

ONLINE PAYMENT SCAM: WHAT HAVE CAUSED  
IT?

CHEANG XIN YI  
LIM JAS MIN  
NG KHA YONG  
THOR MIN HUI

BACHELOR OF ECONOMICS (HONS) FINANCIAL  
ECONOMICS

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE  
DEPARTMENT OF ECONOMICS

MAY 2023

CHEANG, LIM, NG, & THOR

ONLINE PAYMENT SCAM

BFE (HONS)

MAY 2023

ONLINE PAYMENT SCAM: WHAT HAVE CAUSED  
IT?

BY

CHEANG XIN YI  
LIM JAS MIN  
NG KHA YONG  
THOR MIN HUI

A FINAL YEAR PROJECT SUBMITTED IN PARTIAL  
FULFILLMENT OF THE  
REQUIREMENT FOR THE DEGREE OF

BACHELOR OF ECONOMICS (HONS) FINANCIAL  
ECONOMICS

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF BUSINESS AND FINANCE  
DEPARTMENT OF ECONOMICS

MAY 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 10330.

Name of Student:	Student ID:	Signature:
1. CHEANG XIN YI	19ABB02496	<i>Xinyi</i>
2. LIM JAS MIN	19ABB02016	<i>Jamin</i>
3. NG KHA YONG	18ABB06946	<i>Khayong</i>
4. THOR MIN HUI	19ABB02256	<i>Minhui</i>

Date: 2<sup>nd</sup> May 2023

## Table of Contents

CHAPTER 1: RESEARCH OVERVIEW .....	9
1.1 Research background.....	10
1.2 Problem statement.....	11
1.3 Research Objectives & Research Questions .....	13
1.3.1 Research Objective .....	13
1.3.2 Research Questions .....	13
1.4 Significance of the study.....	14
CHAPTER 2: LITERATURE REVIEW .....	17
2.1 Introduction.....	17
2.2 Review of Literature .....	17
2.2.1 Dependent Variable (Online Payment Scam) .....	17
2.2.2 Adoption of Online Payment in The Near Future.....	18
2.2.3 Security Issues .....	19
2.2.4 Perceived Ease Of Use.....	20
2.2.5 Trust .....	21
2.2.6 Government Intention .....	23
2.3 Review of Relevant Theoretical Models and Theory .....	24
2.3.1 Online Trust Model.....	24
2.3.2 Routine Activities Theory.....	26
2.3.3 Technology Acceptance Model (TAM).....	27
2.4 Proposed Conceptual Framework .....	29
2.5 Hypothesis Development.....	30
2.5.1 Adoption of Online Payment in the Near Future and Online Payment Scam .....	30
2.5.2 Security Issue and Online Payment Scam .....	31

2.5.3 Government Intention and Online Payment Scam.....	31
2.5.4 Perceived Ease of Use with Online Payment Scam.....	31
2.5.5 Trust and Online Payment Scam.....	31
2.6 Gap of Literature Review .....	32
CHAPTER 3: METHODOLOGY .....	33
3.1 Research Design .....	33
3.2 Sampling Design.....	34
3.2.1 Target Population.....	34
3.2.2 Frame and Location Sampling .....	34
3.2.3 Technique of Sampling.....	35
3.2.4 Size of Sampling.....	35
3.3 Data Collection Method.....	36
3.3.1 Questionnaire Design.....	37
3.3.2 Pilot Test .....	38
3.4 Data Analysis tools .....	38
3.4.1 Descriptive Analysis .....	38
3.4.2 Binary Logistic Regression.....	39
CHAPTER 4: DATA ANALYSIS AND FINDINGS .....	39
4.1 An Overview.....	40
4.2 Preliminary Data Analysis.....	40
4.2.1 Data Editing .....	40
4.2.2 Data Coding .....	41
4.2.3 Data Entry .....	44
4.3 Response Rate.....	44
4.4 Data Analysis.....	45

4.4.1 Descriptive analysis .....	45
4.4.2 Binary Logistic Regression.....	53
CHAPTER 5: DISCUSSION AND CONCLUSION .....	57
5.1 Introduction .....	57
5.2 Discussion of Major Findings.....	57
5.2.1 The Adoption of Online Payment in The Near Future And Online Payment Scams .....	57
5.2.2 Security Issues and Online Payment Scams .....	57
5.2.3 Perceived Ease of Use And Online Payment Scams .....	58
5.2.4 Trust and Online Payment Scams .....	59
5.2.5 Government Intention and Online Payment Scams .....	59
5.3 IMPLICATION OF STUDY .....	60
5.3.1 Practical Implication .....	60
5.3.2 Theoretical Implication.....	61
5.4 Recommendation for future study .....	62
References.....	63
Appendices.....	74



## LIST OF TABLES

	Page
Table 4.1 Coding for Demographic Profile .....	41
Table 4.2 Coding for the Dependent Variables .....	41
Table 4.3 Coding for the Independent Variables .....	41
Table 4.4 Overall Response Rate .....	45
Table 4.5 Statistics of respondent's experience towards online payment scam .....	46
Table 4.6 Statistics of respondent's gender .....	47
Table 4.7 descriptive statistics for Adoption of online payment in the near future .....	48
Table 4.8 descriptive statistics for security issue .....	48
Table 4.9 descriptive statistics of perceived ease of used .....	49
Table 4.10 descriptive statistic of trust .....	50
Table 4.11 descriptive statistics of government intention .....	51
Table 4.12 case processing summary .....	51
Table 4.13 case processing summary report .....	52
Table 4.14 crosstable of filter*gender .....	52
Table 4.15 Omnibus Tests of Model Coefficients .....	53
Table 4.16 Hosmer and Lemeshow Test .....	54
Table 4.17 Model Summary .....	54
Table 4.18 Classification Table .....	55
Table 4.19 Variables in the Equation .....	55

## LIST OF FIGURES

	Page
Figure 2.1: Research model in the study from Lee, & Turban. (2001).....	25
Figure 2.2: Research model in the study from Akgül, 2021 .....	27
Figure 2.3: Research model in the study from Mondego & Gide, n.d.....	28
Figure 2.4 Determinants of Online Payments Scam.....	29

## **LIST OF ABBREVIATIONS**

<b>BLR</b>	<b>Binary Logistic Regression (BLR)</b>
<b>CSM</b>	<b>Cyber Security Malaysia</b>
<b>FTC</b>	<b>Federal Trade Commission</b>
<b>RAT</b>	<b>Routine Activity Theory</b>
<b>SPSS</b>	<b>Statistical Package for Social Sciences</b>
<b>TAM</b>	<b>Technology Acceptance Model</b>

## LIST OF APPENDICES

	Page
Appendix 1 - Participant Information Page .....	74
Appendix 2 – Questionnaire Format.....	76
Appendix 3 – Filter Respondent .....	86
Appendix 4 - Table .....	87

# CHAPTER 1: RESEARCH OVERVIEW

## 1.1 Research background

Due to the popularization of the Internet, the i-Banking service launched by banks has gradually begun to be accepted and widely used. It also caused many criminals to use fake websites to carry out online payment scams through it.

Especially during covid-19, the phenomenon of online payment scam has become more and more common (Bandyopadhyay, 2020). Several countries have requested people to use cashless transaction as far as possible. Due to the increase of online transaction since 2020 Covid-19 pandemic lockdown, the online payment scam also increases with it but in a rapid way (Bandyopadhyay, 2020).

Similar proof from Interpol's (2020), "Cybercrime: Covid-19 impact," published in August 2020 stated that there is sharp increase of online payment scam as the Covid-19 sweeping the world.

Online payment scam can be detected by viewing and analysed a series of customer transaction data that was done in the past. Normally banks or other transaction authorities warn their customers about the transaction, if they notice any deviation from available patterns; the authorities consider it as a possibly scam transaction (Bandyopadhyay, 2020).

In addition, due to the development and popularization of network social media. As a platform for communication functions, social media has gradually become a part of people's daily life, and many businesses have also begun to use social media as a marketing platform to promote their commercial products and services (Anjum, 2020).

Social media is more direct than i-Banking. By eliminating the intermediate channel of the bank, consumers can directly communicate with sellers and form transactions through social media (Mokhsin, 2019). The powerful convenience has led to third-party exploitation. These criminals

will use fake identities to create fake accounts for business. These fake businesses are usually cheaper than goods of the same value, which helps them attract customers (Mokhsin, 2019).

There is a lot of information and data sharing is taking place virtually, and criminal activity via the internet is on the rise (Interpol's, 2020). Cybercrime happens almost every day unchecked (Interpol's, 2020). Online payment scams via web pages are generally not targeting personal property, but individuals are more vulnerable to them.

There are two main online payment methods, one is physical card, mainly used for physical store payment, payWave or PIN (Sakharova, 2012). The second is card no present, the card holder only needs to enter the card number and credit card or debit card information to make payment via email or SMS (Sakharova, 2012). Both methods of online payment are exploited by these criminals, who do not even need to have access to the victim's physical card to commit scam.

In addition, the sales company suffers losses beyond financial, including branding and customer loyalty (Anjum, 2020). Since many customers do not fully understand how online payment scams work, they tend to blame the seller and start doing less transactions with online sellers. After the reading, we know that the occur of online payment scam is because of the lack of security in technology and the effect of individuals' behaviours. It is a great opportunity for us to do study on factors that may affect the online payment scam.

## **1.2 Problem statement**

We are interested in conducting research on online payment scams because there is a lot of virtual information and data exchange happening and an increase in online criminal activities. Unchecked cybercrime occurs virtually daily. Web-based online payment scams often do not target private property, but people are more susceptible to them.

In March 2020, Europol alerted about new ways in which cybercriminals were benefiting from the pandemic and associated lockdown measures (Kemp, S, 2021), and in October 2020, Europol's

(2020a) Internet Organized Crime Threat Assessment stated that “COVID19 caused an amplification of existing [cybercrime] problems” (p. 6) and noted an increase in scam against businesses “as a result of the global outbreak of COVID-19” (Kemp, S, 2021).

Furthermore, Cyber Security Malaysia reported 4,117 cases, or 51.6% of online security incidents, involving scams, including online shopping scams, and this dominance is expected to continue. According to the report, 46% of respondents had experienced an online payment fraud, putting Malaysia ahead of other Southeast Asian nations such as Thailand, Xinjia, and India. According to the study, Malaysian residents' average cyber knowledge, experience, or abilities are inferior to those of other nations, and the Malaysian government is likewise more casual about cyber security (Yakimin, & Rusly, 2015).

According to reports, 13,703 fraud incidents totalling RM539 million in damages were reported in 2019. The following year, there were 17,227 incidents, resulting in a loss of RM511.2 million. Acryl Sani went on to say that between January 2019 and July 2022, 33,147 cybercrime suspects were captured, and 22,196 were charged. Online scams have grown increasingly common as a result of a number of variables, including increased expertise in technical exploitation and the use of online methods to contact victims with little understanding of cybercrime (Mohamed. Basyir, & Hana. Naz. Harun, 2022).

The victim's financial loss will be jeopardized by the online scams described above. Victims, especially those who rely on the government, such as the elderly, the sick, or other vulnerable groups, may have a traumatic experience. They are ideal, easy candidates for cyber fraud. The disadvantage, fragility, and unfairness they already feel will be made worse by online fraud. Fraud can also leave victims with severe mental and physical distress. Fraud may result in missed opportunities for both people and companies. The government worries about network security when it wants to offer financial assistance. The nation's economy will be impacted if these folks are not assisted. This is because the unemployment rate will increase if fraud results in people and companies losing out on opportunities. When that happens, not only will individuals lose faith in online transfers, but foreign investors will also lose faith in making investments in our nation, which will cause a recession here.

## **1.3 Research Objectives & Research Questions**

### **1.3.1 Research Objective**

Specific objective: To examine whether there is significant relationship between adoption of online payment in the near future, perceived ease of use, security issue, trust, government intention and online payment scam in Malaysia.

RO1: To examine whether there is significant relationship between adoption of online payment in the near future and online payment scam in Malaysia.

RO2: To examine whether there is significant relationship between security issue and online payment scam in Malaysia.

RO3: To examine whether there is significant relationship between government intention and online payment scam in Malaysia.

RO4: To examine whether there is significant relationship between perceived ease of use and online payment scam in Malaysia.

RO5: To examine whether there is significant relationship between trust and online payment scam in Malaysia.

### **1.3.2 Research Questions**



Specific research question: Is there a significant relationship between adoption of online payment in the near future, perceived ease of use, security issue, trust, government intention and online payment scam in Malaysia?

RQ1: Is there a significant relationship between adoption of online payment in the near future and online payment scam in Malaysia?

RQ2: Is there a significant relationship between security issue and online payment scam in Malaysia?

RQ3: Is there a significant relationship between government intention and online payment scam in Malaysia?

RQ4: Is there a significant relationship between perceived ease of use and online payment scam in Malaysia?

RQ5: Is there the significant relationship between trust and online payment scam in Malaysia?

## **1.4 Significance of the study**

The significance of our study is our study is important to online platforms, online sellers, consumers, and government. They will benefit from this study, as detailed below:

This study is important to Lazada, Shopee, and other online platforms because it highlights the need for strong security measures to protect users' payment transactions. This study can serve as a guide for these platforms to identify vulnerabilities in their payment systems and take steps

to improve their security measures, such as implementing firewalls or other protective measures. In addition to protecting their customers and merchants from scams, implementing stronger security measures can also help these platforms build trust with their users. Trust is essential for any online platform that handles financial transactions, and implementing effective security measures can help build that trust.

This study is important to online sellers because it can help them build confidence with their customers. Customers who feel confident in the security of their payment transactions are more likely to make purchases from a particular seller or platform. This study can help online sellers identify common payment scams and take steps to prevent them from happening. By implementing strong security measures, such as using trusted payment gateways, encryption, and two-factor authentication, online sellers can show their customers that they take payment security seriously. In addition, this study can help online sellers communicate their security measures to their customers. By providing clear and transparent information about the security measures they have in place, sellers can help build trust with their customers.

This study is important to consumers because it can help them increase their awareness of the different types of scams and how to protect themselves from becoming victims. This study can provide consumers with valuable knowledge about the common tactics used by scammers. By understanding how these scams work, consumers can be more vigilant when making online payments and avoid falling prey to fraud. In addition, this study can provide consumers with information about the security measures that they should look for when making online payments. This includes checking that the website is secure and using trusted payment gateways. Furthermore, the report can help consumers understand the importance of protecting their personal and financial information. This includes being cautious about sharing personal information online and using strong passwords and two-factor authentication.

This study is important to the government because it can help increase consumer trust in online payment systems by highlighting the risks associated with these transactions and recommending ways to protect against scams. By understanding the common tactics used by scammers to commit online payment scams, the government can identify potential gaps in existing regulations and policies and take steps to tighten them. This can help prevent online payment scams from occurring in the first place and increase consumer confidence in the safety and

security of online payments. In addition, this study can serve as a resource for government agencies responsible for enforcing consumer protection laws related to online payments. By incorporating the recommendations provided in the report into their enforcement activities, these agencies can help prevent fraudulent activities and increase consumer trust in online payments. Furthermore, this study can help the government develop public awareness campaigns to educate consumers about the risks associated with online payments and how to protect themselves. By providing clear and concise information, the government can help consumers make informed decisions when making online payments and reduce the likelihood of falling victim to scams.

## **CHAPTER 2: LITERATURE REVIEW**

### **2.1 Introduction**

In this chapter, we will discuss the independent variable and dependent variable of online payment scam. In this chapter, we will examine past research and articles, and examine five independent variables and a dependent variable. The details of each variable will be shown below.

### **2.2 Review of Literature**

In this era of increasingly developed network technology, online shopping and online transfers have become commonplace. This situation is more common in Malaysia, especially in Lazada and Shopee shopping platforms account for more than 70% of Malaysians' online shopping (Kiew et al., 2021). The popularity of online payment also means that online payment scams have also increased, and has also become a hot topic of discussion. To this end, this study will focus on studying the relationship between online payment scam and determinants, so that people can better understand the formation of online payment scam and reduce this phenomenon.

#### **2.2.1 Dependent Variable (Online Payment Scam)**

Criminals creating tailored scam emails to gain benefits through the victim's personal online account was known as an online payment scam (Chen, 2017). Online payment scams are a crime, but most of the time it has been largely excluded from the main measures of crime. The increase in online payment scam cases in recent years has brought more attention to this issue, but it is still a difficult task to accurately record and catch online payment scam criminals (Button, 2017).

Online payment fraud can cause victims monetary losses, and even mental damage in severe cases. Victims are often willing to hand over their money because of the deception of the fraud group. Criminal members usually use false advertisements or tricks to commit online payment fraud (Raj Singh, 2021).

Due to the development of Internet technology, online shopping has become common all over the world, including Malaysia. Although online transactions bring people a lot of convenience, such transactions without face-to-face also increase the risks of participants (Kiew et al., 2021).

This variable is mainly used to identify victims of online payment scams and victims of similar experiences.

### **2.2.2 Adoption of Online Payment in The Near Future**

There is a significant relationship between the adoption of online payment in the near future and online payment scams. Several studies have examined this relationship and have produced important findings.

For instance, a study found that the adoption of online payment systems was positively correlated with the occurrence of online payment scams in China (Zhu, Sun, and Yan, 2020). The authors argued that the convenience and ease of use of online payment systems make them a prime target for scammers. Similarly, one study found that there is a positive relationship between the adoption of online payment methods and online payment scams. As more people adopt online payment methods, scammers are more likely to target online

payment systems, resulting in an increase in scams (Liu, Lu, & Wang, 2021). This is because scammers see online payment systems as a lucrative target due to the large volume of transactions and the ease with which payments can be made. Furthermore, the relationship between the adoption of online payment systems and the occurrence of payment scams in China (Wang, Xue, and Liang, 2020). The authors found that the adoption of online payment systems was positively correlated with an increase in scams, suggesting that the use of these systems is vulnerable to fraudulent activities.

Moreover, there is also study that supported there is negative relationship between the adoption of online payment in the near future and online payment scams. A study has mentioned there is a negative correlation between the adoption of online payment and online payment scams (Better Business Bureau, 2020). The study found that as more consumers adopt online payment methods, there is a decrease in the number of reported payment scams. Similarly, according to a report by the Federal Trade Commission (FTC, 2021), there is a negative correlation between the adoption of online payment and online payment scams. The report found that as more consumers shift to using online payment methods, the rate of reported payment scams has decreased. This trend can be attributed to improvements in security measures, such as two-factor authentication and fraud monitoring, as well as increased awareness and education about online payment fraud.

### **2.2.3 Security Issues**

There is a significant relationship between security issues and online payment scams. Security issues, such as weak passwords, unsecured networks, and unsecured payment systems, can create opportunities for scammers to steal payment information and defraud consumers (Bryant & Reffett, 2019; Yan, Peng, & Li, 2020).

Online payment systems have become increasingly popular in recent years, offering convenience and ease of use to consumers and businesses alike. However, with the increased use of online payment systems, there has also been a rise in online payment scams. One

study found that there is a positive relationship between security issues and online payment scams, indicating that online payment scams are more likely to occur when there are security vulnerabilities present (Abdul Wahab, Norhayati, & Hamid, 2017). Furthermore, one study that supports the significant relationship between security issues and online payment scams is a research conducted by Tsalis, Papadopoulos, and Karyda (2020). The study aimed to explore the factors that influence consumers' adoption of online payment methods and their perception of the security of such methods. The study found that security issues were a major concern for consumers when it comes to online payment, and that consumers who had experienced security issues were more likely to fall victim to online payment scams. Similarly, Yan et al. (2020) found that security issues, such as unsecured networks and weak passwords, were significant factors in online payment scams in China. The study found that scammers used phishing techniques and malware to steal payment information from unsuspecting consumers.

Moreover, there is also study that supported there is negative relationship between security issues and online payment scams. According to a study by Alomari, Alshurideh, & Tarhini (2020), there is a negative correlation between security issues and online payment scams. The study found that security measures such as two-factor authentication, encryption, and fraud detection technologies significantly reduce the risk of online payment scams. Similarly, according to a study by Lin, Chen, & Chen (2017), there is a negative correlation between security issues and online payment scams. The study found that security measures such as encryption, authentication, and fraud detection technologies play an important role in reducing the risk of online payment scams. Specifically, the study found that the adoption of security measures significantly decreases the likelihood of users falling victim to online payment scams.

#### **2.2.4 Perceived Ease Of Use**

There is a significant relationship between perceived ease of use and online payment scams. Several studies have examined this relationship and have produced important findings.

One study conducted by Alshammari, Aldakhil, and Alzahrani (2021) found a significant relationship between perceived ease of use and susceptibility to online payment scams. The study surveyed 325 participants and used a structural equation modeling approach to analyze the data. The results indicated that perceived ease of use had a positive relationship with susceptibility to online payment scams. This finding suggests that individuals who perceive online payment systems as easy to use may be more vulnerable to scams that exploit their trust in these systems. Therefore, it is important for online payment providers to implement measures to improve security and protect users from fraudulent activities. Similarly, Owusu, Boateng, and Ofori-Boateng (2019) conducted a survey of 392 online shoppers in Ghana to gather data on their perceived ease of use of online payment systems and their experiences with online payment scams. The results showed that the majority of respondents perceived online payment systems to be easy to use, but a significant number also reported falling victim to online payment scams.

Moreover, there is also study that supported there is negative relationship between perceived ease of use and online payment scams. One study that supports the relationship between perceived ease of use and online payment scams is the research conducted by Owusu, Boateng, and Ofori-Boateng (2019). In their study, they found that there was a significant negative relationship between perceived ease of use and online payment scams, meaning that as perceived ease of use increases, the likelihood of falling victim to online payment scams decreases. Further analysis revealed that perceived ease of use was negatively associated with online payment scams, suggesting that the easier an online payment system is perceived to be, the less likely individuals are to fall for online payment scams.

### **2.2.5 Trust**

There is a significant relationship between trust and online payment scams. Several studies have examined this relationship and have produced important findings.



Online payment systems have become increasingly popular, providing consumers with a convenient and efficient way to make transactions. However, the rise of online payment scams has led to concerns about the security of these systems. One factor that has been linked to the occurrence of online payment scams is the level of trust that consumers have in online payment systems. Research has shown that there is a positive relationship between trust and online payment scams, suggesting that when consumers trust online payment systems, they may be more vulnerable to scams (Kim et al., 2019). There is another research suggests that there is a positive relationship between trust and online payment scams. When consumers trust online payment systems, they may be more vulnerable to scams (Holtfreter, Reisig, & Pratt, 2019). The relationship between trust and online payment scams can be explained by the concept of overconfidence. When consumers trust online payment systems, they may be more likely to engage in risky behaviors, such as clicking on suspicious links or providing personal information to unknown parties. This overconfidence can make consumers more vulnerable to scams and other forms of online fraud. Additionally, trust can also be exploited by scammers who create fake websites or email messages that mimic the look and feel of legitimate online payment systems. These scams can be difficult for consumers to detect, as they may appear to be genuine.

Moreover, there is also study that supported there is negative relationship between trust and online payment scams. A study conducted by Wu and Chen (2018) found that trust was significantly related to susceptibility to online payment scams. The study surveyed 389 participants in Taiwan and used a structural equation modeling approach to analyze the data. The results showed that trust had a negative relationship with susceptibility to scams, indicating that higher levels of trust were associated with lower susceptibility to scams. Additionally, a study by Jia and Wang (2020) found that trust was a significant predictor of online payment scams in China. The study found that individuals who had higher levels of trust in online payment systems were less likely to experience scams. On the other hand, individuals who had lower levels of trust were more likely to fall victim to scams. Similarly, a study by Phan, Limbu, and Shah (2020) found that trust was a significant predictor of online payment scams in Malaysia. The study found that individuals who had higher levels of trust in online payment systems were less likely to experience scams. These findings suggest that trust plays an important role in the incidence of online payment scams.

Consumers who trust online payment systems are more likely to use them, but may also be more cautious and aware of potential scams. On the other hand, consumers who have low levels of trust may be more vulnerable to scams.

## **2.2.6 Government Intention**

There is a significant relationship between government intention and online payment scams. Several studies have suggested that government intention and actions can have a significant impact on the occurrence of online payment scams.

There is no study and evidence to support that there is positive relationship between government intention and online payment scams. Governments typically work to prevent scams and protect their citizens from online scams. However, there may be instances where government actions, such as policy changes or inadequate enforcement of regulations, could contribute to an increase in online payment scams. As an example, one article that discusses this issue is "The Impact of E-Commerce Policy on Online Payment Fraud: Evidence from China" by Yan Zhang and colleagues (2020). The study examines the impact of a policy change in China that allowed third-party payment platforms to operate without a banking license. The authors find that this policy change led to an increase in online payment scams, as the new players in the market were not subject to the same regulatory requirements as traditional financial institutions.

Moreover, there are studies that supported there is negative relationship between government intention and online payment scams. For instance, a study by Lin, Tan, and Yang (2020) found that the implementation of regulations and policies by the Chinese government significantly reduced the number of online payment scams in China. The study found that the government's intervention increased consumer trust in online payment platforms, which led to increased usage and reduced scams. Another study by Liu, Huang, and Hu (2020) analyzed the impact of government policies on online payment scams in Taiwan. The study found that government intervention had a significant impact on reducing

online payment scams. The researchers suggested that the government's strict enforcement of regulations and penalties for online payment scams played a role in reducing their occurrence. Additionally, one study that found a significant relationship between government intention and online payment scams is the research by Lee and Song (2020). The study explored the relationship between government policies and online payment scams in South Korea using data from a survey of 1,500 participants. The findings of the study showed that there was a significant negative relationship between government intention and online payment scams. Specifically, when the government was perceived to have a higher intention to prevent online payment scams, the participants reported a lower incidence of online payment scams. Overall, the study suggests that government policies and interventions can play an important role in reducing the prevalence of online payment scams. Additionally, a study by Feng, Zhang, and Zhang (2020) found that the Chinese government's efforts to regulate online payment platforms reduced the occurrence of payment scams. Similarly, a study by Oladejo, Rahman, and Adesina (2021) found that the Nigerian government's introduction of the Cybercrime Act 2015 had a positive effect on reducing online payment scams in the country.

## **2.3 Review of Relevant Theoretical Models and Theory**

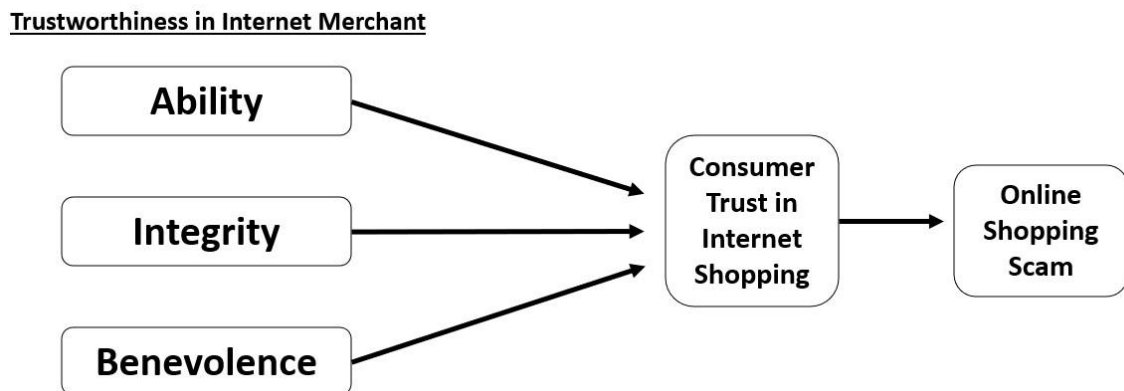
### **2.3.1 Online Trust Model**

Online purchasing saves time and effort over conventional purchasing (Chang, n.d.). Consumers merely need to pay and transfer funds to acquire the things they desire. Traditional shopping requires consumers to spend time, energy, and money traveling to the

location and then selecting and comparing items of various categories. Consumers cannot assess whether what the merchants say is accurate or not, they cannot forecast the quality of things, and they have no control over whether the personal and financial information they gave is secure.

Trust is a crucial component of online purchasing that might influence a customer's decision to buy or not. They discovered that trust is significantly connected with aptitude, morality, and goodness (Lee & Turban, 2001). The capacity to influence whether or not buyers are willing to make a purchase was demonstrated in the internet shopping case. Integrity was viewed as the seller's commitment to being truthful and abiding by the rules. If the vendor didn't comply, the consumer would be the victim of an online purchasing fraud. When a customer shops online, they are acting benevolently if they think the merchant is benefiting others rather than just themselves. These three elements taken together can sometimes be referred to as "reputation". When a company has high reputation, buyer will have high willingness to buy from them. Consumer will trust on the company when they fulfill these 3 components to have a high reputation.

Research model in the study from Lee, & Turban. (2001):



*Figure 2.1: Research model in the study from Lee, & Turban. (2001)*

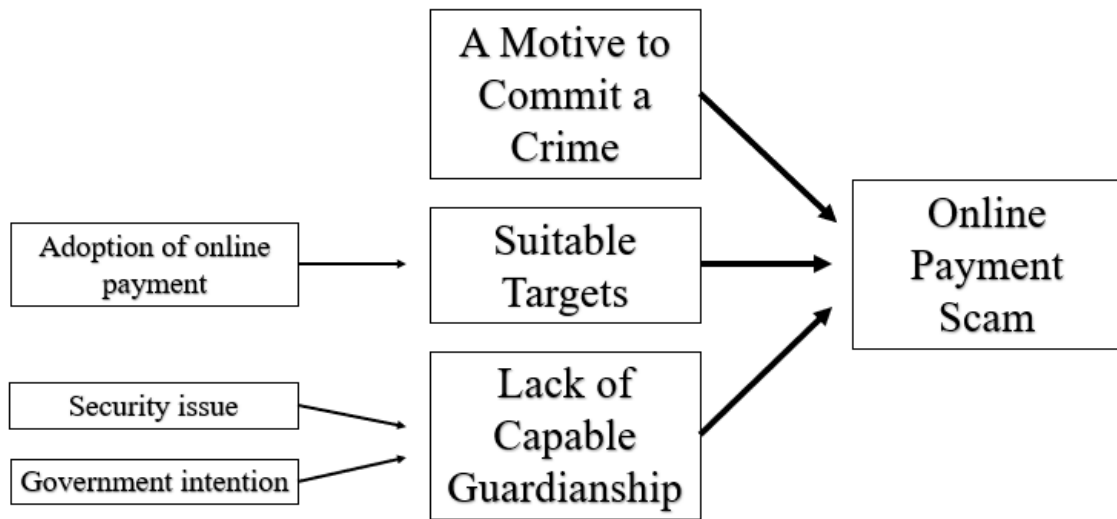
In short, this study was selected as a reference theoretical model because it investigates the factors that influence consumer trust in online shopping, which will easily lead to our dependent variable, online payment scams. Consumer trust in internet shopping can be affected by ability, integrity, and benevolence. The combination of these three elements is

also called reputation. If one of the elements did not fulfil, it will easily cause online payment scams occur. For instance, if the integrity, which is the sellers fail to follow the rules like did not send the parcel to the buyer after payment has made, the online payment scam will occur.

### **2.3.2 Routine Activities Theory**

Routine Activities Theory states that when criminals choose to commit a crime, they will first consider suitable targets and whether they have a backer (Akgül, 2021). The backer can be physical or it can be non-physical like the rules and regulations set by government. Inside the research, there are 3 elements should be fulfilled before a criminals commit a crime. First, the perpetrator needs a motive to commit a crime. Second, the offender must find the right target. Finally, the party needs to be a guardian who lacks criminal capacity.

The motivation of the offender is not necessarily the psychological motive that he had before committing a crime. An ordinary person can also commit a crime under the guidance of others. Besides, suitable targets can be both humans and non-humans. The offender's search for a suitable target will depend on timing and intent at the period. Non-human targets can be objects that are valuables, like a gold necklace (Akgül, 2021), while the human target for online shopping scam purpose can be people who like to make online purchase or people who active use mobile phones to record personal or financial information. Crime can be prevented or reduced under the protection of capable guardians. The capable guardian can be formal or informal (Routine Activity Theory (RAT) | North Miakmi Beach, FL, n.d.).



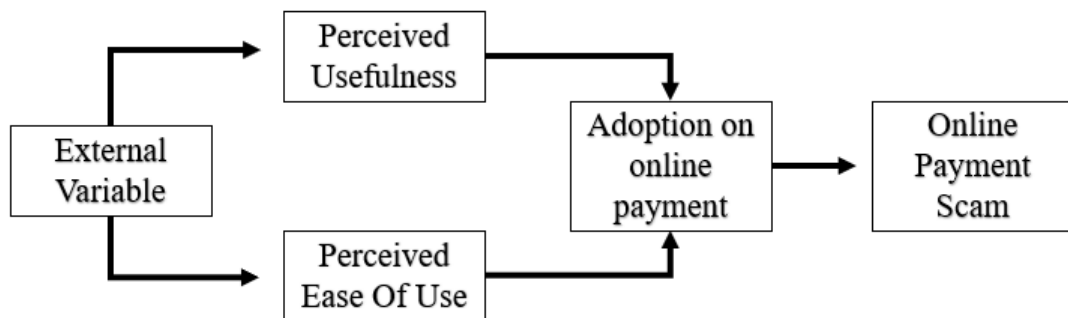
*Figure 2.2: Research model in the study from Akgül, 2021*

In short, this study was selected as a reference theoretical model because it investigates the factors let criminals choose to commit a crime, which can be related to our dependent variables, online payment scam which also is a crime. Just has stated above, 3 elements must fulfil before commit a crime. When committing online payment scam, the scammer will get a motivation which is to trick people to believe that they are trusted. After that, they will try to find suitable targets which is those people who often use online payment to purchase items or those people who have savings account. The last step before committing online payment scam, they will ensure the victim is lack of capable guardianship like unsecured networks and weak passwords, or when there is legal gap.

### **2.3.3 Technology Acceptance Model (TAM)**

Technology Acceptance Model (TAM) tries to assist academics and practitioners in identifying the reasons why a specific technology or system might be acceptable or unsuitable and implements appropriate measures by justification in addition to offering prediction (Rigopoulos & Askounis, n.d.). Davis (1989) asserts that even though the

external stimulus has an influence on the behavior of the desire to use a new technology, the "TAM is founded upon two key constructs: perceived usefulness and perceived ease of use lie within the cognitive response region of human psychology." The term perceived usefulness (PU) refers to a person's perception of how much utilizing a given technology will improve their ability to execute their job (Mondego & Gide, n.d.). A person's degree of assurance that using technology would result in fewer unnecessary efforts is known as perceived ease of use (PEOU) (Indarsin & Ali, 2017). People will continue to utilize technology if it is simple to use, clear and comprehensible, easy to operate, versatile, and easy to get skilled with (Indarsin & Ali, 2017).



*Figure 2.3: Research model in the study from Mondego & Gide, n.d.*

In short, this study was selected as a reference theoretical model because it investigates the factors that influence adoption on online payment, which will easily lead to our dependent variable, online payment scams. Adoption on online payment can be affected by the ease of use of a technology. While the ease of use can be affect by other external variable like security, income, trust, and others.

## 2.4 Proposed Conceptual Framework

Proposed Model:  $PS_t = \beta_0 + \beta_1 AO_t + \beta_2 SI_t + \beta_3 PU_t + \beta_4 T_t + \beta_5 GI_t$

Where,

$PS_t$  = Online Payment Scam

$AO_t$  = Adoption of Online Payment in the Near Future

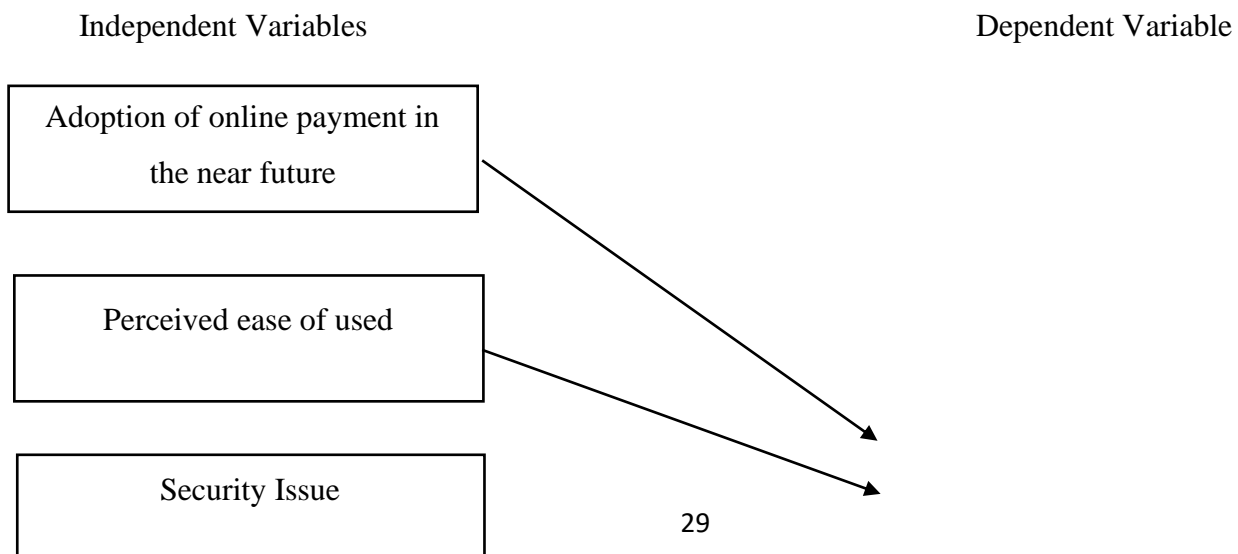
$SI_t$  = Security Issue

$PU_t$  = Perceived Ease of Use

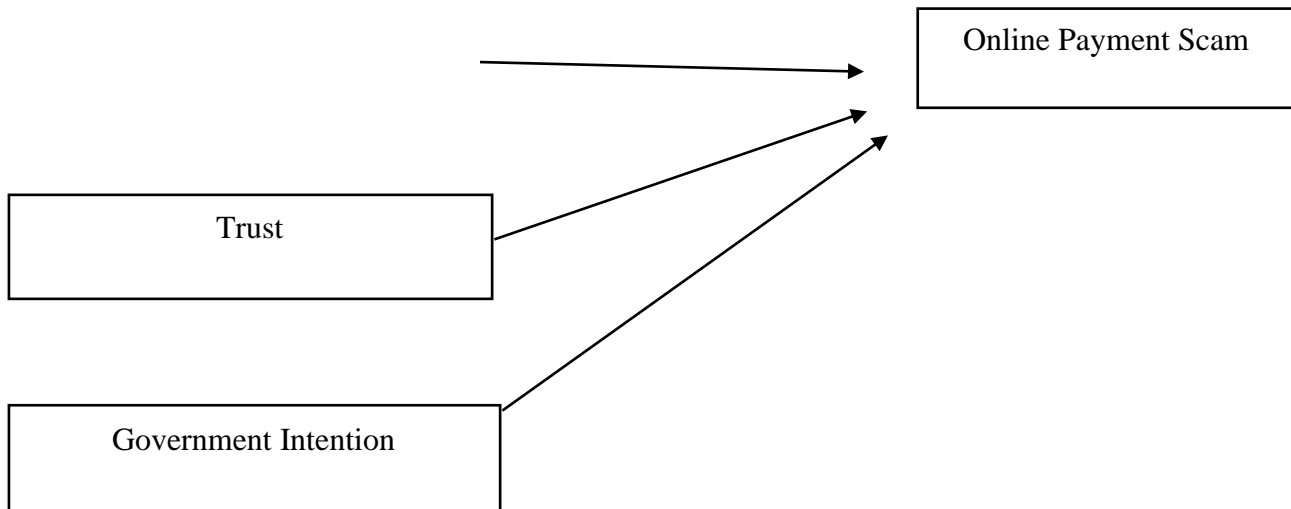
$T_t$  = Trust

$GI_t$  = Government Intention

*Figure 2.4 Determinants of Online Payments Scam*







To study the determinants of online payment scam, a conceptual framework is developed in figure 2.3 by referring to the theoretical models that have been explain and review. The determinants of online payment scam that referring to the independent variable in this research had been illustrated in the figure above which are adoption of online payment in the near future, security issue, perceived ease of use, trust and government intention. It is predicted that the online payment scam will be influenced by these independent variables based on prior studies. Hence, this framework will then be utilized to check the accuracy of the assumption. As a result, this framework will be used to develop the hypotheses in the following section.

## 2.5 Hypothesis Development

### 2.5.1 Adoption of Online Payment in the Near Future and Online Payment Scam

$H_0: \beta_1 = 0$  (There is no relationship between Adoption of Online Payment in the Near Future and online payment scam)

$H_0: \beta_1 \neq 0$  (There is relationship between Adoption of Online Payment in the Near Future and online payment scam)

### **2.5.2 Security Issue and Online Payment Scam**

$H_0: \beta_2 = 0$  (There is no relationship between Security Issue and Online Payment Scam)

$H_0: \beta_2 \neq 0$  (There is relationship between Security Issue and Online Payment Scam)

### **2.5.3 Government Intention and Online Payment Scam**

$H_0: \beta_3 = 0$  (There is no relationship between Government Intention and Online Payment Scam)

$H_0: \beta_3 \neq 0$  (There is relationship between Government Intention and Online Payment Scam)

### **2.5.4 Perceived Ease of Use with Online Payment Scam**

$H_0: \beta_4 = 0$  (There is no relationship between Perceived Ease of Use and online payment scam)

$H_0: \beta_4 \neq 0$  (There is relationship between Perceived Ease of Use and online payment scam)

### **2.5.5 Trust and Online Payment Scam**

$H_0: \beta_5 = 0$  (There is no relationship between Trust and Online Payment Scam)

$H_0: \beta_5 \neq 0$  (There is relationship between Trust and Online Payment Scam)

## **2.6 Gap of Literature Review**

With the rise on online payment scam, it has become a popular topic of massed research. However, types of online scam and how to prevent online scam are always the focus of the majority of research on the research paper while the determinants of online payment scam were still had not sufficient and details research and study especially in Malaysia. Most of the research papers are explaining and defining what is online payment fraud or E-commerce scam and what is the way to prevent or what are the precaution step to avoid it but the information about the main determinant of online payment scam and what causes online payment scam are limited. Hence, our study focuses on the factors or determinants that will affect or lead to online payment scam in Malaysia. With the reference of past studies, we study the determinants of online payment scam in Malaysia from the victims and fraudster perspective.

## **CHAPTER 3: METHODOLOGY**

### **3.1 Research Design**

Research design is the planning or assumption made by the researcher for the specific steps and processes of future research work in order to explore the answer or explanation of the research question (Akhtar, 2016). It includes a series of contents such as clarifying the research purpose, setting the sampling method, determining the analysis unit, selecting the research method and means, and selecting the time frame. It also requires the development of detailed and specific operational steps for the above.

In this study, we will determine the factors of online payment scams. Therefore, the descriptive research design is more appropriate for this study. Descriptive research is a common project research, which refers to the investigation and research of different factors and different aspects of the current situation (Dudovskiy). The collection and recording of data focus on the static description of objective facts.

Besides, quantitative research method will be used in this study by using online questionnaires as data collection tools. Quantitative research is to use observation, experiment, survey, statistics and other methods to study phenomena, and put forward strict requirements on the rigor, objectivity and value neutrality of the research, in order to obtain objective facts. Quantitative research usually takes the form of data to illustrate social phenomena, predict theories through deductive methods, and then collect data and evidence to evaluate or validate models, hypotheses, or theories that were envisioned before the study (Apuke, 2017).

## **3.2 Sampling Design**

Sampling design is an integral part of research. Since sample collection can be financially and time-intensive, sample collection must be precise to save cost and time. To define the characteristics of highly variable populations, more samples are required than for fewer variable populations. In this study, sampling design includes target population, frame and location sampling, technique of sampling, and size of sampling (Wills et al., 2020).

### **3.2.1 Target Population**

The target population is the group of people on whom the initiative will perform research and develop findings (Lavrakas, 2008). The subject of the study were the UTAR's students,

### **3.2.2 Frame and Location Sampling**

Sample frame is the collection of resources from which the sample is chosen (Turner, 2003). In this study, only UTAR students is included. In additional, this study only includes UTAR students who already above 18 years old, because according to Malaysia's law, the Guardianship of Infants Act 1961, the assets of minors, that is, Malaysian citizens under the age of 18, are to be managed and handled by a guardian. Since this study only targeted UTAR students who were able to allocate their finances freely, our sample collection was restricted to UTAR students aged 18 and above. Sample location refers to the location where a geographical sample was collected (Turner, 2003).

### 3.2.3 Technique of Sampling

Technique of sampling can be classified into two categories, which are probability sampling and non-probability sampling (Albaity & Rahman, 2019). Probability sampling is defined as every respondent has an equal chance to be selected in the sample. Non-probability refers to every respondent in the population not having an equal probability of being chosen. The technique of sampling used in this research is non-probability sampling. In addition, non-probability sampling methods can be separated as convenience sampling, purposive sampling, snowball sampling and quota sampling. By refer to similar report, Expectations vs reality: Responding to online scam across the scam justice network (Cross, C. 2018) to fulfil requirement of target population, convenience sampling will be adopted in this study. Convenience sampling is a technique that often selects participants that are available around a location, internet site, or customer-membership list (Stratton, S. J., 2021).

### 3.2.4 Size of Sampling

Sample size is the total number of survey respondents, these respondents will all come from UTAR and collected through online google form. In addition, the size of the sample size is also one of the important considerations. To this end, this study will use Cochran formula to ensure sufficient sample.

$$Sample\ size = \frac{\frac{Z^2 * P(1 - P)}{e^2}}{1 + \left(\frac{Z^2 * P(1 - P)}{e^2 N}\right)}$$

Where:

N= Population size

Z= Z-score

E= margin of error

P= standard of deviation

Based on the formula above, the confidence level is 95% and margin error will be 5%. According to utar.edu, the population of University Tunku Abdul Rahman (UTAR) is 21,000 students as total population. By substitute information into the formula,

$$\begin{aligned} \text{Sample size} &= \frac{\frac{1.96^2 * 0.5(1 - 0.5)}{0.05^2}}{1 + \left(\frac{1.96^2 * 0.5(1 - 0.5)}{0.05^2 * 21,000}\right)} \\ &= 377.2587 \\ &\approx 378 \end{aligned}$$

The result shows the sample size is 377.2587 people. To collect authentic data, the sample size is rounded up to 378 respondents.

### **3.3 Data Collection Method**

Data collection method to measure the variable's interest by gathering the information which can answer the research questions, test the hypothesis, and evaluate results (Syed, 2016). There are two types of data collection methods that can be used while doing research, which are primary data and secondary data.

Primary data is the data that has not been presented and modified, and it is more reliable, accurate, and objective (Syed,2016). Primary data can also be known as the first hand-experience. Primary data can be gathered by using experiments, surveys, questionnaires, interviews, and observations.

In this study, we are using the primary data collection method, and we will collect the data using the questionnaire method. The reason that we use a questionnaire to conduct the study is because a questionnaire can gather a huge amount of data in a short period (Geisinger, 2010). Other than quick collection, the online questionnaire is also cost-effective since we use Google form to conduct the questionnaire is free.

### **3.3.1 Questionnaire Design**

When designing the questionnaire, the first step is to make preliminary decisions by preparing the information required and defining the target population that is needed in the study. The second step is to choose the method to reach out the targeted population by personal interviews, online interviews, mailed interviews, or telephone interviews. The third steps to conduct a good questionnaire is to decide on question content that is able to match the research objectives, as specific as possible. The forth step is determining the response format. It can be closed, open-ended, and open response-option questions. The questionnaire questions should be as short as possible and clearly to be understood easily. The last step is making a pilot test to avoid mistakes.

We can organize our questionnaire into six parts, which included, part 1 introduction. Give an introduce to the research that you are studying and the objectives. Part 2 is to filter the respondent. Not everyone is qualified for the research. Here we prepared a short question is asking whether the participant has the experience on online payment scam or not. The respondent can choose YES to continue answer the following questions or choose NO to quit the questionnaire. Part 3 is some warm-up questions. It can be asking about the demographic profile which includes the respondent's gender, age, income, occupation, education, or work experience. Part 4 is get into detailed questions. This part will be asking more detail question and normally will use a rating scale. For example please rate 1 to 5



on how you satisfy with the online purchase experience. Part 5 is to collect data to filter out unqualified respondents like the data on usage behavior. The last part is to notice that the survey has finished conducted and thank you for their participation.

### **3.3.2 Pilot Test**

A pilot test is used to test a study by conducting small-scale preliminary research. A pilot test is needed because it can help you to determine whether the research is feasible or not and whether the research has the opportunity to publish or not. If the research is published successfully, it can help more researchers in conducting their studies by using your research.

The pilot test can let the researcher notice the issues that will negatively affect the research. Which mean it can reduce mistake in the study. To prepare a pilot test, we should prepare a small-scale sample size within 12 to 50 respondents. The respondents can be different age, gender, backgrounds while it must fulfill your target population. After that, give the questionnaire to the small-scale respondents. After that observe how those respondents complete the survey and make changes if there are mistakes found.

## **3.4 Data Analysis tools**

### **3.4.1 Descriptive Analysis**

Descriptive analysis is commonly referred to descriptive statistic, it is an approach of applying statistical tools to define and summarize a data set (Bush, 2020). This analysis is

not trying to forecast about future but utilize the historical information that has been manipulated to make sense and understanding in order to draw conclusions. The descriptive analysis is famous because it provides simpler to ingest data which make it simpler for analysts to act on it and it can be perform by using Statistical Package for Social Sciences (SPSS). Descriptive analysis can be categories as 4 types which are measures of central tendency, frequency, dispersion or variation, and position. Measure of frequency is to understand of how common or frequent a specific action or activity happens; measure of central tendency is to get the average reaction and there are three indicators which are mean, median, and mode; measure of dispersion is to interpret the distribution of data through a range; measure of position is to determine the stance or role of one case or action compare to others and percentiles and quartiles can be used to measure the position.

### **3.4.2 Binary Logistic Regression**

Binary Logistic regression is employed to examine the relationship between a binary dependent variable that can only take 2 values and one or more independent variable (H2o.ai., 2023). Hence, this model can utilise in this study because the dependent variable of this study has only 2 values which is 0 and 1 and this study consists of 5 independent variables which are adoption of online payment in the near future, trust, government intention, perceived ease of used, and security issues. Predictive analytics and categorization frequently make use of this kind of statistical model to evaluate the cause-effect relationship of one or more predictor factors on the results (ResearchWithFawad, 2021). The objective of logistic regression is to calculate the possibility that the dependent variable will fall into a specific group.

## **CHAPTER 4: DATA ANALYSIS AND FINDINGS**

## **4.1 An Overview**

We have conducted questionnaire by using Google form to gather evidence to support the hypothesis that mentioned in previous chapter 2, hypothesis development. Five to ten minutes were needed for respondents to complete the questionnaire, and all findings were purposefully discussed using SPSS' statistical methodology. In this chapter, we will discuss the details about our results that distributed in questionnaire to support the objectives that were outlined in Chapter 1. The three data analysis methods that mentioned in Chapter were used to analyse data. There is total 386 respondents in the final sample, which has been evaluated, indicate the factors affecting online payment scams by Utarians.

## **4.2 Preliminary Data Analysis**

### **4.2.1 Data Editing**

Data editing is defined as a process of reviewing and improving the collected data to ensure consistency, sufficiency, identifying errors and outliers, and correcting errors within the data to maximize for utility for the purpose for which it was collected (Naeem, 2019). We have gone through the library and canteen in UTAR to collect the data by providing the Google form's QR code. After received enough respondents via the Google form, the data processing process begins with the data editing phase. After that, the data is entered into Excel Spreadsheet and checked for any omissions, ambiguities, and errors after it has been converted to a spreadsheet. Those responses which are incomplete will be deleted to ensure error-free. It will be easier to transfer and analyse using the SPSS software.

## 4.2.2 Data Coding

Data coding refers to the process of converting the data that gathered or observed into a collection of pertinent, coherent categories (Sun, 2018). It is the process of condensing and presenting facts in order to provide a coherent interpretation of events that have been recorded or seen. In this research first, the data were coded by the demographic variable with gender. Then, questions under the dependent variables were coded with number according to the 1=Yes and 0=No. Besides, independent variables were coded with numbers according to the Likert scale, (1=Strongly Disagree), (2=Disagree), (3=Neutral), (4=Agree), and (5=Strongly Agree).

*Table 4.1 Coding for Demographic Profile*

Demographic	Variables	Coding
Gender	Male	0
	Female	1

*Table 4.2 Coding for the Dependent Variables*

Questions	Coding	Source
DV1: Dependent Variable: Experience towards Online Payment Scam		
Did you or your families and friends been experienced scam before while using online payment?	0 = No 1 = Yes	Faisal Alanezi (2015).

*Table 4.3 Coding for the Independent Variables*

Questions	Coding	Sources
IV 1: Independent Variable: Adoption of online payment in the near future		
<p>Do you think online payment brings more convenience to you when compared to traditional payment method?</p> <p>I spent more than 50% of my income per month in online payment.</p> <p>The reason that I choose to adopt online payment because it helps to make expenditure record.</p> <p>The reason that I choose to adopt online payment because it help me save time and effort.</p> <p>I normally use online payment for shopping purpose.</p> <p>I normally use online payment for pay bills purpose.</p> <p>I start using online payment before pandemic.</p> <p>I start using online payment after pandemic.</p>	<p>1 = Strongly Disagree</p> <p>2 = Disagree</p> <p>3 = Neutral</p> <p>4 = Agree</p> <p>5 = Strongly Agree</p>	<p>Faisal Alanezi (2015).</p> <p>Shree, Pratap, Saroy, &amp; Dhal (2021).</p>
Question		
IV 2: Independent Variable: Security Issues		
<p>I worry about the secondary use of the information that I provided when making online payment.</p> <p>It is risky to get scam when using online payment.</p> <p>Making transaction or make payment through online for goods and services is secure.</p> <p>I will reject to use online payment when the third party ask me to provide financial</p>	<p>1 = Strongly Disagree</p> <p>2 = Disagree</p> <p>3 = Neutral</p> <p>4 = Agree</p> <p>5 = Strongly Agree</p>	<p>Jain &amp; Raman (2022)</p> <p>Shree, Pratap, Saroy, &amp; Dhal (2021).</p>

<p>information (account number or bank account password).</p> <p>Dual digital authentications is necessary when using online transfer.</p> <p>I am willing to bind my credit card with the e-payment.</p> <p>Scam detection application is useful in avoid online payment scam.</p> <p>When making online shopping I always worry about the sellers fail to send out the products.</p>		
Question		
IV 3: Independent Variable: Perceived Ease of use		
<p>Online payment is feasible to access.</p> <p>Online payment provides various payment channels to enable me to make payment easily.</p> <p>I feel online payment is easy to use.</p> <p>Online payment provide fast services.</p>	<p>1 = Strongly Disagree</p> <p>2 = Disagree</p> <p>3 = Neutral</p> <p>4 = Agree</p> <p>5 = Strongly Agree</p>	
Question		
IV 4: Independent Variable: Trust		
<p>I trust the online payment system will provide good services than traditional payment method.</p> <p>I trust the service department can provide good solution when online payment has technical issue occur.</p> <p>I trust online payment system will keep our personal or financial information safe.</p> <p>I trust online payment is safe when transferring big sum of funds.</p>	<p>1 = Strongly Disagree</p> <p>2 = Disagree</p> <p>3 = Neutral</p> <p>4 = Agree</p> <p>5 = Strongly Agree</p>	<p>Shree, Pratap, Saroy, &amp; Dhal (2021).</p> <p>Shahzad (2015).</p>

I trust online payment is safe for every online transaction.		
Question		
IV 4: Independent Variable: Government Intention		
I think government should strengthen the policies to fight with online payment scam. Government should promote online payment services. The attitude of government will affect the adoption of online payment. Government should strengthen the facilities of online payment.	1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree	Faisal Alanezi (2015).

### 4.2.3 Data Entry

After done the process of checking, editing, and coding, the data will be analyse by covert into the SPSS software. As a result, 386 completed questionnaires were obtained for this study, and there were no unanswered questions among them. Hence, none of the 386 responses were disregarded, and they were all entered the SPSS software. The Questionnaire was sent in Google form to the respondent through WhatsApp, and by hand. The data take 1 weeks to gather the respondents' responses for this study, then another week to edit, code, and enter the SPSS program.

### 4.3 Response Rate

Response Rate is calculated by dividing the total number of eligible respondents in the sample by the number of use-able responses received (Fincham, 2008). The ratio of returned questionnaires to the entire sample that received the survey initially should be used to compute the survey response rate. Online payment is considered effective and efficient, while they need high respondent rate in judging the quality of the survey (Response Rates of Online Surveys in Published Research: A Meta-analysis, 2022). In order to increase response rates and make their study more credible and publishable, researchers should invest more time and effort in assessing the research topic, objectives, question, and target population (Fincham, 2008). In this study, the Questionnaire were distributed by online platform via WhatsApp, and by hand.

The following table 4.3 provides an illustration of the overall response rate obtained:

*Table 4.4 Overall Response Rate*

Questionnaire (Google-form)	No. of Questionnaire (Google-form)	Percentage(%)
Distributed	386	100
Returned (Valid)	386	100
Returned (Invalid)	0	0
Not return	0	0

Based on the Table 4.4 above, the percentage of responses rate is 100%, which mean the total 386 of distributed questionnaires managed to collect back 386 completed questionnaires. Therefore, there were no invalid returned response or any not return. As a result, the researchers received all of the questionnaires that were delivered correctly and had a 100% response rate.

## **4.4 Data Analysis**

### **4.4.1 Descriptive analysis**



*Table 4.5 Statistics of respondent's experience towards online payment scam*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	120	31.1	31.1	31.1
	1	266	68.9	68.9	100.0
	Total	386	100.0	100.0	

The table above shown that there are 266 respondent experienced scam before when there are using online payment which converted into 68.9% and 120 respondents does not experienced scam before when there are using online payment which translated into 31.1%. The graph below can represent the table above.

*Graph 4.1 Number of respondent's experience towards online payment scam*

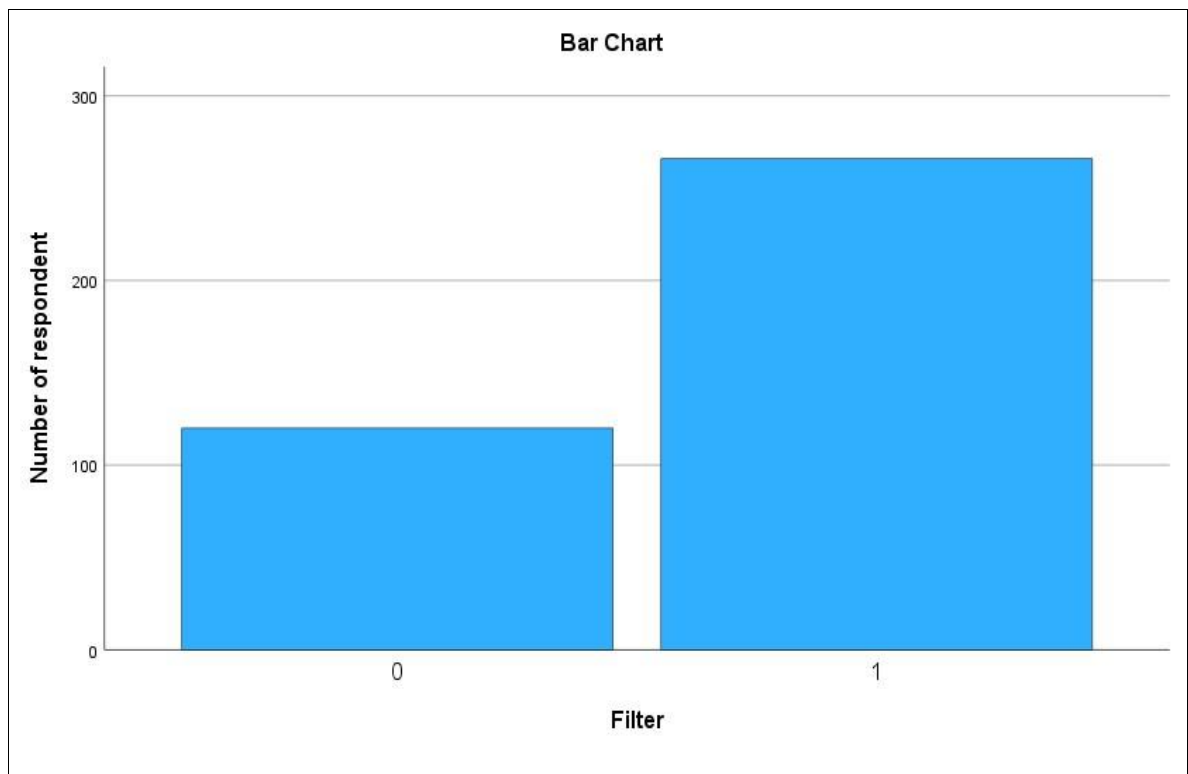
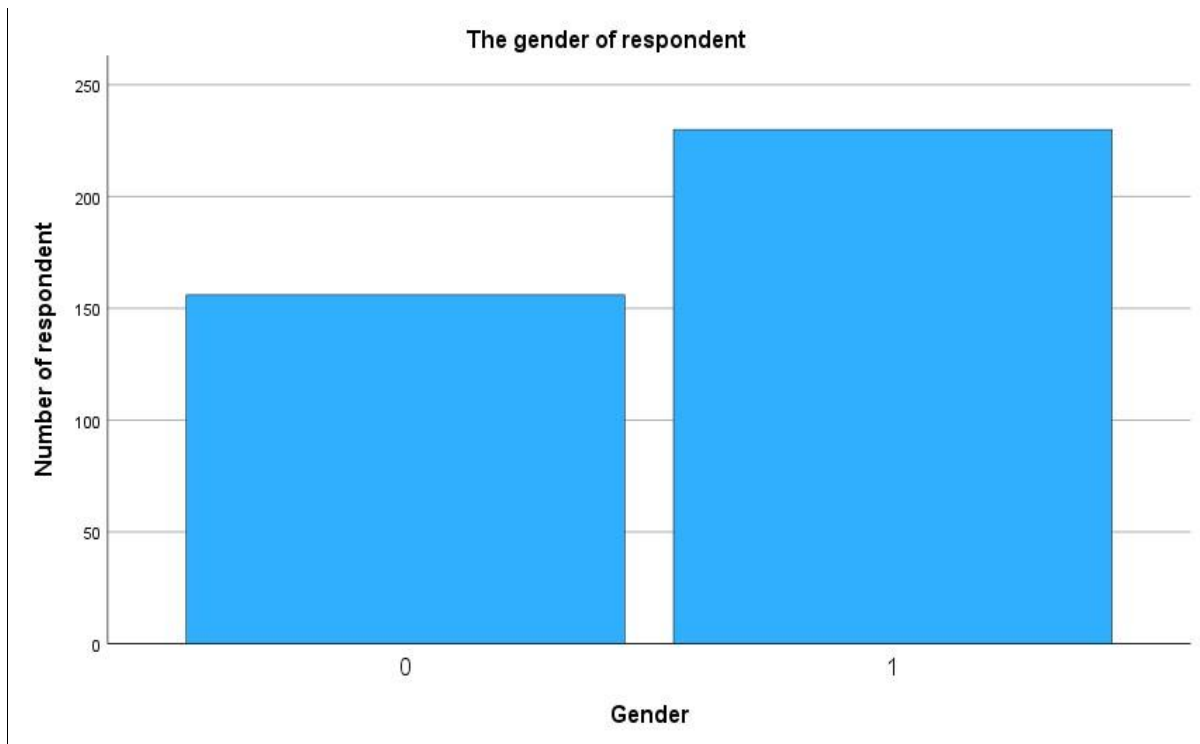


Table 4.6 Statistics of respondent's gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	156	40.4	40.4	40.4
	1	230	59.6	59.6	100.0
	Total	386	100.0	100.0	

Table 4.6 shown that there are 230 were female which represent 59.6% and 156 were male which translated into 40.4% in the total of 386 respondent. The graph below can represent the table above.

Graph 4.2 respondent's gender



## Adoption of online payment in the near future

Table 4.7 descriptive statistics for Adoption of online payment in the near future

Item	N	Minimum	Maximum	Mean	Std. Deviation
A1	386	1	5	4.32	.810
A2	386	1	5	3.69	1.140
A3	386	1	5	3.94	.886
A4	386	1	5	4.20	.740
A5	386	1	5	4.17	.852
A6	386	1	5	4.05	.904
A7	386	1	5	3.50	1.185
A8	386	1	5	3.71	1.249
A	386	1.63	5.00	3.9479	.57884
Valid N (listwise)	386				

Descriptive analysis for Adoption of online payment in the near future that shown in the table 4.7 above, reveal on overall mean score of 3.9479 ( $\approx 4$ ) and standard deviation of 0.57884. This indicated that the respondents agree that adoption of online payment in the near future is having the significant relationship with online payment scam. A1 had the highest mean value ( $4.32 \approx 4$ ), showing that most of the respondents agree that online payment brings more convenience to you when compared to traditional payment method.

## Security Issue

Table 4.8 descriptive statistics for security issue

Item	N	Minimum	Maximum	Mean	Std. Deviation
SI1	386	1	5	4.02	.826
SI2	386	1	5	4.03	.831
SI3	386	1	5	3.66	.852
SI4	386	1	5	4.17	.882
SI5	386	1	5	4.26	.741
SI6	386	1	5	3.18	1.204
SI7	386	1	5	3.90	.865
SI8	386	1	5	3.91	.844
SI	386	2.13	5.00	3.8902	.51846
Valid N (listwise)	386				

Descriptive analysis for security issue that shown in the table 4.8 above, reveal on overall mean score of 3.8902 ( $\approx 4$ ) and standard deviation of 0.51846. This indicated that the respondent agree that the security issue is having significant relationship with online payment scam. SI5 had the highest mean value ( $4.26 \approx 4$ ), showing that most of the respondents agree that dual digital authentications is necessary when using online transfer.

### **Perceived ease of used**

*Table 4.9 descriptive statistics of perceived ease of used*

Item	N	Minimum	Maximum	Mean	Std. Deviation
P1	386	1	5	4.05	.705
P2	386	1	5	4.16	.744
P3	386	1	5	4.28	.687
P4	386	1	5	4.22	.753

P	386	1.00	5.00	4.1762	.58197
Valid N (listwise)	386				

Descriptive analysis for perceived ease of used that shown in the table 4.9 above, reveal on overall mean score of 4.1762 ( $\approx 4$ ) and standard deviation of 0.58197. This indicated that the respondents agree that the perceived ease of used is having significant relationship with online payment scam. P3 had the highest mean value ( $4.28 \approx 4$ ), showing that most of the respondents agree that they feel online payment is easy to use.

### Trust

*Table 4.10 descriptive statistic of trust*

Item	N	Minimum	Maximum	Mean	Std. Deviation
T1	386	1	5	3.92	.849
T2	386	1	5	3.78	.887
T3	386	1	5	3.69	.910
T4	386	1	5	3.44	1.008
T5	386	1	5	3.52	.978
T	386	1.00	5.00	3.6684	.73041
Valid N (listwise)	386				

Descriptive analysis for trust that shown in the table 4.10 above, reveal on overall mean score of 3.6684 ( $\approx 4$ ) and standard deviation of 0.73041. This indicated that the respondent agree that trust is having a significant relationship with online payment scam. T1 had the highest mean value ( $3.92 \approx 4$ ), showing that most of the respondents agree that they trust the online payment system will provide good services than traditional payment method.

## Government intention

*Table 4.11 descriptive statistics of government intention*

Item	N	Minimum	Maximum	Mean	Std. Deviation
GI1	386	1	5	4.38	.795
GI2	386	1	5	4.15	.762
GI3	386	1	5	4.15	.762
GI4	386	1	5	4.15	.762
GI	386	1.00	5.00	4.2085	.67749
Valid N (listwise)	386				

Descriptive analysis for government intention that shown in the table 4.11 above, reveal on overall mean score of 4.2085 ( $\approx 4$ ) and standard deviation of 0.67749. This indicated that the respondents agree that the government intention is having a significant relationship with online payment scam. GI1 had the highest mean value ( $4.38 \approx 4$ ), showing that most of the respondents agree that they think government should strengthen the policies to fight with online payment scam.

*Table 4.12 case processing summary*

	Cases	Percent	Excluded		Total	Percent
	Included (N)		N	Percent	(N)	
A	386	100.0%	0	0.0%	386	100.0%

SI	386	100.0%	0	0.0%	386	100.0%
P	386	100.0%	0	0.0%	386	100.0%
T	386	100.0%	0	0.0%	386	100.0%
GI	386	100.0%	0	0.0%	386	100.0%

The table 4.12 above indicate that there are no case being excluded in the respond that collected from the questionnaire. All 386 respondent has seriously answered the question and all the answer are being recorded. The respond that we received has been fully (100%) utilize in the data analysis of this research.

*Table 4.13 case processing summary report*

A		SI	P	T	GI
Mean	3.9479	3.8902	4.1762	3.6684	4.2085
N	386	386	386	386	386
Std. Deviation	.57884	.51846	.58197	.73041	.67749

Table 4.13 is the summary of the analysis above. It showed the highest mean and the standard deviation of 5 independent variable that we have in this test including A, SI, P, T, G.

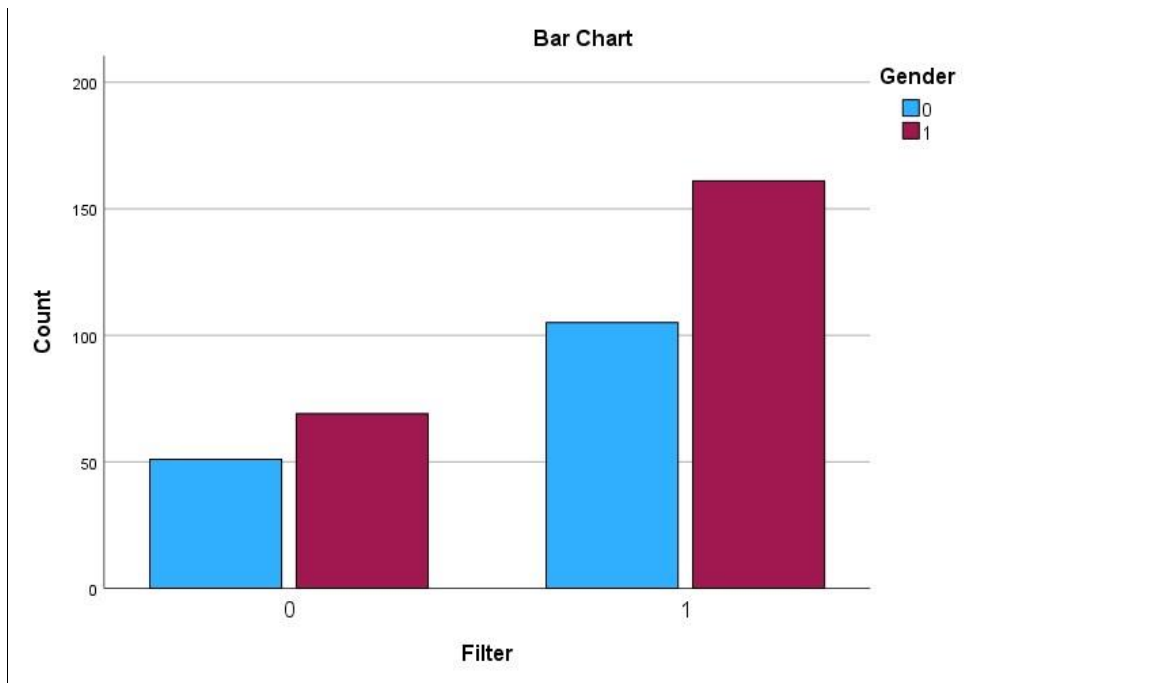
*Table 4.14 crosstable of filter\*gender*

		Gender		Total
		0	1	
Filter	0	51	69	120
	1	105	161	266

Total		156	230	386
-------	--	-----	-----	-----

Table above shown that there are 51 male respondents, and 69 female respondents did not experienced online payment scam whereas 105 male respondents and 161 female respondent experienced online payment scam. In total, there are 120 respondents do not experienced online payment scam and 266 respondents experienced online payment scam. Among 386 respondents, there are 156 male and 230 female. The graph below can represent the table above.

Graph 4.3 Bar chart



#### 4.4.2 Binary Logistic Regression

Table 4.15 Omnibus Tests of Model Coefficients

	Chi-square	df	Sig.
--	------------	----	------



Step 1	Step	13.273	5	.021
	Block	13.273	5	.021
	Model	13.273	5	.021

The model fit is examined using the Omnibus Tests of Model Coefficients. Referring to the table above, we can see from the model column, the p-value is 0.021 which is indicating a significant result as it is lesser than alpha value 0.05. Therefore, this implies that the fit is considerably better than the null model, and the model is demonstrating a good fit meaning that the model could be explain deeper (ResearchWithFawad, 2021).

Table 4.16 Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	10.011	8	.264

Hosmer and Lemeshow Test is another test to check whether the model is fit. The difference with the previous test is that this test shows poor fit when the p-value is lesser than 0.05. However, looking in the sig. in the table above, the model effectively fits the data as it is 0.264 which is greater than 0.05. This result indicate that the observed and anticipated models are identical (ResearchWithFawad, 2021).

Table 4.17 Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	465.216 <sup>a</sup>	.034	.048
a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.			

Pseudo R-Square is shown in the model summary. Pseudo indicates that it isn't actually elucidating the variation. Nonetheless, they can be used to roughly vary the criterion variable. Nagelkerke's R-square, an altered variation of the Cox & Snell R-square, is frequently employed. It modifies the measure of the data to include the entire range from 0 to 1 (ResearchWithFawad, 2021). Table above shown that 4.8% (0.048) change in the dependent variable can be explain by the independent variables. It means that anything happens in the independent variable cause 4.8% change in the dependent variable.

However, Forecast gaps and R-squared serve as measures of variability. Irrespective of the R-squared value, users evaluate the results for significant variables in the same way. Poor R-squared readings can signal that a forecast is not precise but does not diminish the significance of any relevant factors. Statistically significant P-values retain their correlations even with low R-squared, and coefficients still have the same meaning. The combination of statistically significant independent factors and low R-squared value shows that the independent factors and the dependent variable are associated, but they only partially account for the dependent variable's variability (Frost, 2017).

Table 4.18 Classification Table

	Observed		Predicted		
			Filter		Percentage Correct
			0	1	
Step 1	Filter	0	4	116	3.3
		1	4	262	98.5
	Overall Percentage				68.9
a. The cut value is .500					

The classification table above shows how effectively the model can forecast the proper group when the variables are included in the research (ResearchWithFawad, 2021). Overall, 68.9% of samples were correctly classified by the model. The accuracy rate was satisfactory but not especially good as it fall between 60%-70% (Allwright, 2022). The specificity and sensitivity of this model are 3.3% and 98.5% respectively. The percentage of samples that were accurately anticipated by the model to fit into the non-target category and were subsequently seen to do so is known as specificity while the sensitivity is the proportion of samples that were accurately anticipated by the model to belong to the target audience but were nonetheless observed to do so (ResearchWithFawad, 2021). Since 98.5% of those who did experience online payment scam were accurately predicted by the model to do so, the model shows strong sensitivity.

Table 4.19 Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
								Lower	Upper
Step 1 <sup>a</sup>	A	.194	.281	.474	1	.041	1.214	.699	1.107
	SI	.366	.328	1.247	1	.047	1.442	.758	1.742
	P	.216	.302	.510	1	.049	1.241	.686	1.242
	T	.165	.187	.781	1	.037	1.179	.818	1.700
	GI	-.108	.227	.228	1	.633	.897	.575	1.400
	Constant	-2.413	.939	6.608	1	.010	.090		
a. Variable(s) entered on step 1: A, SI, P, T, GI.									

The table above indicating the relationship between predictors and the result. Odds is referring to the ratio of probability. Beta (B) is the anticipated change in Log Odds which means that when 1 unit change in the predictor, the probability of the result will change Exp(B). The negative B indicate that the outcome factor will reduce by the beta coefficient value for every 1 unit increase in the predictor factor (ResearchWithFawad, 2021). Exposure to the predictor raises the probability of the result if the adjusted odds ratio is over 1.0 and the confidence interval is completely above 1.0. Exposure to the predictor reduces the likelihood of the result if the adjusted odds ratio is below 1.0 and the confidence interval is fully below 1.0 (Use and Interpret Logistic Regression in SPSS, 2023). From the table above, the odds of a respondent choosing they have the experience of online payment scam that encounter security issue are 1.442 times higher than those did not experience online payment scam which do not offer encounter security issue, with a 95% CI of 0.758 to 1.742. From the table above, we can see that the p-value of A, SI, P and T are 0.041, 0.047, 0.049, and 0.037 respectively, which added significantly to the model. However, the p-value of GI is 0.633 which is not significantly added to the model.

## CHAPTER 5: DISCUSSIONS AND CONCLUSIONS

## **5.1 Introduction**

In this chapter, we will discuss about the discussion of major findings, implications of study, and recommendation for future study.

## **5.2 Discussion of Major Findings**

### **5.2.1 The Adoption of Online Payment in The Near Future And Online Payment Scams**

Based on the results and discussions in Chapter 4, there is a significant and positive relationship between the adoption of online payment in the near future and online payment scams. Therefore, our major finding is the adoption of online payment in the near future is significantly and positively correlated with online payment scams. This finding supported by a study by Zhu, Sun, and Yan (2020). They found that the adoption of online payment systems was positively correlated with the occurrence of online payment scams in China. There is another study supported this finding, Wang, Xue, and Liang (2020) found that the adoption of online payment systems was positively correlated with an increase in scams.

### **5.2.2 Security Issues and Online Payment Scams**

Based on the results and discussions in Chapter 4, there is a significant and positive relationship between the security issues and online payment scams. Therefore, our major finding is the security issues is significantly and positively correlated with online payment scams. There is one study that supports the significant and positive relationship between security issues and online payment scams, which is a research conducted by Tsalis, Papadopoulos, and Karyda (2020). The study found that security issues were a major concern for consumers when it comes to online payment, and that consumers who had experienced security issues were more likely to fall victim to online payment scams. Furthermore, there is another study found that there is a positive relationship between security issues and online payment scams, indicating that online payment scams are more likely to occur when there are security vulnerabilities present (Abdul Wahab, Norhayati, & Hamid, 2017).

### **5.2.3 Perceived Ease of Use And Online Payment Scams**

Based on the results and discussions in Chapter 4, there is a significant and positive relationship between the perceived ease of use and online payment scams. Therefore, our major finding is the perceived ease of use is significantly and positively correlated with online payment scams. One study conducted by Alshammari, Aldakhil, and Alzahrani (2021) indicated that perceived ease of use had a positive relationship with susceptibility to online payment scams. This finding suggests that individuals who perceive online payment systems as easy to use may be more vulnerable to scams that exploit their trust in these systems. Furthermore, there is another study supported that there is positive relationship between perceived ease of use and online payment scams which is a study by Owusu, Boateng, and Ofori-Boateng (2019). This study indicated that the majority of respondents perceived online payment systems to be easy to use, but a significant number also reported falling victim to online payment scams.

#### **5.2.4 Trust and Online Payment Scams**

Based on the results and discussions in Chapter 4, there is a significant and positive relationship between trust and online payment scams. Therefore, our major finding is trust is significantly and positively correlated with online payment scams. This finding supported by a research. The research has shown that there is a positive relationship between trust and online payment scams, suggesting that when consumers trust online payment systems, they may be more vulnerable to scams (Kim et al., 2019). Furthermore, there is another research suggests that there is a positive relationship between trust and online payment scams. When consumers trust online payment systems, they may be more vulnerable to scams (Holtfreter, Reisig, & Pratt, 2019).

#### **5.2.5 Government Intention and Online Payment Scams**

Based on the results and discussions in Chapter 4, there is no significant relationship between the government intention and online payment scams. Therefore, our major finding is the government intention is not significantly correlated with online payment scams. According to a study by Lim et al. (2020), there is no significant relationship between government intention and online payment scams. The authors conducted a survey of 384 Malaysian consumers and found that while government intention was positively related to consumer trust in online payments, it did not have a significant impact on the occurrence of online payment scams.

## **5.3 IMPLICATION OF STUDY**

In this section, we will discuss the practical and theoretical implications of the study. Under this section, we will explain about what UTAR's students, lecturers, staff and government can do against online payment scam based on the result acquired from Chapter 4.

### **5.3.1 Practical Implication**

From the result, adoption of online payment scam in the near future is having significant and positive affect on online payment scam. This result showing that adoption of online payment in the near future indicates that the development of online payment such as booming Touch and go online payment method during Covid-19 and developed social media sales for all ages like online store on Facebook could increase the chance of user get scammed. Thus, the user of the online payment should have awareness of unknown or newly introduced online payment method, especially those social media online stores which have no legal registered.

Secondly, security issue is showing significant and positive affect on online payment scam too. The online payment scams are a common issue in society, people start to use security systems such as IP address locator and some fraud detection software. Although security measures cannot guarantee 100% online payment security, comprehensive security measures can effectively reduce the number of online payment frauds such as the legal fraud detection software will inform the user while there is an insecure information, websites, or user account therefore when users go through online payment, they can more effectively avoid online payment scam. Additionally, the banker can also use the Neuralnetwork to prevent their user for getting online payment scam, the Neural-network fraud detection software helps the banker analysis the credit card's data to detect whether

there are online payment scam cases and then avoid the crime from happening (G&R, 1994).

Third, the study's result is showing perceived ease of use is having significant and positive affect on online payment scam. From the result of perceived ease of use mostly the user of online payment is using online payment is based on its convenience, some of them also bind their credit card on certain apps, such as Shopee, Lazada and some online stores for easier and faster balance top up. Although binding credit cards with online payment app or online store bring more convenience to user, the risk of getting online payment scam is also increase in this situation.

Last but not least, trust is showing in a significant and positive relationship result between online payment scam from the study. Since e-commerce and virtual communities have changed the way of business nowadays, most people started to fully believe in online shopping and forget about the risk of it. Online shopping users should pay more attention to the safety of online shopping and understand the risks instead of blindly trusting it. According to the result, people who fully trust online payment shopping are more likely to encounter online payment scams.

Finally, the government intention is showing negative relationship between online payment scams. The government intention will not be discuss in this study, although it is having a relationship between online payment scam, the result from the study is showing it is insignificant against the dependent variable, online payment scam which the result cannot be referred.

### **5.3.2 Theoretical Implication**

From the result, all the variables adoption of online payment, security issue, perceived ease of use, trust and government intention are significant which are main factors that will affect online payment scam. Among them, adoption of online payment, perceived ease of use and trust are positive relationship with online payment scam which mean that the increase of



these three variables will theoretically cause the increase of online payment scam. Besides, there are negative relationships from security issue and government intention with online payment scam too, which show us that the increase of security issue and government intention will help less online payment scam.

Last, the Routine activity theory is used in this research. In this theory, when a motivated perpetrator and a targeted victim are present in the same location or platform, the chances of committing a crime increase. This also means that due to the development of Internet technology, victims are more likely to be exposed to online payment scams (Chen, 2017). By this theory, it also stands for the research variable, adoption of online payment which has positive relationship with online payment scams.

## **5.4 Recommendation for future study**

As this research is using quantitative data collection method, the showing result is based on limited respondents, so adding qualitative data collection method in future study is recommended. The qualitative data collection method can lead to more precise results for future researchers, to understand more detailed and perfect methods of response. In addition, to collect more complete data, open surveys are also highly recommended. Through open-ended surveys, respondents can give the most appropriate answers more freely, which is tantamount to helping research to obtain more accurate data (Clements, 2021).

Overall, the recommendation given in this study is to use as large and detailed data as possible for research, including using quantitative data collection method.

## References

- Abdul Wahab, N., Norhayati, Z., & Hamid, N. A. (2017). An analysis of the relationship between security issues and online payment fraud. *Journal of Theoretical and Applied Information Technology*, 95(6), 1272-1283.
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Akgül, G. (2021, October 1). Routine Activities Theory in cyber victimization and cyberbullying experiences of Turkish adolescents. *International Journal of School & Educational Psychology*, 11(2), 135–144. <https://doi.org/10.1080/21683603.2021.1980475>
- Akhtar, I. (2016, September). *Research Design*. ResearchGate. Retrieved August 29, 2022, from [https://www.researchgate.net/publication/308915548\\_Research\\_Design](https://www.researchgate.net/publication/308915548_Research_Design)
- Albaity, M., & Rahman, M. (2019). The intention to use Islamic Banking: An exploratory study to measure Islamic Financial Literacy. *International Journal of Emerging Markets*, 14(5), 988–1012. <https://doi.org/10.1108/ijoem-05-2018-0218>
- Alhaimer, R. (2021). Fluctuating Attitudes and Behaviors of Customers toward Online Shopping in Times of Emergency: The Case of Kuwait during the COVID-19 Pandemic. *Journal of Internet Commerce*, 21(1), 26–50. <https://doi.org/10.1080/15332861.2021.1882758>
- Allwright, S. (2022, May 14). *What is a good accuracy score? Simply explained*. Stephen Allwright; Stephen Allwright. Retrieved from <https://stephenallwright.com/good-accuracy->



- BOTS team. (2022, January 11). #TECH: Watch out for rewards scams -Shopee | New Straits Times - NST Online. Retrieved from <https://www.nst.com.my/lifestyle/bots/2022/01/761954/tech-watch-out-rewards-scamsshopee>
- Boyd, J. (2006). In Community We Trust: Online Security Communication at eBay. *Journal of Computer-Mediated Communication*, 7(3), 0. Retrieved from <https://doi.org/10.1111/j.10836101.2002.tb00147.x>
- Bryant, J., & Reffett, A. (2019). Exploring the barriers and motivations of mobile payment adoption in the United States. *Journal of Retailing and Consumer Services*, 50, 243-249.
- Bush, T. (2020, June 22). Descriptive Analysis: How-To, Types, Examples. Retrieved August 29, 2022, from PESTLE Analysis website: <https://pestleanalysis.com/descriptive-analysis/>
- Button, M., & Cross, C. (2017a). Cyber Frauds, Scams and their Victims. *Routledge EBooks*. Retrieved from <https://doi.org/10.4324/9781315679877>
- Chang, D. J. (n.d.). *Online Shopping: Advantages over the Offline Alternative | Open Access Journals*. Online Shopping: Advantages Over the Offline Alternative | Open Access Journals. <https://www.icommercecentral.com/open-access/online-shopping-advantages-over-the-offline-alternative.php?aid=38815>
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors.
- Chen, H., Beaudoin, C. E., & Hong, T. (2017b). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291–302. <https://doi.org/10.1016/j.chb.2017.01.003>
- Clements, J. (2021). What are the benefits of using interviews in research? MOS Transcription Company. Retrieved September 13, 2022, from <https://www.legaltranscriptionservice.com/blog/what-the-benefits-of-using-interviews-inresearch/>.

- Computers in Human Behavior*, 70, 291–302. Retrieved from <https://doi.org/10.1016/j.chb.2017.01.003>
- Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law Crime and Justice*, 55, 1–12. Retrieved from <https://doi.org/10.1016/j.ijlcj.2018.08.001>
- Dahlgreen, J. (2021). Catastrophic fraud loss lies where it falls? Push payment scams and the bank's duty of care to its customer. *Journal of Financial Crime*. Retrieved from <https://doi.org/10.1108/jfc-10-2021-0223>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340. <https://doi.org/10.2307/249008>
- Dudovskiy, J. (n.d.). *Descriptive Research*. Business Research Methodology. Retrieved August 30, 2022, from <https://research-methodology.net/descriptive-research/>
- European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape for the Finance Sector. Retrieved from <https://www.enisa.europa.eu/publications/threat-landscape-for-the-finance-sector>
- Fatemeh , M., Zuraini, I., & Bharani , S. (2013). *Online Purchase Intention: Effects of Trust and Security Perception* . Australian Journal of Basic and Applied Sciences. Retrieved from [https://www.researchgate.net/publication/280134930\\_ajbaswebcomoldajbas2015Special20IPN20Hatyai38-42pdf](https://www.researchgate.net/publication/280134930_ajbaswebcomoldajbas2015Special20IPN20Hatyai38-42pdf)
- Federal Trade Commission. (2019). Consumer Sentinel Network Data Book 2018. Retrieved from [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer\\_sentinel\\_network\\_data\\_book\\_2018.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018.pdf)
- Federal Trade Commission. (2020). Consumer Sentinel Network Data Book 2019. Retrieved from [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-databook-2019/consumer\\_sentinel\\_network\\_data\\_book\\_2019.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-databook-2019/consumer_sentinel_network_data_book_2019.pdf)

- Federal Trade Commission. (2021). Consumer Sentinel Network Data Book 2020. Retrieved from [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/consumer\\_sentinel\\_network\\_data\\_book\\_2020.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/consumer_sentinel_network_data_book_2020.pdf)
- Feng, Y., Zhang, Y., & Zhang, J. (2020). Regulation, technological innovation, and online payment scams: Evidence from China. *Electronic Commerce Research and Applications*, 41, 100919.
- Fernandes, L. (2013, March). *FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES*. Retrieved from [file:///C:/Users/Asus/Downloads/FRAUDINELECTRONICPAYMENTTRANSACTIONS\\_THREATSANDCOUNTERMEASURES.pdf](file:///C:/Users/Asus/Downloads/FRAUDINELECTRONICPAYMENTTRANSACTIONS_THREATSANDCOUNTERMEASURES.pdf)
- Fincham, J. E. (2008, April 15). *Response rates and responsiveness for surveys, standards, and the journal*. *American journal of pharmaceutical education*. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2384218/#:~:text=Response%20rates%20are%20calculated%20by,eligible%20in%20the%20sample%20chosen>.
- Frost, J. (2017, May 13). *How to Interpret Regression Models that have Significant Variables but a Low R-squared*. Statistics by Jim. Retrieved from <https://statisticsbyjim.com/regression/low-r-squared-regression/>
- G., & R. (1994). Credit card fraud detection with a neural-network. *Hawaii International Conference on System Sciences*. Retrieved from <https://doi.org/10.1109/hicss.1994.323314>
- Geisinger, K. F. (2010, January 30). Questionnaires. *The Corsini Encyclopedia of Psychology*, 1–3. <https://doi.org/10.1002/9780470479216.corpsy0766>
- H2o.ai. (2023). What is Logistic Regression Used for? Retrieved from <https://h2o.ai/wiki/logistic-regression/#:~:text=Logistic%20regression%20is%20used%20to%20predict%20the%20categorical%20dependent%20variable,history%20and%20other%20such%20factors>.
- 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. Retrieved from <https://doi.org/10.5296/jmr.v7i2.6938>

Holtfreter, K., Reising, M. D., & Pratt, T. C. (2019). Explaining online payment fraud victimization: The effects of perceived risk, online purchasing, and trust. *Crime & Delinquency*, 65(3), 279-304.

Indarsin, T., & Ali, H. (2017). Attitude toward Using m-commerce: The analysis of perceived usefulness perceived ease of use, and perceived trust: Case study in Iken's Wholesale Trade, Jakarta–Indonesia. *Saudi Journal of Business and Management Studies*, 2(11), 995-1007.

Jia, Y., & Wang, C. (2020). Understanding online payment scams in China: A routine activity approach. *Asian Journal of Criminology*, 15, 149-167.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*, 37(4), 480–501. Retrieved from <https://doi.org/10.1177/10439862211027986>

Kiew, C. C., Abu Hasan, Z. R., & Abu Hasan, N. (2021). FACTORS INFLUENCING CONSUMERS IN USING SHOPEE FOR ONLINE PURCHASE INTENTION IN EAST COAST MALAYSIA. *Universiti Malaysia Terengganu Journal of Undergraduate Research*, 3(1), 45–56. Retrieved from <https://doi.org/10.46754/umtjur.2021.01.006>

Kim, J., Lee, C. K., Lee, H. J., & Rho, J. (2019). Online trust and its influence on online payment intention: The moderating effect of perceived risk. *International Journal of Information Management*, 45, 16-28.

Lavrakas, P. J. (2008). Target population. *Encyclopedia of Survey Research Methods*. Retrieved from <https://doi.org/10.4135/9781412963947.n571>

Lazar, A. J. P., Sengan, S., Cavaliere, L. P. L., Nadesan, T., Sharma, D., Gupta, M. K., Palaniswamy, T., Vellingiri, M., Sharma, D. K., & Subramani, T. (2021). Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications*. Retrieved from <https://doi.org/10.1007/s11277-021-08585-y>

- Lee, H., & Song, H. (2020). The impact of government policies on online payment fraud in South Korea. *International Journal of Information Management*, 51, 102017.
- Lian, J. W., & Lin, T. M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior*, 24(1), 48–65. <https://doi.org/10.1016/j.chb.2007.01.002>
- Lian, J. W., & Yen, D. C. (2014). Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human Behavior*, 37, 133–143. <https://doi.org/10.1016/j.chb.2014.04.028>
- Liao, Z., Li, Y., Liu, X., & Zhou, T. (2017). Understanding individuals' adoption of mobile payment services: A cognitive processing perspective. *Electronic Commerce Research and Applications*, 26, 22-37. doi: 10.1016/j.elerap.2017.09.005
- Lim, Y. T., Teoh, H. J., Lim, Y. M., & Tan, G. W. H. (2020). Trust in online payment systems: The role of government intention and social influence. *International Journal of Information Management*, 50, 218-230.
- Lin, H., Chen, Y., & Chen, Y. (2017). The impact of security issues on online payment adoption: A study of e-shoppers in Taiwan. *International Journal of Electronic Business Management*, 15(1), 1-12.
- Lin, L., Tan, C., & Yang, X. (2020). The Effect of Government Intervention on Online Payment Scams: Evidence from China. *Sustainability*, 12(21), 8818.
- Liu, C., Huang, Y., & Hu, J. (2020). The impact of government policies on online payment scams in Taiwan. *Electronic Commerce Research and Applications*, 40, 100943.
- Liu, Y., Lu, J., & Wang, X. (2021). Online payment security, payment method, and payment intention: Evidence from China. *Journal of Business Research*, 132, 110-118.
- Mohammad, A., Ferri, N., & Suhana, M. (2018, June 1). *Factors affecting consumers' acceptance towards electronic payment system: Case of a government land and district office / Mohamad Azwan MD ISA, Ferri Nasrul and Suhana Mohamed*. Factors affecting consumers' acceptance



towards electronic payment system: case of a government land and district office / Mohamad Azwan Md Isa, Ferri Nasrul and Suhana Mohamed - UiTM Institutional Repository. Retrieved from <https://ir.uitm.edu.my/id/eprint/41192/>

Mokhsin, M., Aziz, A. A., Zainol, A. S., Humaidi, N., & Zaini, N. A. A. (2019). Probability Model: Malaysian Consumer Online Shopping Behavior towards Online Shopping Scam. *International Journal of Academic Research in Business and Social Sciences*, 9(1). Retrieved from <https://doi.org/10.6007/ijarbss/v9-i1/5478>

Mondego, D., & Gide, E. (n.d.). *THE USE OF THE TECHNOLOGY ACCEPTANCE MODEL TO ANALYSE THE CLOUD-BASED PAYMENT SYSTEMS: a comprehensive review of the literature*. Scielo - brazil - the use of the technology acceptance model to analyse the cloud-based payment systems: a comprehensive review of the literature the use of the technology acceptance model to analyse the cloud-based payment systems: a comprehensive review of the literature. <https://doi.org/10.4301/S1807-1775202219007>

Montague, D. A. (2010). *Essentials of Online payment Security and Fraud Prevention* (1st ed.). Wiley.

Naeem, S. (2019, June 6). *Data editing in research*. ResearchArticles.com. Retrieved from <https://researcharticles.com/index.php/data-editing-in-research/>

Nguyen, H., V. Nguyen, H. Q., & Le, T. (2016). Factors affecting online shopping behavior of consumers in Vietnam. *Journal of Economics, Business and Management*, 4(4), 338-342.

O. Pappas, I., G. Pateli, A., N. Giannakos, M., & Chrissikopoulos, V. (2014). Moderating effects of online shopping experience on customer satisfaction and repurchase intentions. *International Journal of Retail & Distribution Management*, 42(3), 187–204. Retrieved from <https://doi.org/10.1108/ijrdm-03-2012-0034>

Oladejo, T. O., Rahman, A. A., & Adesina, Y. A. (2021). The impact of government regulations on the online payment fraud in Nigeria. *Cogent Business & Management*, 8(1), 1883369.

Owusu, A., Boateng, R., & Ofori-Boateng, K. (2019). Perceived ease of use and online payment scams in Ghana. *International Journal of Bank Marketing*, 37(3), 671- 686.

- Phan, T. B., Limbu, Y. B., & Shah, M. A. A. (2020). Exploring the factors influencing the prevalence of online payment scams in Malaysia. *Journal of Financial Crime*, 27(4), 1126-1142.
- Probowo, H. (2012). Towards a Better Credit Card Fraud Prevention Strategy in Indonesia. *Hendi Yogi Prabowo*.
- Raj Singh, D., & Chudasama, D. (2021). Brief Study of Cybercrime on an Internet. *Journal of Communication Engineering & Systems*. <https://doi.org/10.37591/JoCES>
- ResearchWithFawad. (2021, October 7). *Binary Logistic Regression Analysis in SPSS* - <https://researchwithfawad.com/index.php/lp-courses/data-analysis-using-spss/binary-logistic-regression-analysis-in-spss/>
- Response rates of online surveys in published research: A meta-analysis*. (2022, May 26). Response Rates of Online Surveys in Published Research: A Meta-analysis - ScienceDirect. <https://doi.org/10.1016/j.chbr.2022.100206>
- Rigopoulos, G., & Askounis, D. (n.d.). *A TAM Framework to Evaluate Users' Perception towards Online Electronic Payments | Open Access Journals*. A TAM Framework to Evaluate Users Perception Towards Online Electronic Payments | Open Access Journals. <https://www.icommercecentral.com/open-access/a-tam-framework-to-evaluate-users-perception-towards-online-electronic-payments.php?aid=38520>
- Routine Activity Theory (RAT) | North Miami Beach, FL*. (n.d.). Routine Activity Theory (RAT) | North Miami Beach, FL. <https://www.citynmb.com/194/Routine-Activity-Theory-RAT>
- Sakharova, I. (2012). Payment card fraud: Challenges and solutions. In *Intelligence and Security Informatics*. <https://doi.org/10.1109/isi.2012.6284315>
- Sarstedt, M., Hopkins, L., Kuppelwieser, V. G., & Hair Jr, J. F. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review*, 26(2), 106–121. Retrieved from <https://doi.org/10.1108/eb-10-2013-0128>
- Sperandei, S. (2014, February 15). *Understanding logistic regression analysis*. *Biochemia medica*. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3936971/>

- Statistics Solutions. (2021, June 9). *Pearson's correlation coefficient*. Retrieved from <https://www.statisticssolutions.com/free-resources/directory-of-statisticalanalyses/pearsons-correlation-coefficient/>
- Stratton, S. J. (2021). Population Research: Convenience Sampling Strategies. *Prehospital and Disaster Medicine*, 36(4), 373–374. <https://doi.org/10.1017/s1049023x21000649>
- Sun, Y. (2018, December 19). *The sage encyclopedia of communication research methods*. Sage Research Methods. Retrieved from <https://methods.sagepub.com/reference/the-sageencyclopedia-of-communication-researchmethods/i2620.xml#:~:text=Coding%20of%20data%20refers%20to,the%20recorded%20o%20r%20observed%20phenomenon>.
- Suroso, J. S., Kaburuan, E. R., Lee, D., Tama, N. S., & Tee, K. (2020). Analysis Of E-Commerce System In Marketplace (Shopee Indonesia). *2020 8th International Conference on Orange Technology (ICOT)*. <https://doi.org/10.1109/icot51877.2020.9468783>
- Syed, M. S. K. (2016, July). *method 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)
- Tsalis, V., Papadopoulos, T., & Karyda, M. (2020). Factors Affecting the Adoption of Online Payment Systems by Consumers: A Case Study in Greece. *Journal of Theoretical and Applied Electronic Commerce Research*, 15(5), 27-43.
- Turner, A. G. (2003). Sampling frames and master samples. *United Nations secretariat statistics division*, 1-26.
- Use and Interpret Logistic Regression in SPSS*. (2023). Accredited Professional Statistician for Hire. <https://www.scalestatistics.com/logistic-regression.html>
- UTAR In Brief*. (n.d.). <https://study.utar.edu.my/utar-at-a-glance.php>
- Wang, D., Xue, L., & Liang, J. (2020). Does mobile payment increase the risk of fraud? Evidence from China. *Electronic Commerce Research and Applications*, 40, 100922.

- Wills, S., Roecker, S., & Avello, T. D. (2020). *Sampling Design*. Stats\_for\_soil\_survey. Retrieved April 21, 2022, from [http://ncss-tech.github.io/stats\\_for\\_soil\\_survey/](http://ncss-tech.github.io/stats_for_soil_survey/)
- Wu, J. H., & Chen, Y. C. (2018). Understanding online payment scam victims: A comparative analysis of victims and non-victims. *Telematics and Informatics*, 35(7), 1912-1925.
- Xu, J., Deng, Y., & Chen, H. (2020). Does government intervention reduce online payment scams? Evidence from a cross-country analysis. *Journal of Financial Crime*, 27(4), 1135-1149.
- Yan, L., Peng, Y., & Li, C. (2020). Analysis of online payment scams in China: Characteristics and prevention measures. *Journal of Risk Research*, 23(7), 942- 957.
- Yoon, Y., & Corritore, C. L. (2011). Building trust in online marketplaces through an economic incentive mechanism. *Decision Support Systems*, 52(1), 272-282. Retrieved from doi:10.1016/j.dss.2011.08.003
- Zhang, Y., Gao, Y., Zhang, X., & Yang, K. (2020). The Impact of E-Commerce Policy on Online Payment Fraud: Evidence from China. *Sustainability*, 12(5), 2098.
- Zhu, H., Sun, L., & Yan, J. (2020). Understanding the relationship between the adoption of online payment and online payment scams in China. *Journal of Consumer Behaviour*, 19(6), 660-673.

## Appendices

### Appendix 1 - Participant Information Page

#### Section 1 – Personal Data Protection Statement

---

## 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.


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 [limjasmin2001@1utar.my](mailto:limjasmin2001@1utar.my)

Email \*

Your email

 This is a required question

Next

Clear form

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.

Name \*

Your answer

### Part 1: Introduction

Topic: Online Payment Scam: What Have Caused It?

Dear Respondent:

We are undergraduate students of Bachelor of Economic (Hons) Financial Economics from Universiti Tunku Abdul Rahman (UTAR) based in Kampar campus. We are currently conducting our Final Year Project with the title "Online Payment Scam in Malaysia". The purpose of conducting this academic research is to analyze and determine the increasingly rampant Internet fraud jeopardizes the financial security of many people.

You are highly welcome to partake in this survey if you are:

1. have the experience on online payment scam
2. your friends or families has experienced online payment scam.
3. Malaysia citizen

All your information and responses provided will be solely used for the purpose of this academic research and will be reminded private and confidential. We would like to thank you for spending your time to participant in this survey.

Back

Next

Clear form

## Appendix 2 – Questionnaire Format

### Section 2 – Filter Respondents

#### Part 2: Filter Respondents

Did you or your families and friends been experienced scam before while using online payment? \*

Yes

No

Back

Next

Clear form

## Section 3 – Demographic Information of Respondents

### Part 3: Demographic information

What is your ages? \*

- Below 20 years old
- 21 – 39 years old
- 40 – 59 years old
- 60 years old and above

What is your gender? \*

- Female
- Male

What is your current employment status? \*

- Student
- Part-time employment
- Full-time employment
- Unemployment
- Housewife
- Retired
- Other

How much is your monthly expenses? \*

- Below RM1000 per month
- RM1500 – RM1999 per month
- RM2000 – RM2499 per month
- RM2500 – RM2999 per month
- Over RM3000 per month

Back

Next

Clear form



## Section 4 – Adoption of online payment in the near future (IV 1)

### Adoption of online payment in the near future

Perspectives on online payment method and online payment scam:

Please indicate the extent to which you agreed and disagreed with each statement by using following scale. In this section, we seek your opinion about the experience of online payment scam and the factors affecting the adoption of online payment.

(1) = Strongly Disagree (SD)

(2) = Disagree (D)

(3) = Neutral (N)

(4) = Agree (A)

(5) = Strongly Agree (SA)

Do you think online payment brings more convenience to you when compared to traditional payment method \*

- SD
- D
- N
- A
- SA

I spent more than 50% of my income per month in online payment \*

- SD
- D
- N
- A
- SA

The reason that I choose to adopt online payment because It help to make expenditure record \*

- SD
- D
- N
- A
- SA

The reason that I choose to adopt online payment because It help me save time and effort \*

- SD
- D
- N
- A

I normally use online payment for online shopping purpose \*

- SD
- D
- N
- A
- SA

I normally use online payment for pay bills purpose \*

- SD
- D
- N
- A
- SA

I start using online payment **before** pandemic \*

- SD
- D
- N
- A
- SA

I start using online payment **after** pandemic \*

- SD
- D
- N
- A
- SA

## Section 5 – Security Issue (IV 2)

### Security Issue

I worry about the secondary use of the information that I provided when making \*  
online payment

- SD
- D
- N
- A
- SA

It is risky to get scam when using online payment \*

- SD
- D
- N

Making transaction or make payment through online for goods and services is secure \*

- SD
- D
- N
- A
- SA

I will reject to use online payment when the third party ask me to provide financial information (account number or bank account password) \*

- SD
- D
- N
- A

Dual digital authentications is necessary when using online transfer \*

- SD
- D
- N
- A
- SA

I am willing to bind my credit card with the e-payment \*

- SD
- D
- N
- A
- SA

Scam detection application is useful in avoid online payment scam \*

- SD
- D
- N
- A
- SA

When making online shopping I always worry about the sellers fail to sent out the products. \*

- SD
- D
- N
- A

## Section 6 – Perceived Ease of Use (IV 3)

### Perceived Ease of Use

online payment is feasible to access \*

- SD
- D
- N
- A
- SA

online payment provides various payment channels to enable me to make payment easily \*

- SD
- D
- N

I feel online payment is easy to use \*

- SD
- D
- N
- A
- SA

online payment provide fast services \*

- SD
- D
- N
- A
- SA

## Section 7 – Trust (IV 4)

### Trust

I trust the online payment system will provide good services than traditional payment method \*

- SD
- D
- N
- A
- SA

I trust the service department can provide good solution when online payment has technical issue occur \*

- SD
- D

I trust online payment system will keep our personal or financial information safe \*

- SD
- D
- N
- A
- SA

I trust online payment is safe when transferring big sum of funds \*

- SD
- D
- N
- A
- SA

I trust online payment is safe for every online transaction \*

- SD
- D
- N
- A
- SA

Back

Next

Clear form

## Section 8 – Government Intention (IV 4)

### Government Intention

I think government should stengthen the policies to fight with online payment scam \*

- SD
- D
- N
- A
- SA

Government should promote online payment services \*

- SD
- D
- N

The attitude of government will affect the adoption of online payment. \*

- SD
- D
- N
- A
- SA

Government should strengthen the facilities of online payment. \*

- SD
- D
- N
- A
- SA



## Appendix 3 – Filter Respondent

### Section 1 – Usage Behaviour

#### Part 5: Filter respondent by Usage Behaviour

Which online payment do you know? \*

- PayPal
- Debit card (Visa or MasterCard)
- Alipay
- Shopee Pay
- Touch 'n Go
- Amazon payment
- FPX
- Other

Which online payment do you regular use? \*

- PayPal
- Debit card (Visa or MasterCard)
- Alipay
- Shopee Pay
- Touch 'n Go
- Amazon payment
- FPX
- Other

How much did you spend in online payment (per month)? \*

- Below RM1000 per month
- RM1500 – RM1999 per month
- RM2000 – RM2499 per month
- RM2500 – RM2999 per month
- Over RM3000 per month

What kind of scam have you or your families and friends encountered? \*

- Identify Theft
- Business email compromise
- Payment interception
- Password or code hacking
- Refund fraud

How do you deal with scams when you encountered? \*

- Ignore it
- Report to police immediately
- Download online scam detection application

Which detection or measurement tools did you prefer? \*

- IP Address Locator
- Fraud Detection Software
- ACH Block
- Order dispositioning
- Fraud Claim Management
- Manual review
- UPIC
- Automated Scam Detection

## Appendix 4 - Table

### Section 1: SPSS Output - Descriptive analysis

#### Frequencies

[DataSet1]

		Statistics	
		Filter	Gender
N	Valid	386	386
	Missing	0	0
Mode		1	1
Minimum		0	0
Maximum		1	1

#### Frequency Table

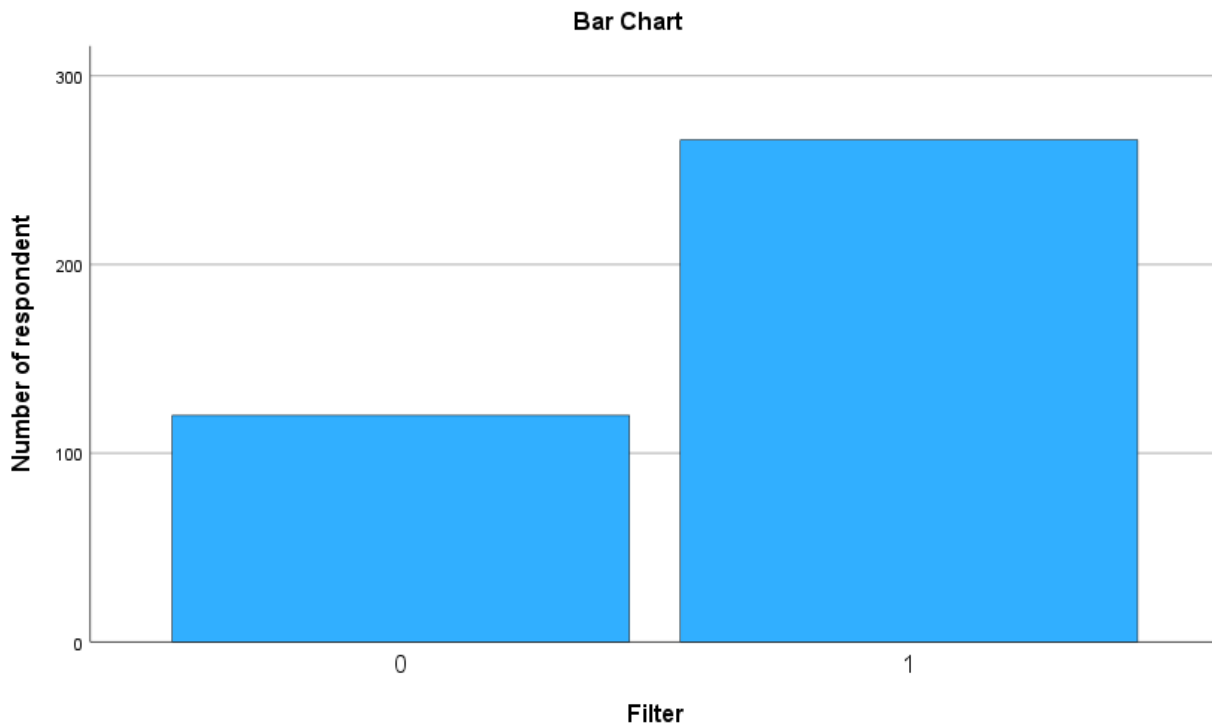
	Filter		
Frequency	Percent	Valid Percent	Cumulative Percent

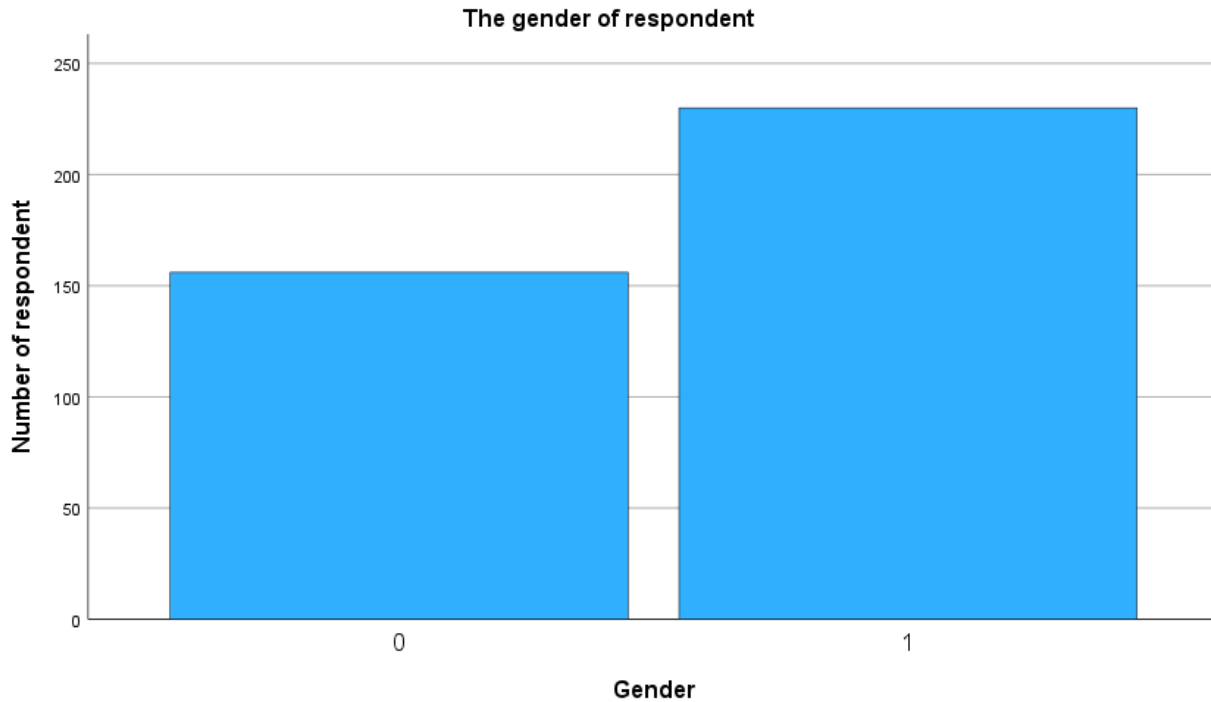
Valid	0	120	31.1	31.1	31.1
	1	266	68.9	68.9	100.0
	Total	386	100.0	100.0	

**Gender**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	156	40.4	40.4	40.4
	1	230	59.6	59.6	100.0
	Total	386	100.0	100.0	

**Bar Chart**





**Descriptives**

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
A1	386	1	5	4.32	.810
A2	386	1	5	3.69	1.140
A3	386	1	5	3.94	.886
A4	386	1	5	4.20	.740
A5	386	1	5	4.17	.852
A6	386	1	5	4.05	.904
A7	386	1	5	3.50	1.185
A8	386	1	5	3.71	1.249
Valid N (listwise)	386				

**Descriptives**

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
A1	386	1	5	4.32	.810

A2	386	1	5	3.69	1.140
A3	386	1	5	3.94	.886
A4	386	1	5	4.20	.740
A5	386	1	5	4.17	.852
A6	386	1	5	4.05	.904
A7	386	1	5	3.50	1.185
A8	386	1	5	3.71	1.249
A	386	1.63	5.00	3.9479	.57884
Valid N (listwise)	386				

## Descriptives

### Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
SI1	386	1	5	4.02	.826
SI2	386	1	5	4.03	.831
SI3	386	1	5	3.66	.852
SI4	386	1	5	4.17	.882
SI5	386	1	5	4.26	.741
SI6	386	1	5	3.18	1.204
SI7	386	1	5	3.90	.865
SI8	386	1	5	3.91	.844
SI	386	2.13	5.00	3.8902	.51846
Valid N (listwise)	386				

## Descriptives

### Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
P1	386	1	5	4.05	.705
P2	386	1	5	4.16	.744

P3	386	1	5	4.28	.687
P4	386	1	5	4.22	.753
Valid N (listwise)	386				

**Descriptives**

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
P1	386	1	5	4.05	.705
P2	386	1	5	4.16	.744
P3	386	1	5	4.28	.687
P4	386	1	5	4.22	.753
P	386	1.00	5.00	4.1762	.58197
Valid N (listwise)	386				

**Descriptives**

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
T1	386	1	5	3.92	.849
T2	386	1	5	3.78	.887
T3	386	1	5	3.69	.910
T4	386	1	5	3.44	1.008
T5	386	1	5	3.52	.978
Valid N (listwise)	386				

**Descriptives**

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
--	---	---------	---------	------	-------------------

T1	386	1	5	3.92	.849
T2	386	1	5	3.78	.887
T3	386	1	5	3.69	.910
T4	386	1	5	3.44	1.008
T5	386	1	5	3.52	.978
T	386	1.00	5.00	3.6684	.73041
Valid N (listwise)	386				

## Descriptives

### Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
GI1	386	1	5	4.38	.795
GI2	386	1	5	4.15	.762
GI3	386	1	5	4.15	.762
GI4	386	1	5	4.15	.762
Valid N (listwise)	386				

### Report

	A	SI	P	T	GI
Mean	3.9479	3.8902	4.1762	3.6684	4.2085
N	386	386	386	386	386
Std. Deviation	.57884	.51846	.58197	.73041	.67749

## Crosstabs

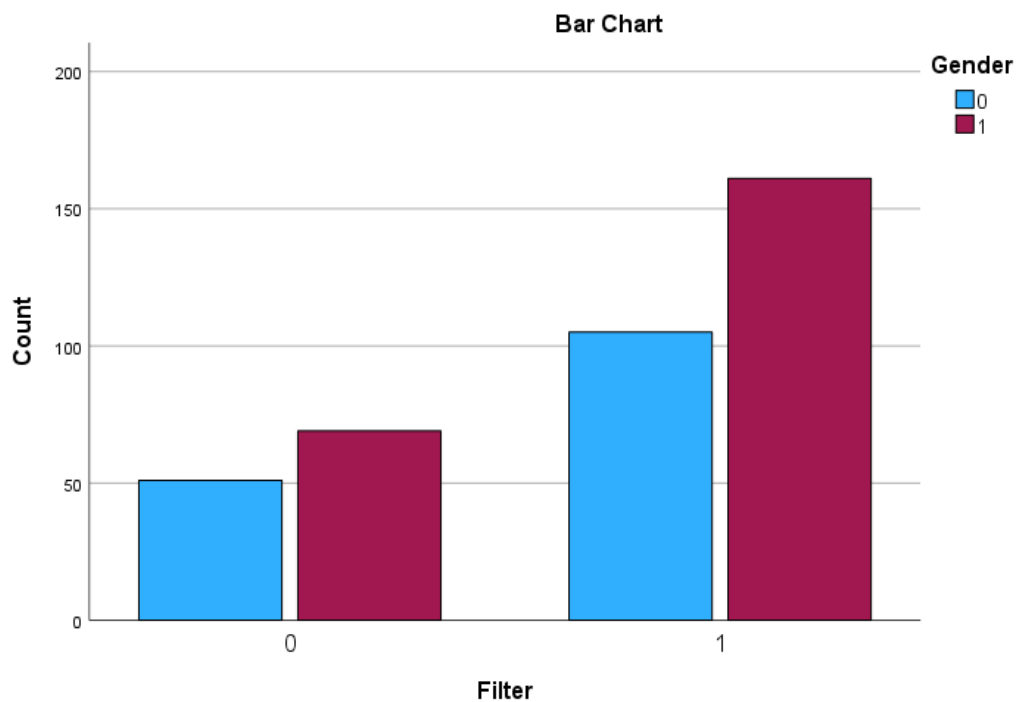
### Case Processing Summary

	Valid		Cases Missing		Total	
	N	Percent	N	Percent	N	Percent
Filer *	386	100.0%	0	0.0%	386	100.0%
Gender						

## Filter \* Gender Crosstabulation

Count

		Gender		Total
		0	1	
Filter	0	51	69	120
	1	105	161	266
Total		156	230	386



## Section 2: SPSS Output – Binary Logistic Regression

### Logistic Regression

#### Case Processing Summary

Unweighted Cases <sup>a</sup>		N	Percent
Selected Cases	Included in Analysis	386	100.0
	Missing Cases	0	.0
	Total	386	100.0
Unselected Cases		0	.0
Total		386	100.0



a. If weight is in effect, see classification table for the total number of cases.

**Dependent Variable Encoding**

Original Value	Internal Value
0	0
1	1

**Block 0: Beginning Block**

**Classification Table<sup>a,b</sup>**

Observed	Filter	Predicted		Percentage Correct
		0	1	
Step 0	0	0	120	.0
	1	0	266	100.0
Overall Percentage				68.9

- a. Constant is included in the model.
- b. The cut value is .500

**Variables in the Equation**

	B	S.E.	Wald	df	Sig.	Exp(B)
Step 0 Constant	.796	.110	52.397	1	<.001	2.217

**Variables not in the Equation**

	Score	df	Sig.
Step 0 Variables	A	8.547	1 .003
	SI	10.423	1 .001
	P	9.038	1 .003
	T	7.045	1 .008
	GI	4.312	1 .038
Overall Statistics	13.150	5	.022

**Block 1: Method = Enter**

**Omnibus Tests of Model Coefficients**

		Chi-square	df	Sig.
Step 1	Step	13.273	5	.021
	Block	13.273	5	.021
	Model	13.273	5	.021

**Model Summary**

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	465.216 <sup>a</sup>	.034	.048

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

**Hosmer and Lemeshow Test**

Step	Chi-square	df	Sig.
1	10.011	8	.264

**Contingency Table for Hosmer and Lemeshow Test**

		Filter = 0		Filter = 1		Total
		Observed	Expected	Observed	Expected	
Step 1	1	18	18.749	21	20.251	39
	2	14	15.268	25	23.732	39
	3	19	14.002	20	24.998	39
	4	14	13.095	25	25.905	39
	5	13	12.229	26	26.771	39
	6	15	12.611	28	30.389	43
	7	8	10.630	31	28.370	39
	8	6	9.677	33	29.323	39
	9	5	8.435	34	30.565	39
	10	8	5.303	23	25.697	31

**Classification Table<sup>a</sup>**

	Observed	Predicted		Percentage Correct
		Filter 0	Filter 1	
Step 1 Filter	0	4	116	3.3
	1	4	262	98.5
Overall Percentage				68.9

a. The cut value is .500

### Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
								Lower	Upper
Step 1 <sup>a</sup>	A	.194	.281	.474	1	.041	1.214	.699	2.107
	SI	.366	.328	1.247	1	.047	1.442	.758	2.742
	P	.216	.302	.510	1	.049	1.241	.686	2.242
	T	.165	.187	.781	1	.037	1.179	.818	1.700
	GI	-.108	.227	.228	1	.633	.897	.575	1.400
	Constant	-2.413	.939	6.608	1	.010	.090		

a. Variable(s) entered on step 1: A, SI, P, T, GI.