

## INTM30LON Dissertation

**Title:**  
**Influence of cyber-crime on E-commerce**

Name : Mohammad Hashtari  
Student ID : J13011909  
Supervisor : Dr. Sumitha A/P Ganesharatnam  
Word Count : 11,785

A research report submitted in partial fulfilment of the requirements for the degree of  
Master of Business Administration (Global Business)  
November 2018

## Acknowledgment:

This work wasn't possible without the priceless efforts and attentions of dear Dr. Sumitha Ganesharatnam, my supervisor, who patiently, guided and motivated me by her kind behaviour and immense knowledge in each step of this research.

My sincere thanks also goes to Dr. Dennis, Dr. Perbaharen, Dr. Poh, and Dr Shanmuga for all the indications and guidance which they've provided for me, sincerely, during my master program.

I would like to thank my dear family, specially my mother, father and my dear sister for all the supports that I've received to achieve my goals.

Last but not the least, I would like to thank my fellow classmates, for good teamwork and sleepless nights before each deadline, also I appreciate the time and efforts of the survey participants, this research wouldn't be completed without you guys.

## **Abstract:**

This paper is aimed at exploring the relationship between the known three beliefs related to online transaction (shopping, payment). The three beliefs are cyber-crime experience, perceived cybercrime and perceived ease of use towards online transactions. A sample of 207 respondents of Malaysian citizens was collected by using convenience sampling method, whereby the respondents had to be frequently internet users. A structured, adopted questionnaire was used to collect the responses from respondents. The findings indicate that cyber-crime experience ( $\beta = 0.303$  & P-Value = 0.013) and perceive ease of use ( $\beta = 0.317$  & P-Value =.047) have a significant and positive impact on user confident towards using online transactions, and user confident mediating the relationship between the mentioned constructs and behavioural avoidance intention. These findings indicate that perceived ease of use and cyber-crime experience are increasing the user confidence towards using online platforms. Age and gender were considered as moderating variables. 56.5% male and 43.5% female were the statistics of participants. The results of multigroup analysis on SmartPLS3 indicates that there is no major differences between the responses based on gender and age, basically their opinions toward the questionnaire were somehow align.

# Table of Contents

Acknowledgment:	2
Abstract:	3
1.0 Introduction	7
1.1 Research background	7
1.2 Problem statement	8
1.3 Research purpose and significant of study	9
1.4 Research question	9
1.5 Research objective	9
1.6 Structure of research	10
2.0 Literature review	11
2.1 Introduction	11
2.2 Theoretical Background	11
2.2.1 TAM Model	11
2.2.2 Review of Previous Studies on TAM Model	11
2.2.3 TAM literature reviews	12
2.2.4 Development and extension of the TAM model	13
2.2.5 Application and modification of TAM model	14
2.3 Potential Direction of Study	14
2.4 Framework of study	14
2.5 conceptual constructs	15
2.5.1 Perceived cyber-crime risk	15
2.5.2 Cyber-crime experience	17
2.5.3 Perceived ease of use	17
2.5.4 User confident	18
2.5.5 Behavioural avoidance intention	18
2.6 Concluding remark	20
3.0 Methodology	21

3.1 Overview.....	21
3.2 Research philosophy .....	21
3.3 Research approach .....	22
3.4 Research strategy.....	24
3.5 Research methodology and data collection .....	24
3.5.1 Data collection.....	24
3.6 Sampling method.....	25
3.7 Data management and analysis techniques .....	25
3.8 Research design.....	26
	27
3.8.1 Measurement of constructs.....	27
3.8.2 Research hypothesis.....	29
3.9 Research ethics .....	29
3.10 Reliability and validity .....	30
4.0 Research Analysis.....	31
4.1 Introduction.....	31
4.1.1 Demographic profile .....	31
<b>Statistics .....</b>	31
4.1.2 Perceived cybercrime risk (PCR) .....	32
4.1.3 Perceived ease of use.....	34
4.1.4 Cyber-Crime Experience.....	36
4.1.5 User confident.....	37
4.1.6 Behavioural avoidance intention .....	39
4.2 Analysis of research .....	40
4.2.1 Reliability and Validity test results .....	41
4.2.2 Reliability of individual items .....	41
4.2.3 Reliability and validity of constructs.....	43
4.2.4 Discriminant validity .....	44

4.2.5 HTMT .....	45
4.2.6 Multicollinearity for inner model.....	46
4.3 Analysis of the model.....	46
4.3.1 R square ( $R^2$ ) .....	47
4.3.2 Path coefficient.....	47
4.4 Multigroup analysis .....	49
4.5 Concluding remark.....	50
5.0 Overview .....	51
5.1 Concluding REMARK .....	51
5.2 Research's purpose.....	53
5.2.1 Government .....	54
5.2.2 Businesses.....	54
5.2.3 End users .....	54
5.2.4 Developer.....	54
5.3 Limitations of the study .....	55
5.4 Recommendations.....	55
5.5 future research direction .....	55
6.0 References .....	57
7.1 Questionnaire .....	63
7.2 Ethics approval checklist .....	71
7.3 Dissertation meeting diary .....	76

# CHAPTER 1 – INTRODUCTION

## 1.0 Introduction

### 1.1 Research background

This paper synthesize works from different fields to explain how cybercrime reduces online participation. By building a framework on Technology Acceptance Model (TAM), this paper is aiming to explain what factors influence the user's intention for using online services.

Since the first commercial use of computers, acceptance of new technology models was the centre of interest to maximize the using intention. Models have been introduced to measure the influence of different factors on individual intention to use a new technology. This paper is applying the acceptance model in context of general online services such as: Online banking, Online shopping, and Online social networking.

The Technology Acceptance Model (TAM) has been used in Information System's researches to examine and explain the level of acceptance of a wide range of new technology from applications, and operation systems, to online services. TAM model is based on the general theory of Reasoned Action (TRA) But has been modified to predict and explain the information technology acceptance.

The research done by Riek et al. (2016), has modified the TAM model to measure the influence of perceived cybercrime on online service avoidance. The paper hypothesize that the avoidance of online shopping, online banking and online social networking had increased due to cybercrime victimization. The effects are mediated by perceived risk of the cybercrime and moderated by user confident. The results of the research confirmed the negative effect of perceived risk on the use of all three mentioned categories, as well as supporting the role of cybercrime experience as a prior of perceived risk. The paper further shows that more level of confident users, perceived less cybercrime risks, and this group are more likely to participate on mentioned online categories, which highlights the importance of the user confidence. The research conducted by Riek and Bohme (2014) used the TAM model to understand the influence of cybercrime on e-services adoption in European internet

users. Considering that the real economic impact is hard to quantify, but its proven that cybercrime is wide, huge, and fast-growing problem. A part of cybercrime cost to society can be traced down to indirect opportunity costs, resulting from avoiding online services to unused online services. This paper presented a theoretically derived model which utilizes technology acceptance and spectrum from criminology to identify the factors that reduce the internet user's intention for using online services.

## 1.2 Problem statement

The global retail E-Commerce sales was estimated as \$1.67 trillion by 2015, an overall growth of 25% from 2015, and it is expected to grow to \$3.57 trillion (12.8%) in 2019. Asia Pacific is considered to be the fastest growing region by contribution more than 50% (\$877 billion) of global E-Commerce retail sales in 2015. The growth of E-commerce sales is expected to grow by 166% to become 2.33 trillion by 2019 (Tabassam et al. 2016).

The fear of online shopping and online transaction is affecting the potential revenue of E-commerce platforms significantly. The fear is driven mainly from bad experiences. Rick (2016) measured the influence of cybercrime on technology avoidance based on secondary data analysed by TAM (Technology acceptance model). Patrick (2015) studied the consumer's fear of online identity thefts based on secondary data.

The revolution of information technology united with leveraging of the internet, has provided considerable new and relatively open societies for the cybercriminal acts, and specifically in commercial business transactions (Smith 2004).

Over past decade the global E-commerce businesses have been growing at an average of 20% annually when compared to Bricks and mortar types. In developed countries the millennials generation are adopting the online purchasing rapidly (Howard 2018).

There is a loss of 9% annually due to customer's security concerns, and its estimated that roughly \$21 billion revenue is lost because of victims of identity thefts annually. Approximately 60% of the consumers believe that the Internet is not a safe place for shopping and online transactions (First Data Corporation 2009).

Report from CSIS (Centre for strategic and International study) estimated that the cost of cybercrime to the global economy is more than \$600 billion annually, better to say that its 0.08% of global GDP (Grobman et al. 2018).

According to global survey by Gemalto, exposure of customer data will have negative effects on the organizations and relationship with their customers (Clickatell 2018).

### 1.3 Research purpose and significant of study

E-commerce had seen a significant growth in terms of its contribution to Malaysia's economic growth. Ahmad Maslan said that the contribution of E-commerce to Malaysia's GDP increased to 6.1% (74.6 billion) in 2016 by comparing to 5.9% (68.3 billion) in 2015. Malaysian government had implemented the NESR (National E-commerce strategic plan) on October/2017 to ensure the continues growth. This plan is aiming to double the E-commerce growth from 10.8% in 2016 to 20.8% by 2020 (*NSTP Team 2018*). This study can be beneficial for online businesses that are targeting to maximize their online activities and increasing online transactions. In other words, it is beneficial for businesses that are transferring from the traditional brick and mortar to click and mortar, as well as the newly established companies that prefer the online platform as a suitable market place.

### 1.4 Research question

Cybercrime has resulted in technology avoidance which is the fear of online transactions among the users, and it reduces the intention of online participation (shopping, banking, and social networking) among the users, which affects the revenue of online platforms significantly. Online platforms must identify solutions to reduce the fear of online transactions among consumers so as to increase the retail volume and profitability of the platform.

This research is aimed at assessing the influence of the determinants on avoidance intention. As such, the research question for this study is as follow:

**To what extend do the determinants of online user avoidance, influence user confidence and behavioural avoidance intention?**

### 1.5 Research objective

The research objectives for this study are as follow:

1. To determine the level of influence perceived cyber risk, cybercrime experience, and perceived ease of use have on user-confidence and behavioural avoidance intention.

2. To identify the extent to which user confidence, which is the mediating variable, influences behavioural avoidance intention.
3. To determine whether demographic factors, such as age and gender, significantly moderate the association between the determinants of online avoidance, user confidence and behavioural avoidance intention.

As such, to sum it up, the objectives of this paper are set to identify the level of influence of the determinants of online avoidance on the user confidence and behavioural avoidance intention. This will help online providers determine the main issues that drive users away from online platforms.

## 1.6 Structure of research

This research paper is structured as below:

Chapter one provides information about the research background, problem statement, significance of study as well as research question and objectives.

Second chapter provides literature review as well as research framework.

The third chapter explains the research methodology, and philosophy. Here we will discuss areas relating to the research approach and strategy, sampling methods, data management and analysis techniques, research design and the hypotheses, research ethics and also the reliability and validity of the research.

The forth chapter includes the research analysis, comprising statistical and graphical analysis, using the SmartPLS 3 statistical software.

The last chapter contains the limitation of the study, recommendations, and future research directions.

# CHAPTER 2-LITERATURE REVIEW

## 2.0 Literature review

### 2.1 Introduction

This chapter provides a comprehensive overview of the past studies conducted in the area of cyber-crime and technology acceptance model. The first part presents a detail discussion about the background of this research and the previous studies. The second part is reviewing the previous studies on TAM model. There will be a discussion about the chosen variables which are influencing the outcome of the model. Research framework will be introduced in the forth. There will be a discussion about concluding remarks of this research for the last part. Also, the comprehensive framework will be discussed in chapter 3.

### 2.2 Theoretical Background

This paper is mainly prepared to provide a view of, to date and well researched sources from the past and current reference to TAM, as well as identifying possible direction for future researches. Technology acceptance model (TAM) is a model driven from information system theory which models how the end users agree to accept and use technologies. TAM model has been considered as a main model for studying the avoidance intention of the users toward new technology since 1989.

#### 2.2.1 TAM Model

TAM model provides a clear understanding of the variables which have impact on the decision making of the end users toward accepting or rejecting the technology. TAM model suggests that, while users are presented to new technology, there are a set of factors which influence their decisions about when and how they are willing to adopt and use the technology.

#### 2.2.2 Review of Previous Studies on TAM Model

According to several methodologies, more than 85 publications have been classified and selected research on TAM, relevant to their specific aim as well as their content, into three main categories (Lai 2017):

TAM literature reviews

Development and extension of the TAM model

Application and modification of TAM model

### 2.2.3 TAM literature reviews

By increasing the development of technology as well as its integration with user's private and privacy, and their professional life, there will be a decision left about acceptance or rejection of technology. There is a respectable amount of papers and researchers, who researched and work on topics which is dealing with technology acceptance model (TAM), since its first appearance in 1986, the model clearly demonstrates the importance as well as the popularity of the model in any field which is connected or related to technology (Hille et al. 2015) (figure 5).

The TAM or technology acceptance model is a theory related to information system, it models how users accept and use a new technology. TAM model suggests that, when users are presented for a new technology, a number of factors will influence their behaviour and decision toward how and when they use it (Richardson 2017). The fear of online shopping and online transaction is affecting the potential revenue of E-commerce platforms significantly. The fear is driven mainly from bad experiences. Technology avoidance is affecting the revenue of online platforms significantly (Lai 2017). Technology avoidance is resulting the fear of online transactions among the users, and it reduces the intention of online shopping among the users. Online platforms must identify solutions to reduce the fear on online transactions in order to increase the retail volume and profitability of the platform (Lai 2017).

TAM is originally from the psychological theory of reasoned action as well as theory of planned behaviour. TAM evolved for becoming the key model for understanding predators of human's behaviour toward potentially acceptance or rejection of the new technology (Richardson 2017).

TAM framework has been as a reference since 1989 (Devis et al. 1989), and many studies have used this framework to measure the influence of different variables on technology acceptance (Marangunić and Granić 2014). There are not many studies conducted to measure the influence of availability and user-interface on reducing the technology avoidance.

The research paper, "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance" (Riek et al. 2016), contained seven hypotheses. Five of the hypotheses are directly related to this research and two of the hypotheses are related to effects of media awareness on behavioural avoidance intention.

## 2.2.4 Development and extension of the TAM model

It's been studied and proven that the technology avoidance influences the online shopping intention among the users. Based on technology acceptance model (TAM), the main variables that influence the customer intention are shown in the figures below (figure 1). Riek et al. (2016) measured the influence of cybercrime on technology avoidance based on secondary data analysed by TAM (Technology acceptance model). On the paper (Riek et al. 2016), researchers identified seven factors which have influence on perceived cyber-crime risk. Financial, privacy, time, performance, overall, social and psychological risks. their paper amid to systematically explain the social effects of cyber-crime with factors that make users avoid online services. The analyse and finding of the research indicates that the perceived risks reduce the intention for users toward using online services.

The drawback of Rick's (2016) paper is that the concentration, is only on perceived risk and the two other dependent variables are not clearly differentiated. Other variables are perceived usefulness and perceived ease of use, which are different but really close to each other. The model developed by this author is shown in the Figure 1.

Figure 2: Perceived Risk extended TAM

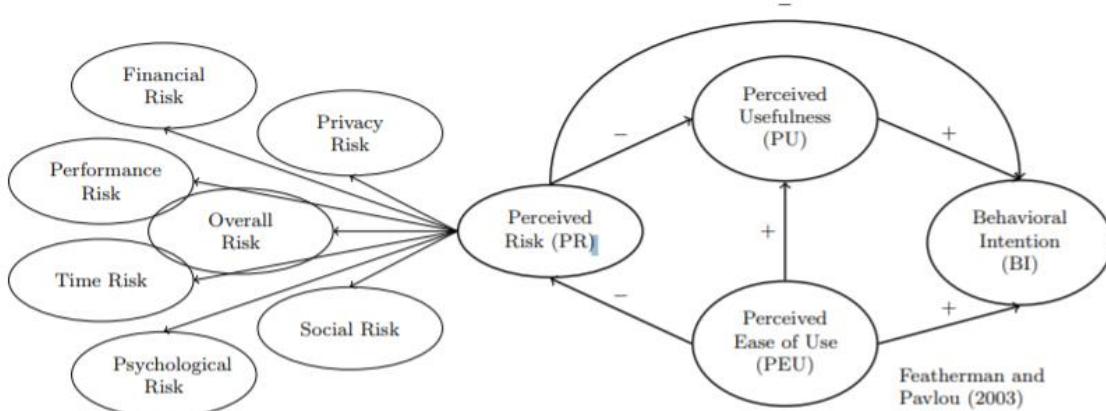
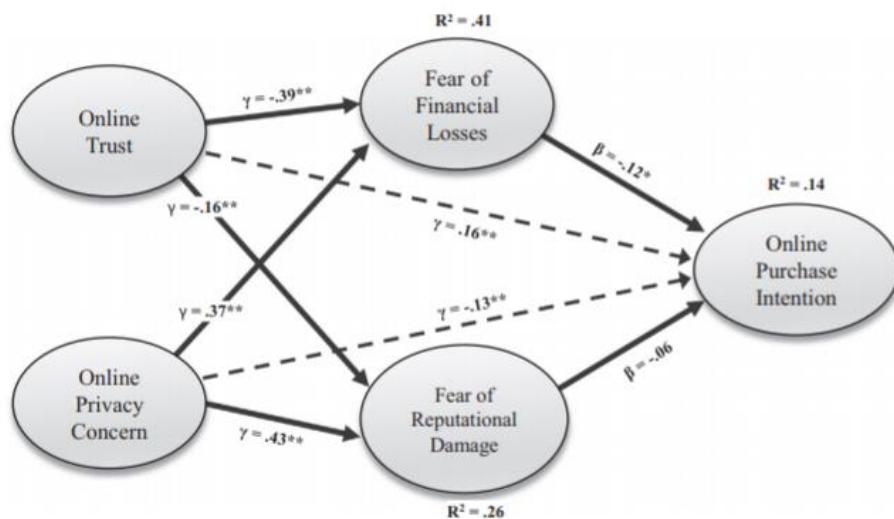


Figure 1  
Source (Rick 2014)  
Featherman&Pavlou framework

## 2.2.5 Application and modification of TAM model

Patrick (2015) studied the consumer's fear of online identity thefts based on secondary data. Patrick (2015) studied and measured the level of impact of financial loses and reputational damage as dependant variables towards online purchase intention as independent variable. He hypothesized that online trust and online privacy concern, have a straight effect on financial loses and reputational damage, which determine the level of user's intention for online purchases (Figure 2).

P. Hille et al. / Journal of Interactive Marketing 30 (2015) 1–19



Note: \*\*  $p < .01$ ; \*  $p < .05$ ; dashed lines represent non-hypothesized relationships examined in the mediation analysis.

Figure 2

Source (Patrick 2015)  
Patrick framework

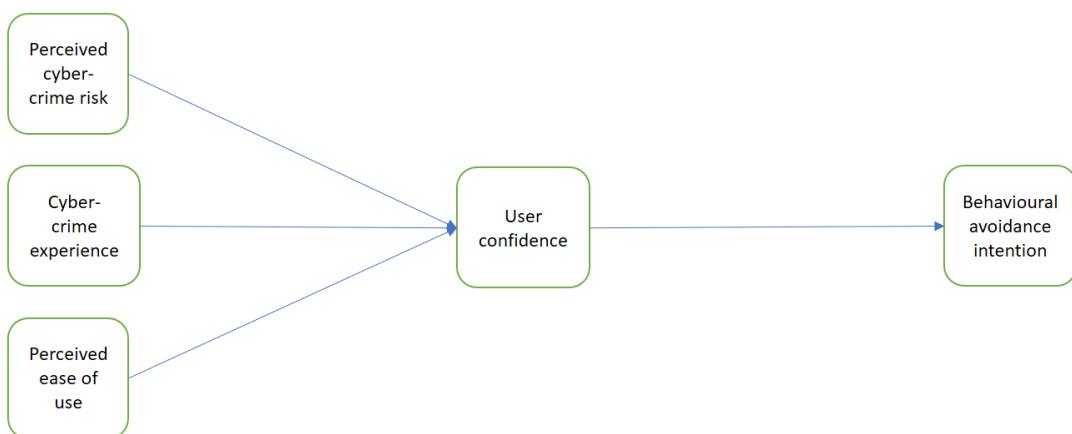
## 2.3 Potential Direction of Study

Regardless of a continuous process and progresses in revealing some new factors which have significant influence on the model core variables, still there are many undiscovered and unexplored area for TAM model potential applications which can contribute to the predictive validity of the model (Riek et al. 2016).

## 2.4 Framework of study

The discussion around the review of literature for this research will be carried out with reference to the constructs that are shown in the conceptual framework that has been developed for the purpose of this study (figure 2.3).

The conceptual framework proposed in this research (figure 2.3) is based on the TAM model proposed by Davis (1989), which is one of the most reliable frameworks and it has been the essential source for papers and researchers to study and determine the factors which are influencing the behavioural avoidance intention of users towards technology.



**Figure 2.3**  
**Study framework**

## 2.5 conceptual constructs

Based on the studies and researches discussed in the previous part, the chosen constructs for this research are: perceived cyber-crime, perceived ease of use, cyber-crime experience, user confidence, and behavioural avoidance intention.

### 2.5.1 Perceived cyber-crime risk

The influence and importance of perceived risk for commercial transactions was identified by Bauer in 1960s, he mentioned that shopping involves with risk always, and the reason drives this fact is that buyer's decisions have consequences that may be unpleasant and not easy to predict (Mortenson and Vidgen 2016). Spatial and sequential separation of consumers and retailers, also the open architecture of Internet increased the uncertainty, therefore the perceived risk is more concern in online shopping than traditional brick and mortar retailers (Mortenson and Vidgen

2016). Uncertainty can be categorized in two types, behavioural and environmental. Behavioural uncertainty is concerned with behaviour of dubious, mostly malicious merchants. Environmental uncertainty demonstrates general concern about the security of Internet as a channel for online transactions. Both factors increase the perceived risk (Riek et al. 2016).

Consequently, perceived risk is most likely is the reason for variance for the behavioural intention variable of TAM model, while applying it to online services (Pavlou and Featherman 2003). Pavlou and Featherman (2003) integrated perceived risk systematically into TAM model, by adding the perceived risk as the multidimensional construct (figure 4). Considering that Perceived risk reduces the intention towards E-commerce and E-services (behavioural avoidance intention) either directly or indirectly by reducing its perceived usefulness. The negative effects exist for initial (first time) and repeated usage of online services as well as it is larger for users with less experiences effecting user-confident. Perceived ease of use can reduce the negative effects of perceived cyber-crime by reducing the level of uncertainty and increasing the level of user's confidence for using online services (Marangunić and Granić 2014). Martins et al. (2014) confirmed the importance of perceived risk by integration of the UTAUT model with perceived risk theory, and their paper indicate a model which can explain 81% of the usage behaviour variance of 248 customers of online banking in Portugal.

Perceived cyber-crime risk is one of the constructs of this model (figure 2.3), which considered (based on the researches) to increase the avoidance intention between the users. The impact of perceived cyber-crime on avoidance intention is moderated by user confident in this framework.

Fig. 1. Perceived Risk-extended TAM

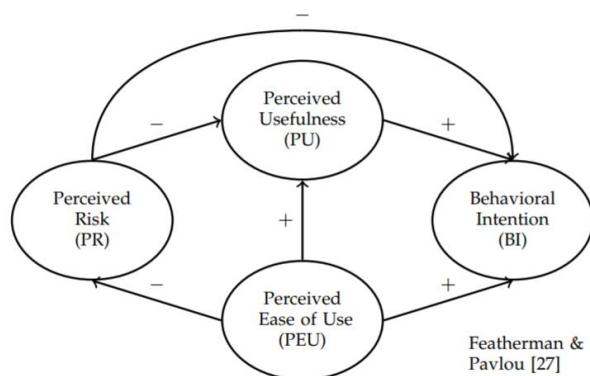


Figure 4  
Source (Featherman and Pavlou 2003)  
Extended TAM model

## 2.5.2 Cyber-crime experience

The research paper by Liébana-Cabanillas et al. (2015) has contributed to the field of satisfaction research of a perspective from electronic banking users. It's a comprehensive review of the scientific literature which is justified the development of the behavioural model which explained satisfaction by using a set of endogenous variables as well as the moderating effects of the experience. The analysis tested relationship between ease of access, trust, ease of use and usefulness. Examining individuals who were victims, as an antecedent of perceived cyber-crime shows mixed results. Mainly the scholars found strong relation and effects, but there are other scholars that found just weak or no effects at all. Rick (2014) state that the examination of the link between victim experience and perceived risk is not clearly conclusive yet. But perceived risk is considered to be the function of probability of becoming victim and the severity of criminal act. Many researchers suspect that experiencing the crime leads to an increase concern about it. Visser et al (2008) provided evidence of the effect based on two representative European survey conducted in 2006 and 2008.

Its stated by many authors that cyber-crime experience increases the avoidance intention of users for using the technology, by increasing the level of fear and uncertainty among the users. User confident is moderating the impact of this construct towards avoidance intention to determine to what extant does a confident user is willing to avoid the experience and use the technology (online services).

## 2.5.3 Perceived ease of use

Davis (1989), explained this as “the degree to which an individual believes using a specific system can be free from efforts”. Davis identified two distinct beliefs, which are perceived ease of use and perceived usefulness that are sufficient enough for predicting the attitude for user toward using the new technology. Davis (1989) with the associates additionally added that attitude doesn't fully mediate the perceived ease of use. Perceived ease of use has an influence on user's intention of online shopping. Researches have established that the perceived ease of use is an important element which influence the user behaviour and user acceptance of information technology. Venkatesh (2000), on his paper presented and examined anchoring as well as adjustment based theoretical model of determining the system

specific perceived ease of use. The model is proposing control, intrinsic motivation, as well as emotion as factors that identify the early perception about the ease of use (Martins et al. 2014).

Based on the findings and researches in previous section, perceived ease of use reduces the level of avoidance intention among the technology users, and user confident is moderating this relation to determine the level of its impact on the relation of dependant and independent variables.

#### 2.5.4 User confident

Studies have shown that the understanding of how different user segments evaluate and perceived online-services, and risk is the essential to explain the adoption. (Riek et al. 2016) suspects that, user's confident for handling the online transactions moderates the effect of perceived risk and influence the user awareness and user experience. The study hypothesizes that the amount of effects that user experience and user awareness have on perceived risk are smaller for more confident users, because they feel more secure about online behaviour and get less uncertainty (Riek et al. 2016). Perceived ease of use can mitigate the negative effect of perceived risk by reducing the level of uncertainty which lead to increase the level on user's intention toward new technology. Various authors stated that, understanding how different segments of customers perceived and evaluate the online services as well as risks is the main factor to explain their intention of adoption. Rick (2016) hypothesized that the effect of cyber-crime experience has on perceived cyber-crime is smaller for users who are more confident, as the confident user is feeling more secure towards the online behaviour and face less uncertainty. Also, more confident users perceive less cyber-crime and are less likely to avoid the usage of online services.

It stated in previous chapter from many authors, that more confident users face less uncertainty and are less likely to experience cyber-crime. In this framework user confident as a mediator is determining to what extant does this factor, reduces the negative effect of cyber-crime experience and perceived cyber-crime risk toward avoidance intention.

#### 2.5.5 Behavioural avoidance intention

- Behavioural avoidance intention

Avoidance intention is described as an individual stated evaluation of his/her intention to perform a certain action. Avoidance intention is a major factor which effect the decision making of individuals based on the definition of Hofstede's cultural dimensions. There are studies that prove the negative affect of avoidance intention on E-commerce platforms. In this study the dependent avoidance intention variable is measured by the level of influence of the independent variables. The review on criminological literature indicates that crime has a negative effect on social life, simply because it makes individual avoid situations and places, therefor studies on TAM model show the same negative impact of perceive risk towards the adoption of online services, which means it increases the avoidance intention. Rick (2016) believes that the impacts can be translated into the online context. Featherman and Pavlou (2003), stated that the financial risk and reputational risk (figure 1) are considered to be the most influential factors, their findings are aligned with the findings of Patrick (2015) research paper.

In this framework behavioural avoidance intention as independent is mediated by user confident from the impact of mentioned dependent variables to determine the level of avoidance intention among the participants of the questionnaire for this research.

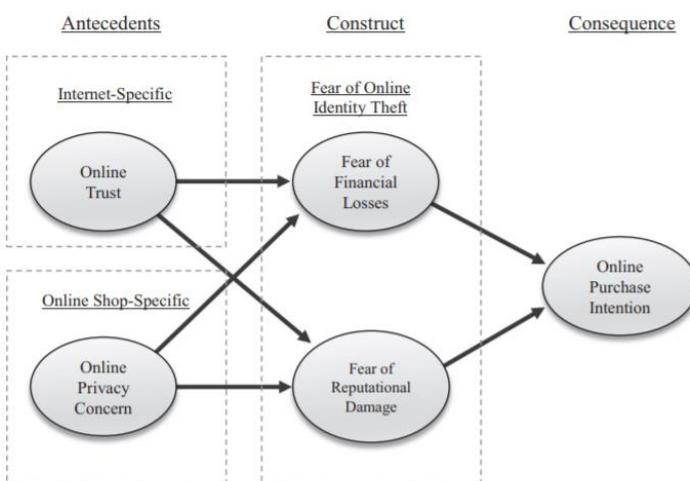


Fig. 1. A model of antecedents, dimensions, and consequences of FOIT.

Figure 5  
Source (Hille et al. 2015)  
Hille framework

The constructs in the above framework will be discussed in the subsequent sections, based on what other researchers have discovered.

## 2.6 Concluding remark

Based on the past studies discussed in these chapters, greater insights have been obtaining in the area of TAM or technology acceptance model. The constructs of the proposed framework have been varified by using the information from previuos researches and studies. Most of the studies, such as Riek et al. (2016) and Martins et al. (2014), have indicated that the proposed constructs of this paper have an impact on the users, whereby some of the papers found it as a significant impact, and some other papers such as Rick (2014) used mediating constructs to measure the level of effects.

# CHAPTER 3-RESEARCH METHODOLOGY

## 3.0 Methodology

### 3.1 Overview

This chapter contains the systematic methodology of this research. Research philosophy and research approach will be explained. There will be an explanation about the research strategy as well as research methodology. The sampling method will be clarified and data management along with analysis techniques will be identified and discussed. Measurement of constructs by using the software and research hypothesis will be explained. Research ethics will be identified and measuring the reliability/validity of the research will be explained. This research paper considers to be an applied research shown in the table (3.1), as it directly suggesting the solution to common business or management issues by direct relevance or implication to the managers in the field (Saunders et al. 2012).

FIGURE – NATURE OF RESEARCH	
Basic research	Applied research
<b>Purpose:</b> <ul style="list-style-type: none"><li>• Expand knowledge of processes of business and management</li><li>• Results in universal principles relating to the process and its relationship to outcomes</li><li>• Findings of significance and value to society in general</li></ul> <b>Context:</b> <ul style="list-style-type: none"><li>• Undertaken by people based in universities</li><li>• Choice of topic and objectives determined by the researcher</li><li>• Flexible time scales</li></ul>	<b>Purpose:</b> <ul style="list-style-type: none"><li>• Improve understanding of particular business or management problem</li><li>• Results in solution to problem</li><li>• New knowledge limited to problem</li><li>• Findings of practical relevance and value to manager(s) in organisation(s)</li></ul> <b>Context:</b> <ul style="list-style-type: none"><li>• Undertaken by people based in a variety of settings including organisations and universities</li><li>• Objectives negotiated with originator</li><li>• Tight time scales</li></ul>
<i>SOURCE: (SAUNDERS ET AL. 2012)</i>	

Table: 3.1

Nature of research

## 3.2 Research philosophy

“Philosophy is concerned with views about how the world works and it focuses primarily on reality, knowledge and existence. Our individual view of the world is

closely linked to what we perceive as reality" (Dudovskiy 2018). The below is the view of the author of how the cyber world works, with focus on the authors perception of what happens in reality.

The beliefs and philosophy which lead to this research paper is the fact that cyber-crime has huge and irreversible impact on a really fast-growing E-commerce. This paper is aiming to identify the factors that effecting the intention of users towards E-commerce platforms, and possibly suggest solutions to overcome the issues and increase E-commerce users.

There is a loss of 9% annually due to customer's security concerns, and its estimated that roughly \$21 billion revenue is lost annually because of victims' identity thefts. Approximately 60% of the consumers believe that the Internet is not a safe place for shopping and online transactions (*First Data Corporation* 2009).

E-commerce had seen a significant growth in terms of its contribution to Malaysia's economic growth. Ahmad Maslan said that E-commerce contribution to Malaysian GDP increased to 6.1% (74.6 billion) in 2016 by compared to 5.9% (68.3 billion) in 2015. Malaysian government had implemented the NESR (National E-commerce strategic plan) on October/2017 to ensure the continues growth. This plan is aiming to double the E-commerce growth from 10.8% in 2016 to 20.8% by 2020 (*NSTP Team* 2018).

Report from CSIS (Centre for strategic and International study) estimated that the cost of cybercrime to the global economy is more than \$600 billion annually; or better to say that it amounts to 0.08% of global GDP (Grobman et al. 2018). According to global survey by Gemalto, exposure of customer data will have negative effects on the organizations and relationship with their customers (Clickatell 2018).

The global retail E-Commerce sales was estimated at \$1.67 trillion by 2015, an overall growth of 25%, and it is expected to grow to \$3.57 trillion (12.8%) in 2019. Asia Pacific is considered to be the fastest growing region as this region has contributed more than 50% (\$877 billion in absolute terms) of global E-Commerce retail sales in 2015. The E-commerce sales is expected to grow by 166% to become \$2.33 trillion by 2019 (Tabassam et al. 2016).

The revolution of information technology united with leveraging of the internet, has provided considerable new and relatively open societies for the cybercriminal acts, specifically in commercial business transactions (Smith 2004).

### 3.3 Research approach

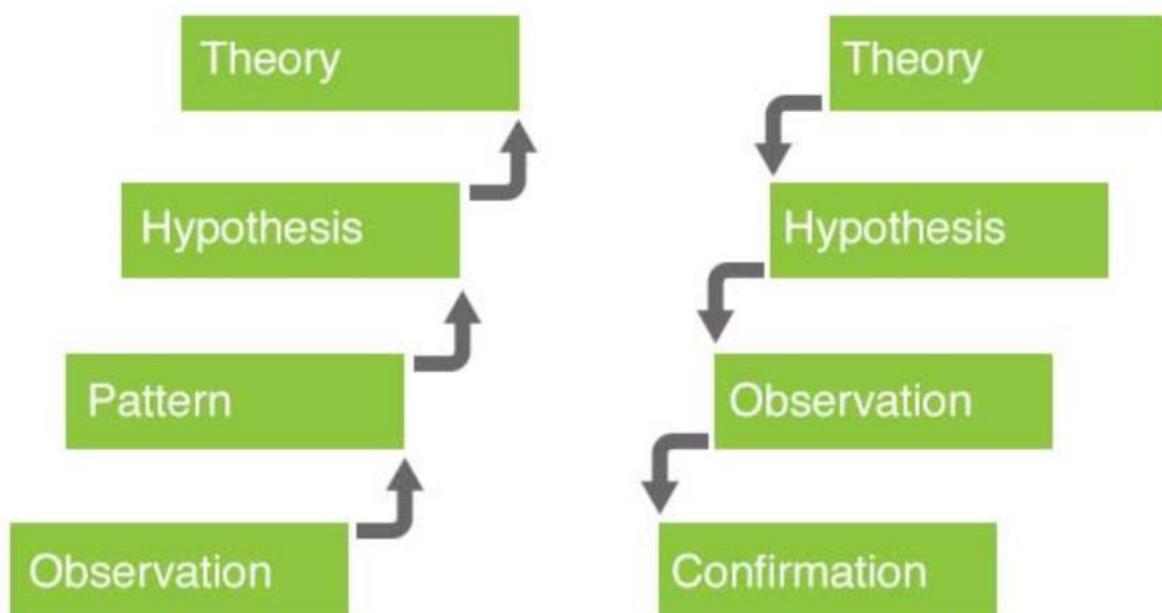
The research approach identifies and explains the method which is used for conducting the research (Cooper and Schindler 2007). Researches can be either conducted by following the inductive or deductive approaches (Saunders et al. 2012).

Inductive approach or inductive reasoning starts through observations as well as theories which are proposed towards the end of research processes. This method involves the research pattern from observation, followed by the development of explanations of the theories for that pattern by using a series of hypotheses (Dudovskiy 2016).

The deductive approach is concerned about developing the hypothesis which is based on an existing theory or theories. Subsequently, a research strategy for testing will be designed. It is known that deductive means reasoning from the particular to general (Dudovskiy 2016).

The deductive method shown in the figure (3.3), is used for this research. The research has been designed by using the TAM (Technology acceptance model), to measure the influence of cybercrime on E-commerce.

## Inductive Reasoning vs Deductive Reasoning



Source (Elmansy 2018)

Figure: 3.3

Research approach

### **3.4 Research strategy**

The research strategy is a step-by-step plan of some actions which provide direction to thoughts and efforts of the researchers, enabling the researchers to conduct the research systematically and on a schedule to produce detailed results with quality (Jenny 2014). Quantitative research, qualitative research and research by practitioners are well known as types of research strategy. The chosen method for this research is quantitative research due to time frame and time restriction as well as the importance of accessing a larger variety of respondents (Saunders et al. 2012)

### **3.5 Research methodology and data collection**

Research methodology has been defined as the processes of collecting information and data for the purpose of decision making by Business Dictionary. Methodology may include interviews, publications research, surveys as well as other research techniques, or may be included of both present and past collection of information (*Businessdictionary* 2018).

A consistence and systematic questionnaire was chosen for the purpose of collecting the information from respondents through Google online survey. The aim of this method was to reach to the maximum possible respondents in a restricted timeline. The collected information is considered as the primary data and has been collected straight from the targeted respondents which are the Internet users between the age of 21 to 50 and have a rush-life style in Malaysian society.

The collected information has been analysed by using the SmartPLS 3 software to measure the relationship between the variables as well as determinants. SmartPLS 3 also measure the reliability and validity of the collected information in order to produce the best possible analysed data to answer the hypotheses.

#### **3.5.1 Data collection**

The common classification of data is dividing the data based on the collection method to two major groups, known as primary data and secondary data. Primary data is considering to be collected by the researchers themselves for a specific purpose through data collection methods from the respondents. Secondary data is the data that has been collected by someone else for other purposes but being

utilized and used for other purposes by researchers (*Communitymedicine4asses* 2018).

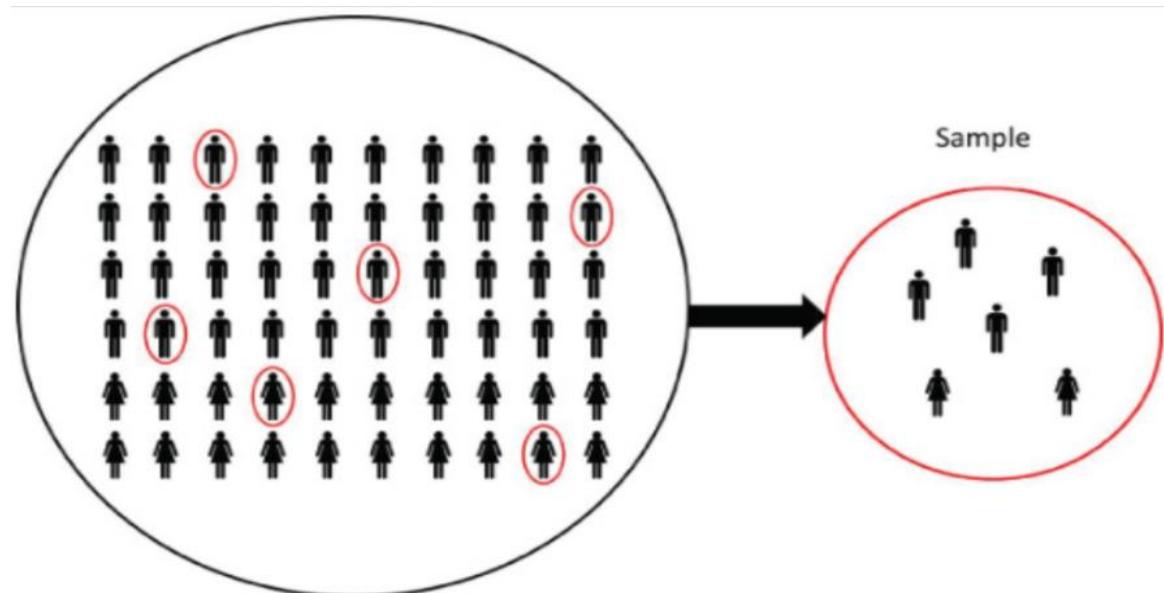
The advantages of using primary data are the fact that the data is being specifically collected for the purpose of the study, and it won't leave any doubt about the quality of the data. The possible disadvantage of the primary data is the process of collecting, managing and analysing the data (*Communitymedicine4asses* 2018).

The information collected for this study is a primary data which has been collected by the survey questionnaire from the respondents.

### 3.6 Sampling method

Research population is a set of large data collection of objects or individual which are the main concern and focus of the study. However due to the difficulties of reaching all the population, and the low possibility of testing every individual, researchers choose the sampling methods and techniques which reach to some part of the society randomly (Explorable.com 2009).

The sampling method (figure 3.6), in this paper was through survey questionnaire from randomly chosen respondents who are Internet users in Malaysia.



Source (Explorable.com 2009)

Figure: 3.6

Sampling method

### 3.7 Data management and analysis techniques

In this research data will be analysed via the SmartPLS 3 software. This research is based on survey questionnaire which was collected from Internet users of the Malaysian society. The primary data collected information will be the input for the SmartPLS 3 software to make sure the high accuracy of the outcome.

### 3.8 Research design

Research design refers to overall strategy which the researcher chooses to integrate the different components of research in a logical way and coherent manner in order to ensure that the study effectively address the problems identified in research (*De Vaus 2013*).

This research contains the determinants of online user avoidance (Independent variables) as Perceived cyber-crime, Perceive ease of use, and Cyber-crime experience. The User confident as the Mediating variables, and Behavioural avoidance intention to be studied as the dependent variable.

The variables of this research paper are shown in the figure 3.8.1. The above framework has been developed based on the literature review, and TAM framework (Davis 1989), and its aiming to achieve each objective that is covered in this research.

There are three identified variables in order to test the hypothesis of this research. Perceived cyber-crime risk, perceived ease of use and cyber-crime experience which are mediated by user confident to determine to which extant do the independent variables affect the behavioural avoidance intention as a dependant variable.

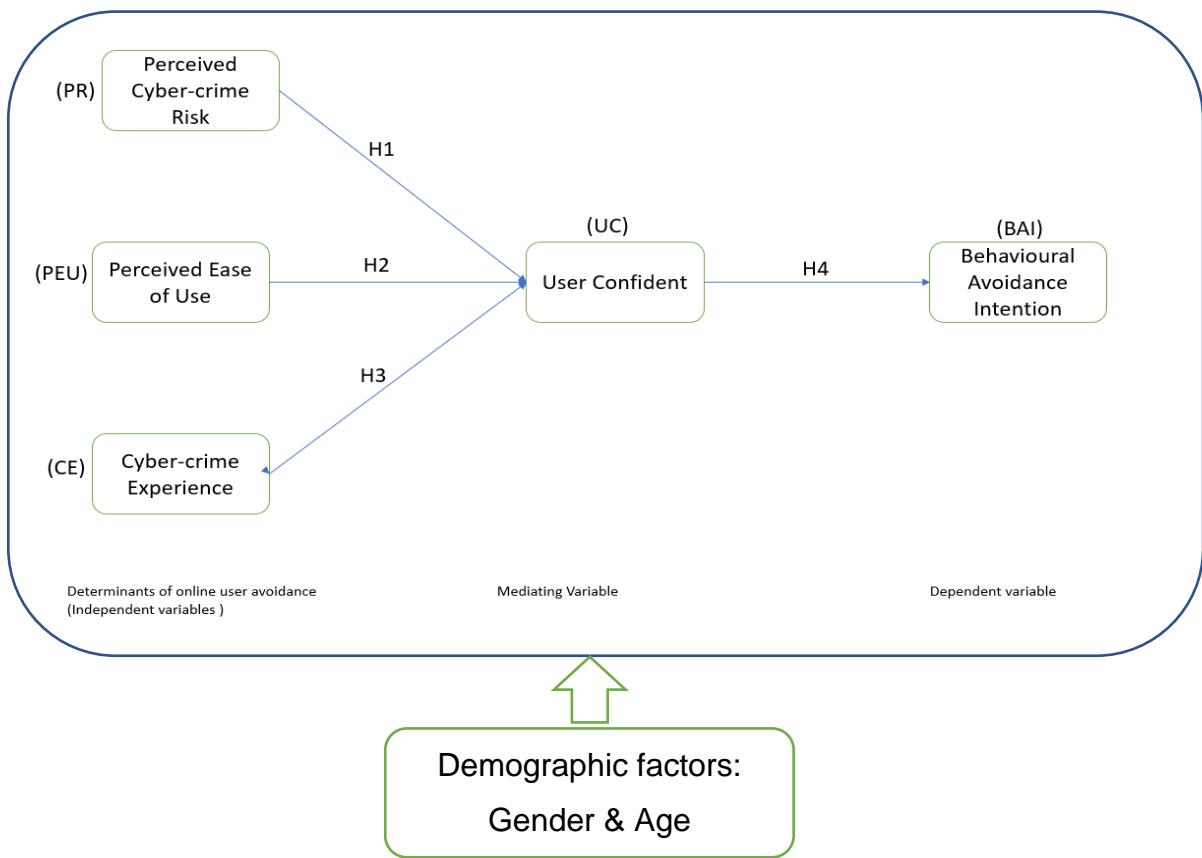


Figure 3.8

Study framework2

### 3.8.1 Measurement of constructs

Researchers use this section to determine how they are going to measure certain concepts of understanding from the respondents. This measurement may provide random results from various respondents, the results are eventually used to perform statistics analysis. Researchers are only allowed to question the respondents on the concept of understanding, but also, they may narrow down to characteristics and demography details which may enhance the research with better results.

Construct	Questions		Referenced from
Perceived ease of use (PEU)	PEU1	I agree that online shopping and web-based online transactions save my time.	(Riek et al. 2016) (B'ohme et al. 2014)
	PEU2	I agree that interaction through web pages is clear and understandable.	(Riek et al. 2016) (B'ohme et al. 2014)
	PEU3	I agree that online shopping and web-based online transactions save cost.	(Riek et al. 2016) (B'ohme et al. 2014)
	PEU4	I agree that it is easy to become skilful at navigating the web pages.	(Riek et al. 2016) (B'ohme et al. 2014)
	PEU5	I agree that online shopping and web-based online transactions are much more convenient.	(Riek et al. 2016) (B'ohme et al. 2014)
	PEU6	I agree that online shopping and web-based online transactions provide more variety of options.	(Riek et al. 2016) (B'ohme et al. 2014)
Perceived cyber-crime risk (PCR)	PCR1	I am personally concerned about becoming a victim of Identity Theft. (using another person's name and personal information)	(Riek et al. 2016) (B'ohme et al. 2014)
	PCR2	I am personally concerned about becoming a victim of Spam E-mails. (unsolicited messages sent in bulk by email)	(Riek et al. 2016) (B'ohme et al. 2014)
	PCR3	I am personally concerned about becoming a victim of Online Fraud? (fraud that is committed with the help of the internet)	(Riek et al. 2016) (B'ohme et al. 2014)
	PCR4	I am personally concerned about becoming a victim of "Content of Racial Hatred" (Incitement to racial or ethnic issues)	(Riek et al. 2016) (B'ohme et al. 2014)
	PCR5	I am personally concerned about becoming a victim of Unavailable Content (The Website's Server Not Available)	(Riek et al. 2016) (B'ohme et al. 2014)
Cyber-crime experience (CE)	CE1	I have experienced or been a victim of Identity Theft	(Riek et al. 2016)
	CE2	I have experienced or been a victim of Spam E Mail	(Riek et al. 2016)
	CE3	I have experienced or been a victim of Identity Illegal Content	(Riek et al. 2016)
	CE4	I have experienced or been a victim of Unavailable Content	(Riek et al. 2016)
	CE5	I have experienced or been a victim of Online Fraud	(Riek et al. 2016)
User confident (UC)	UC2	I'm confident that the information that I have provided on internet won't be used for other purposes.	(Riek et al. 2016) (B'ohme et al. 2014)
	UC3	In general, the Internet is now a safe environment in which I can confidently transact business.	(Riek et al. 2016) (B'ohme et al. 2014)
	UC4	I feel assured that legal and technical structures adequately protect me from problems on the internet.	(Riek et al. 2016)
	UC5	The Internet has enough safeguard measures to make me feel comfortable using it to transact personal business.	(Riek et al. 2016)
Behavioural avoidance intention (BAI)	BAI2	Due to Cyber-Crime I'm less likely to do Online Shopping.	(Riek et al. 2016) (B'ohme et al. 2014)
	BAI3	Due to Cyber-Crime I'm less likely to Publish Personal Information Online.	(Riek et al. 2016) (B'ohme et al. 2014)

Table 3.8.1

Measurement of constructs

### 3.8.2 Research hypothesis

The hypotheses of this study will be shown in the table 3.8.2 based on the conceptual framework. It allows proper indication and connectivity of the dependent and independent variables. Hypothesis is identified as the formal proclamations that state the possible relationship between and independent and dependent variables (Creswell 2003).

	<b>Hypothesis</b>
H1	Perceived cyber-crime risk has a negative effect on user confident.
H2	Perceived ease of use has a positive effect on user confident.
H3	Cyber-crime experience has a negative effect on user confident.
H4	User confident mediates the relationship between the dependent and independent variables.

Table 3.8.2

Hypothesis

### 3.9 Research ethics

Researches which involve with human subjects, raise complex and unique legal, social, ethical and political issues. Ethics in research are specifically interested in the analysis of ethical issues which are raised when human is involved as participant in a research (Saunders et al. 2012). As Bryman and Bell (2007) mentioned, there is a growing pressure on management researchers as well as professional associations to develop ethical codes. The ethical codes are required to address the issues and keep the research methods ethical.

### 3.10 Reliability and validity

Reliability is the consistency of a measure. There are three types of consistency according to psychologist, comprising over time, across items, and across different researches (Price et al. 2015). The targeted population for this study is the Malaysian citizens, age 21 to 50 which are consistently Internet users.

Validity is the extent to which the results of a measure is representing the variable they intent to be (Price et al. 2015). The method of this research (Online questionnaire and the time frame for collecting the responds), shows the fact that the respondents are consistently using Internet for many purposes on a daily schedule. The reliability and validity of the indicators within each of the construct will be statistically teste by using SmartPLS3 and the results will be presented statically as well as graphically in research analysis chapter.

# CHAPTER 4 – RESEARCH ANALYSIS

## 4.0 Research Analysis

### 4.1 Introduction

Chapter four discusses the outcomes of the data analysis, on the data collected through the questionnaire survey that was distributed to Malaysians.

#### 4.1.1 Demographic profile

The initial section of questionnaire comprises of a series of closed-ended questions, targeted at identifying the overall respondents' demographic characteristics, such as gender, age, education status, and income.

Item	Subgroup	Statistics	
		Percentage Participant	Number of participants
Gender	Male	56.5%	117
	Female	43.5%	90
Age	21 and below	1.9%	4
	22 to 30	50.3%	104
	31 to 40	26.6%	55
	41 to 50	15.5%	32
	More than 50	5.8%	12
Education	Secondary/High school	6.3%	13
	Diploma	8.2%	17
	Degree	42.5%	88
	Postgraduate	33.8%	70
	Professional courses	8.7%	18
	Others	0.5%	1
Income	Below 2500	24.2%	50
	2501 to 5000	29%	60
	5001 to 7500	17.9%	37
	7501 to 10000	14%	29
	Above 10000	15%	31

Table 4.1.1

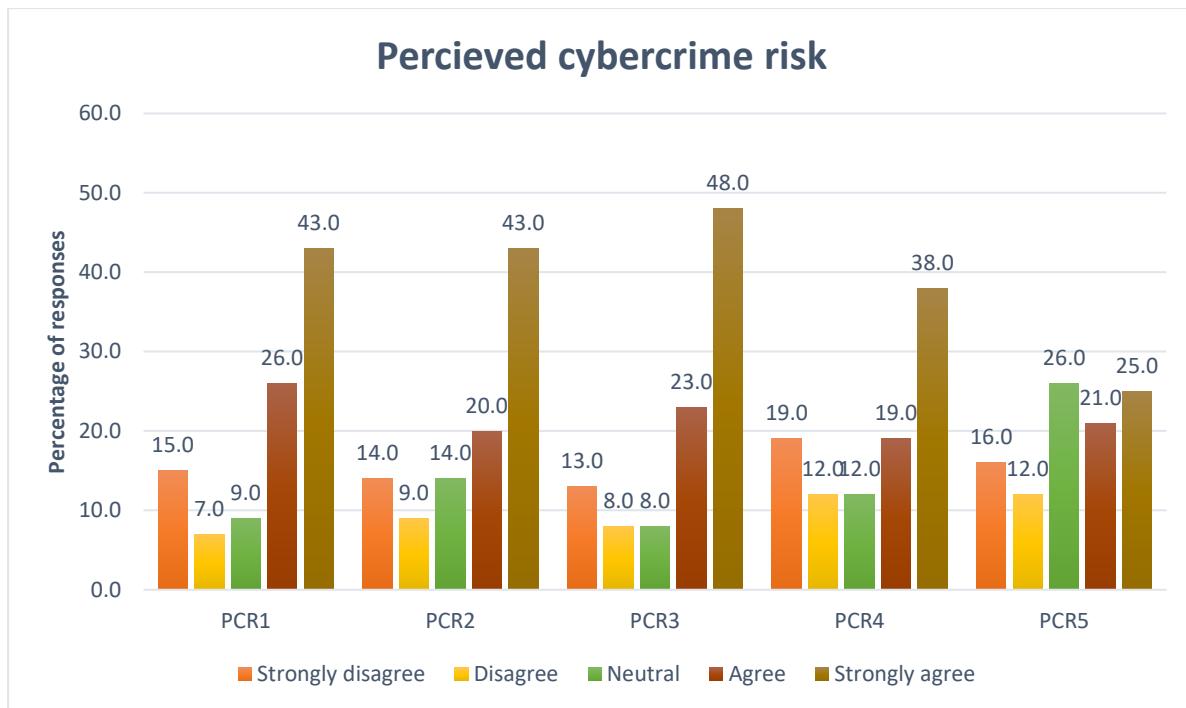
Demography table

The table 4.1.1 demonstrate the demography statistics of this research. Approximately 56.5% male and 43.5% female participated in the research survey. The statistics of age indicates that the majority of participants are in middle ages, which was the main consideration for this research due to the fact that the middle age population are considered to be the main users for E-commerce platforms. The statistics gathered from education section shows that 85% of the participants are highly educated. This fact indicates that mainly the participants had the minimum required knowledge for internet usage and online platforms. 71% of participants are in the middle to lower income category. Middle to lower income category are more attracted to purchasing products with discounts, which is widely available on E-commerce platforms (Planet Retail and NetSuite 2016).

The subsequent sections below present the findings of the constructs based on the conceptual framework of this research. The five-point-likert scale responses was used to measure the individual dimensions of the constructs, whereby "1" for "strongly disagree", "2" for "disagree", "3" for "neutral", "4" for "agree" and "5" for "strongly agree".

#### 4.1.2 Perceived cybercrime risk (PCR)

There are five dimensions of PCR, Becoming victim of identity theft, spam emails, online fraud, content of racial hatred, unavailable content. These dimensions are the determinants of perceived cyber-crime.



PCR graph

Graph 4.1.2

Indicator	Measure	Mean value	Standard division
PCR1	I am personally concerned about becoming a victim of Identity Theft? (using another person's name and personal information)	3.7500	1.45210
PCR2	I am personally concerned about becoming a victim of Spam E-mails? (unsolicited messages sent in bulk by email)	3.6900	1.45432
PCR3	I am personally concerned about becoming a victim of Online Fraud? (fraud that is committed with the help of the internet)	3.8500	1.43208
PCR4	I am personally concerned about becoming a victim of "Content of Racial Hatred" (Incitement to racial or ethnic issues)	3.4500	1.55294
PCR5	I am personally concerned about becoming a victim of Unavailable Content (The Website's Server Not Available)	3.2700	1.38429

PCR table

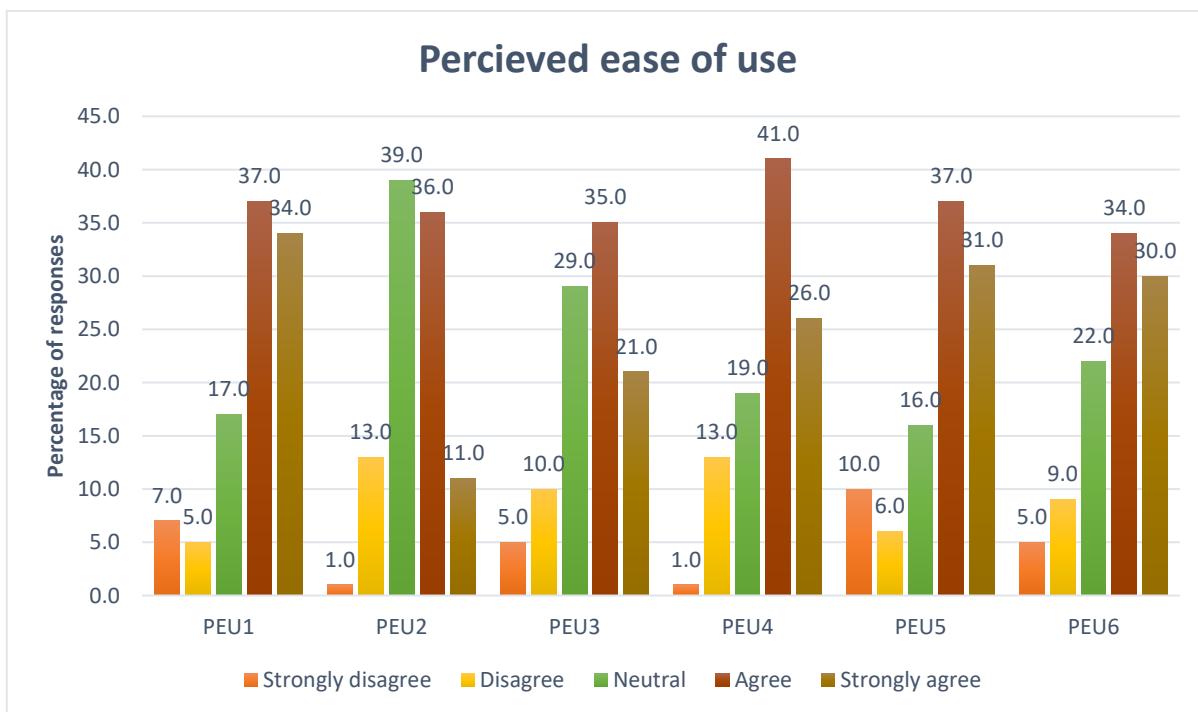
Table 4.1.2

The graph and table above indicate that mainly the participants are concerned about becoming a victim of cybercrime. In the case of PCR3 nearly half of the participants are aware and conscious about online fraud, which consider to be one of the most popular methods in cybercrime. 76% of the participants are aware and concerned about becoming a victim of unavailable content, unavailable content affects the reputation of E-commerce platforms and reduce the level of trust by users towards online platforms. The mean values here are between 3.2 and 3.8, indicating that the responses tend to agree with the questions asked.

The standard deviation indicates the distribution around the mean. A low standard deviation shows a narrow range between the low and high scores, while a high standard deviation indicates a wider range. For example, a standard deviation of 0 indicates that there is no difference in the scores given. Alternatively, a standard deviation that is further away from 0, shows a wider spread of the range of values.

#### 4.1.3 Perceived ease of use

There are six dimensions of PEU, time saving, clarity of user interface, saving cost, ease of navigation, convenience, access to variety of options. These dimensions are the determinants of perceived ease of use.



PEU graph  
Graph 4.1.3

<b>Indicator</b>	<b>Measure</b>	<b>Mean value</b>	<b>Standard division</b>
<b>PEU1</b>	I agree that online shopping and web-based online transactions save my time.	3.8600	1.15488
<b>PEU2</b>	I agree that interaction through web pages is clear and understandable.	3.4300	0.89052
<b>PEU3</b>	I agree that online shopping and web-based online transactions save cost.	3.5700	1.08484
<b>PEU4</b>	I agree that it is easy to become skilful at navigating the web pages.	3.7800	1.01085
<b>PEU5</b>	I agree that online shopping and web-based online transactions are much more convenient.	3.7300	1.24604
<b>PEU6</b>	I agree that online shopping and web-based online transactions provide more variety of options.	3.7500	1.13150

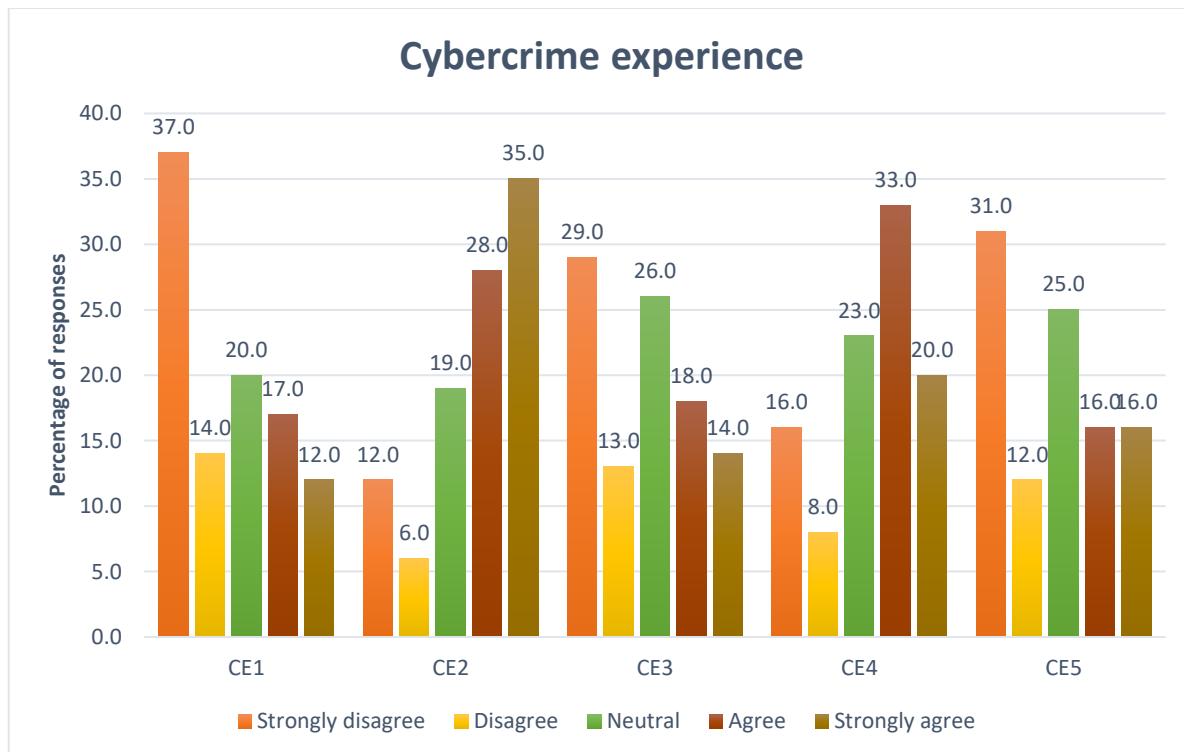
PEU table  
Table 4.1.3

PEU1 indicates that the majority of respondents agreed with time saving factor of online shopping regardless of cybercrime possibility. This can be explained based on the demography factor of the survey which shows mainly the participants are in middle age with rushing lifestyle. For PEU2, the responses are mainly neutral towards being agree, which means the current UI (user interface) of the online platforms is understandable but not good. Basically, there is no standardized or united UI, and each platform is designing or designed according to their capabilities and preference. The PEU3 indicates that the majority of respondents value the time, which can be explained by demography. PUE4 shows that the online platforms provided an acceptable experience for users, but there is a room for improvement. PEU5 indicates that most of the participants are satisfied with online platforms and delivery systems, but this doesn't necessarily mean that the online platforms provided a proper business processes, because the rushing lifestyle of the participants may force them to use online platforms instead of physical shops. Perhaps online platforms can provide access to more variety of options for users, but in the case of PEU6, the neutral responses are actually high as well, which may be

roots in the fact that the online platforms can't provide a tangible goods or services for users. The mean values here are skewed towards agree as they are between 3.4 and 3.8, and it indicates that the responses are agree towards strongly agree.

#### 4.1.4 Cyber-Crime Experience

There are five dimensions of CE, becoming victim of Identity theft, spam emails, illegal content, unavailable content, online fraud. These dimensions are the determinants of cybercrime experience.



CE graph  
Graph 4.1.4

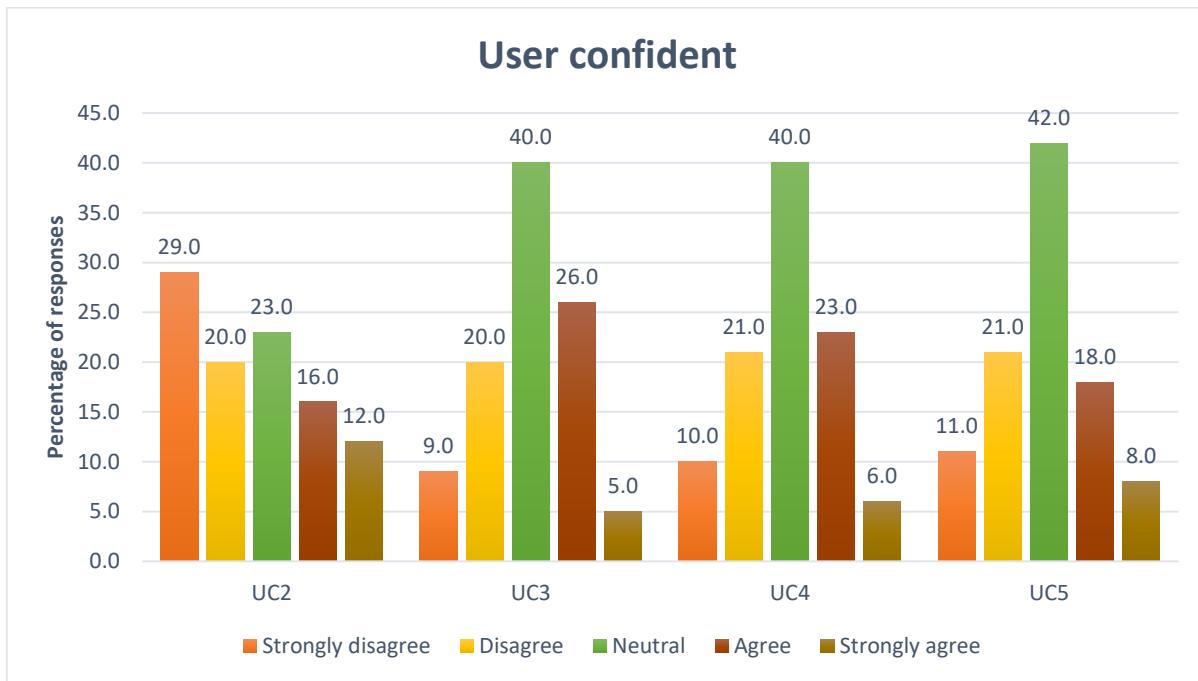
<b>Indicator</b>	<b>Measure</b>	<b>Mean value</b>	<b>Standard division</b>
<b>CE1</b>	I have experienced or been a victim of Identity Theft	2.5300	1.43868
<b>CE2</b>	I have experienced or been a victim of Spam E Mail	3.6800	1.33242
<b>CE3</b>	I have experienced or been a victim of Identity Illegal Content	2.7500	1.40974
<b>CE4</b>	I have experienced or been a victim of Unavailable Content	3.3300	1.32615
<b>CE5</b>	I have experienced or been a victim of Online Fraud	2.7400	1.45380

CE table  
Table 4.1.4

CE1 results indicates that mainly the participants are aware of identity theft and they are conscious about personal information. Spam emails is one of the most popular methods and the results of CE2 indicates the fact that most of the participants have experience of it. CE3 with majority towards strongly disagree response, shows that most of the responses are not aware or not considering the illigal content, as well as they may jot compromise by avoiding it. Unavailable contant (Fake websites, URL, servers) is maily affecting the users trust towards the online platforms, the results of CE4 indicates that the majority of respondents have experienced this issue, this factor must be considered in order to gain the trust of users. The CE5 results indicate that most of the participants had no experience of online fraud, which can be explained by the level of control and monitoring on the online platforms by Malaysian authorities, and the proccess of control and monitoring results in a better experience for users as well as gaining the trust of them towards online platforms. The mean values here a skewed towards agree as they are between 2.5 and 3.6, which indicates that the responses are neutral towards strongly agree.

#### 4.1.5 User confident

There are five dimensions of UC, being concerned about tracking, confidential, transaction trust, technical structure, comfort. These dimensions are the determinants of user confident.



UC graph  
Graph 4.1.5

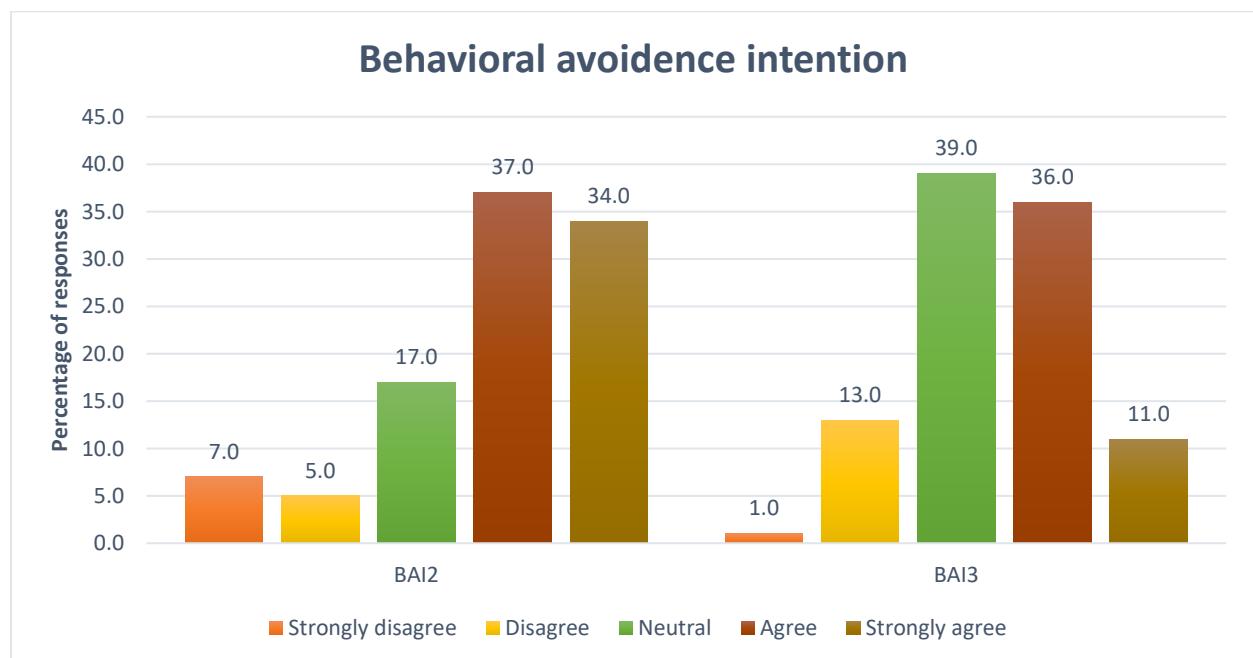
Indicator	Measure	Mean value	Standard division
UC2	I'm confident that the information that I have provided on internet won't be used for other purposes.	2.6200	1.36907
UC3	In general, the Internet is now a safe environment in which I can confidently transact business.	2.9800	1.01484
UC4	I feel assured that legal and technical structures adequately protect me from problems on the internet.	2.9400	1.04272
UC5	The Internet has enough safeguard measures to make me feel comfortable using it to transact personal business.	2.9100	1.07398

UC table  
Table 4.1.5

Based on the results of responses gathered for this section, it's easy to say that the majority of participants have no confidence in using the online platforms, and generally they don't trust the processes and transactions. The majority of responses for UC2, indicates that the participants are aware of the fact that most of the online platforms are using the users' information as a marketing tool. The results of UC3 which is mainly neutral (towards agree), indicate that the participants don't trust the online platforms, and they may use the online transaction based on the forces from rushing lifestyle. UC4's results show the fact that mainly the participants don't feel the necessary security processes while using online platforms or doing online transactions. The results of UC5, emphasize on the findings of UC4, and by mainly responses towards neutral, it shows that the users still have no confidence while using online platforms. The mean values here are skewed towards agree as they are between 2.6 and 2.9, which indicates that the responses are neutral towards agree.

#### 4.1.6 Behavioural avoidance intention

There are three dimensions of BAI, less likely to do online banking, online shopping, publish personal information. These dimensions are the determinants of behavioural avoidance intention.



BAI graph  
Graph 4.1.6

Indicator	Measure	Mean value	Standard division
BAI2	Due to Cyber-Crime I'm less likely to do Online Shopping.	2.7300	1.16216
BAI3	Due to Cyber-Crime I'm less likely to Publish Personal Information Online.	3.2800	1.23157

BAI table  
Table 4.1.6

BAI2's results clearly indicate the fact that the majority of participants are aware of cybercrime and don't really trust the platforms, which leads to less participation of online transactions. The results of BAI3 shows that the majority of participants are not feeling safe as mentioned before but due to other reasons they may share their personal information online. One of the main reason for sharing personal information is the fact that most of the platforms collect user's information in order to open an account for them, which is necessary, because there must be a real identity behind the virtual identity. The mean values here are skewed towards agree as they are between 2.7 and 3.2, which indicates that the responses are neutral towards agree.

## 4.2 Analysis of research

SmartPLS3 is a milestone for latent variable modelling, which combines methods (PLS, POS, IPMA, Bootstrapping) with an easy to use user interface. Partial least squares path modelling or better known as PLS-SEM is a method of the structural equation modelling, that allows estimating complex cause-effect relationship models with latent variables. PLS-SEM considered to be a component-based estimation method. PLS enables the users to analyse the gathered data and provide findings regardless of the sample size and it imposes minimum restriction in order to provide a better service for users (Hair et al. 2017).

Researchers must follow the two-step approach in analysing the research model in order to provide a better outcome. Outer model which is known as measurement model analysis, and inner model as structural model analysis.

- Outer model:

Outer model is the part of the model which explain and describe the relationship between the latent variables and their indicators.

- Inner model:

Inner model is a part of the model that explain and describe the relationship between the latent variables which made the model.

Path coefficients are the inner model parameters estimate, while the weight and loading are the outer model parameters estimate. Inner and outer models are also known as structural and measurement models respectively. The mathematical equations which describe the relationship between latent variables are known as the structural model, and the equations which describe the relationship between latent variables and indicators are known as measurement model. Structural equation model is the term which refer to both methods (Hair et al. 2017).

#### 4.2.1 Reliability and Validity test results

- Reliability test contains: loading, R-square ( $R^2$ ), Composite reliability

The loading test determines the degree of relationship between the indicators. The dimension of construct must be unique and different from each other even though it reflects a portion of another construct. There are a few different ways for evaluating discriminant validity (Hair et al. 2017). Average variance extracted or (AVE) considered to be a common method for testing discriminant validity. Discriminant validity is evaluated by testing the cross loading of each item in the construct and square root ( $R^2$ ) of AVE calculated for constructs (Hair et al. 2017). Composite reliability determines to which extent do a set of construct indicators share in the measurement of a construct (Hair et al. 2017).

- Validity test contains: AVE, Discriminant validity

The discriminant validity assessment is for the purpose of ensuring that the reflective construct has the possibly strongest relationship with its own indicator (Hair et al. 2017). On other hand the average variance extracted, or AVE considered to be the measure of amount of variance which is captured by the construct in relation to the amount of variance, because of measurement errors (Valentini and Damásio 2016).

#### 4.2.2 Reliability of individual items

The result of loading must be more than 0.70 in order to fulfil the satisfactory level of individual items reliability criteria (Rahn 2018). The cut-off value is 0.70 for loading significance, which is confirming the validity of the constructs. But the most important value is AVE (Average Variance Extracted), then in any case, if the loading result is less than 0.70, and the AVE result is more than 0.5, is recommended to keep the variable. If AVE is more than 0.5, then you won't need to look at the loading, mentioned by Hair et al. (2017).

Items	Indicators	Loading
PCR	PCR1	0.740
	PCR2	0.782
	PCR3	0.797
	PCR4	0.692*
	PCR5	0.918
PEU	PEU1	0.847
	PEU2	0.831
	PEU3	0.839
	PEU4	0.722
	PEU5	0.862
	PEU6	0.786
UC	UC2	0.707
	UC3	0.905
	UC4	0.874
	UC5	0.888
CE	CE3	0.904
	CE4	0.468*
	CE5	0.907

Reliability of individual items

Table 4.2.2

Note: \* indicate the loading value <0.7

The loadings that are less than 0.7 at the table above are maintained, as the value of the AVE for those loadings are more than 5.

#### 4.2.3 Reliability and validity of constructs

Cronbach's Alpha (minimum 0.7), Composite reliability (minimum 0.7), AVE (minimum 0.5) are the targeted values.

For the reliability analysis, Cronbach's alpha coefficient for assessing the inter item consistency of the measurement items. The accepted values are 0.7 and above, but, there won't be anything to worry about in a case that the value is less than 0.7, because Cronbach alpha is assuming that all the indicators have the same level of influence on the broad construct, but it's not the case all the times.

For composite reliability (CR), AVE is a better measure for validity and the composite reliability is a better measure for reliability. It's indicating to which extent the constructs (indicators) explain the latent variables. The target value is 0.7.

On the other hand, the AVE (average variance extracted) which is one of the most important variables, measures the variance which is captured by the indicators relative to the measurement error. AVE is an average of the loadings with a recommended value which is more than 0.5. Then the coverage validity is achieved, and the construct can be justified. By referring to AVE result (if more than 0.5), the researchers can ignore the loading values which are less than 0.7. The HTMT value is considered to measure, and its value should be less than 0.85.

Items	Cronbach's alpha (Benchmark of 0.7 or greater)	Composite Reliability (Benchmark of 0.7 or greater)	Average Variance Extracted (Benchmark of 0.5 or greater)
PCR	0.921	0.891	0.623
PEU	0.905	0.923	0.666
UC	0.866	0.910	0.717
CE	0.803	0.852	0.560
BAI	0.665*	0.729	0.604

Reliability and validity table

Table 4.2.3

Note: \* indicate the loading value <0.7

#### 4.2.4 Discriminant validity

Discriminant validity is ensuring that the constructs which expected to be related are related in fact. The square correlation should be less than 0.85.

The discriminant validity is indicating the fact that to which extent dose the construct truly distinct from other constructs. In order for a model to have a high discriminant validity, the AVE values for any two constructs are less than the square of the correlation estimate between them (Hair et al. 2017). Then the square root of construct AVE value must be more than its correlations with another construct.

As shown in the table below the correlation between all the constructs are less than the square root of AVE. the results demonstrate adequate validity in this study. There will be a high amount of overlapping between the constructs if the result is more than 0.85, therefore most probably the constructs are measuring almost the same thing, and discriminant validity between them cannot be claimed.

	<b>Behavioral avoidance intention (BAI)</b>	<b>Cybercrime experience</b>	<b>Percieved cybercrime risk (PCR)</b>	<b>Percieved ease of use (PEU)</b>	<b>User confident (UC)</b>
<b>Behavioral avoidance intention (BAI)</b>	<b>0.777</b>	----	----	----	----
<b>Cybercrime experience</b>	0.175	<b>0.748</b>	----	----	----
<b>Percieved cybercrime risk (PCR)</b>	0.220	0.038	<b>0.789</b>	----	----
<b>Percieved ease of use (PEU)</b>	0.084	-0.121	0.451	<b>0.816</b>	----
<b>User confident (UC)</b>	-0.189	0.263	0.11	0.256	<b>0.847</b>

Discriminant validity table

Table 4.2.4

#### 4.2.5 HTMT

Heterotrait-Monotrait-Ratio (HTMT) was introduced by Henseler et al. (2005) to overcome the issue that cross loading and Fornell-Lacker's criterion are not reliable to assess discriminant validity issue (Hair et al. 2017). Fornell-Lacker's criterion does not perform well if the indicators differ a bit and when loadings vary strongly. It can detect discriminant validity, but not as a strong indicator (Hair et al. 2017).

HTMT is considered as the ratio in between., and within trait correlation. It demonstrates the true correlation between the two constructs and its known as deattenuated correlation. Must be considered that the deattenuated correlation between two constructs which is closer to 1, shows a lack of discriminant validity (Hair et al. 2017). The table below shows that all the constructs are less than 0.85, therefore they appear to be distinct to one another.

	<b>Behavioral avoidance intention (BAI)</b>	<b>Cybercrime experience</b>	<b>Percieved cybercrime risk (PCR)</b>	<b>Percieved ease of use (PEU)</b>	<b>User confident (UC)</b>
<b>Behavioral avoidance intention (BAI)</b>	----	----	----	----	----
<b>Cybercrime experience</b>	<b>0.332</b>	----	----	----	----
<b>Percieved cybercrime risk (PCR)</b>	0.202	<b>0.187</b>	----	----	----
<b>Percieved ease of use (PEU)</b>	0.236	0.349	<b>0.602</b>	----	----
<b>User confident (UC)</b>	0.222	0.292	0.129	<b>0.267</b>	----

HTMT table  
Table 4.2.5

However is better to test whether the HTMT values are significantly different from 1 by testing and running the bootstrapping, and obtain computing bootstrap confidence interval, as anticipated, the conservative HTMT threshold of 0.85 confirms discriminant validity and the bootstrap confidence intervals results also support this.

#### 4.2.6 Multicollinearity for inner model

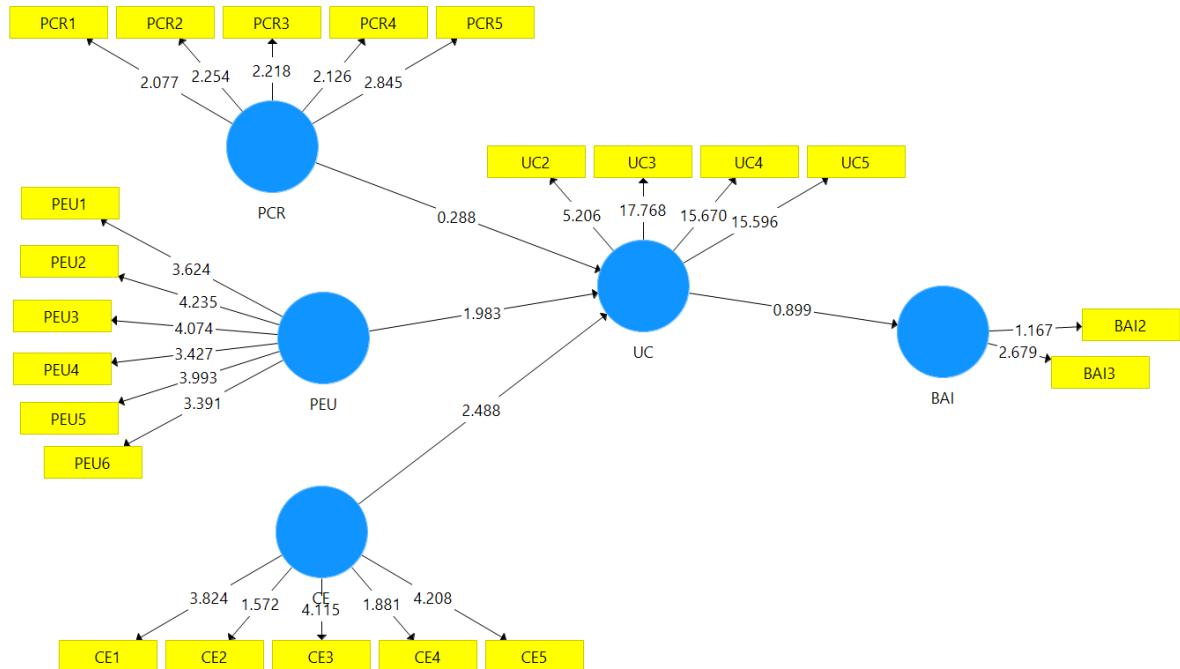
This test is required for inner model, and the VIF values must be less than 5. For checking the multicollinearity within the constructs of the inner model, the VIF (variance inflation factors) for the inner model is obtained. The VIF values which are less than 5, indicate the fact that there is no substantial multicollinearity within the exogenous constructs influencing the mediating variable or the dependent variable. Then the inner VIF values shown in the table below indicates the fact that the latent variables influencing the mediating variable are not correlated with each other.

Items	Inner VIF values
BAI	UC
CE	1.026
PCR	1.269
PEU	1.286

Inner model table  
Table 4.2.6

### 4.3 Analysis of the model

This section is presenting the structural model as well as the assessment and evaluation relating to it by providing the inner model path coefficient significance and size.



**Model 4.3**

#### 4.3.1 R square ( $R^2$ )

R-Square consider to be the measurement of how close the variables are to the fitted regression line. Its known as the coefficient of the determination, also its known as the coefficient of multiple determination for multiple regression.

R-Square values are always between 0% and 100%. The value of 0% indicates that the model doesn't explain any of the variabilities, and 100% explains it all. In general, the higher percentage of R-Square, the better the model fits the data.

	R-Square
<b>BAI</b>	0.100
<b>UC</b>	0.189

R square table

Table 4.3.1

R-Square calculation of this model indicates that changes in BAI is explained by UC by 10%, and CE, PEU, and PCR determine the variation in UC by 18.9%.

#### 4.3.2 Path coefficient

The values shown in the diagram above were obtain by using the PLS-SEM algorithm. The algorithm shows the path coefficients as well as their significance. The higher value of path coefficient, indicates the level of effect which independent variable got on dependent variable. Path coefficient indicates the direct effect of variables which are identified to be the cause on other variable which identified to be an effect. running bootstrapping algorithm is the method to capture both path coefficients and T value. Also, can determine whether they are statistically significant by considering the P value. In cases that the path coefficient value is low, it indicates that its highly unlikely the hypothesized path relationship is significant. Path coefficients with standardized value above 0.20, considered to be mostly significant, those with value less than 0.10 most likely not significant.

Objective	Construct	Hypothesis	Beta ( $\beta$ ) (Path coefficient)	T-Value	P-Value	Decision
<b>To determine the level of influence perceived cyber risk, cybercrime experience, and perceived ease of use have on user-confidence.</b>	PCR → UC	<b>H1</b> Percieved cybercrime has a negative effect on user confident	-0.053	0.288	0.773	Not Supported
	CE → UC	<b>H2</b> Cybercrime experience has a positive effect on user confidence	0.303	2.488	0.013*	Supported
	PEU → UC	<b>H3</b> Percieved ease of use has a positive effect on user confident	0.317	1.983	0.047*	Supported
<b>To identify the extent to which user confidence, which is the mediating variable, influences behavioural avoidance intention.</b>	UC → BAI	<b>H4</b> User confident has a negative effect on behavioral avoidance intention	-0.189	0.899	0.369	Not supported

Path coefficient table

Table 4.3.2

Note: \* indicates  $P < 0.05$  Significant at 5%

By considering the path coefficient results demonstrated in table above, the inner model suggests that the cybercrime experience (CE) has a significant effect on user confident, also the perceived ease of use (PEU) shows a significant effect on user confident (UC), which means the CE and UC, as well as PEU and UC are statistically significant. Then CE and PEU are reliable and predicts UC. But Perceived cybercrime risk (PCR) result, show a lower value, which means it's unlikely to be significant in this structural equation model.

#### 4.4 Multigroup analysis

This section is for comparing between the group based on demography elements. There will be a comparison between the results of the respondents based on their gender and age. Table 4. 4.1 indicates the results with gender as the moderator in this multigroup analysis.

Structural relationship	gender	Path coefficient	T-value	P-value	P-value
CE → UC	Male	0.379	1.460	0.145	0.115
	Female	0.387	2.209	0.028	
PCR → UC	Male	0.361	1.290	0.197	0.955
	Female	-0.087	0.397	0.691	
CE → UC	Male	-0.161	0.513	0.608	0.440
	Female	0.578	2.886	0.004	
UC → BAI	Male	-0.409	1.166	0.244	0.826
	Female	0.309	1.334	0.183	

Multigroup based on gender

Table 4.4.1

Table 4.4.1, demonstrate the results of multigroup test in SmartPLS3. These results differentiate between the respondents based on gender. As it has shown, there is no significant differences between the respondents of male and female participants, which indicates the fact that mainly both genders have almost the same opinions towards the survey of this research. These findings addresses the third objective of this research paper.

Age as the moderator is taken into consideration in the subsequent section and the results are presented in Table 4.4.2.

Structural relationship	Age	Path coefficient	T-value	P-value	P-value
CE → UC	22 to 30	0.265	1.502	0.134	0.115
	41 to 50	-0.200	0.476	0.634	
PCR → UC	22 to 30	-0.392	1.037	0.300	0.955
	41 to 50	0.707	1.654	0.099	
CE → UC	22 to 30	0.116	0.335	0.738	0.440
	41 to 50	0.076	0.133	0.895	
UC → BAI	22 to 30	-0.431	1.318	0.188	0.826
	41 to 50	0.113	0.233	0.816	

Multigroup based on age

Table 4.4.2

The table 4.4.2, which shows the statistics results of multigroup analysis of SmartPLS3 based on age, indicates that there are no significant differences in term of opinions towards the survey of this research, between the two groups which had the highest participants (presented in demography table 4.1.1) in this survey.

## 4.5 Concluding remark

the findings of this research (based on SmartPLS 3 analysis), are align with the previous researches and papers which have been discussed in methodology chapter and literature review, and it indicates that, regardless of country (Malaysia for this paper), cyber-crime has a noticeable effect on accepting the technology by users, and higher level of user confidence will reduce the negative effect of cyber-crime.

# CHAPTER 5 - CONCLUSION & RECOMMENDATION

## 5.0 Overview

In this section, there will be discussion about all the remarked finding of this research paper. All the findings will be based on the analysed information by SmartPLS 3 software. Then, the limitation of study for this research paper will be included. There will be a recommendation part which discusses some possibly solution for E-commerce platforms, based on the findings of this paper, and a future direction for further research on cyber-crime and avoidance intention.

### 5.1 Concluding REMARK

This research paper considers to be an applied research which aims to improve understanding of particular business or management problem. This paper is mainly concentrating on cyber-crime and its effect on the users as avoidance intention. The numbers and statistics discussed in the methodology and the purpose of this research paper indicates the fact that there is a huge loss for E-commerce platforms due to avoidance intention of the users, and many study suggested the fact that cyber-crime is one of the main element to cost the mentioned losses. The research has been designed by using the TAM (Technology acceptance model), to measure the influence of cybercrime on E-commerce.

The chosen method for this research is quantitative research due to time frame and time restriction as well as the importance of accessing a larger variety of respondents.

Based on the problem statement and the nature of this research paper, the targeted population for this paper was the Malaysian citizens who are constantly internet users. The questionnaire was adopted from previous researches and papers on TAM framework with minor modifications. There was a pilot testing (5 people) on questionnaire before distribution, in order to eliminate any misunderstanding and making sure of the required flow. The questionnaire was distributed among 207 participants, the timeframe of collecting the responses indicate that almost all of the

participants are using internet on daily bases. The participants were randomly chosen in order to provide a relatively fair information.

For increasing the accuracy and quality of the data analysing process, the software SmartPLS3 was chosen to provide a complete analysis and measure all aspects of reliabilities and validities of the data. This paper chooses to integrate the different components of research in a logical way and coherent manner in order to ensure that the study effectively address the problems identified in research.

The variables of this research and the framework based on detailed literature reviews and well-designed research paper in order to achieve each objective which is covered in this research paper. There are three identified variables in order to test the hypothesis of this research. Perceived cyber-crime risk, perceived ease of use and cyber-crime experience which are mediated by user confident to determine to which extant do the independent variables affect the behavioural avoidance intention as a dependant variable.

The hypotheses of this study are based on the conceptual framework, and they allow proper indication and connectivity of the dependent and independent variables. Researches which involve with human subjects, raise complex and unique legal, social, ethical and political issues. All the ethical and legal aspects of this research were concerned and there were no data collection processes of the participants.

### Analysis

The initial section of questionnaire comprises of a series of closed-ended questions, targeted at identifying the overall respondents' demographic characteristics, such as gender, age, education status, and income. Approximately 56.5% male and 43.5% female participated in the research survey. The statistics of age indicates that the majority of participants are in middle ages. The statistics gathered from education section shows that 85% of the participants are highly educated, and 71% of participants are in the middle to lower income category.

The second section of questionnaire was related to measure the influence of perceived cyber-crime risk on avoidance intention. The mean value of the collected responses indicate that the majority of the respondents are highly concerned about becoming a victim of cyber-crime (variety).

Third part of questionnaire was specified to measure the impact level of perceived ease of use on avoidance intention. The mean value which is highly toward strongly agree option is indicating that, most of the respondents prefer online activities instead of traditional methods, either shopping or banking. This fact can be explained

by the factor that the majority of respondents are in middle age and try to reduce the time consumption for unnecessary activities.

The level of influence of cyber-crime experience was measured in the fourth section of questionnaire, and the findings indicate that almost all the participants had experience some types of cyber-crime.

The influence of user confident was measured as a mediating effect, to determine that to what extent does this factor mediate the effect of mentioned variables on user's avoidance intention. The mean value indicating that the majority of respondents are agree and satisfy with the general privacy and security of internet. The last section of the questionnaire was specified for behaviour avoidance intention. The results clearly indicate the fact that the majority of participants are aware of cybercrime and don't really trust the platforms, which leads to less participation of online transactions. The results also show that the majority of participants are not feeling safe as mentioned before but due to other reasons they may share their personal information online.

The results of the SmartPLS3 for inner and outer model indicates that all the relations between the latent variables and their indicators as well as the relationship between the latent variables are well established.

Results of the reliability and validity test which contains, loading, R-square ( $R^2$ ), Composite reliability (reliability) and AVE, Discriminant validity (validity), indicates that all the relationships between the parameters are well established, and the results of the model can be considered.

The results of multigroup analysis are divided for two sections. First section based on age and second section based on gender. The result of this analysis indicates that there are no major differences in opinions of respondents toward cyber-crime impact on avoidance intention.

The findings of this research (based on SmartPLS 3 analysis), are align with the previous researches and papers which have been discussed in methodology chapter and literature review, and it indicates that, regardless of country (Malaysia for this paper), cyber-crime has a noticeable effect on accepting the technology by users, and higher level of user confidence will reduce the negative effect of cyber-crime.

## 5.2 Research's purpose

The results and outcome of this research can be beneficial for the future E-Business, and more specifically for the below groups.

### 5.2.1 Government

Perhaps the potential of E-commerce is well known and discussed in the previous chapters. Authorities can provide a guideline and parameters of quality for the E-commerce platforms in order to certify them as a trusted source in the market. This act will increase the potential on observation, therefore the government and authorities can indicate the E-market accordingly. Also, the certificate label for E-commerce platforms will increase the user confidence and result in reducing the user's avoidance intention, as discussed in this research.

### 5.2.2 Businesses

The results of this research are also beneficial for the businesses who are started the E-platforms or the traditional businesses who are moving towards E-platforms. They can identify the necessary acts which are required and identified in this research to maximize the online participants in order to maximize the profit and growth. Also, they can identify the factors which may reduce the intention of users for online transaction and identify factors which increase the intention of existing users and potential users.

### 5.2.3 End users

This research proved that cyber-crime experience has a positive effect on user confidence. The details of this paper can provide more information in order to increase the awareness. Also, users can increase the awareness by sharing their experiences with others through media.

### 5.2.4 Developer

The developers can identify the required and demanded specifications by users in order to improve the user-interface and processes accordingly. The results of improved processes and user-interface will be reflected in perceived ease of use and user confidence, therefore these factors will reduce the avoidance intention and increase the online participation, which is the goal for each E-platform.

## **5.3 Limitations of the study**

The timeframe of this research was the first limit, but the access to the respondents through internet, speeded up the process of collection the data from the respondents. The sample size was another limit, which for the case of this study was 207 participants (Malaysian citizens). This paper studied the opinions of the participants towards online platforms, but the main limit for this paper was the fact that, all of the participants are internet users (already) and there was no opportunity in this paper to measure and study the respondents of non-internet users towards new technology. The main consideration for studying the non-internet user's opinions is that, by analysing the gathered data from their opinions, there will be a better understanding of their demands and need to become an internet user (potential future customers), and based on the findings, platforms can adjust and modify their processes and platforms to increase the participation of users.

## **5.4 Recommendations**

Integrating and providing a unique and united list of processes for online payments and transaction will reduce the level of uncertainty by users and perhaps will increase the participation. E-commerce platforms are required to put more emphasize on designing the user-interfaces of their platforms in order to reduce the level of uncertainty by users, basically the target must be in a way that everyone can navigate through the pages without need for explanations. Increasing the level of security on all aspects on online activities, is crucial. A set of proper user's verification will increase the trust level and perhaps it will reduce the users (hackers) who aim to do harm on online platforms. Advertising by spam email must be eliminated or at least reduced due to the fact that it leaves a negative image on the user's mind. There must be a validity trademark, which is provided by higher authorities for trusted online platforms. This certificate will be issued for genuine and trustworthy platforms, and it will lead to increasing the trust level by users.

## **5.5 future research direction**

Perhaps studying the opinions of internet users will provide information of how and what should be done in order to increase the level of satisfaction and finally increase the intention of usages, but by studying the demands and opinions of non-internet

users will provide a valuable information for the platforms to adjust and modify their online products, services and processes in order to increase the intention of usage among the society. User-interface is well-known by its influence on user's intention, a well-designed user-interface can reduce the level of uncertainty and lead to more participations and, vice-versa. Future researches can use user-interface as a variable which influence the usage's intention.

# REFERENCES

## 6.0 References

Bryman, A. and Bell, E. (2007) *Business Research Methods*. Oxford: Oxford University Press

BusinessDictionary (2018) *Read The Full Definition*. [online] available from <<http://www.businessdictionary.com/definition/research-methodology.html>> [26 November 2018]

Clemes, M., Gan, C. and Zhang, J. (2014) "An Empirical Analysis Of Online Shopping Adoption In Beijing, China". *Journal Of Retailing And Consumer Services* 21 (3), 364-375

Clickatell (2018) *Cybercrime And Its Effect On Businesses - Clickatell* [online] available from <<https://www.clickatell.com/articles/information-security/cybercrime-effect-businesses/>> [26 November 2018]

Coleman, A. (2018) *Cyber Crime - A Business Threat To Take Seriously* [online] available from <<https://www.telegraph.co.uk/sponsored/business/solutions/12013807/cyber-crime-prevention.html>> [26 November 2018]

communitymedicine4asses (2018) *Types Of Data: Primary And Secondary Data* [online] available from <<https://communitymedicine4asses.com/2013/01/07/types-of-data-primary-and-secondary-data/>> [26 November 2018]

Cooper, D., Schindler, P. and Emory, W. (2008) *Business Research Methods*. 10th edn. Boston, Mass.: McGraw-Hill Irwin

Davis, F. (1989) "Perceived Usefulness, Perceived Ease Of Use, And User Acceptance Of Information Technology". *MIS Quarterly* [online] 13 (3), 319. available

from <[https://www.jstor.org/stable/249008?seq=1#page\\_scan\\_tab\\_contents](https://www.jstor.org/stable/249008?seq=1#page_scan_tab_contents)> [26 November 2018]

Davis, F., Bagozzi, R. and Warshaw, P. (1989) "User Acceptance Of Computer Technology: A Comparison Of Two Theoretical Models". *Management Science* 35 (8), 982-1003

De Vaus, D. (2013) *Research Design In Social Research*. 1st edn. London: Sage

Dudovskiy, J. (2016) *The Ultimate Guide To Writing A Dissertation In Business Studies: A Step-By-Step Assistance* [online] 1st edn. available from <<https://research-methodology.net/about-us/ebook/>> [26 November 2018]

Elmansy, R. (2018) *Using Inductive Reasoning In User Experience Research* [online] available from <<https://www.designorate.com/inductive-reasoning-in-user-experience-research/>> [26 November 2018]

Explorable.com (2009) *Research Population - The Focus Group Of A Scientific Query* [online] available from <<https://explorable.com/research-population>> [26 November 2018]

First Data Corporation (2009) *Market Brief: Consumer Online Shopping Fears* [online] First Data Corporation. available from <[https://www.firstdata.com/downloads/thought-leadership/fd\\_consumeronlineshoppingfears\\_research.pdf](https://www.firstdata.com/downloads/thought-leadership/fd_consumeronlineshoppingfears_research.pdf)> [26 November 2018]

Grobman, S., Birdsong, T., Australia, C. and Davis, G. (2018) *Economic Impact Of Cybercrime: Why Cyber Espionage Isn't Just The Military's Problem | McAfee Blogs* [online] available from <<https://securingtomorrow.mcafee.com/business/economic-impact-cybercrime-cyber-espionage-isnt-just-militarys-problem/>> [26 November 2018]

Hair, J., Hult, G., Ringle, C. and Sarstedt, M. (2017) *A Primer On Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 2nd edn

Hille, P., Walsh, G. and Cleveland, M. (2015) "Consumer Fear Of Online Identity Theft: Scale Development And Validation". *Journal Of Interactive Marketing* [online]

30 (1), 1-19. available from <[http://zero.sci-hub.tw/3852/4044d5dcac3b117a7efbe98d5e5ff514/hille2015.pdf?fbclid=IwAR3phd3fi6LB4qwIzR5RTRPsvCux1DSqEnnahR4\\_witFpxy0Sms8jkWVzng](http://zero.sci-hub.tw/3852/4044d5dcac3b117a7efbe98d5e5ff514/hille2015.pdf?fbclid=IwAR3phd3fi6LB4qwIzR5RTRPsvCux1DSqEnnahR4_witFpxy0Sms8jkWVzng)> [26 November 2018]

Jenny (2017) *Phase #2: Clearly Define Your Research Strategy | Mackenzie Corporation* [online] available from <<https://www.mackenziecorp.com/phase-2-clearly-define-research-strategy/>> [26 November 2018]

Joyce, M. and Kirakowski, J. (2014) "Measuring Confidence In Internet Use: The Development Of An Internet Self-Efficacy Scale". *Design, User Experience, And Usability. Theories, Methods, And Tools For Designing The User Experience* 250-260

Lai, P. (2017) "The Literature Review Of Technology Adoption Models And Theories For The Novelty Technology". *Journal Of Information Systems And Technology Management* 14 (1)

Lake, L. (2018) *Learn About Perceived Risk And How To Overcome It With Messaging* [online] available from <<https://www.thebalancesmb.com/what-is-perceived-risk-2295541>> [26 November 2018]

Liébana-Cabanillas, F., Muñoz-Leiva, F., Sánchez-Fernández, J. and Viedma-del Jesús, M. (2015) "The Moderating Effect Of User Experience On Satisfaction With Electronic Banking: Empirical Evidence From The Spanish Case". *Information Systems And E-Business Management* 14 (1), 141-165

Marangunić, N. and Granić, A. (2014) "Technology Acceptance Model: A Literature Review From 1986 To 2013". *Universal Access In The Information Society* 14 (1), 81-95

Martins, C., Oliveira, T. and Popovič, A. (2014) "Understanding The Internet Banking Adoption: A Unified Theory Of Acceptance And Use Of Technology And Perceived Risk Application". *International Journal Of Information Management* 34 (1), 1-13

Mason, P. (2014) *Researching Tourism, Leisure And Hospitality For Your Dissertation*. Oxford: Goodfellow Publishers

Mohinuddin, M. (2018) *Demographic Data Collection; Differences Between Census And Sampling* [online] available from <<https://socialworkeducationbd.blogspot.com/2018/05/demographic-data-collection-differences.html>> [26 November 2018]

Mortenson, M. and Vidgen, R. (2016) "A Computational Literature Review Of The Technology Acceptance Model". *International Journal Of Information Management* 36 (6), 1248-1259

Moskowitz, S. (2017) *Cybercrime And Business: Strategies For Global Corporate Security*. 1st edn. Butterworth-Heinemann

Norman, D. and Nielsen, J. (2018) *The Definition Of User Experience (UX)* [online] available from <<https://www.nngroup.com/articles/definition-user-experience/>> [26 November 2018]

NSTP Team (2018) *E-Commerce Growth Has Been Significant In Malaysia* [online] available from <<https://www.nst.com.my/business/2018/03/345053/e-commerce-growth-has-been-significant-malaysia>> [26 November 2018]

Planet Retail and NetSuite (2016) *UK Discount Pricing Strategies: Optimising Operational, Merchandising & Promotional Plans* [online] Planet Retail and Retail Net Group (RNG). available from <<http://www.netsuite.co.uk/portal/uk/pdf/report-planetretail-uk-discount-pricing-strategies.pdf>> [26 November 2018]

Price, P., Jhangiani, R. and Chiang, I. (2015) *Research Methods In Psychology*. 2nd edn. California

Rahman, M. and Sloan, T. (2017) "User Adoption Of Mobile Commerce In Bangladesh: Integrating Perceived Risk, Perceived Cost And Personal Awareness With TAM". *The International Technology Management Review* 6 (3), 103

Rahn, M. (2018) *Factor Analysis: A Short Introduction, Part 5-Dropping Unimportant Variables From Your Analysis - The Analysis Factor* [online] available from <<https://www.theanalysisfactor.com/factor-analysis-5/>> [26 November 2018]

Research Methodology (2018) *Deductive Approach (Deductive Reasoning) - Research-Methodology* [online] available from <<https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/>> [26 November 2018]

Richardson, C. (2017) *Applications Of The Technology Acceptance Model To Integration Of The Automatic Ground Collision Avoidance System In Fighter Aircraft Operations*. Ph. D. Embry-Riddle Aeronautical University Daytona Beach, Florida

Riek, M., Bohme, R. and Moore, T. (2016) "Measuring The Influence Of Perceived Cybercrime Risk On Online Service Avoidance". *IEEE Transactions On Dependable And Secure Computing* 13 (2), 261-273

Riek, M., Böhme, R. and Moore, T. (2014) *Understanding The Influence Of The Cyber Crime On The E-Service Adoption Of European Internet Users (Working Paper)*. [online] available from <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.8328&rep=rep1&type=pdf>> [26 November 2018]

Robert Niles (2018) *Statistics: Definition Of Standard Deviation* [online] available from <<https://www.robertniles.com/stats/stdev.shtml>> [26 November 2018]

Rouse, M. (n.d.) *What Is User Interface (UI)? - Definition From WhatIs.Com* [online] available from <<https://searchmicroservices.techtarget.com/definition/user-interface-UI>> [26 November 2018]

Sabiote, C., Frías, D. and Castañeda, J. (2012) "The Moderating Effect Of Uncertainty-Avoidance On Overall Perceived Value Of A Service Purchased Online". *Internet Research* 22 (2), 180-198

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods For Business Students*. 5th edn. Harlow: Financial Times Prentice Hall

Sharma, G. and Lijuan, W. (2015) "The Effects Of Online Service Quality Of E-Commerce Websites On User Satisfaction". *The Electronic Library* 33 (3), 468-485

Smith, A. (2004) "Cybercriminal Impacts On Online Business And Consumer Confidence". *Online Information Review* 28 (3), 224-234

Smith, A. (2004) "Cybercriminal Impacts On Online Business And Consumer Confidence". *Online Information Review* 28 (3), 224-234

Tabassam, S., Chaudhry, N. and Nusair, K. (2016) "Using Technology Acceptance Model To Study Adoption Of Online Shopping In An Emerging Economy". *Journal Of Internet Banking And Commerce* [online] 21 (2). available from <<http://www.icommercecentral.com/open-access/using-technology-acceptance-model-to-study-adoption-of-online-shopping-in-an-emerging-economy.pdf>> [26 November 2018]

The Economist (2017) *E-Commerce Takes Off* [online] available from <<https://www.economist.com/special-report/2017/10/26/e-commerce-takes-off>> [26 November 2018]

Valentini, F. and Damásio, B. (2016) "Variância Média Extraída E Confiabilidade Composta: Indicadores De Precisão". *Psicologia: Teoria E Pesquisa* 32 (2)

Venkatesh, V. (2000) "Determinants Of Perceived Ease Of Use: Integrating Control, Intrinsic Motivation, And Emotion Into The Technology Acceptance Model". *Information Systems Research* 11 (4), 342-365

Warrington, T., Abgrab, N. and Caldwell, H. (2000) "BUILDING TRUST TO DEVELOP COMPETITIVE ADVANTAGE IN E-BUSINESS RELATIONSHIPS". *Competitiveness Review* 10 (2), 160-168

# 7.0 APPENDICES

## 7.1 Questionnaire

The screenshot shows a Google Forms survey titled "Survey". The introduction states: "I am a postgraduate student pursuing the Masters in Business Administration - Global Business, at INTI International College Subang. As part of my dissertation requirement, I am conducting a survey to study the Behavioral Avoidance Intention of technology acceptance. Hence, I am seeking your assistance in participating in this study by completing the following questionnaire. The information provided will be kept confidential and it will be used solely for the purpose of completing my dissertation. Thank you very much for your time and assistance." The "Demography" section begins with a question: "1. Please specify your gender \*". There are two options: "1) Male" and "2) Female". Below this is another question: "2. Indicate your age \*".

1. Please specify your gender \*

1) Male  
 2) Female

2. Indicate your age \*

The screenshot continues from the previous one, showing the survey questions. The second question, "2. Indicate your age \*", has five options: "1) 21 and below", "2) 22 to 30", "3) 31 to 40", "4) 41 to 50", and "5) More than 50". The third question, "3. Please specify your level of education \*", has six options: "1) Seconder school / High school", "2) Diploma", "3) Degree", "4) Postgraduate", "5) Professional course", and "6) Other. Please indicate: \_\_\_\_\_".

2. Indicate your age \*

1) 21 and below  
 2) 22 to 30  
 3) 31 to 40  
 4) 41 to 50  
 5) More than 50

3. Please specify your level of education \*

1) Seconder school / High school  
 2) Diploma  
 3) Degree  
 4) Postgraduate  
 5) Professional course  
 6) Other. Please indicate: \_\_\_\_\_

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA6KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe... Other bookmarks

4. Please specify your monthly income \*

1) Below RM 2500  
 2) RM 2501 to RM 5000  
 3) RM 5001 to RM 7500  
 4) RM 7501 to RM 10000  
 5) Above RM 10000

After section 1 Continue to next section

Section 2 of 6

## Perceived Cyber-Crime Risk

Please refer to the scale below when answering the following questions:  
Scale:  
5 = Strongly agree  
4 = Agree  
3 = Neutral  
2 = Disagree  
1 = Strongly Disagree

8:50 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA6KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe... Other bookmarks

Section 2 of 6

## Perceived Cyber-Crime Risk

Please refer to the scale below when answering the following questions:  
Scale:  
5 = Strongly agree  
4 = Agree  
3 = Neutral  
2 = Disagree  
1 = Strongly Disagree

5. I am personally concerned about becoming a victim of Identity Theft? \*  
(using another person's name and personal information)

1  
 2  
 3  
 4  
 5

8:50 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

6. I am personally concerned about becoming a victim of Spam E-mails? (unsolicited messages sent in bulk by email) \*

1  
 2  
 3  
 4  
 5

7. I am personally concerned about becoming a victim of Online Fraud? (fraud that is committed with the help of the internet) \*

1  
 2  
 3  
 4  
 5

8. I am personally concerned about becoming a victim of "Content of Racial Hatred"? (incitement to racial or ethnic issues) \*

1  
 2  
 3  
 4  
 5

9. I am personally concerned about becoming a victim of Unavailable Content? (The Website's Server Not Available) \*

1  
 2  
 3  
 4  
 5

8:50 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

8. I am personally concerned about becoming a victim of "Content of Racial Hatred"? (incitement to racial or ethnic issues) \*

1  
 2  
 3  
 4  
 5

9. I am personally concerned about becoming a victim of Unavailable Content? (The Website's Server Not Available) \*

1  
 2  
 3  
 4  
 5

8:50 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

Section 3 of 6

## Perceived Ease of use

Please refer to the scale below when answering the following questions:  
Scale:  
5 = Strongly agree  
4 = Agree  
3 = Neutral  
2 = Disagree  
1 = Strongly Disagree

10. I agree that online shopping and web-based online transactions save my time.

1  
 2  
 3  
 4  
 5

11. I agree that interaction through web pages is clear and understandable.

1  
 2  
 3  
 4  
 5

12. I agree that online shopping and web-based online transactions save cost.

1  
 2  
 3  
 4  
 5

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

11. I agree that interaction through web pages is clear and understandable.

1  
 2  
 3  
 4  
 5

12. I agree that online shopping and web-based online transactions save cost.

1  
 2  
 3  
 4  
 5

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

13. I agree that it is easy to become skillful at navigating the web pages. \*

1  
 2  
 3  
 4  
 5

14. I agree that online shopping and web-based online transactions are much \* more convenient.

1  
 2  
 3  
 4  
 5

After section 3 Continue to next section

Section 4 of 6

Cyber-Crime Experience

8:51 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

15. I agree that online shopping and web-based online transactions provide \* more variety of options.

1  
 2  
 3  
 4  
 5

After section 3 Continue to next section

Section 4 of 6

Cyber-Crime Experience

8:51 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

Section 4 of 6

## Cyber-Crime Experience

Please refer to the scale below when answering the following questions:  
Scale:  
5 = Strongly agree  
4 = Agree  
3 = Neutral  
2 = Disagree  
1 = Strongly Disagree

16. I have experienced or been a victim of Identity Theft? \*

1  
 2  
 3  
 4  
 5

8:52 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

17. I have experienced or been a victim of Spam E Mail? \*

1  
 2  
 3  
 4  
 5

18. I have experienced or been a victim of Identity Illegal Content? \*

1  
 2  
 3  
 4  
 5

8:52 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA6KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

19. I have experienced or been a victim of Unavailable Content? \*

1  
 2  
 3  
 4  
 5

20. I have experienced or been a victim of Online Fraud? \*

1  
 2  
 3  
 4  
 5

8:52 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA6KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

Section 5 of 6

## User Confident

Please refer to the scale below when answering the following questions:  
Scale:  
5 = Strongly agree  
4 = Agree  
3 = Neutral  
2 = Disagree  
1 = Strongly Disagree

21. I am concerned about the fact that the websites that I have visited might know/track the history of my browser? \*

1  
 2  
 3  
 4  
 5

8:52 PM 22/11/2018

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

22. I'm confident that the information that I have provided on internet wont be \* used for other purposes.

1  
 2  
 3  
 4  
 5

23. In general, the Internet is now a safe environment in which I can confidently transact business.

1  
 2  
 3  
 4  
 5

24. I feel assured that legal and technical structures adequately protect me from problems on the internet.

1  
 2  
 3  
 4  
 5

25. The Internet has enough safeguard measures to make me feel comfortable using it to transect personal business.

1  
 2  
 3  
 4  
 5

Untitled form - Google Forms

https://docs.google.com/forms/d/1sfrm4hEpNyxLOESbA46KjnQu137aBILfQGFdpdkuOE/edit

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

24. I feel assured that legal and technical structures adequately protect me from problems on the internet.

1  
 2  
 3  
 4  
 5

25. The Internet has enough safeguard measures to make me feel comfortable using it to transect personal business.

1  
 2  
 3  
 4  
 5

Untitled form - Google Forms

<https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit>

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

Section 6 of 6

## Behavioral Avoidance Intention

Please refer to the scale below when answering the following questions:

Scale:  
 5 = Strongly agree  
 4 = Agree  
 3 = Neutral  
 2 = Disagree  
 1 = Strongly Disagree

26. Due to Cyber-Crime I'm less likely to do Online Banking. \*

1  
 2  
 3  
 4  
 5

8:53 PM 22/11/2018

Untitled form - Google Forms

<https://docs.google.com/forms/d/1sfrm4hEpNyxLOEsBAA46KjnQu137aBILfQGFdpdkuOE/edit>

Blackboard Learn Inti enrolment BUILDING TRUST TO Cybercriminal impact Online Results for Me tableau software - G Measuring the Influe Other bookmarks

27. Due to Cyber-Crime I'm less likely to do Online Shopping. \*

1  
 2  
 3  
 4  
 5

28. Due to Cyber-Crime I'm less likely to Publish Personal Information Online. \*

1  
 2  
 3  
 4  
 5

8:53 PM 22/11/2018

## 7.2 Ethics approval checklist

## Low Risk Research Ethics Approval Checklist

### Applicant Details

Name: Mohammad Hashtari	E-mail: rezamohammad.h@gmail.com
Department: Postgraduate	Date: 22/11/2018
Course: MBA Global business	Title of Project:

### Project Details

Summary of the project in jargon-free language and in not more than 120 words: Studying the factors that influence the online service user's avoidance intention.

- Research Objectives: Measuring the impact of cybercrime on avoidance intention
- Research Design (e.g. Experimental, Desk-based, Theoretical etc): Theoretical
- Methods of Data Collection: Survey questionnaire

### Participants in your research

1. Will the project involve human participants?	<input checked="" type="checkbox"/> Yes	No
---	---	----

If you answered **Yes** to this questions, this may **not** be a low risk project.

- If you are a student, please discuss your project with your Supervisor.
- If you are a member of staff, please discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval or NHS or Medical Approval Routes.

### Risk to Participants

2. Will the project involve human patients/clients, health professionals, and/or patient (client) data and/or health professional data?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
3. Will any invasive physical procedure, including collecting tissue or other samples, be used in the research?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
4. Is there a risk of physical discomfort to those taking part?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
5. Is there a risk of psychological or emotional distress to those taking part?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
6. Is there a risk of challenging the deeply held beliefs of those taking part?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
7. Is there a risk that previous, current or proposed criminal or illegal acts will be revealed by those taking part?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
8. Will the project involve giving any form of professional, medical or legal advice, either directly or indirectly to those taking part?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

If you answered **Yes** to any of these questions, this may **not** be a low risk project.

- If you are a student, please discuss your project with your Supervisor.
- If you are a member of staff, please discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval or NHS or Medical Approval Routes.

### Risk to Researcher

9. Will this project put you or others at risk of physical harm, injury or death?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
---	------------------------------	--

10. Will project put you or others at risk of abduction, physical, mental or sexual abuse?	Yes	<input checked="" type="checkbox"/>
11. Will this project involve participating in acts that may cause psychological or emotional distress to you or to others?	Yes	<input checked="" type="checkbox"/>
12. Will this project involve observing acts which may cause psychological or emotional distress to you or to others?	Yes	<input checked="" type="checkbox"/>
13. Will this project involve reading about, listening to or viewing materials that may cause psychological or emotional distress to you or to others?	Yes	<input checked="" type="checkbox"/>
14. Will this project involve you disclosing personal data to the participants other than your name and the University as your contact and e-mail address?	Yes	<input checked="" type="checkbox"/>
15. Will this project involve you in unsupervised private discussion with people who are not already known to you?	Yes	<input checked="" type="checkbox"/>
16. Will this project potentially place you in the situation where you may receive unwelcome media attention?	Yes	<input checked="" type="checkbox"/>
17. Could the topic or results of this project be seen as illegal or attract the attention of the security services or other agencies?	Yes	<input checked="" type="checkbox"/>
18. Could the topic or results of this project be viewed as controversial by anyone?	Yes	<input checked="" type="checkbox"/>

If you answered Yes to any of these questions, this is not a low risk project. Please:

- If you are a student, discuss your project with your Supervisor.
- If you are a member of staff, discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval route.

#### Informed Consent of the Participant

19. Are any of the participants under the age of 18?	Yes	<input checked="" type="checkbox"/>
20. Are any of the participants unable mentally or physically to give consent?	Yes	<input checked="" type="checkbox"/>
21. Do you intend to observe the activities of individuals or groups without their knowledge and/or informed consent from each participant (or from his or her parent or guardian)?	Yes	<input checked="" type="checkbox"/>

If you answered Yes to any of these questions, this may not be a low risk project. Please:

- If you are a student, discuss your project with your Supervisor.
- If you are a member of staff, discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval route.

#### Participant Confidentiality and Data Protection

22. Will the project involve collecting data and information from human participants who will be identifiable in the final report?	Yes	<input checked="" type="checkbox"/>
23. Will information not already in the public domain about specific individuals or institutions be identifiable through data published or otherwise made available?	Yes	<input checked="" type="checkbox"/>
24. Do you intend to record, photograph or film individuals or groups without their knowledge or informed consent?	Yes	<input checked="" type="checkbox"/>

25. Do you intend to use the confidential information, knowledge or trade secrets gathered for any purpose other than this research project?	Yes	No
--	-----	----

If you answered **Yes** to any of these questions, this may **not** be a low risk project:

- If you are a student, discuss your project with your Supervisor.
- If you are a member of staff, discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval or NHS or Medical Approval routes.

#### Gatekeeper Risk

26. Will this project involve collecting data outside University buildings?	Yes	No
27. Do you intend to collect data in shopping centres or other public places?	Yes	No
28. Do you intend to gather data within nurseries, schools or colleges?	Yes	No
29. Do you intend to gather data within National Health Service premises?	Yes	No

If you answered **Yes** to any of these questions, this is **not** a low risk project. Please:

- If you are a student, discuss your project with your Supervisor.
- If you are a member of staff, discuss your project with your Faculty Research Ethics Leader or use the Medium to High Risk Ethical Approval or NHS or Medical Approval routes.

#### Other Ethical Issues

30. Is there any other risk or issue not covered above that may pose a risk to you or any of the participants?	Yes	No
31. Will any activity associated with this project put you or the participants at an ethical, moral or legal risk?	Yes	No

If you answered **Yes** to these questions, this may **not** be a low risk project. Please:

- If you are a student, discuss your project with your Supervisor.
- If you are a member of staff, discuss your project with your Faculty Research Ethics Leader.

## Principal Investigator Certification

If you answered **No** to **all** of the above questions, then you have described a low risk project. Please complete the following declaration to certify your project and keep a copy for your record as you may be asked for this at any time.

### Agreed restrictions to project to allow Principal Investigator Certification

Please identify any restrictions to the project, agreed with your Supervisor or Faculty Research Ethics Leader to allow you to sign the Principal Investigator Certification declaration.

Participant Information Leaflet attached.

Informed Consent Forms attached.

Risk Assessment Form attached.

### Principal Investigator's Declaration

Please ensure that you:

- Tick all the boxes below and sign this checklist.
- Students must get their Supervisor to countersign this declaration.

I believe that this project <b>does not require research ethics approval</b> . I have completed the checklist and kept a copy for my own records. I realise I may be asked to provide a copy of this checklist at any time.	<input checked="" type="checkbox"/>
I confirm that I have answered all relevant questions in this checklist honestly.	<input checked="" type="checkbox"/>
I confirm that I will carry out the project in the ways described in this checklist. I will immediately suspend research and request a new ethical approval if the project subsequently changes the information I have given in this checklist.	<input checked="" type="checkbox"/>

### Signatures

If you or your supervisor do not have electronic signatures, please type your name in the signature space. An email sent from the Supervisor's University inbox will be accepted as having been signed electronically.

#### Principal Investigator

Signed

(Principal Investigator or Student)

Date

Students storing this checklist electronically must append to it an email from your Supervisor confirming that they are prepared to make the declaration above and to countersign this checklist. This-email will be taken as an electronic countersignature.

#### Student's Supervisor

Countersigned

Sumitha



(Supervisor)

Date

20/11/2018

I have read this checklist and confirm that it covers all the ethical issues raised by this project fully and frankly. I also confirm that these issues have been discussed with the student and will continue to be reviewed in the course of supervision.

## 7.3 Dissertation meeting diary

### MO301ON DISSERTATION – Meeting Diary

Week	Student Requirements	Summary of Actions Agreed	Meeting Attendance Signatures
Week 1	Review of Research Proposal: Research Topic and Design Meeting diary created	Discussion about the proposed topic. Details about the framework and constructs, and more suggestions provided by doctor. Reviewing the journal articles.	Student: M.Hashthari Supervisor: Dr. Sumitha <i>Sumitha</i> Date: 6/Sep/2018
Week 3	Review of Submitted Literature Review and Methodology Meeting diary updated	Discussing the questionnaire. Adjusting the demographic part and a few more question in order to align with the topic. Reviewing the completed chapters, and adding some suggestions to it by doctor.	Student: M.Hashthari Supervisor: Dr. Sumitha <i>Sumitha</i> Date: 11/Sep/2018
Week 5	Review of Submitted Data Collection Meeting diary updated	Reviewing the responses, and starting the data analysis process. Starting the process of PLS and SPSS. Discussing the literature review, and suggestion made by doctor.	Student: M.Hashthari Supervisor: Dr. Sumitha <i>Sumitha</i> Date: 6/Nov/2018
Week 7	Review of Submitted Analysis Meeting diary updated	Analyzing the gathered information. Reviewing the framework and the scores of PLS, and adding some suggestions by doctor.	Student: M.Hashthari Supervisor: Dr. Sumitha <i>Sumitha</i> Date: 11/Nov/2018
Week 10	Assessed Presentation of Complete Draft to include initial Conclusions	Reviewing the paper and checking the flow of the topic by doctor.	Student: M.Hashthari Supervisor: Dr. Sumitha <i>Sumitha</i>

	Meeting diary updated	Reviewing the slides and doctor added suggestions.	Date: 17/Nov/2018
--	-----------------------	--	-------------------

**Further Information:**

The date and times of each tutorial will be allocated by Coventry University London Campus. Tutorials require compulsory attendance on campus. Students are required to submit specific items of work 4 days in advance of each tutorial. The submitted work will typically form the basis of each tutorial.

Dissertation supervision meetings are a compulsory part of the dissertation module and all students must attend their face to face dissertation meetings with their tutor. Non-attendance at the agreed tutorial time will be counted as absent, and cannot be re-arranged.

A maximum of one tutorial can be delivered virtually, typically where data collection is being carried out. This will be agreed in advance by the Supervisor. This does not apply to the following tutorials:

- Week 5 Review of Data Collection
- Week 10 Assessed Presentation of Complete Draft to include initial Conclusions

It is the responsibility of the student to:

- Provide an agenda for each tutorial 4 days in advance
- Attend on time
- Maintain a log of meetings which are signed by both Supervisor and Student
- Include completed logs in the Appendix of the final submitted dissertation