SHAPING USER CONFIDENCE TOWARDS ONLINE BANKING SECURITY AND SAFETY FEATURES IN MALAYSIA

LEE JENG YANG

LIEW MIN SUN

VIVIAN TAN YUN XIN

WONG YAN MIN

BACHELOR OF BUSINESS ADMINISTRATION (HONOURS) BANKING AND FINANCE

UNIVERSITI TUNKU ABDUL RAHMAN

TEH HONG PIOW FACULTY OF BUSINESS AND FINANCE

DEPARTMENT OF BANKING AND RISK MANAGEMENT

SEPTEMBER 2025

SHAPING USER CONFIDENCE TOWARDS ONLINE BANKING SECURITY AND SAFETY FEATURES IN MALAYSIA

BY

LEE JENG YANG

LIEW MIN SUN

VIVIAN TAN YUN XIN

WONG YAN MIN

A final year project submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF BUSINESS ADMINISTRATION (HONOURS) BANKING AND FINANCE

UNIVERSITI TUNKU ABDUL RAHMAN

TEH HONG PIOW FACULTY OF BUSINESS AND FINANCE

DEPARTMENT OF BANKING AND RISK MANAGEMENT

SEPTEMBER 2025

Copyright Statement

This final year project report is submitted in partial fulfillment of the requirements for the degree of Bachelor of Business Administration (Honours) Banking and Finance at Universiti Tunku Abdul Rahman (UTAR). This final year project report represents the work of the author, except where due acknowledgment has been made in the text. No part of this final year project report may be reproduced, stored, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the author or UTAR, in accordance with UTAR's Intellectual Property Policy.

DECLARATION

We hereby declare that:

(1) This undergraduate FYP is the end result of our own work and that due acknowledgement has been given in the references to ALL sources of information be they printed, electronic, or personal.

(2) No portion of this FYP has been submitted in support of any application for any other degree or qualification of this or any other university, or other institutions of learning.

(3) Equal contribution has been made by each group member in completing the FYP.

(4) The word count of this research report is 17365.

Name of Student:	Student ID:	Signature:
1. Lee Jeng Yang	2106266	
2. Liew Min Sun	2207138	
3. Vivian Tan Yun Xin	2104077	
4. Wong Yan Min	2106833	

Date: 9 September 2025

ACKNOWLEDGEMENT

Firstly, we would like to express our appreciation to Universiti Tunku Abdul Rahman (UTAR) for providing us opportunities to conduct this final year project (FYP). Through this study, we have improved our interpersonal skills, self-management skills and teamwork abilities.

Besides, we would like to express our appreciation to our supervisor, Mr. Koh Chin Min for his continuous guidance, valuable advice, and encouragement throughout the completion of this project. His insights and constructive feedback have been instrumental in shaping our work. We are truly grateful for his mentorship.

Furthermore, we would like to extend our appreciation to our examiner, Ms Zainon Binti Md. Yunus for her time, effort, and constructive evaluation of this project. She has provided feedback, and suggestions have helped us to further improve the quality of my work.

Moreover, we would like to thank all the respondents who participated in this study. Their willingness to share their time, experiences, and honest opinions provided the essential data that made this research possible.

Lastly, we would also truly grateful to each of our team members, whose dedication, teamwork, and contributions played an important role in overcoming challenges and completing this project successfully. Working together has been an invaluable experience.

DEDICATION

First and foremost, we would like to dedicate this study to Universiti Tunku Abdul Rahman (UTAR). The university has provided us with resources and facilities. Access to these resources and facilities allows us to conduct the study smoothly.

Secondly, we would like to dedicate the work to our supervisor, Mr. Koh Chin Min, for his valuable guidance and advice. His unwavering support and expert guidance were essential in guiding us through the challenges we faced during this project. We are deeply grateful for his patience and support.

Besides, we also wish to dedicate to our examiner, Ms Zainon Binti Md. Yunus. She gave us with many useful insightful on how to improve the study. Hence, this enables us to produce a more refined research project.

Lastly, we dedicate this project to our team members. We are truly grateful for the spirit of collaboration, patience, and dedication that we shared throughout this journey. Working together has not only made this project possible but has also created memories and lessons that we will carry with me into the future.

PREFACE

This Final Year Project (FYP) is submitted in partial fulfillment of the requirements for graduate students at Universiti Tunku Abdul Rahman (UTAR) pursuing a Bachelor of Business Administration (Hons) in Banking and Finance which is supervised by Mr. Koh Chin Min. The topic of our study is "Shaping User Confidence towards Online Banking Security and Safety Features in Malaysia". This project was written entirely by the authors and supported by references to the research of others.

The purpose of this research is to investigate the influence of system reliability, user knowledge, perceived data protection and technology infrastructure on user confidence towards online banking security and safety features in Malaysia. With the rapid growth of online banking services, ensuring user confidence has become increasingly critical. This study aims to provide insights into how technical and perceptual factors shape confidence in online banking, which is essential for both financial institutions and policymakers. We hope the findings of this project will contribute to a deeper understanding of online banking security and serve as a useful reference for future research and industry practices.

ABSTRACT

The rapid growth of online banking in Malaysia has transformed the way consumers access financial services, offering greater convenience and efficiency. However, concerns about security and confidence remain key barriers to wider adoption. This research aims to investigate the factors influence user confidence towards online banking security and safety features including system reliability, user knowledge, perceived data protection and technology infrastructure in Malaysia. The study utilises Protection Motivation Theory (PMT) to explain how user knowledge and technology infrastructure affects user confidence in online banking. Besides, Technology Acceptance Model (TAM) is used in this study to explain how user confidence is impacted by system reliability and perceived data protection. The data collection method used in this research is primary data using questionnaire and received a total of 384 responses. IBM Statistical Package for the Social Sciences tool (SPSS) was used to analyse and interpret the relevant data. The data was analysed by using descriptive analysis, reliability test, multicollinearity test, Pearson correlation, normality test and Multiple Linear Regression. The results show that system reliability and perceived data protection are significantly impact with the user confidence. The study provides valuable insight for banking industry and policymakers. This study also provides recommendations for future researchers to perform more precise and accurate studies regarding this area, therefore addressing the limitations of our work.

Keywords: Online Banking; User Confidence; System Reliability; User Knowledge; Perceived Data Protection; Technology Infrastructure

Subject Area: HG501 - 3550 Banking

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SFU	Surplus Fund Unit
DFU	Deficit Fund Unit
ATM	Automatic Teller Machine
BNM	Bank Negara Malaysia
KYC	Know Your Customer
2FA	Two-factor Authentication
AI	Artificial Intelligence
APT	Advanced Persistent Threats
MDEC	Malaysia Digital Economy Corporation
PMT	Protection Motivation Theory
TAM	Technology Acceptance Model
PDPA	Personal Data Protection Act
SPSS	Statistical Package for Social Sciences
MLR	Multiple Linear Regression
VIF	Varian Inflation Factor
ANOVA	Analysis of Variance
IV	Independent Variable
DV	Dependent Variable

SR	System Reliability
UK	User Knowledge
PDP	Perceived Data Protection
TI	Technology Infrastructure
UC	User Confidence
SPM	Sijil Pelajaran Malaysia
PhD	Doctor of Philosophy

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.0 Introduction

This study is studying user confidence towards online banking security and safety features in Malaysia. The research background will be discussed in the first chapter. In addition, the problem statement, research objectives, and research questions will be presented. Last but not least, the significance of this research will also be addressed. This section provides a summary of the research topic.

1.1 Background of Study

According to Akhter and Roy (2017), a bank is a financial institution that acts as a financial intermediary between surplus and deficit units, connecting different aspects of society. The main responsibility of a bank is to accept deposits from surplus fund units (SFUs) and provide loans to deficit fund units (DFUs) (Syafril 2025). Surplus fund units (SFUs) are the individuals who have greater income than expenses. It means that their total expenditures are less than their total income. The example of SFUs is the households that save their money in the bank account. However, deficit fund units (DFUs) are the entities that have greater expenses than income. The common example of DFUs is corporations because a corporation needs to raise a large capital for daily operations and company expansion.

Due to the evolution of technology, the banking system has also developed into different stages, such as the traditional banking system, automatic teller machines (ATMs), phone banking, online banking, mobile banking, and digital banking. The

initial stage of the banking system is traditional banking. In a traditional banking system, customers need to visit the bank branch for banking services. There are face-to-face interactions between the bank's staff and customers, and they are commonly in paper-based transactions, such as providing a bank statement to customers who open a new account. According to Bellis (2019), in 1967, an automatic teller machine (ATM) was first installed in Barclays Bank in London. At that time, an ATM was just a cash dispenser. Then, the ATM that is familiar today was invented in 1971 (Bellis, 2019). It offers the services of depositing money and withdrawing money. In order to withdraw money from an ATM, customers need to hold a debit card or credit card. ATMs are more convenient than traditional banking due to the operating hours of ATMs being longer than traditional banking. Moreover, phone banking, also known as telebanking, allows customers to perform banking services through phone calls. By using phone banking, customers can call the Customer Care Hotline, choose the preferred language, and finally get the services they need. The services provided are fund transfer, bill payment, statement request, and others (Phone Banking Services | Maybank Malaysia, n.d.).

After that, online banking, also known as Internet banking, allows customers to access their account balances through the bank's official website (Online Banking: What It Is, How It Works, and Best Options (Payoneer, 2025). By using online banking, it allows users to handle their funds whenever they have a desktop or laptop and internet connection (Roberte, 2025). The financial services that users can finish by using online banking are fund transfer, bill payment, obtaining a bank statement, and others. Furthermore, mobile banking was introduced to allow customers to conduct their transactions by using a mobile device such as a smartphone or tablet (Pradhan, 2024). In order to use mobile banking services, customers need to make sure their mobile devices are connected to the Internet before conducting their transactions. The functions that are provided by the mobile banking system include accessing the users' bank accounts easily and conducting payments or fund transactions in a few clicks. Apart from that, digital banking is defined as the financial institution that offers banking services such as depositing money and applying for a loan through a digital platform. The digital banking is

operating entirely through an online platform and without physical branches (Abdullah, 2025). The benefit of digital banking is to provide 24/7 customer service. Grab's GXBank was the first digital bank that was authorised by Bank Negara Malaysia (BNM) in November 2023, followed by AEON Bank and Boost Bank (Fintech News Malaysia, 2025).

The topic of this research is online banking. This online banking was introduced when the Internet was widely used. One type of online banking is mobile banking. Both require an Internet connection when customers process the financial services. The only difference is mobile banking is done through mobile applications, while online banking can be done through the bank's website on a desktop or smartphone. The subscribers of online banking in Malaysia have increased from 17,230 in 2019 to 36,254 in 2024 (Bank Negara Malaysia, n.d.). According to Ong et al. (2023), two factors have contributed to the rise in online banking usage in Malaysia: the central bank's instruction and the ease of delivery channels. For example, services such as fixed deposits and loan applications are also available in online banking. This has made online banking more convenient and user-friendly. This is because customers are able to place their fixed deposits in a few clicks and save their time in visiting the bank's branches. Apart from the benefits of time-saving and convenience, online banking also provides the advantages of data transparency and tailored services. In the current technology age, cybersecurity is a major issue for many industries. Online banking, which is operated via the Internet, will also be a main concern in the current era, especially as it relates to money. Thus, online banking is a popular concern compared to other banking systems. Besides, online banking is still the most popular and well-established method of financial interaction in Malaysia, even though digital banking is the latest development in financial services. For more than 20 years, banks and customers have embraced this seasoned and reliable platform, since the first online banking in Malaysia was established by Maybank in June 2000 (Ong et al., 2023). Online banking represents the typical experience of Malaysians today, in contrast to digital banking, which is

still in its early stages of acceptance and could only be accessible to a few tech-savvy consumers.

During the past twenty years, online banking brought accessible banking services, streamlined transactions, and more avenues for user inclusion in the marketplace. Researchers have dedicated extensive study to both security features of online banking and their influence on user actions (Ojo et al., 2022). Researchers have shown that users need both confidence and system functional quality to adopt new services within online banking and online service environments (Yong & Kasiran, 2023). Online financial participation by users depends on their assessments of operational security together with the reliability features that the platform provides. Nevertheless, these platforms face new concerns over cybersecurity, data breaches, and fraud that affect how users interact with and trust these platforms (Gulyas & Kiss, 2023).

Online banking platforms have seen the adoption of financial services in developed and developing economies, transforming the continuity to be more convenient and accessible to consumers. Nowadays, banks are moving towards online service, meaning that data privacy, fraud, and cyber threats are becoming bigger issues. In an online banking environment, platform usability and online service quality determine customer confidence (Akter et al., 2023). Gulyas and Kiss (2023), however, pointed out the growing rate and complexity of cyberattacks against financial institutions as a call for stronger digital safeguards that will guarantee the safety of users and the confidence of the public in the online banking system. Adoption rates increase further when users have more confidence in the online banking system.

The secure online banking system has become necessary and, therefore, the foundation of data protection, making financial institutions implement effective compliance frameworks and encryption protocols. Through their strategic

partnership, financial institutions and banks actively build modern security protocols consisting of encryption systems and authentication layers and physical identity checks (Kovalan et al., 2021). Safety components emerged as solutions because they protect platform trust through protection from escalating cyber dangers as well as unauthorised access threats (Jafri et al., 2024). Similarly, Subri et al. (2024) attempted to study how digital systems such as the electronic know-your-customer (KYC) process and two-factor authentication (2FA) help in improving digital identity verification and blocking unauthorised access. Leschanowsky et al. (2024), in their systematic review of confidence and privacy concerns in AI-powered platforms, highlighted the impact of attitudes to automation on users' concerns in AI-powered platforms. As part of modern cybersecurity development, these security features form an important part of initiatives to protect users against contemporary online security risks. While such studies provide valuable and interesting views on policy and technology, they remain more orientated to structural measures than to the psychological and emotional dimensions of user confidence in an online banking environment.

User awareness and digital literacy are vital for interacting with online banking platforms. Childers et al. (2022) discussed the integration of cybersecurity education in school settings and the lack of foundational digital awareness, which may also be present in adult banking behaviour. According to Khan et al. (2024), perceived cyber risks affect the effects of acceptance of emerging technologies and their psychosocial reluctance when using online financial tools. Ranjan (2025) extended the discussion by introducing behavioural finance in banking and determining the role of the psychological and cognitive factors that affect the users' behaviour in terms of financial decision-making. Together, these studies further show the need for user education, perception, and proper navigation of digital financial services. Still, they fail to fully connect these insights to how Malaysian users develop or sustain confidence in online banking environments, thus providing remaining space for further examining the confidence-building process with a more context-specific focus.

Past studies about technology infrastructure in developing economies consisting of Malaysia emphasise the requirement of strong digital infrastructure because it guarantees secure banking services are always accessible. The research findings in these studies remain isolated because they study elements separately (Mishra et al., 2022). This research focuses on bridging the knowledge gap about how user confidence in Malaysian online banking develops through the collective interaction of security design and performance and technological infrastructure.

Ahmed et al. (2024) looks into how users develop confidence in cybernetic payment networks, especially in developing nations where the number of online transactions is rapidly rising. The study focuses on the factors that give users confidence in these systems, such as the ease of online payments, prior online banking experiences, or the stability of the technology. The authors explore the human side of things, including user perceptions and societal factors, rather than concentrating solely on technical security aspects in order to ascertain what in fact motivates confidence in online financial systems. The study's examination of these factors provides governments and companies with useful information on how to create payment networks that users feel confident using.

Ali (2024) looks into how convenience and security affect mobile banking use in Baguio City, Philippines. Rather than relying solely on technical details, the study explores the experiences of actual users, including how their confidence in mobile banking apps affects their regular purchasing habits. In order to help businesses and app developers create better, more user-friendly banking systems, the author polls Baguio customers to obtain useful insights about what motivates use, whether it's strong safety features, easy transactions, or a combination of the two.

Alnaser et al. (2023) investigate whether banking solutions driven by AI satisfy consumer needs and ultimately boost satisfaction. They're exploring how factors like confidence in the technology, actual usage patterns, and whether the AI meets expectations all affect the user experience, going beyond simple convenience. The research examines the effects of AI features like chatbots, fraud detection, and personalised recommendations on actual user satisfaction rather than speculating. Instead of just following tech trends, the findings provide specific insights for banks looking to implement AI, showing not only which features to add but also how to use them in ways that actually improve customer experience.

Bhattacharya and Sinha (2022) explore how artificial intelligence is changing banking operations by improving customer interactions rather than just bringing in new technology. The researchers look into whether AI-powered solutions like chatbots, fraud detection, and suggested modifications actually make banking better for users. The study looks at real user interactions with AI-powered banking, going beyond presumptions. It looks into the effects of different AI applications on user behaviour, confidence, and satisfaction. The study provides helpful insights for banks attempting to implement AI in ways that benefit users, not just their bottom line, by focusing on practical outcomes rather than just technological capabilities.

Chaimaa et al. (2020) examines online banking in general, including its definition, user motivations, and obstacles. The researchers look into the basic factors that affect online banking, including users' confidence in the technology, how they actually use online banking tools, and whether these systems are simple or harmful. However, they don't stop there. The study also discusses actual issues with online banking, like security risks and technical issues, and even suggests practical fixes to make online banking safer and more convenient for all users. This study helps banks and tech companies develop better, more user-friendly solutions by offering a fair assessment of online banking's strengths and areas for improvement.

According to Che et al. (2023), it explores the reasons behind users' sustained confidence in and use of mobile banking apps, beyond their initial download. The researchers examined users' ongoing interactions with their banking apps in an effort to understand why some users stick with online banking while others stop using it. Since retaining users is just as important as acquiring them in the first place, the study's analysis of these continuing experiences reveals what banks need to do to maintain user confidence after the initial download. The results provide insight into why some mobile banking apps attract loyal users while others are deleted after a short period of use.

Through the implementation of strict access controls and user authentication protocols across canonical, logical, and physical levels, Ghelani et al. (2022) develop multi-layered cybersecurity mechanisms for banking systems to increase confidence in online transactions. This ensures data protection while optimising user convenience. The study addresses the growing challenges of big data management and cloud-based banking in an increasingly digital financial landscape by analysing past threats and vulnerabilities and proposing adaptive security models that strike a balance between robust definitions against cyber risks and seamless user experience.

Johri and Kumar's (2023) study looks at how cybersecurity awareness affects Saudi Arabian banking customers' confidence and satisfaction with online banking services. They find that while phishing awareness has little effect, user confidence is greatly increased by knowledge of cyberthreats like hacking. by examining consumer opinions regarding the ease of bill payment and transfer via internet and mobile banking. The study emphasises how important security literacy is in influencing favourable online banking practices during the online revolution. In an increasingly digital financial ecosystem, the results highlight the necessity for banks to give cybersecurity education top priority in order to increase customer satisfaction and confidence.

The most recent user authentication techniques in online banking, such as knowledge-based, biometric, and multi-factor authentication, are thoroughly reviewed by Karim et al. (2023). In order to strike a balance between security and user convenience, their efficacy against online dangers such as malware and phishing is being examined. Examining current procedures in major banks, the study emphasises the increasing use of biometrics to boost confidence in online transactions while cautioning that new threats necessitate constant innovation to safeguard accounts without sacrificing usability. In light of the constantly changing threat landscape, the findings offer banks a roadmap for fortifying authentication frameworks and guaranteeing safe yet convenient online banking experiences.

Khan et al. (2023) explore that biometric authentication is a crucial way to improve online banking cybersecurity by addressing emerging risks like identity theft and AI-powered deepfakes while striking a balance between security and user convenience. The study emphasises how this technology can increase confidence in online transactions without sacrificing accessibility by putting forth a flexible biometric identification system, even as cybercriminals create increasingly complex attack techniques. The methodical examination highlights the dual function of biometrics in protecting banking systems from new threats and expediting the authentication process for clients tired of conventional verification techniques.

Mgiba and Mxotwa (2024) examine the effects of management communication regarding cybersecurity measures on ethical issues like security, privacy, diversity, and discrimination, as well as the ensuing impact on service satisfaction and loyalty intentions, in order to better understand how AI-driven banking services affect customer confidence and behaviour. The study highlights how user perceptions of online banking in developing nations are shaped by the combined importance of convenience through AI-enabled efficiency and trust through ethical protections.

With a focus on a bank's customers in the Klang Valley, Malaysia, Moksin and Povakalam (2024) investigate customer satisfaction with online banking services. They discover that, in contrast to earlier studies, security has little bearing on customer satisfaction because users take strong security for granted. Rather, convenience elements like usability, transaction speed, and customer service have a more direct impact on satisfaction, indicating that daily usability influences user behaviour and that trust in technology is presumed until it is violated. According to the study, users now place a higher value on smooth functionality than on hidden security issues when it comes to creating satisfying online banking experiences.

Mwiya et al. (2022) examines the factors that genuinely contribute to users' satisfaction with online banking services. In addition to assessing the technology's functionality, the researchers looked into how user satisfaction is impacted by a number of aspects of online service quality, including customer support, security features, online stability, and ease of navigation. To ascertain which service features are most important in creating exceptional online experiences, they asked banking customers directly rather than relying on speculation.

In order to create strategies that improve security and user confidence in online banking platforms, Oyewole et al. (2024) perform a thorough analysis of cybersecurity risks in online banking, looking at recent cyber incidents, financial impacts, and current defence mechanisms. The study promotes dynamic cybersecurity frameworks that safeguard financial systems while preserving user convenience in an increasingly online banking environment by incorporating cutting-edge technologies like artificial intelligence (AI) and big data analytics. To protect against changing threats, maintain user confidence in online financial services, and ensure the integrity of online transactions, the results highlight the vital need for adaptive security measures.

Using a conceptual framework that connects attitudes, intentions, and behaviour to the adoption of digital payments, Rahman and Hassan (2022) investigate the factors influencing trust in cashless transaction technology among Malaysian higher education communities. This highlights how online banking behaviour and the convenience of e-wallets and QR codes are shaped by perceived usefulness, cybersecurity, and transaction processes. In order to promote sustainable cashless practices, the research focuses on belief-driven cultural shifts. This will give educational institutions a model for improving the acceptance of digital payments through better security, usability, and institutional support. education communities. This highlights how online banking behaviour and the convenience of e-wallets and QR codes are shaped by perceived usefulness, cybersecurity, and transaction processes. In order to promote sustainable cashless practices, the research focuses on belief-driven cultural shifts. This will give educational institutions a model for improving the acceptance of digital payments through better security, usability, and institutional support.

The reviewed literature has primarily focused on technical security measures, the functionality of the platform, or user education as elements that influence trust in online banking. While this study attempts to explore how these elements interact with user perceptions, psychological comfort, and emotional response in the Malaysian context, the remaining number of studies are few. This study's approaches are conceptual, exploring how users gain confidence in online banking through integrating digital platforms. It goes beyond isolated technical features to investigate the creation of trust amid transparency, reliability, ease of communications, and safety. The study provides a user-centred perspective that integrates these dimensions and, thus, supplements the current research on the trust and security of online banking.

The study specifically examines how security and safety features impact user confidence in Malaysia's unique online banking context, in contrast to previous research that has typically concentrated on general online banking adoption, AI-driven solutions, or broad cybersecurity measures. While earlier research has examined convenience, AI integration, and authentication techniques, the study Shaping user confidence in online banking security and safety features in Malaysia closes a knowledge gap about the safety mechanisms that Malaysians value by concentrating on the direct effects of security features such as encryption, fraud alerts, and multi-factor authentication on user confidence. Similar studies have been conducted elsewhere, but particular research is required given Malaysia's rapidly growing online banking market, distinct regulatory framework, and user demographics. Regional factors that cannot be generalised across markets, such as the prevalence of cyber threats, financial literacy, and cultural attitudes toward technology, all have an impact on user confidence.

Since Malaysia's quickly growing online banking industry needs targeted insights to boost user confidence, this topic requires further research. This study can offer practical suggestions for banks, legislators, and developers to create more efficient, user-centric online banking solutions, leading to greater adoption and satisfaction in this area, by identifying which security and safety features have the biggest impact on Malaysian users' confidence.

1.2 Problem Statement

In Malaysia, the rapid growth of online banking has revolutionised financial transactions, offering customers convenient access to banking services. However, alongside these benefits, cybersecurity and safety concerns have emerged as barriers to widespread user confidence (Oyewole et al., 2024). Cyber threats in

Malaysia, such as online and cyber fraud and banking fraud, are escalating as more individuals rely on online banking for daily services (Ismail et al., 2023). These rising concerns contribute to a growing scepticism among users, particularly those with limited technological literacy, thereby posing challenges to the sustained success of Malaysia's digital financial ecosystem. Similarly, with the development of technology, online behaviour for illegal financial gain, such as phishing attacks, has typically occurred, particularly in online banking, leading to a significant increase in Malaysia (Kuah et al., 2024). For example, Malaysia incurred losses of RM54.02 billion due to its online fraud transactions, such as phishing attacks that targeted online banking users through messaging apps, social media and emails in 2024 (Shahrizal, 2024). The growing prevalence of cyberattacks has led to an increase in public distrust toward the safety and reliability of online financial platforms. Fraudulent activities have eventually reinforced the belief that online banking systems are prone to risks, eroding users' confidence in their cybersecurity frameworks (Oyewole et al., 2024). Therefore, the fear of financial loss and data breaches continues to be a key deterrent, transitioning to online banking and even impeding Malaysia's efforts towards achieving its financial inclusion.

User confidence in online banking security is a key determinant in the retention of digital financial services. According to research by Siagian et al. (2022), a strong correlation exists between privacy, security and user trust in online banking platforms, indicating that users who feel assured of the safety of online banking systems tend to engage and be confident in online financial transactions. Inadequately addressed cybersecurity issues can erode consumer confidence and even deter potential users over time. Online banking platforms have become a prime target of cybercriminals. The cybersecurity threats in online banking exploit vulnerabilities in systems, networks and user practices, which have significant potential for financial damages (Jimmy, 2024). This rising frequency of such incidents further fuels public confidence regarding the robustness of online banking security systems, heightening concerns about banking institutions' capabilities in safeguarding their personal and financial data. Also, the public perception of a

bank's competence to protect users' data influences the willingness of individuals to continue using online banking services (Alrababah, 2024). Without adequate reassurance, the majority of users may restrict the usage of online banking platforms, potentially slowing the growth of the banking sector in Malaysia.

In the realm of online banking services, the rapid advancement in artificial intelligence (AI) technologies results in the emergence of new and complex cyber threats (Abbadi, 2024). As the continuous emergence of new cyberattack methodologies such as advanced persistent threats (APTs) and AI-driven social engineering attacks highlights the need for more robust security measures, they further present ever-growing challenges to existing security measures (Toback, 2024). Recognising these vulnerabilities, inadequate authentication methods, such as simple username and password combinations, may open a pathway for cybercriminals to directly access accounts and perform unauthorised transactions in online banking platforms. As these threats continue to evolve, the exploitation of outdated systems can even lead to identity theft, potentially even control over core banking institutions. Therefore, the demand for proactive security infrastructure approaches, including multi-factor authentication and behavioural biometrics, may become imperative in mitigating risks (Karim et al., 2023). With a response of failure to reinforce the strong cybersecurity frameworks, it can lead to a less secure online banking environment, which can damage the reputation of financial institutions and diminish customer dissatisfaction and confidence as well. A low level of security in online banking may result in increased regulatory scrutiny and operational disruptions, ultimately threatening the long-term viability of financial institutions in the future banking landscape.

While concerns over cybersecurity threats persist, all Malaysian banks, like Public Bank, Maybank, and Hong Leong Bank, prioritise enhancing their online security frameworks to ensure transparency and foster user confidence. This research aims to examine the significant level of various variables that influence user confidence

towards online banking security and safety features in Malaysia, contributing to a more stable and safe online banking ecosystem and lowering the risk of cyber threats.

1.3 Research Objectives

1.3.1 General Objectives

This study's primary objective is to determine user confidence towards online banking security and safety features in Malaysia as well as identify the factors influencing it, including system reliability, user knowledge, perceived data protection and technology infrastructure.

1.3.2 Research Objectives

1. To investigate the influence of system reliability on user confidence towards online banking security and safety features in Malaysia.
2. To investigate the influence of user knowledge on user confidence towards online banking security and safety features in Malaysia.
3. To investigate the influence of perceived data protection on user confidence towards online banking security and safety features in Malaysia.
4. To investigate the influence of technology infrastructure on user confidence towards online banking security and safety features in Malaysia.

1.4 Research Questions

1. Does system reliability influence user confidence towards online banking security and safety features in Malaysia?
2. Does user knowledge influence user confidence towards online banking security and safety features in Malaysia?
3. Does perceived data protection influence user confidence towards online banking security and safety features in Malaysia?
4. Does technology infrastructure influence user confidence towards online banking security and safety features in Malaysia?

1.5 Significance of Study

The purpose of this study is to examine how the key components – system reliability, user knowledge, perceived data protection, and technology infrastructure – influence user confidence in online banking security and safety features in Malaysia. The results will provide important insights into three significant areas: academic research, the banking and financial industry, and policymaking.

Firstly, this research provides a theoretical framework that future studies can develop to further investigate confidence in online banking security in various situations. This is because this study offers empirical evidence on how important factors like system reliability, user knowledge, perceived data protection, and technology infrastructure affect user confidence. Besides, there are many studies that concentrate on online security and user confidence independently; this study links the technical factors, such as technology infrastructure and system reliability, with user perception factors, such as user knowledge and perceived data protection.

This may provide a more comprehensive understanding of how user confidence arises in online banking security.

Secondly, this study provides practical insights for the banking industry on how to improve customer confidence in online banking security. By recognising the key factors that influence customer confidence, the banking industry can strengthen their online banking features. This may increase the customer usage and retention rate when they provide a safer and user-friendly online banking system. Besides, by providing a secure and safer online banking system, it may reduce the security problems in online banking. The common security problems are phishing attacks and identity theft, which can lead to financial loss and data breaches. In declining the possibility of financial loss, the banking industry can differentiate itself from the competitors.

Lastly, this research provides valuable insight for regulators and policymakers in Malaysia, such as Bank Negara Malaysia (BNM) and the Malaysia Digital Economy Corporation (MDEC), in reinforcing cybersecurity policies such as data privacy and fraud prevention for online banking. In order to reduce the security threats, the findings may contribute to developing stricter regulations and public awareness campaigns. For example, the findings allow regulators to collaborate with the banking industry in developing secure online banking environments through real-time reporting platforms for suspicious transactions. As a result, Malaysia's digital financial ecosystem will become more reliable and secure.

1.6 Conclusion

The summary of this study in the background and issue of user confidence towards online banking security and safety features in Malaysia is discussed in Chapter 1.

This was including variables like user trust, system reliability, user knowledge, perceived data protection and technology infrastructure that correspond with shaping user confidence towards online banking security and safety features in Malaysia; it was possible to establish the research goals and questions. The chapter also covered the value of this research for three major groups, including the banking industry, regulators and policymakers, and academics that study finance.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

The theoretical framework was covered in chapter 2. The literature review of explained and explanatory variables is also discussed in this chapter. Lastly, a conceptual framework was presented.

2.1 Theoretical Framework

2.1.1 Protection Motivation Theory (PMT)

The theoretical framework that directs this study is Protection Motivation Theory (PMT). This theory describes how people evaluate threats cognitively and determine the optimal course of action for self-defence (Hedayati et al., 2023). PMT is a suitable framework to examine user confidence in online banking because of the nature of online banking, which includes security issues and user trust. This theory offers a strong foundation for comprehending how technology infrastructure and user knowledge affect security perceptions, which then affect users' confidence in online banking.

PMT was first proposed by Rogers (1975) and subsequently developed by Maddux and Rogers (1983). This theory is predicated on the basic concepts of cognitive appraisal processes and their relationship to stress management. It suggests that people engage in protection motivation, which is based on the relations between the

threat appraisal and coping appraisal processes (McLeod et al., 2015). Threat appraisal assesses inappropriate behaviours, or harmful behaviours, and is influenced by perceived threat event severity and perceived likelihood of the threatening event happening, which is personal vulnerability. The effectiveness of the suggested response behaviour (response efficacy), perceived self-efficacy, and response costs all influence the coping appraisal process, which assesses one's capacity to deal with and avoid the impending risk.

This theory aids in the explanation of how customers develop confidence in online banking by recognising cyberthreats and trusting in the security measures of the online banking platform. Firstly, PMT explains how user knowledge affects a user's confidence in online banking. The term "user knowledge" describes a person's understanding of an online banking system, including their comprehension of possible security risks and how to take precautions. From the PMT perspective, this user knowledge aligns with its threat appraisal and self-efficacy. This is because a knowledgeable user is more likely to be aware of the potential risks, such as phishing attacks and identity thefts (vulnerability and severity), and to have greater confidence in their capacity to prevent them (self-efficacy). This cognitive comprehension helps self-confidence in using online banking. According to the previous study, user knowledge has a major impact on self-efficacy and perceived danger, both of which have an impact on protective behaviour. For instance, Alrababah et al. (2024) discovered that users' confidence in managing online security risks and perceived threats was strongly predicted by their cybersecurity knowledge.

Apart from that, this study utilises PMT to explain how technology infrastructure affects a user's confidence in online banking. Technology infrastructure implies the accessibility and efficacy of technological security measures such as biometric login and two-factor authentication (2FA). According to PMT, a robust technology infrastructure helps ensure response efficacy by giving users confidence that the

system can effectively mitigate risks and protect them. Users will be more confident in online banking if they believe these security measures to be reliable and efficient. In the other meaning, the users' confidence may increase if financial institutions provide effective and reliable security measures in the online banking system. In the study of Ismail and Kasiran (2023), the authors looked at the security measures of online banking in Malaysia and how they affect user confidence. The results indicate that a user's confidence and inclination to use online banking services are positively impacted by their opinions of a strong security architecture.

User confidence is the assumption that using online banking services is dependable, trustworthy and secure. When users believe that the system offers adequate protection and they have the ability to handle the possible risks with the help of technology and their own knowledge, it is the result of a successful protection motivation process.

2.1.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) serves this research to inspect how system reliability together with perceived data protection affects online banking user confidence. The widely adopted theory created by Davis describes user technology acceptance through TAM (Mishra et al., 2022). This theory provides a suitable framework for explaining how system reliability and perceived data protection influence user confidence in online banking, as online banking is a technology that relies heavily on users' simplicity of use and perceived usefulness.

The technology acceptance model was proposed by Fred Davis (1985) to find out how and why people use new technology. This model was created by Fishbein and

Ajzen (1975) and was derived from the Theory of Reasoned Action. The Theory of Reasoned Action proposed that user motivation can be explained by actual system use, which is directly influenced by system features and capabilities (Chuttur, 2009). According to Chuttur (2009), perceived usefulness, perceived ease of use and attitude toward using the system were the factors suggested by Davis to explain user motivation. The first two essential beliefs on the model refer to perceived usefulness and perceived ease of use because these influence user system adoption intentions before affecting real-world behaviour. TAM can be used with a wide range of technologies, such as online banking and e-commerce. It is also simple and effective.

System reliability can be considered synonymous with the TAM concept of perceived usefulness because it describes the smooth and bug-free operation of online banking platforms (Kovalan et al., 2021). A reliable online banking system with low downtime and minimal transaction faults leads users to maintain trust in the system while continuing their use (Ojo et al., 2022). Users believe that this reliable system will help them manage financial tasks effectively. Additionally, TAM is used in this study to explain how user confidence in online banking is impacted by perceived data protection. Perceived data protection, which signifies information security, builds connections to perceived ease of use and trust in users (Yong & Kasiran, 2023). The combination of encryption methods together with secure access controls and proper privacy policies lets users feel secure enough to rely on their banking platform, hence enhancing their ongoing platform use without hesitation.

An application of TAM should lead to higher user confidence from both reliable systems and well-protected data. People who view their online banking system as both dependable and secure become more trustworthy in the platform as they gain increased confidence and recommend its use to others (Saif et al., 2022). The theoretical connection between this research aligns with the main goal to discover factors influencing user confidence about Malaysian online banking systems.

Modern financial digitisation depends heavily on user confidence because customers need consistent confidence to stay active on online platforms. User behaviour intentions can be viewed through TAM as technical factors combine with psychological factors to create their effects (Pambudi et al., 2021). Studies of these interconnections between factors enable Malaysian financial institutions to develop better digital platforms and enhance customer confidence.

2.2 Review of Literature

2.2.1 User Confidence towards Online Banking Security and Safety Features

User confidence in online banking refers to the trust and assurance users have in the security mechanisms and safety measures implemented by financial institutions to protect their privacy information (Choudhuri et al., 2024). It is the fundamental basis for the establishment of connections between banks and their customers and users, which greatly affects the individuals' readiness to participate in online transactions and disclose sensitive information through digital platforms. According to Siagian et al. (2022), users are more likely to engage in online banking transactions and services when they perceive security measures to be more effective and reliable. This confidence is closely linked to perceived security mechanisms, perceived usefulness, fraud prevention mechanisms and regulatory compliance.

User confidence plays a crucial role in the adoption and continued use of online banking services. It is reinforced when a seamless and user-friendly interface is

combined with intuitive security features, significantly enhancing trust in the safety of online banking transactions (Choudhuri et al., 2024). This measure serves as a protective barrier, safeguarding customer data and ensuring that transactions are secure. Furthermore, the user confidence is shaped by the transparency of security measures, the responsiveness of security breaches, and the effectiveness of their customer support in addressing concerns related to security threats (Ou et al., 2022). A study has discovered that technical glitches, system downtimes and unauthorised transactions contribute to users' scepticism regarding the effectiveness of online banking platforms, further contributing significantly to trust and confidence among users (Vafaei-Zadeh et al., 2024).

With it, a study found that financial literacy and user confidence in cybersecurity play a key role in shaping online banking satisfaction, emphasising concerns about cyberthreats and information security (Hasan et al., 2025). These findings underscore the necessity for banks to continuously enhance cybersecurity measures and user engagement to greatly strengthen confidence in online banking security and safety features. Overall, a secure and reliable online banking environment is essential in fostering user confidence. This study investigates the factors influencing user confidence towards online banking security and safety features.

2.2.2 System Reliability

System reliability is the ability of online banking platforms to conduct secure transactions consistently, steadily, and reliably without interruptions, delays, or security breaches (Khan et al., 2023). Reliability, error-free processing, and resilience to cyber threats are some of its features. Conversely, user confidence is defined as customers' trust and confidence in online banking's security and safety features, which affects their willingness to accept and make use of online banking services (Tian et al., 2023). Customers feel more at ease conducting transactions

and are less concerned about fraud or technical issues when they believe that the system is reliable.

Research has shown that user confidence and system reliability are significantly correlated. When online banking services function properly without problems, delays, or security breaches, users start to have confidence in them (Ayinaddis et al., 2023). For instance, Khan et al. (2023) found that if customers face fewer technical difficulties with online banking services, they are more inclined to stick to them. In a similar vein, Tian et al. (2023) highlights how strong encryption, instant fraud alerts, and seamless transaction processing boost user confidence. In essence, users are more at ease embracing and utilising online banking when the system is more reliable.

The expected relationship is clear: greater user confidence is a direct result of increased system reliability. When banks make investments in strong cybersecurity, minimise interruption, and guarantee smooth transactions, users feel protected (Dangaiso et al., 2024). This statement is proven by Sasono et al. (2021), which shows that banks with fewer technical issues have higher user satisfaction and confidence. Consistently performing users are less likely to worry about fraud or errors, which increases their willingness to use online banking for routine transactions.

According to some research, placing too much emphasis on security measures which are a part of system reliability may occasionally explode. Excessively complicated authentication procedures, frequent password changes, or superfluous security measures can irritate users and reduce their confidence in the system's functionality (Rahi et al., 2020). However, rather than reliability by itself, this is the result of poor implementation. A balanced system that is safe and easy to use increases confidence while reducing challenges.

Some disagreement in studies regarding the significance of this relationship. Even in cases where a system is highly reliable, outside factors like negative media coverage or prior fraud experiences may erode user confidence (Rahi et al., 2021). This implies that while reliability is essential, as other social or psychological variables are involved, it might not always be enough to build confidence.

In conclusion, the majority of studies show that user confidence in online banking is influenced by system reliability. Even though the system remains reliable, there are rare instances when excessive security measures frustrate users or when outside factors decrease confidence. According to this conflicting information, banks must take user experience and outside perceptions into account when fostering confidence, although reliability is significant.

H_1: System reliability significantly influences user confidence towards online banking security and safety features.

2.2.3 User Knowledge

A user's understanding of online banking security features, risks, and standard procedures is known as 'user knowledge'. This entails being aware of phishing attempts, understanding authentication methods such as two-factor authentication, and learning how to protect personal data. User knowledge is essential to building a sense of confidence in online transactions in Malaysia, where the use of online banking is growing (Haider et al., 2024). Lack of basic knowledge may cause users to be unwilling or mistrustful of online banking services because they are unable to assess security measures.

Studies show that greater user knowledge boosts confidence in online banking security. Users feel safer and more knowledgeable once they recognise the way security features, such as encryption, fraud detection, and secure login methods, work (Li et al., 2020). For instance, a Malaysian study discovered that users were more likely to have confidence in banking services after receiving education on security measures (Dogruel et al., 2021). Users can conduct online banking transactions without worrying about fraud or security breaches due to knowledge, which reduces insecurity.

The expected relationship shows positive as confidence rises; user knowledge grows. Users who are well-informed can distinguish between real safety measures and risky situations, which gives them greater confidence during their transactions online. Financial knowledge and security awareness may increase confidence within online banking, according to a Malaysian study on online payments (Chauhan, 2024). Because users are more confident about their transactions, banks that utilise user education programmes typically discover greater rates of acceptance.

Although the majority of research shows a positive correlation, certain studies indicate that overconfidence, which arises from a lack of knowledge, can have a reverse impact. Users who lack insight but believe they understand safety may underestimate risks, leading to irresponsible actions like overlooking security warnings. Conversely, the opposite effect is less common and occurs when knowledge is insufficient rather than achieved (Haider et al., 2024).

According to some studies, knowledge alone might not always improve confidence if it is overshadowed by other factors like prior fraud experiences or a negative bank reputation. For instance, even knowledgeable users might not be sure whether they

think banks have handled safety incidents correctly (Rodrigues et al., 2022). This indicates that although knowledge is important, reliable banking practices must be implemented in order to truly increase confidence.

In conclusion, the findings of prior research were not entirely consistent. Although the majority of studies indicate that user knowledge enhances confidence, some highlight situations in which knowledge is insignificant because of overconfidence or misunderstandings from external sources. More research is needed on this difference, especially in Malaysia's developing online banking sector, where user confidence and knowledge in institutions are always changing.

H_2: User knowledge significantly influences user confidence towards online banking security and safety features.

2.2.4 Perceived Data Protection

Perceived data protection in online banking refers to the extent to which users believe that their personal and financial data is securely handled, transmitted and stored within an online banking system (Wang et al., 2024). Users are concerned that their personal information may be altered or misused without their consent. It encompasses trust and confidence, security technologies and compliance with legal regulations that ensure data confidentiality and integrity. The concept itself is rooted in information security systems, which suggest that users' confidence in online platforms depends on their belief in robust protective measures. Besides, perceived data protection is influenced by transparency in data handling practices and the effectiveness of security measures that are adopted by banks (Lee et al., 2022). A study by Cheryl and Ng (2022) highlights that clear communication about data security policies, such as the Personal Data Protection Act (PDPA), can significantly

impact user confidence in online data protection in the realm of banking systems security.

There are some studies that have shown that perceived data protection has a major impact on user confidence towards online banking security and safety features. Studies highlight that when users perceive their data as securely protected against unauthorised access, they are more likely to trust and continue usage of online banking services (Suci & Dahlan, 2023). This trust will contribute to the user confidence, which is driven by the assurance that financial institutions adhere to stringent security standards, thus reducing concerns over cyber threats such as malware, phishing and even identity theft. On the contrary, their confidence diminishes when users perceive weak data protection mechanisms, leading to reluctance in utilising digital financial services (Gupta & Shukla, 2024). Therefore, perceived data protection plays a crucial role in shaping the overall user confidence towards the security and safety of online banking platforms.

The elements of perceived data protection on user confidence may vary across different demographic groups and levels of digital literacy. However, some research indicates instances where perceived data protection does not significantly influence user confidence towards online banking security. Research found that for certain groups of users, especially those who have previous exposure to digital financial services, the perceived importance of data privacy in influencing their confidence is reduced (Martínez-Navalón et al., 2023). This reduced significance may occur when user trust in financial institutions has already been established, making additional security enhancements seem redundant.

In short, there are inconsistent findings in the prior research about the influence of perceived data protection on user confidence towards online banking security. The bulk of studies indicates that perceived data protection has a significant relationship

to user confidence towards online banking, while some studies have shown an insignificant relationship as well.

H_3: Perceived data protection significantly influences user confidence towards online banking security and safety features.

2.2.5 Technology Infrastructure

In online banking, technology infrastructure includes the basic infrastructure, software, and security mechanisms that allow for online financial transactions. This comprises encryption mechanisms, methods of authentication like fingerprints or two-factor authentication, online computing, and fraud detection software (Kimiagari & Baei, 2021). A solid infrastructure ensures that banking activities run smoothly, securely, and efficiently, reducing risks such as data breaches and illegal access. Without reliable technology, users could experience transaction failures, security concerns, or bad service experiences, weakening their confidence in online banking services (Das & Ganguly, 2024).

User confidence in online banking is highly dependent on perceived safety and system reliability. According to research, when banks invest in advanced safety measures that involve complete encryption, real-time fraud monitoring, and secure mobile payment protocols, users feel more confident about their finances (Bojjagani et al., 2021; Najaf et al., 2021). Biometric identification, such as fingerprint or face recognition, has been shown to improve confidence by reducing the chance of stealing passwords (Das & Ganguly, 2024). Furthermore, cloud-based banking systems increase accessibility and reliability, increasing customer satisfaction with online transactions (Vinoth et al., 2021). Essentially, the more reliable and transparent the technological infrastructure is, the greater the user confidence.

The majority of studies conclude that increased technological infrastructure boosts user confidence. Customers view the system as reliable and are more willing to use online banking when banks have strong cybersecurity measures in place. The impression of control and security is enhanced by AI-powered fraud detection, secure login processes, and instant transaction warnings (Bueno et al., 2024). Research indicates that users in Malaysia, where the use of online banking is growing, prioritise security over convenience, suggesting that technical security has a direct impact on users' confidence (Agu et al., 2024).

Certain studies show that user confidence may motivate banks to upgrade their systems, despite the majority of research suggesting that technological infrastructure has a one-way impact on user confidence. For instance, banks may improve their infrastructure in response to user requests for greater security because of the rise in cyber threats (Dwivedi et al., 2021). The opposite effect, however, is less well-established than the primary association.

According to certain studies, the relationship between technology and confidence is not always significant. Even with increased security measures, some users remain suspicious, particularly if they have already experienced fraud (Bojjagani et al., 2021; Pea-Assounga et al., 2024). Furthermore, users may become dissatisfied rather than comforted by too complicated security measures, such as multi-step authentication, which causes delays in transactions (Kimiagari & Baei, 2021). Occasionally, relying too heavily on equipment without human intervention can undermine confidence, demonstrating that technology may not always be sufficient.

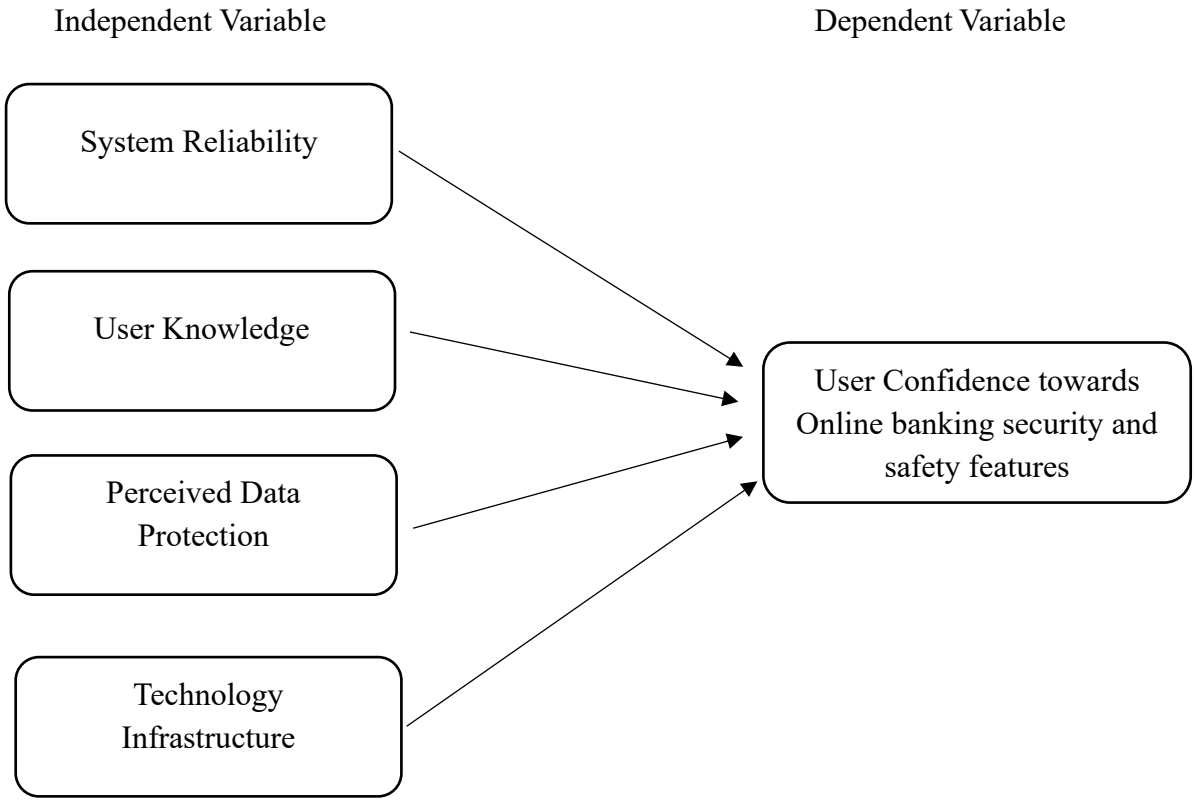
In conclusion, the majority of research indicates that the relationship does not always exist, an efficient technology infrastructure boosts user confidence in online banking. While enhanced security measures usually increase confidence, other

factors include disclosure, prior fraud incidents, and user satisfaction. Some users are still concerned despite technological advancements, which suggests that banks need to strike a balance between safety and convenience to fully gain user confidence.

H_4: Technology infrastructure significantly influences user confidence towards online banking security and safety features.

2.3 Conceptual Framework

Figure 2.1*: Conceptual Framework*



2.4 Conclusion

This chapter covered two theoretical frameworks, namely Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM). The literature review examined the independent variables of system reliability, user knowledge, perceived data protection, and technology infrastructure, as well as the dependent variable of user confidence towards online banking security and safety features. Lastly, the conceptual framework is developed in this chapter.

CHAPTER 3: RESEARCH METHODOLOGY

3.0 Introduction

The research method employed in the study will be presented in this chapter. Firstly, it begins with an overview of the research design, followed by a comprehensive description of the sampling method, research tools, measurement scales, and key terms. The procedures for data processing and analysis are further elaborated. Lastly, a quantitative research design was adopted, which involved the primary data collection method.

3.1 Research Design

A research design is a comprehensive plan or methodology of how a researcher conducts research. The two primary categories of research methods are qualitative and quantitative research. According to Kandel (2020), quantitative research is a systematic technique that uses numerical data collection and analysis to understand and forecast phenomena. Qualitative research is collecting information by observation. This research explored the variables that affect user confidence in online banking using quantitative research. A preset questionnaire would be distributed online by Google Forms to collect information from the respondents that meet the target criteria. Besides convenience sampling, other types of non-probability sampling are adopted in this study due to their time and cost-effectiveness (Stratton, 2021). Statistical Package for Social Sciences (SPSS) was used in this research to analyse data collected to achieve research objectives.

3.2 Data Collection Method

As stated by Mazhar et al. (2021), data collection is a methodical process of obtaining, evaluating, and interpreting information needed to investigate the variables that affect user confidence in online banking. Mazhar et al. (2021) also mentioned that data collection is an important stage for conducting research. The data collection method is a tool or technique used to collect data (Mwita, 2022). The first type of data collection method is primary data, while the second type is secondary data. The accuracy and results of research can be affected by how data was collected.

3.2.1 Primary Data

This study employed primary data to gather information that is needed to achieve research objectives. Primary data is information collected directly from the respondents and is original (Mwita, 2022). These are examples of primary data, including the observation method, interview method, questionnaire, and case study (Mazhar et al., 2021). Primary data has more reliability and authenticity compared to secondary data because primary data is unchanged and unpublished by anyone (Taherdoost, 2021). Primary data was chosen due to its cost-effectiveness, reliability, precision, and convenience. The survey is chosen by distributing an online questionnaire to respondents that meet the criteria to investigate how the variables affect user confidence in online banking. Questionnaires suitable for research need to gather data from a significant number of people quickly.

3.3 Sampling Design

3.3.1 Target Population

All respondent who fulfils the requirements and characteristics relevant to the research objective, as well as the subset of the larger population is target population (Willie, 2024). The selection of survey respondents must be eligible and qualified to meet the requirements, ensuring the accuracy of the data collected. This study proposes to identify the variables that affect user confidence towards online banking security and safety features in Malaysia. According to Harris et al. (2016), individuals above 50 years old prefer to use traditional banking services and are less engaged in online banking, while individuals below 18 are not eligible to use online banking. Therefore, Malaysian citizens aged 18-50 years are the target population in this study.

3.3.2 Sampling Location

The sampling location is the location selected to collect data. The sampling location is chosen as Selangor, Perak, and Penang. According to Selvanathan et al. (2017), Selangor, as one of the developed states, has widespread use of online banking, and users have high technology acceptance. Therefore, Selangor could provide more representative samples and data. Besides, the mature financial background of Penang's users is also suitable for more accurate observation (Syed Mizuri & Mat

Lazim, 2024). This is because they have more experience and stable behavioural patterns. Last but not least, Perak is chosen as one of the sampling locations due to its mix of urban and semi-urban areas, which can get a fresh perspective and reduce regional bias. Although Selangor and Penang also have a mix of urban and semi-urban areas, their populations are largely urban and highly industrialised (Abdullah et al., 2009). This means they mostly reflect urban online banking behaviour. In contrast, Perak offers a more balanced picture and makes the research findings more broadly applicable. These three states also had a mix of young adults and older residents, such as university students and working adults. As a result, selecting Selangor, Perak, and Penang can include Malaysia's diverse socioeconomic backgrounds, which provide a more complete and more efficient overview of the variables affecting user confidence in online banking.

3.3.3 Sampling Technique

According to Taherdoost (2016), sampling techniques can be divided into two categories, which are probability sampling and non-probability sampling. The research shows that probability sampling means every individual has an equal chance and is randomly selected for the sample. Examples of probability sampling include simple random, stratified random, cluster sampling, systematic sampling, and multistage sampling. In contrast, not every individual has an equal chance, and non-random sampling is known as non-probability sampling (Stratton, 2021). Quota sampling, snowball sampling, judgement sampling, and convenience sampling are examples of non-probability sampling.

Since this research focuses on a specific target population, a non-probability sample is chosen for the survey, particularly convenience sampling. Convenience sampling means research collects data from people who are the easiest to reach or most

readily available (Golzar et al., 2022). This method was selected due to its affordability, easy accessibility, time efficiency and ease of implementation (Stratton, 2021). By applying convenience sampling, researchers are able to conduct the study easily and efficiently. Furthermore, the questionnaires will be distributed to respondents who meet specific criteria relevant to the objectives of this research.

3.3.4 Sampling Size

Justifying an adequate sample size is important in any research (Lakens, 2022). According to the author, the main purpose of determining an appropriate sample size is to ensure the data collected is aligned with the research objectives and gives valuable information to the study. Krejcie and Morgan (1970) had proposed the "Table for Determining Sample Size for a Finite Population" to calculate the sample size by the specified population. In order to ensure an adequate sample size, the sampling size in this research is determined based on the table (refer to Appendix 3.1). The Department of Statistics Malaysia reports that the population in Perak, Penang, and Selangor is 7,571,014. Since the target population exceeds 1,000,000, referring to the "Table for Determining Sample Size for a Finite Population", 384 respondents are suggested. Therefore, the minimum number of respondents required is 384.

3.4 Research Instrument

3.4.1 Questionnaire Design

Mcleod (2023) indicated that a questionnaire is a type of research tool used to gather information from individuals. A collection of questions makes up a questionnaire. Questionnaires can evaluate the behaviour, attitudes, preferences, and intentions of relatively large subjects more easily and affordably compared to other approaches. Both open-ended and closed-ended questions are frequently used in questionnaires to gather information. This is advantageous as it allows for the collection of both quantitative and qualitative data. For open-ended questions, respondents can provide a free-form text response (Rosala, 2024). The example of an open-ended question is “Tell me about the last time you used the website.” However, respondents are confined to answering only one of a few viable replies when asked closed-ended questions. “When was the last time you used the website?” is an example of a closed-ended question. In this research, Google Forms was used to conduct the questionnaire online. The Google Forms were distributed to the target population through social media such as WhatsApp, Instagram, and Facebook.

In this research, the questionnaire is separated into 6 parts. The first part, Section A, includes the respondent’s demographic. There are seven demographic questions needed in this section: gender, ethnic group, state, age group, educational level, occupation and online banking services of the respondents. The purpose of this demographic information is to understand the background and characteristics of the respondents. The second part, Section B, includes the questions to determine the dependent variable in this research, which is user confidence towards online banking security and safety features. Sections C to F comprise the questions about the independent variable in this research, which are system reliability, user knowledge, perceived data protection, and technology infrastructure.

There are the seven-point Likert scale and the five-point Likert scale to quantify something that is impossible to measure using standard measurement methods (Joshi et al., 2015). Sections B to F of this questionnaire are measured utilising a Likert scale with five points. This five-point Likert scale is needed to be necessary in order to convert a person's subjectivity into an objective reality. For example, attitudes, perceptions, and views are the qualitative characteristics that can be quantitatively transformed by using a five-point Likert scale. The measurements for the five-point Likert scale are 1 for "Strongly Disagree", 2 for "Disagree", 3 for "Neutral", 4 for "Agree", and 5 for "Strongly Agree" (Nyutu et al., 2020). In Section B until Section F of the questionnaire, respondents are required to answer the questions by choosing one of the scales (1-5).

3.4.2 Scale of Measurement

The scale of measurement is a crucial component of data collection, processing, and presentation of the data (Mishra et al., 2018). There are four types of scales of measurements: nominal scale, ordinal scale, interval scale, and ratio scale. The scales of measurements that are applied in this research are nominal scale, ordinal scale, and interval scale.

3.4.2.1 Nominal Scale

The nominal scale is the most basic level, as the letters and numbers given to the item act as labels for categorisation or identification (Dalati, 2018). There is no intrinsic order, distance, or absolute zero level for the nominal scale. Nominal data is the gathering of information about a variable that can be separated into two or

more classifications which are mutually exclusive and collectively exhaustive. This nominal scale is frequently employed in questionnaires when collecting data from significant subsets of the population. Respondents' gender is the illustration of a nominal scale.

An example of the Nominal Scale

Gender:
( ) Male
( ) Female

3.4.2.2 Ordinal Scale

Ordinal and nominal scales are similar (Mishra et al., 2018). However, an ordinal scale has a distinct ordering, which differentiates these two scales. This means that data are arranged and classified according to their distinct categories on an ordinal scale. There is a ranking and comparison between the data; however, the differences between the rankings might not be equal. An illustration of an ordinal scale that was employed in this questionnaire is the different age groups of the respondents.

An example of the Ordinal Scale

Age:
( ) 18 - 23
( ) 24 - 29
( ) 30 - 35
( ) 36 - 41
( ) 42 - 46
( ) 47 - 50

3.4.2.3 Interval Scale

The interval scale is based on the idea that the distances between 1 and 2 and 2 and 3 should be equal (Dalati, 2018). For instance, the calendar time is also an interval scale. The reason for this is that the gap between 2000 and 2020 is equal to the gap between 2020 and 2040. However, it is not possible to claim that the year of 2020 is twice as much as 1010. The reason for this is that there is not a real zero point on this interval scale. The common example of this interval scale is the temperature in Celsius or Fahrenheit. The Likert scale with five points that was employed from Section B to Section F of the questionnaire is an example of an interval scale.

An example of the Interval Scale

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The use of two-factor authentication increases my confidence in online banking.	1	2	3	4	5

3.4.3 Pilot Test

Pilot test research, according to Lowe (2019), is a tiny feasibility study used to assess several components of the protocols created for larger, more thorough, or confirmatory research. Basically, a pilot study is carried out to avoid the possibility of a fatal problem in a study that is pricey in terms of both time and money. Instead

of addressing particular research issues, its primary objective is to prevent researchers from beginning a large-scale study before having adequate understanding of the recommended methodologies. In every study, a pilot test is carried out to make sure validity is attained (Gani et al., 2020). Before the study is conducted, this is referred to as a test run for a research instrument.

3.4.3.1 Cronbach's Alpha of Pilot Test

According to Cronbach (1951), alpha was developed and first applied to assess a psychometric instrument's reliability. Cronbach's alpha assesses the internal consistency or dependability of several items, measurements, or ratings (Bujang et al., 2018). In other words, it assesses the reliability of a questionnaire's feedback, which will show how stable the tools are. The dependability of a questionnaire's response means the degree of correlation between the responses. In determining the sample size of Cronbach's alpha, Johanson and Brooks (2009) declared that when the sample size (n) is between 30 to 50, it means the sample size is completely random. Therefore, N = 30 is acknowledged as a suitable minimum sample size used in Cronbach's alpha. Besides, a pilot study participation of 10 would be a fair quantity for research that contained a total of 100 participants (Johanson and Brooks, 2009). However, it was uncertain if this meant 10% of the total sample size of the research. In this research, a total sample size of 384 is used. 10% of the total sample size is 38.4 (384 × 10%). Compared with the 30-sample size, 38.4 is higher; therefore, a sample size of 38 is being used to determine the Cronbach's alpha. The diagram below displays the criteria of Cronbach's alpha and its interpretation.

Table 3.1: *Cronbach's Alpha Criteria*

Cronbach's Alpha Criteria	Classification
$\alpha \geq 0.9$	Very good
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Be accepted
$0.6 \leq \alpha < 0.7$	Doubtful
$0.5 \leq \alpha < 0.6$	Bad
$\alpha < 0.5$	Not acceptable

(Source: Siswaningsih et al., 2017)

Table 3.2: *Reliability Assessment for the Pilot Test*

	Variables	Cronbach's Alpha	Dependability
Dependent Variable	User Confidence	0.831	Good
Independent Variable	System Reliability	0.810	Good
Independent Variable	User Knowledge	0.811	Good
Independent Variable	Perceived Data Protection	0.893	Good
Independent Variable	Technology Infrastructure	0.782	Acceptable

Table 3.2 displays the reliability test of a pilot test. Based on the table, the explained variable, user confidence, had a Cronbach's alpha of 0.831, which is considered good in reliability tests. Besides, Cronbach's alpha value for the independent variable of system reliability was high, at 0.810. The Cronbach's Alpha value for the independent variable of user knowledge was 0.811, while the independent variable of perceived data protection provided a Cronbach's Alpha value of 0.893.

These three independent variables were considered good in reliability tests. Among the independent variables, only technology infrastructure presented acceptable reliability, as Cronbach's alpha is 0.782. As a result, all variables show an acceptable to good range in the reliability test.

3.5 Data Analysis

According to Kotronoulas et al. (2023), data analysis is the methodical cleaning, manipulation, and comprehension of raw quantitative data using statistical and computer tools. In order to meet research goals, it looks for patterns, correlations, or trends in data and turns them into relevant evidence. For analysis of statistics, organising data, and visualisation in scientific research, SPSS is a well-liked proprietary application. Its features for descriptive statistics, regression analysis, predictive modelling, and hypothesis testing are extensive (Okagbue et al., 2021). The main advantage of SPSS is that large datasets with many variables are easily handled (Rahman & Muktadir, 2021).

3.5.1 Descriptive Analysis

The first assessment method used in study is descriptive analysis. Sample characteristics are highlighted by descriptive statistics. A simple method for reporting this data is to use frequencies (Kotronoulas et al., 2023). Descriptive analysis for the study will be focusing on demographics. Social demographics examines the population of a region, including its size, makeup, and historical trends (Zahra & Anoraga, 2021). The study selects the minimum number of respondents, 384, that are eligible and qualify for data collection, who are

Malaysian citizens aged 18-50 years from Selangor, Perak and Penang. Descriptive data is presented in tables, and fictitious examples show how to use central tendency and dispersion measurements in different situations (Malakar, 2023).

3.5.2 Inferential Analysis

Inferential analysis is one of the most significant types of data analytics used in research, as it enables researchers to draw conclusions about a larger population based on a representative sample (Alem, 2020). In the context of this study, this approach is particularly useful to investigate the elements that influence user confidence towards online banking security and safety features, based on data gathered from 384 respondents in Selangor, Perak, and Penang, Malaysia. Inferential statistical tools such as reliability testing and Pearson correlation analysis are employed. According to Shrestha (2020), the correlation coefficients help to determine the strength of variables' relationships as well as identify potential multicollinearity. Additionally, MLR analysis is conducted to test the hypothesised influence of the independent variables involving system reliability, user knowledge, perceived data protection and technology infrastructure on the dependent variable, which is user confidence towards online banking security and safety features.

3.5.3 Reliability Test

Reliability test is a fundamental aspect of quantitative research, ensuring that a measurement instrument consistently reflects the construct it intends to measure (Sürücü & Maslakci, 2020). It plays a key role in minimising random errors and supporting the stability of results. One widely used method for evaluating reliability is internal consistency, which is measured using Cronbach's alpha as a common indicator (Saidi & Siew, 2019). This statistic evaluates how closely related the items

in a scale are, indicating the reliability of the instrument. In recent studies, researchers have frequently used Cronbach's alpha to assess the reliability of their model constructs and measurement tools (Zakariya, 2022).

According to Saidi and Siew (2019), Cronbach's alpha values range from 0 to 1, with higher values reflecting stronger internal consistency and greater reliability. In social science research, a high value of above 0.90 indicates excellent internal consistency, while above 0.80 is considered good, and above 0.7 is acceptable. More specifically, values that are above 0.60 are referred to as questionable; those above 0.50 are poor. Any value below 0.50 is typically regarded as unacceptable (Tavakol & Dennick, 2011). By using the SPSS software, researchers can compute these values and eliminate low-performing items to improve the overall reliability of the scale (Rahman & Muktadir, 2021). Consequently, a high level of reliability enhances the accuracy of results, which can help in sound decision-making and research conclusions.

Table 3.3: *Cronbach's Alpha Rule of Thumb*

Cronbach's Alpha	**Internal Consistency**
$\alpha \geq 0.9$	Excellent
$9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

(Source: Saidi & Siew, 2019)

3.5.4 Multicollinearity Test

In a regression model, multicollinearity occurs when two or more predictor variables are closely related, producing similar or redundant data about the dependent variable. Given that it is challenging to discern the distinct impact of each predictor on the result, this could pose problems for regression analysis. Even though complete multicollinearity (an exact linear connection) is rare, it can still distort statistical findings, leading to inflated standard errors and inaccurate coefficient estimates (Chan et al., 2022; Skiera et al., 2021).

Researchers commonly use the Variance Inflation Factor (VIF), a statistical measure derived from regression analysis, to identify multicollinearity. The VIF measures the correlation between variables that increases the variance of a regression coefficient. It is determined by regressing each independent variable with the model's predictions. Multicollinearity is more significant when the VIF is higher (Sulaiman et al., 2019; Shamsabadi et al., 2023). A VIF < 10 indicates moderate multicollinearity, < 5 indicates significant multicollinearity, and ≥ 10 indicates extreme multicollinearity, requiring adjustment. Tolerance is the percentage of a predictor's variance that cannot be accounted for by other predictors. A value near 0 indicates potential danger, while a value near 1 indicates minimal multicollinearity. Myers provides a tolerance value of less than 0.1, while Menard suggests a 0.2 tolerance indicates collinearity issues (Senaviratna & Cooray, 2019).

This threshold point helps researchers decide if multicollinearity is severe enough to call for sophisticated techniques like principal component analysis or corrective measures like variable removal or combination (Kyriazos & Poga, 2023). The null hypothesis (H_0) frequently states that there is no significant multicollinearity among indicators when testing for multicollinearity. Multicollinearity is present, according to the alternative hypothesis (H_1). The study does not reject H_0 if VIF values are below the critical threshold (e.g., VIF < 5 or 10), suggesting that multicollinearity

is not a major concern. The study rejects H_0 if VIF values are greater than the threshold (e.g., VIF > 5 or 10), indicating that multicollinearity is problematic and needs to be fixed for reliable regression results (Chan et al., 2022). By carefully assessing multicollinearity using VIF and hypothesis testing, researchers can increase the precision and interpretability of their regression models.

3.5.5 Pearson Correlation

When assessing linear relationships between two variables, the Pearson correlation coefficient (r) is frequently utilised. It makes the assumptions of normality, linearity, and continuity (El-Hashash & Shiekh, 2022). The adaptive variable grouping method, which is based on Pearson correlation, uses the least amount of processing power to classify variables (Zhang et al., 2023). According to Gong et al. (2024), the range of values for the Pearson correlation coefficient (r) is [-1, 1]. Perfect positive correlation is represented by an r value of +1, while complete negative correlation is represented by an r value of -1. There is no linear signal relation if the value is zero (Šverko et al., 2022).

Table 3.4: *Degree of correlation relationship between two variables*

Condition	Degree of Correlation
$0.8 < P_{x,y} < 1.0$	remarkably strong correlation
$0.6 < P_{x,y} < 0.8$	strong correlation
$0.4 < P_{x,y} < 0.6$	moderate correlation
$0.2 < P_{x,y} < 0.4$	weak correlation
$0.0 < P_{x,y} < 0.2$	remarkably weak or correlated

(Source: Ikhwan et al., 2024)

3.5.6 Normality Test

After that, the normality test acts as a preliminary data screening technique, particularly when using software like SPSS. It plays a critical role in determining the appropriate statistical approaches for data analysis and evaluating measures of central tendency (Mishra et al., 2019). Normality implies that all variables or linear groups of variables must have a normal distribution. According to Hatem et al. (2022), normality can be examined through both statistical procedures and graphical representations such as histograms. These tests are typically conducted before proceeding with inferential statistical analysis to ensure that the underlying population data approximates a normal distribution. It reflects the assumption of normality, which serves as a foundational requirement for conducting inferential statistical analyses.

Shkak et al. (2020) highlighted that the normality of data can be assessed by comparing the distribution curve shapes to a theoretical normal curve. A histogram that shows a bell-shaped curve symmetric around the mean implies that the information is likely normally distributed. In addition, the kurtosis and skewness values serve as quantitative indicators to evaluate the assessment of normality. When sample sizes exceed 300, data can be considered as normally distributed if the skewness and kurtosis values are less than 2 and 7, respectively (Khatun, 2021). Also, the normality assumptions are generally fulfilled when skewness falls within a range of -2 to +2, and kurtosis falls within a range of -7 to +7 (Khatun, 2021). As a result, understanding and testing for normality is essential for guaranteeing the reliability and validity of conclusions drawn from inferential statistics.

3.5.7 Multiple Linear Regression

Multiple Linear Regression (MLR) is a commonly used statistical method that evaluates the explained variable's value with multiple explanatory variables (Martin et al., 2017). Within the framework of this research, MLR is deemed appropriate, as it enables the analysis of how the independent variables, such as system reliability, user knowledge, perceived data protection, and technology infrastructure, affect the dependent variable, which is user confidence towards online banking security and safety features. The MLR analysis was conducted using SPSS, which generated several key outputs involving Model Summary, ANOVA, and Coefficients tables (Adhikari, 2022). These outputs allow researchers to interpret the strength and direction of relationships among the variables.

Additionally, the R-squared value, or coefficient of determination, is applied to assess model fit within the regression analysis. This measure shows the proportion of variance in the explained variable that can be accounted by the explanatory variables (Gao, 2023). In social science research, an R-squared value of 0.10 or above is acceptable when the predictors are statistically significant (Ozili, 2022). Within the IVs – SR, UK, PDP and TI – this approach helps identify the key factors that influence user confidence towards online banking security and safety features in Malaysia.

Hypothesis testing was conducted based on the MLR results. Typically, a null hypothesis (H_0) assumes that a given regression coefficient is equal to zero, implying that there is no significant relationship, while the alternative hypothesis (H_1) posits that the coefficient differs significantly from zero, indicating a significant relationship exists (Kwak, 2023). Also, the individual coefficients were tested using t-tests, and an F-test was used for the overall model fit (Sureiman & Mangera, 2020). The decision was made based on the p-values, whereby if the p-value is less than the significance level (0.05), H_0 is rejected, confirming there is a

truly significant relationship between the DV and the IVs. Conversely, if the p-value is greater than 0.05, H_0 is not rejected, showing there is no statistically significant relationship involved (Kwak, 2023).

The multiple linear regression equation is provided:

Equation 3.1

$$UC_i = \beta_0 + \beta_1 SR_i + \beta_2 UK_i + \beta_3 PDP_i + \beta_4 TI_i + \mu_i$$

Where,

UC_i = User confidence towards online banking security and safety features

β_0 = constant value

β_j = Slope coefficient for each of the independent variables, j = 1,2,3,4

SR_i = System Reliability

UK_i = User Knowledge

PDP_i = Perceived Data Protection

TI_i = Technology Infrastructure

μ_i = Error term

3.6 Conclusion

The methods used in this research are finally studied in chapter three. Since this research is based on the primary research, the data was collected directly from the source of data. Descriptive and inferential statistics are used to analyse survey responses.

CHAPTER 4: RESEARCH RESULTS

4.0 Introduction

This study has gained 400 questionnaires, but only 384 questionnaires were used in this chapter based on the targeted population. Descriptive and inferential analysis were used to analyse data. The data analysis was conducted using SPSS.

4.1 Descriptive Analysis

4.1.1 Respondents' Demographic Profile

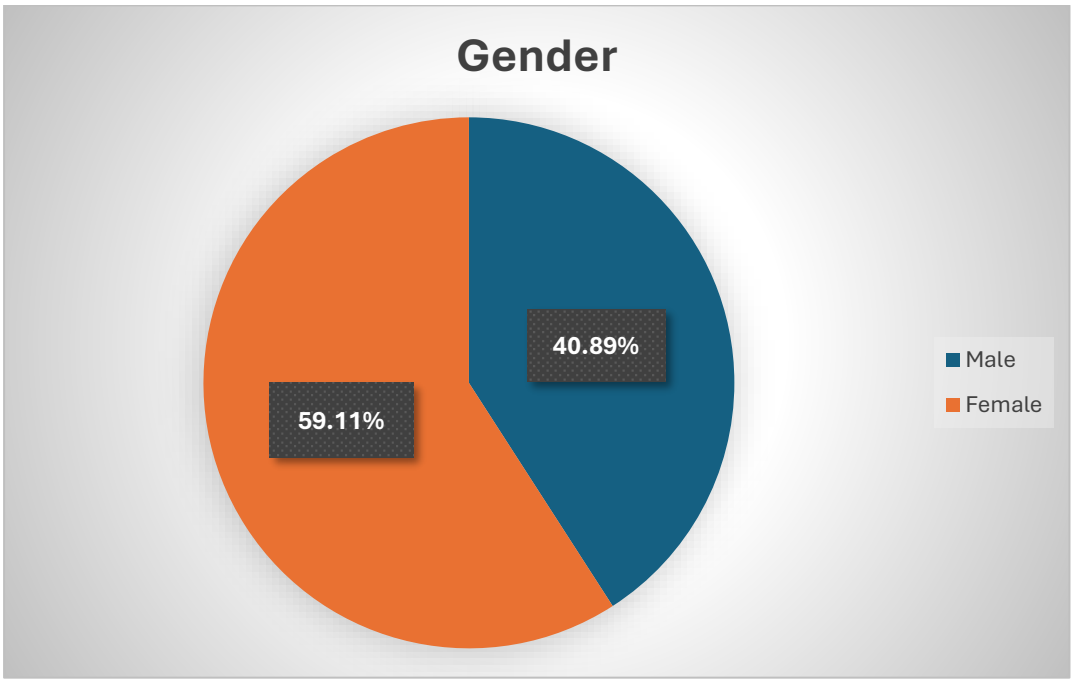
There are seven demographic categories in the questionnaire, including gender, race, state, age, education level, occupation, and online banking experience. Each category is examined in the section below.

4.1.1.1 Gender

Table 4.1: *Descriptive Analysis for Gender*

Gender	Frequency	Cumulative Frequency	Percent	Cumulative Percent
Male	157	157	40.89%	40.89%
Female	227	384	59.11%	100%

Figure 4.1: *Descriptive Analysis for Gender*



The gender ratio among the respondents is summarised in Table 4.1 and Figure 4.1. The respondents collected in this study are 384 respondents. According to the table and figure above, there are 59.11% of female responders and 40.89% of male responders. As a result, the number of female responders is more than male responders.

4.1.1.2 Race

Table 4.2: *Descriptive Analysis for Race*

Race	Frequency	Cumulative Frequency	Percent	Cumulative Percent
Malay	46	46	11.98%	11.98%

Chinese	296	342	77.08%	89.06%
Indian	42	384	10.94%	100%

Figure 4.2: *Descriptive Analysis for Race*

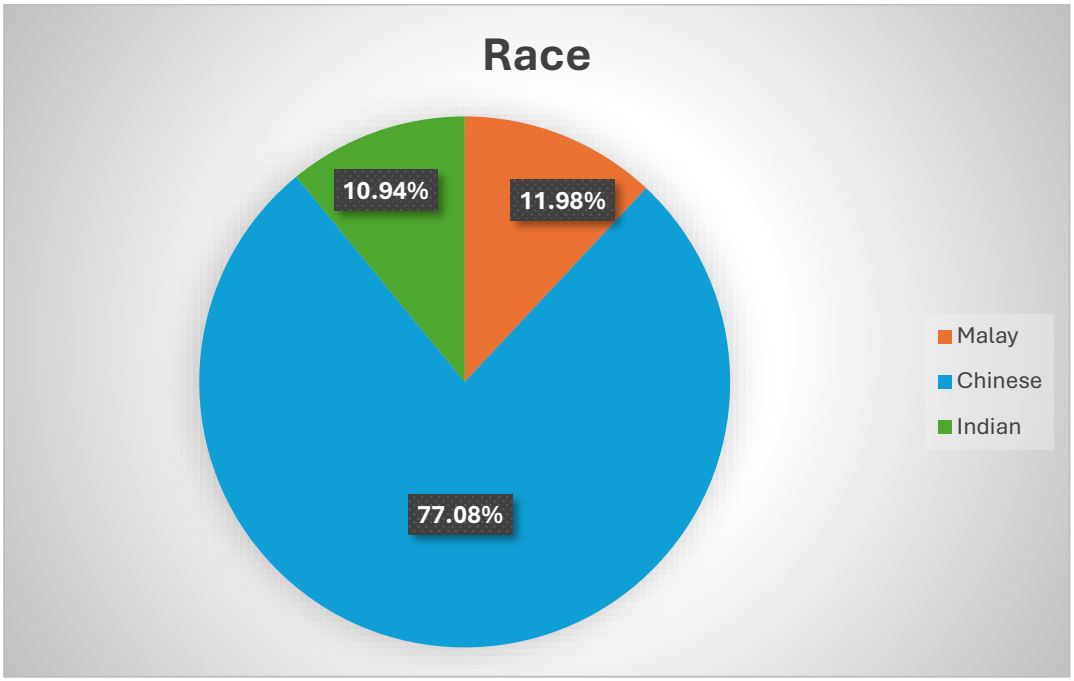


Table 4.2 and Figure 4.2 illustrate the respondents' races. Three races - Chinese, Malay and Indian are used to classify the respondents. From the table and figure above, a total of 296 (77.08%) respondents are Chinese. It means that Chinese make up the majority of the respondents. Besides, this study includes 46 (11.98%) Malay respondents and 42 (10.94%) Indian respondents.

4.1.1.3 State

Table 4.3: *Descriptive Analysis for State*

State	Frequency	Cumulative Frequency	Percent	Cumulative Percent
Penang	116	116	30.21%	30.21%
Perak	175	291	45.57%	75.78%
Selangor	93	384	24.22%	100%

Figure 4.3: *Descriptive Analysis for State*

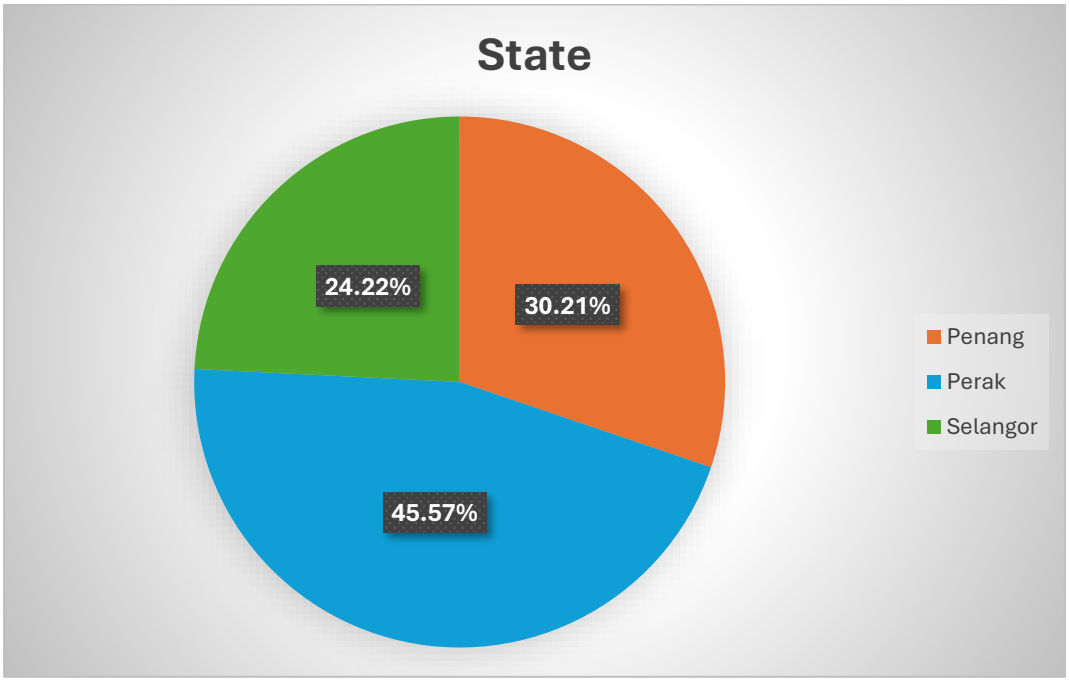


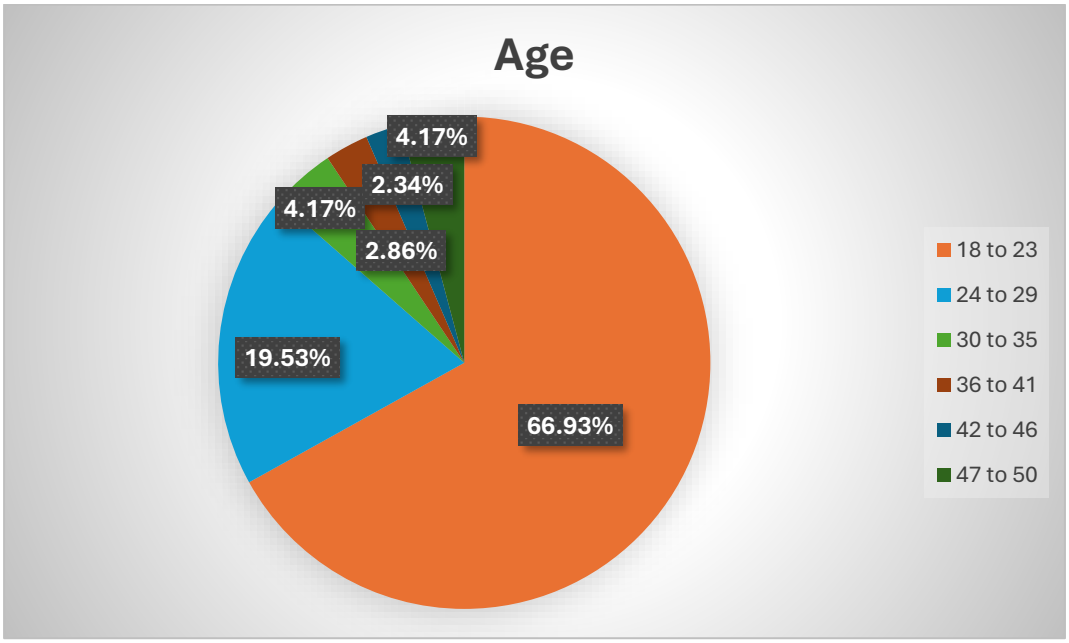
Table 4.3 and Figure 4.3 above show the ratio of states of the respondents. Perak, Selangor and Penang are three states that are included in this study. From the result above, the majority of the respondents are from Perak, which consists of 175 respondents, 45.57% of the total respondents. In addition, Penang provides the second highest number of respondents, which is 116 respondents, 30.21% out of the total respondents. 93 of the remaining respondents are from Selangor.

4.1.1.4 Age Group

Table 4.4: *Descriptive Analysis for Age Group*

Age	Frequency	Cumulative Frequency	Percent	Cumulative Percent
18 to 23	257	257	66.93%	66.93%
24 to 29	75	332	19.53%	86.46%
30 to 35	16	348	4.17%	90.63%
36 to 41	11	359	2.86%	93.49%
42 to 46	9	368	2.34%	95.83%
47 to 50	16	384	4.17%	100%

Figure 4.4: *Descriptive Analysis for Age Group*



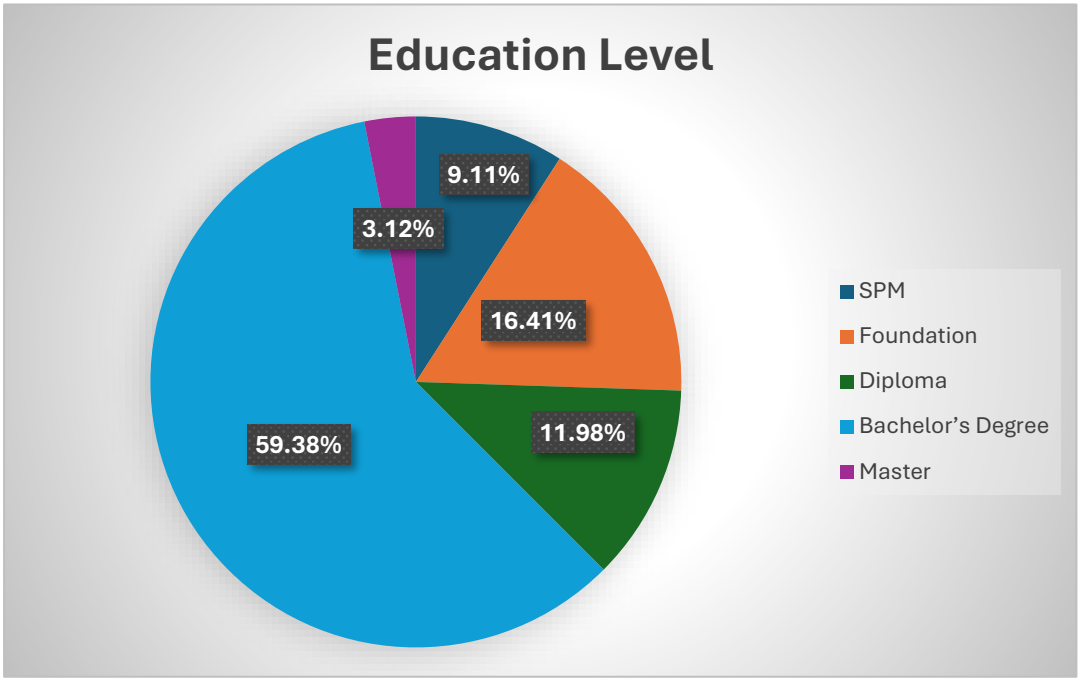
The age group of the respondents who participated in this research is displayed in Table 4.4 and Figure 4.4. From the table, the majority of the respondents are from the age group between 18 and 23 years old, which provides 66.93% of the total respondents. Besides, the age group between 24 and 29 years old involves 75 respondents (19.53%). After that, both age groups, 30 to 35 years old and 47 to 50 years old, include 16 respondents, which provides 4.17% of the total respondents. For the age group between 36 and 41 years old, it consists of 11 respondents, which is 2.86%. However, only 9 respondents out of 384 respondents fall within the age group of 42 to 46 years old.

4.1.1.5 Education Level

Table 4.5: *Descriptive Analysis for Education Level*

Education Level	Frequency	Cumulative Frequency	Percent	Cumulative Percent
SPM	35	35	9.11%	9.11%
Foundation	63	98	16.41%	25.52%
Diploma	46	144	11.98%	37.50%
Bachelor's Degree	228	372	59.38%	96.88%
Master	12	384	3.12%	100%

Figure 4.5: *Descriptive Analysis for Education Level*



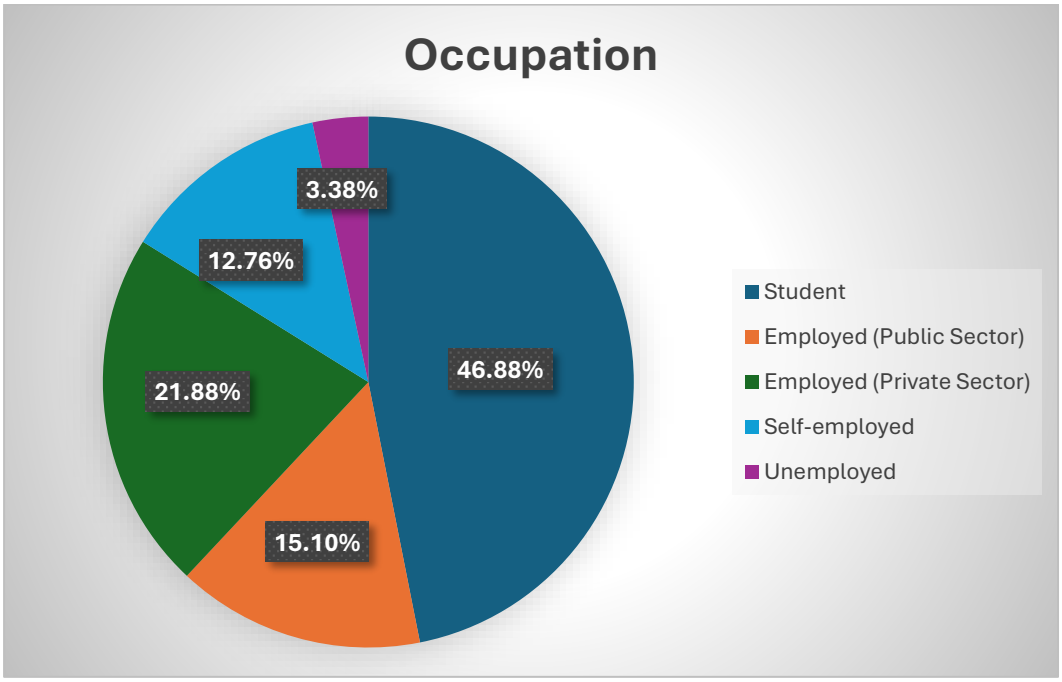
The education level of the 384 respondents is shown in Table 4.5 and Figure 4.5. The 384 respondents are divided into five education levels, which include Sijil Pelajaran Malaysia (SPM), Foundation, Diploma, bachelor's degree and master's degree. The majority of the respondents, as seen in the above table and figure, have a bachelor's degree as their educational background. There are 228 respondents who have the education level of a bachelor's degree, which provides 59.38%. Among these 59.38% of respondents, some of them are still pursuing the bachelor's degree, while some of them have already graduated with a bachelor's degree. The next education level is Foundation, which contains 63 of the respondents. After that, there are 46 respondents who have the educational background of a diploma, which is 11.98% of the total respondents. Besides, there are only 35 respondents who have the educational background of SPM, which comprises 9.11%. Last but not least, the rest of the respondents have the education level of master's, which is 3.12%. The education level of Doctor of Philosophy (PhD) is not included in the questionnaire. This is because there is only a low percentage of PhD holders in Malaysia.

4.1.1.6 Occupation

Table 4.6: *Descriptive Analysis for Occupation*

Occupation	Frequency	Cumulative Frequency	Percent	Cumulative Percent
Student	180	180	46.88%	46.88%
Employed (Public Sector)	58	238	15.10%	61.98%
Employed (Private Sector)	84	322	21.88%	83.86%
Self-employed	49	371	12.76%	96.62%
Unemployed	13	384	3.38%	100%

Figure 4.6: *Descriptive Analysis for Occupation*



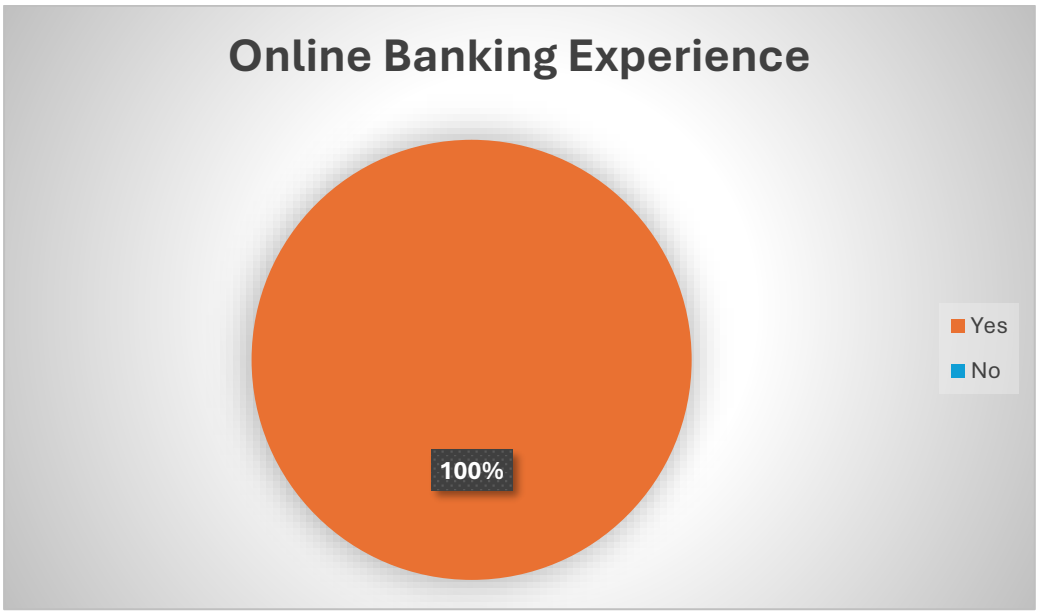
The respondents' occupation is presented in Table 4.6 and Figure 4.6. The various types of occupations included in this research are student, employee of the public sector, employee of the private sector, self-employed and unemployed. From the table and figure above, 180 of the respondents are students, which comprises 46.88% of the total respondents. The next occupation, private sector employed, includes 84 of the respondents. Compared with those employed in the private sector, the number of respondents that are employed in the public sector is lesser, which only includes 58 respondents (15.10%). Apart from that, the respondents who are self-employed include 49 respondents out of the 384 respondents, which is 12.76%. Besides, there is a small number of respondents who are unemployed, which is 13 respondents (3.38%).

4.1.1.7 Online Banking Experience

Table 4.7: *Descriptive Analysis of Online Banking Experience*

Occupation	Frequency	Cumulative Frequency	Percent	Cumulative Percent
Yes	384	384	100%	100%
No	0	384	0%	100%

Figure 4.7: *Descriptive Analysis of Online Banking Experience*



The 384 respondents' online banking experiences are shown in Table 4.7 and Figure 4.7. Online banking experience indicates that the respondents have used online banking services before. From the table and figure above, all the respondents, which is 384, have online banking experience. This means that all the respondents have used online banking services before. The respondents that do not have the online banking experience will not be included in this study since it is research that is related to online banking.

4.2 Inferential Analysis

4.2.1 Reliability Test

Table 4.8: *Reliability Test Result*

	Variables	Number of Items	Cronbach's Alpha	Reliability Test
Dependent Variable	User Confidence	5	0.821	Good
Independent Variable	System Reliability	5	0.754	Acceptable
Independent Variable	User Knowledge	5	0.765	Acceptable
Independent Variable	Perceived Data Protection	5	0.821	Good
Independent Variable	Technology Infrastructure	5	0.798	Acceptable

Table 4.8 above shows the result of the reliability test on the dependent variable and independent variables. From the table above, the Cronbach's Alpha value for the dependent variable in this research, user confidence, is 0.821. It is qualified as good in the reliability test. Apart from the user confidence, the independent variable, perceived data protection, also provided a high Cronbach's Alpha value of 0.821. Same as user confidence, it is also considered good in the reliability test. Besides, according to the table above, there are three independent variables that are considered acceptable in the reliability test. The three independent variables are system reliability, user knowledge, and technology infrastructure. The value of Cronbach's Alpha of system reliability is 0.754, the user knowledge's Cronbach's Alpha value is 0.765, and the technology infrastructure's Cronbach's Alpha value

is 0.798. The outcome of the technology infrastructure is very close to the good range in the reliability test. To conclude, all the variables show acceptable to good value in the reliability test.

4.2.2 Multicollinearity Test

Table 4.9: *Multicollinearity Test Result*

Independent Variable	Collinearity Statistics	
	Variance Inflation Factor (VIF)	Tolerance
IV 1: System Reliability	1.275	0.784
IV 2: User Knowledge	2.853	0.350
IV 3: Perceived Data Protection	2.574	0.388
IV 4: Technology Infrastructure	2.569	0.389

According to Table 4.9, the variance inflation factor (VIF) of every independent variable is greater than 1 but less than 5. The user knowledge has the biggest VIF value, while system reliability has the lowest value. Besides, the tolerance values of all independent variables exceeding 0.10 indicate low multicollinearity. System reliability has the largest tolerance value among the four independent variables, whereas user knowledge has the lowest tolerance value. As a result, it is less likely that a multicollinearity problem will occur among the independent variables in this study.

4.2.3 Pearson Correlation

Table 4.10: *Pearson Correlation Result*

	Pearson Correlation				
	DV: User Confidence	IV 1: System Reliability	IV 2: User Knowledge	IV 3: Perceived Data Protection	IV 4: Technology Infrastructure
DV: User Confidence	1	0.386**	0.519**	0.573**	0.481**
IV 1: System Reliability	0.386**	1	0.437**	0.422**	0.331**
IV 2: User Knowledge	0.519**	0.437**	1	0.732**	0.740**
IV 3: Perceived Data Protection	0.573**	0.422**	0.732**	1	0.711**
IV 4: Technology Infrastructure	0.481**	0.331**	0.740**	0.711**	1

** Correlation is significant at the 0.01 level (2-tailed).

Table 4.10 above shows the relationship between the dependent variable, user confidence, and the four explanatory variables. System reliability, user knowledge, perceived data protection, and technology infrastructure are the four explanatory variables involved.

Based on the result above, there is a strong and positive correlation between user confidence and perceived data protection. The correlation between these two variables is 0.573. Out of all the variables, this is the greatest correlation value. Besides, the correlation between user confidence and user knowledge also offers a strong and positive correlation, which is 0.519. Apart from that, the relationship between user confidence and technology infrastructure is a moderate and positive correlation. The correlation value provided by these two variables is 0.481. In addition, a weak and positive correlation exists between the variables of user confidence and system reliability. The correlation value provided by these two variables is 0.386. Although the variable of system reliability only indicates a weak correlation with the user confidence, it also significantly impacts the dependent variable.

As a conclusion, all the independent variables – system reliability, user knowledge, perceived data protection and technology infrastructure – have a positive and significant correlation with the dependent variable, user confidence, at the 0.01 level. From the result, we know that when the users feel that their data are protected and possess more knowledge about online banking, in addition to the online banking system being more reliable and having improved infrastructure, it will increase the user confidence towards online banking security and safety features.

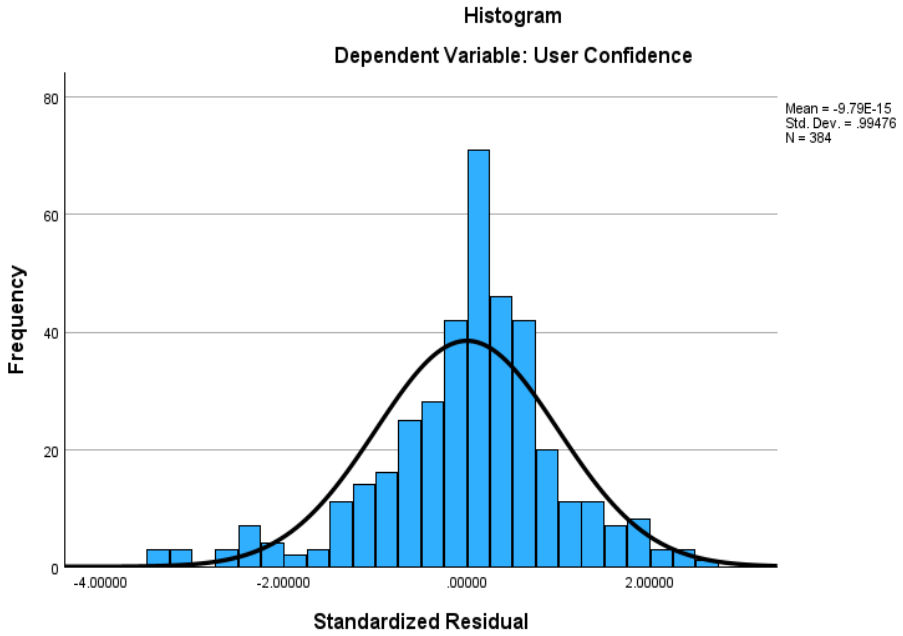
4.2.4 Normality Test

Table 4.11: *Normality Test Result*

Variables	Skewness	Kurtosis
DV: User Confidence	-0.722	-0.091
IV 1: System Reliability	-0.357	-0.114
IV 2: User Knowledge	-0.691	0.138
IV 3: Perceived Data Protection	-0.524	-0.445
IV 4: Technology Infrastructure	-0.581	-0.336

From Table 4.11, system reliability displays the largest skewness value, at -0.357, while user confidence has the smallest value, at -0.722. The variables' skewness values fall between -0.722 and -0.357. All values of skewness fall within a range of -2 to +2. Besides, user knowledge has the highest kurtosis value, at 0.138, while perceived data protection holds the smallest kurtosis value of -0.445. The kurtosis values range from -0.445 to 0.138. Every kurtosis value falls within the range of -7 to +7. All skewness and kurtosis values fall within the acceptable range. As a result, every variable has a normal data distribution.

Figure 4.8: *Histogram*



From Figure 4.8, the histogram illustrates the normality of the dependent variable of the study, which is user confidence. The histogram shows a bell-shaped and approximately symmetrical distribution. The middle or peak is the highest frequency. As it shifts to the left and right, the frequency decreases from its peak. Therefore, the data is normally distributed.

4.2.5 Multiple Linear Regression

Equation 4.1

$$UC_i = 1.146 + 0.137SR_i + 0.142UK_i + 0.347PDP_i + 0.083TI_i$$

Where:

UC_i = User confidence towards Online Banking Security and Safety Features

SR_i = System Reliability

UK_i = User Knowledge

PDP_i = Perceived Data Protection

TI_i = Technology Infrastructure

Table 4.12: *Multiple Linear Regression Result*

	Unstandardised Coefficients Beta	Coefficient Standard Error	Standardised Coefficients Beta	T-statistics	Sig.
(Constant)	1.146	0.196	-	5.842	<0.001
SR	0.137	0.041	0.152	3.301	<0.001
UK	0.142	0.073	0.134	1.949	0.052
PDP	0.347	0.064	0.353	5.389	<0.001
TI	0.083	0.067	0.081	1.234	0.218
R-squared	0.369				
Adjusted R-squared	0.363				
F-test	55.467				
P value (F test)	<0.001				
Durbin - Watson Test	1.736				

From Table 4.12, the connection between the explained variable, user confidence, and four explanatory variables, including system reliability, user knowledge, perceived data protection, and technology infrastructure, is investigated. In this study, the significance level is set at 0.05. The results show that only two variables, system reliability and perceived data protection, are significantly impacting the dependent variable, as their p-values are below 0.05. However, user knowledge and technology infrastructure are insignificant at p-values of 0.052 and 0.218, which are more than 0.05.

Firstly, given that the p-value is less than 0.001, user confidence is significantly affected by system reliability. The outcome is consistent with the studies by

Ayinaddis et al. (2023), which show that user confidence is significantly affected by system reliability. Besides, studies by Khan et al. (2023) and Tian et al. (2023) highlight the significance of technical performance on user confidence. Online banking systems with fewer technical issues and high security can effectively enhance user confidence. Hence, system reliability is an important predictor of user confidence. System reliability has a positive unstandardised coefficient of 0.137, indicating that when system reliability increases by 1 unit, user confidence increases by 0.137 units, ceteris paribus.

Besides, user knowledge is insignificant, and the p-value of user knowledge is 0.052. The result obtained is aligned with Haider et al. (2024) and Rodrigues et al. (2022). Haider et al. (2024) pointed out that limited and misunderstood knowledge of users could lead them to underestimate actual risks. In addition, Rodrigues et al. (2022) indicated that even though some users have enough or even advanced understanding of digital security, they still lack confidence in banks. This is because confidence not only depends on knowledge but also on the bank's reputation, openness, and past experience. Therefore, user knowledge is not sufficient to shape the user confidence towards online banking security and safety features.

Meanwhile, because its probability value is less than 0.001, which is smaller than 0.05, perceived data protection also proved a significant relationship with user confidence. The result aligns with the conclusion made by Suci and Dahlan (2023). Similarly, Gupta and Shukla (2024) note that when users question data protection mechanisms, their confidence in using such services significantly declines. Thus, perceived data protection plays a critical role in user confidence. The coefficient for perceived data protection is the highest among all independent variables, which is 0.347. This indicates that a unit increase in perceived data protection is associated with an increase of 0.347 units in user confidence, ceteris paribus.

Furthermore, technology infrastructure is insignificant since the p-value is 0.218, which is more than 0.05. This outcome is aligned with the research from Bojjagani et al. (2021) and Kimiagari and Baei (2021). According to the research by Bojjagani et al. (2021), users who had experienced fraud lack confidence in the system, even if it had improved and advanced security measures. Besides, Kimiagari and Baei (2021) indicated that the improved security measures, such as multi-step authentication, may irritate users instead of comforting them. This is because the multi-step authentication is complex and may interrupt the transaction. Therefore, the independent variable of technology infrastructure is not sufficient to shape the user confidence towards online banking security and safety features.

Apart from that, the R-squared value is 0.369 according to the table. This result indicates that 36.9% of the variance in user confidence towards online banking security and safety features is explained by the four independent variables, which are system reliability, user knowledge, perceived data protection, and technology infrastructure. Although 36.9% is not a very high percentage, it shows that these four independent variables play a substantial role in user confidence. Nonetheless, the remaining 63.1% of the variation is clarified by other independent variables that are not included in the model.

Additionally, the adjusted R-squared provides the value of 0.363. This proposes that 36.3% of the variance in user confidence towards online banking security and safety features is explained by the four independent variables, which are system reliability, user knowledge, perceived data protection, and technology infrastructure, following taking into account the degree of freedom.

Finally, the model's p-value of 0.001 is below the significant level of 0.05. This model is statistically significant. In addition, the F-value is 55.467. This comparatively high value shows that the variation explained by the model is much more than the variance that cannot be explained. To conclude, the four independent

variables - system reliability, user knowledge, perceived data protection, and technology infrastructure have a significant impact on the user confidence towards online banking security and safety features.

4.3 Conclusion

In this chapter, the data analysis was conducted using SPSS software. The demographic information is presented in table and chart format for easy analysis. The variables of user confidence and perceived data protection get good results in the Cronbach's Alpha test, while the results for the variables of system reliability, user knowledge, and technology infrastructure are acceptable. Then, the multicollinearity problem is less likely to occur among the independent variables in this study. From the Pearson correlation test, all four explanatory variables have a positive and significant correlation with the explained variable at the 0.01 level. Additionally, the distribution of data for all variables is normal. Furthermore, the multiple linear regression analysis illustrates that there are only two independent variables, system reliability and perceived data protection, possess a strong correlation with the dependent variable, whereas user knowledge and technology infrastructure are insignificant with the user confidence towards online banking security and safety features in Malaysia.

CHAPTER 5: DISCUSSION AND CONCLUSION

5.0 Introduction

This chapter explores more into the findings drawn from the last chapter, which is Chapter 4. Firstly, major findings are discussed. Then, some suggestions for the practice of professionals across various sectors are given. Last, it also outlines the study's limitations and offers recommendations for more research.

5.1 Discussion on Major Findings

5.1.1 System Reliability

The study discovered that user confidence in online banking security and safety features was significantly impacted by system reliability. This result aligned with Dangaiso et al. (2024) and Sasono et al. (2021), who reported that stronger system reliability boosts confidence in online banking security and safety features. According to Gazi, Masud, Sobhani, et al. (2024), strong security features that lower the perceived risk of online transactions, like encryption and multi-factor authentication, are crucial for boosting user confidence. Similarly, a study by Piotrowska (2024) discovered that the use of advanced security measures, like biometric authentication, significantly affected the perceptions of security and confidence among users. The study found that a bank builds a solid foundation of confidence with users by investing in and effectively communicating advanced

security measures, which increases the likelihood that users will use online banking. Arora and Banerji (2024) examined the impact of service quality, which encompasses dependability and security, on user confidence and loyalty in online banking. Users' confidence and loyalty are increased when users are comforted that financial information is secured by a reliable system that operates consistently without technical issues and offers high security. The idea that security is an essential part of service quality that upholds users' confidence rather than merely a feature was confirmed by this study.

5.1.2 Perceived Data Protection

The study indicated that perceived data protection had a significant influence on user confidence towards online banking security and safety features. This result is consistent with the findings of Cheryl and Ng (2022) as well as Suci and Dahlan (2023), who reported that users' perception of data protection fosters greater trust and significantly increases user confidence in online banking security. This relationship is reinforced by the fact that most online banking users often handle personal and financial information, making perceived security and privacy key determinants of trust and willingness to use the service (Murthy & Varalakshmi, 2021). As pointed out by Pandey and Tata Consultancy Services Limited (2024), user confidence is more likely to increase when banking systems demonstrate transparent data handling practices and implement advanced encryption as well as provide visible safety features to the users. This is because individuals are more inclined to believe that their personal data is safeguarded against data breaches, thereby reducing the perceived risks and even reinforcing their attention to engage with the online banking platforms. Moreover, Jafri et al. (2023) stated that the assurance of data protection not only strengthens trust but also encourages the user adoption of online banking, particularly in contexts where cybersecurity threats are perceived as prevalent. As a result, user confidence in the security of online banking

is heavily influenced by its perceived data protection, which further contributes to the overall acceptance and retention of online banking services.

5.2 Implications of Study

In this section, the focus is on how the research findings provide valuable insights for relevant parties. These stakeholders may include the banking industry, policymakers and academic researchers who are interested in enhancing user confidence towards the online banking security and safety features in Malaysia. Therefore, this study highlights how system reliability, user knowledge, perceived data protection and technology infrastructure influence users' confidence in the security and safety features of online banking platforms. The insights obtained from this research can be utilised by various parties to formulate the strategic improvements and practical applications.

From the banking industry perspective, the study offers significant guidance on shaping user confidence in online banking security through improvements in the identified variables. Among Malaysian users, system reliability and perceived data protection significantly influence user confidence in using online banking securely and safely. The banking industry may prioritise enhancing the digital performance of online banking services by introducing proactive monitoring and predictive maintenance systems driven by artificial intelligence to anticipate possible disruptions, thereby building confidence among online users. Other than that, this study may be a useful insight for the banking industry, as its results indicate an effect of perceived data protection on user confidence in online banking security. The banking institutions may focus on improving and clearly communicating their data security practices. This includes regularly updating security protocols and end-to-end encryptions, which fosters a sense of safety and trust in shaping user

confidence. The banks may even provide users with access to information on how their personal and financial data is stored, used and protected. By doing so, it will strengthen their perception of cybersecurity, ultimately reinforcing users' confidence in using the online banking platforms.

Furthermore, from the policymakers' perspectives, the conclusions of this research offer valued insights to support the formulation of more robust regulatory frameworks aimed at protecting the online banking users. The results show that perceived data protection has likewise been found to significantly influence user confidence towards online banking security. The policymakers may consider strengthening existing data protection regulations and enforcing stricter compliance standards with cybersecurity guidelines for financial institutions. For instance, reinforcement of policies mandating regular cybersecurity or rigorous penalties for data breaches can assure users of institutional accountability in online banking. As a result, the users are likely to develop more confidence in engaging with such services. This can promote the adoption of secure online banking habits and increase user retention among the population, especially in the face of rising cyber threats.

Overall, it is believed that these authorities will benefit from the findings of this study and use the insights to further explore effective strategies that enhance user confidence towards the security and safety features of online banking in Malaysia.

5.3 Limitation of Study

Following the completion of this study, a few limitations were found that hinder the research's ability to function more effectively and yield better findings.

The first key limitation of this study is reliance on predefined categories and variables, which may restrict the width and depth of information that can be discovered. The use of Likert scales (1–5, "strongly disagree" to "strongly agree") for demographic information, dependent variable and independent variables naturally limits responses to pre-established options. While this methodology provides a systematic and quantifiable approach, it might overlook subtle perspectives, new themes, or other factors that influence users' confidence in online banking security outside of the defined parameters. Malaysia's distinct cultural or socioeconomic contexts, for instance, might have a greater impact on user confidence than the general demographic categories (Gazi et al., 2024).

The second key limitation of this study is that it relied on self-reported statistics. Data for this study was collected via an online questionnaire. Respondents can easily use the online questionnaire, which is an inexpensive and time-efficient method of gathering data. It is vulnerable to survey fraud, though, and does require an internet connection. Because participants without internet access might complete the questionnaire later, researchers do not keep track of every respondent. Additionally, because of misunderstandings of the questions or a lack of oversight, respondents may submit incomplete or erroneous responses, which allows them to make decisions that do not truly represent their opinions. This is a common problem with self-reported data (Yeung & Quek, 2024).

5.4 Recommendation

Future studies could use a mixed-methods approach to get around the problem of depending too much on certain categories and variables. Using qualitative

approaches like structured interviews will allow for the exploration of new themes and generate more in-depth information about user confidence in online banking security than Likert scale responses. Participants would be able to elaborate on their experiences, introduce unexpected elements, and use this to convey complexity, which could lead to the discovery of fresh insights based on particular cultural or socioeconomic contexts. Additionally, open-ended survey questions could be used to gather qualitative data in addition to quantitative scales by enabling respondents to offer more detailed and no-limits comments, thereby expanding the scope and complexity of the information gathered.

Future research could use a range of approaches to overcome the limitations of self-reported statistics and online surveys. To start, including verification processes into the survey design, like attention-check questions or consistency checks, can help identify and minimise responses that are incorrect. Second, even though online surveys are practical, the quality of the data may be enhanced by employing additional or different techniques. For instance, even on a smaller scale, carrying out some of the surveys under supervision in person could prevent misunderstandings and guarantee more thorough results. Future research could examine outreach strategies that offer alternative methods for taking part, such as distributing paper questionnaires in neighbourhood centres or working with local organisations to facilitate access for under-represented demographics.

5.5 Conclusion

Finding the variables that influence user confidence towards online banking security and safety features in Malaysia is the aim of this study. A distributed online questionnaire was used to collect the data, and SPSS was used for analysis. The findings indicate that system reliability, user knowledge and perceived data

protection are significant variables, while technology infrastructure is the only insignificant independent variable. The decision shaping user confidence towards online banking security and safety features in Malaysia is influenced by relationships. The results of the study are fully discussed, along with their implications, limitations, and suggestions for additional research in the future.

References

Abbadi, N. D. (2024). Cyber threats in the age of artificial intelligence: Exploiting advanced technologies and strengthening cybersecurity. *International Journal of Science and Research Archive, 13*(1), 2576–2588. https://doi.org/10.30574/ijsra.2024.13.1.1961

Abdullah, I. N. (2025, February 13). *The full list of digital banks in Malaysia and their top benefits (2025)*. Fintech News Malaysia. https://fintechnews.my/48009/digital-banking-news-malaysia/list-of-digital-banks-in-malaysia-2025/

Abdullah, J., Yahaya, M. Z., Yunus, M. Z., & Safudin, M. S. M. A. (2009). URBAN SPRAWL IN MALAYSIA: EVIDENCES FROM THREE LARGEST METROPOLITAN AREAS. PLANNING MALAYSIA, 7. https://doi.org/10.21837/pm.v7i1.72

Adhikari, G. P. (2022). Interpreting the basic results of multiple linear regression. *Scholars Journal*, 22–37. https://doi.org/10.3126/scholars.v5i1.55775

Agu, N. E. E., Chiekezie, N. N. R., Abhulimen, N. a. O., & Obiki-Osafiele, N. a. N. (2024). Harnessing digital transformation to solve operational bottlenecks in banking. *World Journal of Advanced Science and Technology*, *6*(1), 046–056. https://doi.org/10.53346/wjast.2024.6.1.0046

Ahmed, S., Ahmed, R., Ashrafi, D. M., Ahmed, E., & Annamalah, S. (2024). Building trust in cybernetic payment network: Insights from an emerging economy. Journal of Open Innovation Technology Market and Complexity, 10(3), 100331. https://doi.org/10.1016/j.joitmc.2024.100331

Akter, M. S., Bhuiyan, M. R. I., Poli, T. A., & Hossain, R. (2023). Web-based banking services on E-customer satisfaction in private banking sectors: A cross-sectional study in developing economy. *Migration Letters, 20*(S3),

894-911. https://www.researchgate.net/publication/375742261_Web-based_Banking_Services_on_E-Customer_Satisfaction_in_Private_Banking_Sectors_A_Cross-Sectional_Study_in_Developing_Economy

Akhter, S., & Roy, J. K. (2017). Analysis of credit risk, efficiency, liquidity, and Profitability of selected Non-Bank Financial Institution: an Empirical study. *Journal of Business*, *2*(2), 16. https://doi.org/10.18533/job.v2i2.70

Alem, D. D. (2020). An overview of data analysis and interpretations in research. *International Journal of Academic Research in Education and Review, 8*(1), 1-27. https://www.researchgate.net/publication/365668845_An_Overview_of_Data_Analysis_and_Interpretations_in_Research

Ali, A. O. (2024). THE PAYMENTS SECURITY AND CONVENIENCE ON CONSUMER OF MOBILE PAYMENTS IN BAGUIO CITY, PHILIPPINES. European Journal of Management and Marketing Studies, 9(3). https://doi.org/10.46827/ejmms.v9i3.1872

Alnaser, F. M., Rahi, S., Alghizzawi, M., & Ngah, A. H. (2023). Does artificial intelligence (AI) boost digital banking user satisfaction? Integration of expectation confirmation model and antecedents of artificial intelligence enabled digital banking. Heliyon, 9(8), e18930. https://doi.org/10.1016/j.heliyon.2023.e18930

Arora, P., & Banerji, R. (2024). The impact of digital banking service quality on customer loyalty: An interplay between customer experience and customer satisfaction. *Asian Economic and Financial Review*, *14*(9), 712–733. https://doi.org/10.55493/5002.v14i9.5199

Bank Negara Malaysia. (n.d.) Payment Channel. https://www.bnm.gov.my/payment-statistics

Bellis, M. (2019, April 15). *History of Automatic teller Machines or ATM*. ThoughtCo. https://www.thoughtco.com/automatic-teller-machines-atm-1991236

Bhattacharya, C., & Sinha, M. (2022). The role of artificial intelligence in banking for leveraging customer experience. *Australasian Accounting Business and Finance Journal*, *16*(5), 89–105. https://doi.org/10.14453/aabfj.v16i5.07

Bojjagani, S., Sastry, V. N., Chen, C., Kumari, S., & Khan, M. K. (2021). Systematic survey of mobile payments, protocols, and security infrastructure. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 609–654. https://doi.org/10.1007/s12652-021-03316-4

Bueno, L. A., Sigahi, T. F., Rampasso, I. S., Filho, W. L., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights*, *4*(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230

Bujang, M. A., Omar, E. D., & Baharum, N. A. (2018). A review on sample size determination for Cronbach's Alpha Test: a simple guide for researchers. *Malaysian Journal of Medical Sciences*, *25*(6), 85–99. https://doi.org/10.21315/mjms2018.25.6.9

Chaimaa, B., Najib, E., & Rachid, H. (2020). E-banking Overview: Concepts, challenges and solutions. Wireless Personal Communications, 117(2), 1059–1078. https://doi.org/10.1007/s11277-020-07911-0

Chan, J. Y., Leow, S. M. H., Bea, K. T., Cheng, W. K., Phoong, S. W., Hong, Z., & Chen, Y. (2022). Mitigating the multicollinearity Problem and its

machine Learning Approach: A review. *Mathematics*, *10*(8), 1283. https://doi.org/10.3390/math10081283

Chauhan, V. (2024). Understanding users' protective behavior and its suppressor effect on the perceived risk in M-wallet/banking use: An Indian urban-rural comparison. Technological Forecasting and Social Change, 201, 123255. https://doi.org/10.1016/j.techfore.2024.123255

Che, M., Say, S. Y. A., Yu, H., Zhou, Q., Shu, J., Sun, W., Luo, X., & Xu, H. (2023). Investigating customers' continuous trust towards mobile banking apps. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-02483-3

Cheryl, B., & Ng, B. (2022). Protecting the unprotected consumer data in Internet of Things: Current scenario of data Governance in Malaysia. *Sustainability, 14*(16), 9893. https://doi.org/10.3390/su14169893

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2022). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Computers and Education Open*, *4*, 100119. https://doi.org/10.1016/j.caeo.2022.100119

Choudhuri, D. S., Singh, A., Ravi, R., & Badhusha, M. (2024). An analysis of factors influencing consumer trust in online banking security measures. *Educational Administration: Theory And Practice, 30*(2), 660-666. https://www.researchgate.net/publication/384291207_An_Analysis_of_Factors_Influencing_Consumer_Trust_in_Online_Banking_Security_Measures

Chuttur, M. (2009). *Overview of the Technology Acceptance Model: origins, developments and future directions*. AIS Electronic Library (AISeL). http://aisel.aisnet.org/sprouts_all/290

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/bf02310555

Dalati, S. (2018). Measurement and measurement scales. In *Progress in IS* (pp. 79–96). https://doi.org/10.1007/978-3-319-74173-4_5

Dangaiso, P., Mukucha, P., Makudza, F., Towo, T., Jonasi, K., & Jaravaza, D. C. (2024). Examining the interplay of internet banking service quality, e-satisfaction, e-word of mouth and e-retention: a post pandemic customer perspective. Cogent Social Sciences, 10(1). https://doi.org/10.1080/23311886.2023.2296590

Das, S., & Ganguly, D. (2024). Protecting your assets: Effective use of cybersecurity measures in banking industries. In Blockchain technologies (pp. 265–286). https://doi.org/10.1007/978-981-97-1249-6_12

Dogruel, L., Masur, P., & Joeckel, S. (2021). Development and validation of an algorithm literacy scale for internet users. *Communication Methods and Measures*, *16*(2), 115–133. https://doi.org/10.1080/19312458.2021.1968361

Dwivedi, P., Alabdooli, J. I., & Dwivedi, R. (2021). Role of FinTech adoption for Competitiveness and Performance of the Bank: A Study of Banking industry in UAE. *International Journal of Global Business and Competitiveness*, *16*(2), 130–138. https://doi.org/10.1007/s42943-021-00033-9

El-Hashash, E. F., & Shiekh, R. H. A. (2022). A comparison of the Pearson, Spearman rank and Kendall Tau correlation coefficients using quantitative variables. *Asian Journal of Probability and Statistics*, 36–48. https://doi.org/10.9734/ajpas/2022/v20i3425

Fintech News Malaysia. (2025, January 13). *Malaysia Fintech Report 2024: Will digital banks usher in a new era of banking?* https://fintechnews.my/46894/malaysia/fintech-malaysia-report-2024/

Gani, N. I. A., Rathakrishan, M., & Krishnasamy, H. N. (2020). A Pilot Test for Establishing Validity and Reliability of Qualitative Interview in the Blended Learning English Proficiency Course. *Journal of Critical Reviews. 7*(5), 140–143. http://dx.doi.org/10.31838/jcr.07.05.23

Gao, J. (2023). R-Squared (R2) – How much variation is explained? *Research Methods in Medicine & Health Sciences, 5*(4), 104–109. https://doi.org/10.1177/26320843231186398

Gazi, M. a. I., Masud, A. A., Amin, M. B., Hossain, M. A., Senathirajah, A. R. B. S., & Abdullah, M. (2024). Evaluating customer satisfaction with the quality of online banking services after COVID-19: developing country perspective. *Cogent Business & Management*, *11*(1). https://doi.org/10.1080/23311975.2024.2423057

Gazi, M. a. I., Masud, A. A., Sobhani, F. A., Islam, M. A., Rita, T., Chaity, N. S., Das, M., & Senathirajah, A. R. B. S. (2024). Exploring the mediating effect of customer satisfaction on the relationships between service quality, efficiency, and reliability and customer retention, loyalty in E-banking performance in emerging markets. *Cogent Business & Management*, *12*(1). https://doi.org/10.1080/23311975.2024.2433707

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea (Authorea)*. https://doi.org/10.22541/au.166385206.63311335/v1

Golzar, J., Noor, S. and Tajik, O. (2022). Convenience Sampling. International Journal of Education & Language Studies, 1(2), 72-77. https://doi.org/10.22034/ijels.2022.162981

Gong, H., Li, Y., Zhang, J., Zhang, B., & Wang, X. (2024). A new filter feature selection algorithm for classification task by ensembling pearson correlation coefficient and mutual information. Engineering Applications of Artificial Intelligence, 131, 107865. https://doi.org/10.1016/j.engappai.2024.107865

Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Gupta, V., & Shukla, S. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. *Interdisciplinary Studies in Society, Law, and Politics, 3*(2), 18-24. https://doi.org/10.61838/kman.isslp.3.2.4

Haider, A., Khan, M. A., Khoja, M., Alharthi, S., & Minhaj, S. M. (2024). The role of e-banking, mobile-banking, and e-wallet with response to e-payment and customer trust as a mediating factor using a structural equation modelling approach. *Journal of Infrastructure Policy and Development*, *8*(9), 6644. https://doi.org/10.24294/jipd.v8i9.6644

Harris, M., Cox, K. C., Musgrove, C. F., & Ernstberger, K. W. (2016). Consumer preferences for banking technologies by age groups. International Journal of Bank Marketing, 34(4), 587–602. https://doi.org/10.1108/ijbm-04-2015-0056

Hasan, N. M., Naseem, N. M. R., Salman, N. S. M., Iqbal, N. A., Aziz, N. D. A., & Javaid, N. M. Q. (2025). Evaluating the Impact of Financial Literacy and Cyber Security Perceptions on Customer Satisfaction with Online Banking Services in Pakistan. *Journal for Social Science Archives, 3*(1), 703–723. https://doi.org/10.59075/jssa.v3i1.153

Hatem, G., Zeidan, J., Goossens, M., & Moreira, C. (2022). NORMALITY TESTING METHODS AND THE IMPORTANCE OF SKEWNESS AND KURTOSIS IN STATISTICAL ANALYSIS. *BAU Journal - Science and Technology, 3*(2). https://doi.org/10.54729/ktpe9512

Hedayati, S., Damghanian, H., Farhadinejad, M., & Rastgar, A. A. (2023). Meta-analysis on application of Protection Motivation Theory in preventive behaviors against COVID-19. *International Journal of Disaster Risk Reduction*, *94*, 103758. https://doi.org/10.1016/j.ijdrr.2023.103758

Ikhwan, M. F., Mansor, W., Khan, Z. I., Mahmood, M. K. A., Bujang, A., & Haddadi, K. (2024). Pearson Correlation and Multiple correlation Analyses of the Animal Fat S-Parameter. *TEM Journal*, 155–160. https://doi.org/10.18421/tem131-15

Ismail, N. N. S., & Kasiran, M. K. (2023). Security of internet banking services in Malaysia: A survey of current practices. *International Journal of Computer Applications*, *185*(31), 25–29. https://doi.org/10.5120/ijca2023923071

Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2023). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon*, *10*(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Johanson, G. A., & Brooks, G. P. (2009). Initial Scale development: sample size for pilot studies. *Educational and Psychological Measurement*, *70*(3), 394–400. https://doi.org/10.1177/0013164409355692

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, *2023*, 1–10. https://doi.org/10.1155/2023/2103442

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert scale: explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975

Kandel, B. (2020). Qualitative versus quantitative research. Cdcsit. https://www.academia.edu/49300627/Qualitative_Versus_Quantitative_Research

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A. (2023). Online Banking User Authentication Methods: A Systematic Literature review. *IEEE Access, 12*, 741–757. https://doi.org/10.1109/access.2023.3346045

Khan, A. J., Hanif, N., Iqbal, J., Ahmed, T., Hameed, W. U., & Malik, A. A. (2023). Greening for greater good: investigating the critical factors for customer satisfaction with sustainable e-banking. *Environmental Science and Pollution Research*, *31*(34), 46255–46265. https://doi.org/10.1007/s11356-023-29090-8

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A Systematic analysis. *IEEE Access*, *11*, 80181–80198. https://doi.org/10.1109/access.2023.3298824

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Chen, Y., & Warren, M. (2024). The impact of perceived cyber-risks on automated vehicle acceptance: Insights from a survey of participants from the United States, the United Kingdom, New Zealand, and Australia. *Transport Policy*, *152*, 87–101. https://doi.org/10.1016/j.tranpol.2024.05.002

Khatun, N. (2021). Applications of normality test in statistical analysis. *Open Journal of Statistics, 11*(01), 113–122. https://doi.org/10.4236/ojs.2021.111006

Kimiagari, S., & Baei, F. (2021). Promoting e-banking actual usage: mix of technology acceptance model and technology-organisation-environment framework. *Enterprise Information Systems*, *16*(8–9). https://doi.org/10.1080/17517575.2021.1894356

Kotronoulas, G., Miguel, S., Dowling, M., Fernández-Ortega, P., Colomer-Lahiguera, S., Bağçivan, G., Pape, E., Drury, A., Semple, C., Dieperink, K. B., & Papadopoulou, C. (2023). An overview of the fundamentals of data management, analysis, and interpretation in quantitative research. *Seminars in Oncology Nursing*, *39*(2), 151398. https://doi.org/10.1016/j.soncn.2023.151398

Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users. *International Journal of Advanced Computer Science and Applications*, *12*(7). https://doi.org/10.14569/ijacsa.2021.0120792

Kuah, C. Y., Lee, X. W., Lim, H. N., & Lim, Y. Y. V. (2024). Awareness On Online Financial Scams: A Case Study in Malaysia. *International Journal of Advanced Research in Economics and Finance, 6*(1), 101-116. https://doi.org/10.55057/ijaref.2024.6.1.8

Kwak, S. (2023). Are only P-Values less than 0.05 significant? A P-Value greater than 0.05 is also significant! *Journal of Lipid and Atherosclerosis, 12*(2), 89. https://doi.org/10.12997/jla.2023.12.2.89

Kyriazos, T., & Poga, M. (2023). Dealing with Multicollinearity in Factor Analysis: The Problem, Detections, and Solutions. *Open Journal of Statistics*, *13*(03), 404–424. https://doi.org/10.4236/ojs.2023.133020

Lakens, D. (2022). Sample size justification. Collabra Psychology, 8(1). https://doi.org/10.1525/collabra.33267

Lee, J., De Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach. *Computers & Security*, *121*, 102832. https://doi.org/10.1016/j.cose.2022.102832

Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024). Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. *Computers in Human Behavior*, *159*, 108344. https://doi.org/10.1016/j.chb.2024.108344

Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2020). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*, *64*, 101487. https://doi.org/10.1016/j.techsoc.2020.101487

Lowe, N. K. (2019). What is a pilot study? *JOGN Nursing*, *48*(2), 117–118. https://doi.org/10.1016/j.jogn.2019.01.005

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malakar, I. M. (2023). Conceptualizing central tendency and dispersion in applied statistics. *Cognition*, *5*(1), 50–62. https://doi.org/10.3126/cognition.v5i1.55408

Martínez-Navalón, J., Fernández-Fernández, M., & Alberto, F. P. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? *International Entrepreneurship and Management Journal, 19*(2), 781–803. https://doi.org/10.1007/s11365-023-00839-4

Martín, J., Jiménez, A. M., Navas, M. J., Fernández-Recamales, M. Á., & Asuero, A. G. (2017). Multiple linear regression: an overview with analytical and physico-chemical applications. *Int J Adv Res Chem Sci, 4*, 32-60. https://www.arcjournals.org/pdfs/ijarcs/v4-i11/5.pdf

Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). Methods of data collection: A fundamental tool of research. Journal of Integrated Community Health, 10(1), 6-10. https://doi.org/10.24321/2319.9113.202101

McLeod, L. J., Hine, D. W., Please, P. M., & Driver, A. B. (2015). Applying behavioral theories to invasive animal management: Towards an integrated framework. *Journal of Environmental Management*, *161*, 63–71. https://doi.org/10.1016/j.jenvman.2015.06.048

Mcleod, S. (2023, December 13). *What is a questionnaire and how is it used in research?* Simply Psychology. https://www.simplypsychology.org/questionnaires.html

Mgiba, F. M., & Mxotwa, T. (2024). Communicating banking cyber-security measures, customer ethical concerns, experience, and loyalty intentions: a developing Economy's perspective. *International Review of Management and Marketing*, *14*(3), 123–135. https://doi.org/10.32479/irmm.16095

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations.

Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Mishra, P., Pandey, C. M., Singh, U., & Gupta, A. (2018). Scales of measurement and presentation of statistical data. *Annals of Cardiac Anaesthesia*, *21*(4), 419. https://doi.org/10.4103/aca.aca_131_18

Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. *Annals of Cardiac Anaesthesia, 22*(1), 67. https://doi.org/10.4103/aca.aca_157_18

Moksin, H., & Povakalam, M. (2024). Customer satisfaction in online banking services: A case study of a bank's clientele in Klang Valley, Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *14*(11). https://doi.org/10.6007/ijarbss/v14-i11/23043

Murthy, M. K., & Varalakshmi, S. (2021). Determinants of trust, security, privacy and risk factors in embracing online banking. In *Springer eBooks* (pp. 197–215). https://doi.org/10.1007/978-981-16-2652-4_10

Mwiya, B., Katai, M., Bwalya, J., Kayekesi, M., Kaonga, S., Kasanda, E., Munyonzwe, C., Kaulungombe, B., Sakala, E., Muyenga, A., & Mwenya, D. (2022). Examining the effects of electronic service quality on online banking customer satisfaction: Evidence from Zambia. *Cogent Business & Management*, *9*(1). https://doi.org/10.1080/23311975.2022.2143017

Mwita, K. (2022). Factors to consider when choosing data collection methods. International Journal of Research in Business and Social Science (2147-4478), 11(5), 532–538. https://doi.org/10.20525/ijrbs.v11i5.1842

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, 2150019. https://doi.org/10.1142/s2424786321500195

Nyutu, E., Cobern, W. W., & Pleasants, B. A. (2020). Correlational Study of Student Perceptions of their Undergraduate Laboratory Environment with respect to Gender and Major. *International Journal of Education in Mathematics Science and Technology*, *9*(1), 83–102. https://doi.org/10.46328/ijemst.1182

Ojo, A. O., Fawehinmi, O., Ojo, O. T., Arasanmi, C., & Tan, C. N. L. (2022). Consumer usage intention of electronic wallets during the COVID-19 pandemic in Malaysia. *Cogent Business & Management, 9*(1), 2056964. https://www.tandfonline.com/doi/full/10.1080/23311975.2022.2056964

Okagbue, H. I., Oguntunde, P. E., Obasi, E. C. M., & Akhmetshin, E. M. (2021). Trends and usage pattern of SPSS and Minitab Software in Scientific research. *Journal of Physics Conference Series*, *1734*(1), 012017. https://doi.org/10.1088/1742-6596/1734/1/012017

Ong, H., Jaffar, N., Yap, V., & Norhashim, M. (2023). Empirical analysis of internet and mobile banking in Malaysia. *Asian Economic and Financial Review*, *13*(2), 138–147. https://doi.org/10.55493/5002.v13i2.4717

Online Banking: what it is, how it works and best options | Payoneer. (2025, February 27). Payoneer. https://www.payoneer.com/resources/online-banking/

Ou, C. X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management, 65*, 102498. https://doi.org/10.1016/j.ijinfomgt.2022.102498

Oyewole, N. a. T., Okoye, N. C. C., Ofodile, N. O. C., & Ugochukwu, N. C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Ozili, P. K. (2022). The acceptable R-Square in empirical modelling for social science research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4128165

Pambudi, A., Widayanti, R., & Edastama, P. (2021). Trust and Acceptance of E-Banking Technology Effect of mediation on customer relationship management performance. ADI Journal on Recent Innovation (AJRI), 3(1), 87–96. https://www.academia.edu/62141031/Trust_and_Acceptance_of_E_Banking_Technology_Effect_of_Mediation_on_Customer_Relationship_Management_Performance

Pandey, S. & Tata Consultancy Services Limited. (2024). Improving data security in banking and financial services through API design and transaction management. *International Journal of Intelligent Systems and Applications in Engineering*, 775–782. https://www.researchgate.net/publication/388835248

Pea-Assounga, J. B. B., Yao, H., Bahizire, G. M., Bambi, P. D. R., & Ngapey, J. D. N. (2024). Effect of financial innovation and stakeholders' satisfaction on investment decisions: Does internet security matter? *Heliyon*, *10*(6), e27242. https://doi.org/10.1016/j.heliyon.2024.e27242

Phone Banking Services | Maybank Malaysia. (n.d.). https://www.maybank2u.com.my/maybank2u/malaysia/en/personal/services/phone_banking/phone_banking.page

Piotrowska, N. a. I. (2024). Determinants of consumer adoption of biometric technologies in mobile financial applications. *Economics and Business Review/□the □Poznań University of Economics Review*, *10*(1). https://doi.org/10.18559/ebr.2024.1.1019

Pradhan, D. (2024, July 31). What is mobile banking and how does it work? *Forbes Advisor INDIA*. https://www.forbes.com/advisor/in/banking/what-is-mobile-banking/

Rahi, S., Khan, M. M., & Alghizzawi, M. (2020). Extension of technology continuance theory (TCT) with task technology fit (TTF) in the context of Internet banking user continuance intention. *International Journal of Quality & Reliability Management*, *38*(4), 986–1004. https://doi.org/10.1108/ijqrm-03-2020-0074

Rahi, S., Mansour, M. M. O., Alharafsheh, M., & Alghizzawi, M. (2021). The post-adoption behavior of internet banking users through the eyes of self-determination theory and expectation confirmation model. *Journal of Enterprise Information Management*, *34*(6), 1874–1892. https://doi.org/10.1108/jeim-04-2020-0156

Rahman, A., & Muktadir, M. (2021). SPSS: an imperative quantitative data analysis tool for social science research. *International Journal of Research and Innovation in Social Science*, *05*(10), 300–302. https://doi.org/10.47772/ijriss.2021.51012

Rahman, H. A., & Hassan, R. (2022). Factors influencing cashless transactions behaviour in Malaysia higher education institution. *International Journal of Academic Research in Business and Social Sciences*, *12*(10). https://doi.org/10.6007/ijarbss/v12-i10/15451

Ranjan, R. (2025). Behavioural Finance in Banking and Management: A Study on the Trends and Challenges in the Banking Industry. *Asian Journal of*

Economics, Business and Accounting, *25*(1), 374–386. https://doi.org/10.9734/ajeba/2025/v25i11657

Roberte, L. (2025, February 28). *What is online banking? definition and how it works*. Investopedia. https://www.investopedia.com/terms/o/onlinebanking.asp

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 101616. https://doi.org/10.1016/j.ribaf.2022.101616

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosala, M. (2024, February 5). *Open-Ended vs. Closed Questions in User Research*. Nielsen Norman Group. https://www.nngroup.com/articles/open-ended-questions/

Saidi, S. S., & Siew, N. M. (2019). Investigating the Validity and Reliability of Survey Attitude towards Statistics Instrument among Rural Secondary School Students. *International Journal of Educational Methodology*, 5(4), 651–661. https://doi.org/10.12973/ijem.5.4.651

Saif, M. A., Hussin, N., Husin, M. M., Alwadain, A., & Chakraborty, A. (2022). Determinants of the intention to adopt digital-only banks in Malaysia: The extension of environmental concern. Sustainability, 14(17), 11043. https://www.mdpi.com/2071-1050/14/17/11043

Sasono, I., Jubaedi, A. D., Novitasari, D., Wiyono, N., Riyanto, R., Oktabrianto, O., Jainuri, J., & Waruwu, H. (2021). The Impact of E-Service Quality and Satisfaction on Customer Loyalty: Empirical Evidence from Internet Banking Users in Indonesia. *Journal of Asian Finance Economics and Business*, *8*(4), 465–473. https://doi.org/10.13106/jafeb.2021.vol8.no4.0465

Selvanathan, M., Krisnan, U. D., & Jun, G. K. (2017). Acceptance of Internet Banking among Consumers in Kota Damansara, Selangor, Malaysia. International Journal of Business and Management, 12(2), 103. https://doi.org/10.5539/ijbm.v12n2p103

Senaviratna, N. a. M. R., & Cooray, T. M. J. A. (2019). Diagnosing multicollinearity of logistic regression model. *Asian Journal of Probability and Statistics*, 1–9. https://doi.org/10.9734/ajpas/2019/v5i230132

Shahrizal. (2024, October 4). *Malaysia loses RM54.02 billion to scams, report reveals alarming rise - BusinessToday*. BusinessToday. https://www.businesstoday.com.my/2024/10/04/malaysia-loses-rm54-02-billion-to-scams-report-reveals-alarming-rise/

Shamsabadi, E. A., Salehpour, M., Zandifaez, P., & Dias-Da-Costa, D. (2023). Data-driven multicollinearity-aware multi-objective optimisation of green concrete mixes. *Journal of Cleaner Production*, *390*, 136103. https://doi.org/10.1016/j.jclepro.2023.136103o

Shkak, J., Gasha Technical Institute, Hassan, H. G., & British International University. (2020). Characteristics of normal distribution. *Preprint*. https://doi.org/10.13140/RG.2.2.19914.59846

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. *American journal of applied mathematics and statistics, 8*(2), 39-42.

https://www.researchgate.net/publication/342413955_Detecting_Multicollinearity_in_Regression_Analysis

Siagian, H., Tarigan, Z. J. H., Basana, S. R., & Basuki, R. (2022). The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform. *International Journal of Data and Network Science, 6*(3), 861–874. https://doi.org/10.5267/j.ijdns.2022.2.010

Siswaningsih, W., Firman, H., Zackiyah, N., & Khoirunnisa, A. (2017). Development ofTwo-TierDiagnostic Test Pictorial-Based for identifying high school students misconceptions on the mole concept. *Journal of Physics Conference Series*, *812*, 012117. https://doi.org/10.1088/1742-6596/812/1/012117

Skiera, B., Reiner, J., & Albers, S. (2021). Regression analysis. In *Springer eBooks* (pp. 299–327). https://doi.org/10.1007/978-3-319-57413-4_17

Stratton, S. J. (2021). Population Research: Convenience sampling strategies. Prehospital and Disaster Medicine, 36(4), 373–374. https://doi.org/10.1017/s1049023x21000649

Subri, N. I., Hanafi, A. G., & Pozin, M. A. A. (2024). Comparative Analysis of eKYC and 2FA in Implementing PADU Database System to Strengthen Digital Identity Security. *Journal of Cyber Security Volume*, *5*, 23-34. https://www.researchgate.net/profile/Mohd-Affendi-Ahmad-Pozin/publication/382692843_Comparative_Analysis_of_eKYC_and_2FA_in_Implementing_PADU_Database_System_to_Strengthen_Digital_Identity_Security/links/66a9b559de060e4c7e69ff55/Comparative-Analysis-of-eKYC-and-2FA-in-Implementing-PADU-Database-System-to-Strengthen-Digital-Identity-Security.pdf

Suci, F. C. W., & Dahlan, K. S. S. (2023). The effect of security and trust on mobile banking customer satisfaction mediated by convenience factors. *Journal of Social Science (JoSS),* *2*(10), 888–902. https://doi.org/10.57185/joss.v2i10.144

Sulaiman, M. S., Abood, M. M., Sinnakaudan, S. K., Shukor, M. R., You, G. Q., & Chung, X. Z. (2019). Assessing and solving multicollinearity in sediment transport prediction models using principal component analysis. *ISH Journal of Hydraulic Engineering*, *27*(sup1), 343–353. https://doi.org/10.1080/09715010.2019.1653799

Sureiman, O., & Mangera, C. (2020). F-test of overall significance in regression analysis simplified. *Journal of the Practice of Cardiovascular Sciences, 6*(2), 116. https://doi.org/10.4103/jpcs.jpcs_18_20

Sürücü, L., & Maslakci, A. (2020). VALIDITY AND RELIABILITY IN QUANTITATIVE RESEARCH. *Business and Management Studies an International Journal,* *8*(3), 2694–2726. https://doi.org/10.15295/bmij.v8i3.1540

Syafril, S. (2025). The Nexus between Sharia Principles and Banking: Why Islamic Values Matter in Islamic Banking? *Bukhori Kajian Ekonomi Dan Keuangan Islam*, *4*(2), 95–107. https://doi.org/10.35912/bukhori.v4i2.3486

Syed Mizuri, S. Z., & Mat Lazim, A. (2024). Consumer intention to adopt online banking in Malaysia: A literature review. Jurnal Kejuruteraan, Teknologi dan Sains Sosial, 8(1), 159–171. https://jktss.puo.edu.my/jurnalpuo/index.php/jurnal/article/view/51/42

Šverko, Z., Vrankić, M., Vlahinić, S., & Rogelj, P. (2022). Complex Pearson Correlation Coefficient for EEG connectivity analysis. *Sensors*, *22*(4), 1477. https://doi.org/10.3390/s22041477

Taherdoost, H. (2016). Sampling methods in research methodology; How to choose a sampling technique for research. https://hal.science/hal-02546796v1

Taherdoost, H. (2021, September 22). Data collection Methods and Tools for Research; A Step-by-Step Guide to choose data collection technique for academic and business research projects. https://hal.science/hal-03741847v1

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Tian, Y., Chan, T. J., Suki, N. M., & Kasim, M. A. (2023). Moderating Role of Perceived Trust and Perceived Service Quality on Consumers' Use Behavior of Alipay e-wallet System: The Perspectives of Technology Acceptance Model and Theory of Planned Behavior. *Human Behavior and Emerging Technologies*, *2023*, 1–14. https://doi.org/10.1155/2023/5276406

Toback, M. (2024, October 29). *Unveil the secrets: advanced persistent threat and social engineering explained*. Endpoint Security. https://smallbizepp.com/apt-and-social-engineering/

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*. https://doi.org/10.1108/ijbm-03-2024-0138

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2021). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today Proceedings*, *51*, 2172–2175. https://doi.org/10.1016/j.matpr.2021.11.121

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*, 104051. https://doi.org/10.1016/j.cose.2024.104051

Willie, M. M. (2024). Population and target population in research methodology. Golden Ratio of Social Science and Education, 4(1), 75–79. https://doi.org/10.52970/grsse.v4i1.405

Yeung, E. S., & Quek, K. (2024). Self-reported political ideology. *Political Science Research and Methods*, 1–22. https://doi.org/10.1017/psrm.2024.2

Yong, H. Z., & Kasiran, M. K. B. (2023). Ensuring Trust and Confidence: Safeguarding Online Banking Transactions with Multi-layered Security in Malaysia. https://ijaem.net/issue_dcp/Ensuring%20Trust%20and%20Confidence%20Safeguarding%20Online%20Banking%20Transactions%20with%20Multi%20layered%20Security%20in%20Malaysia.pdf

Zahra, D. R., & Anoraga, P. (2021). The influence of lifestyle, financial literacy, and social demographics on consumptive behavior. *Journal of Asian Finance Economics and Business*, *8*(2), 1033–1041. https://doi.org/10.13106/jafeb.2021.vol8.no2.1033

Zakariya, Y. F. (2022). Cronbach's alpha in mathematics education research: Its appropriateness, overuse, and alternatives in estimating scale reliability. *Frontiers in Psychology, 13*. https://doi.org/10.3389/fpsyg.2022.1074430

Zhang, M., Li, W., Zhang, L., Jin, H., Mu, Y., & Wang, L. (2023). A Pearson correlation-based adaptive variable grouping method for large-scale multi-objective optimization. *Information Sciences*, *639*, 118737. https://doi.org/10.1016/j.ins.2023.02.055

Appendices

Appendix 3.1: "Table for Determining Sample Size for a Finite Population"

Table 1: Krejcie and Morgan Table

N	*S*	*N*	*S*	*N*	*S*
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	1000000	384

Note.—*N* is population size. *S* is sample size.

Source: Krejcie & Morgan, 1970

Appendix 3.2: Pilot test results

User confidence

Reliability Statistics

Cronbach's Alpha	N of Items
.831	5

System reliability

Reliability Statistics

Cronbach's Alpha	N of Items
.810	5

User knowledge

Reliability Statistics

Cronbach's Alpha	N of Items
.811	5

Perceived data protection

Reliability Statistics

Cronbach's Alpha	N of Items
.893	5

Technology infrastructure

Reliability Statistics

Cronbach's Alpha	N of Items
.782	5

Appendix 4.1: Reliability Test

User Confidence

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.821	.821	5

System Reliability

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.745	.754	5

User Knowledge

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.765	.764	5

Perceived Data Protection

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.821	.822	5

Technology Infrastructure

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.798	.798	5

Appendix 4.2: Multicollinearity Test

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.146	.196		5.842	<.001		
	SR	.137	.041	.152	3.301	.001	.784	1.275
	UK	.142	.073	.134	1.949	.052	.350	2.853
	PDP	.347	.064	.353	5.389	<.001	.388	2.574
	TI	.083	.067	.081	1.234	.218	.389	2.569

a. Dependent Variable: UC

Appendix 4.3: Pearson Correlation

Correlations

		UC	SR	UK	PDP	TI
UC	Pearson Correlation	1	.386**	.519**	.573**	.481**
	Sig. (2-tailed)		<.001	<.001	<.001	<.001
	N	384	384	384	384	384
SR	Pearson Correlation	.386**	1	.437**	.422**	.331**
	Sig. (2-tailed)	<.001		<.001	<.001	<.001
	N	384	384	384	384	384
UK	Pearson Correlation	.519**	.437**	1	.732**	.740**
	Sig. (2-tailed)	<.001	<.001		<.001	<.001
	N	384	384	384	384	384
PDP	Pearson Correlation	.573**	.422**	.732**	1	.711**
	Sig. (2-tailed)	<.001	<.001	<.001		<.001
	N	384	384	384	384	384
TI	Pearson Correlation	.481**	.331**	.740**	.711**	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	
	N	384	384	384	384	384

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 4.4: Normality Test

Descriptive Statistics

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
UC	384	3.9036	.73010	-.722	.125	-.091	.248
SR	384	3.5974	.81288	-.357	.125	-.114	.248
UK	384	4.0021	.69267	-.691	.125	.138	.248
PDP	384	3.9307	.74167	-.524	.125	-.445	.248
TI	384	4.0307	.70891	-.581	.125	-.336	.248
Valid N (listwise)	384						

Appendix 4.5: Multiple Linear Regression

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	1.146	.196		5.842	<.001		
	SR	.137	.041	.152	3.301	.001	.784	1.275
	UK	.142	.073	.134	1.949	.052	.350	2.853
	PDP	.347	.064	.353	5.389	<.001	.388	2.574
	TI	.083	.067	.081	1.234	.218	.389	2.569

a. Dependent Variable: UC

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.608[a]	.369	.363	.58290	1.736

a. Predictors: (Constant), TI, SR, PDP, UK

b. Dependent Variable: UC

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	75.383	4	18.846	55.467	<.001[b]
	Residual	128.772	379	.340		
	Total	204.155	383			

a. Dependent Variable: UC

b. Predictors: (Constant), TI, SR, PDP, UK