

AWARENESS ON ONLINE FINANCIAL SCAM: A
STUDY IN MALAYSIA

LEE WEN XIAN
LIM NYA HIA
VIVIAN LIM YAN YI

BACHELOR OF FINANCE (HONS)

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE
DEPARTMENT OF FINANCE

SEPTEMBER 2023

LEE, LIM, & LIM

ONLINE FINANCIAL SCAM

BFN (HONS)

SEPTEMBER 2023

AWARENESS ON ONLINE FINANCIAL SCAM: A
STUDY IN MALAYSIA

BY

LEE WEN XIAN
LIM NYA HIA
VIVIAN LIM YAN YI

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

BACHELOR OF FINANCE (HONS)

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY BUSINESS AND FINANCE
DEPARTMENT OF FINANCE

SEPTEMBER 2023

Copyright @ 2023

ALL RIGHTS RESERVED. No part of this paper may be reproduced, stored in a retrieval system, or transmitted in any form by any means, graphic, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior consent of the authors.

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 or any university, or other institutes 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 16,242 words.

Name of Student:

Student ID:

Signature:


1. Lee Wen Xian

19ABB04593



2. Lim Nya Hia

20ABB05875



3. Vivian Lim Yan Yi

19ABB05417



Date: 5 September 2023

ACKNOWLEDGEMENT

We would like to express our sincere appreciation and gratitude to those who supported and assisted us in completing this entire research project.

Firstly, we would like to express our deepest gratitude to our research project supervisor, Dr. Kuah Yoke Chin for her guidance and valuable opinions throughout the entire research project. We are really grateful for her precious time and patience in guiding us. Her expertise and feedback have been a constant source of inspiration, motivating us to enhance our research project.

Secondly, we would like to extend our gratitude our second examiner, Mr. Adam Lee Aik Keang who have also provided his valuable opinions to us during the presentation, assisting us in improving our work.

Moreover, we would like to thank to all respondents who spent their valuable time for participating in our survey questionnaires. We would not be able to complete our research without their contribution. Besides, we acknowledge and credit to our families and friends for their unwavering support and encouragement throughout the entire research journey.

Last but not least, we would like to express our heartless appreciation to each of our team members for their co-operation in completing this research. Their contribution, effort, and time have played an important role in shaping the outcome of the research.

DEDICATION

This research is dedicated to Universiti Tunku Abdul Rahman (UTAR), which allowed us to utilize and apply the knowledge we learned while pursuing a three-year finance degree.

Additionally, we would like to dedicate the work to Dr. Kuah Yoke Chin, our research project supervisor for the last year, for her persistent support and direction. Without her full-hearted support, it would have been difficult for us to finish this task on time. We sincerely appreciate her contributions throughout this Final Year Project.

In addition, we would like to dedicate our work to Mr. Adam Lee Aik Keang, who is the second examiner to review our Final Year Project. He gave us insightful advice, and we are grateful and happy to have him as our examiner because he greatly improved our research project.

Finally, we'd like to dedicate this essay to our family and friends, who have been supportive of us. We truly appreciate the incredible technical assistance and mental support they provided.

TABLE OF CONTENTS

		Page
COPYRIGHT PAGE		ii
DECLARATION		iii
ACKNOWLEDGEMENT		iv
DEDICATION		v
TABLE OF CONTENTS.....		vi
LIST OF TABLES		x
LIST OF FIGURES		xi
LIST OF ABBREVIATIONS.....		xii
LIST OF APPENDICES.....		xiii
PREFACE.....		xiv
ABSTRACT.....		xv
CHAPTER 1	RESEARCH OVERVIEW.....	1
1.0	Introduction.....	1
1.1	Research Background	1
	1.1.1 Evolution of Money	1
	1.1.2 Adoption of Electronic Payment.....	3
	1.1.3 Online Financial Scam.....	5
1.2	Research Problem	7
1.3	Research Questions	10
1.4	Research Objectives.....	10
1.5	Research Significance.....	11
1.6	Conclusion	12
CHAPTER 2	LITERATURE REVIEW	14
2.0	Introduction.....	14
2.1	Underlying Theories	14

	2.1.1 Technology Threat Avoidance Theory (TTAT)	14
	2.1.2 Theory of Planned Behaviour (TPB)	16
2.2	Review of Variables	18
	2.2.1 Awareness on Online Financial Scam	18
	2.2.2 Cybersecurity Knowledge	20
	2.2.3 Perceived Severity	22
	2.2.4 Subjective Norms	23
	2.2.5 Security and Privacy Concern	24
2.3	Theoretical Framework	26
2.4	Conclusion	27
CHAPTER 3	METHODOLOGY	28
3.0	Introduction	28
3.1	Research Design	28
	3.1.1 Descriptive Research	28
3.2	Data Collection Method	29
	3.2.1 Primary Data	29
3.3	Sampling Design	30
	3.3.1 Target Population	30
	3.3.2 Sampling Frame and Sampling Location	30
	3.3.3 Technique of Sampling	31
	3.3.4 Sampling Size	31
3.4	Research Instrument	32
	3.4.1 Questionnaire Design	32
	3.4.2 Pilot Test	33
3.5	Construct Measurement	33
	3.5.1 Nominal Scale	34
	3.5.2 Ordinal Scale	34

	3.5.3 Interval Scale	35
3.6	Data Processing.....	35
	3.6.1 Data Checking	36
	3.6.2 Data Editing	36
	3.6.3 Data Coding	36
	3.6.4 Data Transcription	37
3.7	Data Analysis	37
	3.7.1 Descriptive Analysis	37
	3.7.2 Partial Least Square Equation Modelling	38
	3.7.3 Internal Consistency Reliability	38
	3.7.3.1 Composite Reliability (CR)	39
	3.7.3.2 Cronbach's Alpha (CA)	40
	3.7.4 Construct Validity.....	40
	3.7.4.1 Discriminant Validity.....	41
	3.7.5 Evaluation of Inner Model	41
3.8	Conclusion	42
CHAPTER 4	DATA ANALYSIS	43
4.0	Introduction.....	43
4.1	Participation Rate.....	43
4.2	Descriptive Analysis	43
	4.2.1 Respondents' Demographic Profile	43
	4.2.1.1 Gender.....	44
	4.2.1.2 Age.....	44
	4.2.1.3 Ethnicity.....	45
	4.2.1.4 Education Level	46
	4.2.1.5 Monthly Income.....	47
	4.2.1.6 Types of E-wallet Account	48

	4.2.1.7 Types of Online Banking Account	49
4.3	Measurement and Structural Model.....	51
	4.3.1 Factor Loadings	51
	4.3.2 Internal Consistency Reliability.....	52
	4.3.2.1 Results for Cronbach’s Alpha, Composite Reliability, Average Variance Extracted	53
	4.3.3 Discriminant Validity.....	54
	4.3.3.1 Fornell-Lacker Criterion	54
	4.3.3.2 Heterotrait-Monotrait (HTMT) ratio.....	55
	4.3.4 Path Coefficient (Bootstrapping)	56
4.4	Conclusion	59
CHAPTER 5	DISCUSSION, CONCLUSION AND IMPLICATIONS	
	60
5.0	Introduction.....	60
5.1	Discussions of Major Findings	60
	5.1.1 Cybersecurity Knowledge	62
	5.1.2 Perceived Severity	63
	5.1.3 Subjective Norms.....	63
	5.1.4 Security and Privacy Concern.....	64
5.2	Implications of the Research.....	65
5.3	Limitations of the Research	67
5.4	Recommendations for Future Researchers	68
5.5	Conclusion	69
REFERENCES	71
APPENDICES	90

LIST OF TABLES

	Page
Table 1.1: Willingness to use E-wallet without incentives.....	5
Table 1.2: Summarized Online Scam Cases and Losses	6
Table 3.1: Rule of Thumb for Cronbach’s Alpha	39
Table 4.1: Gender.....	44
Table 4.2: Age.....	45
Table 4.3: Ethnicity.....	45
Table 4.4: Education Level	46
Table 4.5: Monthly Income.....	47
Table 4.6: Types of E-wallet Account	48
Table 4.7: Types of Online Banking Account	50
Table 4.8: Factor Loadings	51
Table 4.9: Cronbach’s Alpha, Composite Reliability, Average Variance Extracted (AVE)	53
Table 4.10: Fornell-Lacker Criterion.....	54
Table 4.11: Heterotrait Monotrait Ratio (HTMT)	55
Table 4.12: Path Coefficient	57
Table 5.1: Summary of Statistical Analysis.....	60

LIST OF FIGURES

	Page
Figure 1.1: History of Money	1
Figure 1.2: Basic Payment Indicator.....	4
Figure 2.1: Technology Threat Avoidance Theory (TTAT).....	16
Figure 2.2: Theory of Planned Behaviour (TPB).....	18
Figure 2.3: Conceptual Model	27
Figure 4.1: Gender	44
Figure 4.2: Age	45
Figure 4.3: Ethnicity	46
Figure 4.4: Education Level.....	47
Figure 4.5: Monthly Income	48
Figure 4.6: Types of E-wallet Account	49
Figure 4.7: Types of Online Banking Account.....	50
Figure 4.8: Structural Model (Bootstrapping)	56

LIST OF ABBREVIATIONS

AVE	Average Variance Extracted
BNM	Bank Negara Malaysia
BSN	Bank Simpanan Negara
CA	Cronbach's Alpha
CB-SEM	Covariance-Based Structural Equation Modelling
CCID	Commercial Crime Investigation Department
CFA	Confirmatory Factor Analysis
CIMB	Commercial International Merchant Bankers Berhad
CK	Cybersecurity Knowledge
CR	Composite Reliability
DV	Awareness on Online Financial Scam
GDP	Gross Domestic Product
HSBC	Hong Kong and Shanghai Banking Corporation Limited
HTMT	Heterotrait-Monotrait Ratio
MAE	Maybank Anytime Everyone
MDEC	Malaysia Digital Economy Corporation
NSRC	National Scam Report Center
OCBC	Oversea-Chinese Banking Corporation
PLS	Partial Least Square
PLS-SEM	Partial Least Square Structural Equation Modelling
PS	Perceived Severity
SN	Subjective Norms
SP	Security and Privacy Concern
TNG	Touch' n Go
TPB	Theory Planned Behaviour
TTAT	Technology Threat Avoidance Theory

LIST OF APPENDICES

	Page
Appendix 3.1: Sample Size of a Known Population.....	90
Appendix 3.2: Survey Questionnaire Permission Letter.....	92
Appendix 3.3: Survey Questionnaire Sample	93

PREFACE

Malaysia has seen an increase in digitization in almost all aspects of its people's daily lives, especially in the usage of online banking or e-wallet transactions. However, a rise in online financial scams in Malaysia has been reported recently. People have become unaware of the transparency of their information as a result of their reliance on the Internet.

This research project aims to investigate the variables that influence the awareness of online financial scams in Malaysia. The research is based on primary data collected through a survey of 384 respondents across Malaysia. The survey instrument was designed to measure several factors that could affect Malaysians' awareness of online financial scams, including cybersecurity knowledge, perceived severity, security and privacy concerns, and subjective norms.

In conclusion, this research project will provide valuable insights into the determinants of the awareness of online financial scams among Malaysians. The research's findings can assist policymakers and industry players in designing and implementing more effective ways to detect and prevent financial scams. By understanding the determinants that affect awareness of online financial scams, Malaysia can continue to progress effectively in the global financial markets.

ABSTRACT

This research aims to identify the awareness on online financial scam in Malaysia by using Technology Threat Avoidance Theory (TTAT) and Theory of Planned Behaviour (TPB). Independent variables included are cybersecurity knowledge, perceived severity, subjective norm, as well as security and privacy concern. The data collection method in this research is primary data and 384 sets survey questionnaires were collected. Partial Least Square Structural Equation Modelling (PLS-SEM) software was used to generate statistical analysis. The results showed that cybersecurity knowledge, perceived severity, and subjective norm have significant relationship with the awareness on online financial scam; while security and privacy concern has insignificant relationship with the awareness on online financial scam. This research will provide an insight for Malaysian, companies, and policymaker to better understand the ways to increase awareness on online financial scam. Limitations and recommendations are provided in this research for future researchers to have a better understanding in conducting future research.

CHAPTER 1: RESEARCH OVERVIEW

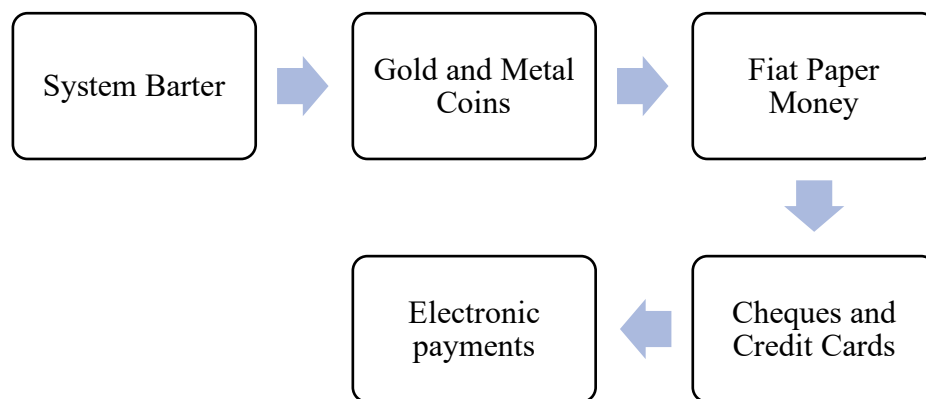
1.0 Introduction

This research focuses on analyzing Malaysians' awareness of online financial scam. Chapter one mainly provides a comprehensive understanding of the topic that is being explored, with the recent statistics and trends of online financial scam, together with problem statements, research questions, research objectives, and importance of the research.

1.1 Research Background

1.1.1 Evolution of Money

Figure 1.1
History of Money



Source: For the research purpose

The payment method has changed dramatically over the years from the barter system to the usage of paper cash and coins, and then to the cheques and credit cards (Yap et al., 2019). The barter system is the earliest form of

trade. It is a system of exchanging goods and services for other goods and services. The exchange of goods and services in a barter system occurs directly between parties, without involving a central intermediary or the use of money. Participants trade their surplus items for items they require or desire. This system was widely used in ancient societies prior to the development of monetary systems. However, the limitation of the barter system is that it lacks a standard estimate of value, which makes it difficult to conduct targeted exchanges and transactions (“History of money: From fiat to crypto, explained”, 2023).

Therefore, money emerged as a technology that could facilitate economic activity, transactions, and specialization. Money is a means of payment, a unit of account, and a store of value. Throughout history and as civilizations progressed, various objects have served as money, such as whale teeth, grains of rice, seashells, livestock, metal coins and paper money (Farras & Salmeron, 2018). The eventual appearance of metal coins and paper money helped establish a common currency. According to Villanueva (2019), gold coins were introduced in 600 BC, but the gold coins or gold bars were too heavy to carry, which is why fiat paper money has emerged as a form of payment. China has first invented fiat paper money and used it for 500 years and influenced the whole world (Arvidsson, 2019). It was not until the 17th century that Europeans modified paper money and began to use it widely in other countries, resulting in paper money becoming the most common form of payment for small purchases today because it is easier to carry a lot of paper money than heavy metal coins anyway.

As time passed, a newer method of payment beyond paper money has emerged, which is the use of cheques. A cheque is a document guaranteeing a certain amount of money, drawn by an account holder, and given to a payee who can negotiate the cash or deposit it into an account. Cheques are used for currency transactions and do not need to be exchanged for physical currency (Kagan, 2021). However, according to Moran (2017), cheques can be expensive, represent a danger of theft and fraud, and complicate cash flow management. One research has showed that as the number of check

payments declined, these payments were replaced by electronic payments and credit card payments. The same study also showed that consumers who cut back on check or cash payments one year were more likely to cut back on check or cash purchases the next, but the reduction did not result in a reduction in the bills they paid. So, this proves that new payment methods namely electronic payment and credit card are open to consumers in the future (Stavins, 2021). Based on Musinski (2021), credit cards originated after World War II, with the first Diners Club Card launched in New York City in 1950. Today's national credit card market, with processing companies such as Visa and Mastercard and bank cards that can be used almost anywhere, originated in the late 1950s.

1.1.2 Adoption of Electronic Payment

Electronic payment can be defined as making financial transactions between buyer and seller through online mode without the involvement of physical cash (Hassan et al., 2021). With the increasing innovation in information technology, the payment method has then evolved into electronic payment such as online credit payment, digital wallet (e-wallet), internet banking, and electronic check. Many transactions that were previously made by cash or cheque are now made through digital channels. In Malaysia, for example, the central bank aims to reduce the use of cheques and increase the use of electronic payments. Accordingly, Malaysia's government has implemented strategies to encourage the use of electronic wallets to promote the development of a cashless society and stimulate the transition to an electronic payment era (Teoh et al., 2020). There are around 75% of Malaysians have successfully gone cashless (Azreen Hani, 2022). It is seen through the payment statistics from Central Bank Malaysia, indicating that the number of electronic payment transactions made per capita has increased from 124.6 in 2018 to 291.0 in 2022. As for cheque payment methods, the number of transactions has decreased from 3.1 in 2018 to 1.4 in 2022 (Bank Negara Malaysia, n.d.). It shows that there is a growing preference for electronic payment among Malaysians. Digital wallet and internet banking

are the popular electronic payment methods in Malaysia, especially due to Covid-19 epidemic, which has accelerated adoption of both electronic payment methods.

Figure 1.2
Basic Payment Indicator

	2018	2019	2020	2021	2022
Population (million)	32.4	32.5	32.6	32.6	32.7
GDP (RM million)	1,447,760	1,513,158	1,416,605	1,545,372	1,788,183
Cash in circulation (CIC) (RM million)	94,307.2	100,158.8	117,687.0	136,520.7	146,269.1
Transaction Volume Per Capita (unit):					
Cheque	3.1	2.6	1.8	1.5	1.4
E-payments:	124.6	150.3	170.3	221.8	291.0
Credit card	13.8	15.7	15.0	17.1	21.9
Charge card	0.2	0.2	0.1	0.1	0.2
Debit card	7.6	11.4	15.3	22.6	36.8
E-money	59.3	64.3	56.3	64.7	97.5
Other cashless instruments	0.2	0.2	0.1	...	0.1
Interbank GIRO	6.4	6.2	8.1	10.8	9.1
Instant Transfer	7.4	13.7	22.3	34.9	45.5
Interbank direct debit	0.1	0.1	0.2	0.3	0.4
ATM	1.1	1.0	0.5	0.3	0.3
Internet banking	19.0	23.1	30.6	40.8	44.5
Mobile banking	5.9	10.1	17.8	25.3	26.6
Mobile payment	0.04	0.2	0.4	1.2	4.4
RENTAS - Third party transactions	0.1	0.1	0.1	0.1	0.1
Intrabank direct debit and standing instructions	3.6	3.9	3.6	3.6	3.7

Source: Bank Negara Malaysia. (n.d.). *Payment statistics*.

People are more adapted to use electronic payment as their payment method because of its convenience. It allows users to make payments or deposit online at anytime and anywhere without having to meet each other physically. Also, those who uses electronic payment will have a greater transparency and control over their finances as they can easily access to transactions history, real-time balances, and spending alerts. An increased trend of Malaysian adults adopting electronic payment from 62.20% in 2014 to 79.30% in 2021 (World Bank Group, 2021).

In Malaysia, there are a variety of digital wallets available for consumers to select such as Touch 'n Go, GrabPay, ShopeePay, BOOST. These are some of the most popular brands, with Touch 'n Go being the most widely used digital wallet in the country. Consumers may just use any of those digital wallets to make online purchases. Age groups of 18 to 44 seem to be more likely to adopt the digital wallet and internet banking as they are more

digitally savvy and familiarize with the digital systems (Gomes, 2022). Even if there are no incentives such as cash back, rebates, or promotions, most Malaysians have adjusted to the new normal and are willing to use digital wallets. From figure 1.4, 70% of respondents will continue to use it even if there were no incentives being offered to them. This indicates that Malaysians are opting to be cashless more frequently in their daily activities.

Table 1.1

Willingness to use e-wallet without incentives

Year	Willing (%)	Maybe (%)	Not Willing (%)
4Q2019	77	10	13
1Q2020	55	22	23
2Q2020	57	20	23
3Q2020	70	17	13

Source: *E-wallet usage in Malaysia 2020: Thriving in lockdown.* (2020). Oppotus.

1.1.3 Online Financial Scam

Due to technological advancement, there is a growing adoption of internet banking and digital wallet by the consumers. It drives Malaysia to form a cashless society as people nowadays are over-reliance on electronic payment. Undeniably, online financial transactions has provided several favourable aspects to the users in comparison to the traditional transactions method, and digital payment are critical to Malaysia’s financial services industry. However, a rise in online financial scam in Malaysia has been reported recently. Online scam refers to a person who responds to an unauthorized request through the Internet by providing private information, thereby suffering from financial and non-financial losses (Ansar et al., 2021). It can be defined as those who uses internet services or software to defraud or exploit victims, usually for financial gain. The ease of online financial transactions has created an opportunity for fraudsters to commit cybercrime.

They are drawn to the increase in money flows as well as inexperienced users, which allows them to discover a new way to deceive consumers online where money is transacted.

Internet users have become unaware of the transparency of their information as a result of their reliance on the internet. According to the Police’s (PDRM) commercial crimes investigation department (CCID), the online scam cases have increased significantly over the years due to the increasing proficiency in exploiting technology, and victims with low awareness of cybercrime via online methods (Basyir & Harun, 2022). The table below shows the total reported online scams and losses from 2019 to 2022.

Table 1.2

Summarized of online scam cases and losses

Year	Total Reported Online Scams	Total Reported Losses (RM)
2019	13,703	RM539.0 million
2020	17,227	RM511.2 million
2021	20,701	RM560.8 million
2022	25,000	RM850.0 million

Source: Basyir, M. & Harun, H. N. (2022). Online scam cases increasing in Malaysia. *New Straits Times*.

People who adopt electronic payment are at the risk of being the victims of online financial scam as they are highly anticipated on the internet until they are unaware of the risk associated with the electronic payment. An example can be seen is that of a woman who lost RM21,399 after being deceived by scammers using the digital wallet redemption ruse (Yahya, 2022). In addition to this example, according to Lee (2020), a Malaysian Facebook user, Jacqueson Cheok, lost RM30,000 in five minutes due to bank fraud in which scammers posed as agents of Bank Negara Malaysia to obtain his personal details and transfer money from his bank account. In the end, Maybank froze his account and returned the money, but Oversea-Chinese

Banking Corporation (OCBC) bank was unable to recover the money he lost. Furthermore, online love scams can not only cause mental loss but also serious monetary loss. The incident took place in Sabah, Malaysia, where a 19-year-old female student lost nearly RM50,000 after falling victim to a love scam syndicate on Telegram. It started when a man she met online asked her for financial help to buy online game software. The victim believed the man and wired the money into five different accounts in stages. After the fact, she realized that she had been cheated (Fong, 2023). Similarly, another case involved a victim who was scammed out of money on social media. The victim lost nearly RM5,000 after buying clothes on social media via a link sent by a clothing seller (“Almost RM40mil lost to scams since October 2022”, 2023). Also, a victim has lost RM4,600 after responding to the fraudulent notification of e-wallet assistance (Fong, 2023). Through the statistics, it has clearly shown that the online financial scams are dramatically increased as time goes by. Significantly, this issue has become a threat to Malaysia’s internet users and it is important to explore Malaysians’ awareness on online financial scam.

1.2 Problem Statement

In this modern era, digitalization is booming as it brings convenience to both consumers and organizations. From consumers’ perspective, digitalization has increased efficiency and convenience (Malak, 2022). While from an organization’s perspective, digitalization allows them to unlock new opportunities and drive organizational change (Prause, n.d.). Therefore, there are more and more organizations are involved in digitalization and trying to adopt digital technologies in their businesses (Mardhiah, 2023). According to Malaysia Digital Economy Corporation (MDEC) CEO Mahathir Aziz, by 2025, the growing usage of digital adoption will account for 25.5% of the nation's GDP. (Gomes, 2022a).

It is undeniable that the contribution of digitalization to Malaysia’s economy is pivotal. However, on the downside, there are opportunities for cybercriminals to

exploit the technological changes and explore even more sophisticated scams against unsuspecting online users (Mardhiah, 2023). Online scam is a critical issue, which has devastating and wide-ranging negative impacts on the victims. It can be catastrophic and drive victims into financial debt, even small losses can have a traumatic impact on people with mental health problems (Lee, 2020). Plus, the online scam can also cause lasting mental trauma for the victims (“The Total Impacts of Fraud”, 2020). For instance, most of the victims feel ashamed and embarrassed, often blaming themselves. As a result, it could have a lasting impact on their confidence in using the internet (Lee, 2020).

Online scam cases are escalating, according to Inspector-General of Police Tan Sri Acryl Sani Abdullah Sani. There were just 13,703 scam cases in 2019 and RM539 million was lost as a result. Nevertheless, the officials had observed 20,701 scams, resulting in an RM560.8 million loss in 2021. According to the authorities, fraudsters have been using advances in technology recently, and their typical victims are individuals who are unaware of how scams operate, which makes them easy prey for deceitful fraudsters (Wong, 2022). Moreover, the Domestic Trade and Consumers Affairs Ministry claims that from 2020 to February 17, 2022, during the Covid-19 pandemic, they received 24,018 complaints that related to online fraud and social media fraud, resulting in losses totalling RM21.7 million (David, 2022).

Overall, Malaysia was experiencing a major problem with online scams. As of 14 October 2022, Tengku Datuk Seri Zafrul Tengku Abdul Aziz, the then-Finance Minister, announced the establishment of the National Scam Response Center (NSRC) to combat online fraud. NSRC has acted as a command center to organize rapid reactions to online financial frauds, including the quicker tracing of stolen funds, criminal investigations, and enforcement action against con artists. The center will concentrate on a variety of online scam techniques, such as phishing scams, Gambling scams, malware attack scams, package delivery scams, and love scams. For instance, victims are urged to get in touch with the NSRC if they were duped into transferring money through online banking services (National Anti-Financial Crime Centre, n.d.).

It can be observed that the impact of online financial scams goes well beyond financial loss, the victims may have a traumatic impact on mental problems (“The Total Impacts of Fraud”, 2020). The main problem is that people may have insufficient awareness of online financial scams. As a result, the scammers will exploit their weaknesses to defraud them. Malaysians seems to have a low awareness of scams. It is due to the evidence from the sharp increase in internet scams over the past two years. For instance, from 2020 to May 2022, the Polis Diraja Malaysia (PDRM) commercial crimes investigation department reported approximately 72,000 scams and RM5.2 billion in damages. According to the data shown, there were 48,850 of the 72,000 frauds, of which was 68% reported over the past two years were linked to online scams (“Scam Awareness: Be Informed To Protect Yourself”, 2022).

According to Financial Capability and Inclusion Demand survey, one in three respondents said they would be willing to disclose their bank account PINs or passwords with close friends. About two-thirds of those polled do not consider a website's security measures before making an online purchase. As a result, people are much more likely to be deceived into giving their banking information to a fraudulent website, which enables criminals to commit fraud (Marzunisham Omar, 2022). In this case, the users should be urged to use different passwords for every website and, whenever feasible, stay away from disclosing sensitive information online (Gainsbury et al., 2019).

The pandemic of Covid-19 has accelerated the rise in use of the social media, and the rapid technological enhancement have led to peoples’ lives becoming more digital. The outbreak and subsequent economic downturn have also disturbed relative demands in ways that will probably lead to an increase in financial fraud during the next few years (Karpoff, 2021). In addition, criminals are also finding innovative ways to commit online financial scams with more sophisticated methods. Moreover, Kadoya et al. (2021) believed that despite the inventive swindling techniques that fraudsters utilise, the authorities were having trouble stopping financial crime was due to the frequent changing of target groups. For instance, the fraudsters were skilled at identifying their victims since they chose particular susceptible groups to prey on. In addition, Karpoff (2021) stated that

some fraud innovations and changes also facilitate the possibility of fraud, such as the anonymity in certain financial transactions. As a result, these factors make people fall prey easily to scam activities. Further, low scam awareness makes people vulnerable to scams. In this case, the fraudsters will always find a way to deceive people as long as people have a low level of scam awareness. Overall, Gamble et al. (2014) believed that the increasing awareness may protect people against the harmful effects of overconfidence that may lead to financial fraud. However, the open availability of instances of potential criminal behaviour makes online fraud somewhat distinctive among other crimes. Although it might appear that people are unable to stop this problem, people may lessen its impacts by raising awareness and understanding (Norris et al., 2019). Therefore, in this research, it is important to explore Malaysians' awareness towards online financial scam.

1.3 Research Question

This research paper aims to examine the following questions.

- Is there any significant relationship between the cybersecurity knowledge with Malaysians' awareness on online financial scams?
- Is there any significant relationship between the perceived severity with Malaysians' awareness on online financial scams?
- Is there any significant relationship between the security and privacy concerns with Malaysians' awareness on online financial scams?
- Is there any significant relationship between the subjective norms with Malaysians' awareness on online financial scams?

1.4 Research Objective

The purposes are to analyze the relationship among cybersecurity knowledge, perceived severity, security and privacy concern as well as subjective norms with Malaysians' awareness on online financial scam.

- To examine the relationship between the cybersecurity knowledge with Malaysians' awareness on online financial scams.
- To examine the relationship between the perceived severity with Malaysians' awareness on online financial scams.
- To examine the relationship between the security and privacy concern with Malaysians' awareness on online financial scams.
- To examine the relationship between the subjective norms with Malaysians' awareness on online financial scams.

1.5 Research Significance

With the rapid popularization of the Internet and the rapid development of financial technology, online financial fraud has become a global problem. In Malaysia, where the number of Internet users is growing, online financial scams pose a threat to the property and safety of the vast number of users. Therefore, it is of great significance to investigate the awareness of Malaysian towards online financial scams.

Furthermore, this research in helping Malaysian, including the younger and older generation to understand the common means and characteristics of financial fraud, so as to improve their cognition and prevention ability of financial fraud. Moreover, this research can also provide reference for Internet enterprises to promote and improve the security mechanism of Internet users, so as to enhance users' sense of trust in e-banking.

Besides, this research can help companies increase customer trust and gain a competitive advantage. By understanding the security needs and risk awareness of customers, companies can develop more secure and reliable financial products and services, thus improving customer satisfaction and trust. Also, it presents an overview of the phenomenon and trend of fraud in the industry, and timely take corresponding risk prevention and control measures to ensure the safety of

customers' assets to gain competitive advantages. In a competitive financial market, customers are more willing to choose companies that offer more security, so by providing more reliable financial products and services for the security needs of customers, companies can win more market share.

Moreover, this research can help consumer protection organizations understand the risks and problems faced by consumers in online financial transactions, such as fraud and information leakage, so as to provide advice to companies to protect the rights and interests of consumers. To this end, consumer protection organisations can take various measures, such as conducting regular research to understand the risks and problems consumers face, raising public awareness of online financial fraud, handling complaints in a timely manner to identify problems in the market, and through the supervision and evaluation of the government and enterprises in a timely manner in the prevention of online financial fraud problems and deficiencies, promote the government and enterprises to strengthen the relevant work.

Lastly, it serves as reference for policymakers and financial institutions to formulate more effective laws and regulations and policies to strengthen the supervision and crackdown on financial fraud. In addition, this study is also significant for driving the digital transformation and upgrading of Malaysia's financial industry. Globally, the financial industry is experiencing a wave of digital change. By understanding Malaysians' awareness of online financial scams, government and financial institutions can better plan and implement digital transformation strategies to enhance the digital level and user experience of the financial industry.

1.6 Conclusion

There are five chapters in our research proposal that are related to the topic of awareness on online financial scam. The first chapter mainly discuss on the intention to explore Malaysians' awareness on online financial scam, and research significance. The digitalization in Malaysia, adoption of electronic payment as well as a brief introduction of online financial scam are being covered. The next chapter,

a literature review based on research topic and theoretical framework will be included.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

In chapter two, relevant theories that contributed to research framework are further discussed. The dependent variables and explanatory variables will be reviewed in upcoming section , followed by the development of hypothesis.

2.1 Underlying Theories

Technology Threat Avoidance Theory (TTAT) and Theory of Planned Behaviour (TPB) are the theories used in this research.

2.1.1 Technology Threat Avoidance Theory

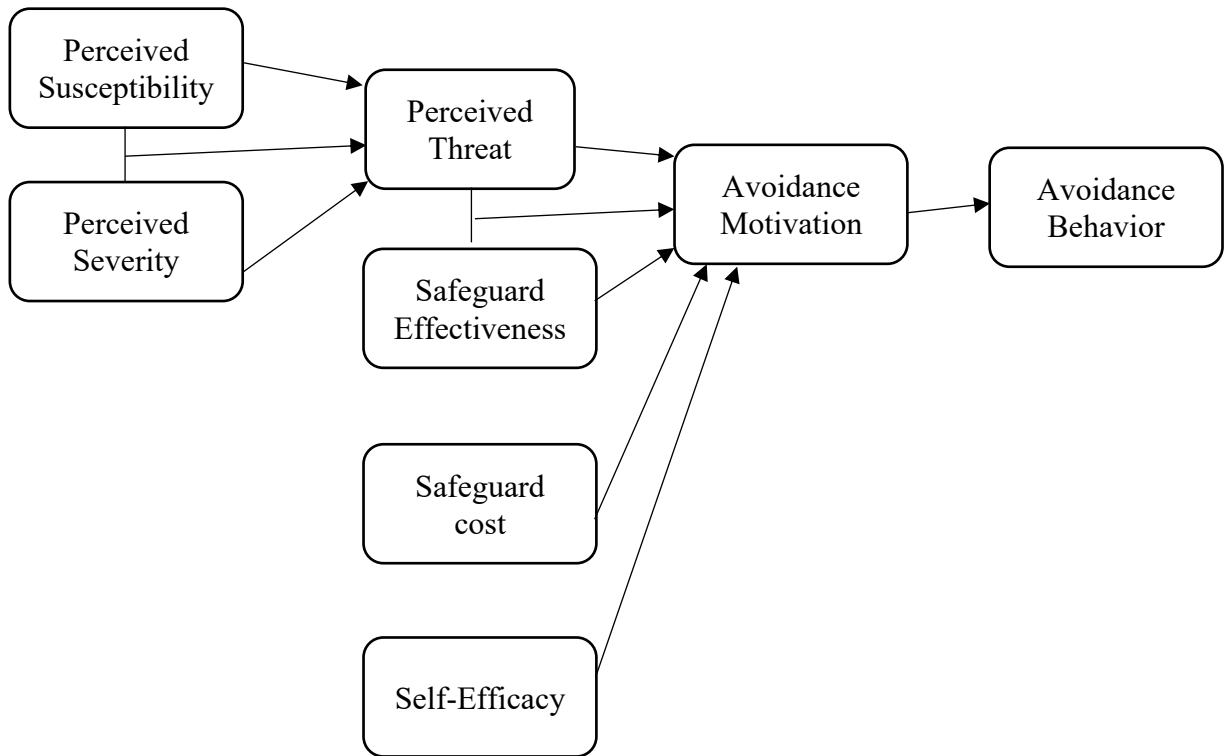
Technology Threat Avoidance Theory (TTAT) is an indigenous information systems theory that synthesizes literature from the fields of psychology, healthcare, and risk analysis and incorporates them into IT security settings. The purpose of TTAT is to explain the avoidance behavior of internet users in the face of IT threats, that is, why people take steps to protect themselves from internet attacks (Chen & Liang, 2019). In addition, TTAT proposes a cognitive and behavioral model to explain how people deal with technological threats when making decisions. Nowadays, the Internet is becoming more and more developed, and there are countless online financial fraud cases. Therefore, people are faced with various technological threats, so it is necessary to make decisions and actions to avoid these threats.

According to Liang & Xue (2009), TTAT describes a dynamic cyclic process. In this process, people need to go through two cognitive processes,

namely threat appraisal and coping appraisal, to decide how to deal with IT threats. The two antecedents of threat perception are susceptibility and severity. Perceived susceptibility is an individual's perception of the risk that a security event will actually affect them, while perceived severity is the perception of the potential negative consequences of that event. For example, in a threat appraisal, people will recognize an IT threat if they believe they are an easy target for a malicious IT attack and the negative consequences are severe. This awareness leads to a coping appraisal, where people consider what safeguards they can take to avoid IT threats. They consider the effectiveness and cost of protective measures, as well as the self-efficacy of taking those measures.

This research will use TTAT to provide a theoretical basis because this theory can be used to explain people's decisions and behaviours in the face of online financial scam. According to the theory, people act based on their cognition and perception of threats, so when people recognize the threat of online financial scams, they may take steps to avoid these threats. In this research, there were four independent variables, including, cybersecurity knowledge, perceived severity, subjective norms, and security and privacy concerns. For example, subjective norms in the TTAT can be used to measure an individual's attitude toward online financial scam to explore how this attitude affects their willingness to adopt safe behaviours. In addition, the security and privacy concern in the TTAT can help researchers delve deeper into the privacy and security risks that individuals face in online financial transactions, and further understand their perception of these risks and coping strategies.

Figure 2.1
Technology Threat Avoidance Theory



Source: Liang, H., & Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, 11(7), 394-413.

2.1.2 Theory of Planned Behaviour

This research uses the theory of planned behaviour (TPB) as the second theoretical basis. Based on Persada et al., (2021), TPB is a development of the theory of reason action (TRA), recognized as one of the classical theories of persuasion, acceptance, and use of technology. In addition, it is one of the most used theories in the field of electronic commerce and has been successfully used to explain and predict user behaviour because it is used to explain the relationship between human attitudes and behaviours, and also to predict how individuals will act according to their existing attitudes and behavioural intentions (Apau & Koranteng, 2019). At the same

time, TPB states that the prediction of intentions to engage in various behaviors is possible through the assessment of attitudes, perceived norms, and perceived behavioral control. In other words, people's behaviour is deeply influenced by how positively others evaluate and recommend them (Vafaei-Zadeh et al., 2019).

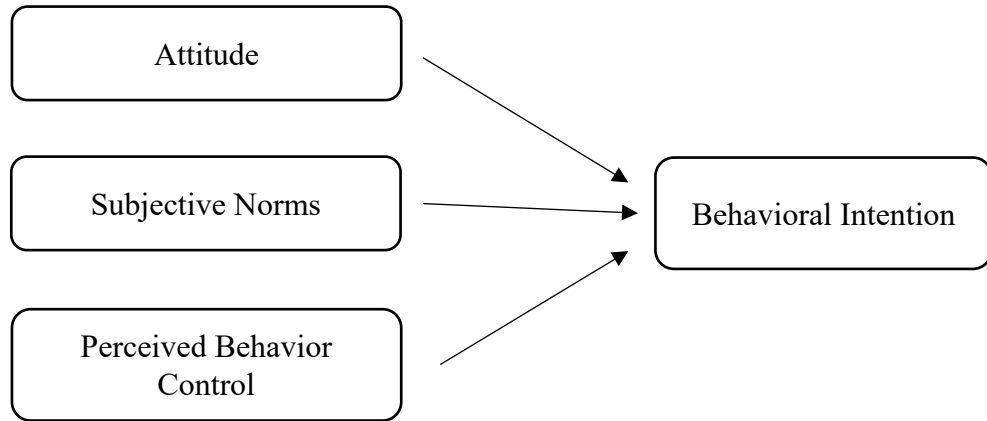
First, in the TPB model, attitude is considered to be a feeling that causes an individual's feeling in relation to the action to be done. In this research, researchers can explore the surveyed consumers' cognition and views on online financial scam. For example, whether they believe there are risks in online transactions, whether they think the probability of fraud is high, etc. Consumer attitudes have an important influence on whether to take preventive measures. Second, subjective norms represent individuals' beliefs about the expectations of certain behaviours from influential people in their lives. The researchers can find out whether the surveyed consumers feel social pressure to take precautions, such as whether the individual's family, friends, or colleagues encourage them to take precautions. Perceived behavioural control represents an individual's perception of how easy it is to achieve a particular behaviour. The researchers were able to find out how confident and confident the surveyed consumers were about taking precautions. For example, does the individual know how to take precautions against online financial scam and feel empowered to take these measures (Persada et al., 2021).

To sum up, TPB emphasizes that behaviour is predictable and controllable, and individual behaviour will be affected by elements like attitude, subjective norm, and perceived behaviour control. In this case, researchers can use TPB to explain the reasons and behaviours of consumers to take preventive measures. Researchers can investigate respondents' attitudes, subjective norms, and behavioural control to understand their likelihood or motivation to take preventive measures. The data can then be used to develop and implement more effective preventive measures. Therefore, in this research, TPB can be used as a basic theory in the case that the

awareness of online financial scam is a dependent variable and help researchers to understand and predict individual prevention behaviours.

Figure 2.2

Theory of Planned Behaviour (TPB)



Source: Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–21.

2.2 Reviews of Variables

2.2.1 Awareness on Online Financial Scam

The expansion of digital financial services (DFE) is providing greater access to financial services in both developed and developing countries, but consumer protection issues are becoming increasingly important as DFE becomes more widespread (Kubilay et al., 2023). Online financial scams are one of the main problems. Online financial scams have become rampant in recent years especially during and after Covid-19 pandemic, costing individuals and institutions around the world billions of dollars. Online financial scams are defined as fraudulent schemes that use the Internet to deceive or make false promises and attempt to obtain money or other valuables from the victim. Based on Cole (2023), the definition of online

financial fraud varies between regulators and criminal agencies, making it challenging to detect and prevent this crime. However, the Federal Bureau of Investigation (FBI) classifies online fraud into seven categories, including phishing and malware, which are common tactics used by cybercriminals to deceive and defraud individuals or organizations.

According to Norris & Brookes (2021), with the development of technology, online behaviour for illegal financial gain or other malicious purposes, such as phishing emails has increased. An estimated 29 billion phishing emails, which victimize individuals and reveal personal information, are sent worldwide every day. This can cause serious psychological and financial hardship for those who are unaware. In addition, online shopping scams often involve scammers creating fake websites or advertisements that resemble legitimate online stores. Scammers may use logos and layouts similar to those of authentic retailers to sell luxury goods at low prices. They typically demand payment through money orders, pre-loaded cash cards or wire transfers, and disappear after making multiple sales (“Online Shopping Scams”, n.d.).

Furthermore, one study found that older people are often less tech-savvy than younger people, due to a lack of technical knowledge and an increased risk of online fraud and social isolation may make older people more susceptible to manipulation, reducing their awareness of potential fraud risks (Kemp & Erades Pérez, 2023). Moreover, in the view of Ahmad et al. (2021), security and privacy concerns are major barriers for customers when conducting e-banking and e-commerce activities. For example, trojans often come in the form of attachments and take advantage of users' lack of security awareness and knowledge, causing them to suffer financial losses.

Besides that, based on “Scam Awareness: Be Informed To Protect Yourself”, (2022), Malaysians' lack of awareness about scams, especially investment and capital market products, has led to a surge in online fraud in the past two years, resulting in nearly 72,000 scams and RM5.2 billion losses. Malaysians have a low level of digital financial literacy, with one in

three willing to share bank account passwords with close friends and many people do not pay attention to websites' security features before making online transactions, which increases their risk of becoming fraud victims. Apart from Malaysia suffering a surge in online fraud, its neighbour, Thailand has also seen an increase in cyber threats and scams due to the expansion of e-commerce. Thailand's online shopping market size is expected to reach \$18.97 billion in 2021, with more than 36 million consumers expected to shop online. As a result of this trend, the ChaladOhn website was developed between the second quarter of 2021 and the first quarter of 2022 to help Thai consumers reduce online financial scam and increase their awareness of online financial scam, especially for small transaction cases that victims often ignore or do not report to the police (Daengsi et al, 2022).

2.2.2 Cybersecurity Knowledge

Cybersecurity knowledge refers to an individual's knowledge about cybersecurity practices to avoid falling into cyber-attacks such as online financial scams. It also known as to what extent an individual understands about the importance of information security and to take out precautions measures to protect personal information being stolen (Zwiling et al., 2020). Most of the online financial scam happened mainly due to the lack of cybersecurity knowledge that help the victims to protect themselves from falling into the trap. According to Das and Patel (2017), people are more vulnerable to cyber-attacks and are ignorant of the risks while providing personal information on social networking sites due to a lack of cybersecurity knowledge. Victims who lack of cybersecurity knowledge tend to trust the internet security without taking any self-precautions to avoid falling into online financial scam. For example, they would just simply login into their online banking account through banking apps such as Maybank2U or PBe without checking whether they are logging into a real online banking website.

It is essential for the individuals to have sufficient cybersecurity knowledge to increase the awareness towards online financial scam. A research from Verkijika (2019) has revealed that increasing of cybersecurity knowledge enhances individual's security threat avoidance. Knowing more about cybersecurity matters will allow an individual to gain awareness about current online financial scam and techniques to avoid financial losses. For example, an individual with higher cybersecurity knowledge led to high awareness towards cybersecurity threats such as online financial scam as they tend to be more careful in dealing with the confidential and private information through online (Inan et al., 2016). They would not simply share their banking information or password to anyone as compared to those who have a lower cybersecurity knowledge, and they have a better understanding on scammers' tactics to adopt best practices for protecting themselves towards online financial scam. Also, the more knowledge they have in cybersecurity, the more aware they are of the threat and the easier it is to identify the online financial scams techniques (Asher & Gonzalez, 2015). This can be supported by research from Purkait, Kumar and Suar (2014), stating that the lack of knowledge in cybersecurity among internet users will cause them to face significant financial losses. Individuals with high level of cybersecurity knowledge are more likely to recognize financial scam and take precautionary measure to avoid falling into the trap.

In summary, past research have revealed that how cybersecurity knowledge affect the awareness towards online financial scam. It is expected to have a significant relationship between cybersecurity knowledge and awareness towards online financial scam.

Hypothesis:

H0: There is no significant relationship between the cybersecurity knowledge and awareness of Malaysians on online financial scams.

H1: There is a significant relationship between the cybersecurity knowledge and awareness of Malaysians on online financial scams.

2.2.3 Perceived Severity

Perceived severity can be described as an individual's subjective assessment of the seriousness of a specific threat or harm. It means that the extent to which an individual believes how serious the threat is, and how the consequences of threats would be harmful. According to Liang and Xue (2009), perceived severity would influence the level of perception towards threat. For example, if an individual believes that the consequences of falling victim to an online financial scam are severe, they are more likely to take precautions and be aware of the risks associated with online financial transactions such as checking account statements on a regular basis and be alert to any suspicious transactions in their accounts.

Also, there are some past researches showed that perceived severity may affect the awareness towards online financial scam. Based on the research from Tsai et al. (2016), perceived severity of online threat has a relationship with individuals' online safety behaviour, including their awareness towards online financial scam. Having high level of perceived severity indicates that an individual will be more aware of the issues of threat such as online financial scam, and has a higher motivation to protect themselves towards the threats (Crossler & Bélanger, 2014; Thompson et al., 2017). For example, an individual with higher perceived severity will be more aware and cautions of potential online financial scam when receiving an e-mail or messages that consists of a suspicious link to obtain the credit credentials. They will be more concerned of the consequences of not verifying the authenticity of the links, e-mail or messages provided and take steps to avoid falling into trap, which will increase towards online financial scam.

However, William and Joinson (2020), pointed out that there is inadequate proof to support perceived severity has a relationship with awareness towards phishing attacks, which is one of the online scams. Also, Ifinedo

(2012) highlighted that perceived severity has no impact on security threat. Individuals who perceive the scam to be more severe are less likely to take protective measures, indicating that they are unaware of the nature of online financial scams.

In summary, this research expects perceived severity affect the awareness towards online financial scam. Most of the researches indicated that perceived severity is important in determining a person's awareness of online financial scams, as this can influence their behaviour and actions when it comes to protecting their personal and financial information online.

Hypothesis:

H0: There is no significant relationship between the perceived severity and awareness of Malaysians towards online financial scams.

H1: There is a significant relationship between the perceived severity and awareness of Malaysians towards online financial scams.

2.2.4 Subjective Norms

Johnson (2017) asserts that the subjective norm reflects the social pressure that an individual perceives to engage in or refrain from engaging in a specific action. According to Macovei (2015), subjective norms represent an individual's sense of the relationship between a particular type of behavior and what the reference group perceives as the behavior.

An individual's choice to participate in a given activity is influenced by the subjective norm of expected behaviors, which is a function of normative ideas about whether such conduct should be performed (Fishbein & Ajzen, 1980). In The Theory of Planned Behavior (TPB), subjective norms stand for the social pressure or influences from others—peers, friends, family, or coworkers—on a certain kind of behavior (Glanz et al., 1992).

However, Alanazi et al. (2022) support the idea that subjective norms favourably influence young adults' behavioural intentions towards cybersecurity behaviours, in contrast to other studies that did not report a significant relationship between behavioural intention and subjective norms (Farooq et al., 2019). For instance, if young adults felt social pressure from their friends, peers, family, or co-workers to adopt cybersecurity behaviours to keep themselves secure online, this perceived social pressure had a favourable impact on their intentions to do so. Young adults should therefore be made aware of the risks of cyber threats that result from ignoring online security practices, as well as how adopting appropriate cybersecurity behaviors can lead to positive outcomes, such as being safe online (Alanazi et al., 2022).

Hence, subjective norms is included in this research to determine Malaysians awareness towards online financial scams. This method will help to distinguish between a person's subjective environment and their cognitive rationale under the protection motivation theory. Overall, it is expected that subjective norms have an impact on awareness of online financial scams as most studies show that subjective norms and online financial fraud are positively correlated.

Hypothesis:

H0: There is no significant relationship between the subjective norms and awareness of Malaysians towards online financial scams.

H1: There is a significant relationship between the subjective norms and awareness of Malaysians towards online financial scams.

2.2.5 Security and Privacy Concern

Online retailers provide privacy and security policies as reassurances that the information about their customers is safe and secure (Ray et al., 2011). According to a survey, one of the main factors influencing consumers' trust in retailers' services is security concerns (Alzaidi & Agag, 2022). When

faced with privacy concerns, consumers would typically reduce their online shopping habits (Cowan et al., 2021). According to Acquisti and Grossklags (2005), the majority of customers who lack sufficient information make privacy-sensitive judgments and are inclined to trade convenience for privacy or personal information. They also refuse to make use of tools that protect privacy. Because of this, Acquisti and Grossklags (2005) point out that customers' views of and privacy concerns differ from their actual online activity.

The control over how personal information is exchanged and shared with others is referred to as privacy (Alan, 1968). Whereas from the perspective of e-commerce, privacy concerns could be seen as one of the most significant risks that have emerged during the expansion and development of e-commerce. Online users have long concurred that disclosing personal information is inherently hazardous for several reasons (Sheehan & Hoy, 2000). While customers are growing more aware of the Internet, according to Graeff (2002), they are more concerned about the extent of the revelation of their privacy.

Wopperer (2002) asserts that a rise in online financial theft will be caused by people's ignorance of security issues. Due to the ease with which fraudsters can exploit flaws, consumers' personal information, including credit card numbers, can be obtained. According to Chawla & Kumar (2021), security concerns pose possibly the biggest threat to e-commerce. Also, according to Rogers (1975), the research showed a favourable correlation between young teenagers' privacy-protecting behaviours and their level of privacy worries. According to Youn (2009), participants that have a lot of privacy concerns might study privacy terms and set up security software like firewalls. Plus, according to Milne et al. (2004), a significant predictor of online privacy and identity protection behaviours, such as refusing to provide information or conducting transactions, was the level of privacy concerns.

However, there are some scholars argued that security and privacy concern has no impact on the awareness of online financial scam. According to Chen

et al. (2017), being a victim of Internet fraud was not predicted by understanding Internet privacy, meaning that Internet privacy did not decrease the likelihood of falling into online scams. Alhassany and Faisal (2018) also stated that the perceived risk factor which included security and privacy concerns was weak compared to other factors.

To sum up, most studies show that people who are concerned with their security and privacy will increase their awareness towards online financial scam. Therefore, it is expected that security and privacy concern is positively related to online financial scam.

Hypothesis:

H0: There is no significant relationship between the security and privacy concern and Malaysian Internet users' awareness of online financial scams.

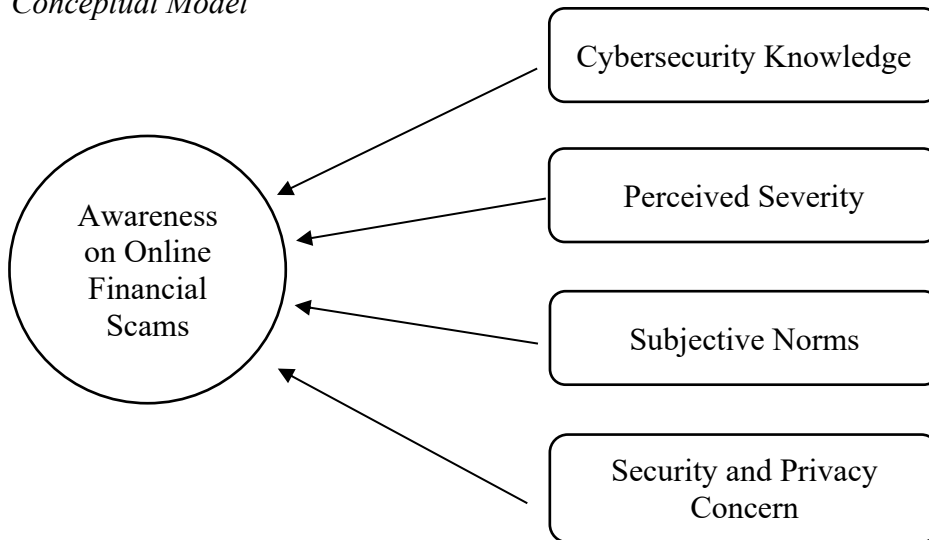
H1: There is a significant relationship between the security and privacy concern and awareness of Malaysians towards online financial scams.

2.3 Theoretical Framework

The research consists of a few independent variables, including cybersecurity knowledge, perceived severity, subjective norms, as well as security and privacy concern. Apart from that, the dependent variable is Malaysian's awareness towards online financial scams. Hence, the independent variables shown in Figure 2.3 are expected to have an impact on dependent variable.

Figure 2.3

Conceptual Model



2.4 Conclusion

This chapter has revealed the relevant theories such as Technology of Threat Theory (TTAT) and Theory of Planned Behaviour (TPB) in details. Also, there are five independent variables that related to the awareness of online financial scam being discussed in this chapter, which are cybersecurity knowledge, perceived severity, subjective norms, as well as security and privacy concern. Lastly, conceptual model and hypothesis also presented within this chapter.

CHAPTER 3: METHODOLOGY

3.0 Introduction

Chapter three primarily focuses on the process of data collection and analysis. It will be categorized into several sections, including research design, data gathered method, sampling method, research measurement, data analysis tools. Detailed explanation will be provided in the following.

3.1 Research Design

It is a structured framework or blueprint that chosen by researchers to achieve the research objectives and questions (Dulock, 1993). There are a variety of research design can be used depending on the purpose of the research, such as descriptive research, exploratory research, causal research, and experimental research.

3.1.1 Descriptive Research

Descriptive research is a methodological approach that aims to describe a given situation, population or phenomenon in an accurate and systematic way (Dulock, 1993). According to Swartzell and Jennings (2007), descriptive research helps to clarify what is frequent or already existent in a population, not to predict or manipulate an outcome. Instead, it focuses on observing, measuring, and simplifying the data that has been collected in a sensible way. Also, the data gathered through descriptive research is respond to a range of questions of what, when, and how, but not the questions of why. There are numerous ways can be used to conduct this descriptive research, including observations, surveys, interviews, and case studies.

In this research, questionnaires, as a form of survey research will be use to collect information from the respondents. By using survey research, researchers are allowed to collect extensive amounts of data, which can then be evaluated to determine the frequencies, averages, and patterns. Besides, questionnaires is more useful and cost-effective for researchers to gather data from a large population.

3.2 Data Collection Method

Techniques that used by the researchers in collecting information to solve the research questions are known as data gathering method (Dudovski, 2022).

3.2.1 Primary Data

Primary data can be defined as the information that gathered by researchers in first-hand without any intermediaries or secondary sources (Mazhar, 2021). Surveys, interviews, and observations are the examples of primary data collection method. Primary data is being used in this research due to its accuracy and reliability as the data has not been used by any other researchers to interpret or analyze it. By collecting the primary data, researchers will have full authority over the data collection process, allowing them to design the questions and research methods that are aligned with their specific research objectives.

This research will use questionnaires to obtain the immediate responses from targeted respondents. This research targets whole Malaysian who hold an e-wallet account or any online banking account in different states. Each respondent will be given the same questions, ensuring that the entire data collection can be fairly analyzed. After collected the questionnaires, the data will then be analyzed by using a software, namely Smart PLS 4.0, which is

designed for conducting structural equation modeling (SEM) and path analysis. This software also capable in handling large datasets.

3.3 Sampling Design

It is impractical for the entire population to participate in the research; hence, a small group is selected and relied upon for data collection. According to Turner (2020), the sampling design involves employing a method to gather a sample from a given population, analyze and draw conclusions from the sample to make inferences about the population.

3.3.1 Target Population

The targeted population for this research is Malaysian that having an e-wallet account or any online banking account. Individuals who are lack of technology knowledge or unaware of the risks associated with online transactions are often more susceptible to being targeted by scammers. The reason of choosing this population is that online financial scams can affect wide range of people of all aged, including both younger and older generations. Hence, it is important to understand their awareness towards online financial scam to design effective ways of preventing such scams.

3.3.2 Sampling Frame and Sampling Location

Sampling frame refers to the list from which a sample is drawn for research (Syed Muhammad Sajjad Kabir, 2016). It serves as a reference for researchers in determining the target population for their research and selecting a representative sample from the population. Frame error will occur if the sampling frame does not accurately represent the population of interest (Stasny, 2001). Therefore, it is important in choosing the sampling

frame in order to reduce the risk of frame error and enhance the reliability and validity of the research. In this research, the sampling frame will be Malaysian who are 18 years old and above that having an e-wallet account or any online banking account. Also, 384 sets of questionnaires will be distributed to collect responses from the targeted participants.

Sampling location refers to the location or geographical area where the sample for the research is selected (Turner, 2003). The sampling location for this research is Malaysia as this research focusing on the awareness of Malaysian towards online financial scams. All Malaysian will be the targeted to participate in this research as long as they have an e-wallet account or online banking account.

3.3.3 Technique of Sampling

There are two methods in conducting sample, which are probability and non-probability sampling. According to Wiśniowski et al. (2020), the former is that a sample is being chosen randomly from the population, ensuring that each member of the population has an equal chance of getting chosen for the sample. The latter is that a sample is being chosen from population using non-random criteria. A non-probability sampling such as convenience sampling will be adopted in this research. Convenience sampling allows researchers to collect the data from a conveniently available pool of respondents (Ilker Etikan et al., 2016). In this research, Malaysians who holds an e-wallet account or any online banking account will be chosen to answer the questionnaire.

3.3.4 Sampling Size

According to the latest demographic statistics released by Department of Statistics Malaysia (2022), the population of Malaysia fourth quarter 2022

has reached 33.0 million, with a growth rate of 1.3% as compared to 2021. Krejcie and Morgan (1970) has suggested that at least 384 questionnaires are needed to explain the population size that exceeds 1,000,000. Also, the questionnaires will be distributed to 40 respondents for conducting the pilot test before distributing to the larger sample size. In order to reduce the sampling errors and to produce a more accurate and reliable results, this research will reach out 384 respondents.

3.4 Research Measurement

This research will employ questionnaires to gather and analyze the information that pertains to the research topic of Malaysian's awareness on online financial scam. Besides that, a pilot test will be performed to analyze the questionnaires' effectiveness in collecting relevant data for the research, thereby improving data's precision and credibility.

3.4.1 Questionnaire Design

A questionnaire survey is a data gathering way that is used to collect, analyze and interpret the views of a targeted population group of people. In the questionnaire, there will be a series of questions that need to be asked to the targeted respondents (Sincero, 2012). Questionnaire is used as it enables researchers to reach large pool of respondents easily. In this research, there are a series of questions being designed that relevant to the research to determine Malaysians' awareness on online financial scam.

The questionnaires will be divided into three sections. Section A was designed to collect respondents' demographic information such as gender, age, ethnicity, education level, monthly income, and subscription of any e-wallet or online banking account. In this section, all questions will be listed in the form of multiple choices.

In Section B, the questions are created to ask for the respondents' opinions and attitudes towards the dependent variable, which is the awareness of online financial scams. Section C consists of questions that related to the independent variables, which are cybersecurity knowledge, perceived severity, subjective norms, as well as security and privacy concern. Likert scales are used, with 1 indicating strongly disagree with the statement and 5 indicating strongly agree with the statement.

3.4.2 Pilot Test

To enhance the quality and effectiveness of the research, a pilot test is a pre-testing of the main research (Van Teijlingen & Hundley, 2002). Before the final survey questions are sent to actual respondents to acquire accurate and meaningful data, the pilot test's goals are to increase the research's viability, eliminate errors, and evaluate the questionnaire's usability (Albaity & Rahman, 2019). The researchers will be able to identify the survey's problems and determine how to address them after receiving the results of the pilot test.

According to Connelly (2008), the pilot test sample size should be 10% of the sample size for main research. Hence, a sample size of 40 respondents will be collected for pilot test since the total respondents for this research is 384 respondents. After the data being collected, Smart PLS 4.0 will be used to examine for any discrepancies, as well as to ensure the accuracy and reliability of questionnaires. For example, the questionnaires is considered as reliable if the Cronbach's Alpha (CA) value is 0.70 or above.

3.5 Construct Measurement

Scale is equipment that is used by the researchers to differentiate how respondents' perceptions differ on the variables in research from one another (Sekaran and Bougie, 2016). The questionnaire incorporates the use of Nominal, Ordinal, and Interval scales.

3.5.1 Nominal Scale

Nominal scale is ideal for qualitative variables where a straightforward naming scheme allows for the differentiation of the observations (Cicchetti, 2011). There is no quantitative relationship between the categories; hence, the data cannot be valued. Race and other factors such as gender, education level, ethnicity are measured on a nominal scale. In Section A, demographic information of target respondents is created using a nominal scale. Some questionnaires listed below were created using nominal scale.

Gender

- Male
- Female

Race

- Malays
- Chinese
- India

3.5.2 Ordinal Scale

An ordinal scale is a variable measurement scale that is used to simply represent the order of variables rather than the difference between each of the variables. In other words, the order matter, but not the difference of variables. The ordinal scale is used to rank and order the categories, such as letter grades, rankings, and achievement. These categories can be ranked in the form of low, medium, and high (Sawamura et al., 2014). The following is part of the questionnaires that designed based on ordinal scale.

Age

- 18-27
- 28-37
- 38-47
- 48-57
- 58 and above

Monthly income

- RM1,000 and below
- RM1,001- RM2,500
- RM2,501- RM5,000
- RM5,001 and above

3.5.3 Interval Scale

The interval scale is a quantitative measurement scale in which order is known as well as the difference between the variables (Statistics Solutions, 2021). It contains the properties of a nominal and ordinal scale. The distances between the intervals on the scale are equivalent along the scale from low to high. For example, 1 to 5 points are used, in which “1” represent strongly disagree, “2” represent disagree, “3” represent neutral, “4” represent agree, and “5” represent strongly agree.

3.6 Data Processing

Data processing is conducted by researchers to guarantee the accuracy and completeness of the survey. The following steps are questionnaire checking, data editing, and data coding. It is crucial for analyzing the survey results and then being translated into usable information (Duggal, 2023).

3.6.1 Data Checking

First, the researchers check the questions to make sure there are no grammatical errors, misunderstandings, or missing details. They will filter out the respondents that is not eligible for further analysis. This is because the overall research objective would be significantly impacted by the questionnaire assessment. The quality of the research will be ensured if the researchers find issues and fix the questionnaire before giving it to the respondents (Wong et al., 2017).

3.6.2 Data Editing

Finding and fixing data inaccuracies in a questionnaire is a process known as data editing. All gathered data should be modified before being presented as usable information to ensure that the data is consistent, accurate, and comprehensive. This is so that the response would not be deceptive if it's inaccurate. As a result, data modification will be a successful method to prevent the repeating of surveys as the issues that happened are addressed.

3.6.3 Data Coding

The process of converting gathered data or observations into a collection of useful, meaningful categories is referred to as data coding. It is the process of representing facts to offer a systematic explanation of the phenomenon that has been recorded or seen (Allen, 2017). Plus, the data will be organized and refined to draw conclusions about the phenomenon. At the same time, the goal of data coding is to bring out the accurate meaning of the data that the respondents have provided (“Data coding in research methodology”, 2014). Data coding will be applied in Section B, where a numerical code will be given to the respondent’s answer.

Section B
Strongly Disagree for “1”
Disagree for “2”
Neutral for “3”
Agree for “4”
Strongly Agree for “5”

3.6.4 Data Transcription

Data transcription refers to converting the survey data into written text for analysis purposes (Shien, 2022). For example, in this research, the researchers records the data received from questionnaires into an Excel file. Then, the Excel data will be exported into Partial least squares structural equation modelling (PLS-SEM) for further analysis.

3.7 Data Analysis Tool

According to Bhat (2019), data is described and processed through the use of statistical techniques. It can be supported with images, tables, and graphs. Also, statistical trends and probability data are analyzed, and meaningful conclusions can be drawn. Hence, the gathered data will be analyzed using PLS-SEM software.

3.7.1 Descriptive Analysis

The process of using statistical techniques to summarise or describe a set of data is known as descriptive analysis (Bush, 2020). Researchers that use descriptive analysis can quickly describe the presented data. Descriptive analysis is used to assist researchers in condensing the vast amount of data into a manageable form (Bhandari, 2020). Certainly, frequency and

percentage will be used to describe all demographic data to illustrate their precise amount. To show the frequency or percentage of categories or values for a single item, a pie chart will be utilized (Sekaran & Bougie, 2016). Section A gathers the respondents' demographic information, including gender, age, race, educational background. Descriptive analysis will be used to analyze this section. In Chapter 4, the findings will be further examined with graphs and table examples.

3.7.2 Partial Least Square Structural Equation Modelling (PLS-SEM)

Structural Equation Modelling (SEM) is a model that combines latent variables with structural relationships, while Partial Least Square Structural Equation Modelling (PLS-SEM) is a multivariate analytic approach for evaluating complex causal models (Cepeda-Carrion et al., 2018). Based on Zeng et al. (2021), PLS-SEM is an alternative to covariance-based structural equation modelling (CB-SEM). Compared with CB-SEM, PLS-SEM can be used in exploratory studies of small sample sizes and formative measures. According to Kante et al. (2018), the correct sample size required to use PLS-SEM is 200 or more. PLS-SEM is a method based on causal prediction relationships, which maximizes the number of variances explained by dependent variables, so the estimated complex always relies on a legal-rational network. In the early stages of theoretical development, PLS-SEM is more suitable for exploring and developing theories, while CB-SEM is usually associated with theoretical confirmation. Therefore, PLS-SEM should be selected as the most effective structural modelling method when prediction is the focus of research (Hair et al., 2020).

3.7.3 Internal Consistency Reliability

Internal consistency reliability is a method to describe the test's reliability, including data reliability, by analysing the connection between each variable within the test. (Hajjar, 2018). According to Jain and Chetty (2021), internal consistency is often measured using the Cronbach α coefficient as known as Cronbach's Alpha (CA), especially when using the Likert scale, which is the most commonly used consistency measure. In addition to the CA, another method for calculating internal consistency is called composite reliability (CR).

3.7.3.1 Cronbach's Alpha (CA)

Cronbach's alpha (CA) is a measure of the reliability or internal consistency of a test or scale item. It is used to measure the strength of agreement for a given measure. In the measurement, the α coefficient of reliability ranges from 0 to 1. Higher coefficients indicate common covariance between items. Cronbach's alpha coefficient minimum of 0.65 to 0.8 or higher is recommended. For single-dimensional scales, coefficients less than 0.5 are generally unacceptable. However, a high alpha coefficient is not necessarily an indicator of good quality or reliability of the item set, as it may be increased by adding items, and a very high coefficient may indicate redundancy of scale items. Moreover, Cronbach's alpha is not a measure of dimension or validity, but rather of reliability. Therefore, a high alpha coefficient does not necessarily indicate one dimension or validity and may require additional analysis (Goforth, 2015).

Table 3.1

Rule of Thumb for Cronbach's Alpha

Cronbach's Alpha	Internal Consistency
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	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: Sharma, B. (2016). A focus on reliability in developmental research through Cronbach's Alpha among medical, dental and paramedical professionals. *Asian Pacific Journal of Health Sciences*, 3(4), 271-278.

3.7.3.2 Composite reliability (CR)

Composite reliability (CR) measures the effect of variables in structural equation models (SEM). It is based on the factor load in confirmatory factor analysis (CFA) and is particularly suitable for single-dimensional scales. It avoids some inappropriate assumptions relative to other methods, such as Cronbach's alpha (Wiryanto, 2018). Similar to other internal consistency indicators, higher composite reliability score indicates better internal consistency. Based on Jain & Chetty (2021), the CR allows the construction reliability coefficient greater than 0.70. To achieve structural reliability, CR values must be greater than or equal to 0.7 (Tentama & Anindita, 2020).

3.7.4 Construct Validity

Karakaya-Ozyer and Aksu-Dunya (2018) claims that validity is defined as the accuracy of test results and validity measures the coverage of actual information in a research tool or data set. Therefore, it is important for researchers to establish validity. In SEM analysis, evidence of validity can help researchers accurately interpret results (Jain & Chetty, 2021). Construct validity is one of the four measurement validity of test validity, referring to the concept of how the test measures what it is designed to evaluate. Convergent validity and discriminant validity are the two seed types of construct validity. Furthermore, correlation and regression analyses are often used to test the effectiveness of measures. Correlation is used to

test convergence validity and discriminant validity, while regression analysis is used to assess whether a measure predicts the expected outcome. If the results of regression analysis support theoretical expectations, the claim of construct validity can be strengthened (Nikolopoulou, 2022).

3.7.4.1 Discriminant Validity

Discriminant validity test is needed when constructing latent variable tools. It is also known as divergent validity, is used to prove the validity of the difference between one construct and another (Taherdoost, 2016). According to Nikolopoulou (2022), discriminant validity is a construct validity that assesses whether an otherwise unrelated construct is actually unrelated. High discriminant validity means that the test is accurate for structures of interest and does not evaluate unexpected structures. The operational accuracy of transforming abstract concepts into measurable variables or observed values is very important for discriminant validity. Three ways can be used for measuring the discriminant validity under PLS-SEM software, which are Fornell-Larker Criterion, Heterotrait-Monotrait Ratio (HTMT), and cross-loading. There are some assumptions that need to be followed in order to satisfy discriminant validity. Discriminant validity exists if the correlation coefficient between the two constructs is less than the square root of the average variance extracted (AVE) value (Engellant et al., 2016). Also, the indicator should has a higher cross-loading on its respective construct than on other constructs. Other than that, HTMT ratio should be lower than 0.85 or 0.9 to ensure discriminant validity (Henseler, 2015).

3.7.5 Evaluation of Inner Model

According to “Introduction to SEM-PLS” (n.d.), the inner model is composed of structural equation modeling based on partial least squares

(SEM-PLS). The inner model identifies the relationships between potential variables and establishes relationships through multiple regression models between an independent potential variable and other potential variables.

In this research, path coefficient are used to measure the strength and significance of the relationships between variables in the model. If the path coefficient is statistically significance, it means that there is a causal relationship between the dependent variable and independent variables. Also, bootstrapping is used to measure the accuracy of path coefficient, checking the significance of the path coefficient. The significance of path coefficient can be seen in the t test that obtained from bootstrapping process. If the t value more than 1.96, the null hypotheses are rejected, and vice versa (Purwanto & Sudargini, 2021). Based on Urbach and Ahlemann (2010), R square is used to measure the proportion of the variance of the dependent variable that can be explained by the independent variable. Generally, a value of about 0.670 of R square is considered substantial, about 0.333 is average, and a value less than 0.190 is considered weak.

3.8 Conclusion

To conclude, this chapter has provided insight to the research's approach. Descriptive research applied to gather data for analysis. Techniques for gathering data, sample design, research measurement, and ways to process and analyze the information also included. The outcomes will be explained and analyzed further in Chapter four.

CHAPTER 4: DATA ANALYSIS

4.0 Introduction

Chapter four focusing on analyzing and interpreting information collected from the 384 survey questionnaires. Descriptive analysis was conducted to analyze the demographic information of the respondents. In this research, Smart PLS 4.0 was used to verify the validity of the hypotheses that previously mentioned in Chapter 2.

4.1 Participation Rate

This research circulated 450 sets of questionnaires, and has collected 400 responses. However, only 384 responses are eligible for further analysis, 16 responses are excluded as they do not fulfill the requirement of the research. Hence, in this research, the total percentage of participation rate will be 88.90%.

4.2 Descriptive Analysis

Descriptive analysis is used to analyze the demographic profile of the respondents in a precise way, including the age, gender, ethnicity, monthly income, education level, and so on. Pie charts and tables will be provided for a clearer understanding and presentation of the data.

4.2.1 Respondents' Demographic Profile

The demographic profile of each respondent is presented in Section A of the questionnaire. The research has successfully gathered 384 eligible participants from various locations in Malaysia.

4.2.1.1 Gender

Table 4.1

Gender

Gender	Number	Percentage (%)
Male	172	44.8
Female	212	55.2

Figure 4.1 *Gender*

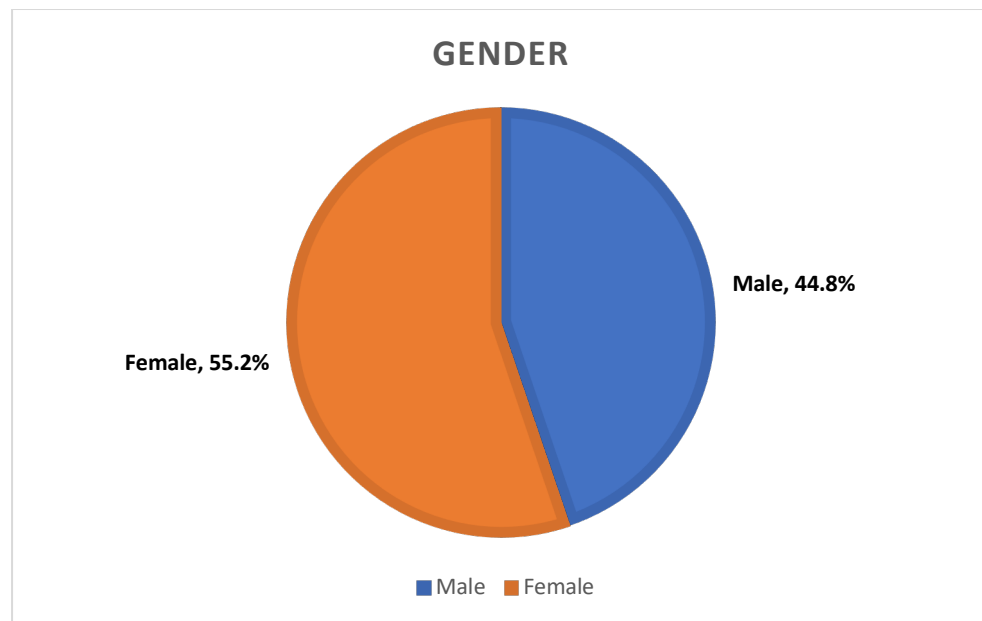


Figure 4.1 shows the gender distribution of the survey respondents. There were 384 respondents in all, with 172 of them being male and 212 being female. It means that females made up a slightly higher percentage (55.2%) of the respondents compared to males (44.8%).

4.2.1.2 Age

Table 4.2

Age

Age	Number	Percentage (%)
18-27	293	76.3
28-37	49	12.8
38-47	24	6.3
48-57	17	4.4

Figure 4.2

Age

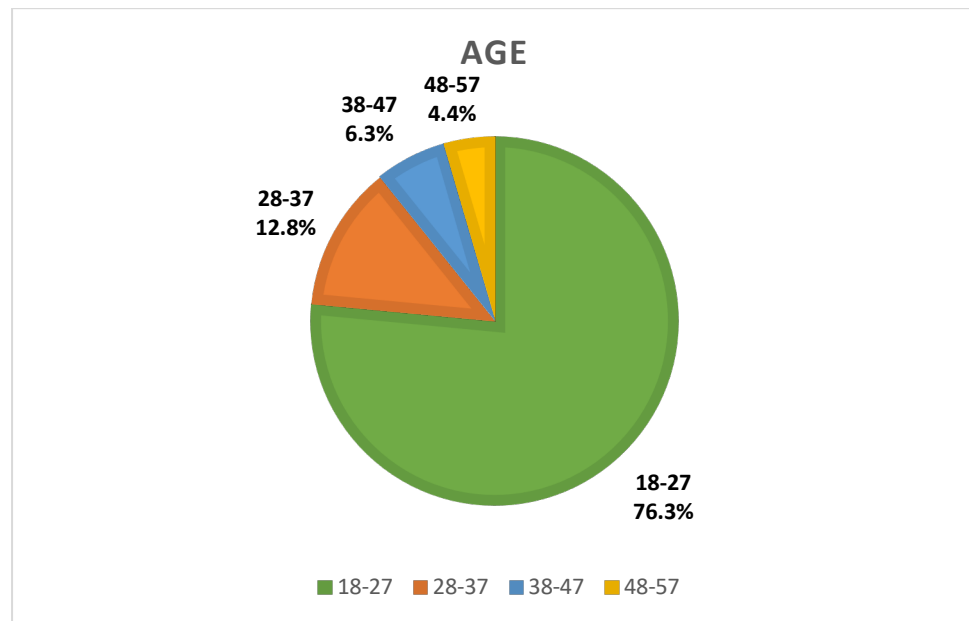


Figure 4.2 presents the distribution of age groups among the respondents, where the age groups are categorized into four intervals. The first age group is 18-27, which represents 293 respondents or 76.3% of the total sample. The second age group is 28-37, which represents 49 respondents or 12.8% of the total sample. The third age group is 38-47, which represents 24 respondents or 6.3% of the total sample. The fourth age group is 48-57, which represents 17 respondents or 4.4% of the total sample.

4.2.1.3 Ethnicity

Table 4.3

Ethnicity

Ethnicity	Number	Percentage (%)
Malay	39	10.2
Chinese	311	81
India	33	8.6

Figure 4.3

Ethnicity

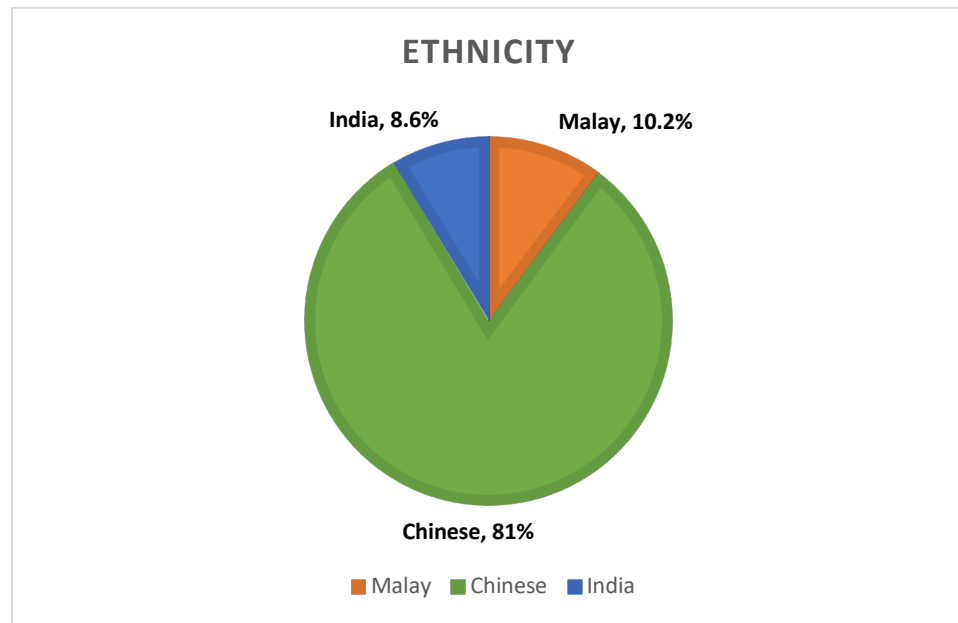


Figure 4.3 displays the race of respondents. According to the pie chart, the greatest number of respondents are Chinese with 311 people accounting for 81%. Lastly, the numbers of Malay and Indian respondents were not significantly different with each other, which accounting for 39 people (10.2%) and 33 people (8.6%).

4.2.1.4 Education Level

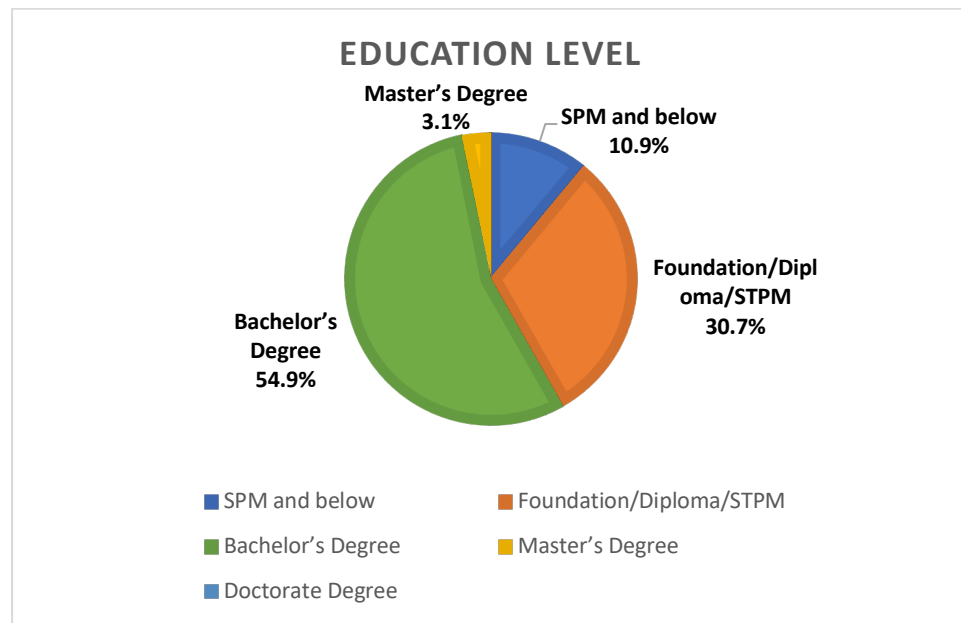
Table 4.4

Education Level

Education Level	Number	Percentage (%)
SPM and below	42	10.9
Foundation/Diploma/STPM	118	30.7

Bachelor’s Degree	211	54.9
Master’s Degree	12	3.1
Doctorate Degree	0	0

Figure 4.4
Education Level



According to Figure 4.4, the highest percentage of respondents, which accounts for 211 respondents with 54.9%, attained a Bachelor’s Degree level of education. The second highest education level achieved by 118 respondents was a Foundation/Diploma/STPM, with a percentage of 30.7%. In contrast, the number of respondents who achieved an SPM and below the level of education and Master’s Degree was relatively low, with only 42 and 12 respondents, respectively. Likewise, there was no respondents (0%) who attained a Doctorate Degree level of education.

4.2.1.5 Monthly Income

Table 4.5
Monthly Income

Monthly Income	Number	Percentage (%)
RM1,000 and below	159	41.4

RM1,001- RM2,500	127	33.1
RM2,501- RM5,000	75	19.5
RM5,001 and above	23	6

Figure 4.5
Monthly Income

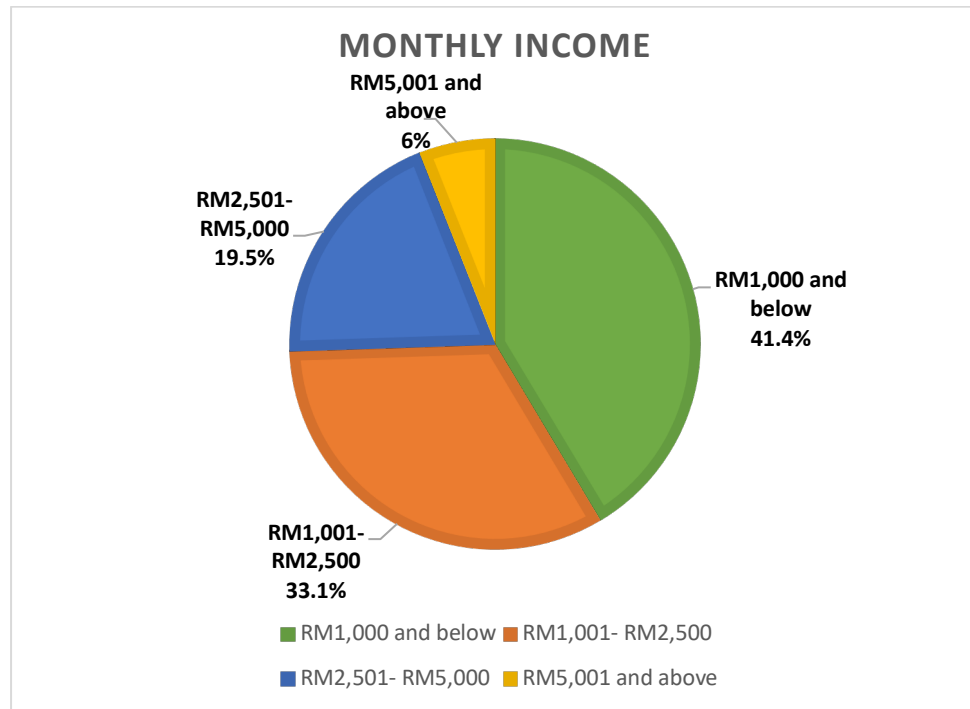


Figure 4.5 illustrates the respondents’ monthly income. Majority of participants earned between RM1,000 and below, accounting for 41.4%. Following this, 127 respondents (33.1%) earned RM1,001- RM2,500. There were 75 respondents (19.5%) reported having an income between RM2,501- RM5,000. Lastly, 23 respondents (6%) reported having an income of RM5,001 or more. In short, more than half of the respondents collected an income of less than RM5,000.

4.2.1.6 Types of E-wallet Accounts

Table 4.6
Types of E-wallet Accounts

Types of E-wallet accounts	Number	Percentage (%)
Touch 'n Go (TNG)	369	96.1
Boost	125	32.6
GrabPay	192	50
ShopeePay	161	41.9
MAE (Maybank)	125	32.6

Figure 4.6
Types of E-wallet Accounts

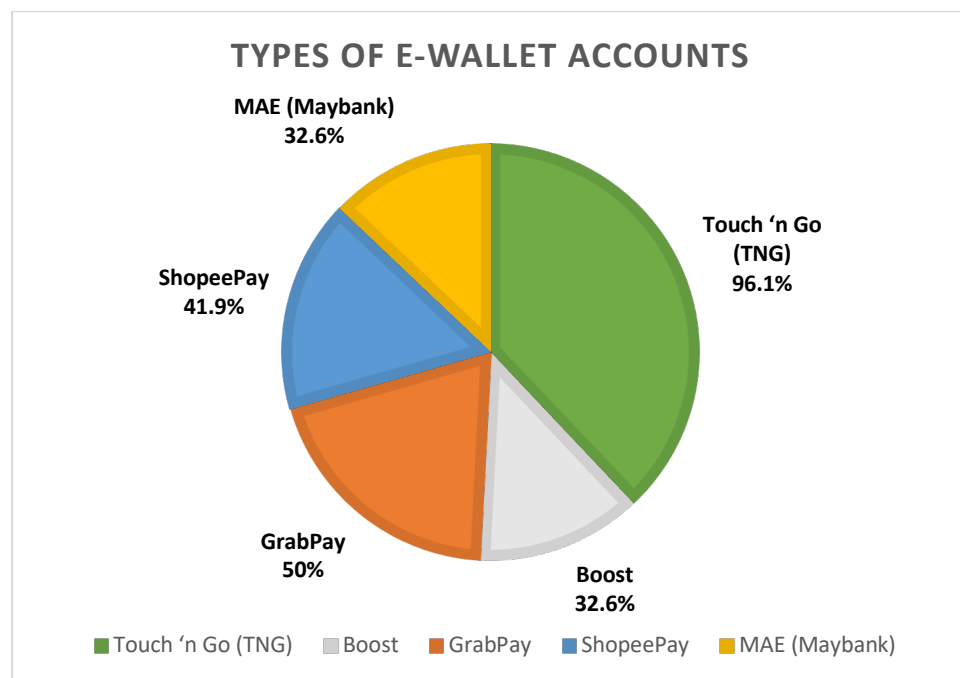


Figure 4.6 shows the types of E-wallet accounts that respondents used while conducting online financial transactions. According to the results obtained, the majority of respondents used Touch 'n Go (TNG), which recorded for 369 respondents with 96.1%. Following this, there were 192 respondents (50%) used GrabPay. In addition, there were 161 respondents used ShopeePay with 41.9%. Last but not least, the percentage of the respondents that used Boost and MAE (Maybank) was the same, which recorded for 125 respondents with 32.6%.

4.2.1.7 Types of Online Banking Accounts

Table 4.7
Account Types of Online Banking

Account Types	Number	Percentage (%)
Public Bank	293	76.3
Maybank	197	51.3
RHB Bank	89	23.2
Hong Leong Bank	75	19.5
UOB Malaysia	38	9.9
CIMB Bank	75	19.5

Figure 4.7
Account Types of Online Banking

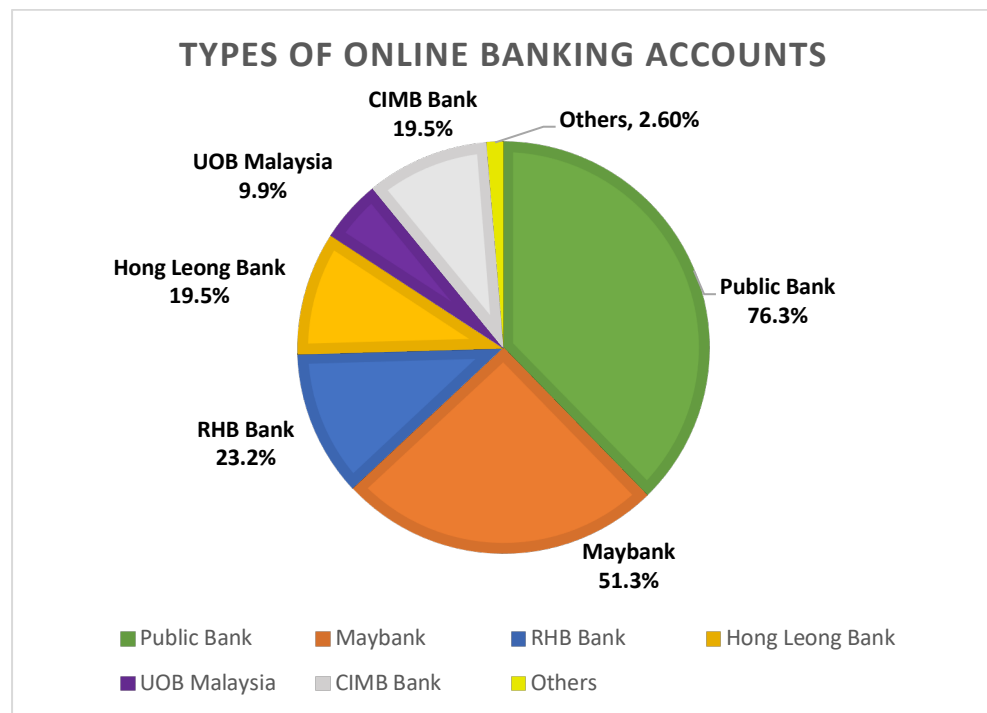


Figure 4.7 shows the types of online banking accounts that the respondents used while conducting online financial transactions. According to the data obtained, the majority of respondents used Public Bank, accounting for 293 respondents with 76.3%. Following this, there were 197 respondents reported using Maybank, which recorded 51.3%. In addition, the RHB Bank users were recorded as 23.2%, which accounting for 89 respondents. Following this, the percentage of the respondents that used Hong Leong

Bank and CIMB Bank were the same, which had 75 people accounting for 19.5%. Lastly, there was the least number of respondents that used UOB Malaysia, which accounted for 38 respondents with 9.9%.

At the same time, there were 2.6% of respondents had chosen “Others”, meanings that they used other online financial accounts which were not shown as an option in the questionnaire. There were 2 respondents (0.5%) who used Ambank. Furthermore, there were 0.3% of respondents chose BSN Bank, HSBC Bank, OCBC Bank, Muamalat Bank, and Bank Rakyat as their online banking accounts that they used, respectively.

4.3 Measurement and Structural Model

This research used PLS-SEM approach to analyze each independent variable and the association amongst themselves. In following section, the results obtained from Smart PLS-SEM 4.0 will be further discussed by using figures and tables.

4.3.1 Factor Loadings

Table 4.8

Factor Loadings

	DV	CK	PS	SN	SP
DV1	0.788				
DV2	0.784				
DV3	0.775				
DV4	0.718				
DV5	0.660				
CK1		0.801			
CK2		0.795			
CK3		0.708			
CK4		0.831			

CK5	0.812	
PS1		0.824
PS2		0.814
PS3		0.718
PS4		0.783
SN1		0.780
SN2		0.845
SN3		0.772
SN4		0.847
SP1		0.712
SP2		0.772
SP3		0.757
SP4		0.756
SP5		0.723
SP6		0.693

Source: For the research purpose

Factor loadings acts as a measure to assess the validity of a construct. It represents the degree to which each variable is related to a particular factor. Therefore, by looking at the factor loading, researchers can understand which variables have the highest correlation with a specific factor (“What are factor loadings?”, 2023). Based on “Factor Analysis” (n.d.), in structural equation modeling (SEM) methods, a factor loading of 0.7 or higher is generally considered to indicate that the factor effectively captures the variability in the corresponding variable. Table 4.8 shows that all indicators are related to their underlying construct, except DV5 and SP6, which have a factor loading of less than 0.7, i.e., 0.660 and 0.693. However, a factor loading of 0.6 is still within the acceptable range.

4.3.2 Internal Consistency Reliability

4.3.2.1 Cronbach’s Alpha (CA), Composite Reliability (CR), Average Variance Extracted (AVE)

Table 4.9

Table of Cronbach’s Alpha, Composite Reliability and Average Variance Extracted

	CA	CR	AVE
Awareness (DV)	0.801	0.810	0.558
Cybersecurity Knowledge (CK)	0.850	0.859	0.625
Perceived Severity (PS)	0.793	0.803	0.618
Subjective Norm (SN)	0.829	0.842	0.659
Security and Privacy Concern (SP)	0.834	0.848	0.542

As previously mentioned in Chapter 3, Cronbach’s Alpha (CA) is an important indicator to assess reliability and internal consistency of the scale item. Based on table 4.9, the results showed that all variables have a Cronbach’s Alpha value of more than 0.7, showing a good internal consistency and high reliability. The variables of awareness, cybersecurity knowledge, subjective norm as well as security and privacy concern have a higher value of CA, which are 0.801, 0.850, 0.829, and 0.834 respectively. As for perceived severity, the value falls between 0.8-0.7, which is 0.793, slightly lower among other variables; however, it is still considered as an acceptable level.

Composite Reliability (CR) acts as another metric in examining internal consistency and reliability. It offers greater reliability than Cronbach’s Alpha in the case that it takes into account the measurement errors or inappropriate assumptions that made by CA. Among the variables, the CR for cybersecurity knowledge is highest, accounting to 0.859, followed by security and privacy concern, subjective norm, awareness of online financial scam, and perceived severity. The CR are 0.848, 0.842, 0.810, and 0.803 respectively. The results show that all variables are highly reliable as they

have a CR value of more than 0.8 and internal consistency is achieved in this research.

Average Variance Extracted (AVE) was applied to evaluate the convergent validity of a factor, showing to what extent the constructs in the model can explain the variance in the dependent variable. A common thumb of rule for AVE is 0.5 or greater than 0.5. A higher AVE means greater proportion of the variation could be explained. In this case, all variables have an AVE value of more than 0.5, with subjective norm having highest AVE at 0.659, accompanied by cybersecurity knowledge (0.625), and perceived severity (0.618), awareness (0.558), security and privacy concern (0.542).

4.3.3 Discriminant Validity

Discriminant validity acts as an important marker to check if variables are highly correlated with each other. This will assist researchers in making accurate interpretation of results.

4.3.3.1 Fornell-Lacker Criterion

Table 4.10

Fornell-Lacker Criterion

	DV	CK	PS	SN	SP
DV	0.747				
CK	0.547	0.790			
PS	0.583	0.474	0.786		
SN	0.590	0.451	0.709	0.812	
SP	0.487	0.528	0.691	0.564	0.736

Other than Heterotrait Monotrait Ratio (HTMT), Fornell-Lacker Criterion is another method to assess the discriminant validity of latent constructs. It tests to what extend the indicator of one variable are strongly related to their

own variable than to others by comparing the square root of AVE of each variable with the correlations between variables (Hamid et al., 2017). Therefore, own variable's square root of AVE needs to be higher in comparison to other variables. Based on the Table 4.10, the square root of AVE each variable is higher as compared to the correlation between other variables. The values are 0.747, 0.790, 0.786, 0.812, and 0.736 respectively. It can be concluded that discriminant validity is achieved in this research.

4.3.3.2 Heterotrait Monotrait Ratio (HTMT)

Table 4.11

HTMT

	DV	CK	PS	SN	SP
DV					
CK	0.646				
PS	0.723	0.574			
SN	0.712	0.529	0.869		
SP	0.569	0.619	0.829	0.658	

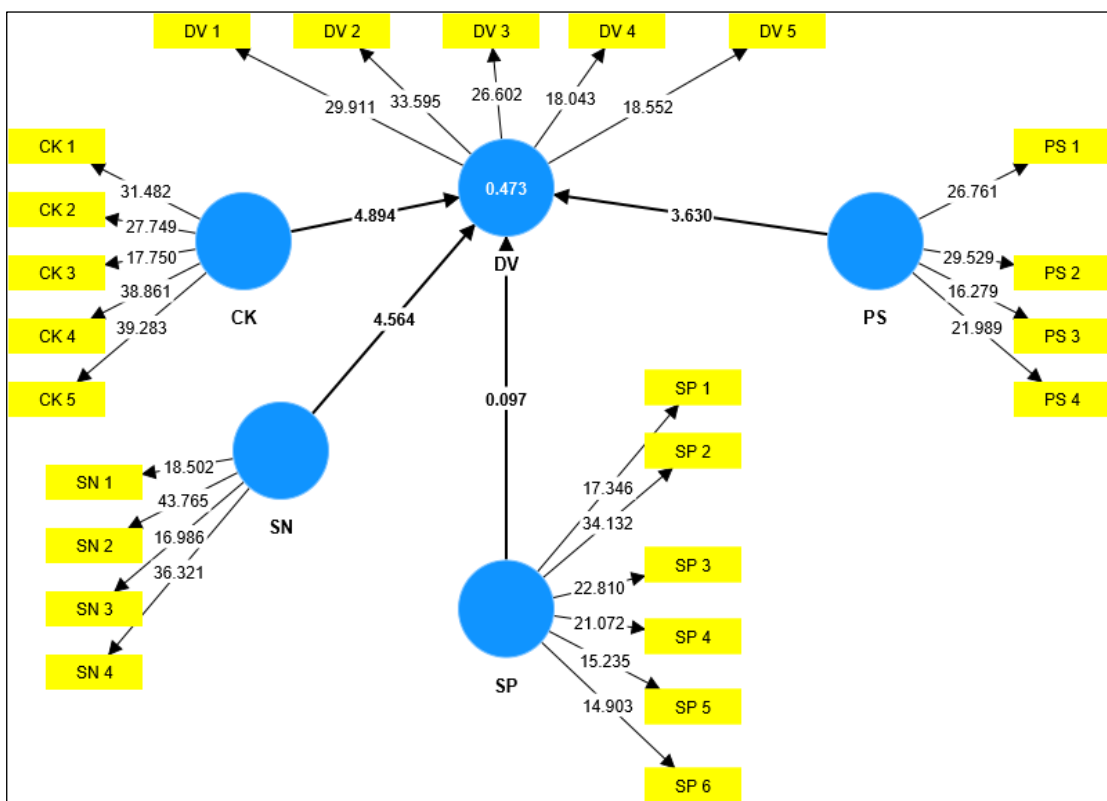
Heterotrait-monotrait ratio of correlations (HTMT) is a new method to evaluate the discriminative validity of variance-based SEM. It is used as a test tool to measure the weakening degree of structural correlation. According to Henseler et al. (2015), HTMT compares the correlations of indicators across constructs with the correlations among indicators within the same constructs. HTMT ratio will be compared to a predefined threshold for use as a standard. If the HTMT ratio exceeds this threshold, it indicates a lack of discriminative validity. The exact threshold level for HTMT is subjective and controversial. Some researchers believe that the threshold should be 0.85 (Clark and Watson 1995; Kline 2011). HTMT 0.85 with higher or equal sensitivity than HTMT 0.90. Despite the lower standard threshold, HTMT 0.85 is still the most conservative standard because it has the lowest specificity across all simulated conditions. Therefore, assuming

that the results of this study are compared with the predefined threshold of 0.85, in the HTMT ratio of each latent variable pair given in Table 4.11, the HTMT ratio of all construction pairs is less than 0.85, except for the SN-PS construction pair, which has an HTMT ratio of 0.869.

4.3.4 Path Coefficient (Bootstrapping)

Figure 4.8

Structural Model (Bootstrapping)



Source: For the research purpose

Figure 4.8 shows inner model analysis concerning the association among the independent and dependent variables. The t-values for perceived severity (PS), subjective norms (SN), and cybersecurity knowledge (CK) are all greater than 1.96 which means that there is sufficient evidence to reject the null hypothesis of no relationship between these independent variables and dependent variable (DV) which is Malaysians' awareness on online financial scams. However, the t-value for security and privacy

concerns (SP) is less than 1.96 which means that there is not sufficient evidence to reject the null hypothesis of no relationship between these independent variables and Malaysians' awareness on online financial scams. Thus, the table suggests that there are significant relationships between DV and PS, SN, and CK, but not with SP.

Table 4.12
Path Coefficient

	Original Sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDE V)	P values	Result
CK -> DV	0.306	0.305	0.063	4.894	0.000(***)	Supported
PS -> DV	0.234	0.235	0.064	3.630	0.000(***)	Supported
SN -> DV	0.284	0.283	0.062	4.564	0.000(***)	Supported
SP -> DV	0.004	0.010	0.045	0.097	0.923 (ns)	Unsupported

Source: For research purpose

Note: Significance level is 5%, p-value below 5% or 0.05 is deemed significant (***), more than 5% or 0.05 considered as insignificant (ns)

A threshold called the significance level (also known as the alpha level) is chosen when statistical tests are performed. This threshold determines the probability of rejecting the null hypothesis if it is true. When conducting a research, the p-value is a calculated value used to determine whether the result has reached the level of significance (McNeese, 2017). Based on Wasserstein & Lazar (2016) and Bonovas & Piovani (2023), p-value provides a way to summarize inconsistencies between a particular set of data and its proposed model. Typically, this model is constructed under a set of assumptions and is called the "null hypothesis". The null hypothesis would

assume that the proportions are the same, while the alternative hypothesis would suggest that there is a difference in the proportions between the two groups. If the underlying assumptions on which the researchers are based are true, then the smaller calculated p-value indicates a higher level of statistical incompatibility between the data and the null hypothesis. In general, when the p-value is less than the significance level of 0.05, the researchers will reject the null hypothesis and indicate statistically significant outcome.

Table 4.12 presents the path coefficient on Malaysians' awareness on online financial scams. The outcomes reveal a substantial and statistically significant relationship between **cybersecurity knowledge (CK)** and Malaysians' awareness on online financial scams (DV), as evidenced by a path coefficient of 0.306 and a p-value of 0.000. Regarding this result, several studies by Das and Patel (2017) and Purkait, Kumar and Suar (2014) have shown a significant relationship between CK and DV. In addition, Verkijika (2019), Inan et al., (2016) and Asher & Gonzalez (2015) have also proven that CK and DV has positive association, which more knowledgeable people are about cybersecurity, the more aware they are of the threat of online financial scams.

Furthermore, for the **perceived severity (PS)**, its path coefficient is 0.234 and p-value is 0.000, indicating a significant relationship between PS and DV. According to several studies carried out by Liang and Xue (2009), Tsai et al. (2016), Crossler & Belanger (2014) and Thompson et al., (2017) indicated PS is positively related to DV.. Their studies found an association between high perceived severity and increased vigilance and proactive behaviour, as it affects an individual's assessment and level of awareness of threats, thereby helping to protect against potential threats.

Similarly, based on the statistical significance analysis of the relationship between **subjective norm (SN)** and DV, the research reveals a strong correlation with a path coefficient of 0.284 and a p-value of 0.000. This indicates a highly significant relationship between SN and DV with a

confidence level of 95%. These results align with previous studies by Johnson (2017), Fishbein & Ajzen (1980), Glanz et al. (1992), and Alanazi et al. (2022), which underscored the role of subjective norms in influencing individual behavior, particularly in cybersecurity practices. Additionally, these studies shed light on the growing awareness of cybersecurity risks among young individuals.

Conversely, for **security and privacy concerns (SP)**, the p-value is found to be higher than 0.05, specifically 0.923, indicating that there is no significant relationship between SP and Malaysians' awareness on online financial scams (DV). There are some scholars who believe that SP have no significant impact on DV. For example, Alhassany & Faisal (2018), Dinev et al. (2008), Govani and Pashley (2005), and Chen et al. (2017) argue that there being concerned of Internet privacy issues does not necessarily translate into taking protective measures to avoid it. For example, people may think that they have taken sufficient measures, but in fact, they have underestimated the risk of falling into the trap.

4.4 Conclusion

In conclusion, all results shown in this chapter are generated from Smart PLS 4.0. The data gathered through questionnaires were utilized for demographic information analysis, reliability testing, discriminant validity, and bootstrapping. Pie charts and tables are provided to present the data in a clearer manner. Next chapter will explore research's implication, limitations, and recommendations in detail.

CHAPTER 5: DISCUSSION, CONCLUSION AND IMPLICATIONS

5.0 Introduction

Chapter five primarily centers on the consolidation of outcomes derived from the preceding chapters and provides explanation based on the findings. Also, implication of the research, limitations and recommendations are included as a reference for prospective scholars.

5.1 Discussions of Major Findings

Table 5.1

Overview of Statistical Analysis

Test	Research Question (RQ) / Research Objective (RO)	Hypothesis	Hypothesis Decision	Results
Cybersecurity Knowledge	<p>RQ: Is there any significant relationship between cybersecurity knowledge and Malaysians' awareness on online financial scams?</p> <p>RO: To evaluate the relationship between cybersecurity knowledge and</p>	<p>H₀: There is no significant relationship between cybersecurity knowledge and Malaysians' awareness on online financial scams.</p> <p>H₁: There is a significant relationship between cybersecurity</p>	<p>Decision rule: Reject H₀ if p-value is smaller than 0.05. Otherwise, do not reject H₀.</p> <p>Decision making: Reject H₀ since p-value is smaller than 0.05.</p>	Significant (P-value = 0.000)

	Malaysians' awareness on online financial scams.	knowledge and Malaysians' awareness on online financial scams.		
Perceived Severity	<p>RQ: Is there any significant relationship between perceived severity and Malaysians' awareness on online financial scams?</p> <p>RO: To evaluate the relationship between perceived severity and Malaysians' awareness on online financial scams.</p>	<p>H₀: There is no significant relationship between perceived severity and Malaysians' awareness on online financial scams.</p> <p>H₁: There is a significant relationship between perceived severity and Malaysians' awareness on online financial scams.</p>	<p>Decision rule: Reject H₀ if p-value is smaller than 0.05. Otherwise, do not reject H₀.</p> <p>Decision making: Reject H₀ since p-value is smaller than 0.05.</p>	Significant (P-value = 0.000)
Subjective Norms	<p>RQ: Is there any significant relationship between subjective norms and Malaysians' awareness on online financial scams?</p> <p>RO: To evaluate the relationship between subjective norms and Malaysians' awareness on</p>	<p>H₀: There is no significant relationship between subjective norms and Malaysians' awareness on online financial scams.</p> <p>H₁: There is a significant relationship between subjective norms and Malaysians' awareness on</p>	<p>Decision rule: Reject H₀ if p-value is smaller than 0.05. Otherwise, do not reject H₀.</p> <p>Decision making: Reject H₀ since p-value is smaller than 0.05.</p>	Significant (P-value = 0.000)

	online financial scams.	online financial scams.		
Security and Privacy Concern	<p>RQ: Is there any significant relationship between security and privacy concern and Malaysians' awareness on online financial scams?</p> <p>RO: To evaluate the relationship between security and privacy concern and Malaysians' awareness on online financial scams.</p>	<p>H₀: There is no significant relationship between security and privacy concern and Malaysians' awareness on online financial scams.</p> <p>H₁: There is a significant relationship between security and privacy concern and Malaysians' awareness on online financial scams.</p>	<p>Decision rule: Reject H₀ if p-value is smaller than 0.05. Otherwise, do not reject H₀.</p> <p>Decision making: Do not reject H₀ since p-value is larger than 0.05.</p>	Insignificant (P-value = 0.923)

Source: For the research purposes

5.1.1 Cybersecurity Knowledge

Cybersecurity knowledge includes practical knowledge to avoid cyber-attacks, as well as personal awareness of information security and preventive measures to protect personal information against theft. In this research, the finding indicated a strong and significant relationship between cybersecurity knowledge and Malaysians' awareness on online financial scams. This finding finds additional support from Ekong (2023), Limna, & Siripipattanakul (2023), as well as Aliebrahimi & Miller (2023). When faced with the risk of cyber victimization, the findings of Lee and Chua (2023) point out that emphasis must be placed on the role of cybersecurity knowledge, especially for those

who frequently use smartphones to access the Internet, in protecting themselves from uncertainty. Besides, this research finding is consistent with Goutam's (2015) assertion that by properly understanding online behaviour and system protection, internet users can reduce the risk of vulnerabilities, enhance the security of the online environment, as well as reduce the financial losses and reputational damage if they strengthen security awareness and adopt appropriate strategies.

5.1.2 Perceived Severity

Perceived severity is an individual's belief about the severity of being affected by a particular security issue and is a judgment made when faced with a threat of potentially causing serious harm at work or in any environment with an Internet connection. In addition, the perceived severity will directly affect the level of threat perception of individuals, and then affect their response and prevention behaviour on security issues. This research indicates a positive and significant correlation between perceived severity and Malaysians' awareness of online financial scams. This correlation is supported by the technology threat avoidance theory (TTAT) and previous studies like Boehmer et al. (2015), Herath & Rao (2009), and Liang and Xue (2009). When users clearly understand the seriousness of vulnerabilities and potential threats in the network, this clarity can motivate them to change their behaviour. For example, through the perception of vulnerability and severity, users can have a deeper understanding of the importance of the network security behaviour they take to resist network threats, thereby improving network security awareness and defence capabilities (Sulaiman, 2022).

5.1.3 Subjective Norms

According to the Theory of Planned Behaviour (TPB), when individuals form beliefs about certain behaviours expected of influential people in their lives,

this is called subjective norms. In this research, the finding shows a clear and statistically association between subjective norms and Malaysians' recognition concerning online financial scams. This finding aligns with prior research by Alanazi et al. (2022) which claimed that subjective norms have a positive impact on the intention of young individuals regarding network security behavior. Research by Kaushik et al. (2018) and Li (2011) further supports the findings of this research. Both of these past studies indicate that subjective norms have significant impact on general and website-specific privacy perceptions and on users' willingness to share information online. When individuals have a stronger sense of social norms about a particular behaviour, their agreement between intent and actual action is also more significant (Ajzen, 2020). Furthermore, with the continuous development of technology, it is known that online scams methods are also constantly changing and evolving. Schepers & Wetzels (2007) reported that subjective norms exert a notable influence on the behavioral willingness to adopt new technologies. That is to say, when new financial fraud technologies appear on the network and the public begins to use them under the influence of society, the public will be more likely to fall into more online financial scams' traps.

5.1.4 Security and Privacy Concern

Security and privacy concerns encompass a range of concerns that primarily revolve around safeguarding personal privacy from misuse, preventing unauthorized access to sensitive information and systems, and addressing the potential risks associated with data breaches and malicious attacks. In this research, the results indicate security and privacy concerns are positively related to Malaysians' awareness of online financial scams, but this relationship was statistically insignificant. This result aligns with previous investigations carried out by Sikdar & Makkad (2015), Alhassany & Faisal (2018), Dinev et al. (2008), Govani and Pashley (2005), and Chen et al. (2017). Additionally, based on research by Xu et al. (2011), it has been shown that the public is willing to trade off personal privacy to a certain extent in exchange for enticing

incentives, such as access to desirable products, valuable coupons, premium services, or economic benefits. In fact, the research also revealed that some individuals have expressed their willingness to forgo privacy to enjoy the anticipated advantages of online personalization. Research findings by Phelps and colleagues (2000) further indicate that experiencing the advantages of shopping leads to a reduction in privacy concerns among consumers.

5.2 Implications of the Research

In this research, there are three independent variables among four independent variables, namely cybersecurity knowledge, perceived severity, and subjective norms show significant result to the awareness of online financial scam. It indicates that most of the Malaysians is still having a low level of scam awareness, especially when it comes to investments and financial matters. The results of this research provided a basis for Malaysians, including companies and policymakers to explore the ways to increase awareness on online financial scams.

Malaysia's younger generation tend to be more digital savvy as they have been exposed to the technologies since their earliest youth. Hence, it is essential for the younger generation to gain cybersecurity knowledge in order to protect themselves from falling into the trap and to reduce the risk of personal information being exposed by the scammers. On the other hand, the older generation in Malaysia are more susceptible to online financial scams. Even if the senior citizens avoid using digital devices, their lack of awareness to recognize the tactics of online financial scams, making them still vulnerable to becoming the victims. Therefore, this research enables Malaysians to learn about common tactics of online financial scams and improve their ability of detecting the financial scams, including the identification of suspicious messages or links that they received. For instance, they need to adopt some practices to ensure their online transactions is always remain secured, including complex password, face ID, and two-factor authentication. Besides, they will learn to be more cautious in sharing their personal information online, and always equip with the latest security measures from the news or

websites. Also, companies that understand the security needs and risk awareness of customers, and emphasize on the cybersecurity knowledge among the employees will gain the customers' trust. Scam education, training, and awareness campaign should be provided for the employees. Employees who have enough knowledge about cybersecurity will be able to detect suspicious transactions and safeguard the company's sensitive information, leading to customer loyalty and increase the reputation of the company.

The results of perceived severity shows that it is an important indicator to the awareness of online financial scams; hence, the policymakers should take the advantage of it by developing rules and regulations that can address the severity of online financial scams effectively. For instance, policymakers can develop a more robust customer protection legislation, such as provides clear instructions for the procedure of reporting scams, and clarify the compensation for the victims in order to ensure that the affected victims are able to receive immediate assistance. This will help the policymaker to respond quickly and prevent further harm to the affected parties. In addition to that, policymakers can conduct public awareness campaign that emphasize the severity of online financial scam, educating the public to be more alert when making an online transaction and not to provide sensitive data to unknown person, at the same time, allowing the public to understand that the impact is always severe financial loss and emotional distress. Other than awareness campaign, policymaker can use advertisement as a tool to promote scam prevention to the public. Moreover, policymaker may collaborate with financial institution to monitor the real-time transaction and further tighten online scam detection procedures to block suspicious scam transactions. They may also consider to develop a more stricter laws and regulations to penalise the criminals that involved in the scam activities as present penalties may not be sufficient to deter fraudulent activities and protect the public. Stricter laws or regulations serves as a warning for potential scammers, sending a message to scammers that their actions will not be tolerated and making them to think twice before proceeding, eventually, reduce the possibility of engaging in such criminal activities.

Furthermore, subjective norms also has impact on awareness on online financial scam. Subjective norms may influence an individual's awareness on online

financial scam due to several reasons. For example, if an individual's social circle, such as family members or friends place high emphasis on scam awareness and always take cybersecurity measures to safeguard their online activities, the individual also may adopt the similar behaviour. Hence, when people observed their social circle take reporting scam seriously, it will motivate them to take the same action, increasing their online scam awareness and preventing further victimization. As for policymakers, they can utilize the influence of subjective norm to foster a sense of alertness towards scam, making it to become a common value among Malaysians. This can be done through the collaboration with the public influencers or social media platforms.

5.3 Limitations of the Research

To ensure the accuracy and validity of the results, it is important to recognize the limitations of this study. First, the limitation of this study is sample size bias, which occurs when one group is overrepresented in the sample and prevents it from being representative of the total population. For example, a sizable proportion of the respondents (76.3%) were between the ages of 18-27. In this case, the samples mainly taken from the 18-27 age group may not be sufficient to represent the population accurately. It may have a restriction on the findings' generalizability to other age groups, since younger people may have different views and attitudes toward online financial scams than elder people. It means that the result obtained from the research may not be sufficient to represent the level of financial scam awareness among Malaysian.

Moreover, the second limitation of this research is that the questionnaire questions had been developed without a feedback section. As a result, some respondents may face obstacles in presenting a genuine response to the questions when they faced the issues of misinterpreting or misunderstanding certain words or sentences used in the survey questions. Also, the researchers cannot capture their comments and feedback. Hence, the researchers may not collect more precise results. In this case, the accuracy and reliability of the data obtained may be affected.

Last but not least, one of the research's limitations is the dearth of prior studies on online financial scams, which prevents from developing an in-depth understanding of the issues. As a result, it has been challenging to collect pertinent and trustworthy data and evaluate and put the findings into context. In this case, it's possible that important factors that could have been discovered through earlier research were missed in this study. Despite these limitations, this study fills a vacuum in the literature by offering a fresh viewpoint and adding to the body of knowledge already in existence. For example, when searching for data and literature for this research, the terms 'cybersecurity' and 'e-commerce' are frequently used in place of online financial scams.

The significance of the research was not affected by any of the limitations that were identified or resolved during this study, despite the possibility that they could have an impact on the analytic results. However, the limitations found in this study may help future researchers do better research that includes more in-depth analysis and debate.

5.4 Recommendations for Future Researchers

The study method has revealed some limitations, and it is critical to solve them for the next advancements. First, the majority of survey respondents in this study were between the ages of 18-27, which suggests a lack of representation for other age groups in the population and represents a significant drawback of this study.

To obtain a more representative sample, future researchers should aim for a more equitable distribution of participants across various age categories. By making sure the sample size is big enough to include a significant number of people from various age groups, this can be accomplished. Working with organizations can be an effective strategy for attracting people from different age groups for research. These groups give researchers the chance to communicate with the target audience.

Additionally, to express gratitude for the time and effort that participants give, researchers may provide incentives like vouchers.

Furthermore, future researchers can design and improve the questionnaires by adding more open-ended questions which require more than a simple one-word answer. Moreover, the questionnaires should include the feedback session to include the comments from the respondents regarding the readability and understandability of all questions. Otherwise, the data validity may be affected if the respondents just simply filled up the questionnaires while they do not have a clear and thorough understanding of the meaning of the questionnaires.

Lastly, future researchers should note the limitation of the scarcity of past studies with the title of Malaysians' awareness of online financial scams. However, similar research problems may have been addressed in related studies carried out in other nations. As a result, it is advised that a thorough literature assessment be carried out to pinpoint pertinent studies, theories, and research gaps that can direct the research. Future scholars can also look at related fields or subjects including how Malaysians feel about technology development in finance, cash-less financial environment, and cybersecurity issues. This will offer a broader view of the online financial scams in Malaysia and help fill the gap in existing research.

5.5 Conclusion

This research has explored Malaysians' awareness of online financial scams, with a focus on identifying the variables that affect awareness of online financial scams. The research revealed that Malaysians' awareness of online financial scams is positively and significantly affected by their perception of cybersecurity knowledge, perceived severity, and subjective norms. However, the security and privacy concerns is found to be insignificant. This research is essential for future investigators who are looking to prevent online financial scams. In conclusion, this research has contributed to the understanding of the factors that affect Malaysians'

awareness of online financial scams and provides valuable insights for preventing the happening of online financial scams in Malaysia.

REFERENCES

- Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE security & privacy*, 3(1), 26-33. <https://doi.org/10.1109/msp.2005.22>
- Aguirre-Urreta, M. I., & Rönkkö, M. (2018). Statistical inference with PLSc using bootstrap confidence intervals. *MIS quarterly*, 42(3), 1001-1020. <https://doi.org/10.25300/misq/2018/13587>
- Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A systematic literature review of e-banking frauds: Current scenario and security techniques. *Linguistica Antverpiensia*, 2(2), 3509-3517.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-t](https://doi.org/10.1016/0749-5978(91)90020-t)
- Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, 2(4), 314-324. <https://doi.org/10.1002/hbe2.195>
- Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136, 107376. <https://doi.org/10.1016/j.chb.2022.107376>
- Albaity, M., & Rahman, M. (2019). The intention to use Islamic banking: an exploratory study to measure Islamic financial literacy. *International Journal of Emerging Markets*, 14(5), 988–1012. <https://doi.org/10.1108/ijoem-05-2018-0218>
- Aliebrahimi, S., & Miller, E. E. (2023). Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour*, 96, 82-91. <https://doi.org/10.1016/j.trf.2023.06.010>
- Allen, M. (Ed.). (2017). *The SAGE encyclopedia of communication research methods*. SAGE publications. <https://doi.org/10.4135/9781483381411>

- Almost RM40mil lost to scams since October 2022. (2023, February 21). *The Star*. <https://www.thestar.com.my/news/nation/2023/02/21/almost-rm40millost-toscams-sinceoctober-2022>
- Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services*, 68, 103042. <https://doi.org/10.1016/j.jretconser.2022.103042>
- Ansar, S. A., Yadav, J., Dwivedi, S. K., Pandey, A., Srivastava, S. P., Ishrat, M., Khan, M. W., Pandey, D., & Khan, R. A. (2021). A critical analysis of fraud cases on the Internet. *Turkish Journal of Computer and Mathematics Education*, 12(1), 424-445.
- Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber Criminology*, 13(2). <http://dx.doi.org/10.5281/zenodo.3697886>
- Arvidsson, N. (2019). *Building a cashless society*. Springer Cham. <https://doi.org/10.1007/978-3-030-10689-8>
- Asher, N. B., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51–61. <https://doi.org/10.1016/j.chb.2015.01.039>
- Azreen Hani. (2022, June 17). Cashless society in Malaysia within 3 years. The Malaysian Reserve. <https://themalaysianreserve.com/2022/06/17/cashless-society-in-malaysia-within-3-years/>
- Bank Negara Malaysia. (n.d.). *Payment statistics*. <https://www.bnm.gov.my/payment-statistics>
- Barker, L. (1989), “Survey research”, in Emert, P. and Barker, L.B. (Eds), *Measurement of Communication Behavior*, Longman, New York, NY.
- Basyir, M. & Harun, H. N. (2022, September 26). Online scam cases increasing in Malaysia. *New Straits Times*. <https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia>

- Bhandari, P. (2020, July 9). *Descriptive Statistics - Definitions, Types, Examples*. Scribbr. <https://www.scribbr.com/statistics/descriptive-statistics/>
- Bhat, A. (2019, May 10). *Data Analysis in Research: Types & Methods*. QuestionPro. <https://www.questionpro.com/blog/data-analysis-in-research/>
- Boehmer, J., LaRose, R., Rifon, N. J., Alhabash, S., & Cotten, S. R. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology*, 34(10), 1022–1035. <https://doi.org/10.1080/0144929x.2015.1028448>
- Bonovas, S., & Piovani, D. (2023). On p-Values and Statistical Significance. *Journal of Clinical Medicine*, 12(3), 900. <https://doi.org/10.3390/jcm12030900>
- Brewerton, P., & Millward, L. J. (2001). *Methods of Data Collection*. SAGE Publications Ltd EBooks, 67–113. <https://doi.org/10.4135/9781849209533.n6>
- Brewerton, P.M., & Millward, L. J. (2001). *Organizational Research Methods*. SAGE Publications, Ltd.
- Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, 15, 48-64. <https://doi.org/10.1057/cpcs.2012.13>
- Bush, T. (2020, June 22). *Descriptive Analysis: How-To, Types, Examples*. PESTLE Analysis. <https://pestleanalysis.com/descriptive-analysis/>
- Cepeda-Carrion, G., Cegarra-Navarro, J. G., & Cillo, V. (2018). Tips to use partial least squares structural equation modelling (PLS-SEM) in knowledge management. *Journal of Knowledge Management*, 23(1), 67-89. <https://doi.org/10.1108/JKM-05-2018-0322>
- Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: the emerging trend. *Journal of Business Ethics*, 180(2), 581-604. <https://doi.org/10.1007/s10551-021-04884-3>
- Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*, 66(4), 552-567. <https://doi.org/10.1109/TEM.2018.2835461>

- Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987-995. <https://doi.org/10.1016/j.chb.2010.02.012>
- Cicchetti, D. V. (2014). On scales of measurement in autism spectrum disorders (ASD) and beyond: Where Smitty went wrong. *Journal of autism and developmental disorders*, 44, 303-309. <https://doi.org/10.1007/s10803-012-1486-z>
- Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, 7(3), 309–319. <https://doi.org/10.1037/1040-3590.7.3.309>.
- Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*, (ahead-of-print). <https://doi.org/10.1108/JFC-10-2022-0261>
- Connelly, L. M. (2008). Pilot studies. *Medsurg Nursing*, 17(6), 411-413.
- Cowan, K., Javornik, A., & Jiang, P. (2021). Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs. *Psychology & Marketing*, 38(10), 1799-1813. <https://doi.org/10.1002/mar.21576>
- Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors. *ACM SIGMIS Data Base*, 45(4), 51–71. <https://doi.org/10.1145/2691517.2691521>
- Daengsi, T., Pornpongtechavanich, P., Sirawongphatsara, P., Thimthong, T., & Sukniyom, N. (2022). A Study of Online Scams Associated with Age, Gender and Loss of Value in Thailand. In *2022 International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 219-222). IEEE. <https://doi.org/10.1109/ICDABI56818.2022.10041456>
- Das, R., & Patel, M. (2017, 04). Cyber security for social networking sites: Issues, challenges and solutions. *International Journal for Research in Applied Science and Engineering Technology*, 5, 833-838. <https://doi.org/10.22214/ijraset.2017.4153>
- Data Coding in Research Methodology*. (2014, November 19). ReadingCraze. <https://readingcraze.com/index.php/data-coding-research-methodology/>

- Data Collection Methods*. (2017, April 1). Research-Methodology. <https://research-methodology.net/research-methods/data-collection/>
- David, A. (2022, August 22). RM5.2B in losses through online scams since 2020. *The New Straits Times*. <https://www.nst.com.my/news/crime-courts/2022/08/819331/rm52b-losses-through-online-scams-2020>
- Department of Statistics Malaysia. (2023, February 9). *Demographic statistics fourth quarter 2022, Malaysia*. https://www.dosm.gov.my/v1/index.php?r=column/cthemByCat&cat=430&bul_id=VndFcmkvVTZoVTNYOTN2MzRtNy9zQT09&menu_id=L0pheU43NWJwRWVSZklWdzQ4TihUUT09
- Determining sample size: how to make sure you get the correct sample size*. (2020, July 7). Qualtrics. <https://www.qualtrics.com/au/experience-management/research/determine-sample-size/>
- Dudovskiy, J. (2022). *An Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-step Assistance*.
- Duggal, N. (2023, February 27). *What Is Data Processing: Cycle, Types, Methods, Steps and Examples*. Simplilearn. <https://www.simplilearn.com/what-is-data-processing-article>
- Dulock, H. L. (1993). Research design: Descriptive research. *Journal of Pediatric Oncology Nursing*, *10*(4), 154-157. <https://doi.org/10.1177/104345429301000406>
- Ekong Eyo, U. (2023). *Impact of Cyber-Security on Financial Fraud in Commercial Banks in Nigeria: A Case Study of Zenith Banks in Abuja* (Doctoral dissertation, AUST).
- Engellant, K. A., Holland, D. D., & Piper, R. T. (2016). Assessing convergent and discriminant validity of the motivation construct for the technology integration education (TIE) model. *Journal of Higher Education Theory & Practice*, *16*(1).
- Evermann, J., & Tate, M. (2014). Comparing The Predictive Ability Of Pls And Covariance Models. In I. 2016 (Ed.), *Thirty Fifth International Conference on Information Systems (Icis)* (Pp. 1–18). Auckland: Aisel.
- E-wallet usage in Malaysia 2020: Thriving in lockdown*. (2020, November 25). Oppotus. <https://www.oppotus.com/e-wallet-usage-in-malaysia-2020/>

- Factor Analysis.* (n.d.). *Statistics Solutions.*
<https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/factor-analysis/>
- Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019, September). Factors affecting security behavior of kenyan students: an integration of protection motivation theory and theory of planned behavior. In 2019 IEEE AFRICON (pp. 1-8). IEEE. <https://doi.org/10.1109/africon46755.2019.9133764>
- Farras, C., & Salmeron, A. M. (2018, May 15). *From barter to cryptocurrency: a brief history of exchange.* Caixa Bank Research. <https://www.caixabankresearch.com/en/economics-markets/monetary-policy/barter-cryptocurrency-brief-history-exchange>
- Fleetwood, D. (2020, February 13). *Non-Probability Sampling: Types, Examples, & Advantages.* QuestionPro. <https://www.questionpro.com/blog/non-probability-sampling/>
- Fong, F. (2022, September 10). Man Loses RM4,600 After Clicking SMS Link, Scammers Use Barisan Nasional's Name To Steal. *The Rakyat Post.* <https://www.therakyatpost.com/news/malaysia/2022/09/10/man-loses-rm4600-after-clicking-sms-link-scammers-use-barisan-nasionals-name-to-steal/>
- Fong, F. (2023, February 18). 19-Year-Old Student Lost Nearly RM50k To Love Scam Syndicate. *The Rakyat Post.* <https://www.therakyatpost.com/news/malaysia/2023/02/18/19-year-old-student-lost-nearly-rm50k-to-love-scam-syndicate/>
- Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society, 21*(6), 1232-1252. <https://doi.org/10.1177/1461444818815442>
- Gamble, K. J., Boyle, P., Yu, L., & Bennett, D. (2014). The causes and consequences of financial fraud among older Americans. *Boston College Center for Retirement Research WP, 13.* <https://doi.org/10.2139/ssrn.2523428>
- Garson, G. D. (2016). *Partial Least Squares: Regression & Structural Equation Models* (2016 Editi). Asheboro: Statistical Associates Publishing.

- Glanz, K., Rimer, B. K., & Viswanath, K. (1992). Health Behavior and Health Education: Theory, Research, and Practice. *Annals of Internal Medicine*, 116(4), 350. https://doi.org/10.7326/0003-4819-116-4-350_1
- Goforth, C. (2015, November 16). *Using and Interpreting Cronbach's Alpha*. University of Virginia Library Research Data Services + Sciences. <https://data.library.virginia.edu/using-and-interpreting-cronbachs-alpha/>
- Gomes, V. (2022a, February 28). E-wallet: Digital payments pivotal to Malaysia's financial services industry. *The Edge Market*. <https://www.theedgemarkets.com/article/ewallet-digital-payments-pivotal-malaysias-financial-services-industry>
- Gomes, V. (2022b, September 27). Catalysing Malaysia's digital economy. *The Edge Markets*. <https://www.theedgemarkets.com/article/catalysing-malaysias-digital-economy>
- Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, 111(7).
- Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of consumer marketing*, 19(4), 302-318. <https://doi.org/10.1108/07363760210433627>
- Hair Jr, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, 109, 101-110. <https://doi.org/10.1016/j.jbusres.2019.11.069>
- Hajjar, S. T. (2018). Statistical analysis: internal-consistency reliability and construct validity. *International Journal of Quantitative and Qualitative Research Methods*, 6(1), 27-38.
- Hamid, M. R. A., Sami, W., & Sidek, M. H. M. (2017). Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion. *Journal of Physics: Conference Series*, 890, 012163. <https://doi.org/10.1088/1742-6596/890/1/012163>
- Hassan, M. A., Shukur, Z., & Hasan, M. K. (2021). Electronic Wallet Payment System in Malaysia. *Data Analytics and Management*, 711-736. https://doi.org/10.1007/978-981-15-8335-3_55

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135. <https://doi.org/10.1007/s11747-014-0403-8>

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, 18, 106-125. <https://doi.org/10.1057/ejis.2009.6>

History of money: From fiat to crypto, explained. (2023, March 21). Crypto News. <https://cryptonews.net/news/other/20694675/>

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31, 83-95. <https://doi.org/10.1016/j.cose.2011.10.007>.

Ilker Etikan, Sulaiman Abubakar Musa, & Rukayya Sunusi Alkassim. Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4. <https://doi.org/10.11648/j.ajtas.20160501.11>

Inan, F. N., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments. *Journal of Educational Technology & Society*, 19(1), 28-40. <http://www.jstor.org/stable/jeductechsoci.19.1.28>

Introduction to SEM-PLS. (n.d.). <https://statisme.com/Learn/IntroductiontoSEMPLS>

Ipsos. (2020, January). *Survey on "Scams and fraud experienced by consumers"*. European Commission. https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Jain, R., & Chetty, P. (2021, September 30). *Criteria for reliability and validity in SEM analysis*. Knowledge Tank. <https://www.projectguru.in/criteria-for-reliability-and-validity-in-sem-analysis/>

Johnson, D. P. (2017). *How attitude toward the behavior, subjective norm, and perceived behavioral control affects information security behavior intention* (Doctoral dissertation, Walden University). <https://scholarworks.waldenu.edu/dissertations/4454>

- Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology, 12*, 649565. <https://doi.org/10.3389/fpsyg.2021.649565>
- Kagan, J. (2021, August 10). *Check: What It Is, How Bank Checks Work, and How To Write One*. Investopedia. <https://www.investopedia.com/terms/c/check.asp>
- Kante, M., Chepken, C., & Oboko, R. (2018). Partial least square structural equation modelling' use in information systems: an updated guideline in exploratory settings. *Kabarak Journal of Research & Innovation, 6*(1), 49-67.
- Karakaya-Ozyer, K., & Aksu-Dunya, B. (2018). A Review of Structural Equation Modeling Applications in Turkish Educational Science Literature, 2010-2015. *International Journal of Research in Education and Science, 4*(1), 279-291.
- Karpoff, J. M. (2021). The future of financial fraud. *Journal of Corporate Finance, 66*, 101694. <https://doi.org/10.1016/j.jcorpfin.2020.101694>
- Kaushik, K., Jain, N. K., & Singh, A. (2018b). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications, 32*, 57-68. <https://doi.org/10.1016/j.elerap.2018.11.003>
- Kemp, S. (2022, February 15). *DIGITAL 2022: MALAYSIA*. Kepios. <https://datareportal.com/reports/digital-2022-malaysia>
- Kemp, S., & Erades Pérez, N. (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact. *International Journal of Environmental Research and Public Health, 20*(7), 5404. <https://doi.org/10.3390/ijerph20075404>
- Kline, R. B. (2011). *Principles and practice of structural equation modeling*. New York: Guilford Press.
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement, 30*(3), 607-610. <https://doi.org/10.1177/001316447003000308>

- Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., & Kaaria, L. (2023). Can you spot a scam? Measuring and improving scam identification ability. <https://dx.doi.org/10.2139/ssrn.4344411>
- Lavrakas, P. J. (2008). *Encyclopedia of survey research methods*. Sage publications. <https://doi.org/10.4135/9781412963947>
- Lee, C. (2020, December 9). *How the government can protect people with mental health problems from online scam*. Money and Mental Health Policy Institute. <https://www.moneyandmentalhealth.org/online-scams-mental-health/#:~:text=The%20impact%20of%20an%20online,living%20on%20a%20low%20income.>
- Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, 00111287231180093. <https://doi.org/10.1177/00111287231180093>
- Lee, C., & Green, R. T. (1991). Cross-cultural examination of the Fishbein behavioral intentions model. *Journal of international business studies*, 22, 289-305. <https://doi.org/10.1057/palgrave.jibs.8490304>
- Lee, Y. J. (2020, November 20). *Malaysian Loses RM30,000 Within 5 Minutes After Scammers Pull Off Complex Bank Fraud*. Says. <https://says.com/my/news/malaysian-loses-rm-30000-over-bank-fraud-security>
- Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, 28(1), 28. <https://doi.org/10.17705/1CAIS.02828>
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90. <https://doi.org/10.2307/20650279>
- Liang, H., & Xue, Y. (2010). "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, 11(7), 394-413. <https://doi.org/10.17705/1jais.00232>
- Lim, Y. S. (n.d.). *Data Transcription in Qualitative Research: Everything You Need to Know*. Speak Ai. <https://speakai.co/data-transcription-in-qualitative-research/>

- Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, 7, 1133-1151.
- Macovei, O. I. (2015). Applying the theory of planned behavior in predicting proenvironmental behaviour: The case of energy conservation. *Acta Universitatis Danubius. Œconomica*, 11(4), 15-32.
- Malak, H. A. (2022, October 24). *10 Untold Advantages of Digitalization That You Should Know*. <https://theecmconsultant.com/advantages-of-digitalization/#:~:text=There%20are%20various%20advantages%20to,advantage%2C%20and%20faster%20decision%20making>.
- Malaysia - History, Flag, Map, Population, Language, Religion, & Facts*. (2023, March 23). Encyclopedia Britannica. <https://www.britannica.com/place/Malaysia/Local-government>
- Mardhiah, A. (2023, January 11). Ramp up security amid rise of financial fraud. *The Malaysian Reserve*. <https://themalaysianreserve.com/2023/01/11/ramp-up-security-amid-rise-of-financial-fraud/>
- Marriott, H., & Williams, M. (2018). Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study. *Journal of Retailing and Consumer Services*, 42, 133–146. <https://doi.org/10.1016/j.jretconser.2018.01.017>
- Marzunisham Omar. (2022, October 30). *Deputy Governor's Speech at the Launch of the National Scam Awareness Campaign*. Bank Negara Malaysia. <https://www.bnm.gov.my/-/dgmo-spch-nsrc-launch>
- Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research*, 2(3), 173-191. <https://doi.org/10.1287/isre.2.3.173>
- McCombes, S. (2019, September 19). *Sampling Methods | Types, Techniques & Examples*. Scribbr. <https://www.scribbr.com/methodology/sampling-methods/>
- McNeese, B. (2017). Interpretation of Alpha and p-Value. Spcforexcel. <https://www.spcforexcel.com/knowledge/basic-statistics/interpretation-alpha-and-p->

- Online scams cost M'sians RM52 mil in 3 months.* (2023, February 19). Focus Malaysia. <https://focusmalaysia.my/online-scams-cost-msians-rm52-mil-in-3-months/>
- Onofrei, N., & Paşa, A. R. (2022). A study on how attitude, subjective norms and perceived behavioral control influence financial awareness. *Sciendobook*, 685–698. <https://doi.org/10.2478/9788366675261-047>
- Peng, M. H., & Hwang, H. G. (2021). An empirical study to explore the adoption of e-learning social media platform in Taiwan: An integrated conceptual adoption framework based on technology acceptance model and technology threat avoidance theory. *Sustainability*, 13(17), 9946. <https://doi.org/10.3390/su13179946>
- Persada, S. F., Dalimunte, I., Nadlifatin, R., Miraja, B. A., Redi, A. A. N. P., Prasetyo, Y. T., ... & Lin, S. C. (2021). Revealing the behavior intention of tech-savvy generation Z to use electronic wallet usage: A theory of planned behavior based measurement. *International Journal of Business and Society*, 22(1), 213-226. <https://doi.org/10.33736/ijbs.3171.2021>
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, 19(1), 27-41. <https://doi.org/10.1509/jppm.19.1.27.16941>
- Prause, J. (n.d.). *Digitization vs digitalization*. SAP Insights. <https://www.sap.com/insights/digitization-vs-digitalization.html#:~:text=The%20Gartner%20Glossary%20says%3A%20%E2%80%9CDigitalization,moving%20to%20a%20digital%20business.%E2%80%9D>
- Purkait, S., De, S. K., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*, 22(3), 194–234. <https://doi.org/10.1108/imcs-05-2013-0032>
- Purwanto, A., & Sudargini, Y. (2021). Partial Least Squares Structural Equation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review. *Journal of Industrial Engineering & Management Research*, 2(4), 114–123. <https://doi.org/10.7777/jiemar.v2i4.168>
- Ray, S., Ow, T., & Kim, S. S. (2011). Security assurance: How online service providers can influence security control perceptions and gain trust. *Decision Sciences*, 42(2), 391-412. <https://doi.org/10.1111/j.1540-5915.2011.00316.x>

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, *91*(1), 93-114. <https://doi.org/10.1080/00223980.1975.9915803>

Rose, G., Khoo, H. M., & Straub, D. (1999). Current technological impediments to business-to-consumer electronic commerce. *Communications of the Association for Information systems*, *1*(1), 16. <https://doi.org/10.17705/1cais.00116>

Sample size and power. (2008, August). Institute for Work & Health. <https://www.iwh.on.ca/what-researchers-mean-by/sample-size-and-power#:~:text=Sample%20size%20refers%20to%20the,the%20study%20to%20draw%20conclusions>.

Sampling frames and master samples. (2008). *Studies in Methods*, 75–97. <https://doi.org/10.18356/eba6d79a-en>

Sawamura, J., Morishita, S., & Ishigooka, J. (2014). Interpretation for scales of measurement linking with abstract algebra. *Journal of clinical bioinformatics*, *4*, 1-9. <https://doi.org/10.1186/2043-9113-4-9>

Scam Awareness: Be Informed To Protect Yourself. (2022, November 14). Smart Investor Malaysia. <https://www.smartinvestor.com.my/scam-awareness-be-informed-to-protect-yourself/#:~:text=A%20survey%20commission%20by%20Bank,mule%20accounts%20to%20perpetrate%20fraud>.

Scam Awareness: Be Informed To Protect Yourself. (2022, November). Smartinvestor. <https://www.smartinvestor.com.my/scam-awareness-be-informed-to-protect-yourself/>

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & management*, *44*(1), 90-103. <https://doi.org/10.1016/j.im.2006.10.007>

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business Students: A Skill Building Approach* (7th ed.). Wiley.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. john wiley & sons. <https://books.google.com.my/books?hl=en&lr=&id=Ko6bCgAAQBAJ&oi=fnd&pg=PA19&dq=Research+Methods+For+Business:+A+Skill+Building+Approach.+John+Wiley+%26+Sons&ots=2C5LZ3LXnR&sig=mmBG>

r2LsLQ-sjL-
ITbpTlaZ2cDc&redir_esc=y#v=onepage&q=Research%20Methods%20F
or%20Business%3A%20A%20Skill%20Building%20Approach.%20John
%20Wiley%20%26%20Sons&f=false

Sharma, B. (2016). A focus on reliability in developmental research through Cronbach's Alpha among medical, dental and paramedical professionals. *Asian Pacific Journal of Health Sciences*, 3(4), 271-278. <https://doi.org/10.21276/apjhs.2016.3.4.43>

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73. <https://doi.org/10.1509/jppm.19.1.62.16949>

Shien, L. Y. (2022, October 27). *Data transcription in qualitative research: Everything you need to know*. <https://speakai.co/data-transcription-in-qualitative-research/>

Shih, H. M., Chen, B. H., Chen, M. H., Wang, C. H., & Wang, L. F. (2022). A Study of the Financial Behavior Based on the Theory of Planned Behavior. *International Journal of Marketing Studies*, 14(2), 1. <https://doi.org/10.5539/ijms.v14n2p1>

Sikdar, P., & Makkad, M. (2015). Online banking adoption. *International Journal of Bank Marketing*, 33(6), 760–785. <https://doi.org/10.1108/ijbm-11-2014-0161>

Sincero, S. M. (2012, July 20). *Surveys and Questionnaires - Guide*. Explorable. <https://explorable.com/surveys-and-questionnaires>

Stasny, E. A. (2001). Nonsampling errors. *International Encyclopedia of the Social and Behavioural Sciences*. <https://doi.org/10.1016/B0-08-043076-7/00414-9>

Stavins, J. (2021). Payments Evolution from Paper to Electronic: Bill Payments and Purchases. *FRB of Boston Working Paper No. 21-5*. <https://dx.doi.org/10.29412/res.wp.2021.05>

Su, L., Swanson, S. R., & Chen, X. (2016). The effects of perceived service quality on repurchase intentions and subjective well-being of Chinese tourists: The mediating role of relationship quality. *Tourism management*, 52, 82-95. <https://doi.org/10.1016/j.tourman.2015.06.012>

- Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information*, 13(9), 413. <https://doi.org/10.3390/info13090413>
- Swatzell, K. E., & Jennings, P. R. (2007). Descriptive research: The nuts and bolts. *Journal of the American Academy of Physician Assistants*, 20(7). <https://doi.org/10.1097/01720610-200707000-00098>
- Syed Muhammad Sajjad Kabir. (2016). *Basic guidelines for research: An introductory approach for all disciplines*. Book Zone Publication. https://www.researchgate.net/profile/Syed-Muhammad-Kabir/publication/325390597_BASIC_GUIDELINES_FOR_RESEARCH_An_Introductory_Approach_for_All_Disciplines/links/5b0a89094585157f8719626c/BASIC
- Syeda Ayeman Mazhar, Rubi Anjum, Ammar Ibni Anwar, & Abdul Aziz Khan (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>
- Taherdoost, H. (2016). Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in a research. *International Journal of Academic Research in Management*, 5(2), 28-36. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205040
- Tentama, F., & Anindita, W. D. (2020). Employability scale: Construct validity and reliability. *International Journal of Scientific & Technology Research*, 9(4), 3166-3170.
- Teoh Teng Tenk, M., Yew, H. C., & Heang, L. T. (2020). E-wallet Adoption: A case in Malaysia. *International Journal of Research In Commerce and Management Studies*, 2(2), 216-233. https://ijrcms.com/uploads2020/ijrcms_02_51.pdf
- The global findex database 2021*. (2021). The World Bank. <https://www.worldbank.org/en/publication/globalfindex/Data>
- The total impacts of fraud*. (2020, July 20). Commonwealth Fraud Prevention Centre. <https://www.counterfraud.gov.au/total-impacts-fraud#:~:text=Fraud%20can%20have%20a%20devastating,opportunities%20for%20individuals%20and%20businesses.>

- Thompson, N., McGill, T. J., & Ferreira, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, 376–391. <https://doi.org/10.1016/j.cose.2017.07.003>
- Tsai, H., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150. <https://doi.org/10.1016/j.cose.2016.02.009>
- Turner, A. G. (2003). Sampling frames and master samples. *United Nations secretariat statistics division*, 1-26.
- Turner, D. P. (2020). Sampling methods in research design. *The Journal of Head and Face Pain*, 60(1), 8-12. <https://doi.org/10.1111/head.13707>
- Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application (JITTA)*, 11(2), 2.
- Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, 48(8), 1565-1585. <https://doi.org/10.1108/K-05-2018-0226>
- Van Teijlingen, E., & Hundley, V. (2002). The importance of pilot studies. *Nursing Standard* (through 2013), 16(40), 33. <https://doi.org/10.7748/ns2002.06.16.40.33.c3214>
- Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, 101, 286–296. <https://doi.org/10.1016/j.chb.2019.07.034>
- Villanueva, J. (2019, February 1). *From Barter System to Cryptocurrency: The Evolution of Money*. LinkedIn. <https://www.linkedin.com/pulse/from-barter-system-cryptocurrency-evolution-money-jake-villanueva/>
- Wasserstein, R. L., & Lazar, N. A. (2016). The ASA statement on p-values: context, process, and purpose. *The American Statistician*, 70(2), 129-133. <https://doi.org/10.1080/00031305.2016.115410>

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166. <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>

What are factor loadings?. (2023, June 20). Collimator. <https://www.collimator.ai/reference-guides/what-are-factor-loadings>

Williams, E., & Joinson, A. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa001>

Wiryanto, H. (2018, December 26). *Reliability Composite*. RPubs. https://rpubs.com/wiryantodatascience/Comp_Reliability

Wiśniowski, A., Sakshaug, J. W., Ruiz, D. A. P., & Blom, A. G. (2020). Integrating Probability and Nonprobability Samples for Survey Inference. *Journal of Survey Statistics and Methodology*, 8(1), 120–147. <https://doi.org/10.1093/jssam/smz051>

Wong, A. (2022, September 26). *Malaysia Police Force said online scam cases have increased higher each year.* TechNave. <https://technave.com/gadget/Malaysia-police-force-said-online-scam-cases-have-increased-higher-each-year-31934.html>

Wong, S. L., Bong, S. C., Khor, S. P., & Wong, K. L. (2017). *Financial Awareness among Universiti Tunku Abdul Rahman Undergraduate Students in Kampar Campus* (Doctoral dissertation, UTAR). <http://eprints.utar.edu.my/2524/1/BF-2017-1401385.pdf>

Wopperer, W. (2002). Fraud risks in E-commerce transactions. *The Geneva papers on risk and insurance. Issues and Practice*, 27(3), 383-394. <https://doi.org/10.1111/1468-0440.00180>

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798-824. <https://doi.org/10.17705/1jais.00281>

Yahya, K. (2022, December 22). Raub housewife duped by scammer using e-wallet redemption ruse. *New Straits Times*. <https://www.nst.com.my/news/crime-courts/2022/12/865937/raub-housewife-duped-scammer-using-e-wallet-redemption-ruse>

- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710-722. <https://doi.org/10.1002/asi.20530>
- Yap, C. M., Ng, B. A (2019). Factors Influencing Consumers' Perceived Usefulness of M-Wallet in Klang Valley, Malaysia. *Review of Integrative Business and Economics Research*, 8(4), 1–23. https://www.researchgate.net/publication/333673692_Factors_Influencing_Consumers'_Perceived_Usefulness_of_M-Wallet_in_Klang_Valley_Malaysia
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389-418. <https://doi.org/10.1111/j.1745-6606.2009.01146.x>
- Yuan, L. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471–481. <https://doi.org/10.1016/j.dss.2012.06.010>
- Zeng, N., Liu, Y., Gong, P., Hertogh, M., & König, M. (2021). Do right PLS and do PLS right: A critical review of the application of PLS-SEM in construction management research. *Frontiers of Engineering Management*, 8, 356-369. <https://doi.org/10.1007/s42524-021-0153-5>
- Zwilling, M., Klien, G. H., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97. <https://doi.org/10.1080/08874417.2020.1712269>

APPENDICES

Appendix 3.1

Sample size of a known population

<i>N</i>	<i>S</i>	<i>N</i>	<i>S</i>	<i>N</i>	<i>S</i>
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	345
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	14	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

Appendix 3.2

Survey questionnaire permission letter



UNIVERSITI TUNKU ABDUL RAHMAN DU012(A)

Wholly owned by UTAR Education Foundation (200201010564(578227-M))

Faculty of Business and Finance
Jalan Universiti, Bandar Barat, 31900 Kampar, Perak
Phone: 05-468-8888
<https://fbf.utar.edu.my/>

3rd July 2023

To Whom It May Concern

Dear Sir/Madam,

Permission to Conduct Survey

This is to confirm that the following students are currently pursuing their *Bachelor of Finance (Honours)* program at the Faculty of Business and Finance, Universiti Tunku Abdul Rahman (UTAR) Perak Campus.

I would be most grateful if you could assist them by allowing the student to conduct his research at your institution. All information collected will be kept confidential and used only for academic purposes.

The student are as follows:

<u>Name of Student</u>	<u>Student ID</u>
Lee Wen Xian	19ABB04593
Lim Nya Hia	20ABB05875
Vivian Lim Yan Yi	19ABB05417

If you need further verification, please do not hesitate to contact me.

Thank you.

Yours sincerely,

.....
Dr Lee Chee Loong
Head of Department
Faculty of Business and Finance
Email: lcloong@utar.edu.my

Administrative Address: Jalan Sg. Long, Bandar Sg. Long, Cheras, 43000 Kajang, Selangor D.E.
Tel: (603) 9086 0288 **Homepage:** <https://utar.edu.my/>

Appendix 3.3

Survey questionnaire sample



UNIVERSITI TUNKU ABDUL RAHMAN

**BACHELOR OF FINANCE (HONOURS)
FACULTY OF BUSINESS AND FINANCE
DEPARTMENT OF FINANCE**

Final Year Project

**Title of topic: Awareness on Online Financial Scam: A Study
in Malaysia**

Survey Questionnaire Sample

Dear respondents,

We are the final year undergraduates students who are currently pursuing Bachelor of Finance (Honours) in Universiti Tunku Abdul Rahman (UTAR). Currently, we are conducting a research for our final year project, with the title of “Awareness on Online Financial Scam: A Study in Malaysia”. The purpose of this research is to identify Malaysians’ awareness towards the online financial scam.

This questionnaire consists of 3 sections and it will takes approximately 10-15 minutes to complete. All data and information gathered from this questionnaire will be kept strictly confidential and used solely for research purposes. Your participation and co-operation in answering this questionnaire is highly appreciated. Should you have further enquiries, please do not hesitate to contact any one of our group members.

Name	E-mail	Phone Number
Lee Wen Xian	leewenxian0402@gmail.com	016-5913142
Lim Nya Hia	nyahia01@gmail.com	011-61500309
Vivian Lim Yan Yi	yyilim0042@gmail.com	016-5459198

PERSONAL DATA PROTECTION STATEMENT

Please be informed that in accordance with Personal Data Protection Act 2010 (“PDPA”) which came into force on 15 November 2013, Universiti Tunku Abdul Rahman (“UTAR”) is hereby bound to make notice and require consent in relation to collection, recording, storage, usage and retention of personal information.

Notice:

1. The purposes for which your personal data may be used are inclusive but not limited to:-
 - For assessment of any application to UTAR
 - For processing any benefits and services
 - For communication purposes
 - For advertorial and news
 - For general administration and record purposes
 - For enhancing the value of education
 - For educational and related purposes consequential to UTAR
 - For the purpose of our corporate governance
 - For consideration as a guarantor for UTAR staff/ student applying for his/her scholarship/ study loan
2. Your personal data may be transferred and/or disclosed to third party and/or UTAR collaborative partners including but not limited to the respective and appointed outsourcing agents for purpose of fulfilling our obligations to you in respect of the purposes and all such other purposes that are related to the purposes and also in providing integrated services, maintaining and storing records. Your data may be shared when required by laws and when disclosure is necessary to comply with applicable laws.
3. Any personal information retained by UTAR shall be destroyed and/or deleted in accordance with our retention policy applicable for us in the event such information is no longer required.
4. UTAR is committed in ensuring the confidentiality, protection, security and accuracy of your personal information made available to us and it has been our ongoing strict policy to ensure that your personal information is accurate, complete, not misleading and updated. UTAR would also ensure that your personal data shall not be used for political and commercial purposes.

Consent:

1. By submitting this form you hereby authorise and consent to us processing (including disclosing) your personal data and any updates of your information, for the purposes and/or for any other purposes related to the purpose.
2. If you do not consent or subsequently withdraw your consent to the processing and disclosure of your personal data, UTAR will not be able to fulfill our obligations or to contact you or to assist you in respect of the purposes and/or for any other purposes related to the purpose.

3. You may access and update your personal data by writing to us at _____.

Acknowledgment of Notice

[] I have been notified by you and that I hereby understood, consented and agreed per UTAR above notice.

[] I disagree, my personal data will not be processed.

.....

Name:

Date:

Section A: Demographic Profile

The following questions refer to the demographic profile to the respondents.

Please provide the appropriate information by placing a (√) in the bracket provided to represent your answer.

1. Gender
 - Male
 - Female

2. Age
 - 18-27
 - 28-37
 - 38-47
 - 48-57
 - 58 and above

3. Ethnic
 - Malays
 - Chinese
 - India
 - Others:

4. Education Level
 - SPM and below
 - Foundation/Diploma/STPM
 - Bachelor's Degree
 - Master's Degree
 - Doctorate Degree

5. Monthly income
 - RM1,000 and below
 - RM1,001- RM2,500
 - RM2,501- RM5,000
 - RM5,001 and above

6. Which state are you from?
 - Johor
 - Kedah
 - Kelantan
 - Melaka
 - Negeri Sembilan
 - Pahang
 - Perlis

- Perak
 - Penang
 - Sabah
 - Sarawak
 - Selangor
 - Terengganu
6. Do you have any e-wallet or online banking account?
- Yes
 - No, thank you for your participation
7. Which e-wallet account are you using? You may choose more than 1.
- Touch 'n Go (TNG)
 - Boost
 - GrabPay
 - ShopeePay
 - MAE (Maybank)
8. Which online banking account are you using? You may choose more than 1.
- Public Bank
 - Maybank
 - RHB Bank
 - Hong Leong Bank
 - UOB Malaysia
 - CIMB Bank
 - Others:_____

Section B

Please choose the best answer based on the scale of 1 to 5.

Note: Scale 1 indicates that you strongly disagree with the statement and 5 indicates you strongly agree with the statement.

Awareness on Online Financial Scam

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	I am aware of online financial scams.	1	2	3	4	5
2.	I always read materials about online financial scams on bank websites, the internet, or social media.	1	2	3	4	5
3.	I have heard of someone around who has been a victim of ewallet online fraud.	1	2	3	4	5
4.	I would immediately report to the banks when there is a suspicious transaction.	1	2	3	4	5
5.	I am aware that online financial scams usually threaten through SMS, phone calls, online websites and email.	1	2	3	4	5
6.	I am aware that online financial scams will lead to money losses, damage reputation, damage society and	1	2	3	4	5

	ruin economic growth.					
7.	I have installed an Ad-blocker on my mobile, laptop, or other gadgets, which helps prevent ads and other malicious tracers.	1	2	3	4	5
8.	I update the systems and software on my mobile and laptop frequently.	1	2	3	4	5

Section C

Please choose the best answer based on the scale of 1 to 5.

Note: Scale 1 indicates that you strongly disagree with the statement and 5 indicates you strongly agree with the statement.

Cybersecurity Knowledge

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	I feel that sharing passwords with others is unsecure.	1	2	3	4	5
2.	I am able to keep up to date with online financial scam techniques.	1	2	3	4	5
3.	I possess the knowledge and skills to take the necessary security measures against online financial scams.	1	2	3	4	5
4.	I am familiar with using any scam detection application to prevent online financial scam.	1	2	3	4	5
5.	I am confident in my ability to identify potential online financial scams.	1	2	3	4	5
6.	I have an idea of the techniques used by the scammers that lead to online financial scams.	1	2	3	4	5

Perceived Severity

*Perceived severity measures an individual’s subjective assessment of the seriousness of a specific threat. This part aims to know to what extent people believe how serious the threat is, and how the consequences of the threats would be harmful.

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	I considered the potential impact of falling victim to an online financial scam to be extremely severe.	1	2	3	4	5
2.	I am concerned about the potential financial loss from an online financial transaction.	1	2	3	4	5
3.	I am worried about the possibility of having my personal information stolen in an online financial transaction.	1	2	3	4	5
4.	I place importance on protecting my personal financial information.	1	2	3	4	5
5.	I am worried about the efforts and resources needed to recover if I fall into online financial scam.	1	2	3	4	5
6.	I believe that the emotional and psychological effects of being a victim of an online financial scam are severe.	1	2	3	4	5

Subjective Norms

		Strong Disagree	Disagree	Neutral	Agree	Strong Agree
1.	I always heard of my family member who has been a victim of e-wallet financial scam.	1	2	3	4	5
2.	I always heard of my friend who has been a victim of e-wallet financial scam.	1	2	3	4	5
3.	I always heard of my family member who has been a victim of online banking financial scam.	1	2	3	4	5
4.	I always heard of my friend who has been a victim of online banking financial scam.	1	2	3	4	5
5.	I will strongly recommend my family member to aware of e-wallet financial scam.	1	2	3	4	5
6.	I will strongly recommend my family member to aware of online banking financial scam.	1	2	3	4	5
7.	I will strongly recommend my friends to aware of e-wallet financial scam.	1	2	3	4	5
8.	I will strongly recommend my friends to aware of online banking financial scam.	1	2	3	4	5

Security and Privacy Concerns

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	I always concerned about the security of my personal information when conducting online transactions or activities.	1	2	3	4	5
2.	I always ensure that my passwords of all the accounts are made up of 12 letters and a combination of letters, digits, or signs.	1	2	3	4	5
3.	I always use different passwords for different accounts (E-wallet account and online banking account).	1	2	3	4	5
4.	I always use two factor authentication (e.g. combination of fingerprint and password to unlock) on phone and account to protect my security and privacy.	1	2	3	4	5
5.	I always share the password (bank account, card, e-wallet and other financial related instruments) to family members and friends.	1	2	3	4	5
6.	I always feel safe providing personal	1	2	3	4	5

	privacy information over the e-wallet or online banking account.					
7.	I always reply to the unknown phone calls and messages.	1	2	3	4	5
8.	I always open the website URL without “https” and any email from a suspicious sender.	1	2	3	4	5

Thank you for your participation.