students in higher education brought more than one mobile device and mobile phone to campus for communication and learning. However, the ownership of mobile phone and mobile devices change based on the student's dependency on them. Moreover, data security in mobile phone and mobile devices usage have become a major concern since a lot of cyber-crimes have been reported such as scam callers, money lost in the account and social-engineering. In fact, the malware virus is the most cyber-attack that is launched to mobile devices. The motivation for this study is to investigate the significant of data security awareness among student of Universiti Teknikal Malaysia Melaka (UTeM). Therefore, this research attempts to explain the relationship between data security awareness and university's students in mobile phone usage. There are 8 faculties involved in this study and the data has been collected using social media platform of 258 participants. The 258 survey questionnaires received and analyzed using SPSS software. Based on the ANOVA analysis, students encompassing both IT-literate and non-IT-literate, it is crucial to note that despite their varying levels of technical expertise, all respondents share a common educational background rooted in a technical or IT-centric environment.

ABSTRAK

Telefon mudah alih dan peranti mudah alih adalah alat yang biasa digunakan oleh fakulti dan pelajar di kampus kolej di pelbagai universiti. Penggunaan peranti mudah alih dalam pendidikan semakin meningkat disebabkan oleh akses yang cepat dan mudah untuk bahan pembelajaran dan penyerahan tugasan. Pelajar di pendidikan tinggi membawa lebih daripada satu peranti mudah alih dan telefon bimbit ke kampus untuk komunikasi dan pembelajaran. Walau bagaimanapun, pemilikan telefon mudah alih dan peranti mudah alih berubah berdasarkan pergantungan pelajar terhadapnya. Selain itu, keselamatan data dalam penggunaan telefon mudah alih dan peranti mudah alih telah menjadi kebimbangan utama kerana banyak jenayah siber telah dilaporkan seperti pemanggil penipuan, wang hilang dalam akaun dan kejuruteraan sosial. Malah, virus perisian hasad adalah serangan siber paling banyak yang dilancarkan ke peranti mudah alih. Motivasi kajian ini adalah untuk mengkaji signifikan kesedaran keselamatan data dalam kalangan pelajar Universiti Teknikal Malaysia Melaka (UTeM). Oleh itu, kajian ini cuba menjelaskan hubungan antara kesedaran keselamatan data dan pelajar universiti dalam penggunaan telefon bimbit. Terdapat 8 fakulti yang terlibat dalam kajian ini dan data telah dikumpul menggunakan platform media sosial seramai 258 orang peserta. 258 soal selidik tinjauan diterima dan dianalisis menggunakan perisian SPSS. Berdasarkan analisis ANOVA, pelajar yang merangkumi kedua-dua celik IT dan bukan celik IT, adalah penting untuk ambil perhatian bahawa walaupun tahap kepakaran teknikal mereka berbeza-beza, semua responden berkongsi latar belakang pendidikan yang sama yang berakar umbi dalam persekitaran teknikal atau tertumpu IT.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

IT – Information Technology

VPN – Virtual Private Network

EMM – Enterprise Mobility Management

GPS – Geo Location Services

NLP – Natural Language Processing

AI – Artificial Intelligence

PU – Perceived Usefulness

PEOU – Perceive Ease of Use

TOE – Technology Organisation Environment

UTAUT – Unified Theory of Acceptance and Adoption of Technology

CFC – Consideration of Future Consequences

UTeM – Universiti Teknikal Malaysia Melaka

ANOVA – Analysis of Variance

SPSS - Statistical Package for Social Sciences

FKE - Fakulti Kejuruteraan Eletrik

FKP - Fakulti Kejuruteraan Pembuatan

FKEKK - Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer

FTMK - Fakulti Teknologi Maklumat dan Komunikasi

FPTT - Fakulti Pengurusan Teknologi dan Teknoushawan

FKM - Fakulti Kejuruteraan Mekanikal

FTKEE - Fakulti Teknologi Kejuruteraan Eletrik Eletronik

FTKMP - Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan

UVA – User Vulnerability Awareness

UTA – User Threat Awareness

USP – User Security Practices

SUPD – Secondary Utilisation of Personal Data

PR – Perceived Risk

C – Competence

T - Trust

CHAPTER 1: INTRODUCTION

1.1 Project Background

In today's digital era, mobile devices have emerged as one of the most popular and ubiquitous gadgets, granting users unprecedented access to the vast realm of the internet, empowering them to effortlessly download apps, explore websites, stay connected through emails and social media, and indulge in the seamless streaming of captivating videos. Cellular networks and Wi-Fi connections are just two of the technologies used by mobile phones to offer internet access. Mobile phones can access the internet utilising the network infrastructure supplied by telecommunications firms through cellular networks, such as 4G or 5G. This enables users to access the internet wherever there is cellular coverage. In addition, mobile devices have witnessed an exponential rise in popularity, captivating a vast multi-level user, such as tech-savvy professionals, students, government, private sector and customers.

One of the largest demographics of smartphone users is university students. Teenagers utilize their smartphones for a range of academic and extracurricular activities, such as research, communication, and enjoyment. On their phone, they keep all of their private information, including all of their sensitive information. University students exhibit a degree of unawareness when it comes to crucial aspects of data security. This is because they are unaware or did not know about certain aspects of data security. However, this project will analyse the level of awareness of university student regarding to data security in mobile phone.

The primary objective of mobile device security is to prevent unauthorised users from entering the corporate network (VMWare, 2022). Furthermore, malicious mobile apps, phishing scams, data leaks, malware, and insecure Wi-Fi networks are a few potential hazards to smartphones (VMWare, 2022). In fact, the main way to secure mobile devices is through encryption, which encrypts user data on a device using encryption (White, T. 2020) keys but most of university student did not familiar with this term.

Therefore, this analysis focuses more on how much university student know about the mobile device security and find out how much they understand about the mobile security vulnerabilities as well as user education and awareness.

1.2 Problem Statement (PS)

Data security has become a top priority because to the quick development of mobile phone technology and the growing reliance on mobile devices for communication, productivity, and access to sensitive information. A sizable portion of mobile phone users, in particular university students, rely extensively on their devices for a variety of tasks, including contact with friends and family, accessing internet resources, and participating in academic activities. But little is known about how well-aware university students are of data security issues and how they protect sensitive and private data on their phones.

PS	Problem Statement
PS_1	University students unaware of the potential consequences of mobile security breaches, such as identity theft, financial lost and damages to their reputation.
PS_2	University students not taking an adequate precaution to protect themselves from mobile security threats such as malware and phishing.
PS_3	The level of understanding for university students is not much as an IT expert for them to know the threats.

Table 1.1 Summary of Problem Statement

1.3 Project Question (PQ)

This research analysis is to identify the mobile data security awareness among university students. This study focused on the following analysis question:

PS	PQ	Project Question
PS_1	PQ_1	What is the level of awareness among university students regarding the potential consequences of mobile security breaches?
PS_2	PQ_2	How knowledgeable are university students about the specific risks associated with malware and phishing attacks on mobile devices?
PS_3	PQ_3	Are there any differences in the level of understanding and awareness of mobile security threats among university students from different academic disciplines or educational backgrounds?

Table 1.2 Summary of Project Question

1.4 Project Objective

Based on project question above, Table 1.3 will show the summary of the project objectives based on each project question:

PS	PQ	PO	Project Objective
PS_1	PQ_1	PO_1	To study the level of awareness of university students.
PS_2	PQ_2	PO_2	To analyze the understanding of security on mobile phone among university students.
PS_3	PQ_3	PO_3	To compare the level of awareness among IT students and non-IT students.

Table 1.3 Summary of Project Objective

- **PO_1: To study the level of awareness of university students.**

  By studying the level of awareness of university student, we can determine how much the security awareness of data security affect them.

- **PO_2: To analyse the understanding of security on mobile phone among university students.**

  By analysing the understanding of university student in security in mobile phone, we can assess students' understanding of security practices and measures if they protect their mobile phones.

- **PO_3: To compare the level of awareness among IT students and non-IT students.**

  By designing a questionnaire and asked for university student to fill it to differentiate the level of awareness between IT students and non-IT students' comprehension of the numerous mobile-related information security concerns and do the statistical analysis to analyse their understanding of data security in mobile phone.

1.5 Possible Hypothesis

1. H0: There is no difference in Level of Awareness among University Students between faculty groups Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE).

   H1: There is difference in Level of Awareness among University Students for the faculty groups Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE).

2. H0: There is no difference in Vulnerabilities Behaviour Assessment between faculty groups Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE).

   H1: There is difference in Vulnerabilities Behaviour Assessment between faculty groups Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE).

1.6 Project Scope

The scope of this project will focus on some issues regarding the objective of the project stated earlier. The scopes are shown as below:

1. Questionnaire or Survey Design where I will make a question based on security threats, that cover all the topic of cyber security and university student will fill in the form.
2. Analysis of the collected data from the questionnaire and used statistical analysis to summarize the findings by using sampling method.

1.7 Project Contribution

The finding of this study is to analyse about the data security awareness in mobile phone usage among university student. Therefore, it will improve the knowledge of security threats among them.

1.8 Report Organization

CHAPTER 1: Introduction

This chapter will be discussed about the project background, problem statement, project question, project objective, project scope, project contribution and report organization.

CHAPTER 2: Literature Review

This chapter will focus more on the past research and reading. The vulnerabilities of mobile phone are stated based on findings. these includes, the introduction and previous work to explain about this study.

CHAPTER 3: Project Methodology

This chapter will describe the project process and the method used to analyses the data security on mobile phone among university student. The framework of this methodology is being explained in detail. In addition, the action plan of project milestone also was explained in this chapter.

CHAPTER 4: Design

The problem analysis and software requirements will be covered in this chapter. The software that used in this project is explained.

CHAPTER 5: Implementation

This chapter will describe the method to implement the data in order to carry out statistical analysis of all the findings.

CHAPTER 6: Testing and Analysis

This chapter describe the analysis result and analysis. A graphical result will make based on the data collected.

CHAPTER 7: Conclusion

This chapter will summarize all chapters as a conclusion. The chapter also discusses the flaws and strengths of analysis study.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Smartphone security comprises a variety of mechanisms and features designed to safeguard the device, safeguard sensitive data, and ensure user privacy, including strong operating system security, device authentication systems, and data encryption techniques. One of the reasons why mobile phone security is crucial is to protect information, which entails making sure that its accessibility, confidentiality, and integrity are not compromised (Ngoqo, B. and Flowerday, S.V., 2015). In fact, there are many technologies that can help securing our data privacy such as encryption, authentication, tracking software, remote wipes, antivirus and Virtual Private Networks (VPN) which is the most popular technologies that people used in their mobile phones.

Sensitive data stored in mobile phone must be protected, and device encryption is a key component of that protection (Bibeau, R., 2011). Encryption is a component of the control environment used by the organization to safeguard the information and applications on mobile devices from dangers and threat (White, T., 2020). Besides, authentication activate by the implementation of passwords, unlock patterns, biometrics, and signature cards as necessary (White, T., 2020). Other technologies that can secure data in mobile phone is Virtual Private Network (VPN. Users can securely connect to a head-end site, typically a main office, from a distance using a virtual private network (VPN) to view files, share printers, access email, and perform other network-related functions (Bibeau, R., 2011). Besides, studies have shown that virtual private network (VPN) technologies have been widely used by organization to secure data in mobile phone.

Virtual private networks (VPNs) are constructed as an overlay on the public infrastructure of one or more providers to enable access between a specific range of devices (Alshalan, A., Pisharody, S. and Huang, D., 2016) A virtual private network (VPN) is basically a secured tunnel that acts as a virtual leased line over a network that is shared by many people (Alshalan, A., Pisharody, S. and Huang, D., 2016). Even though VPN has been used by a wide user, it still has the advantages and disadvantages based on their criteria. Figure 2.1.1 shows the classification criteria of mobile VPN including their advantages and disadvantages.

Classification Criteria	Class	Advantages	Disadvantages
Tunnel Establishment	Voluntary	- Simple Client/Server model. - No need for intermediary devices; thus, no compromise to the end-to-end encryption, and no SLA's required.	- Need for NATing or IPv6. - Packets cannot be inspected for QoS. - Requires encapsulation over lossy wireless links.
	Compulsory	- No encapsulation needed between MN and service provider. - No VPN support needed in MN. - Ability to provide QoS.	- Data is partially transmitted over insecure channel. - Intermediary devices have to be trusted. - Need for SLA which may not be suitable for low-budget organizations.
	Chained	- Eliminates the need for insecure channel between the service provider and the MN. - Allows for QoS and traffic shaping.	- Intermediary devices have to be trusted. - Need for SLA.
Layer of Mobility	Network Layer Mobility	- Solves the problem of IP address change in network layer transparently from the above layers of TCP/IP stack.	- Transport layer protocols may time out if the recovery of the IP layer is not done in a timely manner especially during long gaps in network coverage.
	Application Layer Mobility	- Supports mobility by creating session binding above the IP layer so it is not affected by IP address changes.	- More overhead on the mobile VPN to keep track of the session information.
Security Protocol	IPsec	- better performance than TLS.	- Requires establishing the security association from scratch unless MOBIKE is used.
	TLS and its variants	- NAT-friendly since they do not include IP addresses is part of the security association.	- Performance is not as good as IPsec. - Does not authenticate the sender's IP address.

Figure 2.1.1 General Classification Criteria for Mobile VPN (Alshalan, A., Pisharody, S. and Huang, D., 2016).

The variety of technologies available to secure mobile phones may not be fully understood by a sizable fraction of users. They are only familiar with the terms "VPN" and "Antivirus". Therefore, to investigate the level of knowledge of the beginners and expert, questionnaire technique will be used to measure the level of awareness of the user regarding mobile phone security. For each question, frequency tests were run to see how frequently participants gave a given response. The frequency with which a population sample chooses a particular response reflects how the entire population feels about the question (McGovern Cole, E. L., 2019).

Overall, this review of the literature intends to provide a thorough overview of data security awareness in mobile phone usage among university students, highlighting the most important conclusions and suggestions from past studies and recommending areas for further research.

2.2 Vulnerabilities of a mobile phone

2.2.1 Bluetooth

Bluetooth is a wireless communication technology used for transmitting data over short distances. Without the use of cables or wires, it enables the connection and data sharing of devices like speakers, computers, and smartphones. Radio waves are used by Bluetooth technology to transmit data between devices that are near to one another, usually within a range of up to 10 meters (33 feet). There are several attacks that target an open Bluetooth connection, such as Bluejacking, Bluesnarfing, and Bluebugging (McGovern Cole, 2019). Same as other attacks, cybercriminals may carry out these attacks with the goal of stealing financial information, personal information, or other private data from a victim's device. Hacker gains access through the Bluetooth in the Bluejacking event which the goals is to send an unsolicited message to other Bluetooth enabled devices (McGovern Cole, 2019).

Other than that, the Bluesnarfing was proposed by Adam Laurie in 2003 while he was evaluating the security features and capability of Bluetooth devices. It enables unauthorized access to data stored on devices, usually portable ones like computers, mobile phones, and PDAs (Liao M, 2012). It also requires that the phones Bluetooth is on, which are most of the phone has default setting on their phone. Thus, while "invisible" mode or automatic concealed mode will provide some security, Bluetooth must be off entirely for the device to be fully protected (Liao M, 2012).

Next, Bluebugging attack is considered as the most dangerous Bluetooth-based attack. Herfurt and Laurie successfully discovered and demonstrated the attack using 50 phones during CeBit 2004 (Liao M, 2012). In this attack, the device that attacker control will be paired with the targeted device and the attacker will install a backdoor on the targeted device. It automatically provides the attacker access to the device without their knowledge, allowing them to read any saved texts, send text messages, access contacts, make phone calls, set call forwarding, and connect to the Internet (McGovern Cole, E. L. ,2019). A backdoor is a security flaw or a deliberate access point that can be used to go beyond a device's standard security safeguards. As a result, attackers may be able to use the device without authorization, obtain private data, or run harmful software.

In 2017, Blueborne was discovered which is it is the new attack that vector utilizing Bluetooth. It is based on its biological-like spread (McGovern Cole, E. L. ,2019). In order to take control of the device or steal sensitive data without the user's knowledge or agreement, the

assault takes advantage of Bluetooth protocol flaws. Attackers do not need to be close to the target device in order to conduct a BlueBorne assault remotely. Being able to target devices in public locations like airports, coffee shops, and libraries makes it extremely risky. When a device is infected with BlueBorne, the attacker has access to private data including contacts, images, and messages. They can even use the device to infect other adjacent devices. Figure 1 below illustrates how the BlueBorne can spread via airwaves (McGovern Cole, E. L. ,2019).

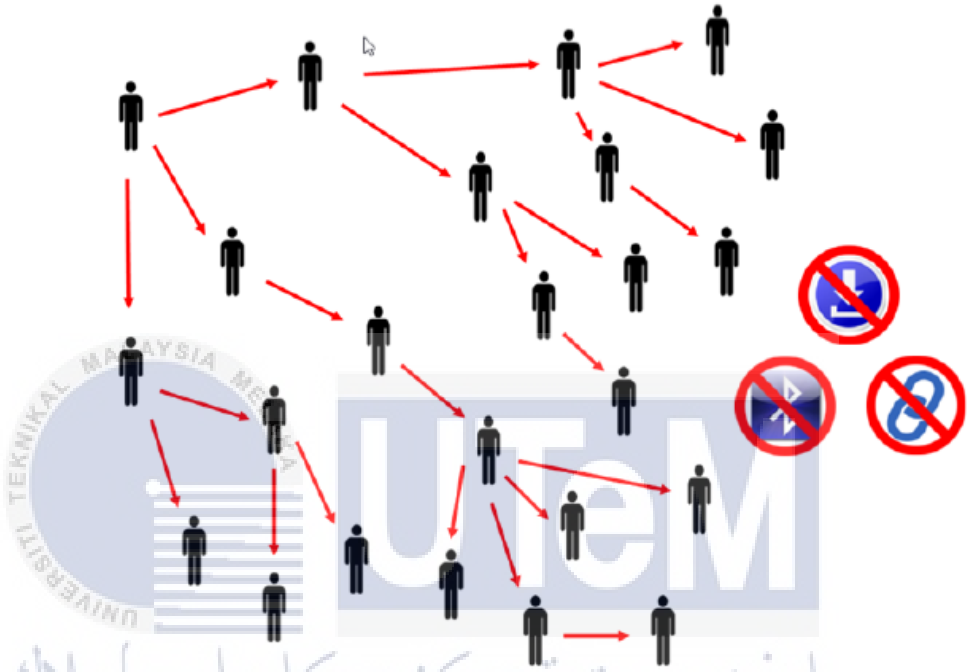

Figure 2.2.1.1 The Illustration of Blueborne attack (McGovern Cole, E. L. ,2019).

The owner of the device has no idea if their mobile phones got attacked (McGovern Cole, E. L. ,2019). Thus, mobile phones are a common target due to their lack of security given the information they store. Enterprise Mobility Management (EMM) tool MobileIron provides mobile security platforms to businesses (McGovern Cole, E. L. ,2019).

2.2.2 Data Vulnerabilities

All systems have technical and human faults, and sensitive information that may be transmitted without the user's explicit consent. Data leaking may happen purposefully, accidently, or maliciously. Mobile devices are more susceptible to malicious assaults and security issues when connected in a static, uninterrupted manner **(**White, T., 2020). Malware, phishing scams, and data breaches are just a few examples of the hazards that could be present.

Mobile phones are frequently used in a static, uninterrupted way, which means that they are connected to the internet for extended periods of time without being disconnected or restarted. This is one factor that makes mobile devices more vulnerable to these assaults. As a result, attackers may have more time to find flaws and use them to access the system without authorization or access the data on the device. In businesses, some of the misguided acts of displeased employees include disclosing information to the company's rival in an effort to cause harm or as payback. Employee noncompliance with contracts, regulations, and policies is another effect of security attacks **(**White, T., 2020). Due to the storage of personal information and login credentials on mobile devices, the privacy of the employees is also in danger **(**White, T., 2020).

Moreover, malware is swiftly developing into a worry for mobile devices (White, T., 2020). To harm or infiltrate mobile devices, malware is characterized as "worms, viruses, Trojans, bots, Spyware, logic bombs, and other harmful software" (White, T., 2020).

2.2.3 Geo Location Services (GPS)

Geo Location Services (GPS) is a phrase that describes the use of GPS technology to pinpoint the exact location of a person or an object. When there is an unimpeded line of sight to four or more GPS satellites, the satellite-based navigation system GPS may deliver precise location and time information everywhere on or near the Earth. While this is very useful to a user, it also can gather data about the user (McGovern Cole, E. L., 2019).

The cyber environment is replete with everything a cyber stalker needs, and it gives those actors who utilize the environment to pursue their target and learn more about their goals a very simple approach to locate them (McGovern Cole, E. L., 2019). For instance, if a device's GPS location is monitored without the user's knowledge or agreement, it may be used to compile sensitive data like the user's home address, workplace, daily schedule, and other private details. Then, this information might be utilised maliciously for things like identity theft, stalking, or physical violence. Another example in real life is GPS was utilised to track

the victim in a murder case heard in Kansas City, Missouri, before the victim was shot (McGovern Cole, E. L., 2019). Lester Brown, the suspect, is accused of using a GPS tracking device that he secretly installed on the vehicle of a rival drug dealer (McGovern Cole, E. L., 2019). Affidavits submitted to the Western District of Missouri U.S. Attorney's Office state that the GPS was used to find Mr. Harris so that he might be killed (McGovern Cole, E. L., 2019).

One further thing to think about with GPS is that a corporation could be able to maintain tabs on its staff using business tools like a time clock system with geotagging or stamping by adding a location tag to data entry, a photo, or a video is known as geo stamping (McGovern Cole, E. L., 2019). The method of geo-stamping involves tagging various forms of digital content, such as images, movies, and other data entries, with location information. The longitude and latitude coordinates of the place where the item was made or recorded are frequently included in this metadata.

2.2.4 Digital Assistant

A software program known as a digital assistant, often referred to as a virtual assistant, can carry out different functions and services for consumers. Natural language processing (NLP) and artificial intelligence (AI) technologies are often used to power these assistants, enabling users to communicate with them via text messages or voice commands.

The practice of phone phreaking started in the late 1950s (McGovern Cole, E. L., 2019). Phone phreaking, which involves mimicking the tones that phone companies used to connect calls, involves breaking into hard-wired phone lines (McGovern Cole, E. L., 2019). The switching systems used by the phone provider were the source of the vulnerability. The switching systems of the period routed calls between various areas of the network using audible tones. However, The Dolphin Attack is the most recent iteration of sound-based phone hacking (McGovern Cole, E. L., 2019).

The Dolphin Attack is a sort of cyberattack that uses ultrasonic frequencies to send commands to voice-controlled gadgets like smartphones, smart speakers, and virtual assistants. Although noises over 20 kHz are inaudible to the adult human ear, a smartphone may detect and react to sounds in this range, allowing a hacker to control the device without the owner's awareness (McGovern Cole, E. L., 2019). The maximum separation between the transmitter and receiver is 175 cm, or slightly more than 5.5 ft (McGovern Cole, E. L., 2019).

In January 2019, Apple acknowledged the existence of the after receiving a report from the 14-year-old Fortnite player's mother, Michele, who also informed the news media (McGovern Cole, E. L., 2019). It happened when a Facetime request was made but not accepted or rejected, the bug allowed a caller to hear conversations happening around the iPhone (McGovern Cole, E. L., 2019).

2.3 Related Work/Previous Work

Mobile phone is a portable electronic device that combines the functionality of a regular telephone with cutting-edge features and capabilities. Recently, the use of mobile phones has increased significantly, especially among teenagers (Scott, S., 2006). In Japan, there were over 147 million mobile phone users worldwide by March 2015 (Inoue, A., Saito, M. and Iwashita, M., 2015). The shipments of mobile phones are anticipated to increase to nearly two billion by 2016 from the 2012 shipment record high of over one billion (Riola, P. A., 2014). While in Malaysia, around 87.61% of Malaysians are expected to have used a smartphone in 2020 and this number is expected to rise over time (Fook, C.Y. et al., 2022). This is because mobile phones' popularity is mostly attributed to their pervasiveness, which is caused by their compact size, sophisticated processing and communication capabilities, low cost, and capacity to run diverse third-party applications (Irwan, Asnar, Y. and Hendradjaya, B., 2015). All user's daily lives are now very reliant on their mobile phones.

In fact, the majority of mobile phone users are young adults in university (Riola, P. A., 2014). Besides, a lot of university students now consider having a phone essential (Ngoqo, B. and Flowerday, S.V., 2015). They can take use of a variety of advantages and conveniences that smartphones provide, which helps explain why they are so common and thought of as necessary. The major reasons why university students use mobile phone is because with the mobile devices linked to the Internet and they may learn whenever and wherever they want (Fook, C.Y. et al., 2022). From this, students can access a wide range of online learning tools, including educational websites, video tutorials, e-books, podcasts, and online courses, if they have internet access. With the help of these tools, learning can be flexible, allowing students to explore more topics at their own speed and go deeper into their areas of interest.

However, it makes them vulnerable to security risks that could lead to information loss (Ngoqo, B. and Flowerday, S.V., 2015). It is because university students are unaware regarding their data security in mobile phone. The usage of mobile technology by students has some security repercussions in terms of the users' privacy, integrity, and confidentiality (Shonola, S.A. and Joy, M.S., 2014). According to a study by Alzaza and Yaakub that was carried out in Malaysia, students had sufficient knowledge and high awareness of the usage of mobile technology for their educational needs, but it is not cover about the mobile phone security awareness (Shonola, S.A. and Joy, M.S., 2014). A previous study shown that 63% of female respondents and 78% of male respondents reported that their portable device had been stolen or lost, while 63% of female respondents and 78% of male respondents reported that friends

and colleague had used it without their permission. On the other hand, 25.4% of female respondents and 33.33% of male respondents mentioned denial of service, 74.6% of female respondents and 75.44% of male respondents said that virus or malware attacks are a concern to them (Shonola, S.A. and Joy, M.S., 2014). From this, some of university students are familiar with the security terms and some are not.

There are several key terms that will be mentioned in this study such as data security, security threat and mobile phone. Mobile data security is a constantly evolving topic where no detail should be ignored. According to the Minnesota Bureau of Criminal Apprehension and the Federal Bureau of Investigation of the United States of America, the use of mobile data security standards is required in contexts involving mobile public safety (Bibeau, R., 2011). Meanwhile, security threats are potential risks or hazards to the availability, confidentiality, and integrity of digital information and systems. These dangers may originate from a number of things, such as nefarious actors, software flaws, incorrect system setups, or social engineering strategies. A mobile phone is a mobile phone that has additional functionality, like internet access. It is frequently used in the same way as a mobile computer. Cellular, Bluetooth for close range transmissions, or wireless fidelity are the three types of wireless transmission available (Riola, P. A., 2014).

Therefore, understanding the level of data security knowledge among university students is crucial given the prevalence of mobile phone use in this demographic. Despite this, there hasn't been a lot of research on data security awareness, particularly among university students who use mobile phones especially in Malaysia.

2.4 Critical Review of Current Problem and Justification

The problem of this study was based on the awareness of data security in mobile phone among university students especially between IT and non-IT students and their concerns about the security threats in their mobile phone. This section will explain about four (4) past research paper.

2.4.1 Framework

1. **TAM- TOE Framework (An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment) written by Elizabeth L. McGovern Cole.**

In this research paper, Encyclopaedia Britannica defines technology as "the application of scientific knowledge to the practical aims of human life" or, as it is frequently put, "to change and manipulation of the human environment," and the researcher decided that the TAM-TOE framework was a good fit for this definition (McGovern Cole, E. L., 2019). The security procedures for mobile phones fall under the technology category and can be incorporated in the TAM-TOE framework for security adoption since computer science and the software created for computers are both regarded to be technologies (McGovern Cole, E. L., 2019).

Firstly, The Technology Acceptance Model (TAM), created in 1989 by Fred D. Davis, has gained popularity as a method for gauging a user's receptivity to new information systems and technologies. According to Fred Davis's explanation, a technology's acceptability is influenced by its perceived usefulness (PU) and perceived ease of use (PEOU) (Davis, 1989). In addition to the PU and PEOU, the behavioural intent to use, which is the acceptance of the technology, is another aspect in user acceptance (McGovern Cole, E. L., 2019). TAM framework is shown as in figure 2.4.1 below.

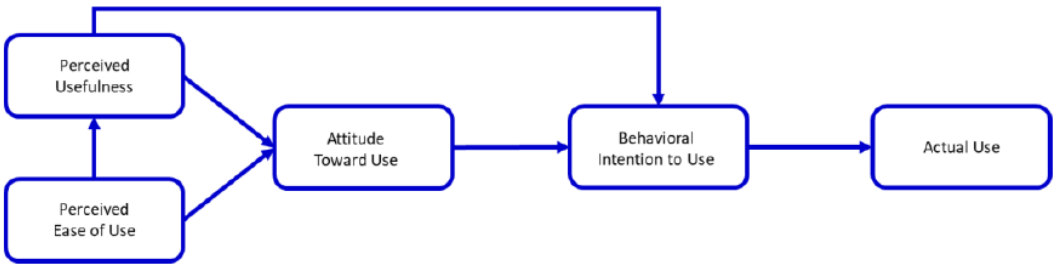

Figure 2.4.1.1 TAM Framework

(McGovern Cole, E. L., 2019).

Meanwhile, Rocco DePietro, EdithWiarda, and Mitchell Fleischer created the TOE Framework in 1990 (McGovern Cole, E. L., 2019). TOE represents "Technology Organization Environment Framework". The TOE Framework, as shown in Figure 2.4.2 below, illustrates the connection between the adoption of innovations and the environment, technology, and organization (McGovern Cole, E. L., 2019).

Three characteristics of a firm's context are identified by TOE as having an impact on a technical innovation's adoption and implementation:

a) The technical environment, including internal and external technology pertinent to the business.
b) The organizational context - descriptive information about the organization, including business size and scope, managerial structure, and internal resources
c) The environment in which a company operates, including its market, rivals, and interactions with the government

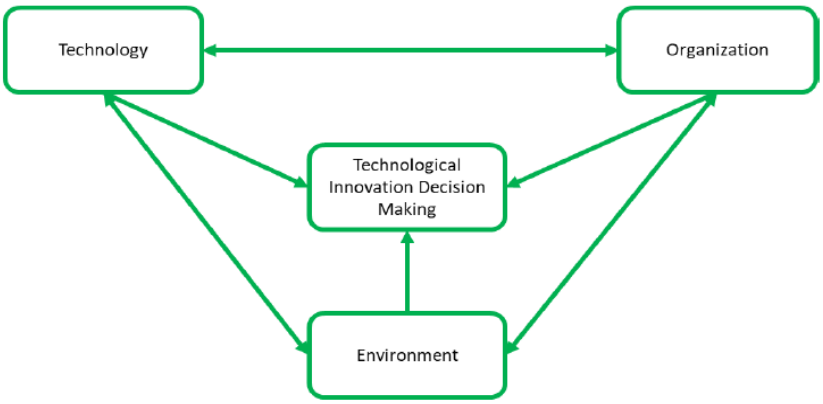

Figure 2.4.1.2 TOE Framework

(McGovern Cole, E. L., 2019).

From these two theories, Combining the TAM theory with TOE framework will increase the predictive potential of the new theory, according to Gangwar, Date, and Ramaswamy (2015). The user's perception of the system's usability and simplicity of use will be influenced by the external factors of the technological and organisational setting. The adoption intent will result from the PU and PEOU. The adoption intentions of users will also be influenced by the environmental situation (Gungwar et al., 2015). Below is the figure that shows the combination of TAM and TOE framework theory.

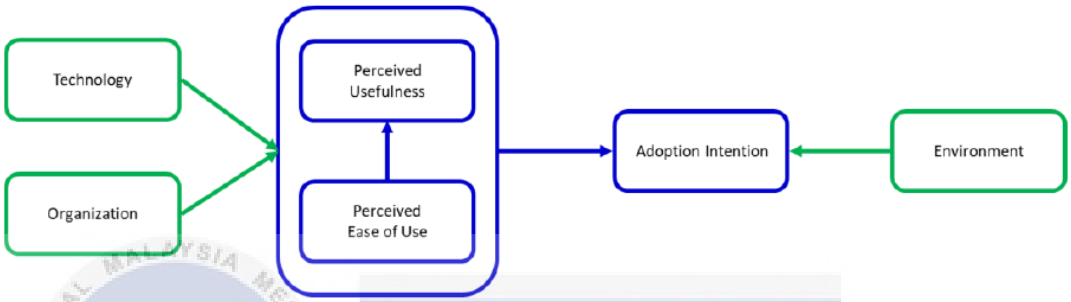

Figure 2.4.1.3 TAM-TOE Framework
(McGovern Cole, E. L., 2019).

The TAM-TOE Framework is suited for this study because, according to Gangwar et al.'s findings, users already perceive the usefulness and usability of their smartphone but may not have done so for the application of security measures. This is suitable if this study be handled among the university students.

2. **Unified Theory of Acceptance and Adoption of Technology (UTAUT) (Smartphone Security: A Quantitative Analysis of Security Usage and Outcomes) written by Barron Winters.**

In this research paper, this study used the Unified Theory of Acceptance and Use of Technology (UTAUT) to examine the persuasive reasons influencing users' employment of security measures when using their smartphones. According to the UTAUT, performance expectations, effort expectations, and social influence are the three main factors that determine developmental meaning (Afonso, Carlos, José Roldán, Manuel J. Sánchez-Franco, & Gonzalez, 2012).

Additionally, UTAUT was utilized as the baseline model for this investigation and enhanced to account for the two variables of security awareness and utilization

(Chen, Zhang, Hu, Taleb, & Sheng, 2015). However, there are numerous theories to consider when it comes to the acceptance of use in relation to technology. In the study of technology adoption, the UTAUT and the technology acceptance model (TAM) have both been extensively used and quoted hundreds of times (Venkatesh et al., 2012). Nevertheless, this research study was based on UTAUT as mentioned before.

The UTAUT is divided into four primary constructs which are social influence, performance expectancy, effort expectancy, and enabling variables (usefulness) (Attuquayefio & Addo, 2014). Figure 2.4.1.4 below shows the conceptual framework of Winter's research study.

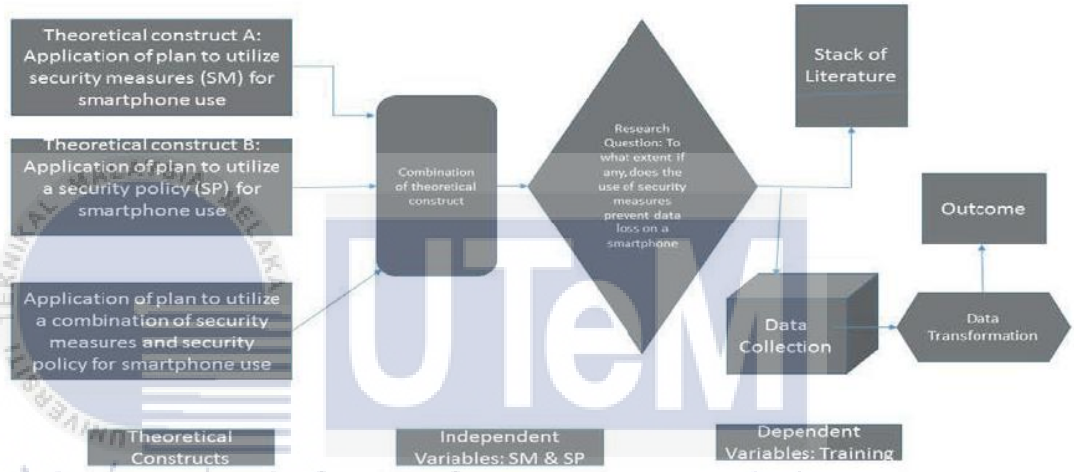

Figure 2.4.1.4 Winter's Conceptual Framework

3. Electronic Survey Form (Security and Privacy Awareness of Smartphone Users in Indonesia) written by M Amin.

M Amin chose electronic survey form. This survey aims to gauge smartphone users' level of security and privacy awareness. An online user survey is used to gather data (Amin, M. et al., 2021). He created a questionnaire for this study using Google Form, and after that, he used the crowdsourcing technique to gather data. He sends links to questionnaires to smartphone users in Indonesia who are at least 12 years old via Facebook, WhatsApp, Telegram, and SMS.

A questionnaire was created by him using a modified approach design. The methods currently in use give rise to many concerns about privacy and security of smartphone. Its only required six most significant questions. Additionally, he creates straightforward, easy-to-understand question formulations. In numerous areas, he changed the approaches that were already in use.

4. **Electronic Survey Form (Examining Smartphone Security Behaviour of College Students) written by Patricia A. Riola.**

Same as “Security and Privacy Awareness of Smartphone Users in Indonesia that written by M Amin, this research also uses electronic survey form for the flow of this research.

Community colleges in the United States (U.S.) made up the majority of the population. The study population of college students was chosen due to their familiarity with computers and smartphones and their capacity to generalise to a larger population (Niederman & DeSanctis, 1995). The study received 573 useable replies, which is a sufficient sample size from which to draw conclusions (Riola, P. A., 2014).

2.4.2 Technique Used

1. **Cross Tabulation Analysis and Pearson Chi-Square (An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment) written by Elizabeth L. McGovern Cole.**

In this research paper, it used Cross Tabulation Analysis and Pearson Chi-Square to analyze the data. Understanding the link between several variables is done using the crosstabs approach. The number of responses that suit that particular combination is listed in each cell of the Crosstabs table. The degree of education of the participant served as the independent variable utilized to compare all dependent variables in the analysis of the two surveys (McGovern Cole, E. L., 2019). On the other hand, Chi-Square tests were used to analyze the significance of the association between participants' awareness of smartphone security and educational attainment. The Chi-Square test, sometimes called the "Goodness of Fit" test, assesses the chance that knowledge of smartphone security and educational attainment are correlated surveys (McGovern Cole, E. L., 2019).

2. **Chi-Squared Test (Smartphone Security: A Quantitative Analysis of Security Usage and Outcomes) written by Barron Winters.**

In this research paper, they used Chi-Squared test to acquire the data, analyse it, and determine the results based on the data collected in accordance with the study's sample size. to do the necessary calculations to be used in the presentation of the results. This research conducts a quantitative non-experimental study utilising a validated survey instruments to fill research need that has been discovered.

The researcher chose the demographic being studied and examined the data received from the selection of smartphone users from ages 18 to 70. Following the collection of the necessary sample size, the findings were assessed, and a conclusion was drawn (Creswell & Creswell, 2017).

3. **Level of Awareness Equation (LoA) (Security and Privacy Awareness of Smartphone Users in Indonesia) written by M Amin.**

This research paper analyzes the data using LoA equation. Figure 2.4.2.1 shows how the equation looks like where Q is the total of each question's Q values. Using this formula, the LoA will be equal to 0 - 1. The LoA is 100% if the user selects all safe responses for all questions, and it will be close to 0% if the user selects all risky responses with the highest weight (Amin, M. et al., 2021).

$$LoA = 1 - \left(\frac{2}{1 + e^{-Q}} - 1 \right)$$

Figure 2.4.2.1 Equation for LoA

(Amin, M. et al., 2021)

The safe responses that been mentioned above are; Nothing, Always, No and for the unsafe responses are; Yes, Sometimes, rarely. However, this equation rarely being used by other researches.

4. **Shapiro-Wilk Test, T-Test and ANOVA Test (Examining Smartphone Security Behaviour of College Students) written by Patricia A. Riola.**

In this research paper, the Shapiro-Wilk normality test was used to determine whether the data were normal. This include demographic, security, and behavioural data were gathered to checked for normality test. For variables with regularly distributed data, mean and standard deviation were presented (Riola, P. A., 2014).

Besides, the necessary parametric tests were used to apply descriptive tests, and the mean and standard deviation were given. Using the standard T-Test, gender comparisons were made. ANOVA was used to compare different age groups. Pearson correlational tests were used to correlate the security level to computer experience.

The appropriate parametric correlation tests were used to assess the level of correlation between the independent variables of age, gender, year in school, major, years working with computers, and Consideration of Future Consequences (CFC) level and the dependent variable, smartphone security level. To examine the connection between the level of security and considerations of potential future effects, a correlational analysis between smartphone security levels and the CFC level was carried out.

To represent the associations between smartphone security and each of the independent factors, regression models were developed. The four security methods were measured using regression analysis.

2.4.3 Software/ Hardware Used

1. **QuestionPro (An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment) written by Elizabeth L. McGovern Cole.**

The survey was distributed to people in the United States who were over the age of 18, owned a smartphone, and used the device to carry out at least some of their job duties for the company where they worked by Question Pro (McGovern Cole, E. L., 2019).

By using QuestionPro, a total of 1,460 participants visited the User Survey's initial cover page, 1,338 began the survey, 437 were disqualified due to unanswered qualifying questions, 196 abandoned the survey, and 705 finished it. When asked about their employment status in the demographics, 19 participants first indicated that they used their smartphones for work, but they later indicated that they were unemployed or disabled.

After the data was cleansed for valid answers and these 21 responses were eliminated, there were a total of 684 participants who answered all the questions correctly.

2. **SurveyMonkey™ (Smartphone Security: A Quantitative Analysis of Security Usage and Outcomes) written by Barron Winters.**

A quantitative approach utilizing SurveyMonkeyTM was adopted (Cooper, 2014). By examining the security concerns users have with the proliferation of IoT devices, particularly smartphones, this research also aimed to advance Dr. Harper's (2016) study. In order to fill a known research gap, a quantitative non-experimental study employing a trusted survey instrument was chosen over a qualitative approach.

3. **SurveyMonkey™ Professional and Statistical Package for the Social Sciences (SPSS) (Examining Smartphone Security Behaviour of College Students) written by Patricia A. Riola.**

Survey Monkey Professional was used to carry out the survey (Survey Monkey, 2014). This particular technology was chosen because it provides secure sockets layer (SSL) certificates and encryption, which guard survey replies from unauthorised access and manipulation. Only the researcher had access to the material, which was password-protected and kept on a biometrically guarded laptop. The researcher lived alone in a secluded home where the laptop was kept. No personally identifying data was gathered, and the researcher took all reasonable steps to preserve anonymity and confidentiality.

In addition, a spreadsheet was used to import and analyse the data that had been gathered. Excel (Microsoft Office, 2010) and Statistical Package for the Social Sciences (SPSS) were used to analyse the data.

2.4.4 Summarization of Previous Research

Table 2.4.4.1 shows the summary of the previous research for critical review. It shows four (4) related research with the current project research. This table is divided by 4 sections which are Research Title and Author, Type of Framework Used, Type of Technique Used and Type of Software Used.

Research Title and Author	Type of Framework Used	Type of Techniques Used	Type of Software Used
An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment (McGovern Cole, E. L., 2019).	TAM-TOE Framework	Cross Tabulation Analysis and Pearson Chi-Square	Question Pro
Smartphone Security: A Quantitative Analysis of Security Usage and Outcomes (Winters, B., 2019)	Unified Theory of Acceptance and Adoption of Technology (UTAUT)	Chi-Squared Test	SurveyMonkey™
Security and Privacy Awareness of Smartphone Users in Indonesia (Amin, M. et al., 2021)	Electronic Survey Form	Level of Awareness Equation (LoA)	N/A
Examining Smartphone Security Behavior of College Students (Riola, P. A., 2014)	Electronic Survey Form	Shapiro-Wilk Test, T-Test and ANOVA Test	SurveyMonkey™ Professional and Statistical Package for the Social Sciences (SPSS)

Table 2.4.4.1 Summarization of Critical Review

2.5 Proposed Solution

Based on the related work, it is regarded appropriate to use a quantitative technique for this research project because survey questionnaires will be used to collect responses that include multiple-choice answer possibilities. Quantitative measurements will be made of the research variables, especially as they relate to the demographic questions on the questionnaire. Additionally, a survey using a Likert scale will be used to gauge the university student's level of data security awareness.

The ANOVA test will be used in the research project's analysis phase to look at the differences and relationships between variables. Correlation and ANOVA tests will be used to determine the level of awareness regarding the data security in mobile phone among university students.

Besides, Google Form will be used as the software platform for distributing surveys to participants in order to collect data. A user-friendly interface is offered by Google Form for developing and disseminating online surveys.

IBM SPSS (Statistical Package for the Social Sciences) software will be used to manage and analyze the gathered data. Statistical processes and data analysis tools are included in the widely known software programmed SPSS, which makes it appropriate for analyzing quantitative data from survey questions. All descriptive statistics and a number of statistical tests, including ANOVA, are all possible using SPSS.

The study project intends to effectively acquire and analyze the survey results, giving useful insights into the research variables and their interactions, by using Google Form for data collecting and SPSS for data administration and analysis.

2.6 Summary of Chapter 2

To summarize, this chapter discuss about all the vulnerabilities in mobile phone and also the previous research that related to the title of this study. The next chapter will cover about the methodology of this research and the milestone of this research project.

CHAPTER 3: PROJECT METHODOLOGY

3.1 Introduction

This chapter highlights the techniques and methods used to perform this research study and acts as a guide to it. It explained a clear and concise overview of the data collection methods and data analysis techniques that used to analyze data of the university student regarding to data security in mobile phone. In addition, this chapter also shows the project milestone that act as the action plan of this project.

3.2 Methodology

In this section, the project methodology will be discussed. Figure 3.2.1 shows the step of the project methodology for data security in mobile phone among university student analysis. It consists of 6 phases, which are includes, identifying the problem statement, the preparation of pilot questionnaire, the validation of questionnaire, the development of questionnaire, collection of data and lastly data analysis (Amin, M. et al., 2021). During the initial phase, the problem of this study will be identified. For the second phase, it will determine what kind of question should be asked according to previous research paper. Next, third phase is approval of the questionnaire from the experts in information security. For the fourth phase, the questionnaire will be given to the university students. For the fifth phase, survey questionnaire will be gathered and finally, all the data will be analysis using a statistic analysis software in the final phase.

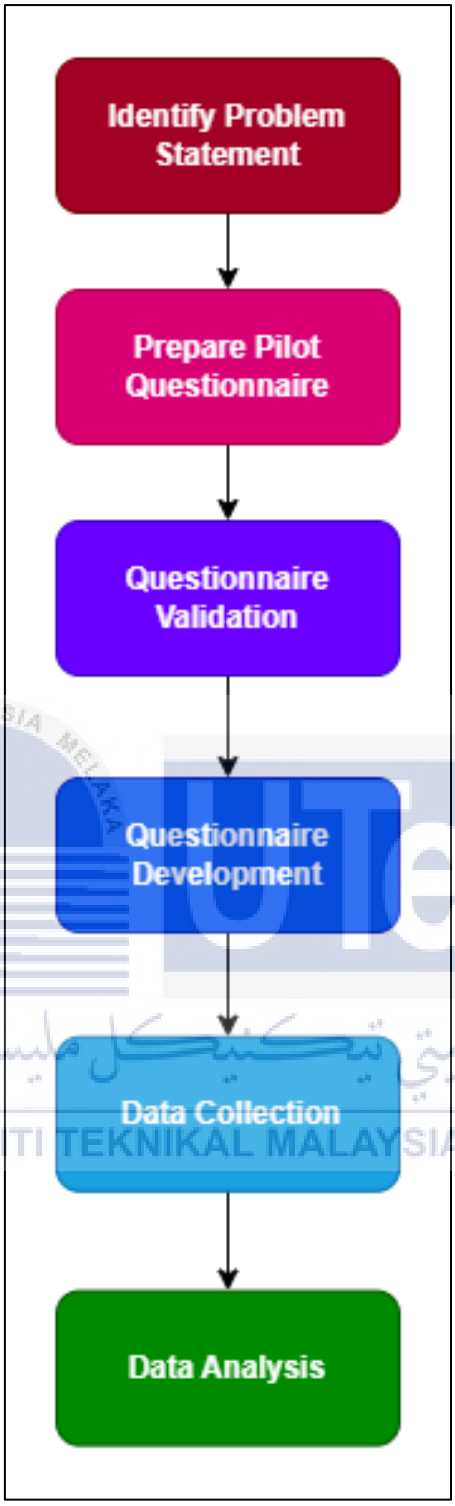

Figure 3.2.1 Project Methodology

3.2.1 Identify Problem Statement

In this phase, the problem statement will be the concerned. This phase will identify the problem of data security and level of awareness in mobile phone among the university student. During this first phase, all problem will be gathered.

3.2.2 Prepare Pilot Questionnaire

During this phase, a pilot questionnaire will be design. All the question are being referred to the previous research paper. The question will consist of the awareness of data security including data security practices and threat awareness. The questionnaire will divide by three (3) section which are Section A, Section B and Section C. The first section of this questionnaire will be asking about their demographic of the university student; the total question in this section is eight (8). Next, Section B will cover about User Vulnerability Awareness (UVA), User Threat Awareness (UTA) and User Security Practices (USP) which total of eighteen (18) questions. Lastly, Section C consist of twenty-two (22) question which covered about Perceived Risk (PR), Secondary Utilization of Personal Data (SUPD), Competence (C) and Trust (T).

3.2.3 Questionnaire Validation

In this phase, the pilot questionnaire will be validated, and the best question will be chosen to represent the variable in the project research. To validate the pilot questionnaire, the chosen experts will be provided with the content validation template for their evaluation. This pilot questionnaire was evaluated by information security professional. Table 3.2.3.1 shows the list of the experts' information.

No	Name	Profession	Expertise	Qualification
1	Ts. Dr. Mohd Zaki Mas'ud	Senior Lecturer	Computer system and Network, Web Applications Development, Multimedia Content Development	PhD in Computer Science (Universiti Teknikal Malaysia Melaka), Masters in IT (Computer Science) From (Universiti Kebangsaan Malaysia), Bachelor of Engineering (Hons) Electronic (Multimedia University).

2	Dr. Nur Fadzilah Binti Othman	Senior Lecturer	Information Security and Privacy	PhD. in Information Security (UTeM), Master in Educational Technology (UTM), Degree in Computer Engineering (UTM)

Table 3.2.3.1 List of Expert's Information for Pilot Questionnaire

3.2.4 Questionnaire Development

This phase focuses on developing the pilot questionnaire that was examined and approved by information security experts from the phase before. The instrument is prepared through online platform which is Google Form and published it to the university students.

3.2.5 Data Collection

This phase focused on the data gathering where the survey questionnaire will be given to Universiti Teknikal Malaysia Melaka (UTeM) students. The target of overall sample of the student will be at least 250 respondents. This is because after all the data has been gathered, the data will be analyses in the next phase.

3.2.6 Data Analysis

All the data that already collected before will be analyzed in this phase. The sample of the data will be analyzed using SPSS software. The result of statistical analysis will be shown and it will determine the level of data security awareness in mobile phone usage among university student.

3.3 Project Milestone

Project Milestone is used to monitor and plan a project's progress and as a point of comparison to determine whether the project is on track and accomplishing its goals. Table 3.3.1 shows the PSM 1 milestone and table 3.3.2 shows the Gantt Chart of PSM 1 of this research project.

WEEK	ACTIVITY	NOTES
W1 (20/03 - 24/03)	• Choosing a topic and potential supervisor. • Proposal PSM: Discussion with Supervisor. • Proposal assessment and verification.	• Title is chosen. • Develop a proposal • Deliverable at email PIC (Dr. Fadzilah Othman)
W2 (27/03 - 31/03)	• List of students with project title versus supervisor and evaluator. • Proposal correction and improvement. • Proposal approval	• Email Committee for proposal approval. • Upload approved proposal at Ulearn.
W3 (03/04 - 07/04)	Chapter 1 • Meeting 2	
W4 (10/04 - 14/04)	Chapter 1 • Report Writing Progress 1	• Log progress on ePSM. • Deliverable of Chapter 1 on ePSM.
W5 (17/04 - 21/04)	Chapter 2	
W6 (24/04 - 28/04)	**MID-SEMESTER BREAK**	
W7 (01/05 - 05/05)	Chapter 2 • Report Writing Progress • Project Progress 1	• Log progress on ePSM. • Deliverable of Chapter 2 on ePSM. • Progress Presentation 1 to supervisor.
W8 (08/05 - 12/05)	Chapter 3	

W9 (15/05 - 19/05)	Chapter 3 • Report Writing Progress	• Log progress on ePSM • Deliverable of Chapter 2 on ePSM
W10 (22/05 - 26/05)	Chapter 4 • Project Progress 2 • Meeting with supervisor	• Log progress on ePSM. • Progress Presentation 2 to supervisor.
W11 (29/05 - 02/06)	Chapter 4 • Report Writing Progress 2	• Log progress on ePSM • Deliverable of Chapter 2 on ePSM
W12 & W13 (05/06 - 16/06)	• PSM1 Draft Report preparation	
W14 (19/06 - 23/06)	• PSM1 Draft Report submission to SV & Evaluator • Report Evaluation	• Log Progress on ePSM • Deliverable of Complete PSM1 Draft Report on ePSM
W15 (26/06 - 30/06)	• PSM 1 Demo and Report Presentation to Supervisor & Evaluator • Presentation Skill • Submission of PSM 1 documents to PSM supervisor, evaluator and committee in ePSM	• Log Record on ePSM • Submission of logbook in ePSM • Submission of Project Report PSM 1 on ePSM.

Table 3.3.1 PSM 1 Milestone

Progress / Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FYP Proposal															
Project Progress 1															
Report Writing Progress 1															
Project Progress 2															
Report Writing Progress 2															
Report Evaluation															
Demonstration															
Presentation															

Table 3.3.2 PSM 1 Gantt Chart

WEEK	ACTIVITY	NOTE / ACTION
W1 (31/7 - 4/8) Meeting 1	Chapter 4	• PSM 1 correction and PSM 2 planning discussed with the supervisor.
W2 (7/8 - 11/8) Meeting 2	Chapter 5 Project Progress 1 [PRJ-1]	• Log Progress on ePSM. • Progress Presentation 1 (KP1).
		• Supervisor evaluate on ePSM.
W3 (14/8 -18/8)	Chapter 5	• Student working on Chapter 5.
	Report Writing Progress [PRJ-3]	• Log Progress on ePSM. • Deliverable of Chapter 5 to SV through email.
		• Supervisor evaluate on ePSM.
	Student Status	• Warning Letter 1 from supervisor and Committee.
W4 (21/8 - 25/8) Meeting 3	Chapter 6	• Student working on Chapter 6.
	Project Progress 2 [PRJ-2]	• Log Progress on ePSM. • Progress Presentation 1 (KP2).
		• Supervisor evaluate on ePSM.
W5 (28/8 - 1/9) Meeting 4	Chapter 6	• Chapter 6
	Report Writing Progress [PRJ-3]	• Log Progress on ePSM. • Deliverable of Chapter 6 to SV through email.
		• Supervisor evaluate on ePSM.
	Chapter 7	• Student working on Chapter 7.
	Student Status	• Warning Letter 2 from supervisor and Committee.
	Schedule the presentation	• Presentation Schedule on ULearn.

W6 (4/9 - 8/9) Meeting 5	- Chapter 7 Report Writing Progress [PRJ-3]	• Log Progress on ePSM. • Deliverable of Chapter 7 to SV through email.
		• Supervisor evaluate on ePSM.
	- Determination of student status (Continue/Withdraw)	• Supervisor submit student status to Committee.
	- PSM2 Draft Report preparation. - PSM2 Draft Report submission to SV & Evaluator.	• Deliverable of PSM 2 Draft Report on ePSM.
W7 (11/9 - 15/9) FINAL PRESENTATION	- Report Evaluation [PRJ6] [PRJ-10] - DEMONSTRATION Supervisor [PRJ-4] [PRJ-5] - DEMONSTRATION Evaluator [PRJ-9]	• Log Progress on ePSM.
		• SV and EV evaluate on ePSM.
	- English Proficiency [PRJ-7]	• Log Progress on ePSM.
		• Supervisor evaluate on ePSM.
	- Presentation Skill [PRJ-8]	• Log Progress on ePSM.
		• EV evaluate on ePSM.
W8 (18/9 - 22/9) FINAL EXAMINATION WEEKS	- Based on suggestions made by the Supervisor and Evaluator during the final presentation session, the draft report was corrected. - Fill out an EoS Survey form online.	• Deliverable of EoS Survey, Online Form.
	- Complete of overall marks to Committee	• SV, EV and Committee Overall Evaluation PSM2 on ePSM
	- Submission of the final complete report, which is the updated & corrected PSM2 report.	• Deliverable the complete Final PSM Report on ULearn.

W9 (25/9 - 29/9) INTER-SEMESTER BREAK	Submission of the final complete report, which is the updated & corrected PSM2 report and Plagiarism Report etc. onto the OneDrive	• Deliverable the complete Final PSM Report, Plagiarism Report.

Table 3.3.3 PSM2 Milestone

Progress / **Week**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Project Progress 1									
Project Progress 2									
Report Writing Progress									
Report Evaluation									
Demonstration									
Presentation									
Submission Report									

Table 3.3.4 PSM2 Gantt Chart

3.4 Summary of Chapter 3

This section describes the project's methodology which consists of 6 phases, which are includes, identifying the problem statement, the preparation of pilot questionnaire, the validation of questionnaire, the development of questionnaire, collection of data and lastly data analysis. Besides, this section shows the project milestone and Gantt Chart of the research project. The upcoming section will explain more detail regarding the design of the analysis.

CHAPTER 4: DESIGN AND IMPLEMENTATION

4.1 Introduction

The results of the preliminary design analysis and the detailed design result will be covered in this chapter. These results will help comprehend the design process and its implications. This chapter will also provide into the particulars of the information that will be gathered from respondents, including the reasons behind their selection as the sample for data collection. Following a description of the population being studied, the research designs chosen for the study will be outlined. Additionally, sampling techniques and processes will be described. Finally, a discussion of the data gathering instrumentation will take place.

4.2 Research Instrument

In this section, the research instrument design will be explained. The focus of this research topic is the level of awareness of data security in mobile phone among university students. Thus, this research instrument design consists of three sections with a total of 46 questions in each. The design of the research instrument is depicted in the table below.

Section	Title	No. Question	References
A	Demographic	1-8	Sletten, M. A. (2020). Security in a Mobile Learning Environment. Ph. D Thesis, University of Illinois at Urbana-Champaign, Urbana, Illinois.
B	Level of Awareness Among University Students.	User Vulnerability Awareness (1-6)	McGovern Cole, E. L. (2019). An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment. Ph. D Thesis, B.S. Information Technology and Information Security Systems, University of Phoenix.
		User Threat Awareness	McGovern Cole, E. L. (2019). An Exploratory Study: The Knowledge Gaps of Smartphone Security

		(7-14)	Between Users and IT Security Professionals in the Emerging BYOD Environment. Ph. D Thesis, B.S. Information Technology and Information Security Systems, University of Phoenix.
		User Security Practices (15-18)	McGovern Cole, E. L. (2019). An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment. Ph. D Thesis, B.S. Information Technology and Information Security Systems, University of Phoenix.
C	Vulnerabilities Behaviour Assessment	Perceived Risk (1-7)	Cooper, C. (2014). Smartphone privacy perceptions and behaviours generational influence quantitative analysis: Communications privacy management theory. Master dissertation, Colorado Technical University [Preprint].
		Secondary Utilisation of Personal Data (8-12)	Cooper, C. (2014). Smartphone privacy perceptions and behaviours generational influence quantitative analysis: Communications privacy management theory. Master dissertation, Colorado Technical University [Preprint].
		Competence (13)	Bibeau, R. (2011). Mobile data security: Research and analysis of mobile data security with emphasis on mobile public safety users. Master's dissertation, The College of St. Scholastica.

		14	Cooper, C. (2014). Smartphone privacy perceptions and behaviours generational influence quantitative analysis: Communications privacy management theory. Master dissertation, Colorado Technical University [Preprint].
		15-17	Amin, M. et al. (2021). 'Security and privacy awareness of smartphone users in Indonesia', Journal of Physics: Conference Series, 1882(1), p. 012134. doi:10.1088/1742-6596/1882/1/012134.
		Trust (18)	Riola, P. A. (2014). Examining Smartphone Security Behaviour of College Students. In Google Books. Northcentral University. https://books.google.com.my/books/about/Examining_Smartphone_Security_Behavior_o.html?id=z7n2oAEACAAJ&redir_esc=y.
		19	Scott, S. (2006). Mobile phone usage amongst teenagers: An analysis of research methods specific to teenage mobile phone use. Ph. D Thesis, University of Glasgow Faculty of Information and Mathematical Sciences Department of Computing Science.
		20	Bibeau, R. (2011). Mobile data security: Research and analysis of mobile data security with emphasis on mobile public safety users. Master's dissertation, The College of St. Scholastica.

		21-22	Amin, M. et al. (2021). 'Security and privacy awareness of smartphone users in Indonesia', Journal of Physics: Conference Series, 1882(1), p. 012134. doi:10.1088/1742-6596/1882/1/012134.

Table 4.2.1 Research Instrument Design

4.2.1 Data Collection

For data collection, the target responder for this survey questionnaire is among Universiti Teknikal Malaysia Melaka (UTeM) students. The survey instrument will be given to different faculty in UTeM through social media application such as WhatsApp, Telegram, Instagram and Twitter using shared link created in Google Forms. The purpose of target responder being in different faculty is to differentiate the knowledge between IT and non-IT students. After a few weeks the instrument survey was develop, the data will be collected. All the answers of the survey questionnaire will be gathered and recorded for the data analysis.

4.3 Questionnaire Design

This section shows the survey questionnaire design of each section in instrument questionnaire. For the first section, it is used to identify the demographic of the respondents which are their information like gender, age and which faculty. Moreover, it is also identifying their background in using mobile phone. Next, section B will collect data that can be used to assess the respondent's existing understanding of data security measures and their awareness as mobile phone users. Lastly, section C will identify the respondent's perception of data security in mobile phone. The flow diagram of each question together with-it subsection is shown as figure below.

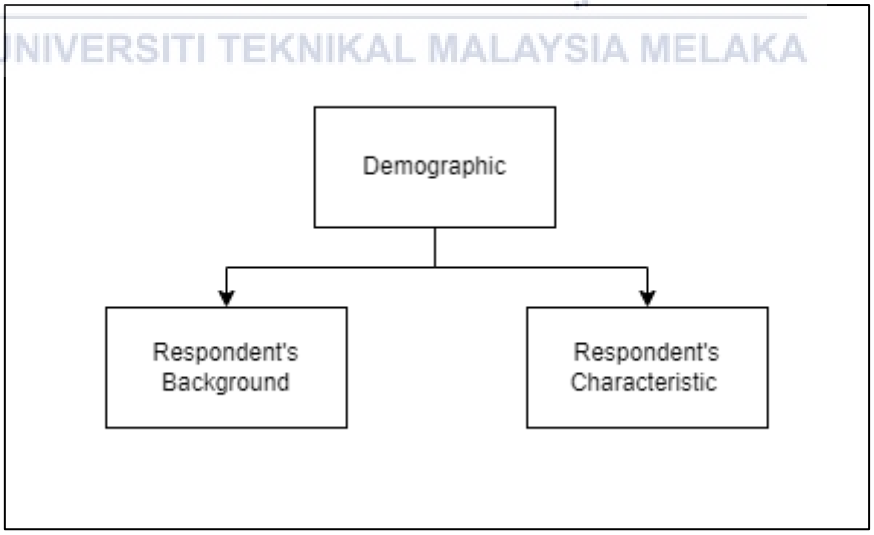

Figure 4.3.1 Subsection A for Questionnaire

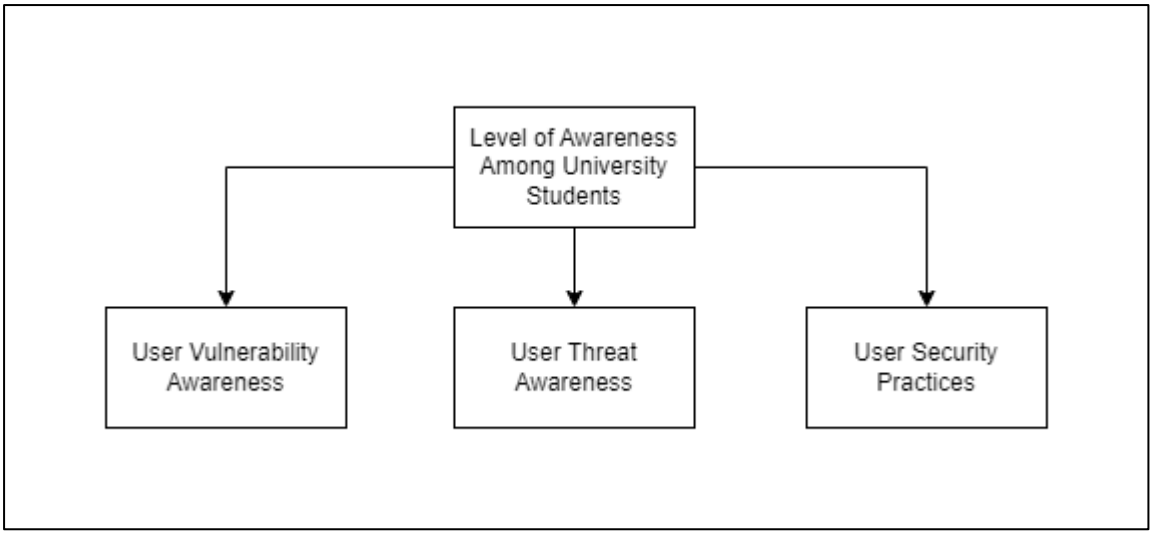

Figure 4.3.2 Subsection B for Questionnaire

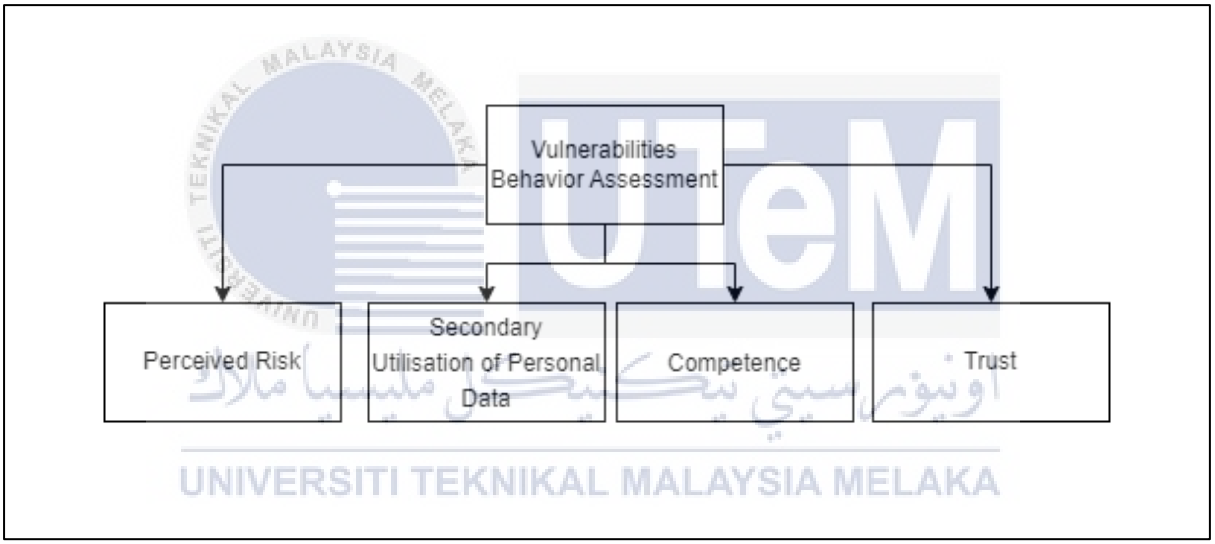

Figure 4.3.3 Subsection C for Questionnaire

4.4 Summary of Chapter 4

This chapter explains the design of the survey questionnaire. It also shows the subsection of each section in questionnaire. The target responder for this survey questionnaire is at least 250 respondents. The questionnaire will be posted online using the shared link creates in Google Form. The results and data gathering of the feedback questionnaire will be used in next chapter.

CHAPTER 5: ANALYSIS AND FINDINGS

5.1 Introduction

The implementation of the research survey is described in detail in this section, along with the results obtained after the survey was distributed and finished. 258 reliable respondents within the specified area of the study provided responses to the survey. These participants have previous knowledge of their personal information security in mobile phone. The ANOVA test methodology will next be used to analyse the survey data in more detail. Utilising both IT and non-IT fields, this method entails analyzing the differences between response groups from various faculties. The objective is to examine potential connections that could have an impact on how much university students are aware of mobile phone data security. The study compares these talents to discover if there are any meaningful correlations. The results of this analysis will ultimately be used as a parameter to determine which faculty group demonstrates the highest level of awareness and their understanding regarding mobile phone data security.

5.1.1 Research Survey Objectives

Three sections will be used to examine the findings of this research study that was conducted utilising a questionnaire instrument from Google Form. The respondents' perspective will be evaluated by all this section which are Section 1: Demographic, Section 2: Level of Awareness Among University Students and Section 3: Vulnerabilities Behavior Assessment as the variable in the ANOVA test. Before performing ANOVA test, descriptive analysis is an essential initial step in this research that forms the basis for understanding, summarizing, and exploring the respondent research survey essential characteristics. Through the use of descriptive statistics and data visualization techniques, this research study gains valuable insights into the central tendencies, variability, and distribution of the respondent data. Next, to ensure the reliability of the online survey instrument, this research study assessed the internal consistency using Cronbach's alpha. Lastly, in order to determine whether the distribution of this research data was normal, Skewness and Kurtosis normality test will be performed. This research study data significantly varied from normality according to the both Skewness and Kurtosis values themselves, which prompted to investigate data transformations for subsequent studies. After conducting a comprehensive step of preliminary tests, including assessments of normality, reliability, and other relevant checks, Analysis of Variance

(ANOVA) test will be proceeded to the next step. These preliminary steps have allowed to ensure the quality and validity of the data, paving the way for a robust ANOVA analysis to investigate the relationships and differences among the groups in this research study.

The following are the research survey objectives:

i) To gauge university students' knowledge and their familiarity with a certain topic of data security in mobile phone.

ii) To assess how well university students understand the idea of mobile phone security.

iii) To compare and contrast the awareness levels displayed by students studying IT and those pursuing non-IT fields.

5.2 Descriptive Analysis

A descriptive analysis is carried out based on the demographic section. It requires assessing the data sampling from the respondents' gathered data and clearly displaying it. Furthermore, it helps to clarify the significance of the variation in the sample group of respondents' data. As a result, the respondents in this study include university students from various faculties who have expertise utilising mobile phones. Eight (8) faculties make up the faculty which are Fakulti Kejuruteraan Eletrik (FKE), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE) and Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP).

5.2.1 Respondent Demography

The variety of responder demographics are covered in this section. An extensive set of eight (8) questions pertaining to participant segment data were included in the survey's initial phase. These questions asked about their gender, age, faculty affiliation, academic year, marital status and three (3) questions on their prior mobile phone usage.

The total of 258 respondents were contributed successfully to complete the form where the target respondent is at least 250. The information was gathered online using online survey which is Google Form for conducting surveys, and all of the respondents were gained through social media mostly among Universiti Teknikal Malaysia Melaka (UTeM) students. Firstly, the responses are divided into two gender categories which are male and female. Female has the highest percentage in contributing to filled the survey which consist of 163 (63.2%) participants. In the meantime, 95 (36.8%) of total respondents were male participants.

Moving forward, the participants were categorized into three (3) age groups: Teens, Pre-adults and Adults. These groups were labelled as follows: group A – Teens (18-20), group B – Pre-adults (21-24) and group C – Adults (24-30). A majority number of participants were collected for group B. Precisely, group A comprised 25 participants (9.7%), group B involved 213 participants (82.6%) and group C encompassed 20 participants (7.8%).

Continuing with the survey question, the participant was asked for their faculty in UTeM. Out of the surveyed participants, 25 (9.7%) participants identified themselves with Fakulti Kejuruteraan Eletrik (FKE) and 17 participants (6.6%) affiliated with Fakulti Kejuruteraan Pembuatan (FKP). Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) is chosen by 25 (9.7%) participants in this online survey. Next, a significant 86 (33.3%) participants indicated their association with Fakulti Teknologi Maklumat dan Komunikasi (FTMK). Furthermore, 29 (11.2%) participants identified themselves as part of Fakulti Pengurusan Teknologi dan Teknousahawan (FPTT), 25 (9.7%) participants were aligned with Fakulti Kejuruteraan Mekanikal (FKM), 17 (6.6%) participants indicated their association with Fakulti Kejuruteraan Teknikal Eletrik Eletronik (FTKEE), and 34 (13.2%) participants declared affiliation with Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP). This breakdown provides valuable insights into the distribution of respondents across the various faculties at UTeM in comparing the level of awareness in data security in mobile phone between IT and non-IT students.

Then, the academic year data of their study were collected. The academic year in UTeM is divided by Year One, Year Two, Year Three and Year Four. Year Three shows the majority participants with 111 (43%) participants, followed by Year Two with 89 (34.5%) participants. Next, the participants who are currently in Year One is 34 (13.2%) participants and Year Four which is the least participants with the total of 24 (9.3%) participants. In this online survey

research, marital status of participants also was collected to form a data where 247 (95.7%) participants are single, 6 (2.3%) are married and others with 5 (1.9%). The following table and figure outline the detailed demographic characteristics of Universiti Teknikal Malaysia Melaka (UTeM) students participating as respondents in the research study

Gender	**Frequency** (N= 258)	**Percentage (%)**
Male	95	36.8
Female	163	63.2

Table 5.2.1.1 Gender List

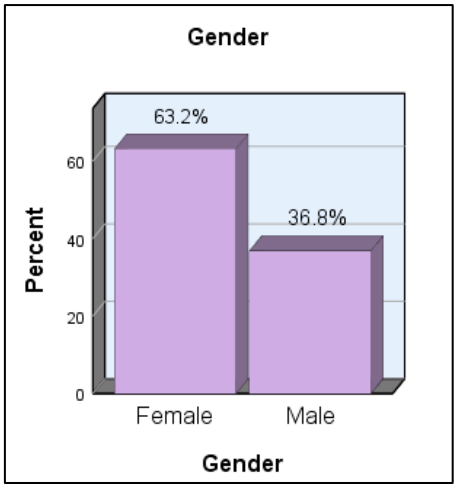

Figure 5.2.1.1 Gender List Bar Chart

Age	**Frequency** (N= 258)	**Percentage**
18-20	25	9.7%
21-24	213	82.6%
24-30	20	7.8%

Table 5.2.1.2 Age List

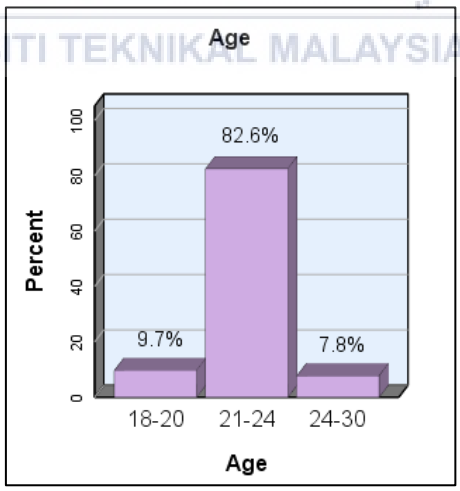

Figure 5.2.1.2 Age List Bar Chart

Faculty	Frequency (N=258)	Percentage
Fakulti Kejuruteraan Eletrik (FKE)	25	9.7%
Fakulti Kejuruteraan Pembuatan (FKP)	17	6.6%
Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK)	25	9.7%
Fakulti Teknologi Maklumat dan Komunikasi (FTMK)	86	33.3%
Fakulti Pengurusan Teknologi dan Teknousahawan (FPTT)	29	11.2%
Fakulti Kejuruteraan Mekanikal (FKM)	25	9.7%
Fakulti Teknologi Kejuruteraan Eletrik Elektronik (FTKEE)	17	6.6%
Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP)	34	13.2%

Table 5.2.1.3 Faculty List

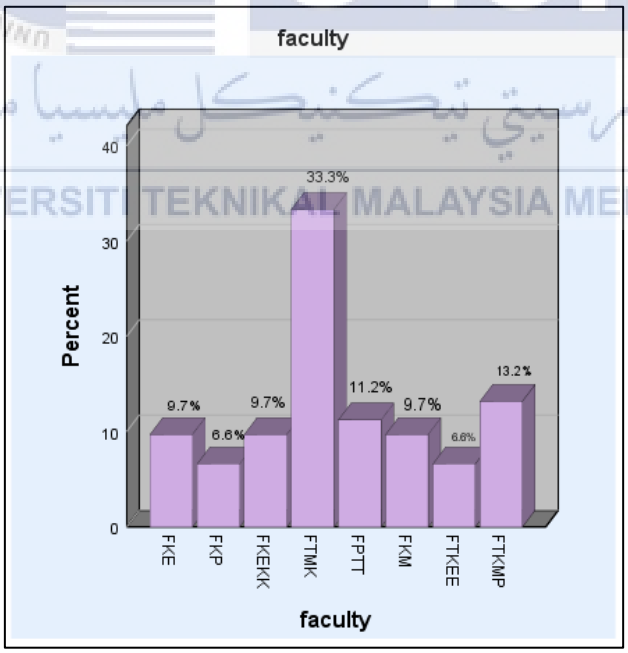

Figure 5.2.1.3 Faculty List Bar Chart

Academic Year	Frequency (N= 258)	Percentage
Year One	34	13.2%
Year Two	89	34.5%
Year Three	111	43%
Year Four	24	9.3%

Table 5.2.1.4 Academic Year List

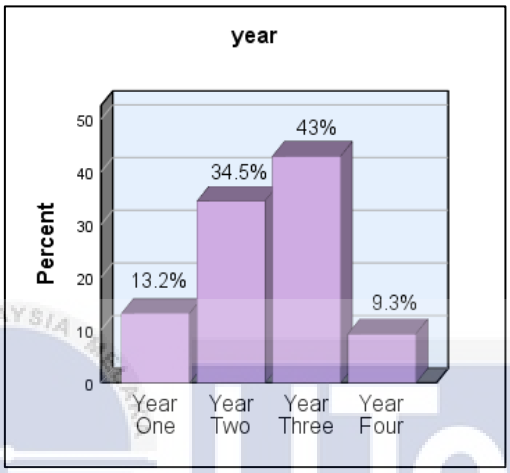

Figure 5.2.1.4 Academic Year List Bar Chart

Marital Status	Frequency (N=258)	Percentages
Single	247	95.7%
Married	6	2.3%
Other	5	1.9%

Table 5.2.1.5 Marital Status List

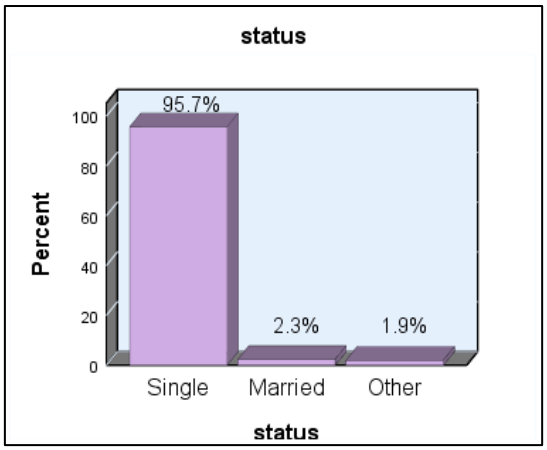

Figure 5.2.1.5 Marital Status List Bar Chart

Furthermore, section A goes into great detail on how consumers have used mobile phones historically. The survey's sixth question asks respondents to select either an Android or an Apple as their mobile device. According to the findings, out of all participants, 145 (56.2%) are using Apple, while the remainder 113 (43.8%) are using Android devices. The following inquiry then gathered information about whether any social media application was installed on their cell phones. Only 1 respondent (1.4%), who said they had no social media applications installed, was among the 257 respondents who indicated they had social media apps installed. The last inquiry in this section asks information on the individual social media platforms that respondents have installed in their mobile devices. The result of this survey question is shown in Figure 5.2.1.6 where an equal number of respondents, 250 (96.9%) participants reported having both WhatsApp and Instagram installed on their mobile devices. Additionally, Facebook was installed by 197 (76.4%) participants, TikTok by 229 (88.8%) participants, LinkedIn by 91 (35.3%) participants, Twitter by 179 (69.4%) participants, Snapchat by 128 (49.6%) participants and 9 (3.6%) participants mentioned using other social media platforms.

Brand	Frequency (N= 258)	Percentages
Apple	145	56.2%
Android	113	43.8%

Table 5.2.1.6 Brand List

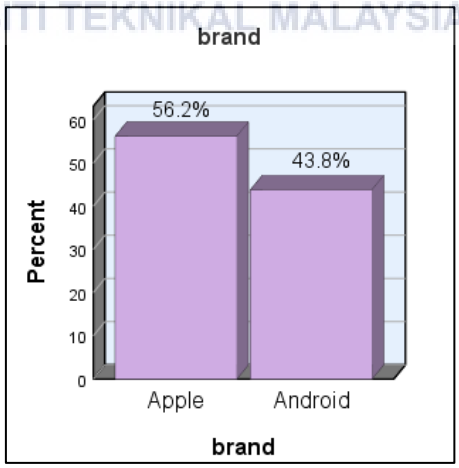

Figure 5.2.1.6 Brand List Bar Chart

Installed	Frequency (N= 258)	Percentages
Yes	257	99.6%
No	1	0.4%

Table 5.2.1.7 Installed List

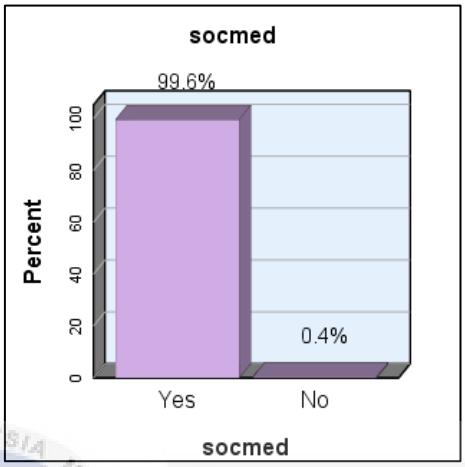

Figure 5.2.1.7 Installed List Bar Chart

Application	Frequency (N= 258)	Percentages
Facebook	197	76.4%
Instagram	250	96.9%
TikTok	229	88.8%
LinkedIn	91	35.3%
Twitter	179	69.4%
Snapchat	128	49.6%
WhatsApp	250	96.9%
Others	9	3.6%

Table 5.2.1.8 Application List

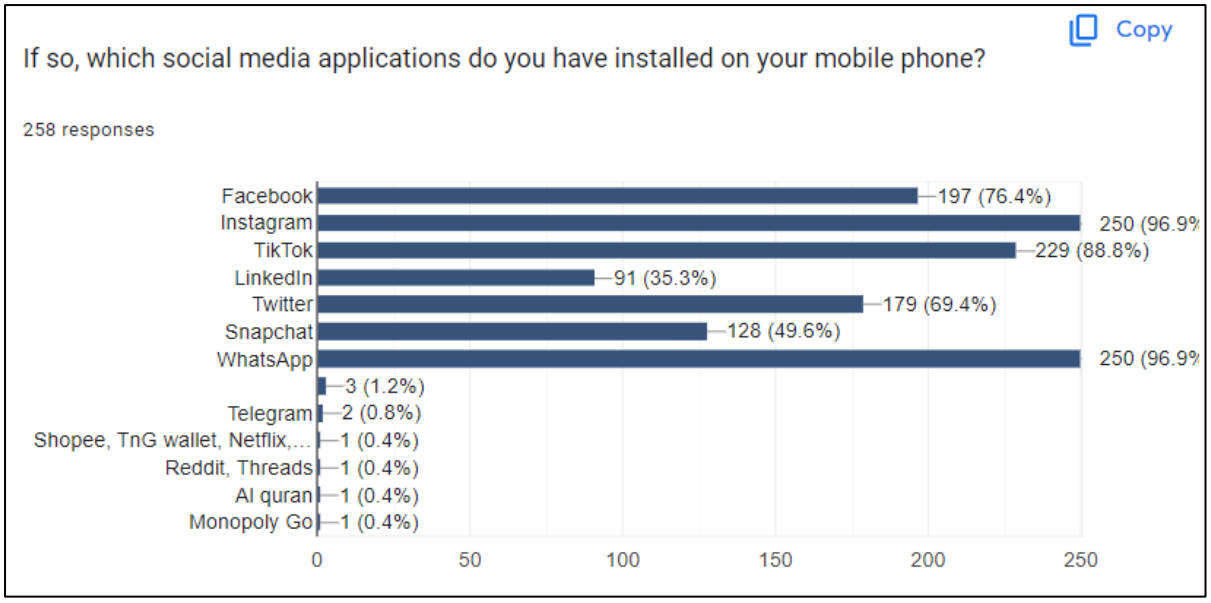

Figure 5.2.1.8 Application List Chart

5.3 Reliability Analysis

Reliability analysis was performed to assess the instrument's internal consistency. Table 5.3 findings show that the calculated alpha values for each variable lie between the ranges of 0.721 and 0.960. A reliability score below 0.6 is regarded as poor according to (Nunnaly's. ,1980) stated criteria, whereas scores between 0.60 and 0.70 are seen as acceptable, those between 0.80 and 0.90 as good, and values above 0.90 as excellent. Therefore, we can state with confidence that the reliability of each variable in our study falls within the "good" and "excellent" categories, highlighting the dependability and consistency of the data measuring instrument. As a result, the reliability of each variable of the study is good and excellent.

Reliability Score	Relation of Data with Reliability Analysis
< 0.6	Poor
0.60 – 0.69	Acceptable
0.70 – 0.89	Good
>0.9	Excellent

Table 5.3.1 Reliability Score Scale

Variable	Item	Alpha Value
User Vulnerability Awareness	uva_information	0.904
	uva_gather_data	0.902
	uva_GPS	0.904
	uva_assistant	0.909
	uva_Bluetooth	0.918
	uva_Wi-Fi	0.918
User Threat Awareness	uta_malware	0.960
	uta_BlueBorne	0.960
	uta_Dolphin	0.957
	uta_Spyware	0.955
	uta_leakage	0.954
	uta_Spoofing	0.954
	uta_tampering	0.953
	uta_Phishing	0.954
User Security Practices	usp_screenlock	0.872
	usp_passwords	0.840
	usp_clean_malware	0.834
	usp_antivirus	0.881
Perceived Risk	pr_tracked	0.878
	pr_apps	0.875
	pr_daily	0.888
	pr_privacy	0.871
	pr_utilized	0.873
	pr_privatecom	0.886
	pr_unauthorized	0.885
Secondary Utilisation of Personal Data	supd_utilize	0.905
	supd_much_info	0.894
	supd_smartphone	0.905
	supd_claim	0.895
	supd_organization	0.893
Competence	c_VPN	0.752

	c_configured	0.732
	c_signout	0.721
	c_read	0.737
	c_Biometric	0.838
Trust	t_encrypted	0.911
	t_trusted	0.922
	t_improved	0.898
	t_SMS	0.894
	t_read	0.902

Table 5.3.2 Results of Reliability Analysis

5.4 Normality Test

To get a fundamental knowledge of the data available, data examination for main constructs of study is undertaken This involves displaying measures for mean and standard deviation on each construct. The rank of the scale point and the construct's degree are also mentioned in the information. In order to verify the data's distribution, the inspection of normality was also carried out.

George and Mallery (2010) state that the skewness and kurtosis values must fall within ranges of ±2 in order for the distribution of data to be considered normal. According to (Hair et al., 2010) and (Bryne, 2010), data is deemed normal if the skewness and kurtosis are within a range of -2 to +2 and -7 to +7, respectively. Additionally, in line with (Kline's, 2011) thesis, values above 20 may point to more serious issues, with absolute values of Skewness greater than 3 and Kurtosis is greater than 10 and 20, respectively, indicating problems. In light of this, it was advised that Skewness and Kurtosis' absolute values should not exceed 3 and 10, respectively.

Based on figure 5.4.1, the study's variables are distributed normally in accordance with the recommendations of (Hair et al., 2010) and (Bryne, 2010).

Descriptive Statistics

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
uva	258	24.63	5.425	-1.128	.152	.968	.302
uta	258	32.16	7.434	-.784	.152	.174	.302
usp	258	17.70	3.253	-1.756	.152	2.752	.302
perceived_risk	258	27.69	5.976	-.632	.152	-.069	.302
supd	258	19.91	4.354	-.563	.152	-.464	.302
competence	258	18.16	4.686	-.026	.152	-.910	.302
trust	258	20.93	4.234	-.979	.152	.425	.302
Valid N (listwise)	258						

Figure 5.4.1 Skewness and Kurtosis Normality Test Result

Based on figure 5.4.1 above, the study variables are considered normal distribution are based on the Skewness and Kurtosis statistic value. Section B of the online research survey consist of three (3) sub sections. Level of Awareness Among University Students is the main variable for section B. In the figure above, User Vulnerability Awareness (UVA), User Threat Awareness (UTA) and User Security Practices (USP) are the variable under this section. User Vulnerability Awareness (UVA) is considered normal as the skewness value is -1.128 and the kurtosis value is 0.968. Next, User Threat Awareness (UTA) also score exhibits a normal distribution, with a skewness value of 0.784 and a kurtosis value of 0.174, indicating a well-balanced and representative assessment of user threat within the system. Lastly, with a skewness value of -1.756 and a kurtosis value of 2.752, the User Security Practices (USP) metric demonstrates a statistically typical distribution.

Next, the primary factor of interest in section C is "Vulnerabilities Behaviour Assessment". Perceived Risk (PR), Secondary Utilisation of Personal Data (SUPD), Competence (C) and Trust (T) are the four (4) sub variables that make up this variable. The data for Perceived Risk as in the table above known as “perceived_risk” exhibits a normal distribution, as shown by the values of skewness (-0.632) and kurtosis (-0.69). Besides, a normal distribution is also shown by Secondary Utilisation of Personal Data (SUPD), which has a skewness value of -0.563 and a kurtosis value of -0.464. The Competence (C) metric has a skewness value of -0.026 and a kurtosis value of -0.910, while Trust (T) has skewness value of 0.979 and kurtosis value of 0.425, both of which indicate that the distribution it displays is statistically normal.

As a result, the data analysis is valid because the Skewness and Kurtosis values are strong indicators that the study variables in Sections B and C follow a normal distribution.

5.5 Level of Awareness Among University Students Analysis

Section B of the questionnaire focuses on measuring Level of Awareness Among University Students regarding data security in mobile phone. This section assesses respondents' awareness of data security practice among Universiti Teknikal Malaysia Melaka (UTeM) students in IT and non- IT field. Respondents were asked to provide their insights by responding to 18 inquiries related to their concerned to data security, knowledge of security threats and attacks and related activities that might be happened towards their personal data in mobile phone. The data from these responses is presented in Appendix C1, which aids in determining the level of awareness among the UTeM students regarding data security in mobile phone. The study uses faculty in UTeM as independent variables and considers three sub-sections: User Vulnerability Awareness (UVA), User Threat Awareness (UTA) and User Security Practice (USP) questions as variables in the analysis.

5.5.1 Inferential Statistic

The study on Data Security in Mobile Phone Among University Students included 258 respondents in total. Obtaining a standard P-value is the first and most important step in an ANOVA analysis. If the P-value for the ANOVA test is significant, at least one group's mean has a statistically significant difference from the other groups' means. Therefore, we used IBM SPSS version 25, a statistical programme specialized for social science research, to carry out a One-Way ANOVA analysis. In this analysis, we used respondents' faculty as an independent variable to assess their awareness of three different levels of data security: User Vulnerability Awareness (UVA), User Threat Awareness (UTA) and User Security Practice (USP). With the goal of making this analysis easier, we coded the variable "faculty" as follows: "Fakulti Teknologi Maklumat dan Komunikasi (FTMK)" as 1, "Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP)" as 2, "Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE)" as 3, "Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT)" as 4, "Fakulti Kejuruteraan Pembuatan (FKP)" as 5, "Fakulti Kejuruteraan Mekanikal (FKM)" as 6, "Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK)" as 7 and "Fakulti Kejuruteraan Eletrik (FKE)" as 8.

5.5.2 User Vulnerability Awareness (UVA)

The study investigates the impact of various faculty in UTeM on six variables related to level of awareness and knowledge regarding potential risks or vulnerabilities related to mobile phone. These six variables are labeled as uva_information, uva_gather_data, uva_GPS, uva_assistant, uva_Bluetooth and uva_Wi-Fi. The findings obtained from the One-way ANOVA analysis are presented in the figure and table below.

No.	Question	Faculty	N	Mean	F	Sig.
1.	Are you concerned that some of your apps might be collecting information about you?	FTMK	86	4.35	2.404	**0.021**
		FTKMP	34	3.68		
		FTKEE	17	4.12		
		FPTT	29	4.38		
		FKP	17	4.24		
		FKM	25	**4.52**		
		FKEKK	25	4.20		
		FKE	25	4.28		
2.	Are you concerned that your social media applications gather a lot of your data.	FTMK	86	4.26	2.275	**0.029**
		FTKMP	34	3.68		
		FTKEE	17	4.24		
		FPTT	29	4.38		
		FKP	17	4.18		

		FKM	25	**4.56**		
		FKEKK	25	4.08		
		FKE	25	4.24		
3.	Are you concerned that GPS could be used to track your whereabouts?	FTMK	86	4.22	1.928	0.066
		FTKMP	34	3.68		
		FTKEE	17	4.29		
		FPTT	29	4.31		
		FKP	17	4.35		
		FKM	25	4.56		
		FKEKK	25	3.96		
		FKE	25	4.16		
4.	Are you concerned that your personal digital assistant, such as Siri, Hey Google, Bixby, etc., is constantly watching what's going on around it?	FTMK	86	3.87	2.371	**0.023**
		FTKMP	34	3.41		
		FTKEE	17	4.29		
		FPTT	29	4.10		
		FKP	17	4.12		
		FKM	25	**4.44**		
		FKEKK	25	3.88		

		FKE	25	4.08		
5.	Are you concerned that Bluetooth is vulnerable to the attacks? (For instance, a hacker may take over the phone and use it to read texts, send texts on behalf of the owner, make phone calls, and access the Internet.)	FTMK	86	3.80	1.399	0.206
		FTKMP	34	3.32		
		FTKEE	17	4.12		
		FPTT	29	4.07		
		FKP	17	4.12		
		FKM	25	3.92		
		FKEKK	25	3.92		
		FKE	25	3.96		
6.	Are you concerned about the public Wi-Fi where anyone can access the Internet via an unsecured, public Wi-Fi access point because it does not require a password.	FTMK	86	4.31	1.446	0.188
		FTKMP	34	3.68		
		FTKEE	17	4.29		
		FPTT	29	4.28		
		FKP	17	4.24		
		FKM	25	4.32		
		FKEKK	25	4.28		
		FKE	25	4.28		

*Table 5.5.2.1 ANOVA UVA Result, *p :< 0.05*

5.5.2.1 ANOVA Test Result

Based on the table 5.5.2.1, the one-way ANOVA result for the variable uva_information indicates that there was a statistically significant difference between the groups (F (7,250) = 2.404, p = 0.021). Variable uva_gather_data shows that there was statistically significant difference between group means as determined by one-way ANOVA (F (7,250) = 2.275, p = 0.029). Lastly, according to one-way ANOVA (F (7,250) = 2.371, p = 0.023), there was a statistically significant difference between group means, as indicated by the variable uva_assistant.

However, one-way ANOVA results (F (7,250) = 1.928, p = 0.066) indicate there were no statistically significant differences between group means, as indicated by the variable uva_GPS. One-way ANOVA results (F (7,250) = 1.399, p = 0.206) reveal that there were no statistically significant differences between group means, as indicated by the variable uva_Bluetooth. Lastly, one-way ANOVA results (F (7,250) = 1.446, p = 0.188) indicate that there was no statistically significant difference between the groups, as indicated by the variable uva_Wi-Fi. The lack of statistically significant differences suggests that there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees of vulnerability awareness in mobile phone among UTeM students.

Therefore, based on the preceding analysis, we can formulate the following hypothesis:

Hypothesis	Description
H0	The mean level of awareness and behaviour of 258 users is the same for the faculty groups Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP), Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE), Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT), Fakulti Kejuruteraan Pembuatan (FKP), Fakulti Kejuruteraan Mekanikal (FKM), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE).

H1	Group FKM exhibits a higher level of user vulnerability awareness (UVA) of application collect personal information are more aware of vulnerabilities in mobile phone.
H2	Group FKM exhibits a higher level of user vulnerability awareness (UVA) of social media applications gather a lot of data are more aware of vulnerabilities in mobile phone.
H3	Group FKM exhibits a higher level of user vulnerability awareness (UVA) of personal digital assistant watching the user environment are more aware of vulnerabilities in mobile phone.

Table 5.5.2.1.1 Hypothesis Result

- **H1: Group FKM exhibits a higher level of user vulnerability awareness (UVA) of application collect personal information are more aware of vulnerabilities in mobile phone.**

  Given that the p-value is 0.021, the finding demonstrates that the FKM group had the highest level of concerned regarding applications that collect their personal information. Accordingly, this analysis supports H1.

- **H2: Group FKM exhibits a higher level of user vulnerability awareness (UVA) of social media applications gather a lot of data are more aware of vulnerabilities in mobile phone.**

  Given that the p-value is 0.029, the finding demonstrates that the FKM group had the highest level of concerned social media gathering lot of data. Accordingly, this analysis supports H2.

- **H3: Group FKM exhibits a higher level of user vulnerability awareness (UVA) of personal digital assistant watching the user environment are more aware of vulnerabilities in mobile phone.**

  Given that the p-value is 0.023, the finding demonstrates that the FKM group had the highest level of concerned of personal digital assistant watching the user environment. Accordingly, this analysis supports H3.

5.5.3 User Threat Awareness (UTA)

The table below shows the findings of an ANOVA investigation into the effects of different faculty and eight data security variables on knowledge of potential threat and attack related to mobile phone.

No.	Question	Faculty	N	Mean	F	Sig.
1.	Are you concerned that malware attack such as viruses' worms, and Trojan horses, can attack electronic devices and cause damage, compromise security, and even result in hardware malfunctions and data loss?	FTMK	86	**4.37**	3.321	**0.002**
		FTKMP	34	3.47		
		FTKEE	17	4.12		
		FPTT	29	4.34		
		FKP	17	4.06		
		FKM	25	4.04		
		FKEKK	25	4.16		
		FKE	25	4.04		
2.	Are you concerned that a Bluetooth attack can exploit vulnerability related to access devices, intercept data, or carry out unwanted actions. For example, BlueBorne Attack.	FTMK	86	4.00	1.303	0.249
		FTKMP	34	3.47		
		FTKEE	17	3.76		
		FPTT	29	3.90		
		FKP	17	4.12		
		FKM	25	4.16		

		FKEKK	25	3.96		
		FKE	25	4.04		
3.	Are you concerned that Dolphin attack can target assistants like Siri, Google Assistant, and Amazon Alexa by taking use of ultrasonic frequencies that are undetectable to humans but difficult to be heard by the microphones of these gadgets.	FTMK	86	3.80	0.883	0.521
		FTKMP	34	3.41		
		FTKEE	17	3.88		
		FPTT	29	3.83		
		FKP	17	4.06		
		FKM	25	3.88		
		FKEKK	25	3.96		
		FKE	25	3.96		
4.	Are you concerned that Spyware is secretly installed on a system without the user's knowledge or agreement. Sensitive data about the user, such as their web surfing patterns, private information, login information is collected using Spyware.	FTMK	86	4.20	2.849	**0.007**
		FTKMP	34	3.35		
		FTKEE	17	4.00		
		FPTT	29	4.10		
		FKP	17	4.12		
		FKM	25	4.04		
		FKEKK	25	4.08		
		FKE	25	**4.32**		

5.	Are you concerned that Data leakage which the term used to describe the unauthorized transmittal of information or disclosure of information. It happens when unauthorised people access and share sensitive or confidential data in mobile phone.	FTMK	86	4.29	3.139	**0.003**
		FTKMP	34	3.44		
		FTKEE	17	3.94		
		FPTT	29	4.07		
		FKP	17	4.00		
		FKM	25	**4.32**		
		FKEKK	25	4.24		
		FKE	25	4.24		
6.	Are you concerned that Spoofing Attack might targeting your phone where a person, programme, website, or email poses as a trustworthy organisation or procedure in order to obtain sensitive data.	FTMK	86	4.17	2.010	0.054
		FTKMP	34	3.50		
		FTKEE	17	4.00		
		FPTT	29	3.86		
		FKP	17	4.06		
		FKM	25	4.08		
		FKEKK	25	4.24		
		FKE	25	4.28		
7.		FTMK	86	4.14		
		FTKMP	34	3.47		

	Are you concerned Data tampering attack might targeting your mobile phone where unknown parties purposefully alter, manipulate, delete, or amend data on a person's phone without the person's knowledge or agreement.	FTKEE	17	4.00	1.782	0.091
		FPTT	29	3.97		
		FKP	17	4.29		
		FKM	25	4.04		
		FKEKK	25	4.12		
		FKE	25	4.20		
8.	Are you concerned that Phishing attacks are attempts to fool and collect sensitive information, such as login passwords, credit card numbers, or personal information, through the use of fake emails, phone calls, or texts.	FTMK	86	4.20	1.914	0.068
		FTKMP	34	3.53		
		FTKEE	17	4.06		
		FPTT	29	3.97		
		FKP	17	4.29		
		FKM	25	4.16		
		FKEKK	25	4.08		
		FKE	25	4.32		

*Table 5.5.3.1 ANOVA UTA Result, *p :< 0.05*

5.5.3.1 ANOVA Test Result

Based on the table 5.5.3.1, the one-way ANOVA result for the variable uta_malware indicates that there was a statistically significant difference between the groups (F (7,250) = 3.321, p = 0.002). Variable uta_Spyware shows that there was statistically significant difference between group means as determined by one-way ANOVA (F (7,250) = 2.849, p = 0.007). Lastly, according to one-way ANOVA (F (7,250) = 3.139, p = 0.003), there was a

statistically significant difference between group means, as indicated by the variable uta_leakage.

However, one-way ANOVA results (F (7,250) = 1.303, p = 0.249) indicate there were no statistically significant differences between group means, as indicated by the variable uta_BlueBorne. One-way ANOVA results (F (7,250) = 0.883, p = 0.521) reveal that there were no statistically significant differences between group means, as indicated by the variable uta_Dolphin. Next, one-way ANOVA results (F (7,250) = 2.010, p = 0.054) indicate that there was no statistically significant difference between the groups, as indicated by the variable uta_Spoofing. One-way ANOVA results (F (7,250) = 1.782, p = 0.091) reveal that there were no statistically significant differences between group means, as indicated by the variable uta_tampering. Lastly, one-way ANOVA results (F (7,250) = 1.914, p = 0.068) indicate that there was no statistically significant difference between the groups, as indicated by the variable uta_Phishing. The lack of statistically significant differences suggests that there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees of threat awareness in mobile phone among UTeM students.

Therefore, based on the preceding analysis, we can formulate the following hypothesis:

Hypothesis	**Description**
H4	Group FTMK exhibits a higher level of user threat awareness (UTA) in malware attack are more aware of threat in mobile phone.
H5	Group FKE exhibits a higher level of user threat awareness (UTA) in Spyware attack are more aware of threat in mobile phone.
H6	Group FKM exhibits a higher level of user threat awareness (UTA) in Data Leakage are more aware of threat in mobile phone.

Table 5.5.3.1.1 Hypothesis Result

- **H4: Group FTMK exhibits a higher level of user threat awareness (UTA) in malware attack are more aware of threat in mobile phone.**

  Given that the p-value is 0.002, the finding demonstrates that the FTMK group had the highest level of concerned in Malware Attack in their mobile phone. Accordingly, this analysis supports H4.

- **H5: Group FKE exhibits a higher level of user threat awareness (UTA) in Spyware attack are more aware of threat in mobile phone.**

  Given that the p-value is 0.007, the finding demonstrates that the FKE group had the highest level of concerned in Spyware Attack in their mobile phone. Accordingly, this analysis supports H5.

- **H6: Group FKM exhibits a higher level of user threat awareness (UTA) in Data Leakage are more aware of threat in mobile phone.**

  Given that the p-value is 0.023, the finding demonstrates that the FKM group had the highest level of concerned in Data Leakage in their mobile phone. Accordingly, this analysis supports H6.

5.5.4 User Security Practices (USP)

The different faculty in UTeM with four variables regarding users concerned about applying security practices when using mobile phone. The ANOVA results are conveniently summarized in the table below for reference.

No.	Question	Faculty	N	Mean	F	Sig.
1.	How important is screen locking on mobile phones to you?	FTMK	86	4.70	2.570	**0.014**
		FTKMP	34	4.03		
		FTKEE	17	4.71		
		FPTT	29	4.59		
		FKP	17	4.59		

		FKM	25	**4.80**		
		FKEKK	25	4.64		
		FKE	25	4.36		
2.	How important to protect the data on your mobile phone with complicated passwords and passphrases?	FTMK	86	4.65	3.234	**0.003**
		FTKMP	34	3.97		
		FTKEE	17	4.65		
		FPTT	29	4.69		
		FKP	17	4.59		
		FKM	25	4.68		
		FKEKK	25	**4.80**		
		FKE	25	4.40		
3.	How important to clean off malware on your mobile phone?	FTMK	86	4.47	1.224	0.290
		FTKMP	34	3.97		
		FTKEE	17	4.59		
		FPTT	29	4.38		
		FKP	17	4.41		
		FKM	25	4.44		
		FKEKK	25	4.44		

		FKE	25	4.44		
4.	How important to install antivirus software on your mobile phone?	FTMK	86	4.24	1.138	0.340
		FTKMP	34	3.79		
		FTKEE	17	4.29		
		FPTT	29	4.45		
		FKP	17	4.12		
		FKM	25	4.36		
		FKEKK	25	4.24		
		FKE	25	4.08		

*Table 5.5.4.1 ANOVA USP Result, *p:< 0.05*

5.5.4.1 ANOVA Test Result

Based on the table 5.5.4.1, the one-way ANOVA result for the variable usp_screenlock indicates that there was a statistically significant difference between the groups (F (7,250) = 2.570, p = 0.014). Next, according to one-way ANOVA (F (7,250) = 3.234, p = 0.003), there was a statistically significant difference between group means, as indicated by the variable usp_passwords.

However, one-way ANOVA results (F (7,250) = 1.224, p = 0.290) indicate there were no statistically significant differences between group means, as indicated by the variable usp_clean_malware. Lastly, one-way ANOVA results (F (7,250) = 1.138, p = 0.340) indicate that there was no statistically significant difference between the groups, as indicated by the variable usp_antivirus. The lack of statistically significant differences suggests that there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees of security practices in mobile phone among UTeM students.

Therefore, based on the preceding analysis, we can formulate the following hypothesis:

Hypothesis	Description
H7	Group FKM exhibits a higher level of user security practices (USP) in using a screen lock are more aware of data security in mobile phone.
H8	Group FKEKK exhibits a higher level of user security practices (USP) in forming complicated password and paraphrases are more aware of data security in mobile phone.

Table 5.5.4.1.1 Hypothesis Result

- **H7: Group FKM exhibits a higher level of user security practices (USP) in using a screen lock are more aware of data security in mobile phone**

  Given that the p-value is 0.014, the finding demonstrates that the FKM group had the highest in knowing to use a screen lock on their mobile phone. Accordingly, this analysis supports H7.

- **H8: Group FKEKK exhibits a higher level of user security practices (USP) in forming complicated password and paraphrases are more aware of data security in mobile phone.**

  Given that the p-value is 0.003, the finding demonstrates that the FKEKK group had the highest in knowing to form a complicated password and paraphrases on their mobile phone. Accordingly, this analysis supports H8.

5.6 Vulnerabilities Behaviour Assessment Analysis

Section C of the questionnaire is dedicated to the measurement of Vulnerabilities Behaviour. In Appendix C2, the respondents' data pertaining to inquiries designed to assess their behavioural tendencies. These responses aim to gauge how these behaviours might impact the how vulnerable certain devices are to security flaws. The independent variable for this analysis was the respondents' faculty, while the test considered four sub-sections: Perceived Risk (PR), Secondary Utilisation of Personal Data (SUPD), Competence (C), and Trust (T) as variables under examination.

5.6.1 Inferential Statistic

A total of 258 respondents successfully completed the study on Data Security in Mobile Phone Among University Students. The analysis involved conducting a One-way ANOVA using statistical software, specifically IBM SPSS version 25, tailored for social sciences. In this examination, faculty served as the independent variable to assess four distinct perspectives of respondents' behavior. Furthermore, the faculty variable was categorized as follows: "Fakulti Teknologi Maklumat dan Komunikasi (FTMK)" as 1, "Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP)" as 2, "Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE)" as 3, "Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT)" as 4, "Fakulti Kejuruteraan Pembuatan (FKP)" as 5, "Fakulti Kejuruteraan Mekanikal (FKM)" as 6, "Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK)" as 7 and "Fakulti Kejuruteraan Eletrik (FKE)" as 8 for the purpose of coding.

5.6.2 Perceived Risk (PR)

Faculty was considered alongside seven variables related to perceiving risk from a perceptual perspective. The ANOVA results for this analysis are presented in table below.

No.	Question	Faculty	N	Mean	F	Sig.
1.	I believe that my mobile phone's location sometimes is tracked by the GPS.	FTMK	86	4.20	1.237	0.283
		FTKMP	34	3.74		
		FTKEE	17	4.41		
		FPTT	29	4.34		
		FKP	17	4.24		
		FKM	25	4.08		
		FKEKK	25	4.12		
		FKE	25	4.08		
2.	I believe that mobile apps were gathering too much data about me.	FTMK	86	4.17	1.327	0.238
		FTKMP	34	3.76		
		FTKEE	17	4.29		
		FPTT	29	4.34		
		FKP	17	4.06		
		FKM	25	4.32		
		FKEKK	25	3.96		

		FKE	25	4.28		
3.	I believe other people knows more about my daily life due to always using the social media.	FTMK	86	3.62	0.950	0.469
		FTKMP	34	3.74		
		FTKEE	17	4.00		
		FPTT	29	3.83		
		FKP	17	3.71		
		FKM	25	4.16		
		FKEKK	25	3.56		
		FKE	25	4.08		
4.	I believe that using mobile apps has made my privacy information more easily accessible to others.	FTMK	86	4.14	1.021	0.417
		FTKMP	34	3.79		
		FTKEE	17	4.18		
		FPTT	29	4.24		
		FKP	17	4.18		
		FKM	25	4.40		
		FKEKK	25	3.96		
		FKE	25	4.16		
		FTMK	86	4.19		

5.	I believe that since I use mobile apps, there is confidential information that might be utilised to invade my privacy.	FTKMP	34	3.82	1.627	0.128
		FTKEE	17	4.18		
		FPTT	29	4.31		
		FKP	17	4.24		
		FKM	25	4.48		
		FKEKK	25	3.84		
		FKE	25	4.32		
6.	How likely do you think it is that someone will read the private communications you sent?	FTMK	86	3.55	0.462	0.861
		FTKMP	34	3.47		
		FTKEE	17	3.82		
		FPTT	29	3.59		
		FKP	17	3.82		
		FKM	25	3.72		
		FKEKK	25	3.32		
		FKE	25	3.64		

7.	How likely are you aware that unauthorised individuals could use your smartphone to access information about your online activities?	FTMK	86	3.74	0.658	0.707
		FTKMP	34	3.59		
		FTKEE	17	4.00		
		FPTT	29	3.72		
		FKP	17	4.18		
		FKM	25	3.88		
		FKEKK	25	3.52		
		FKE	25	3.76		

*Table 5.6.2.1 ANOVA PR Result, *p :< 0.05*

5.6.2.1 ANOVA Test Result

Based on table 5.6.2.1 above, the one-way ANOVA results (F (7,250) = 1.237, p = 0.283) indicate there were no statistically significant differences between group means, as indicated by the variable pr_tracked. One-way ANOVA results (F (7,250) = 1.327, p = 0.283) reveal that there were no statistically significant differences between group means, as indicated by the variable pr_apps. Next, one-way ANOVA results (F (7,250) = 0.950, p = 0.469) indicate there were no statistically significant differences between group means, as indicated by the variable pr_daily. One-way ANOVA results (F (7,250) = 1.021, p = 0.417) reveal that there were no statistically significant differences between group means, as indicated by the variable pr_privacy. Besides, for variable pr_utilized one-way ANOVA results is (F (7,250) = 1.627, p = 0.128) indicate there were no statistically significant differences between group means. Moving to next variable, one-way ANOVA results (F (7,250) = 0.462, p = 0.861) reveal that there were no statistically significant differences between group means, as indicated by the variable pr_privatecom. Lastly, one-way ANOVA results (F (7,250) = 0.658, p = 0.707) indicate that there was no statistically significant difference between the groups, as indicated by the variable pr_unauthorized. The lack of statistically significant differences suggests that

there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees in perceived risk in mobile phone among UTeM students.

5.6.3 Secondary Utilisation of Personal Data

Faculty, along with five variables related to users concerned about whether their personal information is being used by mobile application, has been examined. The ANOVA results for this analysis are displayed in the table 5.6.3.1 below.

No.	Question	Faculty	N	Mean	F	Sig.
1.	I believe that mobile applications might utilise my personal data for other purposes without notifying me.	FTMK	86	3.99	0.827	0.566
		FTKMP	34	3.82		
		FTKEE	17	4.06		
		FPTT	29	4.07		
		FKP	17	3.88		
		FKM	25	4.24		
		FKEKK	25	3.68		
		FKE	25	4.12		
2.	I believe that I am asked for too much personal information when purchasing.	FTMK	86	3.84	1.398	0.207
		FTKMP	34	3.68		
		FTKEE	17	4.47		
		FPTT	29	4.00		
		FKP	17	4.06		

		FKM	25	4.08		
		FKEKK	25	3.84		
		FKE	25	4.12		
3.	I believe that unauthorised individuals using my smartphone to access information about my online activities.	FTMK	86	3.73	1.768	0.094
		FTKMP	34	3.76		
		FTKEE	17	4.35		
		FPTT	29	3.97		
		FKP	17	3.88		
		FKM	25	4.16		
		FKEKK	25	3.68		
		FKE	25	4.32		
4.	I believe that individuals on the internet are not who they claim to be.	FTMK	86	4.16	1.695	0.111
		FTKMP	34	3.76		
		FTKEE	17	4.59		
		FPTT	29	3.93		
		FKP	17	4.12		
		FKM	25	3.96		
		FKEKK	25	3.80		

		FKE	25	4.12		
5.	I believe that online organisation on the internet is not who they claim to be.	FTMK	86	4.13	2.234	**0.032**
		FTKMP	34	3.68		
		FTKEE	17	**4.65**		
		FPTT	29	3.86		
		FKP	17	4.18		
		FKM	25	4.08		
		FKEKK	25	3.80		
		FKE	25	4.04		

*Table 5.6.3.1 ANOVA SUPD Result, *p :< 0.05*

5.6.3.1 ANOVA Test Result

Based on the table 5.6.3.1, the one-way ANOVA result for the variable supd_organization indicates that there was a statistically significant difference between the groups (F (7,250) = 2.234, p = 0.032).

However, one-way ANOVA results (F (7,250) = 0.827, p = 0.566) indicate there were no statistically significant differences between group means, as indicated by the variable supd_utilize. One-way ANOVA results (F (7,250) = 1.398, p = 0.207) reveal that there were no statistically significant differences between group means, as indicated by the variable supd_much_info. Next, one-way ANOVA results (F (7,250) = 1,768, p = 0.094) indicate that there was no statistically significant difference between the groups, as indicated by the variable supd_smartphone. Lastly, one-way ANOVA results (F (7,250) = 1.695, p = 0.111) indicate that there was no statistically significant difference between the groups, as indicated by the variable supd_claim. The lack of statistically significant differences suggests that there is no strong

evidence to conclude that the different faculty groups exhibit noticeably different degrees of secondary utilisation of personal data in mobile phone among UTeM students.

Therefore, based on the preceding analysis, we can formulate the following hypothesis:

Hypothesis	Description
H9	Group FTKEE exhibits a higher level of secondary utilisation of personal data (SUPD) believing that online organisation on the internet is not who they claim to be are more aware of data security in mobile phone.

Table 5.6.3.1.1 Hypothesis Result

- **H9: Group FTKEE exhibits a higher level of secondary utilisation of personal data (SUPD) believing that online organisation on the internet is not who they claim to be are more aware of data security in mobile phone.**

  Given that the p-value is 0.032, the finding demonstrates that the FTKEE group had the highest level of doubting online organisation on the internet in their mobile phone. Accordingly, this analysis supports H9.

5.6.4 Competence (C)

Faculty was considered alongside five variables related to Users' competency of securing their personal data on mobile phone. The ANOVA results for this analysis are presented in Table 5.6.4.1 below.

No.	Question	Faculty	N	Mean	F	Sig.
1.	My mobile phone used VPN (Virtual Private Network) to secure my connection on my mobile phone.	FTMK	86	3.48	0.728	0.648
		FTKMP	34	3.32		
		FTKEE	17	3.71		
		FPTT	29	3.72		

		FKP	17	3.76		
		FKM	25	3.88		
		FKEKK	25	3.32		
		FKE	25	3.60		
2.	My mobile phone is configured with security services so that no one can identify me while browsing the Internet.	FTMK	86	3.64	1.402	0.205
		FTKMP	34	3.56		
		FTKEE	17	4.24		
		FPTT	29	3.86		
		FKP	17	3.71		
		FKM	25	3.96		
		FKEKK	25	3.44		
		FKE	25	4.00		
3.	I sign out from my Personal Account after I used my mobile phone.	FTMK	86	2.98	2.473	**0.018**
		FTKMP	34	3.29		
		FTKEE	17	**4.24**		
		FPTT	29	3.52		
		FKP	17	2.88		
		FKM	25	3.28		

		FKEKK	25	2.68		
		FKE	25	3.32		
4.	I always read Application's Privacy and Policy before installed an application.	FTMK	86	3.06	1.472	0.177
		FTKMP	34	3.47		
		FTKEE	17	3.94		
		FPTT	29	3.48		
		FKP	17	3.41		
		FKM	25	3.52		
		FKEKK	25	3.00		
		FKE	25	3.60		
5.	I used Biometric Authentication such as fingerprint, and face ID for my lock screen on mobile phone.	FTMK	86	4.45	2.332	**0.025**
		FTKMP	34	3.76		
		FTKEE	17	**4.71**		
		FPTT	29	4.55		
		FKP	17	4.47		
		FKM	25	4.28		
		FKEKK	25	4.28		
		FKE	25	4.24		

*Table 5.6.4.1 ANOVA C Result, *p :< 0.05*

5.6.4.1 ANOVA Test Result

Based on the table 5.6.4.1, the one-way ANOVA result for the variable c_signout indicates that there was a statistically significant difference between the groups (F (7,250) = 2.473, p = 0.018). Next, according to one-way ANOVA (F (7,250) = 2.332, p = 0.025), there was a statistically significant difference between group means, as indicated by the variable c_Biometric.

However, one-way ANOVA results (F (7,250) = 0.728, p = 0.648) indicate there were no statistically significant differences between group means, as indicated by the variable c_VPN. Next, one-way ANOVA results (F (7,250) = 1.402, p = 0.205) indicate there were no statistically significant differences between group means, as indicated by the variable c_configured. Lastly, one-way ANOVA results (F (7,250) = 1.472, p = 0.177) indicate that there was no statistically significant difference between the groups, as indicated by the variable c_read. The lack of statistically significant differences suggests that there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees of competence in mobile phone among UTeM students.

Therefore, based on the preceding analysis, we can formulate the following hypothesis:

Hypothesis	Description
H10	Group FTKEE exhibits a higher level of competence (C) in signing out from personal account after used are more aware of data security in mobile phone.
H11	Group FTKEE exhibits a higher level of competence (C) in using biometric authentication are more aware of data security in mobile phone.

Table 5.6.4.1.1 Hypothesis Result

- **H10: Group FTKEE exhibits a higher level of competence (C) in signing out from personal account after used are more aware of data security in mobile phone.**

  Given that the p-value is 0.018, the finding demonstrates that the FTKEE group had the highest in knowing to sign out from their personal account after used it on their mobile phone. Accordingly, this analysis supports H10.

- **H11: Group FTKEE exhibits a higher level of competence (C) in using biometric authentication are more aware of data security in mobile phone.**

  Given that the p-value is 0.025, the finding demonstrates that the FTKEE group had the highest in knowing to use biometric authentication on their mobile phone. Accordingly, this analysis supports H11.

5.6.5 Trust (T)

Faculty and five variables regarding users' belief or confidence of their mobile phone itself. The results obtained through ANOVA are displayed in table below.

No.	Question	Faculty	N	Mean	F	Sig.
1.	I believe that when I use my mobile phone to connect to Wi-Fi network, it is important to make sure connecting only to encrypted, password-protected networks.	FTMK	86	4.31	1.341	0.232
		FTKMP	34	3.82		
		FTKEE	17	4.35		
		FPTT	29	4.45		
		FKP	17	4.12		
		FKM	25	4.28		
		FKEKK	25	4.16		
		FKE	25	4.28		

2.	I believe mobile phone is a trusted gadget because of its trustworthy functionality, strong security features, and security precautions.	FTMK	86	4.01	1.033	0.409
		FTKMP	34	3.65		
		FTKEE	17	4.18		
		FPTT	29	4.28		
		FKP	17	4.00		
		FKM	25	4.16		
		FKEKK	25	3.96		
		FKE	25	4.04		
3.	I believe that mobile phone security can be improved by using antivirus software, hardware encryption, data transfer encryption, and physical device security.	FTMK	86	4.26	1.436	0.191
		FTKMP	34	3.79		
		FTKEE	17	4.24		
		FPTT	29	4.34		
		FKP	17	4.41		
		FKM	25	4.28		
		FKEKK	25	4.12		
		FKE	25	4.44		
		FTMK	86	4.35		
		FTKMP	34	3.79		

4.	I believe that mobile phone holds our important personal information such as photos and videos, SMS, email, contact list and social media accounts.	FTKEE	17	4.24	2.365	**0.023**
		FPTT	29	**4.48**		
		FKP	17	4.29		
		FKM	25	4.40		
		FKEKK	25	3.92		
		FKE	25	4.44		
5.	I believe that before installing application, I must read through application's phone access permissions so that my mobile phone will no affected by malware.	FTMK	86	4.33	2.388	**0.022**
		FTKMP	34	3.71		
		FTKEE	17	4.18		
		FPTT	29	**4.48**		
		FKP	17	3.88		
		FKM	25	4.24		
		FKEKK	25	4.12		
		FKE	25	**4.48**		

*Table 5.6.5.1 ANOVA T Result, *p :< 0.05*

5.6.5.1 ANOVA Test Result

Based on the table 5.6.5.1, the one-way ANOVA result for the variable t_SMS indicates that there was a statistically significant difference between the groups (F (7,250) = 2.365, p = 0.023). Next, the one-way ANOVA result for the variable t_read indicates that there was a statistically significant difference between the groups (F (7,250) = 2.388, p = 0.022).

However, the one-way ANOVA results (F (7,250) = 1.341, p = 0.232) indicate there were no statistically significant differences between group means, as indicated by the variable t_encrypted. Besides, one-way ANOVA results (F (7,250) = 1.033, p = 0.409) reveal that there were no statistically significant differences between group means, as indicated by the variable t_trusted. Lastly, one-way ANOVA results (F (7,250) = 1.436, p = 0.191) indicate that there was no statistically significant difference between the groups, as indicated by the variable t_improved. The lack of statistically significant differences suggests that there is no strong evidence to conclude that the different faculty groups exhibit noticeably different degrees of trust in mobile phone among UTeM students.

5.6.5.2 Post-Hoc Test Analysis

Given the similarity in mean values for Fakulti Pengurusan Teknologi dan Teknousahawan (FPTT) and Fakulti Kejuruteraan Eletrik (FKE) which is 4.48, post-hoc tests are performed to unveil precise nuances between the two faculties. These tests contribute depth and detail to the analysis by discerning between statistically significant differences and those that may not have practical significance. The Post- Hoc test that being used in this analysis Tukey's Honestly Significant Difference (Tukey HSD). The Tukey HSD test is a post-hoc analysis technique that is frequently used to determine the significance of differences between pairs of group averages. The result of post-hoc analysis between these two faculties is shown in table below.

Faculty (I)	Faculty (J)	Mean Difference (I-J)	Sig.
Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT)	Fakulti Kejuruteraan Eletrik (FKE)	0.003	1.000
Fakulti Kejuruteraan Eletrik (FKE)	Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT)	-0.003	1.000

Table 5.6.5.2.1 Post-Hoc Analysis Result

Based on table 5.6.5.*2*.1 above, the post-hoc analysis of the mean differences between Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT) and Fakulti Kejuruteraan Eletrik (FKE) does not reveal any statistically significant distinctions. Both directions of the comparison yield a negligible mean difference of 0.003 with a p-value of 1.000, signifying that there is no significant variance in the measured parameter between these two faculties. Thus, this analysis did not find sufficient evidence to reject the null hypothesis.

5.7 ANOVA Analysis Summary

Table 5.7.1 shows the summary of the ANOVA analysis result. It shows the faculty with the highest knowledge and awareness within the variable given through the online survey research. This table is divided by six (6) sections which are Sub-section, Faculty, Variable, F Value, Sig. Value and Mean Value.

Sub- section	Faculty	Variable	F	Sig.	Mean
User Vulnerability Awareness (UVA)	Fakulti Kejuruteraan Mekanikal (FKM)	uva_information	2.404	0.021	4.52
		uva_gather_data	2.275	0.029	4.56
		uva_assistant	2.371	0.023	4.44
User Threat Awareness (UTA)	Fakulti Teknologi Maklumat dan Komunikasi (FTMK)	uta_malware	3.321	0.002	4.37
	Fakulti Kejuruteraan Eletrik (FKE)	uta_Spyware	2.849	0.007	4.32
	Fakulti Kejuruteraan Mekanikal (FKM)	uta_leakage	3.139	0.003	4.32
User Security Practice (USP)	Fakulti Kejuruteraan Mekanikal (FKM)	usp_screenlock	2.570	0.014	4.80
	Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK)	usp_password	3.234	0.003	4.80
Secondary Utilisation of Personal Data (SUPD)	Fakulti Teknologi Kejuruteraan Eletrik Elektronik (FTKEE)	supd_organization	2.234	0.032	4.65
Competence (C)	Fakulti Teknologi Kejuruteraan Eletrik Elektronik (FTKEE)	c_signout	2.473	0.018	4.24
		c_Biometric	2.332	0.025	4.71

Table 5.7.1 ANOVA Analysis Summary

Based on table 5.7.1 above, FTMK and FKEKK are considered IT faculties, while the FKM, FKE and FTKEE are designated as non-IT faculties. In the summary table, the level of awareness regarding data security in mobile phone among university students from Fakulti Kejuruteraan Mekanikal (FKM) state the highest level of awareness with the highest mean value in five (5) variables. The five variables are uva_information, uva_gather_data, uva_assistant, uta_leakage and usp_screenlock. Next, Fakulti Teknologi Kejuruteraan Eletrik Elektronik (FTKEE) ranked number two as the highest level of awareness in this research study for variable supd_organization, c_signout and c_Biometric. Lastly, Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) and Fakulti Kejuruteraan Eletrik (FKE) has the highest knowledge in variable uta_malware, usp_password and uta_Spyware. These results highlight the differing levels of data security awareness among university students in various faculties, highlighting the particular strengths and areas of specialisation of each department in this field.

A more comprehensive perspective, it is worth emphasizing that FKM, FTKEE, and FKE despite not being traditionally designated as IT faculties, have showcased a commendable level of awareness regarding data security in mobile phones. This attributed to their collective emphasis on cultivating a conscientious and resolute mindset when it comes to addressing cybercrime activities in the cyber world. Their proactive efforts in knowing a basic cybersecurity education and fostering a strong sense of determination among the students have undoubtedly contributed to their high levels of awareness regarding data security in mobile phone among UTeM students.

5.8 Summary of Chapter 5

Finally, the findings that follows offers a thorough reason for a better understanding of the outcome analysis is explained in this chapter. Moreover, the upcoming chapter will elaborate on the study's conclusions and present the recommendations and contribution based on the research outcomes. This transition from the findings to the conclusions and suggestions chapter is essential for providing a holistic understanding of the study's implications and actionable insights.

CHAPTER 6: CONCLUSION AND FUTURE RECOMMENDATION

6.1 Introduction

The examination of data security awareness in mobile phones among university students is undertaken with a specific focus on those enrolled in a technical university which is Universiti Teknikal Malaysia Melaka (UTeM) students. Encompassing both IT-literate and non-IT-literate students, it is crucial to note that despite their varying levels of technical expertise, all respondents share a common educational background rooted in a technical or IT-centric environment. Thus, both IT-literate and non-IT-literate students exhibit a comparable level of awareness concerning data security in mobile phones.

6.2 Project Summarization

The research study that has been conducted is to analyze the awareness of university student regarding the Data Security. Following the three (3) goals for carrying out this research study are PO_1, PO_2 and PO_3. The project objective for PO_1 is to study the level of awareness of university students. The project objective of PO_2 is to analyze the understanding of security on mobile phone among university students. Finally, the last objective of PO_3 is to compare the level of awareness among IT students and non-IT students.

Furthermore, the problem statements from PS_1, PS_2 and PS_3 have been the motivation for carrying out this research investigation. The first problem statement, PS_1 is university students unaware of the potential consequences of mobile security breaches, such as identity theft, financial lost and damages to their reputation. Next, the second problem statement, PO_2 is university students not taking an adequate precaution to protect themselves from mobile security threats such as malware and phishing. Following the last problem statement, PO_3 is the level of understanding for university students is not much as an IT expert for them to know the threats. Therefore, the research study was directed to fulfil those three primary project goals in order to enhance the awareness of data security among university students no matter what their major is.

Lastly, the study was conducted through an online survey, with the first component used to determine the respondent's demographics. Secondly, measuring the level of awareness

among university students, and the third measuring the vulnerability behaviours assessment. Three (3) levels of sub-categories which are User Vulnerability Awareness (UVA), User Threat Awareness (UTA) and User Security Practices (USP) that make up the first measurement of degree of knowledge among university students about data security in mobile phones. The other component has four (4) subcategories that will assess the respondent's perceptual perspective which are Perceived Risk (PR), Secondary Utilisation of Personal Data (SUPD), Competence (C) and Trust (T). The Trust (T) will then be used to gauge respondents' belief or confidence of their mobile phone.

6.3 Project Contribution

The findings of this study of research are intended to increase awareness among university students of the essential significance of data security in mobile phone usage. In fact, this study encourages safe mobile phone usage among university students and improves data security awareness. University students especially UTeM students are better able to handle confidential and personal information because of their increased awareness through this online survey research.

Additionally, this research study considerably deepens the understanding of data security awareness in the context of academic research, especially among the university students. Future researchers in the field can use this newly discovered information as a valuable resource, advancing scholarly work in this significant field.

Lastly, this online research survey may influence behavior change models, encouraging safer mobile phone usage practices and contributing to interdisciplinary collaboration among students in IT literate or non-IT literate. As a result, this study represents an important contribution to the fields of data security, education, and statistical analysis because it has the potential to benefit both the researcher and the respondents.

6.4 Future Recommendation

Future research endeavors in this field ought to encompass all universities across Malaysia, both government-funded and privately-run institutions, to ensure comprehensive insights that transcend institutional boundaries. Given the differences between IT students and non-IT students, this inclusive approach has the potential to uncover unique and valuable nuances in data security awareness among university students. The rationale behind this recommendation lies in the current observations, where the collected data reveals a conspicuous lack of differentiation in awareness levels among these two student groups, IT and non-IT, emphasizing the significance of such research initiatives that span the entire Malaysian higher education landscape. Lastly, the study also recommended that the findings and insights garnered from this study be disseminated to the general public, with a particular emphasis on reaching individuals from diverse income generations. This proactive approach to knowledge sharing can empower people from various economic backgrounds with the information and awareness necessary to navigate the complex landscape of data security in mobile phone effectively.

6.5 Summary of Chapter 6

In summary, this research comprehensively analyzes the level of awareness and knowledge among university regarding the topic data security in mobile phone. The study examines how university students are aware of their personal information and threats when using mobile devices, including their understanding, viewpoints, and practices. Lastly, this research culminates by offering valuable recommendations for the future researcher to improve the research among university students across Malaysia.

REFERENCES

Moletsane, T. and Tsibolane, P. (2020) 'Mobile Information Security Awareness among students in Higher Education: An exploratory study', *2020 Conference on Information Communications Technology and Society (ICTAS)* [Preprint]. doi:10.1109/ictas47918.2020.233978.

Priambodo, D.F. et al. (2022) 'Mobile Health Application Security Assessment based on OWASP top 10 mobile vulnerabilities', 2022 International Conference on Information Technology Systems and Innovation (ICITSI) [Preprint]. doi:10.1109/icitsi56531.2022.9970949.

King, E. E. (2021). Bring your own device security awareness and security behaviour: A quantitative explanatory. Ph. D Thesis, Capella University.

Bibeau, R. (2011). Mobile data security: Research and analysis of mobile data security with emphasis on mobile public safety users. Master's dissertation, The College of St. Scholastica.

Irwan, Asnar, Y. and Hendradjaya, B. (2015) 'Confidentiality and privacy information security risk assessment for Android-based mobile devices', 2015 International Conference on Data and Software Engineering (ICoDSE) [Preprint]. doi:10.1109/icodse.2015.7436972.

Scott, S. (2006). Mobile phone usage amongst teenagers: An analysis of research methods specific to teenage mobile phone use. Ph. D Thesis, University of Glasgow Faculty of Information and Mathematical Sciences Department of Computing Science.

Zheng, H., Li, D. and Gao, Z. (2006) 'An epidemic model of mobile phone virus', 2006 First International Symposium on Pervasive Computing and Applications [Preprint]. doi:10.1109/spca.2006.297477.

McGovern Cole, E. L. (2019). An Exploratory Study: The Knowledge Gaps of Smartphone Security Between Users and IT Security Professionals in the Emerging BYOD Environment. Ph. D Thesis, B.S. Information Technology and Information Security Systems, University of Phoenix.

George, O. (2019). The Impact of Mobile Devices in Higher Education: Student Perceptions on the Advantages and Disadvantages. Ph. D Thesis, Wilmington University.

White, T. (2020). IT Managers' and IT Professionals' Mobile Device Security Strategies: A Qualitative Exploratory Case Study. Ph. D Thesis, University of Phoenix.

McCray, K. L. (2023). Vulnerabilities and Threats in Mobile Banking that Financial Institutions Must Understand to Reduce Mobile Banking Fraud. Ph. D Thesis, College of Business, Innovation, Leadership, and Technology, Marymount University.

Khokhlov, I. and Reznik, L. (2018) 'Android System Security Evaluation', 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) [Preprint]. doi:10.1109/ccnc.2018.8319325.

Sun, Z. (2021). Understanding and Defending against the Security Threats on Mobile and IoT Devices. Ph. D Thesis, Northeastern University Boston, Massachusetts.

Sletten, M. A. (2020). Security in a Mobile Learning Environment. Ph. D Thesis, University of Illinois at Urbana-Champaign, Urbana, Illinois.

Liao, M. (2012). Bluetooth vulnerabilities in data security of mobile phones. Master dissertation, Purdue University West Lafayette, Indiana.

InspiringApps, Inc [Online] Available: https://www.inspiringapps.com/Blog/92/mobile-device-security-data-protection-on-i-os-and-android/ .

VMWare, Inc [Online] Available: https://www.vmware.com/topics/glossary/content/mobile-device security.html#:~:text=Mobile%20Device%20Security%20refers%20to,from%20accessing%20the%20enterprise%20network.

Ngoqo, B. and Flowerday, S.V. (2015). 'Information security behaviour profiling framework (ISBPF) for student mobile phone users', Computers & Security, 53, pp. 132–142. doi:10.1016/j.cose.2015.05.011.

Alshalan, A., Pisharody, S. and Huang, D. (2016). ‘A survey of Mobile VPN Technologies’, IEEE Communications Surveys & Tutorials, 18(2), pp. 1177–1196. doi:10.1109/comst.2015.2496624.

Ravindran, R.S., Huang, C. and Thulasiraman, K. (2007). ‘Managed dynamic VPN service: Core Capacity Sharing Schemes for improved VPN performance’, 2007 IEEE International Conference on Communications [Preprint]. doi:10.1109/icc.2007.43.

Inoue, A., Saito, M. and Iwashita, M. (2015). ‘Behavior analysis on mobile-carrier choice & Mobile-Phone Purchase’, 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence [Preprint]. doi:10.1109/acit-csi.2015.79.

Riola, P. A. (2014). Examining Smartphone Security Behavior of College Students. In Google Books. Northcentral University. https://books.google.com.my/books/about/Examining_Smartphone_Security_Behavior_o.html?id=z7n2oAEACAAJ&redir_esc=y .

Hair, J.F. (2019) Multivariate Data Analysis. Andover, Hampshire: Cengage.

Chen, Y. (2007). The mobile phone and socialization: The consequences of mobile phone use in transitions from family to school life of U.S. college students. Ph. D Thesis, Rutgers, The State University of New Jersey. [Preprint].

Fook, C.Y. et al. (2022). ‘The mediating effect of academic behaviour towards mobile phone use and intention for mobile learning among university students’, 2022 International Conference on Engineering and Emerging Technologies (ICEET) [Preprint]. doi:10.1109/iceet56468.2022.10007290.

Shonola, S.A. and Joy, M.S. (2014). ‘Mobile learning security concerns from university students’ Perspectives’, 2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014) [Preprint]. doi:10.1109/imctl.2014.7011125.

Zhang, S. and Costa, S. (2016). ‘A survey study of young generation’s mobile phone usage and security concerns’, 2016 17th International Conference on Parallel and Distributed

Computing, Applications and Technologies (PDCAT) [Preprint]. doi:10.1109/pdcat.2016.075.

Linh, V.H. (2022). 'Determinants of Vietnamese farmers' intention to adopt Ecommerce platforms for fresh produce retail: An integrated toe-TAM framework', International Journal of Social Science and Human Research, 05(03). doi:10.47191/ijsshr/v5-i3-16.

Cooper, C. (2014). Smartphone privacy perceptions and behaviors generational influence quantitative analysis: Communications privacy management theory. Master dissertation, Colorado Technical University [Preprint].

Amin, M. et al. (2021). 'Security and privacy awareness of smartphone users in Indonesia', Journal of Physics: Conference Series, 1882(1), p. 012134. doi:10.1088/1742-6596/1882/1/012134.

Winters, B. (2019). Smartphone security: A quantitative analysis of security usage and outcomes. Ph. D Thesis, Colorado Technical University. [Preprint].

APPENDIX A

PILOT QUESTIONNAIRE FIRST DRAFT

Study On Data Security Awareness in Mobile Phone Usage Among University Student Using Statistical Analysis

Section A: Demographic

For each question, please mark (/) or fill in the blanks in the related information.

Validation	
No.	Comment
1	
Citation	
(Sletten, M. A., 2020)	

1. Gender:

   Male ☐ Female ☐

2. Age:

   18-20 ☐ 24-30 ☐

   21-24 ☐

3. Which faculty in UTeM you belong?

   Fakulti Kejuruteraan Eletrik (FKE) ☐

   Fakulti Kejuruteraan Pembuatan (FKP) ☐

   Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) ☐

   Fakulti Teknologi Maklumat dan Komunikasi (FTMK) ☐

   Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT) ☐

   Fakulti Kejuruteraan Mekanikal (FKM) ☐

   Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE) ☐

   Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP) ☐

Validation	
No.	Comment
2	
Citation	
(Sletten, M. A., 2020)	

Validation	
No.	Comment
3	

4. What year are you in?

   Year One ☐

   Year Two ☐

   Year Three ☐

   Year Four ☐

Validation	
No.	Comment
4	

5. What is your marital status?

   Single ☐

   Married ☐

   Other ☐

Validation	
No.	Comment
5	
Citation	
(Sletten, M. A., 2020)	

6. What brand of mobile phone you are using?

   Android ☐

   Apple ☐

Validation	
No.	Comment
6	
Citation	
(Sletten, M. A., 2020)	

7. Do you have any social media application installed in your mobile phone?

   Yes ☐

   No ☐

Validation	
No.	Comment
7	
Citation	
(Sletten, M. A., 2020)	

For question number 8, please (/) for relevant information. You can choose more than one answer.

8. If so, which social media applications do you have installed on your mobile phone?

Facebook ☐

Instagram ☐

TikTok ☐

LinkedIn ☐

Twitter ☐

Snapchat ☐

WhatsApp ☐

Others (please specify) ☐

Yes/ No	Comment
Citation	
(Sletten, M. A., 2020)	

Section B: Level of Awareness Among University Students

These questions assess the degree of knowledge among university students about data security in mobile phones. This part attempts to compile information that assists in evaluating the students' current comprehension of data security precautions and their awareness as mobile phone users.

User Vulnerability Awareness Please select the response that best represents how much of each statement applies to you: *Scoring: Not Concerned = 1; Slightly Concerned = 2; Neutral = 3; Very Concerned = 4; Extremely Concerned = 5*							Validation		Citation
							Yes/ No	Comment	
1	Are you worried that some of your apps might be collecting information about you?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
2	Social media application gathers a lot of data on the user. What do you think about this?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
3	Are you concerned that GPS could be used to track your whereabouts?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
4	Do you ever worry that your personal digital assistant, such as Siri, Hey Google, Bixby, etc., is constantly watching what's going on around it?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

5	Do you aware that Bluetooth is vulnerable to the mentioned attacks? (For instance, a hacker may take over the phone and use it to read texts, send texts on behalf of the owner, make phone calls, and access the Internet.)	1	2	3	4	5			(McGovern Cole, E. L., 2019)
6	Anyone can access the Internet via an unsecured, public Wi-Fi access point because it does not require a password. Are you aware about the public Wi-Fi?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
User Threat Awareness Please select the response that best represents how much of each statement applies to you: *Scoring: Not Concerned = 1; Slightly Concerned = 2; Neutral = 3; Very Concerned = 4; Extremely Concerned = 5*							Validation		Citation
							Yes/ No	Comment	
7	Malicious software, such as viruses, worms, and Trojan horses, can attack electronic devices and cause damage, compromise security, and even result in hardware malfunctions and data loss. This type of attack is referred to as malware. Do you worry about this malware attack?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

8	A Bluetooth attack refers to exploiting vulnerabilities related to the use of Bluetooth technology to access devices, intercept data, or carry out unwanted actions. For example, BlueBorne Attack. Are you concerned about the possibility of an attack targeting your Bluetooth?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
9	The Dolphin attack is a particular kind of attack that target on digital assistants like Siri, Google Assistant, and Amazon Alexa by taking use of ultrasonic frequencies that are undetectable to humans but difficult to be heard by the microphones of these gadgets. Do you worry that a Dolphin Attack will target your personal digital assistant?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
10	Spyware refers to software that is secretly installed on a system without the user's knowledge or agreement. Sensitive data about the user, such as their web surfing patterns, private information, login information is collected using Spyware. Are you concerned about the possibility of having Spyware installed on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

11	Data leakage is the term used to describe the unauthorized transmittal of information or disclosure of information. It happens when unauthorised people access and share sensitive or confidential data in mobile phone. Are you concerned that Data Leakage might have happened on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
12	Spoofing is a dishonest technique when a person, programme, website, or email poses as a trustworthy organisation or procedure in order to obtain sensitive data. Are you concerned that Spoofing Attack might targeting your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
13	Data tampering attack happened when unknown parties purposefully alter, manipulate, delete, or amend data on a person's phone without the person's knowledge or agreement. Are you concerned that Data Tampering attack might targeting your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

14	Phishing attacks are attempts to fool and collect sensitive information, such as login passwords, credit card numbers, or personal information, through the use of fake emails, phone calls, or texts. Are you concerned that Phishing attack might targeting your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
User Security Practices Please select the response that best represents how much of each statement applies to you: *Scoring: Not important at all = 1; Unimportant = 2; Neutral = 3; Important = 4; Very Important = 5*							Validation		Citation
							Yes/ No	Comment	
15	How important is screen locking on mobile phones to you?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
14	Do you believe it is important to protect the data on your mobile phone with complicated passwords and passphrases?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
15	Did you think it is important to clean off malware on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
16	Do you think antivirus software should be installed on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

Section C: Vulnerabilities Behaviour Assessment

This part evaluates the respondent's perception of mobile phone data security, which may affect how vulnerable certain devices are to security flaws.

Perceived Risk Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
1	I believe that my mobile phone's location sometimes is tracked by the GPS.	1	2	3	4	5			(Cooper, C., 2014)
2	I believe that mobile apps were gathering too much data about me.	1	2	3	4	5			(Cooper, C., 2014)
3	I believe other people knows more about my daily life due to always using the social media.	1	2	3	4	5			(Cooper, C., 2014)
4	I believe that using mobile apps has made my privacy information more easily accessible to others.	1	2	3	4	5			(Cooper, C., 2014)
5	I believe that since I use mobile apps, there is confidential information that might be utilised to invade my privacy.	1	2	3	4	5			(Cooper, C., 2014)

Answer the following questions in light of your experiences, attitudes, and believes: *Scoring: Strongly Unlikely = 1; Unlikely = 2; Neutral = 3; Likely = 4; Extremely Likely = 5*							Validation		Citation
							Yes/ No	Comment	
6	How likely do you think it is that someone will read the private communications you sent?	1	2	3	4	5			(Cooper, C., 2014)
7	How likely are you aware that unauthorised individuals could use your smartphone to access information about your online activities?	1	2	3	4	5			(Cooper, C., 2014)

Secondary Utilisation of Personal Data Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
8	I'm worried that mobile applications might utilise my personal data for other purposes without notifying me.	1	2	3	4	5			(Cooper, C., 2014)
Competence Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
9	I use a VPN (Virtual Private Network) on my mobile phone.	1	2	3	4	5			(Bibeau, R., 2011).
10	My mobile phone is configured with security services so that no one can identify me while browsing the Internet.	1	2	3	4	5			(Cooper, C., 2014)
Trust What are your main reasons using mobile phone? *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
11	According to my understanding and experience, online information is very secure.	1	2	3	4	5			(Cooper, C., 2014)

12	A mobile phone is considered as a trusted gadget because of its trustworthy functionality, strong security features, and security precautions.	1	2	3	4	5			(Scott, S., 2006)
13	Mobile phone security can be improved by using antivirus software, hardware encryption, data transfer encryption, and physical device security.	1	2	3	4	5			(Bibeau, R., 2011).

Comments and Recommendations

Evaluated by:

(Signature & Official Stamp) Name:

Date:

APPENDIX B

FINAL PILOT QUESTIONNAIRE

Study On Data Security Awareness in Mobile Phone Usage Among University Student Using Statistical Analysis

Section A: Demographic

For each question, please mark (/) or fill in the blanks in the related information.

Validation	
No.	Comment
1	
Citation	
(Sletten, M. A., 2020)	

1. Gender:

   Male ☐ Female ☐

2. Age:

   18-20 ☐ 24-30 ☐

   21-24 ☐

3. Which faculty in UTeM you belong?

   Fakulti Kejuruteraan Eletrik (FKE) ☐

   Fakulti Kejuruteraan Pembuatan (FKP) ☐

   Fakulti Kejuruteraan Eletronik dan Kejuruteraan Komputer (FKEKK) ☐

   Fakulti Teknologi Maklumat dan Komunikasi (FTMK) ☐

   Fakulti Pengurusan Teknologi dan Teknoushawan (FPTT) ☐

   Fakulti Kejuruteraan Mekanikal (FKM) ☐

   Fakulti Teknologi Kejuruteraan Eletrik Eletronik (FTKEE)

   Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP) ☐

   Fakulti Teknologi Kejuruteraan Mekanikal Pembuatan (FTKMP) ☐

Validation	
No.	Comment
2	
Citation	
(Sletten, M. A., 2020)	

Validation	
No.	Comment
3	

4. What year are you in?

Year One ☐

Year Two ☐

Year Three ☐

Year Four ☐

Validation	
No.	Comment
4	

5. What is your marital status?

Single ☐

Married ☐

Other ☐

Validation	
No.	Comment
5	
Citation	
(Sletten, M. A., 2020)	

6. What brand of mobile phone you are using?

Android ☐

Apple ☐

Validation	
No.	Comment
6	
Citation	
(Sletten, M. A., 2020)	

7. Do you have any social media application installed in your mobile phone?

Yes ☐

No ☐

Validation	
No.	Comment
7	
Citation	
(Sletten, M. A., 2020)	

For question number 8, please (/) for relevant information. You can choose more than one answer.

8. If so, which social media applications do you have installed on your mobile phone?

Facebook	☐
Instagram	☐
TikTok	☐
LinkedIn	☐
Twitter	☐
Snapchat	☐
WhatsApp	☐
Others (please specify)	☐

Yes/ No	Comment
Citation	
(Sletten, M. A., 2020)	

Section B: Level of Awareness Among University Students

These questions assess the degree of knowledge among university students about data security in mobile phones. This part attempts to compile information that assists in evaluating the students' current comprehension of data security precautions and their awareness as mobile phone users.

User Vulnerability Awareness **Level of awareness and knowledge regarding potential risks or vulnerabilities related to mobile phone.** Please select the response that best represents how much of each statement applies to you: *Scoring: Not Concerned = 1; Slightly Concerned = 2; Neutral = 3; Very Concerned = 4; Extremely Concerned = 5*							Validation		Citation
							Yes/ No	Comment	
1	Are you concerned that some of your apps might be collecting information about you?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
2	Are you concerned that your social media applications gather a lot of your data.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
3	Are you concerned that GPS could be used to track your whereabouts?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
4	Are you concerned that your personal digital assistant, such as Siri, Hey Google, Bixby, etc., is constantly watching what's going on around it?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

5	Are you concerned that Bluetooth is vulnerable to the attacks? (For instance, a hacker may take over the phone and use it to read texts, send texts on behalf of the owner, make phone calls, and access the Internet.)	1	2	3	4	5			(McGovern Cole, E. L., 2019)
6	Are you concerned about the public Wi-Fi where anyone can access the Internet via an unsecured, public Wi-Fi access point because it does not require a password.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
User Threat Awareness **Level of awareness and knowledge regarding potential threat and attack related to mobile phone**. Please select the response that best represents how much of each statement applies to you: *Scoring: Not Concerned = 1; Slightly Concerned = 2; Neutral = 3; Very Concerned = 4; Extremely Concerned = 5*							Validation		Citation
							Yes/ No	Comment	
7	Are you concerned that malware attack such as viruses' worms, and Trojan horses, can attack electronic devices and cause damage, compromise security, and even result in hardware malfunctions and data loss?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

8	Are you concerned that a Bluetooth attack can exploit vulnerability related to access devices, intercept data, or carry out unwanted actions. For example, BlueBorne Attack.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
9	Are you concerned that Dolphin attack can target assistants like Siri, Google Assistant, and Amazon Alexa by taking use of ultrasonic frequencies that are undetectable to humans but difficult to be heard by the microphones of these gadgets.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
10	Are you concerned that Spyware is secretly installed on a system without the user's knowledge or agreement. Sensitive data about the user, such as their web surfing patterns, private information, login information is collected using Spyware.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
11	Are you concerned that Data leakage which the term used to describe the unauthorized transmittal of information or disclosure of information. It happens when unauthorised people access and share sensitive or confidential data in mobile phone.	1	2	3	4	5			(McGovern Cole, E. L., 2019)

12	Are you concerned that Spoofing Attack might targeting your phone where a person, programme, website, or email poses as a trustworthy organisation or procedure in order to obtain sensitive data.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
13	Are you concerned Data tampering attack might targeting your mobile phone where unknown parties purposefully alter, manipulate, delete, or amend data on a person's phone without the person's knowledge or agreement.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
14	Are you concerned that Phishing attacks are attempts to fool and collect sensitive information, such as login passwords, credit card numbers, or personal information, through the use of fake emails, phone calls, or texts.	1	2	3	4	5			(McGovern Cole, E. L., 2019)
User Security Practices **Users concerned about applying security practices when using mobile phone.** Please select the response that best represents how much of each statement applies to you: *Scoring: Not important at all = 1; Unimportant = 2; Neutral = 3; Important = 4; Very Important = 5*							Validation Yes/ No	Validation Comment	Citation
15	How important is screen locking on mobile phones to you?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

16	How important to protect the data on your mobile phone with complicated passwords and passphrases?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
17	How important to clean off malware on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)
18	How important to install antivirus software on your mobile phone?	1	2	3	4	5			(McGovern Cole, E. L., 2019)

Section C: Vulnerabilities Behaviour Assessment

This part evaluates the respondent's perception of mobile phone data security, which may affect how vulnerable certain devices are to security flaws.

Perceived Risk **User expectations of losses associated to the disclosure of personal information due to the vulnerabilities of mobile phone.** Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
1	I believe that my mobile phone's location sometimes is tracked by the GPS.	1	2	3	4	5			(Cooper, C., 2014)
2	I believe that mobile apps were gathering too much data about me.	1	2	3	4	5			(Cooper, C., 2014)
3	I believe other people knows more about my daily life due to always using the social media.	1	2	3	4	5			(Cooper, C., 2014)
4	I believe that using mobile apps has made my privacy information more easily accessible to others.	1	2	3	4	5			(Cooper, C., 2014)
5	I believe that since I use mobile apps, there is confidential information that might be utilised to invade my privacy.	1	2	3	4	5			(Cooper, C., 2014)

Answer the following questions in light of your experiences, attitudes, and believes: *Scoring: Strongly Unlikely = 1; Unlikely = 2; Neutral = 3; Likely = 4; Extremely Likely = 5*							Validation		Citation
							Yes/ No	Comment	
6	How likely do you think it is that someone will read the private communications you sent?	1	2	3	4	5			(Cooper, C., 2014)
7	How likely are you aware that unauthorised individuals could use your smartphone to access information about your online activities?	1	2	3	4	5			(Cooper, C., 2014)

Secondary Utilisation of Personal Data **Users concerned about whether their personal information is being used by mobile application.** Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
8	I believe that mobile applications might utilise my personal data for other purposes without notifying me.	1	2	3	4	5			(Cooper, C., 2014)
9	I believe that I am asked for too much personal information when purchasing.	1	2	3	4	5			(Cooper, C., 2014)
10	I believe that unauthorised individuals using my smartphone to access information about my online activities.	1	2	3	4	5			(Cooper, C., 2014)
11	I believe that individuals on the internet are not who they claim to be.	1	2	3	4	5			(Cooper, C., 2014)
12	I believe that online organisation on the internet is not who they claim to be.	1	2	3	4	5			(Cooper, C., 2014)

Competence **Users' competency of securing their personal data on mobile phone.** Please select the response that best represents how much of each statement applies to you: *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
13	My mobile phone used VPN (Virtual Private Network) to secure my connection on my mobile phone.	1	2	3	4	5			(Bibeau, R., 2011).
14	My mobile phone is configured with security services so that no one can identify me while browsing the Internet.	1	2	3	4	5			(Cooper, C., 2014)
15	I sign out from my Personal Account after I used my mobile phone.	1	2	3	4	5			(Amin, M. et al., 2021)
16	I always read Application's Privacy and Policy before installed an application.	1	2	3	4	5			(Amin, M. et al., 2021)
17	I used Biometric Authentication such as fingerprint, and face ID for my lock screen on mobile phone.	1	2	3	4	5			(Amin, M. et al., 2021)

Trust **Users' belief or confidence of their mobile phone itself.** *Scoring: Strongly Disagree = 1; Disagree = 2; Neutral = 3; Agree = 4; Strongly Agree = 5*							Validation		Citation
							Yes/ No	Comment	
18	I believe that when I use my mobile phone to connect to Wi-Fi network, it is important to make sure connecting only to encrypted, password-protected networks.	1	2	3	4	5			(Riola, P. A., 2014)
19	I believe mobile phone is a trusted gadget because of its trustworthy functionality, strong security features, and security precautions.	1	2	3	4	5			(Scott, S., 2006)
20	I believe that mobile phone security can be improved by using antivirus software, hardware encryption, data transfer encryption, and physical device security.	1	2	3	4	5			(Bibeau, R., 2011).
21	I believe that mobile phone holds our important personal information such as photos and videos, SMS, email, contact list and social media accounts.	1	2	3	4	5			(Amin, M. et al., 2021)
22	I believe that before installing application, I must read through application's phone access permissions so that my mobile phone will no affected by malware.	1	2	3	4	5			(Amin, M. et al., 2021)

Comments and Recommendations

Evaluated by:

(Signature & Official Stamp)

Name:

Date:

APPENDIX C

Prove of Validation Pilot Questionnaire

Evaluated by:

fadzilah
DR. NUR FADZILAH BINTI OTHMAN
Pensyarah Kanan
Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka (UTeM)

(Signature & Official Stamp)

Name: Dr. Nur Fadzilah binti Othman

Date: 22 June 2023

Evaluated by:

DR. MOHD ZAKI BIN MAS'UD
Pensyarah Kanan
Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka (UTeM)

(Signature & Official Stamp)

Name: MOHD ZAKI BIN MAS'UD

Date: 26/June/2023