

THE INFLUENCING FACTORS OF ONLINE  
BANKING FRAUD AWARENESS IN UTAR KAMPAR

CHIN KE LI  
TAN XIN TONG  
TANG JIA HOOI  
TOH KHAI LI

BACHELOR OF ECONOMICS (HONS)  
FINANCIAL ECONOMIC

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE  
DEPARTMENT OF ECONOMICS

APRIL 2023

THE INFLUENCING FACTORS OF ONLINE BANKING  
FRAUD AWARENESS IN UTAR KAMPAR

BY

CHIN KE LI  
TAN XIN TONG  
TANG JIA HOOI  
TOH KHAI LI

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

BACHELOR OF ECONOMICS (HONS)  
FINANCIAL ECONOMIC

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE  
DEPARTMENT OF ECONOMICS

APRIL 2023

Copyright @ 2023

ALL RIGHTS RESERVED. No part of this paper may be reproduced, stored in a retrieval system, or transmitted in any form or 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 of this or any other 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 23,238.

Name of Student:	Student ID:	Signature:
1. <u>Chin Ke Li</u>	<u>19ABB02377</u>	<u><i>Kelly Chin</i></u>
2. <u>Tan Xin Tong</u>	<u>19ABB02308</u>	<u><i>Xin Tong</i></u>
3. <u>Tang Jia Hooi</u>	<u>19ABB03439</u>	<u><i>Jia Hooi</i></u>
4. <u>Toh Khai Li</u>	<u>20ABB03846</u>	<u><i>Kelly Toh</i></u>

Date: 28/4/2023

#### ACKNOWLEDGEMENT

The author would like to express her utmost gratitude to Universiti Tunku Abdul Rahman for providing the author with the opportunity to conduct a study regarding the influencing factors of online banking fraud awareness in UTAR Kampar as her graduation project alongside with her team which consist of 4 Bachelor (Honors) in Economics in Financial Economics students.

Throughout this study, the author and her team have gained an overwhelming number of skills. Therefore, a lot of people's encouragement and direction is crucial to the study's success. The author and her team would want to use this opportunity to thank everyone who contributed to the success of their initiative and to show their gratitude.

Puan Siti Nur Amira Binti Othman's supervision, advice, and provision of vital information regarding the study to completion are all greatly appreciated by the author and her team. We value her eagerness to impart to us her insightful experiences, ideas, and knowledge. The author and her team would like to express their gratitude to the professors and staffs of the Faculty of Business and Finance UTAR for their assistance throughout the study, which provided helpful information, recommendations, and direction in the compilation and preparation of this final year project report.

Lastly, the author and her team would like to express our gratitude to every respondent for spending the time and effort to complete the questionnaires. Due to their participation in the survey, the study was able to get 400 replies.

TABLE OF CONTENTS

	Page
Copyright Page.....	ii
Declaration .....	iii
Acknowledgement .....	iv
Table of Contents .....	v
List of Tables .....	x
List of Figures .....	xii
List of Abbreviations .....	xiii
List of Appendices .....	xv
Preface.....	xvi
Abstract .....	xvii
CHAPTER 1: INTRODUCTION .....	1
1.1 Background of the study .....	1
1.2 Problem Statement .....	5
1.3 Research Objectives .....	10
1.3.1 General Objective .....	10
1.3.2 Specific Objectives .....	10
1.4 Research Questions .....	11
1.5 Significance of the study .....	12
1.6 Conclusion.....	13
CHAPTER 2: LITERATURE REVIEW .....	15

2.1	Underlying theories .....	15
2.1.1	Theory of Planned Behavior .....	16
2.1.2	Protection Motivation Theory .....	17
2.1.3	Technology Acceptance Model .....	18
2.2	Review of variables .....	19
2.2.1	Fraud Awareness .....	20
2.2.2	Personal Financial Distress .....	22
2.2.3	Empathy .....	24
2.2.4	Knowledge of Online Banking .....	26
2.2.5	Attitude towards Fraud .....	28
2.3	Conceptual framework .....	30
2.4	Hypothesis .....	32
2.4.1	Fraud Awareness and Personal Financial Distress .....	32
2.4.2	Fraud Awareness and Empathy .....	35
2.4.3	Fraud Awareness and Knowledge of online banking .....	37
2.4.4	Fraud Awareness and Attitude towards fraud .....	39
2.5	Conclusion .....	40
CHAPTER 3: METHODOLOGY .....		41
3.1	Research Design .....	41
3.1.1	Quantitative Research .....	41
3.1.2	Descriptive research .....	42
3.2	Data Collection Method .....	42
3.2.1	Primary data .....	43
3.3	Design of sampling .....	43
3.3.1	Target Population .....	44

3.3.2	Frame and location of sampling.....	45
3.3.3	Technique of Sampling.....	45
3.3.4	Size of Sampling.....	46
3.4	Research Instrument.....	48
3.4.1	Questionnaire Design.....	48
3.4.2	Questionnaire Reliability.....	49
3.4.3	Ethical Consideration.....	50
3.4.4	Pilot test.....	51
3.5	Constructs Measurement.....	52
3.5.1	Scale of Measurement.....	53
3.5.1.1	Nominal Scale.....	53
3.5.1.2	Interval Scale.....	53
3.5.2	Operational Definition for the Measurement of Independent Variables and Dependent Variable.....	54
3.5.2.1	Fraud awareness.....	55
3.5.2.2	Personal Financial Distress.....	55
3.5.2.3	Empathy.....	55
3.5.2.4	Knowledge towards online banking.....	56
3.5.2.5	Attitude towards fraud.....	56
3.6	Data Processing.....	57
3.6.1	Data Checking.....	57
3.6.2	Data Editing.....	58
3.6.3	Data Coding.....	58
3.6.4	Data Transferring.....	59
3.7	Data Analysis.....	59



3.7.1	Descriptive Analysis .....	59
3.7.2	Scale Measurement .....	60
3.7.2.1	Reliability test.....	60
3.7.3	Preliminary Data Screening .....	62
3.7.3.1	Normality.....	62
3.7.3.2	Pearson correlation .....	63
3.7.3.3	Multicollinearity .....	63
3.7.4	Inferential analysis .....	63
3.7.4.1	Multiple Regression Analysis.....	64
3.8	Conclusion.....	65
CHAPTER 4: DATA ANALYSIS .....		66
4.1	Descriptive analysis.....	66
4.1.1	Respondents' Demographic Profile .....	66
4.1.1.1	Gender .....	67
4.1.1.2	Age Group .....	68
4.1.1.3	Number of Internet Bank Account Holding .....	71
4.1.1.4	The Frequency of Using Online Banking.....	72
4.1.1.5	The frequency of Getting into Online Banking Fraud.....	74
4.1.2	Central Tendencies and Measurement of Constructs' Dispersion Dispersion .....	75
4.1.2.1	Fraud awareness .....	75
4.1.2.2	Personal Financial Distress.....	77
4.1.2.3	Empathy.....	78
4.1.2.4	Knowledge of online banking.....	79
4.1.2.5	Attitude towards fraud .....	81

4.2	Scale Measurement .....	83
4.2.1	Reliability test .....	83
4.3	Preliminary Data Screening .....	84
4.3.1	Normality Test .....	84
4.3.2	Pearson Correlation.....	86
4.4	Inferential Analysis .....	91
4.4.1	Multiple Regression Analysis .....	91
4.5	Conclusion.....	93
CHAPTER 5: DISCUSSION AND CONCLUSION .....		95
5.1	Statistical Analysis Summary.....	95
5.2	Discussion on Major Findings .....	96
5.2.1	Personal Financial Distress and fraud awareness .....	96
5.2.2	Empathy and fraud awareness .....	97
5.2.3	Knowledge on online banking and fraud awareness.....	98
5.2.4	Attitude towards fraud and fraud awareness.....	99
5.3	Implications of the study .....	101
5.3.1	Practical implications.....	101
5.3.2	Theoretical implications.....	102
5.4	Limitations of study .....	103
5.5	Recommendations for future research.....	105
5.6	Conclusion.....	106
References.....		107
Appendices.....		121

LIST OF TABLES

	Page
Table 1.1: Number of new unknown media content received by MCMC, Malaysia in 2019 and 2020.....	7
Table 3.1 Example of Likert scale .....	54
Table 3.2 : Answer coded for Section A.....	58
Table 3.3: Cronbach Rule of Thumb .....	60
Table 3.4: Result of reliability test for pilot test .....	61
Table 4.1: Descriptive Analysis for Gender .....	67
Table 4.2: Descriptive Analysis for Age Group .....	68
Table 4.3: Descriptive Analysis for Number of Internet Bank Account Holding. ....	71
Table 4.4: Descriptive Analysis for the Frequency of Using Online Banking .....	72
Table 4.5: Descriptive Analysis for the frequency of Getting into Online Banking Fraud .....	74
Table 4.6: Central Tendencies Measurement for Fraud Awareness. ....	75
Table 4.7: Central Tendencies Measurement for Personal Financial Distress .....	77
Table 4.8: Central Tendencies Measurement for Empathy .....	78
Table 4.9: Central Tendencies Measurement for Knowledge of Online Banking.....	79
Table 4.10: Central Tendencies Measurement for Attitude towards Fraud.....	81
Table 4.11: Reliability Analysis. ....	83
Table 4.12: Normality Test Results .....	85
Table 4.13: Correlations for Fraud Awareness and Personal Financial Distress.....	87
Table 4.14: Correlations for Fraud Awareness and Empathy.....	88
Table 4.15: Correlations of Fraud Awareness and Knowledge on Online Banking...	89
Table 4.16: Correlations of Fraud Awareness and Attitude Towards Fraud .....	90
Table 4.17: Model Summary .....	91

Table 4.18: Multiple Regression Analysis.....	92
Table 5.1: Summary of the Statistical Findings.....	95

LIST OF FIGURES

	Page
Figure 1.1: The relationship between Research Objectives and Research Questions	11
Figure 2.1: Conceptual Framework .....	30
Figure 4.1: Descriptive Analysis for Gender .....	67
Figure 4.2: Descriptive Analysis for Age Group .....	70
Figure 4.3: Descriptive Analysis for Number of Internet Bank Account Holding .....	71
Figure 4.4: Descriptive Analysis for the Frequency of Using Online Banking .....	73
Figure 4.5: Descriptive Analysis for the frequency of Getting into Online Banking Fraud. ....	74

LIST OF ABBREVIATIONS

ACFE	Association of the Certified Fraud Examiners
ATF	Attitude towards Fraud
BNM	Bank Negara Malaysia
CID	Commercial Item Determination
DAP	Democratic Action Party
E	Empathy
FA	Fraud Awareness
FLM	Financial Literacy Month
FTC	Federal Trade Commission
IC	Identity card
KOB	Knowledge of Online Banking
OCBC Bank	Oversea-Chinese Banking Corporation, Limited
OECD	Organization of Economic Co-operation and Growth
OTP	One-Time Password
PFD	Personal Financial Distress
PTPTN	Perbadanan Tabung Pendidikan Tinggi Nasional
NASCA	National Cyber Security Agency

NSAC	National Scam Awareness Campaign
PDRM	Polis Diraja Malaysia
PMT	Protection Motivations Theory
SMS	Short Message Service
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
UTAR	Universiti Tunku Abdul Rahman
QR code	Quick Response Code
VIF	Variance Inflation Factor

LIST OF APPENDICES

	Page
Appendix 1: Ethical Approval for Research Project.....	121
Appendix 2: Survey Questionnaire.....	123
Appendix 3: SPSS Data Analysis Result.....	138
Appendix 3.1: Reliability Tests for variables.....	138
Appendix 3.2: Multiple Regression Analysis Result.....	138



## PREFACE

The project was crucial to the completion of study for our undergraduate program offered by the university which is Bachelor in Economics (Hons) Financial Economics. The study entitled the influencing factors of online banking fraud awareness in UTAR Kampar. As per the title, this study mainly focuses on investigating the factors that influence online banking fraud awareness among the youth or university students in UTAR Kampar.

Recently, there is an increasing trend of number in online banking fraud cases faced and reported by consumers in Malaysia. This persistent phenomenon has caused a serious threat to the consumer confidence on tin security of the bank account which is not a good occurrence to all the parties, such as consumers, businesses, and government. In this case, public awareness on fraud is vital to prevent the tragedy from happening. Each of the parties have the responsibility to play their role for increasing online banking fraud awareness.

As a result, this study investigates the influencing factors on online banking fraud awareness because it is able to prevent the case occur. In this case, there are 4 influencing factors which include personal financial distress, empathy, knowledge on online banking, and attitude towards fraud. At the end, this research project will provide useful information to each party on the prevention of online banking fraud cases for university students.

## ABSTRACT

As the use of online banking becomes more widespread, the frequency of online banking fraud is also on the rise. The purpose of this research is to examine the factors that impact consumers' awareness towards online banking fraud. To gather information for this study, questionnaires were given to 400 UTAR Kampar students between the ages of 18 and 24 by using the convenient non-random sampling. The questionnaire assessed participants' levels of understanding about online banking fraud related to the relationship between personal financial distress, empathy, attitude towards fraud and knowledge of online banking. In this study, several analysis tests have been used to analyze the hypothesis such as descriptive analysis, scale measurement, preliminary data screening and inferential analysis. The outcomes of this research are significant for financial institutions and policymakers as they work to combat online banking fraud. In the future, this study will draw attention to new paradigms that will be useful for discussions of the online fraud trend and could contribute to a more comprehensive analysis.

Keywords: Fraud Awareness, Personal Financial Distress, Empathy, Knowledge of Online Banking, Attitude towards Fraud.

## **CHAPTER 1: INTRODUCTION**

### **1.0 Introduction**

The topic of this research study is the influencing factors of online banking fraud awareness in UTAR Kampar. In this chapter, a detailed and specific introduction of the topic will be discussed and explained. The researcher will first justify the background of study, and the problem statement. It is then followed by the research questions, research objectives, and significance for the research study conducted.

### **1.1 Background of the study**

Nowadays, there is more than 70% of people with bank accounts to utilize online banking, which was formerly a novel and infrequently used technology. Online banking has undergone a significant transformation in numerous banking and financial services and will continue to grow as long as financial institutions continue to encourage customers to use online banking for such things as funds transfer, accessing account information as well as payment of monthly bills (Ling et al., 2015). Due to the continuous advancement in information and communication technology, online banking was first introduced in Malaysia on June 1, 2000. Online banking allows customers of a bank or other financial institution to complete a range of transactions through the website. Especially due to Covid-19, it has given a significant boost to the digitalization of banking in Malaysia.

In general, the concept for traditional banking system is where it required the customers to visit the bank physically to carry out and complete their requirements, needs and wants, such as open account, funds transfer, money withdrawal and other services (Golden, 2016). In this case, the customer is required to set aside a long time to visit the bank branch and queue up at the bank to get the financial services demanded. On top of that, there is a limited parking lot for the customers to park their car, especially in the urban area. Hence, it is time consuming for customers on the traditional banking model.

On the other hand, according to Indra (2014), the company report stated that the current traditional banking system able to survive at the meantime, however, it encountered some problems or difficulties, which are the customers behavior has been changing due to the advancement of technology and the decline of the level of customer's satisfaction on the banking services offered. These unexpected difficulties coupled with the technology enhancement in the banking and financial sector has successfully transform the business model to digital online banking where it is only required one fingertip to enjoy the financial services that offered in the bank branch.

According to Pappu Rajan and Saranya (2018), digital banking is defined as the provision of financial services and products to the customers via electronic means, such as mobile phone, laptop, and tablet. Generally, it comprises a variety of banking activities that may be carried out from any location at any time. The services included transferring funds from one account to another account, paying bills, placing fixed deposits, investing in securities offered by the banks, looking up monthly bank statements and so on. Rupeika-Apoga et al. (2018) stated that modern financial technology is the driving force behind the developments occurring in the banking sector since the global banking sector has made digitalization a strategic priority in today's world.

In accordance with Galazova & Magomaeva (2019), from the customer perspective, there is few benefits gained from the online banking model. Firstly, customers are promised immediate transaction and action from online banking which has an unlimited time frame for the customer to carry out the banking activities. Next, the maintenance fees which the cost is charged by the banks is relatively low or free of charge compared to the brick-and-mortar bank business model where the customers are required to pay for a particular amount of transactions or maintenance fees for the services provided. Online banking offers unlimited scope of services where it do not limit the geographical location of the customers which is convenient to the customers living in rural area. For example, the foreign banks, OCBC Bank has a total of 38 branches in Malaysia (Branch locations, 2023). In this case, the online banking features provide advantages to the customers that live in rural areas to perform transactions easily.

However, there were a lot of fraud cases led by phishing through online banking, although there was never proof that local commercial banks were involved in security breaches. As stated in Chakrabarty (2013), fraud is defined as a person taking action that intent to acquire an unfair advantage over another person which will then leads to an imbalanced gain for two people, whether via the hiding of facts or another method. In addition, USI Web Services (n.d.) mentioned that fraud is the intentional use of dishonesty, false statements, the omission of information, or other unethical tactics that others are led to believe and rely upon in order to get an unauthorized advantage, either for oneself or for the institution in some circumstances, a criminal may mislead an individual into making a fraudulent money transfer on their own. Online banking fraud is a type of identity theft where the fraudsters obtain access and transfer funds illegally from a person's online bank account which is often made possible by techniques such as phishing.

In general, phishing is a form of social engineering assault that is frequently employed to obtain the user's information, such as login credentials and credit card details. It happens when an attacker deceives a victim into opening an email, text message, or instant message by disguising themselves as a reliable source. Next, when the recipient is deceived into clicking a fraudulent link which can cause malware to be installed on the recipient's computer, a ransomware assault to lock it down, or the disclosure of private data. In fact, the Malaysian Police has disclosed a warning not to click on a widely circulated URL promoting a spurious Petronas lucky draw (B, 2022). According to Bukit Aman's director of commercial crime investigations from Free Malaysia Today (2022), Kamarudin Md Din mentioned that the link would lead users to a phishing website through chat messages. After accessing the link, users will be instructed to complete a survey question that is intended for the purpose of obtaining user information.

Nevertheless, the banks have implemented sufficient security measures to ensure the security of online banking systems, however, there are many fraudulent emails or scam banking websites designed to trap bank users. As a result, it is critical to avoid searching for unknown links and should seek the banks' confirmation instead. This is due to the fact that banks would never send any online advertising messages for upgrades to bank accounts. Since there are multiple relevant instruments or systems to deal with it, online banking fraud has not been distinguished by the association of banks in Malaysia as a threat to banking services. Besides, in order to protect customers' personal information, banks and other financial institutions should raise the awareness of their customers in terms of fraud strategies to ensure it is secured. For the users themselves, they should be cautious about clicking on suspicious links or exposing their passwords to unknown parties on websites.

## 1.2 Problem Statement

Over the centuries, fraud has gone hand in hand with money. From the smallest of opportunistic scams to bigger, more structured groups working towards the same fraudulent goal. Wherever there have been financial opportunities, there have also been fraudsters planning their execution. The earliest recorded instance of fraud can be traced as far back as the year 300 BC in Greece (Faith, 2015). Hegestratos, a Greek sea trader, purchased an insurance policy against his ship and cargo in order to protect them. At the time, the policy was known as a bottomry and operated on the principle that a trader borrowed money according to the worth of his ship and cargo. The loan was repaid with interest as long as the ship arrived at its destination safely with all of its cargo intact. For sure, the boat and its cargo were seized if the loan was not paid back upon safe delivery.

As computers began to play a role in banking and finance, the stock market expanded dramatically both in size and speed. While many earlier frauds made use of technology, it was not until the late 1980s that fraud that was totally electronic began to become widespread (Marshall, 1999). Attempts were made to persuade people to contact expensive premium-rate numbers in an early scam that exposed gaps in the laws governing premium-rate telephone lines.

In 1994, the rise of eCommerce opened the way for the first instance of online credit card fraud. An early instance involved thieves using cards made out to a famous person to make expensive purchases. There was a brief period when this strategy was effective before cards could be instantaneously checked online. Due to this, sellers and fraudsters have been competing to keep one step ahead of one another ever since. However, there

was a case of Baring Bank that disclosed a devastating lack of supervision in financial reporting that caused in the collapse of the UK's oldest investment bank in 1995 (A., 2021). Nick Leeson, the head of derivatives of Barings Bank Singapore, triggered a catastrophic financial crisis for the bank that resulted in its ultimate failure. In order to conceal his actions, the rogue trader took unhedged bets worth over US\$1 billion on the markets and falsified internal accounting records. When the markets failed to turn in their favour, the losses increased. Interestingly, Leeson's actions were discovered through a letter of admission delivered to the head of the bank as his losses increased, not through internal audit or supervision.

In the context of Malaysia, there has recently been an increasing number of internet banking fraud instances which has raised concerns about the security of Malaysian banking institutions. As stated from Nair (2022), Malaysia has lost a total of RM415 millions to scammers in the first half of 2022, it is obvious that the amount of money being scammed has reach to an eye-popping level. Supt Mohamad Musa Marsidi, deputy head of the Kuala Lumpur Commercial CID, said that the 54-year-old victim filed a report on April 1, 2022, after realizing he had been duped whereby the victim had arranged for an RM80,000 loan by filling out a form with an online money lending company that claimed to give low-interest loans. The victim was after that called by a corporate representative who demanded payment for the loan processing and was required to send money in stages to nine accounts totaling RM243,000 from February 28 to the end of March when the loan was approved (Mail, 2022). Besides that, the Democratic Action Party (DAP) Sarawak chairman, Chong Chieng Jen stated that Malaysian banks' online security measures appear so porous that anyone could unknowingly fall victim to internet banking fraud and forfeit their savings (Borneo Post, 2022).

Besides, according to Dewan Rakyat, 51,631 online fraud instances were registered from 2019 to 2021 which has resulted in a loss of RM1.6 billion. In addition, Deputy Home Affairs Minister Jonathan Yasin has disclosed that there are more than 18,800



cases involved in online purchase fraud, while 15,546 cases featured bogus loans tied to sales (Azhar, 2022). In addition, Table 1.1 shows the new and unknown media content would tempt users to click to enter the screen and direct them to the payment fraud website. Moreover, Covid-19 pandemic is another driver for the increasing number of cases of online banking fraud where the number of transactions using online banking has been increasing where it has given the opportunity to the scammer to take illegal action stated by the group president and chief executive officer of Maybank.

Table 1.1

*Number of new unknown media content received by MCMC, Malaysia in 2019 and 2020.*

Elements of complaints	2019	2020	YoY (%)
Obscene	850	1,637	92.6
False	3,050	6,637	117.6
Offensive	2,312	4,535	96.2
Indecent	188	373	98.4
Menacing	88	151	71.6
Others (outside the jurisdiction of the CMA 1998)	3,938	7,472	89.7
Total	10,426	20,805	99.5

Source: Malaysian Communications and Multimedia Commission (2021)

While the number of online banking frauds is still increasing lately, according to one report, Thesundaily (2021), males are more likely than women to fall victim to online shopping scams over the past 5 years as stated by the Royal Malaysia Police (PDRM). 9,993 out of 17,520 victims who had their identities stolen through online transactions between 2017 and October of 2021 were men, according to Deputy Home Minister II Datuk Jonathan Yasin. On the other hand, Jonathan revealed that in the category of

non-existent fraud loans, there are a total of 8,264 victims who are men and 6,624 women.

In addition, there were a total of 814 incidents recorded in 2012, with losses of around RM33.61 million. However, in 2013, the number of cases increased to 1,095 resulting in losses of RM35.69 million (Hamsi et al., 2015). According to data obtained from Bukit Aman, 2,747 individuals were arrested in 2013 as a result of fraud, which also includes crimes such as love scams. For instance, there was a victim reported in one case on November 21, 2012. She was a bank customer services officer who had lost her mother's savings totaling around Ringgit Malaysia RM61,200.00 to a man she befriended on Facebook. The woman transferred RM47,000.00 on March 15 and RM14,200.00 two days later into three different bank accounts via online banking. But the bank accounts were in the names of individuals that she was not even familiar. After receiving the money, the person could no longer be reached.

The seriousness of the issue of online banking fraud has caught the attention of Bank Negara Malaysia (BNM) to announce on few solution for combating and preventing the happened of such cases where the BNM has improved the authentication method as SMS One Time Passwords (OTP) has been removed and replaced to a more secure method of authentication for online transactions or activities related to account opening, fund transfers, and payments, as well as modifications to personal data and account settings. (BNM: Banks to migrate from SMS OTP to more secure forms of authentication, 2022). In addition, the financial institutions will be facing further tightening of the regulations and triggers for rejecting scam-related transactions which wish to minimize the possibility of fraud. For example, customers should immediately know and be aware when their account has been detected with some activities that is abnormal and the bank should block the transaction or activity. On the other hand, from the customer perspective, BNM has restricted customers to authenticate transaction by using only one mobile devices. BNM also set up a specific hotline for customers to report the cases of online banking fraud (Migrate from OTP texts to curb online scams, BNM tells banks, 2022).

On the other hand, people always thought that the elderly are the group that most easily encountered online banking fraud where they were less internet savvy. However, according to a recent study, only 25% of British between the ages of 18 and 34 are adequately wary of phone emails and texts (Malay Mail, 2022). To be specific, the probability of the elderly respondents fell into fraud in only encounter for 11% which is partially because younger British overlook red flags like the spelling and grammar of fraudulent emails and SMS messages. This has shown that their online banking fraud awareness is relatively lower. These statistics are supported by the Better Business Bureau's survey research where the study stated that younger persons are far more likely than older adults to fall into fraud, whereby the percentage of the group aged of 20 – 29 that fall into fraud is 44% where the figure is nearly double up compared with the 20% for group age of 70 – 79 (Auto, 2021).

## **1.3 Research Objectives**

### **1.3.1 General Objective**

This study aims to identify the influencing factors of online banking fraud awareness in UTAR.

### **1.3.2 Specific Objectives**

Four specific objectives are established to achieve the general objectives as followings:

1. To examine the relationship between personal financial distress and fraud awareness in UTAR Kampar.
2. To examine the relationship between empathy and fraud awareness in UTAR Kampar.
3. To examine the relationship between knowledge of online banking and fraud awareness in UTAR Kampar.
4. To examine the relationship between attitudes towards fraud and fraud awareness in UTAR Kampar.

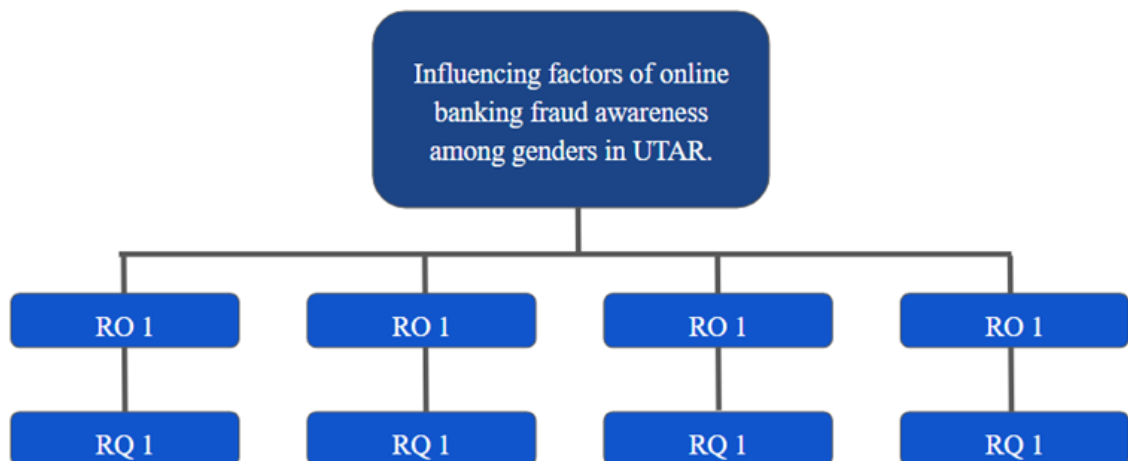
## 1.4 Research Questions

The 4 research questions will be answered by the data collected from UTAR Kampar campus and it also provide a clear direction for the research study, where it is as below:

1. Is there any significant relationship between personal financial distress and online banking fraud awareness in UTAR Kampar campus?
2. Is there any significant relationship between empathy and online banking fraud awareness in UTAR Kampar campus?
3. Is there any significant relationship between knowledge on online banking and online banking fraud awareness in UTAR Kampar campus?
4. Is there any significant relationship between attitude towards fraud and online banking fraud awareness in UTAR Kampar campus?

Figure 1.1

*The relationship between Research Objectives and Research Questions.*



## **1.5 Significance of the study**

The purpose of this study is to investigate the factors of online banking fraud awareness. In evaluating fraud in Malaysia's online banking system, it is important to determine independent variables that might affect the level of fraud awareness. A few factors account for most online banking fraud cases, such as personal financial distress, empathy, knowledge concerning online banking, attitude towards fraud. Individuals may not be aware of these fraud issues that occur in online banking, or maybe some people do not give alert during their online purchases, contributing to the tragedy of increasing online fraud rates. Consequently, this study helps to provide a by more comprehensive understanding of the problems encountered by the online banking user in their online experiences. Upon completing the survey, individuals will be able understand the factors and determine their level of alertness in this fraudulent issue. In this way, individuals can learn how to use online banking more effectively to avoid falling into the trap of fraud.

As a result of this study, Malaysia's online banking system can be made more secure and fraud rates will be reduced. The bank should formulate security plans and procedures that are the best in the industry and have backup and contingency strategies of the highest quality. By identifying which methods are more effective in dealing with different types of fraud in the ecosystem, this study will try to explore some ways for banks to improve their security standards. Banks should not solely rely on one method to combat fraud; instead, they should have a system of checking and upgrading outdated techniques to more advanced ones. To gain insights into banking security and determine the reasons for the happening of fraudulent activities on online transactions, the quantitative study analyzes the experiences of online fraud victims help a lot.

Furthermore, this study assists government agencies in reducing fraudulent activity by implementing policies. Through it, the government can have an idea of how to implement the best practice of good governance to reduce financial fraud in

government policies. For financial crimes to be prevented, governments seek different remedies since detection isn't always easy. For example, National Cyber Security Agency (NASCA) in Malaysia, it has the role of formulating a practical solution to combat banking frauds, spurring cyber security alertness and consolidating the cyber security recommendations to Bank Negara Malaysia (BNM) (Cyber Security Strategy to Provide Direction on Curbing Cyber Threats, 2020). As well, NACSA must always keep government agencies informed of new cyber threats in order to secure and strengthen Malaysia's resilience in the face of cyber-attacks. These findings will greatly assist all these government agencies in making Malaysian policy decisions.

According to data from 2020 to May 2022, 68% of all Malaysian commercial crime cases were related to online fraud (Online Fraud Accounts for 68% of Commercial Crime, Says IGP, 2022). In turn, it is important to investigate the awareness level of Malaysians who are currently using online banking systems and their attitude towards online fraud in order to accomplish the main goal of this paper. In light of the fact that online banking fraud activities can affect a country's reputation and even its economic growth, it is important to contribute new knowledge to the literature in this area. In the future, this overview will draw attention to new paradigms that will be useful for discussions of the online fraud trend and could contribute to a more comprehensive analysis. Study contributors focus on cybercrime at a time when globalization of the Internet is accelerating.

## **1.6 Conclusion**

In conclusion, the issue of online banking fraud is a hot topic recently where the number of cases is high and the amount being fraud is huge. From here, the researcher would investigate the influencing factors of online banking fraud awareness in UTAR Kampar

campus to achieve the research objectives and answered the research questions. The 4 factors are personal financial distress, empathy, knowledge on online banking, and attitude towards fraud.



## **CHAPTER 2: LITERATURE REVIEW**

### **2.0 Introduction**

In this chapter, the researcher will be discussed on the dependent variable and independent variables by review the variables to identify the correlation between the dependent variable of fraud awareness and the independent factors of personal financial distress, empathy, knowledge on online banking and attitude towards fraud. Additionally, a discussion of the conceptual framework and underlying theories is conducted. Finally, this chapter constructs the hypothesis.

### **2.1 Underlying theories**

The research is utilizing several theories to investigate the objectives of the research. The theories that will be used are Theory of Planned Behaviour, Protection Motivation Theory and Technology Model. In the below section, all the theories will be deeply discussed.

### **2.1.1 Theory of Planned Behavior**

The Theory of Planned Behavior, also known as TPB, refers to how a person's intent to act is affected by their beliefs and values, their sense of agency, and the subjective standards of their social group. If someone is pessimistic and thinks they won't be able to influence the consequences of their actions, they may be less likely to take part in the activity (Ajzen, 2020). According to the concept of this theory, TPB suggests that an individual's behavior is determined by their intentions, which are shaped by three factors: attitudes, subjective norms, and perceived behavioral control. The theory is linked with the attitude as it explains to an individual's positive or negative evaluation of a behavior and how they are affected by beliefs about the behavior's outcomes. In the context of fraud awareness, an individual's attitude towards fraud can be affected by their beliefs about its consequences, such as the potential harm it can cause to individuals and society. Therefore, by using TPB to understand the relationship between fraud awareness and attitude, one can examine the beliefs and attitudes of individuals as well as the social and personal factors that may influence their behavior.

The Theory of Planned Behavior (TPB) proposes that an individual's actions related to financial fraud and their financial stability are influenced by their perception of control over their finances and their personal beliefs regarding financial responsibility. TPB suggests that individuals who are not aware of financial fraud may have a pessimistic outlook on financial responsibility and may be disinclined to take precautionary measures to manage their finances, which can heighten their susceptibility to financial difficulties. Those who feel in control of their ability to prevent fraud, perceive social norms that encourage this behavior, and have a positive attitude towards preventing financial fraud may be more likely to take action to safeguard themselves (Burns & Roberts, 2013).

### **2.1.2 Protection Motivation Theory**

The protection motive theory, also known as PMT, is a conceptual framework that is frequently applied in the study of how people react when confronted with stimuli that cause them to perceive that they are in danger. Fear messages that motivate individuals to take preventive measures or to withdraw from behaviors that might hurt themselves or others are examples of these triggers. This idea can be placed within the category of expectancy-value theories, which hold that a person's beliefs or attitudes will eventually lead to actions (Wang et al, 2019). The PMT hypothesizes that individuals go through a process of danger assessment and coping evaluation in order to evaluate potential responses. The process of evaluating threats involves determining both the seriousness of the danger and the likelihood (or exposure) of it occurring. Vulnerability is another word for likelihood. The process of coping assessment involves thinking about whether or not the reaction is effective, how challenging it is to execute the response (in terms of, for example, response cost), and how confident the individual feels in their ability to carry out the coping response (Shafiei and Maleksaeidi, 2020). The theory is linked with empathy as it explains that to feel compassion for another person is not an immediate reaction to their pain; rather, it is a social bridge that helps individuals connect with one another. Rather, it is a phenomenon reflecting the approach and avoidance motivations that lead people to participate in or refrain from it. For instance, if someone is empathic, they may be more likely to recognise the emotional impact that fraud has on innocent victims, which could raise their perception of threat and lead them to take defensive action.

The idea proposes that two important variables, perceived threat and perceived efficacy, influence an individual's decision to participate in preventive activity. Perceived threat refers to how a person believes in their ability to effectively fight off the threat, whereas perceived efficacy deals with how serious and likely they think the threat to be (Lee et

al., 2023). When referring to fraud, the term perceived threat can refer to both the potential for becoming a victim of fraud as well as its likely financial and emotional consequences. A person's self-assurance in their capacity to spot and avoid situations involving fraud as well as their knowledge of the steps they can take to protect themselves from fraud may be factors in perceived efficacy. Financial stress can influence both how a threat is viewed and how effective it is. For instance, if someone is experiencing financial difficulties, they can see the threat of fraud as being more serious because the potential financial penalties of fraud could be more harmful. Also, experiencing financial difficulty may make someone feel less effective because they may doubt their abilities to protect oneself from fraud. Hence, PMT could be a useful framework for understanding the relationship between fraud awareness and personal financial distress.

### **2.1.3 Technology Acceptance Model**

The Technology Acceptance Model (TAM), also known as TAM, is considered the most significant and widely used theory for characterizing an individual's acceptance of information systems. According to the concept of this theory, there are several factors that influence technology acceptance, which included perceived ease of use and attitude towards using the technology (Granic and Marangunic, 2019). Users who are more aware of the risks of fraud and have a better understanding of how online banking works are more likely to accept and use online banking technology as well as more useful in terms of managing their finances such as providing access to account information, transferring funds as well as paying bills, and avoiding fraud. This is because they perceive technology as more useful and easier to use, which can lead to a more positive attitude towards this digital era. The theory is linked with knowledge of online banking as it explains to the users' understanding of the features and functionality of online banking. In addition, perceived ease of use can be related to

users' perceptions of how easy it is to navigate and use online banking such as by accessing their accounts and making transactions (Jones, 2009). Based on Rahimi et al (2018), adopting technology can contribute to the enhancement of people's lives in a number of ways. Literacy in data is a crucial ability that has a utilitarian character because of the positive impact it has on a vast number of people who adopt the knowledge (Rahimi et al, 2018).

According to this theory, it can be hypothesized that the users who are more aware of fraud and have more knowledge of online banking are more likely to perceive online banking as useful and easy to use, which in turn increases their intention to use it. Davis (1989) posited that the perceptions of ease of use and usefulness were key indicators of consumers' intentions to adopt a new technology. In summary, relating TAM towards the relationship between fraud awareness and knowledge of online banking involves understanding how users' perceptions of the usefulness and ease of use of online banking are influenced by their fraud awareness and knowledge of online banking. By examining these relationships researchers can develop interventions to increase users' fraud awareness and knowledge of online banking which can improve their acceptance and use of online banking.

## **2.2 Review of variables**

The research topic is estimating the influencing factors of online banking fraud awareness in UTAR. In this research, dependent variable is fraud awareness while the independent variable is personal financial distress, empathy, knowledge of online banking and attitude towards fraud.

### **2.2.1 Fraud Awareness**

A dependent variable is one that can be predicted or used to interpret another variable. In today's culture, fraud is a widespread issue that has the potential to lead to major financial losses, injury to one's reputation, and even harm to persons and groups. Fraud can happen in the context of financial transactions in a number of ways, including through credit card fraud, identity theft, and investment schemes. Fraud awareness is a key factor that people can use to recognize and stop fraudulent behaviour, which lowers the financial and emotional costs associated with fraud.

Fraud awareness is described as an initiative to educate all levels of the Bank's institution and various parties connected to the Bank about the value of fraud prevention. Fraud awareness includes the understanding of the risks, consequences, and types of fraudulent practices involving all organization-wide components (Ramadhan, 2022). Fraud awareness is a complex attribute that includes a person's capacity to spot and react to dishonest activity. The capacity to recognize fraud warning indicators, the desire to report suspicious activity, and the ability to take preventative steps are just a few examples of the cognitive and affective components that go into it. Self-report surveys and behavioural tests are both effective ways to gauge fraud awareness.

Understanding fraud contributes to shaping fraud awareness so that everyone in the organization is aware of their responsibilities for preventing, identifying, and responding to potential fraud risks. Raising fraud awareness among people can aid individuals in spotting potentially dangerous behaviour down the line and protect profitability. The need for continuous alertness from all parties will be reinforced by reminders and increased awareness, which will help foster a culture where everyone is

risk-averse and accountable for defending one another's interests. Additionally, there is an urgent need to inform the public about new and growing fraud concerns.

People nowadays and financial institutions must adapt in this situation, especially regarding the use of digital technology. Currently, financial institutions must deal with both cyber and non-cyber risks, including lending and internal fraud. Cyber risks include illegal financial transactions through online banking. The likelihood of digital fraud has increased as more people use digital transactions, which gives fraudsters more possibilities. Technology has been used by fraudsters to increase the complexity and scope of their activities. Via technology, scammers can carry out worldwide scams with surprising simplicity and constantly change their strategy to uncover new weaknesses. Thus, people must have a high level of fraud awareness in order to recognize fraud traps and be aware of possible solutions.

Fraud knowledge is a crucial component of fraud prevention and detection, according to research. For example, research conducted by the Association of Certified Fraud Examiners (ACFE) discovered that firms with higher levels of fraud awareness experienced lower fraud losses and shorter fraud durations than those with lower levels of knowledge (ACFE, 2020). Also, people who are more aware of fraud are less likely to become victims of fraud schemes, protecting them from losses in money and reputation. Fraud awareness is essential when conducting business online because it's simple for scammers to pass as reliable companies and people in order to acquire sensitive data. Identity theft was the second most reported type of fraud in 2020, according to the Federal Trade Commission (FTC), with more than 1.3 million reports (FTC, 2021). Those who are aware of fraud can avoid fraudulent transactions, secure their online accounts, and spot phishing frauds.

Besides, regulators like Bank Negara Malaysia and the Securities Commission of Malaysia have launched a number of ongoing campaigns to highlight the issues that investors should watch out for when making online transactions. They also publish the

Financial Fraud Alert List as a guide to raise awareness of entities or schemes that may have been wrongly assumed to be licensed or controlled by the regulatory agencies or mistakenly represented as such (Bernama, 2022). The banking sector is placing a high priority on these fraud awareness concerns and has continued its efforts to combat and inform consumers about scams by launching the National Scam Awareness Campaign (NSAC) in conjunction with the Financial Literacy Month 2022 (FLM 2022) exhibition.

In conclusion, fraud awareness is a crucial element in preventing and detecting fraud, with enormous ramifications for people, companies, and society at large. We can create more effective tactics for promoting fraud prevention and detection and lowering the costs and hazards associated with engaging in fraudulent behaviour by studying the elements that influence fraud awareness.

### **2.2.2 Personal Financial Distress**

Several research have investigated the connection between fraud knowledge and personal financial suffering. The degree to which people face financial issues or hardships, such as debt, unemployment, or foreclosure, is referred to as personal financial distress.

When someone is experiencing financial distress, such as tension from debt or an inability to fulfill responsibilities, they are anxious about their finances. Personal finances are negatively correlated with financial stress. These two factors will constantly be in opposition, which will cause financial stress to have a bad impact on financial well-being. The conceptualizations of financial distress, shortage, and shock are connected to the fact that people suffer from financial difficulties on an emotional



and physical level. The financial distress framework is used to employ indicators of financial well-being like creditworthiness, the total count of available emergency funds, the distribution of monthly card payments, monthly repayments, monthly allocations of funds for savings, and future pension preparation because of financial well-being (Mansor et al., 2022).

Financial stress is a complex combination of financial obligations and a lack of finances. A subjective evaluation of one's financial condition, including perceived ability to pay bills, satisfaction with someone's economic state, level of investments and savings and concern about indebtedness, is known as financial stress (Kim & Garman, 2003). Financial stress, taken in its fullest sense, conflicts with regular financial management, such as being inadequate, and usually implies psychological stress. Nevertheless, given that individuals are in financial stress and embark down the road to significant losses, this relationship might have an impact on people's awareness towards fraud.

Huang et al. (2020) 's study investigated the connection between personal financial difficulty and fraud awareness in China. The researchers examined the levels of personal financial distress and fraud knowledge among 782 Chinese individuals. According to the study's findings, lower levels of fraud awareness were correlated with higher degrees of personal financial distress. This implies that those who are having trouble making ends meet may be less likely to be aware of the possibility of financial fraud, which may make them more open to fraudsters.

Another study by Rezvani et al. (2016) looked at the connection between older persons' awareness of fraud and personal financial difficulty in the US. The researchers gathered information from 1,250 older persons and assessed their degrees of financial literacy, financial distress, and awareness of fraud. Even after accounting for financial literacy, the study's findings revealed that higher degrees of individual financial distress were linked to lower levels of fraud awareness. This shows that when developing

interventions to increase older people's awareness of and ability to recognise fraud, financial suffering may be a crucial element to take into account.

Overall, these studies indicate that it may be crucial to take personal financial suffering into account when analyzing the association between fraud awareness and other variables like age, gender, and financial literacy. Those who are struggling financially may be more susceptible to financial fraud than other people, so targeted interventions to raise their knowledge of potential scams and fraudsters may be beneficial.

### **2.2.3 Empathy**

One aspect of social concern and the capacity to identify and emotionally engage with others' emotions is empathy. The relationship between empathy and other aggressive behaviors has been the subject of significant research. Evidence has consistently demonstrated that empathy is linked with criminal activity, acceptance of online abuse, cyberbullying and so on (Choi et al., 2022). People who have empathy are better equipped to maintain their moral beliefs without being forced to compromise them in order to fit in or behave in a way that will make them worse off.

It takes a certain amount of empathy and self-awareness to manage interactions with suspected scammers. Understanding personal attitude can help people close the gap in an encounter if people notice the counter part is a scammer. Having empathy for fraudsters can assist individuals in understanding how the fraudsters defend their acts because many of them don't consider themselves as horrible people but rather as good individuals who committed a negative thing. In consequence, people in empathy behavior will be highly cautious during using online banking transactions, since morality ethics have provided insight into how to combat fraud all the time.

In a study by Liang and Chen (2019) had investigated the connections between self-efficacy, moral identity, and financial fraud reporting. The researchers gathered information from 212 Taiwanese workers across a range of industries, assessing their degrees of self-efficacy, empathy, and moral identity as well as how likely they were to report financial wrongdoing. Even after accounting for moral identity and self-efficacy, the study's findings revealed that higher levels of empathy were positively associated with higher levels of financial fraud reporting. This implies that those who are more empathic may be more likely to notice and report instances of financial fraud, which may help spread awareness of and prevent fraud.

With empathy sensitivity, a person can evaluate a situation in terms of the potential consequences and those who might be impacted by each course of action. Using empathy judgment, a person determines what to do in that specific circumstance due to the fact that the person needs to act morally and make ethical decisions that can avoid falling into any scam. According to the research, the intention to report misbehavior to authorities within the organization with the purpose of not covering up the evil things done by the fraudsters is predicted by higher rates of empathy (Hildebrand & Shawver, 2016).

The study by Kouchaki et al. (2020) looked at the connection between empathy and dishonesty. Researchers examined participants' degrees of empathy and participation in dishonest behaviour through a series of tests involving 3,557 participants. The study's findings demonstrated that those who scored higher on empathy tests were less likely to commit fraud themselves. The researchers hypothesised that this would be because people with higher degrees of empathy may become more concerned about other people's wellbeing, which might make them less likely to engage in actions that might hurt others, like financial fraud.

Ma-Kellams and Blascovich (2011) investigated the connection between empathy and the capacity to spot fraud. The researchers tested 150 undergraduate students in a series of trials to gauge their empathy and ability to spot deception and lying. Higher degrees of empathy were linked to more accurate lie detection, according to the study's findings, but they had no discernible relationship with people's general capacity to spot fraud. According to this study, the connection between empathy and fraud awareness may be more nuanced than previously believed. Although greater empathy may be linked to greater accuracy in detecting lies, this association does not necessarily imply greater capacity to detect fraud. This may be since identifying fraud frequently necessitates knowledge of the various types of financial fraud that may occur in addition to a more thorough understanding of financial systems and rules.

Overall likewise, these studies point to a potential link between empathy and fraud awareness/prevention actions, as those who have higher levels of empathy may be more likely to spot and report cases of financial fraud and less likely to engage in fraudulent behaviour themselves. It's vital to remember that because these studies are correlational, it is not possible to infer a causal link between empathy and fraud knowledge or prevention. To further understand the mechanisms underlying this association and to find efficient strategies for raising fraud awareness and preventing financial crimes, more study is required.

#### **2.2.4 Knowledge of Online Banking**

Knowledge of online banking is the set of abilities and information that enables a person to make good use of their financial resources wisely and effectively. People that are financially literate will be capable of improving their budgeting abilities, comprehend credit, and develop spending and saving plans. With the knowledge of

financial concerns, people may be familiar with the tips and tricks of online banking nowadays and see through the authenticity of the transactions. With financial knowledge, the essential components such as budgeting, personal financial management, and borrowing can be safely transacted.

The Organization for Economic Co-operation and Growth (OECD) describes financial literacy as knowledge about financial concepts, risks regarding information, and financial attitude (Mohd Padil et al., 2021). As a sense, someone who is financially literate has the abilities, desire, and consciousness to use skills and knowledge to make decisions in a variety of financial circumstances. When the people are unable to control their desire to live a luxurious lifestyle as represented by the lower financial literacy, people with lower degrees of self-control are more likely to be identified as fraud victims.

Making financial decisions is probably becoming more difficult for consumers, which worsens the issues brought on by frauds and scams. Knowledge of financial concerns is coming together to show how important it is to make cautious and knowledgeable financial decisions. When a person has high financial inclusion, those who will eventually achieve financial security, which is described as having enough money to support the lifestyle while moving toward the financial goals.

Much research has examined the connection between these two factors, looking at how understanding online banking affects actions related to fraud awareness and prevention. For instance, a study by Jones and Schilling (2019) discovered that greater adoption of fraud prevention practises, such as routinely reviewing bank statements and changing passwords, related to higher levels of knowledge about online banking. Similar to this, Wang and Wang's study from 2020 found that those who had more understanding about online banking were less likely to become victims of phishing scams and other forms of online banking fraud.

However, some research has revealed contradictory results, with some showing that having more information about online banking does not always translate into more vigilant fraud awareness or preventative measures (Chin et al., 2018). Several research have identified demographic and psychological variables including age, gender, and risk perception that may function as moderators in the association between knowledge of online banking and fraud awareness (Bagnoli et al., 2017; Liao et al., 2021).

There are still gaps in the literature despite the extensive research on these topics. For instance, very little research has looked into how technical literacy or education influences people's understanding of online banking and fraud awareness.

### **2.2.5 Attitude towards Fraud**

The standards define a fraud attitude as a state of mind, set of moral principles, and justification for fraudulent activity. An important factor connected to fraud awareness that has been researched in the past is attitudes against fraud. As "evaluative assertions or judgements involving objects, people, or events," attitudes are described (Eagly & Chaiken, 1993). Individuals' opinions or ideas about fraud, whether favourable or unfavourable, are referred to as attitudes towards fraud. Although it is often emphasized how essential mindset is in determining fraud risk, it is also crucial to consider how consumers perceive the threat of fraud and what security precautions people consider are necessary when transacting money online. Although people are aware of the terms associated with fraud, attitude toward fraud risk measures whether people believe that they have a deep understanding of it (Wilkes, 1978). Since identifying security measures is a key concern in the banking industry, this is mainly because fraudsters will often benefit from this expertise and pay much closer attention than genuine customers who have lower attitude towards fraud risk.

Since they may affect how seriously people take fraud, how eager they are to take steps to prevent it, and how likely they are to report it, attitudes regarding fraud are crucial. For instance, those with negative attitudes towards fraud may be more inclined to consider fraud as a serious issue and take precautions against it, such as routinely scrutinising financial documents and exercising caution when disclosing personal information. Those who have a favourable attitude towards fraud, on the other hand, can be more inclined to engage in fraudulent behaviour or less likely to report fraud when they see it.

Past studies have investigated the demographic, personality, and risk tolerance aspects that affect attitudes against fraud, as well as demographic parameters including age, gender, and education. For instance, studies have indicated that people with high moral standards or poor risk tolerance are more likely to have unfavourable opinions of fraud (Button & Brooks, 2012). Similarly, studies have indicated that those with higher incomes or educational levels are more likely to have unfavourable opinions against deception (Greenberg, 2016).

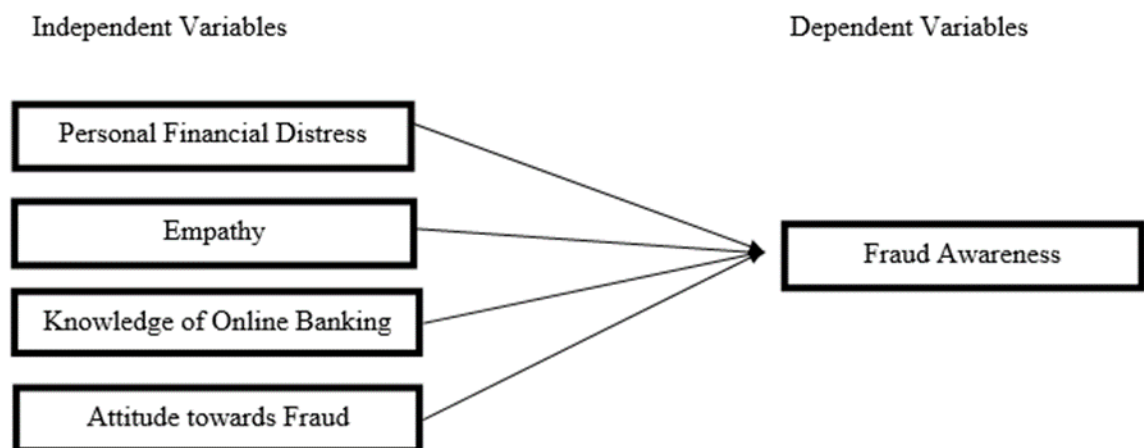
A range of techniques, such as self-report questionnaires, in-person interviews, or behavioural assessments, can be used to gauge attitudes about fraud. Self-report surveys frequently question participants to rate how much they agree with statements like "Fraud is a big problem in society" or "I would never engage in fraudulent activities." Interviews can reveal more detailed information on people's perspectives on fraud and the elements that shape these perspectives. Behavioral measurements, such as watching people's responses to fraudulent tasks or circumstances, can offer a more impartial indicator of attitudes towards fraud.

In conclusion, attitudes about fraud are a significant factor associated with fraud awareness that has been researched in the past. Individuals' attitudes can affect how seriously they take fraud, how eager they are to take steps to prevent it, and how likely they are to report it. Future studies should continue to look at the variables that affect attitudes about fraud and how they connect to other elements of fraud awareness.

### 2.3 Conceptual framework

Figure 2.1

*Conceptual Framework.*



Source: Develop for the Research

Based on the theoretical models, the diagram above proposed a conceptual framework to illustrate the relationships between independent variables (personal financial distress, empathy, knowledge of online banking and attitude towards fraud) and dependent variables (fraud awareness). In this research, the relationship between the dependent variable and the 4 independent variables has been examined.



Personal financial distress is the inability of a person to feel secure in their financial situation to the point where the financial issues stress them about their mental wellbeing. To better their financial status, they make an effort to make wise financial decisions such as spending, saving, borrowing, and other actions. The physical impacts of stress include bad financial circumstances and a multitude of health issues. In reality, financial satisfaction moderates the relationship between these determinants and personal well-being, with some individual differences. How much credit someone owes, how effectively they can handle financial shock, how well they can diversify their investment portfolio, and how much stress they can take before becoming financially independent until they become less aware of fraud all have a direct impact on their financial situation.

Empathy is a good way to observe people who are more likely to forgive or empathize with cases of fraud and think that it is best to avoid fraud and be cautious when doing online transactions. This is because empathic people are more self-aware and sensitive to others, which might adequately protect us from negative actions. Currently, there is little research on how individual differences and contextual factors impact susceptibility to such forms of malicious influence on online banking systems. In a recent study, researchers found that a small number of victims are at risk of being victimized again by fraudsters. The problem is that people tend to underestimate the vulnerability of phishing attacks based on factors such as different behavior (Williams et al., 2017). This demonstrated how ethics in real life can aid in preventing and discouraging fraudulent incidents through fraud awareness because morality allows people to discriminate between right and wrong without acting on emotions.

Financial literacy, which includes knowledge of online banking, can provide people the skills they need to become more aware of fraudulent conduct, best equipped to detect fraud, and more able to avoid fraud. This framework examines the role of financial

literacy in detecting fraud using aspects of financial knowledge and financial behaviour. The purpose of this study was to determine whether more financially literate people would be better able to identify fraud incidents and assess fraud risk due to their increased financial knowledge and sensible financial behaviour. Consumers' ability to accurately identify fraudulent promotions is significantly influenced by their level of consumer literacy in relation to recognizing various financial marketplaces.

Generally, a change in attitude can make people aware of a risk. This is because it is crucial to understand risk attitudes and the effects, they may have on the risk management process if they are not acknowledged or controlled in order to identify fraud. For instance, if a person perceives a lack of appreciation from a certain fraud application, this may cause them to lose trust in the application and prevent them from performing transactions. This theoretical approach contributes to the discovery that attitudes towards fraud might introduce bias and negatively impact assessments of the risks of engaging in fraud.

## **2.4 Hypothesis**

In this section, hypothesis to investigate the relationship between dependent variables and independent variables have been developed and will be deeply discussed.

### **2.4.1 Fraud Awareness and Personal Financial Distress**

H<sub>01</sub>: There is no relationship between personal financial distress and fraud awareness.

H<sub>A1</sub>: There is a significant relationship between personal financial distress and fraud awareness.

A 2019 study looking at 400 Malaysian participants' degrees of financial distress and knowledge of online banking fraud was published in the *International Journal of Consumer Studies*. Financial distress was found to be negatively associated with general financial knowledge but not significantly with awareness of online banking fraud (Ali, Ismail, & Wahab, 2019).

The 2018 study, which was published in the *Journal of Financial Crime*, looked into the connection between financial hardship and UK consumers' awareness of financial fraud, especially online banking fraud. In their study of 297 participants, the researchers discovered no connection between financial difficulty and fraud awareness. Nonetheless, through its effect on financial literacy, the study discovered an indirect association between financial distress and fraud awareness. According to the study, persons who are in financial trouble may be less financially literate, which may influence their capacity to recognize and stay away from financial fraud, especially internet banking fraud. In order to raise consumer awareness of financial scams, particularly among individuals who may be in financial trouble, the researchers advise financial institutions and authorities to concentrate on enhancing financial literacy (Bene & Lee, 2018).

According to Dew, Stewart, & Kinsey (2017) study's findings, people who said they were in financial trouble were less likely to use online banking services and more likely to stay away from financial websites. The perceived vulnerability to online banking fraud between those who experienced financial difficulties and those who did not, according to the study, did not differ significantly between the two groups. This implies that although financial hardship may have an impact on online banking behaviour, it does not necessarily mean that people will be more aware of the risks associated with

online banking fraud. Overall, this study emphasises the necessity of heightened awareness and education regarding online banking fraud, as well as the significance of considering financial distress as a potential factor impacting people's online banking activity and information-seeking habits.

According to Jones and Han (2018) study's findings, there is a connection between personal financial suffering and fraud knowledge. In order to investigate the connection between financial stress, financial self-efficacy, and fraud susceptibility, the study interviewed 389 people in the United States. The study discovered that weaker financial self-efficacy and increased susceptibility to fraud, particularly online banking fraud, were related to higher levels of financial stress. The authors concluded that people may be less able to make wise financial decisions and more susceptible to deception as a result of financial stress.

To better understand the connection between financial distress and knowledge of electronic banking fraud in Nigeria, a study was conducted and published in the International Journal of Economics, Commerce and Management in 2016. The 384 participants in a study by the researchers revealed that they were more likely to be aware of and take precautions against electronic banking fraud if they had previously experienced financial difficulty. This implies that people who are struggling financially may be more watchful and cautious when conducting banking transactions, which may increase public knowledge of fraudulent activity in the electronic banking sector. In order to evaluate people's degrees of knowledge and readiness for electronic banking fraud, the study highlights the significance of taking financial misery into account (Adewumi, Aworinde, & Adewumi, 2016).

There is research conducted in 2015 which investigates the connection between financial stress and Americans' awareness of financial fraud. To do this, researchers polled 1,207 individuals in an online survey to learn about their experiences with financial stress and their knowledge of different kinds of financial fraud. The study's

findings revealed that people who said they were under financial stress were more likely to be aware of financial fraud and to take precautions against it. The researchers hypothesize that this might be caused by a heightened awareness of the need for protective measures brought on by financial stress, which in turn leads to a larger perception of susceptibility to financial risks (Huang, Soutar & Brown, 2015).

### **2.4.2 Fraud Awareness and Empathy**

H<sub>02</sub>: There is no relationship between empathy and fraud awareness.

H<sub>A2</sub>: There is a significant relationship between empathy and fraud awareness.

The purpose of the study by Razak, Dahalan, and Ahmed (2017) was to examine the connection between empathy and fraud awareness among Malaysian users of online banking. 409 users of online banking were polled by the researchers, who gathered information on their empathy and awareness of fraud. The findings revealed a link between empathy and fraud awareness, suggesting that people with higher levels of empathy were more cognizant of online banking fraud. This implies that people's views of online banking fraud may be greatly influenced by empathy, which may also increase their knowledge of potential threats.

The intention of Al-Aali and Tee's study conducted in Saudi Arabia in 2021 was to look at the connection between empathy and knowledge or awareness of online banking fraud. They conducted a survey of 286 Saudi online bankers and discovered a link between empathy and knowledge of and awareness of online banking fraud. The study concluded that consumers' knowledge and awareness of online banking fraud are significantly influenced by their empathy. To increase consumers' knowledge and awareness of online banking fraud, the authors advise banking institutions to consider

integrating empathy-building programmes into their fraud prevention and security policies.

In Bangladesh, Hossain, Sarker, and Rayhan (2021) investigated the connection between individual inventiveness, empathy, and knowledge of online banking fraud. They polled 200 users of online banking, and they discovered that empathy acted as a mediating factor in the association between personal inventiveness and awareness of online banking fraud. They concluded that empathy was crucial in raising people's knowledge and understanding of online banking fraud, which might therefore help prevent and lessen fraud in online banking transactions.

Teo and Yap (2019) investigated the impact of affective states and empathetic concern on 369 Singaporean online banking users' knowledge of security threats. They discovered that whereas affective states like anxiety and fear were significantly related to awareness of online banking security issues, including fraud, empathic concern was not significantly related. This implies that while emotional emotions can affect how aware people are of security vulnerabilities to online banking, empathy may not be a significant component in doing so.

Omar, Muda, and Zainuddin (2019) looked at the correlation between empathy and knowledge of online banking fraud among 200 Malaysian users of online banking. According to the study, there was no connection between participants' awareness of online banking fraud and empathy. Similar to this, Akhtar, Amin, and Azeem (2020) conducted a study of 360 Pakistani users of online banking to look at the connection between empathy and knowledge of online banking fraud. The findings demonstrated that there was no connection between the participants' awareness of online banking fraud and empathy.

### **2.4.3 Fraud Awareness and Knowledge of online banking**

H<sub>03</sub>: There is no relationship between knowledge of online banking and fraud awareness.

H<sub>A3</sub>: There is a significant relationship between knowledge of online banking and fraud awareness.

Researchers at the University of Kent, Blythe and Coventry (2019) undertook a study to examine the association between knowledge of internet banking and awareness of the risks associated with it. The study's participants were questioned about their understanding of online banking as well as the hazards associated with online banking fraud. Those who reported having more knowledge about internet banking had higher levels of perceived security, according to the study. This indicates that participants felt more secure using internet banking when they had more expertise. The study did discover, however, that this information did not always transfer into a heightened awareness of the hazards associated with online banking fraud. In other words, participants' increased sense of security did not necessarily translate into increased awareness of the specific hazards related with online banking fraud. This emphasises how crucial it is to grasp the hazards connected to online banking fraud in addition to having general knowledge of online banking. It also implies that in order to effectively lower the risk of online banking fraud, steps to raise awareness of those hazards, like focused education and training programmes, may be required.

Alzahrani and Goodwin (2018) from the University of Wolverhampton's study sought to determine the association between the frequency of online banking use, understanding of online banking, and awareness of the risks with online banking fraud. The study's participants were questioned regarding their online banking practices,

understanding of online banking, and awareness of online banking fraud. According to the study, those who used online banking more regularly were more aware of the risks associated with it. This implies that regular online banking users may be more exposed to online banking fraud and, as a result, may be more knowledgeable about the hazards associated with it. However, there was no connection between participants' knowledge of internet banking and their awareness of fraud dangers. It cannot be assumed that participants were more aware of the specific hazards related to online banking fraud just because they had more knowledge about online banking. Since understanding online banking may not be sufficient to completely comprehend the hazards involved with online banking fraud, this emphasizes the significance of focused education and training programmes to raise awareness of these risks. It also implies that proficiency with online banking may contribute to greater knowledge of hazards related to online banking fraud.

The University of Alabama study sought to examine the association between knowledge of online banking security measures and awareness of fraud concerns in online banking. The study's participants were questioned regarding their familiarity with online banking fraud threats and security features. The study discovered that participants who claimed to know more about online banking security features had higher degrees of awareness of the hazards associated with online banking fraud. Participants were more likely to notice potential online banking fraud dangers and take precautions if they were more educated about features like encryption and password protection. These results emphasize how crucial it is to inform online banking users about the security features and protocols employed in online banking systems in order to help them better understand the risks associated with online banking fraud. By learning more about these security elements, customers may be better able to recognise and steer clear of potential hazards from online banking fraud (Hoggatt, Leach, & Warren, 2016).



#### **2.4.4 Fraud Awareness and Attitude towards fraud**

H<sub>04</sub>: There is no relationship between attitude towards fraud and fraud awareness.

H<sub>A4</sub>: There is a significant relationship between attitude towards fraud and fraud awareness.

According to Rozmita Dewi YR and Irfan Ariandi (2017), one of the instructional tools underscores the significance of spreading public knowledge, or so-called fraud awareness, throughout every community. To play a more direct part in providing early warning and boosting the efficacy of risk management in carrying out the obligations and activities of governmental agencies, the inspectorate must modify its role in the transition that takes place. The creation of an early warning system, which will be referred to as such henceforth, is anticipated to help BPKP achieve its organisational objectives. The early detection system used in this study is to approach each in-house auditor in the Inspection with a fraud awareness attitude. The Ramamoorti et al. (2010) study looked at the connection between accounting professionals' awareness of fraud and their ethical attitudes and actions. The study discovered that ethical attitudes and behaviors, such as reporting fraud, were positively correlated with fraud awareness. Higher fraud awareness among accounting professionals was associated with greater likelihood of reporting fraud and ethical behaviour. Similar to this study, Bédard et al. (2015) looked into how accounting students' understanding of fraud related to their ethical thinking and actions. According to the study, ethical thinking and behaviour are positively correlated with fraud awareness. Higher fraud awareness among students was associated with more ethical behaviour and thought.

However, Albrecht et al.'s (2010) study, in contrast, discovered that although attitudes against fraud were associated to fraud awareness, the association was not statistically significant. In a sample of people who have reported fraud, the study looked at the association between awareness of fraud and attitudes towards it. The results imply that although attitudes towards fraud may be connected to fraud awareness, other factors

may have a bigger influence on how people view fraud. Krambia-Kapardis and Zopiatis (2017) also looked at the association between fraud awareness and attitudes among workers in the hotel industry. The study showed no connection between attitudes towards fraud and fraud awareness that was significant. The results imply that while fraud awareness may be crucial for stopping and identifying fraud, it may not always have an impact on people's views towards fraud.

The research by Pugazhendhi and Kanimozhi is another study that shows there is no correlation between fraud awareness and attitude towards fraud. (2019). The study looked at the association between fraud awareness and fraud-related attitudes among Indian banking personnel. According to the results, there is no connection between fraud awareness and attitude towards fraud. According to the authors, organisational culture and job satisfaction may have a bigger impact on employees' attitudes towards fraud than other aspects. Similar to this, a 2019 study by Junaidi and Lestari looked into the connection between fraud awareness and attitude among Indonesian auditors. The study could not discover any correlation between fraud awareness and fraud attitudes. According to the authors, personal characteristics like moral fervour and ethical standards may have a greater influence on auditors' attitudes towards fraud.

## **2.5 Conclusion**

This chapter has reviewed and explained the dependent variable (online banking fraud awareness) and the 4 independent variables (personal financial distress, empathy, knowledge on online banking, attitude towards fraud). Besides, the underlying theories and conceptual framework has been discussed and the 4 hypotheses has been constructed.

## **CHAPTER 3: METHODOLOGY**

### **3.0 Introduction**

This chapter clearly outlines the research methodology in this study. The elements that are discussed and explained in this chapter include the research design, data collection method, sampling design, research instrument, constructs measurement, data processing, and data analysis techniques. Throughout this chapter, the reader is able to understand better the study's objective.

### **3.1 Research Design**

This section describes the conceptual framework for every research whereby a researcher creates a strategic plan for the study. Research design is a master plan that specified the procedures and strategies for gathering and analysing the required data and it is not linked to a certain method of data collecting or a specific kind of data. It is essential to select an appropriate research design to avoid mistakes in gathering information and data.

#### **3.1.1 Quantitative Research**

This research will be adopting the quantitative research method whereby it is a formal, objective, and systematic method for learning the world by using numerical data (Apuke, 2017). The quantitative research method can test the hypothesis, measure the cause-and-effect relationship between the dependent variable and independent variables, and therefore make predictions. In addition, it enables the researcher to cover a big population sample size compared to the qualitative research method. The results obtained from the quantitative approach are statistical analyses which enable the researcher to evaluate the results by confirming or retorting on the original hypothesis stated in this research.

### **3.1.2 Descriptive research**

Under quantitative research, descriptive research is applied in this study as the research aims to the influencing factors of online banking fraud awareness in UTAR Kampar. It is a style of research methodology that seeks data in order to comprehensively explain phenomena, circumstances, or populations. According to Nassaji (2015), although the data in this type of study may be gathered qualitatively, it is frequently statistically examined with relationships being found using statistics like frequencies, percentages, and averages. Nassaji (2015) also stated that qualitative research is more comprehensive and frequently entails a broad gathering of data from several sources to better understand specific participants, including their thoughts, viewpoints, behaviours and attitudes.

## **3.2 Data Collection Method**

Data collection is important to a research project where the reliability of the data gathered from those intended respondents determines the outcome and quality of the research. According to Sekaran & Bougie (2010), primary data and secondary data is the few sources of data that the researcher might normally adopt. This research entitled the influencing factors of online banking fraud awareness in UTAR Kampar campus, primary data has been adopted to perform the data analysis.

### **3.2.1 Primary data**

Primary data was applied in this research to collect the first-hand data of the targeted participants (Kabir, 2016). Interviews, surveys, experiments, and other methods can be used to obtain primary data directly from primary sources. In this research, a questionnaire survey will be used to acquire the primary data regarding the dependent and independent variables. The level of authenticity of the data was strengthened through independent, original collecting. At the same time, as stated from Kabir (2016), primary data is able to improve the accuracy of the data since it is originated from the respondents.

### **3.3 Design of sampling**

Designing a sample refers to establishing a plan for drawing a sample from a particular population. The probabilities of each element or respondent included in the sample are known. It was necessary to use a best-fit sampling technique to collect the data for the research since samples are used to get first-hand information about the topic. The

researcher will demonstrate and justify the sampling method used to obtain data about the influencing factors of online banking fraud awareness in UTAR in this section.

### **3.3.1 Target Population**

According to Mohsin (2016), a research study should use a defined target audience that includes all respondents who match the requirements and standards. To guarantee the degree of accuracy and trustworthiness of the data gathered, the researchers must accurately and carefully identify the targeted respondents.

In this research study, its focus on evaluating the influencing factors of the online banking fraud in UTAR Kampar campus. Hence, the research focuses exclusively on the students at University Tunku Abdul Rahman (UTAR), Kampar, especially those between 18 - 24. According to Nurzali et al., 2018, the research stated that youth between the ages of 18 and 24 are the largest users of social media in Malaysia. Youth in the 18-24 age group are more likely to be exposed to risky online activities due to their less cautious online behaviour (Hasan et al., 2015). Over 80% of people in this age group (18-24) are willing to let their friends know their personal security questions which is supported by their less cautious online behaviour (Nurzali et al., 2018). Besides, Facebook, Youtube and Instagram, which have a high online explosion, are more popular among youth. Thus, this makes UTAR students the best candidates for this study. UTAR students were chosen as a sample because they are more likely to be exposed to online activities that need them to be aware of fraud issues, and since the majority of fraud cases involve people who are between the ages of 18 and 24 and who attend universities. They therefore require more exposure to reality and education about how to avoid falling victim to fraud later on now in their university degrees.

### **3.3.2 Frame and location of sampling**

The study is restricted to students from UTAR Kampar, Perak aged 18-24, so respondents from other countries cannot participate. This research will include distributed questionnaires to students in UTAR Kampar from Perak. Since Kampar has the highest concentration of students between the ages of 18-24, this study focuses on the sampling location in Kampar, Perak. This study will analyze what online applications or online shopping the targeted respondents use to make online payments via online banking. Aside from that, this research study will conduct an Internet survey by sending the questionnaire via an online application, as the respondents are exposed to technology nowadays.

### **3.3.3 Technique of Sampling**

Since this study is in Malaysia, it is impossible to target all people in the targeted group to carry out the survey. It will therefore be necessary to select samples by using specific techniques so that the researchers are able to obtain survey data by looking at the results of a subset of the population without having to examine each individual's responses individually. Non-random sampling has been used in this study. Everyone in the population does not have an equal chance of being selected and taking part in the survey. This study will not benefit from random sampling, as the results from a random sample have to approximate those obtained from measuring the entire population. Researchers would not use random sampling due to cost and time constraints.

In addition, non-random sampling has 3 types of factors, which are convenience, judgment, and experience. In this research, convenient non-random sampling would be adopted as it would be useful for exploratory tests like pilot surveys to carry out research. Convenience sampling was used by the researchers to select the respondents from the sample who are convenient for them to access. This study will select a sample which is a convenient source of data and easy to recruit. The advantage of convenience sampling is that it is cost-effective and conducive for the researcher to deploy on the questionnaire.

The questionnaire survey will be distributed to all UTAR students aged 18 - 24 that have been involved in online banking transactions activity who are willing to participate in this survey. As a result, this study can observe and investigate the influencing factors of online banking fraud awareness of the selected sample in a convenient manner. It is useful when the sample has the same traits which are used by the online banking system in their daily life.

### **3.3.4 Size of Sampling**

Sample size is important for this research since it acts as an indicator of the sampling to be included in how many respondents are in the questionnaire survey. It provides guidelines for the study to target the total number of respondents. By using Taro Yamane's (1967) formula, this study adopted the calculated sample size instead of the entire population in the target group.



The Taro Yamane (1967) formula is as below:

$$n = \frac{N}{1 + N(e)^2}$$

Where:

n = Sample size

N = Population size

E = Margin of error

To calculate the reasonable precision, this research should determine the total population size for the target group and the margin of error according to the Taro Yamane formula shown above. As shown above, this study will target UTAR students aged between 18-24 from Kampar and the total number of 21,000 UTAR students was shown (WebWay E Services, 2021).

As long as there is a 0.05 margin error added to the Taro Yamane formula, the figure would be interpreted as follows:

$$n = \frac{21,000}{1 + 21,000(0.05)^2}$$

$$n = 392.52$$

$$n \approx 400$$

As the figure shown above, this study has calculated the suggested sample size that will get approximately 400 respondents for this survey.

### **3.4 Research Instrument**

In this study, the method to analyze the topic is to use a research instrument as a tool to calculate, gather and analyze data relevant to the research purpose. Since the pandemic has restricted the movement between people and people and thus, this study is adopted online questionnaire distribution by using Google Form to gather feedback through. It is a free online tool, and it is able to allow everyone to obtain information in an easier and more efficient way. The QR code and the access link to the google form will be shared via utilizing social media platforms such as Facebook, WhatsApp, emails, and more other platforms. It is one of the best strategies to reach a huge number of respondents in order to achieve a certain target.

#### **3.4.1 Questionnaire Design**

A questionnaire is a research instrument that consists of a series of questions for the purpose of obtaining information from respondents through a survey. One of the advantages of using a questionnaire is that it is one of the most affordable ways to achieve this data collection. Moreover, it is also a cost-efficient way to obtain many respondents in a short period of time and able to allow this study to gather relevant information that is required. As a result, this study will be going to design an online questionnaire with a series of questions in the most appropriate and proper structure. The online survey has been used by Yuri & Sari (2022), Burke et al. (2021) to study the factors that influence fraud awareness.

The questionnaire for this study has included a few different structures or forms of questions which cover the non-structured, structured, multiple choice, and scaled response questions. It has been divided into a cover layout, personal data protection notices and followed by 6 sections. Section A mainly focuses on the personal information or background of the respondents, whereby there is a total of 5 demographic questions has been inserted. The questions include age, gender, number of online banking accounts, frequency on using online banking services, and the frequency that encountered fraud in online banking application. On the other hand, section B is constructed to collect the data of the dependent variables (fraud awareness) which consisted of 6 questions in this section. Besides, section C to section F is set for each independent variables where it consists of 5 questions for section C and section D respectively that used to collect data for personal financial distress and empathy, while section E and section F contained 6 questions accordingly that are used to examine the knowledge on online banking and the attitude towards fraud.

In general, Section B to Section F uses the rating scale methods to measure. This is because it is direct and clear where it is easy to understand and do not cause a confusion for the respondents (Babakus and Mangold,1992).

### **3.4.2 Questionnaire Reliability**

There are several crucial qualities that a study must uphold when conducting a questionnaire survey. One of the crucial qualities is questionnaire reliability. Reliability is the scope to which an instrument will produce the same results on repeated trials (Morrison, 2019). All measurement instruments are consistent and accurate, and that can only be evaluated by taking into account how reliable and valid the survey is. One estimate of reliability is test-retest reliability. This includes doing the survey with a

certain group of respondents and conducting the survey again with the same group at a later point in time. The study will then compare the responses after conducting both surveys with the same group of respondents. It is demonstrated that reliability has occurred if the outcomes collected are the same for repeated testing with the same group. However, to apply this test-retest method, there are 2 assumptions that need to be fulfilled. One of the assumptions is that the characteristic being assessed must remain constant throughout the “testing effect” period. While for the second assumption is that the time interval is long enough yet short enough to prevent the “memory effect”, which is when test-takers recall taking the test for the first time, from having an impact on their results on subsequent administrations of the test. In general, the correlation coefficient ( $r$ ) values will be taken if  $r$  is around 0.70 (Bolarinwa, 2016).

### **3.4.3 Ethical Consideration**

In a study, ethical consideration is considered one of the most important parts of the research. It is a series of values and principles that should be maintained when conducting human affairs. No one could behave in such a way in the ethical consideration that would be damaging to society or an individual. It forbids individuals and organizations from engaging in destructive behaviour. The main purpose of having ethical considerations is to ensure there are no people who will be damaged by the study.

There are a few key points that represent the most essential principles that are linked to ethical considerations in dissertations. In a study, the researcher must have the responsibility to protect the private information, identity, dignity, integrity, and right to self-determination of the research subjects. Throughout the whole research process, all data must be consistently protected. In general, the respondents should not be required

to fill in the survey form with their names, IC number and any other identifiable information, unless there is any identifiable information needed to be filled in, but the researcher should promise to keep it confidential. This is to avoid any disclosure of respondents' private information and the cause of inappropriate harm to them, including psychological harm.

Meanwhile, the researcher of the study must request permission from every single respondent before filling out the survey form to obtain their data and information. As the respondents have the right to know what kind of study they are participating in and what is required of them, the researcher should indicate clearly what exactly the purpose of the study is.

Lastly, if there are any problems occur, the respondents have the right to withdraw from the research process. Researchers are not allowed to put respondents under any kind of pressure throughout the process of rejecting a study project. Additionally, it is important to avoid fraud when conducting research. Even though dishonesty is sometimes necessary for research purposes, it must also be able to explain itself to the respondents.

#### **3.4.4 Pilot test**

During the study, the researcher will be implementing a pilot test in order to determine the feasibility of the research design before starting to distribute the questionnaire study to the targeted audience. A pilot test refers to a small-scale preliminary investigation carried out prior to any large-scale quantitative research in order to assess the feasibility of a potential full-scale project in the future. The objective of the pilot test is to assist

the researcher by assisting in obtaining additional information about the targeted population. On the other hand, a pilot test is also able to assist in determining the potential success of a research study based on the responses of respondents. It is also successful in developing the proper questions and a consolidated research ideal strategy for a study.

In addition, the influencing factors of online banking fraud awareness in UTAR will be the focus of this research study, which will be conducted among 40 UTAR students. This study will be using Google Forms to carry out and share it through Facebook, WhatsApp, and Instagram. With the support of the researcher, the respondents must complete the Google Form as the questionnaire, which is one of the measurement tools. Moreover, the respondents might also provide the researcher with constructive feedback on how to improve the questions and avoid using any terms that the general public may not be familiar with. Therefore, to assess the feasibility of the questionnaire survey, the researcher may beforehand select a group of respondents from the sample size. The data and information will be used to obtain from the 400 respondents by using Google Form, and it could be used to examine and organize the results by using the specified codes assigned to each questionnaire.

### **3.5 Constructs Measurement**

Since the construct measurement is essential in the study to maintain the reliability of the findings and outcomes, hence, analyst always focus much on the construct measurement (Boyd, Bergh, Ireland & Ketchen, 2013).

### 3.5.1 Scale of Measurement

It is used to categorize the variables into groups specifically. There are four common scales of measurement which are nominal, ordinal, interval, and ratio whereby it was created by psychologist Stanley Stevens (UNSW Online, 2020). Each scale of measurement has characteristics that dictate how the data should be analyzed. In this research study, the scale that adopted are nominal, and interval.

#### 3.5.1.1 Nominal Scale

According to Sekaran & Bougie (2013), the nominal scale can be applied for the elements that without value which labeling will used for categorizing. Besides, there is no ranking applied in nominal scale where it is simply used to define the characteristics of a particular element. Nominal scale was implied in section A of the questionnaire for this study research. For example, the gender is examined (refer to example of nominal scale).

Example of nominal scale:

Gender: <input type="checkbox"/> Male <input type="checkbox"/> Female
--

#### 3.5.1.2 Interval Scale

Interval scale combined the properties of nominal scale and ordinal scale. However, it has an advancement which is the scale are in an order manner that have a specific meaning for each scaling (Sekaran & Bougie, 2013). This scale has been utilized and implied in Section B to Section F which is to examine the dependent variable and 4 independent variables. The types of interval scale can be likert scale (Joshi, Kale, Chandel & Pal, 2015).

Table 3.1

*Example of Likert scale.*

	Strongly disagree	Agree	Neutral	Disagree	Strongly agree
I install anti-spam software or anti-virus software.	1	2	3	4	5

### **3.5.2 Operational Definition for the Measurement of Independent Variables and Dependent Variable**

The dependent variables fraud awareness is influenced by 4 independent variables which are personal financial distress, empathy, knowledge on online banking, and attitude towards fraud. As mentioned above, interval scale was applied which is likert scale.



### **3.5.2.1 Fraud awareness**

Fraud awareness is the dependent variable in this research study where it has been examined at Section B in the questionnaire by using the likert scale. It measures the degree of fraud awareness among the university students in UTAR Kampar.

The scale was adopted by the European Commission (2020). Some of the sample items included “I install anti-spam software or anti-virus software”, “I avoid clicking links in emails or text messages unless I know the sender”, and “I only provide my identity card or information on a secured application”.

### **3.5.2.2 Personal Financial Distress**

Personal financial distress is one of the independent variables that would like to be investigated by the researchers on the influencing factors of online banking fraud awareness. It has been constructed in Section C by using the likert scale. It measures the level of an individual’s stress from their financial situation.

The scale was used by Prawitz et al. (2006). Some of the sample items included “I often worry about being able to meet my normal monthly living expenses”, “I seldom go out to eat, watch movies or any entertainment activity because I can’t afford it”, and “I feel stressed about my personal finances in general”.

### **3.5.2.3 Empathy**

Empathy is one of the independent variables in this research study where it has been examined in Section D by using likert scale. It measures the level of empathy an individual would show if they encountered some uncertainty or difficulties. In another words, it is the feeling, emotions, or action of an individual when they are facing problems.

The scale was supported by Davis (1983), where some of the sample items included “I find difficulties in being capable of empathizing with the fraudsters' perspective”, “It is quite common for me to criticize fraudsters that I feel are unfair or harmful”, and “Fraudsters are not a person that I feel empathy toward”.

#### **3.5.2.4 Knowledge towards online banking**

Knowledge towards online banking is one of the independent variables that is structured in Section E by using likert scale to examine. It measures the level of knowledge an individual possesses on the sector of online banking. It can be influenced by the people from surrounding, such as family members and peers.

The scale was supported by Lewis (2019), Cheng et al. (2006), and Nor et al. (2008) where the sample items included “I would find it easy to get the online banking services to do what I want to do”, “In my opinion, using online banking services is a good and wise idea”, and “My family, friends, and peers are currently using online banking.”

#### **3.5.2.5 Attitude towards fraud**

Attitude towards fraud is the fourth independent variable for the influencing factors of online banking fraud awareness. It was examined in the last section of the questionnaire (Section F) by using likert scale. It measures how positively or negatively people assess fraud.

The scale was adapted from Apaua & Lallieb (2022), where the sample items included “I trust the bank’s system will perform my process of transaction correctly”, “I always believe that the information provided on the bank's website is accurate”, and “When online banking involves fraud, I intend to stop using it”.

## **3.6 Data Processing**

In this stage, researchers are required to transform the primary data that was collected from the respondents by using the questionnaire to informative data to achieve the objectives of the study and validate the hypothesis. It consists of several processes which are data checking, editing, coding, and transfer (Kveder and Galico, 2008). This process is to ensure that the information collected does not contain any errors or mistakes where it could affect the whole outcome of the research study.

### **3.6.1 Data Checking**

At the first stage, the researcher should carry out the data checking process after collected the data from the respondents. This is because there is a possibility that respondents may make mistakes when answering the questions. Data checking could

help to reduce those errors and mistakes which could affect the final outcome for the research study. Error and mistakes including omission or missing of data.

### 3.6.2 Data Editing

In the second stage of data processing, the researcher is required to reduce the number of inadequate responses. According to Sekaran and Bougie (2009), when the incomplete responses are discovered, the researchers have to complete the data by mimicking the respondents' habit of answering. This action is to ensure that the consistency of the data is improved. In short, the data needs to be altered to guarantee that the outcomes are consistent and persistent.

### 3.6.3 Data Coding

At this particular stage, the raw data that is collected from the questionnaire needs to be coded into numerical numbers to input into SPSS for data analysis. The data coding of this research study is shown at the Table 3.2:

Table 3.2

*Answer coded for Section A*

Q3	Gender	“Male” = 0 “Female” = 1
----	--------	----------------------------

Q6	The frequency of getting into online banking fraud	“Never” = 0 “Yes ” = 1
----	--	---------------------------

### **3.6.4 Data Transferring**

In the last stage of data processing, the data that has been checked, edited, coded are transcribed to SPSS 29.0 for data running and analysis process.

## **3.7 Data Analysis**

The collected data are required to be analyzed by using SPSS 29.0 to validate the hypothesis that is stated in Chapter 2. Besides, the outcome of the data analysis will be able to answer the research questions mentioned in Chapter 1. There are several tests that are required to be performed by the researcher to ensure the outcome is sufficiently supported overall.

### **3.7.1 Descriptive Analysis**

To present the data in an understandable and straightforward manner, researchers must first do a descriptive analysis. It is a fundamental analysis where it separates into 2 parts. The first is central tendency where it involved the frequency and percentage

(Aldrich, 2019), on the other hand, the second part will be the measure of variability where the particular items are examined by the mean and standard deviation. In this part, table, graphs, pie charts are being used to present the data outcome generated by SPSS 29.0.

### 3.7.2 Scale Measurement

#### 3.7.2.1 Reliability test

The reliability test is carried out, in accordance with Pallant (2013), to make sure the scales are trustworthy. In this case, Cronbach's Alpha has been used to examine the level of scales reliability (Pallant, 2013). This statistic is within the range of 0 to 1 where the higher value indicates that the higher level of reliability. The below Table 3.3 shown the Cronbach' rule of thumb.

Table 3.3

*Cronbach Rule of Thumb.*

Cronbach's Alpha	Reliability level
$\alpha < 0.60$	Poor
$0.60 \leq \alpha < 0.70$	Fair
$0.70 \leq \alpha < 0.80$	Good

$0.80 \leq \alpha \leq 0.95$	Excellent
------------------------------	-----------

Source: Zikmund, Babin, Carr and Griffin (2010)

According to Table 3.3, if the alpha level is less than 0.60, the reliability is poor. When the alpha level rises to the region of 0.6 to 0.70, the reliability will be fair. The scales will be good reliable if the alpha value is between 0.71 and 0.80. While when the value is between 0.81 and 0.95, the scales are considered at an excellent level of reliability.

Table 3.4

*Result of reliability test for pilot test.*

Variables	Cronbach's alpha	Reliability level
Fraud awareness	0.607	Fair
Personal financial distress	0.502	Poor
Empathy	0.602	Fair
Knowledge of online banking	0.860	Excellent
Attitude towards fraud	0.664	Fair

The results of the pilot test for each dependent and independent variable are displayed in Table 3.4 above. Independent variables, knowledge of online banking has an excellent level of reliability where the cronbach's alpha is at 0.860. On the other hand,

the level of reliability of dependent variables, fraud awareness and 2 independent variables, empathy and attitude towards fraud are categorized as fair as their alpha values are at 0.607, 0.602, and 0.664 respectively. However, personal financial distress is considered poor reliability due to the low alpha value. In this case, the fifth item has been deleted from the particular section due to the Cronbach's Alpha if item deleted is 0.648 which is considered at fair.

### **3.7.3 Preliminary Data Screening**

#### **3.7.3.1 Normality**

Normality test has been performed in the section of preliminary data screening where it is used to ensure that the inferential analysis can be well carried out which does not contain any non-normality (Aldrich, 2018). The researcher will find the data is not accurate and reliable because the data set does not have a normal distribution. In this case, the data set would be biased, as a result, the data set is not suitable for the researcher to use for analyzing the data (Ghasemi & Zahediasl, 2012).

One of the methods adopted to test for normality will be the skewness and kurtosis value. If skewness deviates significantly from zero, it suggests that the dataset is not normally distributed. While for sample sizes larger than 300, if the skewness value falls within the range of -2 to +2 and the kurtosis value falls within the range of -7 to +7, then the data is considered to have a normal distribution.



### **3.7.3.2 Pearson correlation**

Pearson correlation will be performed after the normality test, whereby it is a statistical measure that quantifies the strength and direction of the linear relationship between two variables. It ranges from -1 to +1, where -1 represents a perfect negative correlation, 0 represents no correlation, and +1 represents a perfect positive correlation. Pearson correlation assumes that both variables are normally distributed and have a linear relationship. The "Correlate" feature can be applied to multiple variables at once, resulting in a table that displays all the correlations between them.

### **3.7.3.3 Multicollinearity**

The multicollinearity test, which is used to determine whether there is a significant correlation of two independent variables because greater correlation representing the higher the level of error will be, where it is the final preliminary data screening (Abdulwahab, Zulkhairi, & Galadima, 2011). In order to assess whether multicollinearity is present, VIF statistics can be observed for each of the variables. There is no multicollinearity problem when the VIF value is between 1 and 10. In contrast, there is a multicollinearity problem when the VIF value is higher than 10.

### **3.7.4 Inferential analysis**

This is a vital analysis of the data whereby it makes assumptions about the population. In this case, a total of 400 responses collected from the university students at UTAR Kampar campus can study on the fraud awareness for online banking. This research has adapted multiple regression analysis.

### 3.7.4.1 Multiple Regression Analysis

According to Aldrich (2019), multiple regression analysis is suitable to use when there is one dependent variable and more than one independent variable. As a result, given that there was just one dependent variable (fraud knowledge) and 4 independent variables (personal financial distress, empathy, knowledge on online banking, attitude towards fraud), it was appropriate to use in this research investigation.

It can be examined in the model summary table whereby it contains all the needed information or indicator. The R-squared is a statistical metric that measures the goodness of fit of a regression model, indicates how much of the variance in the dependent variable is accounted for by the independent variables.

The equation of the model as below:

$$FA_i = \beta_0 - \beta_1 PFD_i + \beta_2 E_i + \beta_3 KOB_i + \beta_4 ATF_i + \mu_i$$

Where,

$FA_i$  = Fraud awareness

$PFD_i$  = Personal financial distress

$E_i$  = Empathy

$KOB_i$  = Knowledge on online banking

$ATF_i$  = Attitude towards fraud

$\mu_i$  = Error term

The equation demonstrates the direction of the relationship between the independent variables on the right-hand side and the dependent variable on the left-hand side. The multiple regression equation for this research investigation is, in essence, represented by this.

### **3.8 Conclusion**

In a nutshell, this chapter has covered the methodology of the research study whereby it is quantitative research and primary data is collected. Pilot test will be implied before conducted the real test for the 400 respondents in UTAR Kampar. After that, data processing and data analysis will be carried out.

## **CHAPTER 4: DATA ANALYSIS**

### **4.0 Introduction**

The data analysis in this chapter is completed. The descriptive analysis is done initially. The reliability test is carried out in order to confirm the dependability of the scales. In the third step, preliminary data screening, multicollinearity and non-normality issues are looked for. SPSS 29.0 is used for all these analyses.

### **4.1 Descriptive analysis**

To make the data simple to comprehend, a descriptive analysis is first carried out. The demographic information acquired in Section A of the survey questionnaire is first subjected to a descriptive analysis. The information from Sections B and F is also subject to descriptive analysis. Tables and charts are created to summarize the data in the analysis that follows. To summarize the data for the analysis that accompanies, tables and charts are generated.

#### **4.1.1 Respondents' Demographic Profile**

There are five areas of demographic information, including gender, age group, the number of online banking accounts owned, how frequently users use online banking, and how frequently users commit online banking fraud, are included in this study. The next sections examine each one separately.

#### 4.1.1.1 Gender

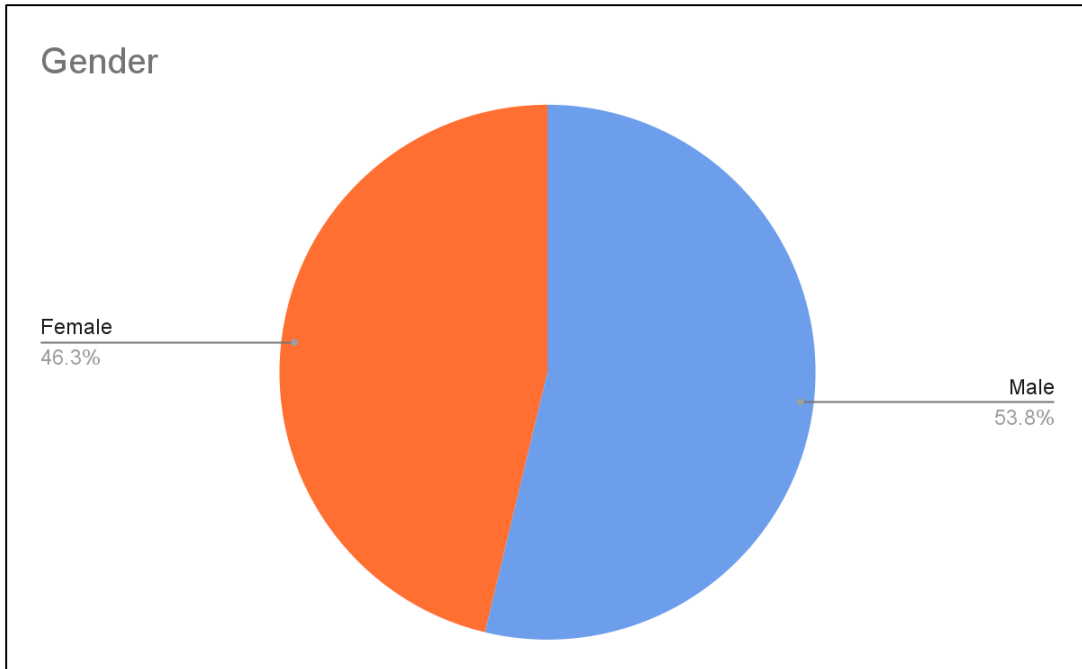
Table 4.1

*Descriptive Analysis for Gender.*

<b>Gender</b>	<b>Frequency</b>	<b>Percentage (%)</b>	<b>Cumulative Frequency</b>	<b>Cumulative Percentage (%)</b>
<b>Male</b>	215	53.8	215	53.8
<b>Female</b>	185	46.3	400	100.0

Figure 4.1

*Descriptive Analysis for Gender.*



The responses are first divided into gender-specific groups. A total of 400 students from UTAR took part in this study. There are 215 male respondents and 185 female respondents, with a sex ratio of 53.8% to 46.3%, as shown in Table 4.1 and Figure 4.1. Consequently, there are more men participating than women.

#### 4.1.1.2 Age Group

Table 4.2

*Descriptive Analysis for Age Group.*

Age Group	Frequency	Percentage (%)	Cumulative Frequency	Cumulative Percentage (%)
18 years old	24	6.0	24	6.0

---

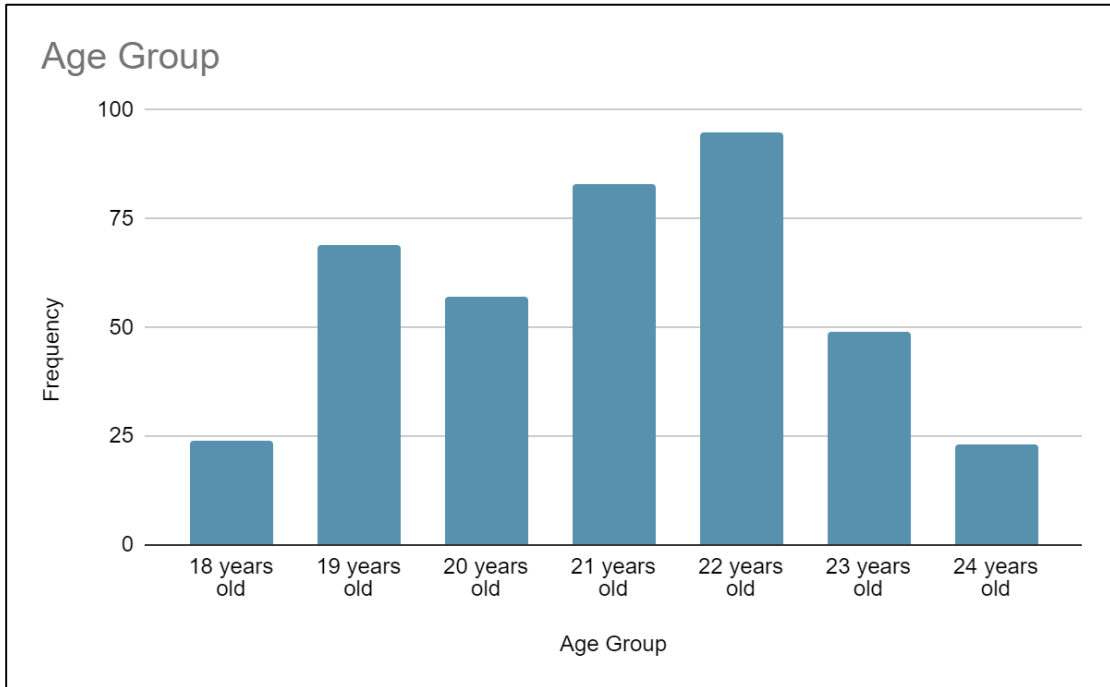
The Influencing Factors of Online Banking Fraud Awareness in UTAR Kampar

---

<b>19 years old</b>	69	17.3	93	23.3
<b>20 years old</b>	57	14.2	150	37.5
<b>21 years old</b>	83	20.8	233	58.3
<b>22 years old</b>	95	23.8	328	82.0
<b>23 years old</b>	49	12.3	377	94.3
<b>24 years old</b>	23	5.8	400	100.0

Figure 4.2

*Descriptive Analysis for Age Group.*



Along with gender, the responses are divided into groups based on the age ranges to which they belong. Based on the table 4.2, there are 6% (24 respondents) of the participants are 18 years old, 17.3% (69 respondents) of the participants are 19 years old, 14.2% (57 respondents) of the participants are 20 years old, 20.8% (83 respondents) of the participants are 21 years old, 23.8% (95 respondents) of the participants are 22 years old, 12.3% (49 respondents) of the participants are 23 years old, and 5.8% (23 respondents) of the participants are 24 years old.



**4.1.1.3 Number of Internet Bank Account Holding**

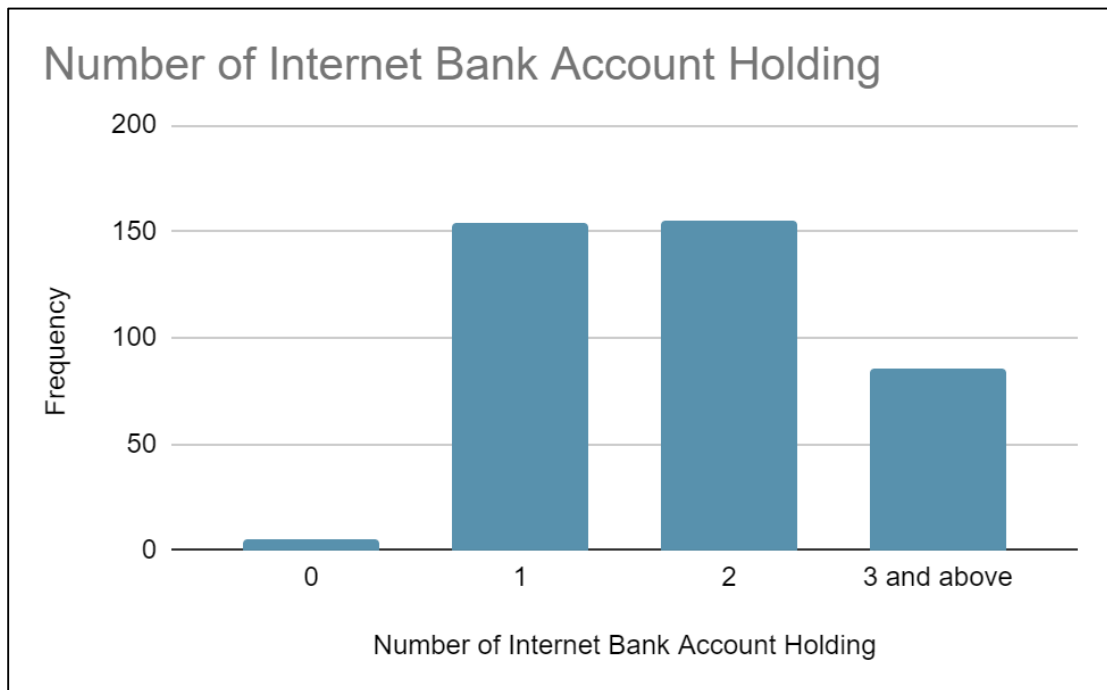
Table 4.3

*Descriptive Analysis for Number of Internet Bank Account Holding.*

<b>Number of Internet Bank Account Holding</b>	<b>Frequency</b>	<b>Percentage (%)</b>	<b>Cumulative Frequency</b>	<b>Cumulative Percentage (%)</b>
<b>0</b>	5	1.3	5	1.3
<b>1</b>	154	38.5	159	39.8
<b>2</b>	155	38.8	314	78.5
<b>3 and above</b>	86	21.5	400	100.0

Figure 4.3

*Descriptive Analysis for Number of Internet Bank Account Holding.*



The respondents are also categorized based on the number of internet bank accounts held. According to Table 4.3 and Figure 4.3, out of a total of 400 respondents, 155 respondents (or 38.8%) reported having two internet banking accounts. 154 respondents (38.5%) have just one internet banking account, though. Participants who had more than three online banking accounts totalled 21.5% (86 respondents). Additionally, 5 respondents stated that they do not have an internet bank account.

#### 4.1.1.4 The Frequency of Using Online Banking

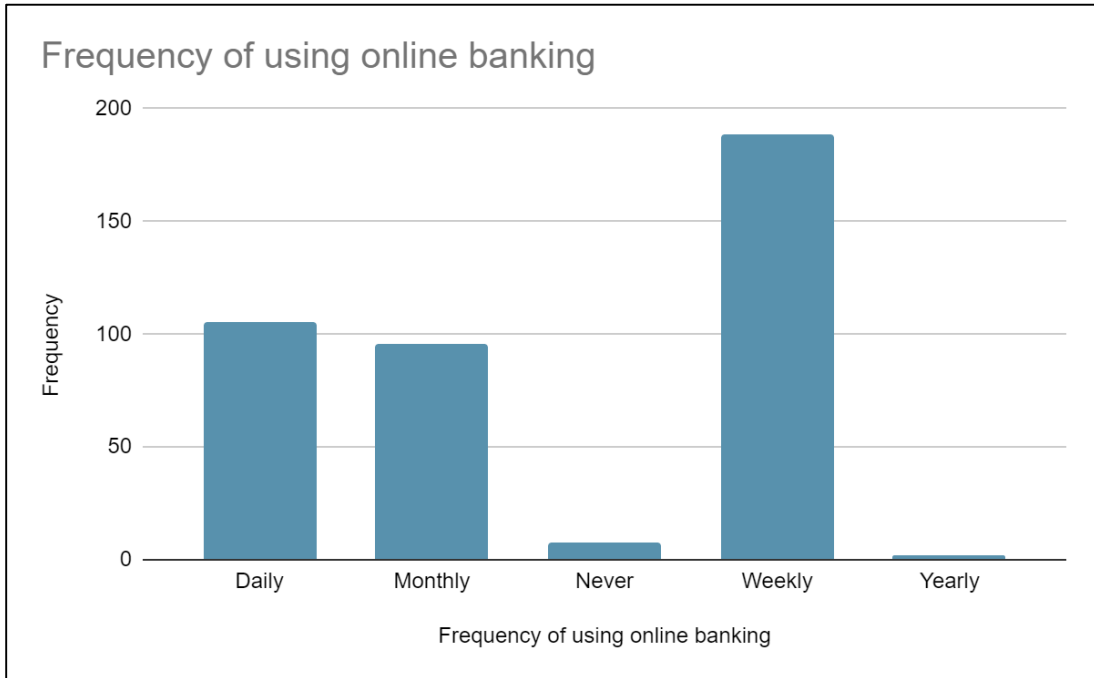
Table 4.4

*Descriptive Analysis for the Frequency of Using Online Banking.*

<b>Frequency of using online banking</b>	<b>Frequency</b>	<b>Percentage (%)</b>	<b>Cumulative Frequency</b>	<b>Cumulative Percentage (%)</b>
<b>Daily</b>	105	26.3	105	26.3
<b>Monthly</b>	96	24.0	201	50.2
<b>Never</b>	8	2.0	209	52.3
<b>Weekly</b>	189	47.3	398	99.5
<b>Yearly</b>	2	0.5	400	100.0

Figure 4.4

*Descriptive Analysis for the Frequency of Using Online Banking.*



Moreover, the frequency of using online banking is also one of the factors to group the respondents. According to Figure 4.4, 47.3% of the respondents reported using internet banking weekly. There are 105 respondents (26.3% of respondents) using online banking on a daily basis. Fewer than 5% of respondents, or 2 respondents, said they regularly use online banking. Additionally, everyday internet banking was used by 96 respondents (or 24.0% of respondents). On the other hand, there are 8 respondents who have never used online banking before.

**4.1.1.5 The frequency of Getting into Online Banking Fraud**

Table 4.5

*Descriptive Analysis for the frequency of Getting into Online Banking Fraud.*

<b>The frequency of Getting into Online Banking Fraud</b>	<b>Frequency</b>	<b>Percentage (%)</b>	<b>Cumulative Frequency</b>	<b>Cumulative Percentage (%)</b>
<b>1</b>	114	28.5	114	28.5
<b>0</b>	286	71.5	400	100.0

Figure 4.5

*Descriptive Analysis for the frequency of Getting into Online Banking Fraud.*



Finally, the respondents are categorised based on how frequently they engage in online banking fraud. According to Table 4.5 and Figure 4.5, 114 respondents, or 28.5%, reported having experienced online banking fraud. Of the 286 respondents, 71.5 percent had never experienced online banking fraud. Most respondents in UTAR have never experienced online banking fraud, according to the report.

#### **4.1.2 Central Tendencies and Measurement of Constructs' Dispersion**

This section examined the responses of the survey questions that were answered by the respondents by using central tendencies which is mean, and dispersion measurement which is standard deviation. The measurements will be ranked one by one.

##### **4.1.2.1 Fraud awareness**

Table 4.6

*Central Tendencies Measurement for Fraud Awareness.*

No.	Question	Sample size, N	Mean	Standard deviation	Mean Ranking	Standard deviation Ranking
FA1	I am suspicious of letters or emails containing spelling	400	3.08	1.353	3	4

	and grammar mistakes.					
FA2	I avoid clicking links in emails or text messages unless I know the sender.	400	3.49	1.446	2	2
FA3	I install anti-spam software or anti-virus software.	400	2.86	1.370	4	3
FA4	I only provide my identity card or information on a secured application.	400	3.60	1.495	1	1
FA5	I subscribe to a specific service to avoid commercial calls.	400	2.63	1.335	5	5
FA6	I transfer money from any platform to someone that I don't know.	400	1.76	1.057	6	6

According to the Table 4.6 where the 6 questions of dependent variable were answered by respondents are examined. FA4 has the highest mean and standard deviation which are 3.60 and 1.495 accordingly. It was then followed by FA2 which has the second highest mean (3.49) and standard deviation (1.446). Besides, FA1 has the third highest mean which is 3.08, yet its standard deviation, 1.353 is in the fourth highest place. The fourth highest mean goes to FA3 at 2.86, but its standard deviation is placed at the third ranking at 1.370. The fifth highest mean and standard deviation belongs to FA5 which

recorded at 2.63 and 1.335 respectively. Lastly, FA6 are the lowest mean and standard deviation which is respectively 1.76 and 1.057.

#### 4.1.2.2 Personal Financial Distress

Table 4.7

*Central Tendencies Measurement for Personal Financial Distress.*

No.	Question	Sample size, N	Mean	Standard deviation	Mean Ranking	Standard deviation Ranking
PFD1	I feel stressed about my personal finances in general.	400	3.58	1.035	2	4
PFD 2	I often worry about being able to meet my normal monthly living expenses.	400	3.61	1.017	1	5
PFD 3	I frequently find myself just getting by financially and living paycheck to paycheck.	400	3.38	1.043	3	3
PFD 4	I seldom go out to eat, watch movies or any entertainment activity because I can't afford it.	400	3.21	1.199	5	1
PFD5	I am satisfied with my current financial situation.	400	3.30	1.126	4	2

Table 4.7 shows the 5 questions under independent variable regarding personal financial distress answered by respondents and being examined. Although PFD2 has the highest mean ranking (3.61), its standard deviation value (1.017) is the lowest. PFD1 has the second-highest averages, which are 3.58, and the second-lowest standard deviations, which are 1.035. Besides, the third highest mean and standard deviation belongs to PFD3 at 3.38 and 1.043 respectively. Despite having the second highest standard deviation of 1.126, PFD5 has the second lowest mean of 3.30. PFD 4 is last, with a mean score of 3.21 but a standard deviation of 1.199, which is the largest.

#### 4.1.2.3 Empathy

Table 4.8

*Central Tendencies Measurement for Empathy.*

No.	Question	Sample size, N	Mean	Standard deviation	Mean Ranking	Standard deviation Ranking
E1	I tend to lose control if I am falling into an online fraud trap.	400	2.72	1.281	4	3
E2	In the case of unfair online shopping experiences, I tend to seek revenge.	400	2.56	1.151	5	1
E3	I find difficulties in being capable of empathizing with the	400	2.80	1.234	3	5



	fraudsters' perspective.					
E4	It is quite common for me to criticize fraudsters that I feel are unfair or harmful.	400	2.97	1.251	2	4
E5	Fraudsters are not a person that I feel empathy toward.	400	3.17	1.372	1	2

Table 4.8 shows the 5 questions under independent variables regarding empathy that are answered by the participants and being examined. Based on the results recorded in the table, with a mean score of 3.17 and a standard deviation of 1.372, E5 has the highest average. Besides, the second largest means goes to E4 which recorded at 2.97, however, it has the second lowest standard deviation of 1.251. The elements E3 has the third highest ranking of means at 2.80, but it has the lowest standard deviation at 1.234. It then followed by E1 where the mean has the fourth highest ranking at 2.72 and its standard deviation of 1.281 is being placed at the third ranking. Lastly, the lowest mean ranking belongs to E2 where it recorded at 2.56, yet, it has the highest standard deviation among the 5 questions at 1.151.

#### 4.1.2.4 Knowledge of online banking

Table 4.9

*Central Tendencies Measurement for Knowledge of Online Banking.*

No.	Question	Sample size, N	Mean	Standard deviation	Mean Ranking	Standard deviation Ranking
KOB 1	I would find it easy to get the online banking services to do what I want to do.	400	3.24	1.317	5	4
KOB 2	I would find this online banking services is user-friendly and easy-to-use.	400	3.30	1.305	4	5
KOB 3	Online banking has enhanced my productivity and efficiency in performing the banking services.	400	3.33	1.364	3	2
KOB 4	In my opinion, using online banking services is a good and wise idea.	400	3.37	1.381	2	1
KOB 5	I would feel secure sending sensitive information across the online banking.	400	2.79	1.294	6	6
KOB 6	My family, friends, and peers are currently using online banking.	400	3.53	1.334	1	3

Table 4.9 shows the 6 questions under independent variable regarding the knowledge of online banking that has been answered by the respondents and being examined. As per the table shown, KOB6 owns the highest average, 3.53, and the third-lowest standard deviation, 1.334. The second highest means goes to KOB4 where it has the means of 3.37 and the standard deviation is placed at the first ranking which is 1.381. It was then followed by KOB3 where it has the third highest means ranking at 3.33 and second highest of standard deviation of 1.364. In addition, KOB2 possess the fourth-highest mean score among the six questions (3.30), and its standard deviation is the second-lowest among them (1.305). The means of KOB1 is at the fifth-highest ranking of 3.24 and 1.317 is the standard deviation which placed in the fourth-highest. Lastly, KOB5 has the lowest ranking in means and standard deviation where it has been recorded at 2.79 and 1.294 respectively.

#### 4.1.2.5 Attitude towards fraud

Table 4.10

*Central Tendencies Measurement for Attitude towards Fraud.*

No.	Question	Sample size, N	Mean	Standard deviation	Mean Ranking	Standard deviation Ranking
ATF1	Although I have used online banking safely for many times, fraudulent problems may occur in the future.	400	3.28	1.378	1	2

ATF2	I trust the bank's system will perform my process of transaction correctly.	400	3.15	1.244	2	4
ATF3	I always believe that the information provided on the bank's website is accurate.	400	3.05	1.267	4	3
ATF4	The chances of losing money if I use online banking are low.	400	2.78	1.204	6	6
ATF5	Scammers might take control of my account if I use online banking.	400	2.89	1.237	5	5
ATF6	When online banking involves fraud, I intend to stop using it.	400	3.08	1.392	3	1

Table 4.10 above shows the 6 questions under the independent variables regarding attitude towards fraud has been answered and being examined. As per the table shown, the highest mean goes to ATF1 where it has the mean of 3.28, and its standard deviation of 1.378 is ranked at the second highest position. ATF2 has the second-highest mean, which is 3.15, and the fourth-highest standard deviation, which is 1.244. Besides, ATF6 has the third highest mean at 3.08, and the highest standard deviation among the 6 questions at 1.392. The fourth highest mean value belongs to ATF3 at 3.05 and its standard deviation of 1.267 is at the third highest ranking. ATF5 has the second lowest

mean and standard deviation which are 2.89 and 1.237 respectively. The element of ATF4 had the lowest mean and standard deviation, with measurements of 2.78 and 1.204, respectively.

## 4.2 Scale Measurement

### 4.2.1 Reliability test

Table 4.11

*Reliability Analysis.*

No.	Variables	Name of variable	Number of items	Cronbach's Alpha	Results of reliability
1	Dependent variable	Fraud awareness	6	0.828	Excellent
2	Independent variable	Personal Financial Distress	5	0.729	Good
3	Independent variable	Empathy	5	0.865	Excellent
4	Independent variable	Knowledge of online banking	6	0.947	Excellent
5	Independent variable	Attitude towards fraud	6	0.904	Excellent

The reliability analysis for 1 dependent variable and 4 independent variables is shown in Table 4.11 above. According to Zikmund, Babin, Carr and Griffin (2010), the reliability values is within 0 to 1 where the rating scale starts from poor (less than 0.60), fair (0.60 – 0.70), good (0.70 – 0.80), excellent (0.80 - 0.95).

Based on the results generated, the cronbach's alpha for all variables have exceeds 0.6. For instance, because the independent variable (Personal Financial Distress) has a cronbach's alpha of 0.729, which is higher than 0.7 but lower than 0.8, it is thought to be reliable. Additionally, because the cronbach's alpha of the dependent variable (fraud awareness) and the independent variables (empathy, knowledge on online banking, and attitude towards fraud) is greater than 0.8 but less than 0.95, they are both regarded as excellent variables. Hence, all the items are kept and being examined in this research study.

### **4.3 Preliminary Data Screening**

#### **4.3.1 Normality Test**

Firstly, in order to determine whether the data has a normal distribution, a normality test is first to be performed. In this study, two methods which are skewness and kurtosis values were used to assess the data's normality.

Table 4.12

*Normality Test Results.*

Variables	Skewness	Kurtosis
Dependent variable: Fraud awareness	(3.644)	(3.070)
Independent variable 1: Personal Financial Distress	1.393	(2.131)
Independent variable 2: Empathy:	(3.467)	(1.947)
Independent variable 3: Knowledge on online banking:	(4.418)	(4.156)
Independent variable 4: Attitude towards fraud:	(4.328)	(3.549)

Source: Data generated from SPSS Statistics.

Normality tests are employed in statistics to determine whether a dataset can be adequately modelled by a normal distribution. As many statistical functions depend on normal or nearly normal distributions, it is important to verify normality before using such functions (The GoodData Community, n.d.). One of the functions to evaluate normality is numerical measures of shape namely skewness and kurtosis. If skewness deviates significantly from zero, it suggests that the dataset is not normally distributed. While for sample sizes larger than 300, if the skewness value falls within the range of -2 to +2 and the kurtosis value falls within the range of -7 to +7, then the data is considered to have a normal distribution.

With the exception of personal financial distress, all skewness values from Table 4.12 are outside the range of between -2 and +2. In the meantime, personal financial distress has the highest skewness value of 1.393 while knowledge has the lowest skewness value of -4.418. On the other hand, all kurtosis values fall within the range of -7 to +7. The kurtosis value for empathy was the highest at -1.947, while the kurtosis value for knowledge was the lowest at -4.156. In summary, the variables data for skewness are not normally distributed since only of the variables data is in the range of -2 to +2. On the contrary, all the kurtosis values are in the range of -7 to +7, all variables' data are normally distributed.

Although only kurtosis achieved the criteria within the range of  $-7$  to  $+7$  but in contrast, skewness is not achieving the criteria in within the range of  $-2$  to  $+2$ . However, according to Kim (2013), as the sample size increases, the standard errors tend to decrease. Consequently, when performing under null hypothesis of a normal distribution, it becomes easier to reject the hypothesis in large samples that may not substantially deviate from normality. Conversely, in small samples, the null hypothesis of normality tends to be more easily accepted than needed. In addition, according to Demir (2022), due to the central limit theorem, when dealing with large samples, the data will tend to follow a normal distribution. Therefore, it is reasonable to assume that the normal distribution assumption holds true for large samples, regardless of the techniques used to assess normality.

### **4.3.2 Pearson Correlation**

Pearson correlation is a statistical measure that quantifies the strength and direction of the linear relationship between two variables. It ranges from -1 to +1, where -1



represents a perfect negative correlation, 0 represents no correlation, and +1 represents a perfect positive correlation. Pearson correlation assumes that both variables are normally distributed and have a linear relationship. The "Correlate" feature can be applied to multiple variables at once, resulting in a table that displays all the correlations between them. This table is arranged in a matrix format which shown below:

Table 4.13

*Correlations for Fraud Awareness and Personal Financial Distress.*

Correlations			
		Total Fraud Awareness	Total Personal Financial Distress
Total Fraud Awareness	Pearson Correlation	1	-.527**
	Sig. (2-tailed)		<.001
	N	400	400
Total Personal Financial Distress	Pearson Correlation	-.527**	1
	Sig. (2-tailed)	<0.001	
	N	400	400
**. The significance level for correlation is 0.01 (2-tailed).			

Source: Information produced by SPSS Statistics.

Based on Table 4.13, the correlation between fraud awareness and personal financial distress (reported as the statistics  $r$ ) takes value  $-.527$ . According to the widely used rules established by Cohen, a correlation coefficient of  $r=.1$  is considered small,  $r=.3$  is moderate, and  $r=.5$  is large. In this situation, there is a large negative correlation. The correlation is given in the table, along with a significance value and a sample size of 400. This is the number of observations in which both fraud awareness and personal

financial distress were observed. The p-value (quoted under Sig. (2-tailed)) is  $<.001$  which reported as  $p < 0.001$  which is less than 0.01. Thus, there is significant evidence to reject the null hypothesis that the correlation is less than 0.001. As a result, this study would report the result as the variables fraud awareness and personal financial distress were significantly and largely negatively correlated  $r = -.527$ ,  $N = 400$ ,  $p < 0.001$ .

Table 4.14

*Correlations for Fraud Awareness and Empathy.*

Correlations			
		Total Fraud Awareness	Total Empathy
Total Fraud Awareness	Pearson Correlation	1	.788**
	Sig. (2-tailed)		<.001
	N	400	400
Total Empathy	Pearson Correlation	.788**	1
	Sig. (2-tailed)	<0.001	
	N	400	400
**. The significance level for correlation is 0.01 (2-tailed).			

Source: Information produced by SPSS Statistics.

Based on Table 4.14, the correlation between fraud awareness and empathy (reported as the statistics  $r$ ) takes value .788. In this situation, there is a large positive correlation. The correlation is given in the table, along with a significance value and a sample size of 400. This is the number of observations in which both fraud awareness and empathy were observed. The p-value (quoted under Sig. (2-tailed)) is  $<.001$  which reported as  $p < 0.001$  which is less than 0.01. Thus, there is significant evidence to reject the null hypothesis that the correlation is less than 0.001. As a result, this study would report

the result as the variables fraud awareness and empathy were significantly and largely positively correlated  $r=.788$ ,  $N=400$ ,  $p < 0.001$ .

Table 4.15

*Correlations of Fraud Awareness and Knowledge on Online Banking.*

Correlations			
		Total Fraud Awareness	Total Knowledge
Total Fraud Awareness	Pearson Correlation	1	.826**
	Sig. (2-tailed)		<.001
	N	400	400
Total Knowledge on online banking	Pearson Correlation	.826**	1
	Sig. (2-tailed)	<0.001	
	N	400	400
**. The significance level for correlation is 0.01 (2-tailed).			

Source: Information produced by SPSS Statistics.

Based on Table 4.15, the correlation between fraud awareness and knowledge (reported as the statistics  $r$ ) takes value 0.826. In this case, there is a significant positive association. The association is given in the table, along with a significance value and a sample size of 400. This is the number of observations in which both fraud awareness and knowledge were observed. The  $p$ -value (quoted under Sig. (2-tailed)) is <.001 which reported as  $p < 0.001$  which is less than 0.01. Thus, there is significant evidence to reject the null hypothesis that the correlation is less than 0.001. As a result, this study would report the result as the variables fraud awareness and knowledge were significantly and largely positively correlated  $r=.826$ ,  $N=400$ ,  $p < 0.001$ .

Table 4.16

*Correlations of Fraud Awareness and Attitude Towards Fraud.*

Correlations			
		Total Fraud Awareness	Total Attitude
Total Fraud Awareness	Pearson Correlation	1	.830**
	Sig. (2-tailed)		<.001
	N	400	400
Total Attitude	Pearson Correlation	.830**	1
	Sig. (2-tailed)	<0.001	
	N	400	400
**. The significance level for correlation is 0.01 (2-tailed).			

Source: Information produced by SPSS Statistics.

Based on Table 4.16, the correlation between fraud awareness and attitude (reported as the statistics  $r$ ) takes value .830. In this situation, there is a large positive correlation. The correlation is given in the table, along with a significance value and a sample size of 400. This is the number of observations in which both fraud awareness and knowledge were observed. The  $p$ -value (quoted under Sig. (2-tailed)) is <.001 which reported as  $p < 0.001$  which is less than 0.01. Thus, there is significant evidence to reject the null hypothesis that the correlation is less than 0.001. As a result, this study would report the result as the variables fraud awareness and attitude were significantly and largely positively correlated  $r = 0.830$ ,  $N = 400$ ,  $p < 0.001$ .

## 4.4 Inferential Analysis

### 4.4.1 Multiple Regression Analysis

Multiple linear regression techniques involve the use of two or more independent variables to make predictions about the dependent variable Y.

Table 4.17

*Model Summary.*

Model	R	R-square	Adjusted R-square	Std. Error of the Estimate	Durbin-Watson	F-Test	Probability of F test
1	0.866	0.750	0.747	2.97933	1.779	291.425	0.000

Source: Data generated from SPSS Statistics

R-squared is a statistical metric that measures the goodness of fit of a regression model, indicating the extent whereby the independent factors account for variation in the dependent variable. From Table 4.17, the R-squared value is 0.750, which implies that 75% of the variance in fraud awareness can be accounted for by the model that includes personal financial distress, empathy, knowledge of online banking, and attitude towards fraud. The R-squared value of 75% is quite high and it indicates that the predictions generated by the regression equation are relatively dependable.

Based on Table 4.17, the Durbin-Watson statistic has a value of 1.779. Typically, a value between 1.5 and 2.5 suggests the absence of significant autocorrelation, whereas values below 1.5 imply positive autocorrelation and values above 2.5 indicate negative autocorrelation. As the statistic is very near to 2, it can be concluded that there is no autocorrelation issue in this particular model. In this analysis, the F-value is 291.425 and the p-value is less than the significant level of 0.05. This indicates that the predictors in the model are both individually and collectively significant in explaining the variance in the outcome variable. When combined with a high R-squared value, a high F-value in a multiple regression analysis can point to both individually and collectively significant predictors, and it shows that the model fits the data well (Voyer & Voyer, 2014).

Table 4.18

*Multiple Regression Analysis.*

Model 1	Unstandardized Beta	Coefficient Std. Error	Standardized Beta	t-statistics	P-value (Sig.)	Collinearity Tolerance	Statistics VIF
Constant	5.695	1.1.92		4.778	<0.001		
PFD	-0.139	0.048	-0.089	-2.910	0.004	0.688	1.453
E	0.278	0.052	0.248	5.390	<0.001	0.301	3.318
KOB	0.208	0.052	0.250	3.983	<0.001	0.162	6.186
ATF	0.337	0.058	0.361	5.806	<0.001	0.165	6.069

Source: Data generated from SPSS Statistics.

The b-coefficients determined regression model:

$$\text{Fraud Awareness} = 5.695 - 0.139 \text{ Personal Financial Distress} + 0.278 \text{ Empathy} + 0.208 \text{ Knowledge} + 0.337 \text{ Attitude}$$

The above multiple linear equation demonstrates that there exists a negative relationship between fraud awareness and personal financial distress. Specifically, with every unit increase in personal financial distress, there is a decrease of 13.9% in fraud awareness. Conversely, there is a positive relationship between fraud awareness with empathy, knowledge of online banking, and attitude towards fraud. Each unit increase in empathy, knowledge of online banking, and attitude towards fraud results in an increase of 27.8%, 20.8%, and 33.7%, respectively, in fraud awareness.

In the coefficients table, the "Sig." column displays the p-value (2-tailed) for each b-coefficient. Typically, a b-coefficient is regarded as statistically significant if its p-value is less than 0.05. Given that all b-coefficients in the table have p-values below 0.05, it can be concluded that they are highly statistically significant.

In order to assess whether multicollinearity is present, VIF statistics can be observed for each of the variables. When the VIF value is between 1-10, it indicates that there is no multicollinearity issue. Conversely, if the VIF value is greater than 10, then there is a multicollinearity issue. In this case, the VIF values for each predictor variable are 1.453, 3.318, 6.186, and 6.069, respectively. As all these VIF values are between 1-10, it can be concluded that there is no multicollinearity between the independent factors.

## **4.5 Conclusion**

In short, several tests have been carried out to analyze the data that have been obtained from the survey questions that were distributed to approximately 400 respondents. The researcher has performed the test by using SPSS 29.0. From the reliability test, it is found that all the survey questions are reliable. Besides, the result also shows that there

is no autocorrelation, multicollinearity, and non-normality issue in this research study. Through the results of multiple regression analysis, there is a significant relationship between the dependent variable and 4 independent variables which are personal financial distress, empathy, knowledge on online banking, and attitude towards fraud.



## CHAPTER 5: DISCUSSION AND CONCLUSION

### 5.0 Introduction

This chapter goes into further depth on the findings from chapter four. First, a summary of the inferential analysis's findings is provided. Second, the explanations for how these outcomes were reached are examined. Thirdly, some recommendations for how to use the results are made. Finally, limitations of the study and ideas for further investigation are also covered.

### 5.1 Statistical Analysis Summary

Table 5.1

*Summary of the Statistical Findings.*

Independent Variables	T- statistics	P-value	Results
Personal Financial Distress	-2.910	0.004	significant
Empathy	5.390	<0.001	significant
Knowledge of Online Banking	3.983	<0.001	significant
Attitudes towards Fraud	5.806	<0.001	significant

Source: Data generated from SPSS Statistics.

Table 5.1 shows substantial connections between online banking fraud awareness and personal financial distress, empathy, online banking knowledge, and attitudes towards fraud. All the independent variables are therefore significant contributors to online banking fraud among UTAR students.

## **5.2 Discussion on Major Findings**

After being briefly described in section 5.1, the significant findings are more thoroughly examined in this section. Each of these findings is explored individually while being related to the university's work.

### **5.2.1 Personal Financial Distress and fraud awareness**

Based on the information obtained from SPSS statistics, it has indicated that there is significant relationship between personal financial distress and fraud awareness since the coefficient value is  $-0.527$  and the p-value ( $<0.001$ ) is lesser than the significance level (0.05). In this scenario, personal financial distress and fraud awareness are inversely correlated, whereby the higher the personal financial distress, the lower the fraud awareness. Therefore, it has verified this study's alternative hypothesis. Besides, it is also supported by the findings of Utami et al. (2019) which analyzed the financial distress in detecting fraudulent financial reporting.

Personal financial distress refers to a state of financial hardship or difficulty experienced by an individual, especially for a student. This can include a range of

financial problems such as high levels of debt in student fees, rental fees, overhead etc. For example, UTAR students were mainly from low to middle income families. Personal funding by parents was seen as the second most common source of funding after government scholarships or loans. Students who were personally funded were also most likely students who were not entitled to scholarships or loans due to a higher socioeconomic family background. A slightly worrying finding was that students who received PTPTN loans claimed that the amount that they received was not sufficient to pay their student fees and daily expenses due to the higher cost of living nowadays.

Personal financial distress can be a significant contributor to result in low fraud awareness among university students when they could not secure an education loan or scholarship and could struggle in paying their necessities such as accommodation, food, and academic materials.

### **5.2.2 Empathy and fraud awareness**

According to the data generated by using SPSS statistics, it has shown that empathy and fraud awareness have a significant relationship since its p-value ( $<0.001$ ) is lesser than the significance level (0.05). In this case, there is a positive relationship of empathy and fraud awareness, whereby the higher the degree of empathy, the higher the fraud awareness. It is also supported by the findings according to Krummeck (2000), which examined the role of ethical values in fraud prevention.

Typically, an educational organization will outline the importance of conveying ethical awareness, key moral values, ethical logical thinking and assure that students are aware of these ethical conduct in order to apply in life. Due to a desire to act morally, students

who show empathy in their personality can make moral decisions. In research from Brown et al.(2010), the case takes an example of fraud from the ACFE report to develop scenarios for asset misappropriation, and collects student feedback to learn more about their perception of and degree of awareness regarding fraud. The findings showed a correlation between empathy and ethical decision-making, indicating that those with higher levels of empathy are more likely to make ethical judgments. As a result, by extending the empathetic intentions that may have stronger self-awareness and caution towards financial fraud in real life, this study makes a significant contribution to the literature that is already in existence.

Individuals who are more empathic may be better able to understand the wants and motives of others, which may improve their capacity to spot and report fraudulent activity in an organisation. Also, those who are highly empathic might prioritise the welfare of others more frequently, which might lead to a higher commitment to moral behaviour and a deeper sense of responsibility to avoid fraudulent activity.

### **5.2.3 Knowledge on online banking and fraud awareness**

The results that generated by SPSS have indicated that the independent variable, knowledge on online banking and the dependent variable, fraud awareness have the significant relationship between each other since its p-value ( $<0.001$ ) is lesser than the significance level (0.05). In this case, there is a positive relationship of knowledge on online banking and fraud awareness, whereby the more the knowledge gained on online banking, the higher the fraud awareness. Therefore, it has validated the alternative hypothesis in the study. In addition, the findings is supported by Mat Dangi & M. Yacob (2013) and Leonard (2014).

Knowledge on online banking refers to the respondents' knowledge level on online banking. This related to one's educational level whereby Leonard (2014) has found out that influence on forensic accounting expertise has been enhancing fraud detection. The study has also pointed out that the knowledge gained from taking forensic lessons has helped and improved the students' abilities to spot fraud. It was evidenced by a higher overall average and higher individual scores. The design of this study makes it clear that the outcomes were caused by the forensic students' greater exposure to fraud training and instruction than by any other likely factor. Furthermore, Barker (2018) has also pointed out that using knowledge management approach has a significance in the management and control of messages on fraudulent e-banking transactions.

From the results shown, it is clearly stated that there is a significant relationship between knowledge and fraud awareness on online banking. In this case, each of the parties has to play their role in providing solutions for prevention. For example, UTAR could enhance the knowledge level of the students in this area by conducting talks or workshops for students to have a deeper understanding.

#### **5.2.4 Attitude towards fraud and fraud awareness**

According to the SPSS results, since the independent variable's p-value ( $<0.001$ ) is less than the significance level (0.05) and the dependent variable (fraud awareness) has a significant link with the independent variable (attitudes towards fraud). Therefore, there is a significant relationship between the two variables. Similar to this study, Bédard et al. (2015) investigated the relationship between accounting students' perceptions of fraud and their ethical decisions and behaviour. The study found a correlation between ethical behaviours and thinking and awareness of fraud. Students that were more conscious of fraud exhibited greater ethical action and cognition.

The study carried out by Ramanathan et al. (2020) in India is one study that offers proof of a substantial association between online banking fraud awareness and attitude towards fraud. The study sought to determine how customer trust and intent to use online banking services were affected by knowledge of online banking fraud. The findings revealed a substantial correlation between online banking fraud knowledge and attitude towards fraud, as well as a favourable association between online banking fraud awareness and customer trust and intention to use online banking services.

Similar to this, a study by Akar and Topcu (2018) looked at how trust, perceived risk, and awareness of online banking fraud relate to customers' intentions to use online banking in Turkey. The findings revealed a substantial correlation between online banking fraud awareness and attitude towards fraud, with online banking fraud awareness being positively connected to perceived risk and negatively related to trust.

Although the form and intensity of this association may differ based on the demographic and setting being investigated, these findings imply that there may be a significant relationship between online banking fraud awareness and attitude towards fraud. It is crucial that banks and other financial institutions take action to raise client knowledge of the risks associated with online banking fraud and to offer sufficient security measures to reduce those risks.

## **5.3 Implications of the study**

### **5.3.1 Practical implications**

The study showed a negative and significant relationship between personal financial distress and fraud awareness. The results showed that the higher the personal financial distress, the lower the fraud awareness. Therefore, increasing fraud awareness for those who are experiencing personal financial distress can be an important part in reducing their risk of financial harm. For example, there are still many UTAR students who may not have a good understanding of basic financial concepts such as budgeting, saving and investing. The school should provide financial education and resources that can assist them in developing the skills and knowledge to manage their finances effectively and avoid fraudulent activity. This can include workshops, seminars, and online resources on financial literacy.

Next, a positive and significant relationship has existed between empathy and fraud awareness. In order to increase fraud awareness, it could be helpful to approach the issue from an empathetic perspective. For example, UTAR students could discuss their thoughts and experiences on fraud and how to prevent it. This can create a sense of community and shared responsibility for preventing fraud. Moreover, customers like UTAR students should learn to evaluate information critically, especially those online informations. This can help them in identifying false information and scams.

In addition, the study showed that there is a positive and significant relationship between knowledge of online banking and fraud awareness. The best way to protect ourselves is to equip ourselves with knowledge on financial literacy as it is the best

protection against scams. Thus, the government should educate users about the different types of online banking such as phishing scams, malware and identity theft. Users like UTAR students should identify how these scams work and learn some tips on how to avoid them. Also, users like UTAR students must monitor accounts regularly for suspicious activity such as unauthorized transactions or changes to their account information.

Lastly, the attitude showed a positive and significant towards fraud awareness. With a positive attitude, users would always stay informed about the latest fraud trends and scams. This could help in recognizing suspicious activity and take steps to protect ourselves. As a result, the school should encourage individual like UTAR students to be skeptical of offers that seem too good to be true or that require them to disclose personal or financial information. They should also be aware of unsolicited emails, phone calls or text messages requesting such information. Furthermore, the school has to emphasize the consequences of fraud both for individuals who fall victim to it and society as a whole. This could help individuals understand the importance of taking steps to prevent fraud.

### **5.3.2 Theoretical implications**

Theory of Planned Behavior (TPB) explained fraud awareness issues in the context of predicting consumer behaviour in online banking. The theoretical implications include forecasting customer behavior in purchase decisions, such as the attitudes that UTAR students should have against fraud that occurs in this digital age. While using online banking to complete transactions, this predictive capability can help users build interventions based on the scenario while also being always aware of the presence of fraud. Each person behaves differently in terms of whether they have a positive or



negative attitude towards the risk of fraud in their lives; as a result, TPB can aid in improving their theoretical understanding to increase their shifting behaviour.

In contrast, the Protection Motivation Theory (PMT) explains why people choose to engage in protective behaviour when they perceive a threat and are motivated to defend themselves against it. In cases involving empathy and fraud awareness, PMT is used to encourage people to adopt protective behaviours so they can recognise the danger of online fraud that will affect them and create measures that enhance empathy and encourage extra caution in to prevent fraud. On the other hand, it is crucial for people to adopt protective behaviours in instances of personal financial difficulty related to fraud awareness in order to prevent losing control when under stress and losing their ability to distinguish between the appropriate actions and positive consequences to be taken.

While Technology Acceptance Model (TAM) contributes to enhancing users' experience in using online banking through convenient and perceived knowledge. With more in-depth knowledge of online banking, customers like UTAR students can adopt the right practises for using the service in the current digital era. Additionally, it helps the researcher increase user acceptance of online banking and improve user experience while lowering fraud risk all the time.

## **5.4 Limitations of study**

This section will explain a few of the study's limitations that were discovered. Firstly, the targeted audience of this research is university students that study in UTAR Kampar campus wher they have the highest percentage in encountered online banking fraud

since they are technology-savvy user. Besides, all of the undergraduate students that were taken into this survey study are Generation Z where they have followed the pace of digital technology development closely. In this case, it is interesting to investigate their fraud awareness in online banking. However, due to this study solely focuses on university students that pursue study in UTAR Kampar campus, it is impossible to accurately convey the knowledge that was gained on the influencing factors of online banking fraud awareness for the whole university students in Malaysia. It may be possible that the undergraduate student in other university in Malaysia have different perception and characteristics towards the topic.

In addition, as previously stated, this research study's participants are undergraduate students from the UTAR Kampar campus since they are all generation z where they have the high chances to encounter the online banking fraud and their awareness towards fraud is relatively low. Yet, there is other group age that have the higher possibility to run into online banking fraud or lower fraud awareness, such as Generation Z (1965 – 1979) and Millennial (1980 – 1994). It could provide a more interesting and comprehensive insight on the influencing factors on the online banking fraud awareness.

Last but not least, the core data for this study, which is quantitative research, was collected from 400 respondents on the UTAR Kampar campus using a questionnaire. The link between the dependent variable, fraud awareness, and the 4 independent variables which are personal financial distress, empathy, knowledge on online banking, and attitude towards fraud has been examined using the questionnaire. Questionnaire is being used in this research study due to it is convenience for the researchers to collect a huge amount of data that required 400 respondents. In other words, it improves the efficiency in the data collecting process. However, in the other side, the researchers unable to capture the feelings or emotions of the respondents throughout the questionnaire. In this case, the thoughts, ideas, behavior of the respondents towards the

online banking fraud awareness are difficult to examine and analyze in depth by the researchers.

## **5.5 Recommendations for future research**

In order that the topic may be studied more thoroughly, several components of the research can be improved in the upcoming studies looking at the influencing factors of online banking fraud awareness in UTAR. As a result, this section contains some recommendations.

The first recommendation is that future studies might take into account extending the reach of participants beyond simply those at UTAR Kampar campus when examining the influencing elements of online banking fraud awareness for undergraduate students in Malaysia. This would entail carrying out similar surveys at other universities or possibly among a larger group of Malaysian undergraduate students. This could increase the reliability of the findings and the capacity to extrapolate the findings to undergraduate students at other Malaysian universities.

The second recommendation is that future studies could take into account utilizing a mixed-methods methodology that blends quantitative surveys with qualitative interviews or focus groups (Yoon & Kim, 2018). This would enable researchers to learn more about the attitudes, beliefs, and actions of participants about their awareness of online banking fraud as well as their feelings and emotions to improve the validity and reliability of data collection methods. Researchers may get a completer and more accurate picture of people's awareness and behaviour regarding online banking fraud by combining a variety of study approaches. This can offer rich data that can

supplement the quantitative information gleaned from questionnaires and aid researchers in better understanding the variables affecting awareness of online banking fraud.

## **5.6 Conclusion**

The main purpose of this study is to understand the influencing factors to identify the influencing factors of online banking fraud awareness in UTAR. Data collection was done by the distribution of questionnaires, and data analysis was done using SPSS 29.0. The findings show that all the H1–H5 hypotheses are accepted. From the analysis conducted in the previous chapter, it shows that personal financial distress, empathy, knowledge of online banking and attitudes towards fraud have significant influence on fraud awareness. These findings are in-depth discussed, and some ramifications are offered. Finally, the limitations of the study are explored along with the associated recommendations for further research. As a result, this study may offer future researchers some valuable suggestions for choosing respondents and gathering data.

## REFERENCES

- A. (2021). 5 Cases of Historical Fraud that Transformed the World. Neural Technologies.
- Abdulwahab, L., Zulkhairi, M. D., & Galadima, M. B. (2011). Data screening and preliminary analysis of the determinants of user acceptance of Telecentre. *Journal of Information Systems: New Paradigms*, 1(1), 11-23.
- Adewumi, O. B., Aworinde, O. B., & Adewumi, A. O. (2016). The relationship between financial distress and electronic banking fraud awareness in Nigeria. *International Journal of Economics, Commerce and Management*, 4(11), 93-104.
- Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, 2(4), 314-324. DOI: <https://onlinelibrary.wiley.com/doi/abs/10.1002/hbe2.195>
- Akar, E., & Topcu, I. (2018). Examining the relationship between online banking fraud awareness, perceived risk, trust, and intention to use online banking in Turkey. *Electronic Commerce Research and Applications*, 30, 1-8. doi: 10.1016/j.elerap.2018.07.004
- Akhtar, N., Amin, M., & Azeem, M. U. (2020). Awareness of online banking frauds: The role of empathy, trust, and perceived risk in Pakistan. *Journal of Financial Crime*, 27(1), 190-203.
- Al-Aali, A. A., & Tee, M. Y. (2021). The influence of empathy on knowledge and awareness of online banking fraud among Saudi Arabian online banking users. *Journal of Financial Crime*, 28(1), 280-296.
- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2010). *Fraud examination*. South-Western Cengage Learning.
- Aldrich, J. O. (2018). *Using IBM SPSS statistics: An interactive hands-on approach*. Sage Publications

- Aldrich, J. O. (2019). *Using IBM SPSS statistics* (3rd ed.). Los Angeles, CA: SAGE Publications, Inc.
- Ali, M., Ismail, A. G., & Wahab, E. (2019). Financial literacy and its determinants among undergraduate students in Malaysia. *International Journal of Educational Research*, 1(1), 1-13. <https://doi.org/10.11648/j.ijedu.20190101.11>
- Alshare, K. A., & Alkhateeb, F. (2008). Predicting Students Usage of Internet in Two Emerging Economies Using an Extended Technology Acceptance Model (Tam). *The Academy of Educational Leadership Journal*, 12(2), 109. Retrieved from <https://www.questia.com/library/journal/1G1-190795467/predicting-students-usage-of-internet-in-two-emerging>
- Alzahrani, F., & Goodwin, R. (2018). The relationship between online banking fraud awareness and online banking usage: Evidence from Saudi Arabia. *International Journal of Business and Management*, 13(3), 60-67.
- Apuke, O. D. (2017). Quantitative Research Methods: A Synopsis Approach. Kuwait Chapter of Arabian Journal of Business and Management Review, 6(11), 40–47. <https://doi.org/10.12816/0040336>
- Association of Certified Fraud Examiners. (2020). Report to the Nations 2020: Global Study on Occupational Fraud and Abuse. Retrieved from <https://www.acfe.com/report-to-the-nations/2020/>
- Auto, H. (2021, August 1). Oh yes, young people may be easier targets for scams. *The Straits Times*. Retrieved from <https://www.staitstimes.com/business/invest/oh-yes-young-people-may-be-easier-targets-for-scams-0>
- Azhar, D. (2022). RM11k lost to online purchase fraud over 3 years. *Free Malaysia Today*. Retrieved from <https://www.freemalaysiatoday.com/category/nation/2022/03/14/rm1-6bil-lost-to-online-purchase-fraud-over-3-years/>
- Babakus, E., & Mangold, W. G. (1992). Adapting the SERVQUAL scale to hospital services: An empirical investigation. *Health Services Research*, 26(6), 767-786.

- Bagnoli, C., Lopes, R. A., & Marques, R. C. (2017). Online banking fraud prevention: Awareness versus behaviour. *Journal of Financial Crime*, 24(1), 122-133. <https://doi.org/10.1108/JFC-09-2015-0047>
- Barker, R. (2018). Knowledge management to prevent fraudulent e-banking transactions. *Communitas*, 23(1), 71–86. Retrieved from <https://doi.org/10.18820/24150525/comm.v23.5>
- Bédard, J. C., Bera, P., & Biggs, T. (2015). The impact of anti-fraud education on ethical perceptions of accounting students. *Journal of Business Ethics*, 126(1), 151-163. <https://doi.org/10.1007/s10551-013-1942-3>
- Bene, K. E., & Lee, J. (2018). The role of financial literacy in the relationship between financial distress and consumer fraud. *Journal of Financial Crime*, 25(4), 905-918. <https://doi.org/10.1108/JFC-11-2017-0091in>
- Bernamea. (2022). Banking industry launches National Scam Awareness Campaign. Retrieved from <https://www.nst.com.my/news/nation/2022/10/844999/Banking-industry-launches-national-scam-awareness-campaign>
- Blythe, J. M., & Coventry, L. (2019). Knowledge and awareness of online banking fraud among UK consumers. *Journal of Financial Crime*, 26(3), 769-781.
- BNM: Banks to migrate from SMS OTP to more secure forms of authentication. *www.thesundaily.my*. (2022). Retrieved from <https://www.thesundaily.my/business/bnm-banks-to-migrate-from-sms-otp-to-more-secure-forms-of-authentication-XK9873653>
- Borneo Post. (2022, June 1). Rampant internet banking fraud cases: Chong tells Putrajaya to look into banks' security system. Retrieved from <https://www.theborneopost.com/2022/06/02/rampant-internet-banking-fraud-cases-chong-tells-putrajaya-to-look-into-banks-security-system/>
- Boyd, B. K., Bergh, D. D., Ireland, R. D., & Ketchen, D. J. J. (2013). Constructs in strategic management. *Organizational Research Methods*, 16(1), 3-14.

- Branch locations. OCBC Bank. (2023). Retrieved from <https://www.ocbc.com.my/assets/pdf/branch-listing.pdf>
- Brown, T. A., Sautter, J. A., Littvay, L., Sautter, A. C., & Bearnes, B. (2010). Ethics and Personality: Empathy and Narcissism as Moderators of Ethical Decision Making in Business Students. *Journal of Education for Business*, 85(4), 203–208. <https://doi.org/10.1080/08832320903449501>
- Burke, J., Kieffer, C. N., Mottola, G. R., & Pérez-Arce, F. (2021, January 14). Can educational interventions reduce susceptibility to financial fraud? SSRN. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3747165](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747165)
- Burns, S., & Roberts, L. D. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, 15(1), 48–64. <https://doi.org/10.1057/cpcs.2012.13>
- Button, M., & Brooks, G. (2012). Identifying and understanding fraud risks. In M. Button & G. Brooks (Eds.), *Handbook of fraud* (pp. 25-38). Wiley.
- Chakrabarty, K. C. (2013). Fraud in the banking sector—causes, concerns and cures. In National Conference on Financial Fraud organised by ASSOCHAM, New Delhi, 26
- Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of internet banking: An empirical study in Hong Kong. *Science Direct*, 1558–1572. Retrieved from <https://doi.org/10.1016/j.dss.2006.01.002>
- Chin, L. K., Chua, Y. X., & Choo, K. L. (2018). Factors influencing individual behaviour in online banking fraud. *Journal of Financial Crime*, 25(1), 169-182. <https://doi.org/10.1108/JFC-07-2016-0049>
- Choi, J., Kruis, N., & Lee, J. (2022). Empathy, self-control, and online harassment: A partial test of Agnew's social concern theory. *Computers in Human Behavior*, 136, 107402. <https://doi.org/10.1016/j.chb.2022.107402>



- Christian, N., Basri, Y. Z., & Arafah, W. (2019). Analysis of fraud pentagon to detecting corporate fraud in Indonesia. *International Journal of Economics, Business and Management Research*, 3(8). DOI: [https://ijebmr.com/uploads/pdf/archivepdf/2020/IJEBMR\\_420.pdf](https://ijebmr.com/uploads/pdf/archivepdf/2020/IJEBMR_420.pdf)
- Cressey, D. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. New York, NY: Free Press.
- Cyber security strategy to provide direction on curbing cyber threats. (2020, September 14). *TheMalaysianReserve.Com*. Retrieved from <https://themalaysianreserve.com/2020/09/14/cyber-security-strategy-to-provide-direction-on-curbing-cyber-threats/>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340. Retrieved from <https://www.jstor.org/stable/249008>
- Demir, S. (2022). Comparison of normality tests in terms of sample sizes under different skewness and Kurtosis coefficients. *International Journal of Assessment Tools in Education*, 9(2), 397-409. <https://dergipark.org.tr/en/pub/ijate/issue/69546/1101295>
- Devi, P. N. C., Widanaputra, A. A. G. P., Budiasih, I. G. A. N., & Rasmini, N. K. (2021). The effect of fraud Pentagon theory on financial statements: Empirical evidence from Indonesia. *The Journal of Asian Finance, Economics and Business*, 8(3), 1163-1169. DOI: <https://koreascience.kr/article/JAKO202106438543732.page>
- Dew, J., Stewart, R., & Kinsey, J. (2017). Financial distress and online banking behavior. *Journal of Financial Counseling and Planning*, 28(2), 235-248. <https://doi.org/10.1891/1052-3073.28.2.235>
- Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers.
- European Commission. (2020). *Consumers - european commission. SURVEY ON "SCAMS AND FRAUD EXPERIENCED BY CONSUMERS" Final Report*. Retrieved from [https://ec.europa.eu/info/sites/default/files/aid\\_development\\_cooperation\\_fundamental\\_rights/ensuring\\_aid\\_effectiveness/documents/survey\\_on\\_scams\\_and\\_fraud\\_experienced\\_by\\_consumers\\_-\\_final\\_report.pdf](https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf)

- Faith, J. (2015, December 2). A history of fraud through the ages and how to avoid being a victim - Your Money. Retrieved from <https://www.yourmoney.com/credit-cards-loans/a-history-of-fraud-through-the-ages-and-how-to-avoid-being-a-victim/>
- Federal Trade Commission. (2021). Consumer Sentinel Network Data Book 2020. Retrieved from [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book2020/consumer\\_sentinel\\_network\\_data\\_book\\_2020.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book2020/consumer_sentinel_network_data_book_2020.pdf)
- Free Malaysia Today. (2022). Fake Petronas Lucky Draw Ad Contains Malware, Say Police. Retrieved from <https://www.freemalaysiatoday.com/category/nation/2022/04/22/fake-petronas-lucky-draw-ad-contains-malware-say-police/>
- Galazova, S. S., & Magomaeva, L. R. (2019). The transformation of traditional banking activity in digital. *International Journal of Economics and Business Administration*, VII(Special Issue 2), 41–51. Retrieved from <https://doi.org/10.35808/ijeba/369>
- Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism*, 10(2), 486-489.
- Golden, S. a. R. (2016). Users' Preference Towards Traditional Banking Versus E-Banking – An Analysis. Retrieved from <https://www.semanticscholar.org/paper/USERS%E2%80%99-PREFERENCE-TOWARDS-TRADITIONAL-BANKING-%E2%80%93-AN-Golden/208399870768fef9020b0ff91cc978d9bd598fd3>
- Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, 50(5), 2572-2593. DOI: <https://bera-journals.onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12864>
- Greenberg, M. J. (2016). *Ethical dilemmas and decisions in criminal justice* (10th ed.). Cengage.
- Hamsi, A. S., Bahry, F. D. S., Tobi, S. N. M., & Masrom, M. (2015). *Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives*,

Connecting Factors and Keys to the Problem. *Journal of Management Research*, 7(2), 169. <https://doi.org/10.5296/jmr.v7i2.6938>

Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11 11(4), 395–404. <https://doi.org/10.3844/jssp.2015.395.404>

Hoggatt, J., Leach, J., & Warren, J. (2016). Knowledge, awareness, and attitudes of online banking users in Alabama. *Journal of Financial Crime*, 23(4), 942-955.

Horwarth, C. (2011). *The Mind Behind the Fraudster Crime: Key Behavioral and Environmental Element*. USA Crowe Horwarth International. Retrieved from [https://www.fraudconference.com/uploadedFiles/Fraud\\_Conference/Content/Course-Materials/presentations/23rd/ppt/10C-Jonathan-Marks.pdf](https://www.fraudconference.com/uploadedFiles/Fraud_Conference/Content/Course-Materials/presentations/23rd/ppt/10C-Jonathan-Marks.pdf)

Hossain, M. M., Sarker, A. H., & Rayhan, A. (2021). The mediating role of empathy on the relationship between personal innovativeness and online banking fraud awareness. *Journal of Financial Crime*, 28(2), 630-647. Retrieved from <https://www.yourmoney.com/credit-cards-loans/a-history-of-fraud-through-the-ages-and-how-to-avoid-being-a-victim/>

Huang, L., Lu, Y., & Zhang, Y. (2020). Understanding the impact of personal financial distress on fraud victimization: Evidence from China. *Journal of Financial Crime*, 27(2), 374-388. <https://doi.org/10.1108/JFC-05-2019-0073>

Huang, L., Soutar, G. N., & Brown, A. (2015). Financial stress and financial fraud awareness: Lessons from the US experience. *Journal of Financial Services Research*, 47(3), 291-310. <https://doi.org/10.1007/s10693-014-0192-1>.

Indra. (2014). *From the traditional banking system to the customer-centric financial ecosystem* Retrieved from [https://www.indracompany.com/sites/default/files/banking\\_trends\\_october\\_2014\\_v.\\_pc.pdf](https://www.indracompany.com/sites/default/files/banking_trends_october_2014_v._pc.pdf)

Jones, B., & Han, S. (2018). Financial self-efficacy, financial stress, and fraud susceptibility. *Journal of Financial Crime*, 25(1), 186-199. <https://doi.org/10.1108/JFC-05-2017-0041>

- Jones, C. J., & Schilling, J. (2019). Consumer fraud prevention behaviors in online and offline channels. *Journal of Financial Services Marketing*, 24(4), 96-107. <https://doi.org/10.1057/s41264-019-00062-4>
- Jones, C. M. (2009). Utilizing the technology acceptance model to assess employee adoption of information systems security measures. Nova Southeastern University. Retrieved from <https://search.proquest.com/openview/5610192cb80f662d4308633147e172c/1?pq-origsite=gscholar&cbl=18750>
- Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British Journal of Applied Science and Technology*, 7(4), 396-403
- Junaidi, J., & Lestari, S. P. (2019). Fraud awareness, moral intensity, and ethical values: The Indonesian auditors' perspective. *Journal of Financial Crime*, 26(2), 479-489. <https://doi.org/10.1108/JFC-08-2018-0099>
- Kabir, S. S. (2016). Methods of data collection. ResearchGate. Retrieved from [https://www.researchgate.net/publication/325846997\\_Methods\\_Of\\_Data\\_Collection](https://www.researchgate.net/publication/325846997_Methods_Of_Data_Collection)
- Kim, J., & Garman, E. T. (2003). Financial Stress and Absenteeism: An Empirically Derived Model. Social Science Research Network. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2265634](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265634)
- Kim, H. Y. (2013). Statistical notes for clinical researchers: assessing normal distribution (2) using skewness and kurtosis. *Restorative dentistry & endodontics*, 38(1), 52-54. <https://synapse.koreamed.org/articles/1090037>
- Knechel, W. R., & Mintchik, N. (2021). Do Personal Beliefs and Values Affect an Individual's "Fraud Tolerance"? Evidence from the World Values Survey. *Journal of Business Ethics*, 177(2), 463–489. <https://doi.org/10.1007/s10551-020-04704-0>
- Kouchaki, M., Wilson, D. S., & Lount Jr, R. B. (2020). The dark side of empathy in the workplace. *Academy of Management Review*, 45(1), 112-135. <https://doi.org/10.5465/amr.2017.0355>

- Krambia-Kapardis, M., & Zopiatis, A. (2017). The relationship between fraud awareness and attitudes towards fraud: Evidence from the hospitality industry. *Journal of Financial Crime*, 24(2), 263-276. <https://doi.org/10.1108/JFC-11-2015-0065>
- Krummeck, S. (2000). The role of ethics in fraud prevention: a practitioner's perspective. *Business Ethics: A European Review*, 9(4), 268-272. <https://doi.org/10.1111/1467-8608.00200>
- Kveder, A., & Galico, A. (2008). Guidelines for cleaning and harmonization of generations and gender survey data. Retrieved from [https://www.ggp-i.org/sites/default/files/questionnaires/GGP\\_2008\\_DCHGuide\\_1.pdf](https://www.ggp-i.org/sites/default/files/questionnaires/GGP_2008_DCHGuide_1.pdf)
- Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, 20(4), 3514. <https://doi.org/10.3390/ijerph20043514>
- Leonard, M. (2014). The Impact of Fraud Education on Fraud Detection. *Accounting*. 10. Retrieved from [https://scholarsarchive.library.albany.edu/honorscollege\\_accounting/10](https://scholarsarchive.library.albany.edu/honorscollege_accounting/10)
- Lewis, J. R. (Jim). (2019). Comparison of Four TAM Item Formats: Effect of Response Option Labels and Order. *Journal of User Experience*, 14(4), 224-236. Retrieved from [https://uxpajournal.org/wp-content/uploads/sites/7/pdf/JUS\\_Lewis\\_August2019.pdf](https://uxpajournal.org/wp-content/uploads/sites/7/pdf/JUS_Lewis_August2019.pdf)
- Liang, W., & Chen, C. (2019). Can empathy lead to financial fraud reporting? The roles of moral identity and self-efficacy. *Journal of Business Ethics*, 158(1), 207-222. <https://doi.org/10.1007/s10551-017-3685-7>
- Ly, B., & Ly, R. (2022). Internet banking adoption under technology acceptance model—evidence from Cambodian users. *Computers in Human Behavior Reports*, 7, 100224. <https://doi.org/10.1016/j.chbr.2022.100224>

- Mail, M. (2022). In KL, bank officer loses more than RM200,000 to online loan fraud. *Malay Mail*. Retrieved from <https://www.malaymail.com/news/malaysia/2022/04/06/in-kl-bank-officer-loses-more-than-rm200000-to-online-loan-fraud/2051960>
- Ma-Kellams, C., & Blascovich, J. (2011). The effects of self-affirmation on implicit associations of the self with honesty and fraud. *Personality and Social Psychology Bulletin*, 37(4), 490-499. <https://doi.org/10.1177/0146167211399103>
- Malay Mail. (2022, May 3). How young people could be more likely than their elders to get scammed online. *Malay Mail*. Retrieved from <https://www.malaymail.com/news/life/2022/05/03/how-young-people-could-be-more-likely-than-their-elders-to-get-scammed-onli/2056882>
- Mansor, M., Sabri, M. F., Mansur, M., Ithnin, M., Magli, A. S., Husniyah, A. R., Janor, H. (2022). Analysing the Predictors of Financial Stress and Financial Well-Being among the Bottom 40 Percent (B40) Households in Malaysia. *International Journal of Environmental Research and Public Health*, 19(19), 12490. Retrieved from <https://doi.org/10.3390/ijerph191912490>
- Mat Dangi, M. R., & M. Yacob, N. H. (2013). Examining the fraud awareness from the university's academic staffs perspectives / Mohamad Ridhuan Mat Dangi and Noor Hasimah M. Yacob. *UiTM Institutional Repository*. Retrieved from <https://ir.uitm.edu.my/id/eprint/29604/>
- Migrate from OTP texts to curb online scams, BNM tells banks. *TheSunDaily*. (2022). Retrieved from <https://www.freemalaysiatoday.com/category/nation/2022/09/26/migrate-from-otp-texts-to-curb-online-scams-bnm-tells-banks/>
- Mohamad, M. M., Sulaiman, N. L., Sern, L. C., & Salleh, K. M. (2015). Measuring the validity and reliability of Research Instruments. *Procedia - Social and Behavioral Sciences*, 204, 164–171. Retrieved from <https://doi.org/10.1016/j.sbspro.2015.08.129>
- Mohd Padil, H., Kasim, E. S., Muda, S., Ismail, N., & Md Zin, N. (2021). Financial literacy and awareness of investment scams among university students. *Journal of Financial Crime*, 29(1), 355–367. <https://doi.org/10.1108/jfc-01-2021-0012>

- Mohsin, H. A. (2016). A manual of selecting sampling techniques in research. ResearchGate. Retrieved from [https://www.researchgate.net/publication/303941309\\_A\\_Manual\\_for\\_Selecting\\_Sampling\\_Techniques\\_in\\_Research](https://www.researchgate.net/publication/303941309_A_Manual_for_Selecting_Sampling_Techniques_in_Research)
- Nair, K. (2022, October 1). The rise of online financial fraud in Malaysia. The Star. Retrieved from <https://www.thestar.com.my/business/business-news/2022/10/01/the-rise-of-online-financial-fraud-in-malaysia>
- Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research*, 19(2), 129–132. <https://doi.org/10.1177/1362168815572747>
- Nor, K. M., Shanab, E. A. A., & Pearson, J. M. (2008). Internet banking acceptance in Malaysia based on the theory of reasoned action. *Journal of Information Systems and Technology Management*, 5(1).
- Omar, S. S., Muda, M., & Zainuddin, Y. (2019). Online banking fraud: Investigating the relationship between awareness and personal values in Malaysia. *Journal of Financial Crime*, 26(1), 59-70.
- Online fraud accounts for 68% of commercial crime, says IGP. (2022). *Freemalaysiatoday*. Retrieved from <https://online-fraud-accounts-for-68-of-commercial-crime-says-igp/>
- Pappu Rajan, A., Saranya, G. (2018). Digital Banking Services: Customer Perspectives, 5(12). Retrieved from [https://www.researchgate.net/publication/332028540\\_Digital\\_Banking\\_ServicesCustomer\\_Perspectives](https://www.researchgate.net/publication/332028540_Digital_Banking_ServicesCustomer_Perspectives)
- Prawitz, A. D., Garman, E. T., Sorhaindo, B., O'Neill, B., Kim, J., & Drentea, P. (2006). The incharge financial distress/financial well-being scale: Establishing validity and reliability. *Fin Counsel Plan*, 17, 34-50. Retrieved from <http://pfeef.org/wp-content/uploads/2016/09/Establishing-Validity-and-Reliability-Proceedings.pdf>
- Pugazhendhi, S., & Kanimozhi, V. (2019). Fraud awareness and attitude towards fraud among banking employees in India. *International Journal of Ethics and Systems*, 35(3), 419-436. <https://doi.org/10.1108/IJOES-11-2018-0137>

- Rahimi, B., Nadri, H., Afshar, H. L., & Timpka, T. (2018). A systematic review of the technology acceptance model in health informatics. *Applied clinical informatics*, 9(03), 604-634. DOI: <https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0038-1668091>
- Ramadhan, D. (2022). Strengthening Integrity and Fraud Awareness in Preventing Fraud During the Covid-19 Pandemic. *Asia Pacific Fraud Journal*, 7(2), 213. <https://doi.org/10.21532/apfjournal.v7i2.266>
- Ramamoorti, S., Robertson, J., Sylph, J., & Cochran, J. (2010). The impact of fraud awareness education on student attitudes and intentions. *Journal of Education for Business*, 85(3), 141-149. <https://doi.org/10.1080/0883232090352374>
- Ramanathan, R., Raja, S., & Srinivasan, A. (2020). Impact of online banking fraud awareness on customer trust and intention to adopt online banking services. *International Journal of Bank Marketing*, 38(1), 16-33. doi: 10.1108/IJBM-03-2019-0098
- Razak, N. A., Dahalan, N. H., & Ahmed, U. (2017). Understanding online banking frauds: The role of empathy and fraud awareness. *Journal of Financial Crime*, 24(2), 246-259.
- Rezvani, S., Mohammadi, M., Dehkordi, A. H., & Zarafshani, K. (2016). Factors affecting the fraud awareness of the elderly in the United States: A study based on the National Elder Fraud Survey. *Journal of Financial Crime*, 23(4), 841-855. <https://doi.org/10.1108/JFC-01-2016-0005>
- Rupeika-Apoga, R., Zaidi, H.S., Thalassinios, E.Y. and Thalassinios, I.E. 2018. Bank Stability: The Case of Nordic and Non-Nordic Banks in Latvia. *International Journal of Economics & Business Administration*, 6(2), 39-55
- Sekaran, U., & Bougie, R. (2009). *Research methods for business: A skill-building approach* (5th ed.). West Sussex, United Kingdom: John Wiley & Sons, Inc.
- Sekaran, U., & Bougie, R. (2010). *Research methods for business* (5th ed.). West Sussex, United Kingdom: John Wiley & Sons, Inc.



- Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th ed.). West Sussex, United Kingdom: John Wiley & Sons, Inc.
- Shafiei, A., & Maleksaeidi, H. (2020). Pro-environmental behavior of university students: Application of protection motivation theory. *Global Ecology and Conservation*, 22, e00908. DOI: <https://www.sciencedirect.com/science/article/pii/S2351989419305955>
- Siahaan, M., Umar, H., & Purba, R. B. (2019). Fraud Star Drives to Asset Misappropriation Moderated by Internal Controls. *Journal of Southwest Jiaotong University*, 54(4). Retrieved from <http://www.jsju.org/index.php/journal/article/view/336>
- Teo, T. S. H., & Yap, K. H. (2019). The influence of affective states and empathic concern on online banking security threat awareness. *Internet Research*, 29(2), 376-396.
- UNSW Online. (2020, January 30). Types of data & the scales of measurement. Retrieved from <https://studyonline.unsw.edu.au/blog/types-of-data#:~:text= Scales%20of%20measurement%20is%20how,to%20properly%20analyse%20 the%20data.>
- Voyer, D., & Voyer, S. D. (2014). Gender differences in scholastic achievement: A meta-analysis. *Psychological Bulletin*, 140(4), 1174–1204. <https://doi.org/10.1037/a0036620>
- Wang, J., Liu-Lastres, B., Ritchie, B. W., & Mills, D. J. (2019). Travellers' self-protections against health risks: An application of the full Protection Motivation Theory. *Annals of Tourism Research*, 78, 102743. DOI: <https://www.sciencedirect.com/science/article/abs/pii/S0160738319300945>
- Wang, Y., & Wang, Y. (2020). Examining the effectiveness of educational intervention on phishing susceptibility: The moderating role of online banking knowledge. *Journal of Financial Crime*, 27(2), 438-452. <https://doi.org/10.1108/JFC-05-2019-0057>
- WebWay E Services. (2021). Profile Universiti Tunku Abdul Rahman (UTAR) - Where To Study. StudyMalaysia.Com. Retrieved from <https://www.study-malaysia.com/where/profile.php?code=utar>

- Wilkes, R. E. (1978). Fraudulent Behavior by Consumers. *Journal of Marketing*, 42(4), 67. <https://doi.org/10.2307/1250088>
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. <https://doi.org/10.1016/j.chb.2017.03.002>
- Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond : Considering the Four Elements of Fraud: Certified Public Accountant. *The CPA Journal*, 74(12), 38-42.
- Yoon, D., & Kim, H. (2018). Understanding the factors influencing online banking fraud awareness of Korean consumers: A comparative analysis between non-victims and victims. *Journal of Financial Crime*, 25(2), 361-374. doi: 10.1108/JFC-09-2016-0069
- Yr, R. D., & Ariandi, I. (2017). The effect of internal control and anti-fraud awareness on fraud prevention (A survey on inter-governmental organizations). *Journal of Economics, Business & Accountancy Ventura*, 20(1), 113. <https://doi.org/10.14414/jebav.v20i1.751>
- Yuri, I.A. and Sari, M.R. (2022) “Fraud awareness and fraud detection-prevention methods in the Indonesian private and public sector,” *Global Financial Accounting Journal*, 6(1), p. 100. Retrieved from <https://doi.org/10.37253/gfa.v6i1.6529>.
- Yuriev, A., Dahmen, M., Paillé, P., Boiral, O., & Guillaumie, L. (2020). Pro-environmental behaviors through the lens of the theory of planned behavior: A scoping review. *Resources, Conservation and Recycling*, 155, 104660. DOI: <https://www.sciencedirect.com/science/article/abs/pii/S092134491930566>

## APPENDICES

### Appendix 1: Ethical Approval for Research Project



**UNIVERSITI TUNKU ABDUL RAHMAN** DU012(A)  
Wholly owned by UTAR Education Foundation Co. No. 578227-M

Re: U/SERC/216/2022

3 November 2022

Ms Thavamalar a/p Ganapathy  
Head, Department of Economics  
Faculty of Business and Finance  
Universiti Tunku Abdul Rahman  
Jalan Universiti, Bandar Baru Barat  
31900 Kampar, Perak.

Dear Ms Thavamalar,

#### Ethical Approval For Research Project/Protocol

We refer to your application for ethical approval for your students' research project from Bachelor of Economics (Honours) Financial Economics programme enrolled in course UBEZ3026. We are pleased to inform you that the application has been approved under Expedited Review.

The details of the research projects are as follows:

No.	Research Title	Student's Name	Supervisor's Name	Approval Validity
1.	The Influencing Factors of Online Banking Fraud Awareness Among Genders in UTAR	1. Chin Ke Li 2. Tan Xin Tong 3. Tang Jia Hooi 4. Toh Khai Li	Pn Siti Nur Amira Binti Othman	3 November 2022 – 2 November 2023
2.	Factors Influence Senior Tourism in Malaysia	1. Chong Zi Cheng 2. Leong Mun Heng	Ms Kalai Vani a/p Kalimuthu	
3.	Determinants of Unemployment Among Fresh Graduates in Malaysia Before and During Covid-19 Pandemic	1. Heng Han Quan 2. Lim Chan Hong 3. Theo Daniel Wee Xin Lik 4. Yep Zhen Yi	Ms Thavamalar a/p Ganapathy	
4.	Online Payment Fraud: What Have Cause It?	1. Cheang Xin Yi 2. Lim Jas Min 3. Ng Kha Yong 4. Thor Min Hui	Dr Chen Fanyu	

The conduct of this research is subject to the following:

- (1) The participants' informed consent be obtained prior to the commencement of the research;
- (2) Confidentiality of participants' personal data must be maintained; and
- (3) Compliance with procedures set out in related policies of UTAR such as the UTAR Research Ethics and Code of Conduct, Code of Practice for Research Involving Humans and other related policies/guidelines.
- (4) Written consent be obtained from the institution(s)/company(ies) in which the physical or/and online survey will be carried out, prior to the commencement of the research.

Kampar Campus : Jalan Universiti, Bandar Barat, 31900 Kampar, Perak Darul Ridman, Malaysia  
Tel: (603) 468 8888 Fax: (603) 466 1313  
Sungai Long Campus : Jalan Sungai Long, Bandar Sungai Long, Cheras, 43000 Kajang, Selangor Darul Ehsan, Malaysia  
Tel: (603) 9086 0288 Fax: (603) 9019 8868  
Website: www.utar.edu.my



Should the students collect personal data of participants in their studies, please have the participants sign the attached Personal Data Protection Statement for records.

Thank you.

Yours sincerely,



**Professor Ts Dr Faidz bin Abd Rahman**  
Chairman  
UTAR Scientific and Ethical Review Committee

c.c    Dean, Faculty of Business and Finance  
         Director, Institute of Postgraduate Studies and Research

Kampar Campus : Jalan Universiti, Bandar Barat, 31900 Kampar, Perak Darul Ridzuan, Malaysia  
Tel: (605) 468 8888 Fax: (605) 466 1313  
Sungai Long Campus : Jalan Sungai Long, Bandar Sungai Long, Cheras, 43000 Kajang, Selangor Darul Ehsan, Malaysia  
Tel: (603) 9086 0288 Fax: (603) 9019 8868  
Website: [www.utar.edu.my](http://www.utar.edu.my)



Appendix 2: Survey Questionnaire.

Dear Respondents,

We are undergraduates from Universiti Tunku Abdul Rahman. There is a total of 4 of us in a group, and we are currently taking Bachelor of Economics (Honours) Financial Economics. As partial fulfillment for the completion of our degree program, we are now conducting research entitled: The Influencing Factors of Online Banking Fraud Awareness in UTAR

This study investigates the relationships between personal financial distress, empathy, knowledge of online banking, and attitude towards fraud-on-fraud awareness among the UTAR students.

Your participation in this research is greatly appreciated to make this study successful. There are no right or wrong answers to the questionnaire as the survey is on individual perceptions, and participation in this study is voluntary. This questionnaire would take a few minutes of your valuable time to complete by answering all the questions. We are highly appreciative of your contribution to this study since it might contribute to improving higher levels of fraud awareness among genders.

This survey is a complete requirement for academic research. This study will use only aggregated data for academic work and not for commercial purposes. Your particulars will remain anonymous and will be treated as strictly confidential.

Should you have any doubt feel free to contact the researchers:

Tan Xin Tong(tanxintong27@lutar.my)

Chin Ke Li (kellychin@lutar.my)

Tang Jia Hooi (jtangh100@lutar.my)

Toh Khai Li (kellytoh0622@1utar.my).

Thank you very much for your valuable time and kind cooperation.

#### PERSONAL DATA PROTECTION NOTICE

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.

1. Personal data refers to any information which may directly or indirectly identify a person which could include sensitive personal data and expression of opinion. Among others it includes:

- a) Name
- b) Identity card
- c) Place of Birth
- d) Address
- e) Education History
- f) Employment History
- g) Medical History
- h) Blood type
- i) Race
- j) Religion

- k) Photo
  - l) Personal Information and Associated Research Data
2. The purposes for which your personal data may be used are inclusive but not limited to:
- a) For assessment of any application to UTAR
  - b) For processing any benefits and services
  - c) For communication purposes
  - d) For advertorial and news
  - e) For general administration and record purposes
  - f) For enhancing the value of education
  - g) For educational and related purposes consequential to UTAR
  - h) For replying any responds to complaints and enquiries
  - i) For the purpose of our corporate governance
  - j) For the purposes of conducting research/ collaboration
3. 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.

4. 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.

5. 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:

6. By submitting or providing your personal data to UTAR, you had consented and agreed for your personal data to be used in accordance to the terms and conditions in the Notice and our relevant policy.

7. 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.

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



Acknowledgment of Notice

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

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

SECTION A: DEMOGRAPHIC

Please tick at the appropriate box or fill in the blank for each of the following questions:

UTAR Mail:

---

Age:

18

19

20

21

22

23

24

others

Gender:

Female

Male

Number of online banking accounts:

0

1

2

3 and above

How often do you use online banking:

Daily

Weekly

Monthly

Yearly

Never

Have you ever encountered online banking fraud?

Yes

No

If yes, please state the number of times getting into fraud:

\_\_\_\_\_

SECTION B: FRAUD AWARENESS

On a scale from 1 (**Strongly Disagree**) to 5 (**Strongly Agree**), how much do you agree or disagree with the following statements:

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I am suspicious of letters or e-mails containing spelling and grammar mistakes.					
I avoid clicking links in emails or text messages unless I know the sender.					
I install anti-spam software or anti-virus software.					
I only provide my identity card or					

information on a secured application.					
I subscribe to a specific service to avoid commercial calls.					
I transfer money from any platform to someone that I don't know.					

SECTION C: PERSONAL FINANCIAL DISTRESS

On a scale from 1 (**Strongly Disagree**) to 5 (**Strongly Agree**), how much do you never or always with the following statements

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	1	2	3	4	5
I feel stressed about my personal finances in general.					
I often worry about being able to meet my					

normal monthly living expenses.					
I frequently find myself just getting by financially and living paycheck to paycheck.					
I seldom go out to eat, watch movies or any entertainment activity because I can't afford it.					
I am satisfied with my current financial situation.					

SECTION D: EMPATHY

On a scale from 1 (**Strongly Disagree**) to 5 (**Strongly Agree**), how much do you agree or disagree with the following statements:

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I tend to lose control if I am falling into an online fraud trap.					
In the case of unfair online shopping experiences, I tend to seek revenge.					
I find difficulties in being capable of empathizing with the fraudsters' perspective.					
It is quite common for me to criticize fraudsters that I feel are unfair or harmful.					

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I tend to lose control if I am falling into an online fraud trap.					
In the case of unfair online shopping experiences, I tend to seek revenge.					
Fraudsters are not a person that I feel empathy toward.					

SECTION E: KNOWLEDGE OF ONLINE BANKING

On a scale from **1 (Strongly disagree)** to **5 (Strongly agree)**, how much do you agree or disagree with the following statements:

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I would find it easy to get the online banking services to do what I want to do					
I would find this online banking services is user-friendly and easy-to-use					
Online banking has enhanced my productivity and efficiency in performing the banking services					
In my opinion, using online banking					



services is a good and wise idea					
I would feel secure sending sensitive information across the online banking					
My family, friends, and peers are currently using online banking					

SECTION F: ATTITUDE TOWARDS FRAUD

On a scale from 1 (**Strongly Disagree**) to 5 (**Strongly Agree**), how much do you agree or disagree with the following statements:

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
Although I have used online banking safely for many times, fraudulent problems may occur in the future.					
I trust the bank's system will perform my process of transaction correctly.					
I always believe that the information provided on the bank's website is accurate.					
The chances of losing money if I use online banking are low.					

	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
Scammers might take control of my account if I use online banking.					
When online banking involves fraud, I intend to stop using it.					

Appendix 3: SPSS Data Analysis Result

Appendix 3.1: Reliability Test of Variable.

1) Fraud Awareness

<b>Case Processing Summary</b>			
		N	%
Cases	Valid	400	100.0
	Excluded <sup>a</sup>	0	.0
	Total	400	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability

Scale: ALL VARIABLES

<b>Reliability Statistics</b>		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.828	.813	6

2) Personal Financial Distress

**Case Processing Summary**

		N	%
Cases	Valid	400	100.0
	Excluded <sup>a</sup>	0	.0
	Total	400	100.0

a. Listwise deletion based on all variables in the procedure.

**Reliability Statistics**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.729	.733	5

3) Empathy

		N	%
Cases	Valid	400	100.0
	Excluded <sup>a</sup>	0	.0
	Total	400	100.0

a. Listwise deletion based on all variables in the procedure.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.865	.865	5

4) Knowledge on Online Banking

**Case Processing Summary**

		N	%
Cases	Valid	400	100.0
	Excluded <sup>a</sup>	0	.0
	Total	400	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability

Scale: ALL VARIABLES

**Reliability Statistics**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.947	.947	6

5) Attitude Towards Fraud

**Case Processing Summary**

		N	%
Cases	Valid	400	100.0
	Excluded <sup>a</sup>	0	.0
	Total	400	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability

Scale: ALL VARIABLES

**Reliability Statistics**

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.904	.905	6



Appendix 3.2: Multiple Regression Analysis Result

<b>Model Summary<sup>b</sup></b>										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson					
1	.866 <sup>a</sup>	.750	.747	2.97933	1.779					
<p>a. Predictors: (Constant), Total_Attitude, Total_Personal_Financial_Distress, Total_Empathy, Total_Knowledge</p> <p>b. Dependent Variable: Total_Fraud_Awareness</p>										
<b>ANOVA<sup>a</sup></b>										
Model		Sum of Squares	df	Mean Square	F	Sig.				
1	Regression	10446.266	4	2611.566	294.215	<.001 <sup>b</sup>				
	Residual	3488.420	396	8.876						
	Total	13934.686	400							
<p>a. Dependent Variable: Total_Fraud_Awareness</p> <p>b. Predictors: (Constant), Total_Attitude, Total_Personal_Financial_Distress, Total_Empathy, Total_Knowledge</p>										
<b>Coefficients<sup>a</sup></b>										
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	5.695	1.192		4.778	<.001	3.352	8.039		
	Total_Personal_Financial_Distress	-.139	.048	-.089	-2.910	.004	-.233	-.045	.688	1.453
	Total_Empathy	.278	.052	.248	5.390	<.001	.176	.379	.301	3.318
	Total_Knowledge	.208	.052	.250	3.983	<.001	.105	.311	.162	6.186
	Total_Attitude	.337	.058	.361	5.806	<.001	.223	.451	.165	6.069
<p>a. Dependent Variable: Total_Fraud_Awareness</p>										