CYBERSTALKING ON FACEBOOK:
EXAMINING THE RELATIONSHIP BETWEEN FACEBOOK USAGE CHARACTERISTICS AND CYBERSTALKING VICTIMIZATION AMONG YOUNG MALAYSIAN FACEBOOK USERS

By

ALAN CHEW JIAN LOONG

A dissertation submitted to the
Department of Internet Engineering and Computer Science,
Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Master of Information Systems
November 2014

ABSTRACT

CYBERSTALKING ON FACEBOOK:
EXAMINING THE RELATIONSHIP BETWEEN FACEBOOK USAGE CHARACTERISTICS AND CYBERSTALKING VICITMIZATION AMONG YOUNG MALAYSIAN FACEBOOK USERS

Alan Chew Jian Loong

Social media has become a major facet of life, especially for members of younger generations who thrive on the social aspect offered by the instant-gratification of being online. The problem that exists with the advancement of social media technology is that just about anyone can gain access to any information posted online, despite user preferences and despite user awareness. With the availability of information and the willingness of users to blindly share information to an almost exponential number of other users, the issue of safety and privacy become very important. Furthermore, the continuing advances in technology have actually made cyberstalking much easier than ever before, with smartphones capable of logging in and tagging one’s location, with check-in features provided by Facebook’s tracking system, and by the growing list of friends of friends who can see every posts or tags. This research aims to study and determine the relationship between Facebook usage characteristics and cyberstalking victimization among young Malaysian Facebook users. The five objectives of this research are to determine the relationship of: 1) the use of location disseminating features; 2) accepting strangers’ friend requests; 3) using default security settings; 4) using public privacy settings; 5) gender of Facebook users, in affecting cyberstalking victimization. In order to achieve that, this study utilized an online self-administered questionnaire to survey a representative sample of young Malaysian Facebook users in Malaysia. From the results of hypotheses testing, it was found that accepting strangers' friend requests and using public privacy settings on Facebook are significantly related to cyberstalking victimization among young Malaysian Facebook users. Furthermore, the results also indicated that approximately 40% of young Malaysian Facebook users had experienced some kind of cyberstalking victimization on Facebook or resulting from the use of Facebook.

ACKNOWLEDGEMENT

First of all, I would like to thank my parents for giving me the opportunity to pursue my Master's degree in full time. I would not dare to even think about quitting my job to continue my studies without their financial and moral support.

I would like to extend my utmost gratitude to my supervisor, Ms Chow Mee Mooi from the Department of Game Studies, Universiti Tunku Abdul Rahman, for agreeing to be the supervisor for my Master's project. Your continuous guidance and encouragement throughout the year have given me the confidence and strength to complete the dissertation.

I am truly grateful to my girlfriend Ooi Sze Hwei, who had been supporting me by my side since Diploma, lifting me up when I am at the low point of my life. I am really happy that we are going to accomplish our Master's together soon.

Last but not least, I would like to thank all my friends and course mates that have been supporting me all the time.

APPROVAL SHEET

This dissertation entitled "**CYBERSTALKING ON FACEBOOK: EXAMINING THE RELATIONSHIP BETWEEN FACEBOOK USAGE CHARACTERISTICS AND CYBERSTALKING VICTIMIZATION AMONG YOUNG MALAYSIAN FACEBOOK USERS"** was prepared by ALAN CHEW JIAN LOONG and submitted as partial fulfillment of the requirements for the degree of Master of Information Systems at Universiti Tunku Abdul Rahman.

Approved by:

____

(Ms Chow Mee Mooi) Date:…………………..
Supervisor
Department of Game Studies
Faculty of Creative Industries
Universiti Tunku Abdul Rahman

FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: ___________________

SUBMISSION OF DISSERTATION

It is hereby certified that **Alan Chew Jian Loong** (ID No: **13UEM02125**) has completed this dissertation entitled "**CYBERSTALKING ON FACEBOOK: EXAMINING THE RELATIONSHIP BETWEEN FACEBOOK USAGE CHARACTERISTICS AND CYBERSTALKING VICTIMIZATION AMONG YOUNG MALAYSIAN FACEBOOK USERS**" under the supervision of Ms Chow Mee Mooi (Supervisor) from the Department of Game Studies, Faculty of Creative Industries.

I understand that the University will upload softcopy of my dissertation in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

____

(Alan Chew Jian Loong)

DECLARATION

I Alan Chew Jian Loong hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

____

(ALAN CHEW JIAN LOONG)

Date ________________________

TABLE OF CONTENTS

Page

CHAPTER

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Goodman (2012), a global security advisor, mentioned in an interview to CNN that every newer form of technology introduced into society produces new opportunities for criminal to misuse it to their benefit. Technology can be considered as a double-edged sword as it brought positive and negative effects to our daily lives. In this digital era, the complexity of crime has become more sophisticated because of the existence of technology. As technology is advancing through time so are crimes.

The advent of Web 2.0 and the consequent emergence of social media have irrevocably transformed the nature of human communication, creating social networks which are unprecedentedly broad and divergent from normative, interpersonal relationships in numerous ways. In September 2014, Facebook (2014a) announced that they currently have 1.35 billion monthly active users, 1.12 billion mobile monthly active users, 864 million daily active users, and 703 million mobile active users, these numbers represent staggering amounts of online users. While social media is heralded for affording voice to previously vulnerable populations throughout the global community, it has also been condemned by those who target the media as potentially detrimental to human society, creating conditions through which human relationships are characterized by quantity over quality. Also, perhaps the most severe issue of all is the rise of privacy concerns among users of social networking sites.

With the continuing advances in technology and the introduction of Internet to the public, it has given stalkers a new platform to stalk their victims, thus given rise to a new form stalking which is cyberstalking. Cyberstalking has actually become much easier than ever before, with smartphones capable of logging in and tagging one's location, with check-in features provided by Facebook's tracking system, and by the growing list of friends of friends who can see every posts or tag. For example, cyberstalker can use Facebook's friend of a friend mechanism to see that their target has been tagged at a location, and can then find them; or even, go to their home and wait until they return. A friend of a friend comments on a post, and the stalker can see that information; and sometimes even have access to other photos or information based upon how the albums are set up. The advances in technology and social networking sites have made cyberstalking laughably easy.

With the availability of information and the willingness of users to blindly share information to an almost exponential number of other users, the issue of safety and privacy become very important. This study attempts to collect data on young Malaysian Facebook users' privacy and security settings, their usage frequency of Facebook features that pose privacy and security risks, and their tendency to accept strangers' friend requests on Facebook. By doing so, this research aims to determine the relationship between Facebook usage characteristics and cyberstalking victimization among young Malaysian Facebook users.

The main motivation for choosing this topic is due to the tremendous growth of Facebook users in Malaysia. A study conducted by research firm TNS has revealed that Malaysians have most social network friends globally, at an average of 233 friends per person, at the same time, are also the heaviest users of social networking sites in the world, spending nine hours per week on social networks (The Star, 2010; Yap, 2010). Secondly, there has not been any research done in the Malaysian context to examine and find out the relationship between cyberstalking attacks and the users' Facebook usage characteristics. With cyberstalking cases on the rise, people need to be made aware of privacy and security risks on Facebook because social media is such a major part of life now.

1.2 Problem Statement

Social media has become a major facet of life, especially for members of younger generations who thrive on the social aspect offered by the instant-gratification of being online. The problem that exists with the advancement of social media technology is that just about anyone can gain access to any information posted online, despite user preferences and despite user awareness. With the availability of information and the willingness of users to blindly share information to an almost exponential number of other users, the issue of safety and privacy become very important.

More saliently, research on social media has highlighted the ways in which criminal behaviour is influenced by online communities, with the ability to create an online identity relatively easily, seek out information on individuals using only very limited information on hand, and facilitate relationships with individuals through social media generating a new and thus dangerous form of criminal stalking behaviour - cyberstalking (Piotrowski and Lathrop, 2012).

The seriousness of cyberstalking through social networking sites are further supported by research reports done by The Electronic Communication Harassment Observation (ECHO) of University of Bedfordshire, and cybercrime reports by Symantec Corporation, a famous security solutions provider. According to Maple et al. (2011) from ECHO, the most common persecution ground for cyberstalking is social networking sites, and the finding is not surprising at all as it was reported by Norton (2012) that 36% of social network users had accepted friends' requests from people they do not know in social networking sites. In 2011, The Guardian reported that cyberstalking is now more common than real-world stalking (McVeigh, 2011). Hence, privacy and security issues become even more vital for users to understand.

Even though cyberstalking incidents are on the rise worldwide, but there is no specific Malaysian law that governs or criminalises stalking and harassment behaviours, and it's time for the Malaysian government to start looking into this issue before it's too late, said Leong (2014), an Advocate and Solicitor of the High Court of Malaya and Chairman of the Kuala Lumpur Bar Information Technology Committee. Leong cites that "Many victims suffer in silence as they tend to ignore their stalkers and hope that they go away. Sometimes this works, sometimes is does not". He further added that it is difficult to determine whether such acts amount to harassment due to the lack of a legal definition by the law.

While earlier study in Malaysia had looked at the psychological and behavioural effects on victims that had been previously cyberstalked, this study looks at how Facebook usage characteristics relates to cyberstalking victimization among young Malaysian Facebook users. In order to better understand the problem, the researcher categorised cyberstalkers into three categories, which are unintentional, mutual friends, and stranger cyberstalkers. Three case scenarios have been formed to outline the possible risks faced by Facebook users.

1.2.1 Case Scenario 1: Unintentional Cyberstalkers

Meet Melissa, a girl who currently has 400 friends on her Facebook, and when given a friend request from stranger, she would certainly accept the offer. Melissa had recently broke up with her boy-friend, however, due to nostalgia reason, she constantly check her ex-boyfriend's activities on Facebook. As things stand now, she can watch his activity from afar, never commenting, just viewing. She checks his page every few hours to see recent updates and note his presence at local bars, restaurants, or stores. She takes no action other than annoyance. She is the unintentional cyberstalker, choosing to view her ex's activities because she has not yet moved on; however, she is still a stalker in the traditional sense of the word.

Melissa is also a low-activity Facebook user. She posts important events, shares random funny dog photos, and will tag herself at locations on girl's night out. Her actual activity is limited, but her posts are highly relevant to her current situation. She believes she has her privacy settings on the above-average security, but has not checked since the beginning of the year because she is unaware of any Facebook changes that would actually have an impact on her Facebook usage. Currently, all 400 friends can see her activity, where she tags herself, and who she tags herself with.

1.2.2 Case Scenario 2: Mutual Friends Cyberstalkers

Melissa's friends can see everything she does on Facebook, and so can people who are not her friends if they are friends of her friends. For example, she tags herself with a friend, Alison, who has 500 friends online. All 900 friends (plus Melissa's original 400 friends) now know that Melissa and Alison are having dinner together. From there, should one of Alison's friends comment or like the post, all friends of that friend can now see that activity as well. The limits to activity viewing are almost exponential at this stage. They might be limited by Alison or Melissa's privacy settings as to action they can take on the post (e.g., liking, sharing, commenting), but they still have access to the activity itself.

Now, consider Melissa's stalker. He does not need to be friends with her to see any activity of relevance, he only needs to be a mutual friend, or a friend of a friend, to see into her life. He can watch from afar, not breaking any actual laws, and certainly not gaining her attention, because he has the power of

Facebook's social network on his side. With Melissa's current privacy settings, a cyberstalker can gain enough information to be satisfied watching their mark.

1.2.3 Case Scenario 3: Stranger Cyberstalkers

Alex, who is not a friend of Melissa's Facebook network, decided to stalk and hunt her down using Facebook messenger app. Alex can message Melissa through Facebook even though they are not friend, if Melissa happens to reply his message through Facebook messenger app with location sharing setting on, Alex can actually get hold of Melissa's exact location on a map, and can use the information to find her in real life.

Also, as previously mentioned, Melissa tends to accept friend requests from people she does not know. Out of the 400 friends on her friend list, 70 are strangers, now they have access to everything she posted on her profile.

1.3 Research Objectives and Hypotheses

The main objective for this study is to examine the relationship between Facebook usage characteristics and cyberstalking victimization among young Malaysian Facebook users. Five objectives have been identified for this research:

1. To determine the relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users

2. To determine the relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users
3. To determine the relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users
4. To determine the relationship between the use of "Public" privacy settings and cyberstalking victimization among young Malaysian Facebook users
5. To determine the relationship between gender and cyberstalking victimization among young Malaysian Facebook users

Five hypotheses are formulated based on the objectives identified above:

H1: There is a significant relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users dissemination

H1a: There is a significant relationship between the use of location tagging features and cyberstalking victimization among young Malaysian Facebook users

H1b: There is a significant relationship between the use Facebook Messenger app without turning off location sharing and cyberstalking victimization among young Malaysian Facebook users

H2: There is a significant relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users

H3: There is a significant relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users

H4: There is a significant relationship between the use of "Public" privacy settings and cyberstalking victimization among young Malaysian Facebook users

H5: There is a significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users

1.4 Scope of Work

The scope of this discourse focuses on Facebook as it is currently the world's number one and most visited social networking sites (Alexa, 2014a; Discovery Communication, 2012; EBiz MBA, 2014). It is easily justified that why Facebook is chosen as there are a lot of statistics available and consider the fact that Facebook is also Malaysia's number one most visited social networking site (Alexa, 2014b). This research will only focuses on the geographical region of Malaysia.

At the same time, in attempt to fill the void in the area of cybercrime within Malaysia, this research will look into a narrow type of cyber-abuse known as cyberstalking; as most past research in Malaysia focuses on the psychology of the victims and cyberstalkers, rarely considering the relationship between usage characteristics of users on platform that allowed and even aided the situation. Below are the summaries of the scope set for the study, the reasoning behind each of the scopes will be elaborated in chapter 3.

Scope of the research:

- This research only focus on geographical region of Malaysia
- This research only focus on Facebook users who are citizens of Malaysia
- This research only focus on one social networking site that is Facebook
- This research only focus on respondents whose age group is between 20 to 30 years old
- This research did not include or consider incidents of corporate cyberstalking

The scope of work include:

- Perform a detailed literature review
- Collect primary data from young Malaysian Facebook users in Malaysia through survey and analyse it with the aid of statistical analysis software - SPSS
- Critical review and further discussion of primary data collected

1.5 Novelty of the Research

The only published academic research in Malaysia that touches on the relationship between social networking sites and incidents of cyberstalking is “Cyber Stalking: The Social Impact of Social Networking Technology” by Haron and Yusof (2010). However, it is a qualitative research that focuses more on finding the psychological and behavioural effects on victims that had been previously cyberstalked. In contrast, the current study attempts to collect data on the usage characteristic of Malaysian Facebook users who aged 20 to 30 years old, and to study whether is there any relationship between their Facebook usage characteristics and the likelihood of them receiving attacks from cyberstalkers.

1.6 Conclusions

This chapter clearly demonstrates that social networking has become a major facet of life, and it has irrevocably transformed the way people communicate and disseminate information. However, no matter how great a new technology is, there is always a downside of it. For social networking, the rise of privacy concerns is among the most notable.

Overall, this research aims to study the relationship between the usage characteristics of young Malaysian Facebook users and cyberstalking victimization. The research findings could raise awareness for Facebook users or users of other social networking sites to better protect themselves with privacy settings and through “safer” usage characteristics, at the same time provide proper guidelines to shield users from cyberstalkers.

1.7 Dissertation Structure

This dissertation is comprised of five chapters. Chapter 1 outlines the introduction and background of the study by providing the problem statement, research objectives and hypotheses, scope of work and novelty of the research.

Chapter 2 reviews the literature on existing theories, articles, incidents, concepts and researches which are related to the current study. This chapter presents on several topics which include overview of social networking sites and its progression, overview of cyberstalking, the impact of social networking on cyberstalking, overview of Facebook and its features that pose privacy and security risks, cyberstalking incidents and the increased amount of smartphones users. Then, hypotheses for this study were formed from the findings of this chapter. The formulated hypotheses are then tested in chapter 4 and the results discussed in chapter 5.

Chapter 3 covers the research methodology used by the study by presenting the research methods, population, sampling method, data collection methods, procedures and data analysis. This chapter also lists the independent and dependent variables of the hypotheses testing.

Chapter 4 analyses the data collected from the research samples through self-administered questionnaires. The data analysis is done using SPSS (Statistical Package for Social Science). The findings are then presented through several topics including the demographic profile, results of data analysis and results of hypotheses testing.

Chapter 5 presents the discussion of the research outcomes in relation to past studies and literatures, at the same time responds to the research objectives. This chapter also gives an overall conclusions for the study through several sub topics ranging from research contributions, general recommendations on cyberstalking prevention, limitations of the study, along with recommendations for future study.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, a series of literature review will cover on several correlated topics in regard to the research. The following section provides a broad overview of social networking sites, affording particular attention to accurately contextualizing Facebook within the broader dimension of social networks. It also helps to find out factors that may affect Facebook users to receive attacks from cyberstalkers.

This chapter contains a series of literature reviews covering the following topics:

- Understanding social networking sites
- The progression of social networking sites
- Facebook security and privacy concerns
- Cyberstalking
- Impact of social networking sites on cyberstalking
- Facebook features that pose privacy and security risks
- Actual cyberstalking incidents
- Advancement of smartphone technology and its impact
- Related studies

2.2 Understanding Social Networking Sites

While all social networking sites fall under the categorical umbrella of social media, not all forms of social media are social networking sites; these terms are often used inaccurately as interchangeable. Social media can be framed as file-sharing sites such as YouTube or Instagram, micro-blogging sites such as Twitter, community gaming sites such as World of Warcraft, and social networking sites such as MySpace or the far more popular Facebook (Bajrektarevic, 2012; Lin et al., 2012; Moo, 2013). Lin et al. (2012) cite that Facebook is the most exponentially growing social networking site in the world, with global membership mounting to 500 million from 350 million in less than seven months in 2010. Founded less than one decade ago, Facebook has become a genuine force in human social communication, with behavioural patterns of particular interest to researchers in a wide range of fields.

In conceiving of social networking's impact on the global community, it is critical to highlight the ways in which communication is affected by these networks. Lin et al. (2012) cites that Web 2.0 technology permits the creation and fluid exchange of information. User-generated content then allows for communications to be multi-directional in the online space. The same author further cites that "because of the intrinsic nature of humans, users are not likely to exhibit a single or simple behaviour. Thus, the understanding of features of individual users' behavioural patterns in social media is of immense importance…" (p. 201). A study by Brandtzæg and Heim (2009) has identified twelve reasons why people use social networking sites, which are listed as follows:

1. **New relations:** seeking new relations and the opportunity to meet new people.
2. **Friends:** to keep in touch with close friends and acquaintances.
3. **Socializing:** allows people to share experiences in general, making small-talk and commenting on each other's profile.
4. **Information:** access to information about products or services, learn new things, and keep up-to-date with real world social events.
5. **Debating:** the ability to express one's opinions and thoughts, and to discuss different things with people you know and do not know.
6. **Free SMS:** get access to free SMS (short messaging service).
7. **Time-killing:** is great at passing time.
8. **Sharing/consuming content:** is a great platform to share and view pictures and videos about others and themselves.
9. **Unspecified fun:** respondents reporting "fun" without describing any particular reason.
10. **Profile surfing:** the ability to search and browse other users' profiles.
11. **Family**: to keep in touch with family members
12. **Other:** any others things not listed above such as curious about other cultures, promoting and publishing their own work, marketing their own businesses.

Lafferman (2012) cites that social media cannot be framed as similar to other web-content, as it creates communications which are entirely divergent from those which characterized the internet prior to Web 2.0 technology. Social media is unique, with internal privacy mechanisms one of the key traits of social networking sites such as Facebook; this renders examination of criminal behaviours on these sites particularly pertinent if the sites are simultaneously boasting privacy settings as a key feature and yet facilitating cyberstalking behaviour. Lafferman (2012) describes these privacy mechanisms in relation to other distinguishing features of social media as follows:

> One distinguishing feature is that social media has internal privacy mechanisms. These mechanisms give the user a range of privacy options, from making all of their information publicly available to restricting access to an exclusive group of predetermined users. The ability to limit access on social media differs from the generally open nature of the Internet. While private blogs and web pages may offer this opportunity to users, these forums do not offer another distinguishing social media characteristic: the sheer number of people participating in a structured online community with each user possessing identical web capabilities. The third difference between social media and other Internet platforms is the public expectations of these forums. Many see social media platforms as an extension of their social life in the material world. These three dissimilarities create a unique challenge for applying the public figure doctrine in the social media context (p. 202).

The evolution of social networking sites has been fuelled largely by these distinguishing features, with the exponential growth of Facebook membership during recent years highlighting how Facebook, additionally, diverges from other social networking sites. The following section explores the progression of social networking sites toward their current role in the twenty-first century.

2.3 The Progression of Social Networking Sites

Social networking sites have shifted considerably since their inception, marked generally by progression toward significantly greater user membership;

this, in turn, has allowed social networks to become integral to political campaigns, large-scale social and political movements in the developed and developing world alike, and the creation of a global community concerned with human rights and sustainability issues (Banerjee and Dey, 2013; Lafferman, 2012). Cocheo (2009) asserts that social network's current role in the economic dimension is paramount, with organizations forced to engage regularly in social network in order to sustain competitive advantage. Stuart (2014) highlights that while social networking technology has not advanced substantially since the advent of social media in general, it has been exponentially increasing popularity that has fuelled the changing impact had by the media on society; the same author suggests that as millions of users engage in social networks, criminal behaviour on these sites will continue to increase.

Riedel (2008) cites that the conditions which drive internet safety have not evolved at the same rate as social networking's popularity; this has allowed for cyberbullying, cyberstalking, and other incidences of cyber abuse to continue to increase. Like stalking, bullying is a longstanding behaviour that has affected human society historically, but the nature of social networks has transformed the ease with which these behaviours are carried out (Riedel, 2008). The evidence suggests that 25% of high school students between 2006 and 2007 knew someone who had been cyber-bullied, with 32% of the same population admitting to communicating something hurtful on social networks (Riedel, 2008).

In another study, Agosto et al. (2012) mention that while the evidence regarding the danger of social media for vulnerable populations may be slightly exaggerated, it remains that these environments do require a new form of defensive behaviour: “As a whole, research is converging to suggest that although there are indeed privacy and security risks associated with social media use, they are not markedly higher than the risks of most everyday activities in the offline world” (p. 40). The same authors characterized cyberstalking as a falling under the categorical umbrella of cyberbullying, as do harassment, denigration of character, impersonation, and exclusion. The authors cite that the same protections had by social networking sites such as Facebook against one of these behaviours will impact all of them, with similar social forces behind the behaviour itself. Overall, the progression of social networking toward the support of broad, social networks and mounting worldwide membership has created changes in access for criminals to victims. The following section explores the dominant security and privacy concerns relative to Facebook, specifically, affording particular attention to attempts to counter privacy issues.

2.4 Facebook Security and Privacy Concerns

Concerns regarding Facebook’s security and privacy issues are not new; they surfaced generally in parallel with the advent of the site (Mathiyalakan et al., 2013; Williams et al., 2011). Facebook emerged as an effort to promote exclusivity within social networks via Web 2.0 media; this was unique as other sites such as MySpace allowed broad access to user profiles and very minimal privacy protections. Mathiyalakan et al. (2013) cite the following as rationale for their examination of privacy issues on Facebook:

> Research shows that Facebook profile data tends to mirror the user's actual traits rather than an idealized version of the self. Such usage of Facebook can lead to unwanted information disclosure that can be harmful to the user if proper privacy settings are not used. In effect, a user could share private information such as name, address, contact information, gender, birthdate, views and affiliations with everyone without intending to so (p. 44).

Facebook's privacy settings permit users to control access to their information, with a common criticism of the site being that default options permit too-open access to user profiles and promote vulnerability for those who do not know how to control their privacy settings (Mathiyalakan et al., 2013; Williams et al., 2011). In 2012, a study by U.S. magazine Consumer Reports revealed that out of the 188 million Facebook users in the U.S., 13 million of them have never put any effort in protecting their own private information (e.g., birthdate, love life drinking habits, and sexual preferences) they shared on their Facebook profile; of the 13 million, approximately 3.25 million users had their privacy settings set to Public, meaning they are displaying their data to everyone, not just their friends and family; 4.8 million users had posted status sharing how and where they would be spending their day, exposing themselves up to the risk of burglary (Wrenn, 2012).

Ardito (2003) cites that privacy settings on Facebook are informed significantly by economic motives, as user preferences, or “likes” are publically available information. Marketing revenue is a substantial profit stream for the site, and the default privacy settings may well be linked to marketing motives. Ardito (2003) highlights that several cases of cyber-abuse on Facebook have been linked to information brokers, or those who seek out information regarding people, businesses, and other entities in order to sell the information or data for profit.

2.5 Cyberstalking

Prior to examination of the literature focusing upon the aforementioned issues, it is crucial to accurately define cyberstalking, a recently developed behavior which was birthed in parallel with the World Wide Web. In order to clearly understand what cyberstalking is, one must first comprehend its traditional form - offline stalking. According to Lewis et al. (2001), the behavior of stalking has been reported back in the 19th century. Mullen et al. (2004) describe stalking as a course of conduct by which one person repeatedly inflicts on another unwanted intrusions to such an extent that the recipient fears for his or her safety.

With the continuing advances in technology and the introduction of Internet to the public, it has given stalkers a new platform to stalk their victims, thus given rise to a new form of stalking which is cyberstalking. There is a wide range of cyber-abusive behaviours, with cyberstalking receiving the most attention in empirical research due to its impact on younger, vulnerable populations (Piotrowski and Lathrop, 2012). Piotrowski and Lathrop (2012) describe cyberstalking as follows:

> Cyberstalking has emerged as a new form of stalking…. Cyberstalking is largely viewed as inappropriate, unwanted social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices. The proliferation of smartphones and social networking has exacerbated the incidence of cyberstalking, and related cyber-abuse behaviours, over the past 5 years (p. 535).

Besides the above mentioned, there are a lot more definitions available for cyberstalking. Bocij (2004) provides a coherent and comprehensive definition of cyberstalking by citing it as:

> A group of behaviours in which individual, group of people or organization uses information and communication technology (ICT) to harass another individual, group of people or organization. These behaviours include but not limited to the transmission of threats, false accusations, identity theft, data theft, and damage to data or equipment, computer monitoring, solicitation of minors for sexual purposes or any form of aggression (p. 14).

Perhaps, a simpler definition of cyberstalking would be the use or aid of any electronic communications or tracking technologies to stalk or harass another person (Hensler-McGinnis, 2008). However, it must also be made known that the term cyberstalking is often used interchangeably with cyberharassment and cyberbullying due to the fact that all three misuse digital technology to inflict unwanted torment to victims (Maple et al., 2011).

Besides the aforementioned cyberstalkers' attacks, Commander Dave Pettinari from Pueblo County Sheriff's Office had further listed threats that one might faces from cyberstalkers, which includes but not limited to: unsolicited email, threatening or hostile messages, spreading vicious rumours, impersonation of the user online, electronic sabotage which includes sending viruses or malware, vandalism of property and physical attack in real life

(Pettinari, 2002). This is similar to cyberstalking activities defined by Cyber Security Malaysia (2014a), which includes threatening messages, death threats, sexual harassment, slander, or any form of harassment. Furthermore, former U.S. Attorney General Janet Reno cites that cyberstalking is usually “a prelude to more serious behaviour, including physical violence”, at times, cyberstalking can lead to stalking in the physical world (Rouse, 2007).

In another report, Piotrowski and Lathrop (2012) cite that research highlighting the nature of cyberstalking has profiled the typical cyberstalker; he or she is educated, tending to perform well academically, over the age of sixteen, and prone to internet addiction. Also, the most typical cyberstalker and cyberstalking victim is a college student, with the researchers highlighting that evidence from nations external to United States borders regarding this type of criminal behaviour is very limited (Piotrowski and Lathrop, 2012). On the other hand, a study by the National White Collar Crime Center (NWCCC, 2013) has discovered that typical cyberstalkers are similar to traditional stalkers in that most are male with mood disorders and histories of substance abuse. Victims are very typically female, with most victims having a history of face-to-face contact with their stalkers. While cyberstalking emerged prior to social media, the role of social media in facilitating cyberstalking is notable (Piotrowski and Lathrop, 2012).

Although cyberstalking is not as serious as physical crimes like murdering, raping, and robbing, but it may causes long term psychological trauma that includes physical and emotional reactions. Some of the effects identified by Cyber Security Malaysia (2014a) are: changes in sleeping and eating patterns, depression, anger, nightmares, anxiety, helplessness, fear, shock and disbelief. The above mentioned distresses are hard to detect in the earlier stage as victims might often choose to ignore it. The same firm also reported that cyberstalking related incidents in Malaysia saw an increase of 41.4% from 300 incidents in year 2012 to 512 incidents in year 2013 (Cyber Security Malaysia, 2014b).

Similarly, a research report by Maple et al. (2011) prove that cyberstalking had in some cases, caused victims to lose their jobs due to poorer job performance at work, lost touch with friends and family or gave up social activities, at worst gave up on their current relationship. Cyberstalking has also place burden on victims financially as they are being forced to move to different houses or pay additional fee for better security measures. Similarly, another study published by Nobles et al. (2012) found similar results in which they state that the trauma faced by victims of cyberstalking is greater that of physical stalking in the long run as the victims reported that they had to gradually increase protective measures such as take additional time off; change or quit a job or school; avoid relatives, friends or holiday celebrations; and change their email address. Even more, the study also revealed that the financial costs associated with victimization of cyberstalking are much higher for cyberstalking victims, with an average dollar value of more than $1,200 spent compared to about $500 for traditional stalking victims (Nobles et al., 2012).

2.6 Impact of Social Networking Sites on Cyberstalking

Cyberstalking is promoted through online venues like Facebook due to their information sharing mechanisms that provide access to friends of friends, who the original user may not even know. A research by Maple et al. (2011) from University of Bedfordshire has found that social networking sites are the most common prosecution ground for cyberstalking activities. According to Perry (2012), there are 150 settings in Facebook that are directly related to security, and it is important to note that default Facebook security settings can increase the potential for stalking and put victims at greater risk.

Delaney (2012) and McClure (2010) identified that social media is not only a staple in the modern person's life, but that people give access to their information without considering the consequences of sharing to a larger audience. Indeed, "technological change does not occur within a social vacuum and social upheaval in the face of technological change is not new. Some of this change is undesirable, it has usurped powers and enforced mind-sets that a fully attentive culture might have wished to deny it" (Basu and Jones, 2007). At the same time, cyberspace brings together the potentially exciting cocktail of technology, and its unique group of users, within the context of anonymity and an environment lacking in consistent norms. While the potentially democratizing effect is to be welcomed, the potential for perverse activity is not (Basu and Jones, 2007).

The situation was worsen by Facebook's decision to introduce 'Check-In' service in 2010 that allowed users to check-in their current locations using mobile devices and the ‘check-in’ will appears as a News Feed on user’s Timeline (Gross and Hanna, 2010; Sharon, 2010; Singel, 2010). The introduction of this feature raises several controversies, as Perez (2010) claimed in her article “Nearby Friends: New Cyber-Stalking App for Tracking Facebook Places Check-Ins” that this feature will become a new tool for cyberstalker to take advantage of as they can now get the location information of their victims more easily.

Even though Facebook argues that this feature will only display the check-in information to user’s own friends and not everyone, yet, having one’s profile set to private makes little difference if the user is allowing strangers to access their profiles and information. As study has shown that 36% of users accepted friend requests from people they do not know in social networking sites (Norton, 2012). Even more specifically, a study into the habits of UK Facebook users revealed that 51% of users have accepted friend requests from people they do not know in Facebook, exposing themselves to cyberstalkers (Wrenn, 2012). Purcell (2012) advised users of social network to resist the urge to check-in regularly as this will give cyberstalkers an insight of one’s daily habits. She also mentioned that Facebook’s Timeline allows cyberstalkers to seek back entire online history of users, including the early days where users are less social media savvy.

An incident happened in the United States clearly demonstrated that simply accepting friend request can turn a person’s life into turmoil. In 2013, Becky accepted a friend request from an unknown person named Pashayan but she never realize that Pashayan was stalking her Facebook posts all the time and he would showed up at parties that Becky posted on her Facebook that she will be attending (Silva, 2014). Becky continued to receive numerous physical and mental harassment until the Los Angeles City Attorney's office filed charges against Pashayan for stalking and violating restraining order (Silva, 2014).

Cyberstalking has long been "gaining the attention of the media and the public as the nature of the crime incorporates elements of new technology and threatening behaviours, which symbolize a new form of threat" (Ogilvie, 2000). In reality, cyberstalking is a threat that most people are not aware of until it is too late – their information has been shared, they have been tagged at too many locations or too many of their friends are friends of friends of the stalker. The insidious nature of the cyberstalker is that with Facebook, and with users who do not understand what can happen when they tag themselves willingly at locations without regard to who can see that information, users put themselves at great risk with every post due to the nature of security and privacy settings on the social networking site.

2.7 Facebook Features That Pose Privacy and Security Risks

Facebook's most important features are the user's wall, or also known as "Timeline", status update, news feed, and notifications, all of which facilitate actions between those who are "friends" on the site. Posing the greatest security risk are the default privacy settings on Facebook and the ability of "friends" to not actually be members of the individual's social network, be able to see his or her postings through friends of friends mechanism; as the typical user on Facebook has hundreds of friends and very often only knows most of them casually. The cases of cyberstalking have highlighted, additionally, that the messaging capability that is permitted to any Facebook user who does not specifically change his or her privacy settings allows for negative communications to be sent. Mensch and Wilkie (2011) cite that security risks on social networking sites will persist, as human advancement in criminal behaviour tends to occur more rapidly than security protections against the behaviour.

Frequently highlighted as a threat to Facebook users and undoubtedly a significant issue with respect to cyberstalking is the location-specific features of the site which allow for users to be readily located; these included geo-location tagging or check-in feature and Facebook messenger app sharing user's location by default. These features allow for individuals to be located when in their friends network, with research suggesting that merely having only friends be able to use these location features is not a sufficient barrier to victimization (Gilchrist, 2010).

As for Facebook messenger app, it is even more deceptive in the sense that it automatically shares the user's current location on a map to anyone she is chatting with while using her smartphones, and it also easily provides the person she is chatting with the exact direction to her precise location, and worst the function is turned on by default (Murphy, 2012; Pannoni, 2014; Song, 2013). By that, cyberstalkers can track down his or her victim with ease. Even worse, starting from August 2014, Facebook declared its Messenger app as mandatory for all mobile users who wishes to use the chat function on Facebook, this will certainly lead to a massive rise of Facebook Messenger app users in the near future (Cutlack, 2014; Page, 2014).

Gilchrist (2010) highlights these location features, which recommends friend requests to be sent when there are mutual friends between the users, does not take into account whether the users actually know each other, with a significant number of users simply accepting most friend requests. Gilchrist (2010) cites that the location features in conjunction with the mutual friends feature render Facebook a particularly fertile area for cyberstalking due to compromised privacy issues associated with these features. Thus, CNN (2014) recommended Facebook users to only share their location to a customized list of people they feel comfortable with, in order to minimize the potential stalking factor from cyberstalkers.

On the other hand, Perry (2012) cites that default Facebook security settings can increase the potential for stalking and put victims at greater risk. Thus, Facebook recommended its users to use the extra security features provided, one of the good example is the ‘Login Approvals’ feature. Once turned on, the user will be asked to enter a special security code each time he attempts to access his Facebook account from a new computer or mobile phone (Facebook, 2014b). This is very useful is the sense that, if a cyberstalker anyhow found a way to obtain a user’s Facebook credentials, he or she will still not able to take over the user’s Facebook account, as the special security code can only be obtained from the user’s own mobile phone or email address.

Hane (2012) argues that increased regulations must be instilled external to Facebook itself, as the internal mechanisms for accountability and security protections are insufficient. In making recommendations for how to address the most dominant security risks on Facebook and other social media, the same author suggests that it is information access which must be addressed, with significant data on Facebook publically available and thus potentially publically owned. The following section explores specific cases of cyberstalking that have been linked to privacy issues both on and off Facebook during recent years.

2.8 Actual Cyberstalking Incidents

The Association of Independent Information Professionals (AIIP) emerged in 1989, grounding their principles in a code of ethics stipulating that honesty and confidentiality are paramount and no projects should be accepted that compromise the integrity of the profession (Ardito, 2003). Prior to the advent of Facebook, the most publicized case of cyberstalking was related to information brokerage, with Remburg v. Docusearch case, with the latter party successfully sued after Amy Boyer was cyberstalked, shot and killed by her former high school classmate in 1999 through information obtained from Docusearch, an information brokerage company (Ardito, 2003). O’Brien and Torres (2012) cite that Facebook made its most recent changes to privacy settings in 2010 in order to combat the ability of criminals to garner information about users, but East Carolina University (ECU, 2012) refuted Facebook's claim by saying these changes have not been particularly effective in combating cyberstalking.

ECU (2012) mentions that Facebook permits cyberstalking through several features despite privacy settings; these include the ability to trace the user easily through status updates. ECU (2012) cites that recent cases of cyberstalking have included the posting of sexually offensive images, attaching spyware to emails, and generally tracking victims by becoming "friends" with the victim and using posted information to trace him or her. ECU (2012) further mentions that recent cases include an incident within which a fifty year-old man was rejected by a young woman, with him retaliating by posting her information garnered through social networks all over the internet. In another case, a Federal agent was charged with cyberstalking when he made use of a Department of Homeland Security (DHS) database to track the activities of an ex-girlfriend. Finally, a case of cyberstalking on Facebook occurred through which an ex-boyfriend solely used the social network to track his ex-girlfriend and send her continuously threatening messages before posting nude photographs of her online (ECU, 2012).

Ironically, the Facebook account of Mark Zuckerberg, the company's co-founder and CEO, was actually hacked in December 2011, as 14 private photos of his were leaked to a photo sharing site with the headline "it's time to fix those security flaws Facebook" (Burnham, 2011). In the same year, Mark Zuckerberg was cyberstalked on his own social networking site by a 31 years old man, Pradeep Manukonda, in which Zuckerberg claimed that Manukonda bombarded him with messages through Facebook, emails, and handwritten notes (Daily Mail, 2011; THR, 2011). The reports also revealed one of the Facebook messages Manukonda sent to Zuckerberg, which consists of chilling words such as “I owe my entire life at your service. Please help me, then I am ready to die for you. Please understand my pain”.

In 2009, Shawn Memarian pleaded guilty to stalking a woman he had dated for just over one month, with the stalking lasting over two years; during this time, the stalker posted the victim’s personal information routinely, citing that she performed sexual favours (NWCCC, 2013). In 2012, James Allen used Facebook to demand communication from multiple young women, asserting that if they did not send him nude photos of themselves, he would target their family members maliciously (NWCCC, 2013).

In Malaysia, perhaps the better known cyberstalking incident was that of Lee David Clayworth, a former Vancouver teacher who had a relationship with then 29 years old Malaysian citizen Lee Ching Yan. According to a CNET report, their relationship lasted for only a few months, after they broke up in 2010, his ex-girlfriend stole his computer and hard drive and proceed to post naked pictures of him online. She also accused Clayworth as a paedophile and enjoyed sexual relationships with his underage students (Matyszczyk, 2013).

2.9 Advancement of Smartphone Technology and its Impact

The internet is not the only technology advancing in the 21st century, but as well as smartphone. Rapid growth of smartphone in the past ten years has been witnessed by everyone. A smartphone is a combination of mobile phone and classic PDA, but focusing more on mobile phone part. Basically, it has advanced functions like email, internet connection, built-in camera, storage for information and many more. In recent years, most of the smartphones come with the touch-screen capability, but some still come with classic keypad.

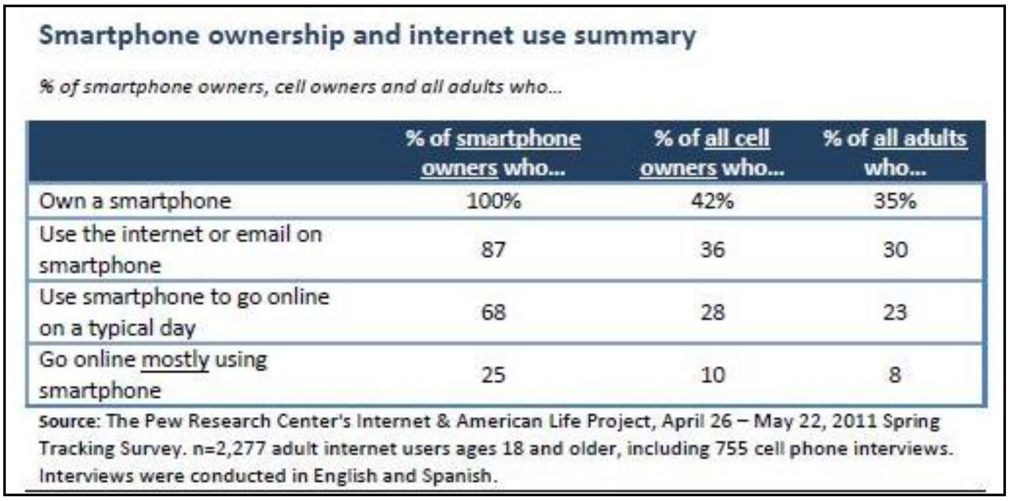
Do et al. (2011) identified smartphone is having a speedy growth is partly due to its increase functionalities such as GPS, Bluetooth, accelerometer, microphone, camera, web browser and others. Etherington (2011) has a different point of view and claimed that the popularity of smartphone is possibly made by the entertainment features. It would be difficult to define the growth speed of smartphone in the modern world; thus, experts compared it with other technology developments. “Smart phones, after a relatively fast start, have also outpaced nearly any comparable technology in the leap to mainstream use”, reported by DeGusta (2012) in his article, “Are smart phones spreading faster than any technology in human history”.

“There are many reasons consumers are using the mobile Web now more than ever. For one, carriers are offering a flat-rate mobile data plan, which makes subscribing to these services more affordable. New 3G networks are also making accessing the mobile Web much faster”, a reason provided by Reardon (2008) in her article on why web browsing on smartphone is getting popular.

Besides, consumers wish to have full web access on their smartphone, which cause the growth in the mobile browser market. It is obvious that consumers have started to browse the web with their smartphone since few years back. According to statistics and facts from GO-Gulf (2012), they discovered:

- 5 billion mobile phones in the world, and 1.08 billion of it are smartphones
- 89% of the smartphone users used their phones throughout the day
- 47% are female, and 53% are male
- Top three activities for smartphone are texting (92%), internet browsing (84%), and emailing (76%).
- 25-34 age group have the most smartphone users

At the same time, a study by the Pew Internet Project (Smith, 2011), showed raw statistics collected from 2,277 Americans, conducted from April 26 to May 22, 2011 (see Figure 2.1).



Smartphone ownership and internet use summary

% of smartphone owners, cell owners and all adults who...

	% of smartphone owners who...	% of all cell owners who...	% of all adults who...
Own a smartphone	100%	42%	35%
Use the internet or email on smartphone	87	36	30
Use smartphone to go online on a typical day	68	28	23
Go online mostly using smartphone	25	10	8

Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey. n=2,277 adult internet users ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish.

Figure 2.1: Survey from the Pew Internet Project

Source: Smith (2011)

The outcome of the Pew Internet Project's survey is similar to statistics from GO-Gulf.com. Internet browsing and emailing are the top activities for Americans. Furthermore, 25% of the respondents use smartphones to go online instead of computers and laptops. It can be clearly seen that smartphones with sophisticated functions are starting to replace computer in consumers' daily life.

Additionally, The Week (2012) magazine reported that Cisco estimated number of smartphones and tablets used worldwide by 2016 is 10 billion. In 2016, each person on this earth will own 1.4 smartphones. These numbers could be good news for cyberstalkers as the more people have access to smartphones means higher chances of them checking-in or tagging themselves or their friends in places they went.

A research was conducted by International Data Corporation (IDC) on a total of 7,466 respondents aged between 18-44 years old in the Unites States, and the report revealed some staggering numbers on smartphone usage on Facebook. A study by IDC reported that smartphone users check his or her Facebook 13.8 times a day averagely using their smartphones (Levitas, 2013). Furthermore, the average daily time spent on Facebook by smartphone users is 33 minutes, and Facebook is dominant when it comes to the total time spent on social and communication activities on a smartphone, it which Facebook makes up one out of every four minutes.

The development of smartphone is a big leap for human technology; it certainly does bring positive impact to human daily, also, relationship among people are getting better and closer as it brought conveniences to communications. Nevertheless, such a development could be a double-edged sword; it brought several concerns to modern society, and also provides new platforms and opportunities for cyber criminals to commit crimes.

2.10 Previous Research on Facebook Security and Privacy Risks

In order to further understand this topic, three highly accredited studies had been identified and thoroughly reviewed:

- Facebook: Threats to Privacy (Jones and Soltren, 2005)
- Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization (Henson et al., 2011)
- An Exploratory Study of User's Facebook Security and Privacy Settings (Hoffmann, 2012)

A significant amount of research has been done in the area of Facebook privacy and security risks. The first ever research performed on Facebook's security and privacy issues was by Jones and Soltren in 2005, the time when Facebook was still not available to the public. At that moment, only universities in Canada and United States have access to Facebook. The motivation behind the study is that Jones and Soltren noticed users constantly shared their personal information on Facebook, but there are no previous academic research specifically aim at the privacy and security within the site. In their research "Facebook: Threats to Privacy", Jones and Soltren (2005) discussed and identified privacy and security threats faced by Facebook users in the form of viruses, malware at the same time exploring vulnerability of Facebook website itself.

They employed two methods of data collection. First, they conducted a survey on 419 Massachusetts Institute of Technology students, seek to collect user's usage patterns and knowledge or understanding on Facebook's features. Second, through data mining on Facebook site from University of Oklahoma, New York University, Harvard and MIT using self-written computer scripts. After collecting data, they analysed it using aggregate statistics. This study used a threat model to identify and analyse certain privacy and security risks on Facebook, then made recommendations to Facebook for each identified threat.

From the study, they stated there are three principal factors that undermined privacy on Facebook: "users disclose too much personal information, Facebook does not take adequate steps to protect user privacy and third parties are actively seeking out end-user information using Facebook" (Jones and Soltren, 2005). The research also concluded that "mistakes on privacy will continue to occur and lasting change will only come from a gradual development of common sense regarding what is appropriate to post in social networking sites" (Jones and Soltren, 2005). This study from Massachusetts Institute of Technology also demonstrated it is possible for anyone to actually harvest large amount of profile data from Facebook site directly using information collection system during that period of time.

There are other study similar to Jones and Soltren such as Hoffmann's (2012) "An Exploratory Study of User's Facebook Security and Privacy Settings" where user's perception on privacy and security settings were analysed. The author collected data through surveys, Facebook screenshots and journal logs. Questionnaires were distributed to students at Minnesota State University, it was intended to collect information to measure the user's attitudes and beliefs on roles and responsibilities of Facebook privacy and security. The data collected is then analysed using T-Test. Hoffman (2012) concluded that the average Facebook users do not realize the importance of cyber security and will only pay close attention to their Facebook settings after they have fallen victim to an attack. Also, the study also found that Facebook users who utilized custom privacy settings are less vulnerable to privacy attack than those who are using default settings.

Third study was done by Henson et al. (2011). Instead of examining user perceptions of privacy and security issues, they aim to examine the link between social network privacy and security towards online victimization that includes unwanted harassment like cyberstalking. In doing so, this study attempted to answer three questions: "Does the use of privacy settings protect users from online interpersonal victimization", "does allowing strangers access to social network profile information increase the likelihood of users experiencing online victimization", and lastly "do other security related behaviours influence one's likelihood of being victimized online".

Researchers used web-based survey and invitation was sent by email to a simple random sample of undergraduate college students. The authors surveyed fellow students by asking them if they had ever experienced any harassment behaviours through social networking sites. The researchers then divided key independent variables into three main categories which consist of demographic information, basic social network information and social network security information. The study indicated approximately 42% of social network users experienced some kind of interpersonal victimization before. There were a few major findings from this study. First, females are two times more likely to experience online interpersonal victimization. Second, the more number of daily updates on one's online social networks will increase the odds of online victimization. Lastly, person who accepted stranger's friend request are 2.6 times more likely to be victimized.

2.11 Tools to Perform Statistical Analysis

There are significant amount of statistical analysis software available in the market to assist researcher. Three statistical analysis software have been identified and the reason for choosing these packages is because they are well known and most frequently used by statisticians or others in commercial and scientific research.

- SPSS (Statistical Package for the Social Sciences) Statistics by IBM Corporation
- Minitab by Minitab, Inc
- SAS by SAS Institute

First and foremost, SPSS is one of the most widely used statistical package in the market. It was first developed by researchers at Stanford University as a tool to help them with quantitative research by turning raw data into useful information for decision making (SPSS, 2009). SPSS is easy to learn and easy to use because it has a menu-driven graphical user interface that enables pull-down menus thus users can specify or change data attributes by just several clicks without the need of complicated programming languages (Tuffery, 2011). A review by Kennesaw State University (2013) also agreed to the point that SPSS is user friendly because it's "point and click" orientation and is one of the most preferred packages among non-statisticians. However there are also downside for SPSS whereby it lacks behind SAS and Minitab on the measurement of association between response variable and predicted probabilities, discordant, tied pairs and number of concordant. (Ibrahim, 2001).

The second software is Minitab which was developed by statistics professors of Pennsylvania State University to aid students in repetitive calculations so that they could focus more on their analyses result (Minitab, 2013). Similar to SPSS, Minitab's is a user-friendly statistics package (Ibrahim, 2001; Lee et al., 2000). Minitab combined the user friendliness of Microsoft Excel with the ability to perform complex statistical analysis (Arora and Mahankale, 2012). Besides, Minitab has the strongest graphics and visualization capabilities compared to other statistical analysis packages (Kennesaw State University, 2013). Minitab is most often used in Six Sigma, the world's leading quality improvement methodology (Minitab, 2013). Though with several advantages, Minitab lacks behind SAS for not able to provide c-correlation value (Ibrahim, 2001).

Lastly, SAS by SAS Institute which is considered as the most complete statistical analysis software on the market and is the choice of most applied statisticians (Ibrahim, 2001; Kennesaw State University, 2013). It is powerful as it can delivers all the above mentioned limitations of SPSS and Minitab. However, due to the fact that SAS uses scripting language to perform manipulation of data therefore it requires hard work and longer learning curve for new users (Ibrahim, 2001; Kennesaw State University, 2013).

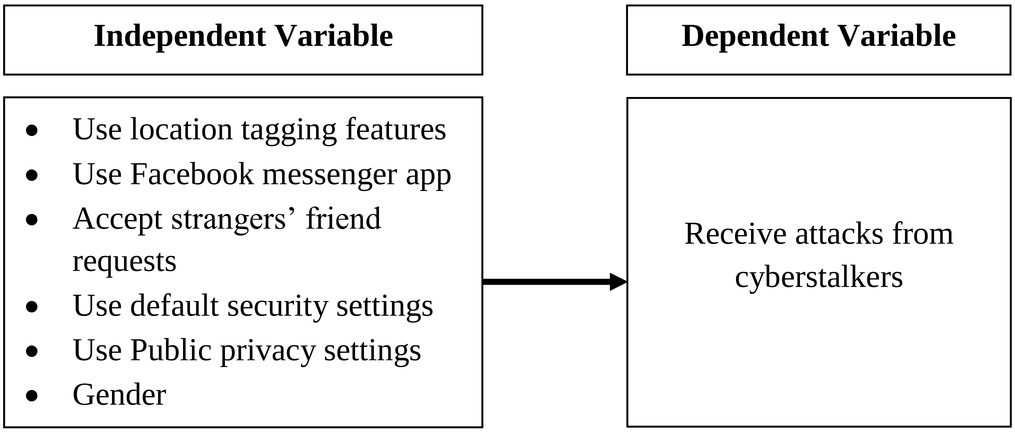
In conclusion, SPSS and Minitab are easier to use compared to SAS as both of them require little to no programming knowledge to operate. SPSS is also good for social sciences research as it was initially developed for that purpose. Though SAS is a very powerful statistical analysis software, it requires users to understand programing language in order to fully utilize its features.

2.12 Conclusions

The purpose of the literature review is to study what are the factors that can put Facebook users on risk for cyberstalking attacks. Through literature review, it was made known that cyberstalking is very real and the number of cases are on the rise every year. Furthermore, it was found that the effect caused by cyberstalking can be severe and may causes long term psychological trauma in both physical and emotional pain.

Based on the literature review, the factors that exposed Facebook users to the risk of cyberstalking attacks are identified and listed in Table 2.1.

Table 2.1: Independent and Dependent Variables for the Study



Independent Variable

- Use location tagging features
- Use Facebook messenger app
- Accept strangers' friend requests
- Use default security settings
- Use Public privacy settings
- Gender

Dependent Variable

Receive attacks from cyberstalkers

Table 2.2 below shows the literatures which supported the factors listed above, and the research hypotheses (alternate hypotheses) formulated based on the factors identified.

Table 2.2: Summary of Research Hypotheses and Supporting Literatures

Research Hypotheses Formulated	Supporting Literature

H1: There is a significant relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users	CNN (2014);
	Gilchrist (2010);
	Perez (2010);
	Purcell (2012);
	Song (2013)

H2: There is a significant relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users	Henson et al. (2011);
	Silva (2014);
	Wrenn (2012)

H3: There is a significant relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users	Perry (2012)

Table 2.2 (Continued)

Research Hypotheses Formulated	Supporting Literature

H4: There is a significant relationship between the use of “Public” privacy settings and cyberstalking victimization among young Malaysian Facebook users	Hoffmann (2012);
	Mathiyalakan (2013);
	Williams et al. (2011)

H5: There is a significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users	Henson et al. (2011); NWCCC (2013)

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

The purpose of this section is to demonstrate the actions taken in order to achieve all the research objectives detailed in chapter 1. Included in this chapter will be the research methods, population size, sampling method, data collection and analysis methods and procedures, and the tools that are used to perform statistical analysis. The methods discussed herein were chosen based upon their ability to provide the answers to the research.

3.2 Research Methods

A quantitative research approach has been chosen to study the usage characteristic of young Malaysian Facebook users. According to Muijs (2004), quantitative research is especially suited to test hypothesis formulated for a particular study. Therefore, the primary reason for choosing quantitative approach for this study is because it allows the researcher to test hypotheses formulated for the study. Secondly, the outcomes of quantitative research can be used to enable generalizability to the population studied as quantitative approach involves a large number of respondent samples (Baines et al., 2010).

As such, it is suitable to use this approach for the current study as the research outcomes can be generalized to the target population.

In order to conduct quantitative research, a survey research method is employed for the study. According to Leedy and Ormrod (2005), survey research involves acquiring information about one or more groups of people, perhaps about their characteristics, opinions, attitudes, or previous experiences, by asking respondents several questions and tabulating their answers. The ultimate goal of survey research is to learn about a large population by surveying a sample of that population (Leedy and Ormrod, 2005).

From the definition declared above, survey research method is suitable to be used for this particular study as the survey aims to collect data on the frequency of users using Facebook features that is deem a threat to privacy, the likeliness of users to accept friend requests from strangers, the level of privacy setting users set for their Facebook account (i.e., Public, Friends or Custom), and whether users have modify their security settings to better safeguard themselves from cyberstalkers. The method of data collection is through online self-administered questionnaire which allows the researcher to collect raw data from a large sample size with minimal cost and shortest time possible.

3.3 Population

This research aims to collect data on the usage characteristic of young Facebook users in Malaysia, and to study whether is there any significant relationship between their Facebook usage characteristics and them receiving attacks from cyberstalkers. A recent news article reported by Borneo Post indicates that 13.3 million (45.5%) of the total population in Malaysia are Facebook users (Mahadi, 2013). It is evident that the amount of Facebook users in Malaysia is high, however, the scope would be too broad for the research if it includes all Facebook users in Malaysia, and it will be virtually mission impossible to study all of them.

In order to reduce the scope, the targeted age group of the population is set at 20 to 30 years old. The reason to focus on this particular age group is based on the data obtained from Malaysian Communication and Multimedia Commission (MCMC). In their recent report, the combined percentage of users from the age group of 20 – 29 proved to be the biggest group of internet users in Malaysia (MCMC, 2014). In another similar report, MCMC (2012) conveyed that the average age of smartphone users in Malaysia is 29.3 years old, and the age group of 20 – 29 is the largest percentage of smartphone users in Malaysia at 33.1%.

Even though Piotrowski and Lathrop (2012) mentioned in their study that college students are the most typical cyberstalking victims, but they have also highlighted that evidence from nations external to United States regarding this type of criminal behaviour is very limited. Also, the reports displayed by Cyber Security Malaysia regarding cyberstalking incidents only showed the total number of incidents, without providing any information regarding the characteristics of the victims.

Based on the information evidenced above and the unavailability of data to precisely specify the typical age group and characteristics of cyberstalking victims in Malaysia, the researcher decided to set the target population as Malaysian citizens, aged between 20 to 30 years old, whom at the same time are also Facebook users.

3.4 Sampling Size and Method

According to Pickard (2007), sampling is very important for a research because it is not possible or even practical to survey the entire targeted population in the study. Hence, a subset of the population will be selected for this research, as Leary (2008) cites that researcher can learn about a population by analysing a relatively small sample of individuals.

This research employs the non-probability sampling method. Zikmund and Babin (2006) mentioned that in non-probability sampling, the probability of any particular member of the population being chosen is unknown, meaning the samples are gathered in a manner that does not ensure each member of the population has an equal chance of being selected, and the samples selected rely heavily on the personal judgment of the researcher. Nevertheless, Adler and Clark (2007) cite that this sampling method is useful when the researcher has limited resources or an inability to identify all the members of the population. Wimmer and Dominick (2013) further suggest that the usage of this method is not totally oblivious to the sampling frame as it still provides the researcher with sufficient information needed to accomplish the research objectives.

There are three major types of non-probability samplings available, which are: convenience sampling, quota sampling and purposive sampling (Leedy and Ormrod, 2005). Purposive sampling is used for this study as all respondents were selected for a particular purpose, relevancy to the study and the sample frame. According to Neville (2007), purposive sampling enables the researcher to use his or her judgment to choose people that are presented or are available that best meet the objectives or target groups of the study.

The use of purposive sampling method is appropriate for this study for the following reasons: 1) Even if the population size is broken down to cover only young Malaysian Facebook users who aged 20 to 30 years old, it is still impossible to obtain a full list of them due to the large amount of users, it will be very time consuming and costly to use random sampling for this study. 2) There is time limitation as the researcher is required to complete the research project within two trimesters. 3) High numbers of sample size (300) required for this study, hence, the responses must be collected in the fastest time possible in order for the researcher to have sufficient time to analyse, run statistical analysis and present the discussion in regards to the collected data.

As for sample size, a guideline by Gay and Airasian (2003) clearly states that if the population size is at 5,000 units or more, a sample size of 400 should be adequate. Apparently, this research has both resource and time constraints. First, the research is not funded by any sponsors, thus, there is no funds available to be used as incentives for respondents to improve the response rate. The first constraint is unexceptionally true as study by Göritz (2006) has concluded that “incentives promote response and retention rate in online surveys”, he further elaborate by stating incentives increased the odds of a person responding by 19% over the odds without incentives, whereas incentive also increased retention rate by 4.2%. Secondly, the time constraint is due to the fact that the researcher must complete the research within two trimesters. Owing to reasons stated above, the researcher set the sample size of the study at 300.

3.5 Data Collection Methods and Procedures

A survey data collection method through self-administered questionnaire is used for this study. The reason in choosing questionnaire for data collection is because it is a quicker, more convenient and less expensive way of collecting data from multiple people simultaneously (Hillier and Jameson, 2003).

The purpose of the questionnaire is to collect required data from respondents in shortest time possible and at minimal cost. The following subsections describe how the researcher develop, design, test and distribute the self-administered questionnaire.

3.5.1 Questionnaire Development

Before deciding on which online survey tool to be used for the study, the researcher had explored on several well-known free online survey software. After much trial and error, the researcher had decided to proceed to develop the questionnaire using Google Forms, a free online survey tool established by Google. There are several reasons for choosing Google Forms, while most of the renowned online survey tools offer free-to-use option, they usually limit the maximum amount of questions and responses allowed. Google Forms allows free users to create and collect up to a maximum of 255 questions and 200,000 responses, as compared to other free online survey tools which offered a maximum of 10 questions and 100 responses for free users. This is particularly important as the study aims to collect 300 responses.

Besides, only Google Forms permits the use of "skip logic" in questionnaire for free users, whereas the "skip logic" function will only be made available to paid users for other online survey tools. Last but not least, Google Forms also supports "questionnaire logic" which allows the researcher to set questions as "required question", meaning when respondents accidentally missed certain questions, he or she will not be allowed to proceed further and a notification sign will be displayed to inform the respondents in regards to which questions he or she missed, this will completely eradicate the issue of missing data during collection.

3.5.2 Questionnaire Design and Measurement

The developed questionnaire as appended in Appendix A consists of five sections and has a total of 22 questions. Most of the questions are adopted from the study of Hoffmann (2012) and modified to better suit in providing answers to objectives of this research. The questionnaire uses structured questions which consist of both closed-ended and open-ended questions whereby respondents could further express and elaborate on their answers.

The first section (Section A) of the survey questionnaire aims to collect data from the respondents in regards to their actual usage of Facebook. Section B concerns on the usage characteristics of certain Facebook features such as check-in feature, Facebook Messenger app, and the likeliness of them accepting friend requests from strangers, using 5-point Likert scale, moving from a range of Never, Rarely, Sometimes, Often, to Every time. Section B also collects data on cyberstalking attacks experienced by the respondents.

In the subsequent sections (Section C and D), respondents were asked to select the current privacy and security settings of their Facebook account, respondents were also requested to give their perception on cyberstalking. The last section in the survey questionnaire was used to collect demographic data of respondents which include age, gender, level of education, states living in and industry they are working in.

3.5.3 Questionnaire Validity and Reliability Test

Development of a valid and reliable questionnaire is important to ensure there is no measurement error (Radhakrishna, 2007). Hence, the questionnaire for this research had gone through both validity and reliability testing. To enhance questionnaire validity, Radhakrishna (2007) has suggested to carry out a readability test using Gunning Fog Index to measure and improve the readability of English writing.

The Gunning Fog Index was developed by Robert Gunning in 1952, it is a test designed to measure the readability of English language in a document (Landau, 2011). The "Fog Index Number" indicates the numbers of years of formal education that a person requires in order to easily understand the text on his or her first reading (Landau, 2011). The main idea behind the calculation of the Gunning Fog Index is to locate and count those words with three or more syllables. According to Landau (2011) and ESD (2011), texts that are designed for a wide audience generally require a fog index of less than 12, whereas texts that require near-universal understanding ought to have an index of 8 or less.

The researcher applied the Gunning Fog test on all questions of the questionnaire using two Gunning Fox Index calculators from "readability-score.com" and "gunning-fog-index.com". The reason for using two different calculators is because the indexes returned are slightly different due to distinctions in the text-processing algorithm behind each calculators. The "Gunning Fog Index" obtained from both calculators are then compiled and the mean value of each questions are demonstrated in the Table 3.1 below.

Table 3.1: Gunning Fog Index of Questionnaire

Questions No.	Gunning Fog Score/Index
Q1	11.5
Q2	3.6
Q3	3.6
Q4	8.6
Q5	5.6
Q6	8
Q7	7.3

Table 3.1 (Continued)

Questions No.	**Gunning Fog Score/Index**
Q8	15.3*
Q9	9.9
Q10	6.8
Q11	8.5
Q12	10.7
Q13	8.5
Q14	5.7
Q15	5.6
Q16	4
Q17	12
Q18	1.6
Q19	1.6
Q20	8.2
Q21	14.2*
Q22	13*

*. Gunning Fog Index that exceeds 12

Out of twenty two questions, only three questions have Gunning Fog Index of more than 12 (i.e., Q8, 21 and 22). After reviewing those questions, the researcher noticed that two of them are demographic related (i.e., Q21 and 22), and the other (i.e., Q8) being slightly longer but it is specifically Facebook usage related question. After considering the fact that the targeted samples for this study are Facebook users between the ages of 20 to 30 years old, hence, the researcher assumes that the respondents have sufficient English proficiency and literacy in terms of Facebook features to comprehend the actual meaning of the questions.

By that, a pilot test has been carried out on 20 individuals to observe whether the respondents are able to comprehend all the questions listed in the questionnaire. As mentioned by Gideon (2012), running a pilot test on the questionnaire before distributing it to all samples is important as it allows the researcher to detect mundane errors such as typos, grammar mistakes, jumbled question order, numbering or unnecessary repetitiveness in questions. This will allow the researcher to make appropriate amendments to the questionnaire as required.

From the pilot test, all feedbacks collected have been taken into consideration. The comments collected regarding the readability are all fairly positive, some of the remarks given are “the questions are easy to understand”, “very straight forward” and “simple and easy to understand”. There is not a single respondent who commented negatively in regards to the readability of questions. Still, despite all the positive comments, the researcher had corrected some grammar, vocabulary and typographical errors found after the pilot test. Next, the researcher proceeds to test the reliability of the questionnaire by measuring the Cronbach’s alpha value.

Data collected from the pilot test were analysed using SPSS to find the reliability coefficient (Cronbach’s alpha). According to Andrew et al. (2011), Cronbach’s alpha is a popular method to measure the internal consistency in questionnaire, it works by measuring how well a set of variables or items measures a single, one-dimensional latent construct. In simple words, Cronbach’s alpha is best used to measure items that are intended to measure the same construct. Also, Cronbach's alpha is most relevant and commonly used when the test is evaluating a single factor using multiple Likert scale questions to determine if the scale is reliable (Leroy, 2011; Vogt et al., 2014). Vogt et al. (2014) further added that if the questions are actually correlated to each other in measuring a same factor, the Cronbach's alpha value should be above 0.70, if not, then it is probably the case where the questions are not really measuring aspects of the same thing, and the questions should not be summed up to make an overall rating scale.

Due to the nature of the questionnaire for this study, there are only two items in the main construct that are measuring the same factor using Likert scale, which is in question six. Thus, the Cronbach's alpha test was performed on the data collected for that particular question. A reliability coefficient of 0.70 or higher is considered acceptable reliability (Radhakrishna, 2007; Vogt et al., 2014). The Cronbach's alpha obtained for question six is 0.767, which exceeded the minimum acceptance level of 0.70 (see Table 3.2, for full analysis result, refer to Appendix C). The results of Cronbach's analysis indicate that this part of the survey questionnaire is reliable and well-constructed. After the ensuring the questionnaire's validity and reliability, the researcher proceeds to distribute the questionnaire to all targeted samples.

Table 3.2: Cronbach's Alpha Coefficient for Survey Question Six

Research Construct	Cronbach's Alpha Coefficient
Usage Characteristics of Facebook Location Tagging Features	0.767

3.5.4 Questionnaire Distribution

As aforementioned in section 3.4, this study employed the purposive sampling method. Therefore, the researcher distributes the survey link of the questionnaire to all targeted samples through online channels via Facebook and email. The online survey form was distributed and stayed available from 6th September 2014 to 16th September 2014, where a total of 304 responses were collected at the end of the day.

3.6 Data Analysis

The data analysis techniques used for this research are descriptive and inferential statistics. Descriptive statistics involves the organization, summarization and display of data (Asadoorian and Kantarelis, 2005), it is also described by McCue (2006) as the process of categorizing and describing the information from the data collected. However, descriptive statistics do not allow the researcher to make conclusions on the hypotheses formulated for the research as it does not involve any test of statistical significance. They are just used to describe the information gathered from the survey. Therefore, inferential statistics (i.e., Binary Logistic Regression) is then used to test the hypotheses formulated for the study by determining the relationships between independent and dependent variables (McCue, 2006).

Binary logistic regression is one of the two models of logistic regression analysis. According to Anderson (1982), logistic regression analysis examines the influence of various factors on an outcome by estimating the probability of the event's occurrence. Logistic regression can examine the relationship between one or more independent variables against the dependent variable by calculating changes in the log odds ratio (Anderson, 1982). Binary logistic regression was chosen to test the hypotheses formulated for the study because it is most suitable to be used when the dependent variable is dichotomous (e.g., 0 or 1; yes or no), which the dependent variable of this study is.

Primary data from the survey are coded and analysed using IBM SPSS software. SPSS is a computer application used for statistical analysis of data, it allows for in-depth data access and preparation, analytical reporting, graphics and modelling (Flinders University, 2013). There is a general agreement that outcomes associated with probabilities of 5 times out of 100 (i.e., 0.05) if the null hypothesis were true are said to be statistically significant (Richardson et al., 2005). Therefore, all hypotheses are to be tested at a minimum of the 0.05 level of significance. Table 3.3 summarizes the null hypothesis and the statistical analysis method used to test them.

Table 3.3: Summary of Statistical Analysis Method Used in Hypotheses Testing

Null Hypotheses	Statistical Analysis Method
$H_0 1$: There is no significant relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users	Binary Logistic Regression

Table 3.3 (Continued)

Null Hypotheses	Statistical Analysis Method
$H_0$2: There is no significant relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users	Binary Logistic Regression
$H_0$3: There is no significant relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users	Binary Logistic Regression
$H_0$4: There is no significant relationship between the use of "Public" privacy settings and cyberstalking victimization among young Malaysian Facebook users	Binary Logistic Regression
$H_0$5: There is no significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users	Binary Logistic Regression

3.7 Independent and Dependent Variables

According to Anderson (2001), binary logistic regression is used to examine the influence of various factors on a dichotomous outcome by estimating the probability of the event's occurrence. It does this by examining the relationship between one or more independent variables against the dependent variable itself (Anderson, 2001). This section will present the independent and dependent variables identified for the study.

3.7.1 Dependent Variables

As aforementioned, the researcher had defined cyberstalking attacks in several number of ways, which include any or all of the following behaviours: users receiving threat or hostile messages, sexual messages, viruses or malware, account hijacked or password stolen, account used to send false accusations, vicious rumours were spread about users, identity theft or impersonation, real life physical attack or vandalism of private property. Respondents were asked if they had ever experienced these behaviours on Facebook or resulting from the use of Facebook. Each type of the behaviours were coded as a simple "yes" or "no" dichotomous variable. The "yes" responses were summed across all of the behaviours and recoded to create a single dichotomous measure of receiving cyberstalking attacks, indicating whether or not the respondents had ever experienced any of the attacks.

3.7.2 Independent Variables

There are six independent variables identified through the literature review, which are:

1. **Used location tagging features:** indicates whether the respondent has previously used Facebook location tagging features such as check-in and adding location to photos
2. **Used Facebook messenger app:** indicates whether the respondent has previously chatted with others using Facebook messenger app on his or her smartphone without turning off the location sharing setting

3. **Accepted strangers' friend requests:** denotes whether the respondent has previously added people they do not know as friends on Facebook
4. **Used default security settings:** determine whether the respondent had left his or her Facebook security settings on default
5. **Used public privacy settings:** determine whether the respondent is using "Public" privacy option as his or her Facebook privacy settings
6. **Gender:** indicates the gender of respondent

3.8 Statistical Analysis Software

A literature review has been carried out to compare three statistical analysis software under section 2.11. From the findings, IBM SPSS was selected as the statistical analysis tool to analyse data collected for the research. One of the reason for choosing SPSS is due to its popularity as it is one of the most widely used statistical package in the market, hence, there are a lot of books and articles that the researcher can refer to when using SPSS.

Secondly, SPSS is easy to learn and easy to use because it has a menu-driven graphical user interface that enables pull-down menus thus users can specify or change data attributes by just several clicks without the need of complicated programming languages (Tuffery, 2011). A review by Kennesaw State University (2013) also agreed to the point that SPSS is user friendly because it's "point and click" orientation and is one of the most preferred packages among non-statisticians.

Acock (2005) further confirmed the ease of use of SPSS software by concluding “SPSS is all you need if you are not going to do cutting edge statistical analysis. SPSS has clear advantages because it is so much like the familiar Excel spreadsheet”. Thus, SPSS is suitable for the current study as it does not require cutting edge statistical analysis.

3.9 Conclusions

This chapter presented the research methods used in conducting the study. The research methodology is the most important aspect of a research as it concerns with where and how the researcher will gather the data and analyse them to acquire findings that can provide an answer to the objectives of the study.

This study employed a quantitative survey research method which involves the use of survey questionnaire to collect data on the usage characteristics of young Malaysian Facebook users. The population identified for the study is young Malaysian citizens who has a Facebook account, and the sampling method used for the study is purposive sampling, a type of non-probability sampling method. Also, the self-administered questionnaire was pilot-tested before being distributed to target samples through online channels via Facebook and email. All data collected is then analysed using SPSS. The research methodology explained in this chapter leads to the presentation and discussion of research findings in the subsequent chapters.

CHAPTER 4

RESEARCH FINDINGS

4.1 Introduction

This chapter displays the research findings after analysing the data collected from the research samples. Three hundred responses were expected during the research design, however, a total of 304 responses were received after eleven days (sample data is appended in Appendix B). All respondents for this survey are Malaysians and all responses were obtained through self-administered questionnaires. The collected data were then analysed using SPSS and results demonstrated in both descriptive (i.e., using graphs and charts, showing frequency and percentage of usage) and inferential statistics (results of hypotheses testing).

This chapter contains a series of topics covering the results of data analysis through following titles:

- Demographic profile of respondents
- Results of data analysis using descriptive statistics
- Results of hypotheses testing using inferential statistics
- Summary of hypotheses testing

4.2 Demographic Profile of Respondents

This section provides an overview of the demographic profile of all 304 respondents. The demographic data presented here consist of gender, age, education level, states living in, and industry where the respondents are working in.

4.2.1 Respondents' Demographic Data: Gender

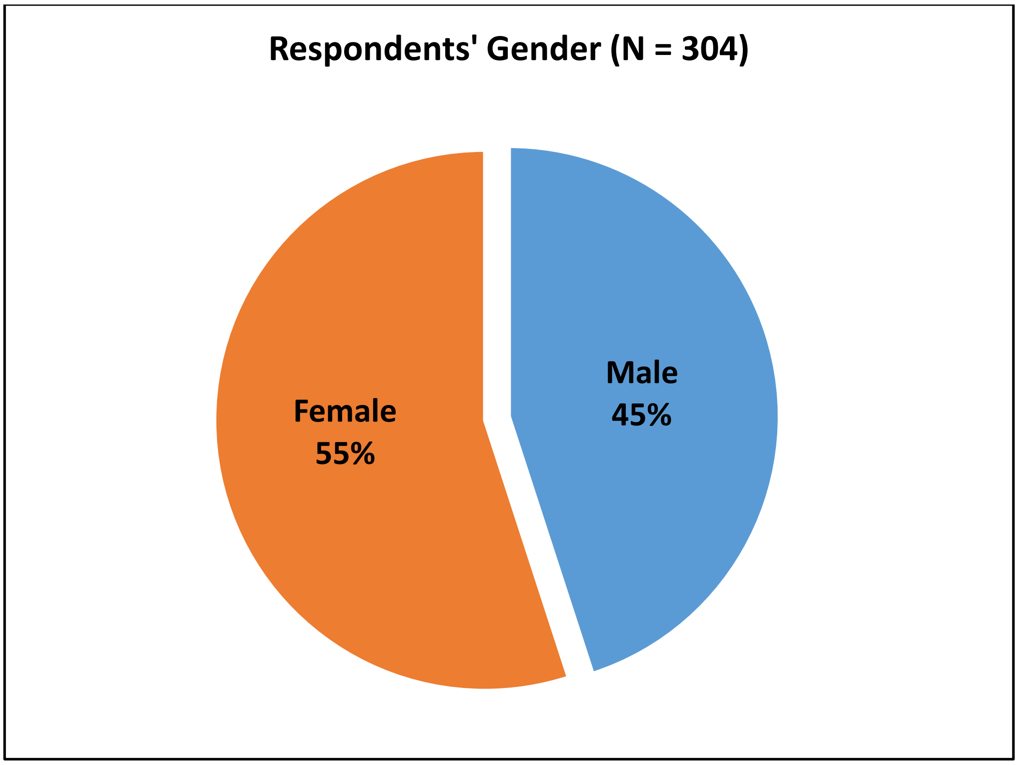


Figure 4.1: Respondents' Demographic Data – Gender

The chart in Figure 4.1 shows that of the 304 respondents, 55% (166 respondents) are female and 45% (138 respondents) are male.

4.2.2 Respondents’ Demographic Data: Age

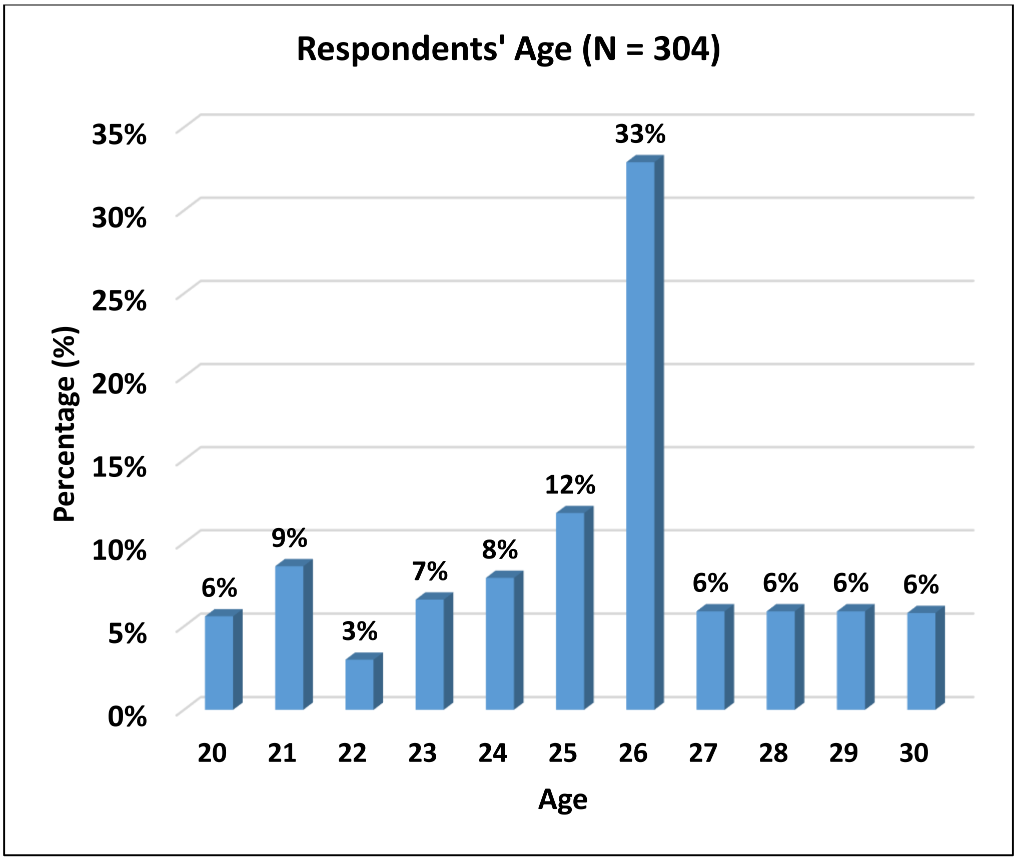


Figure 4.2: Respondents’ Demographic Data – Age

The target group for this study are young Malaysian who aged between 20 to 30 years old. Therefore, respondents were asked to select their age from a list that ranged from 20 to 30 years old. Based on the chart, the age of 26 represented the largest portion with 33% and constituted the majority of the sample. This is followed by the age of 25 at 12%. The lowest portion is the age of 22 with only 3%. The complete age distribution of the respondents is exhibited in Figure 4.2.

4.2.3 Respondents’ Demographic Data: Education Level

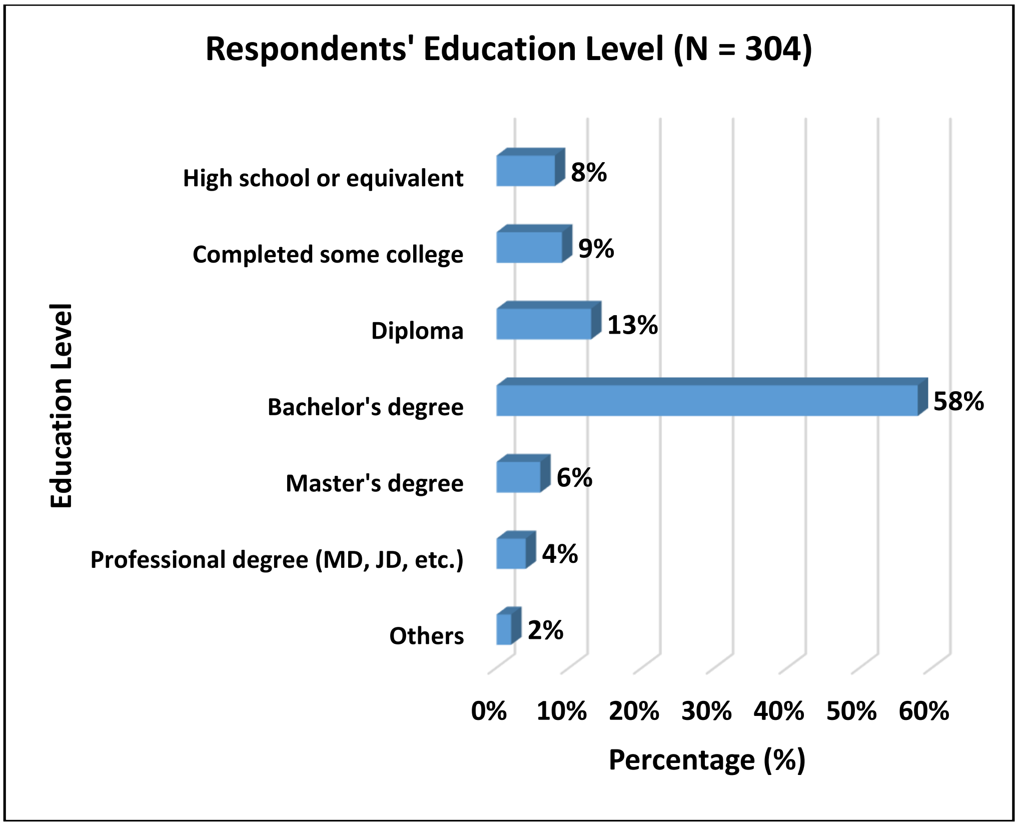


Figure 4.3: Respondents’ Demographic Data – Education Level

Respondents were asked to select their last completed year in school from a list of education levels. Majority of them are bachelor’s degree holders which consist of more than half at 58%, it is followed by diploma holders at 13%. Instead of selecting from the available list, 2% of the respondents stated their education levels as others, which are: “advanced diploma”, “A-level”, and “professional course” without further elaborating what course. Please refer to Figure 4.3 for the complete distribution about respondents’ education level.

4.2.4 Respondents’ Demographic Data: States Living In

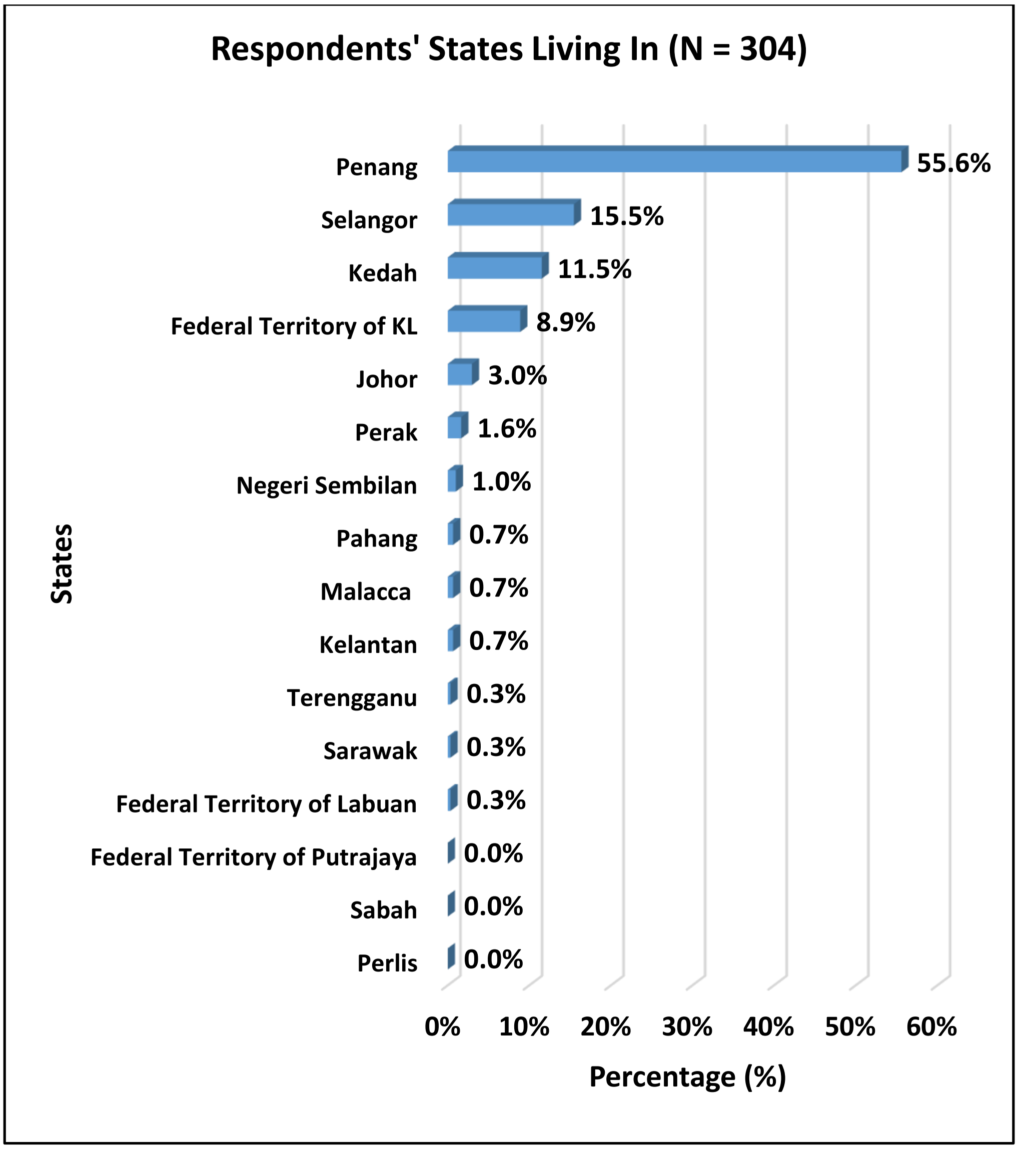


Figure 4.4: Respondents’ Demographic Data – States Living In

The states where the respondents currently lives in are displayed in Figure 4.4. From the data, it can be seen that majority of respondents came from the states of Penang, Selangor, Kedah and Kuala Lumpur. Small amount of respondents came from other states such as Johor, Kelantan, Melacca, Negeri Sembilan, Pahang, Perak, Sarawak, Terengganu and Labuan. However, it was noticed that there was no respondent that came from the states of Perlis, Sabah and Putrajaya.

4.2.5 Respondents’ Demographic Data: Working Industry

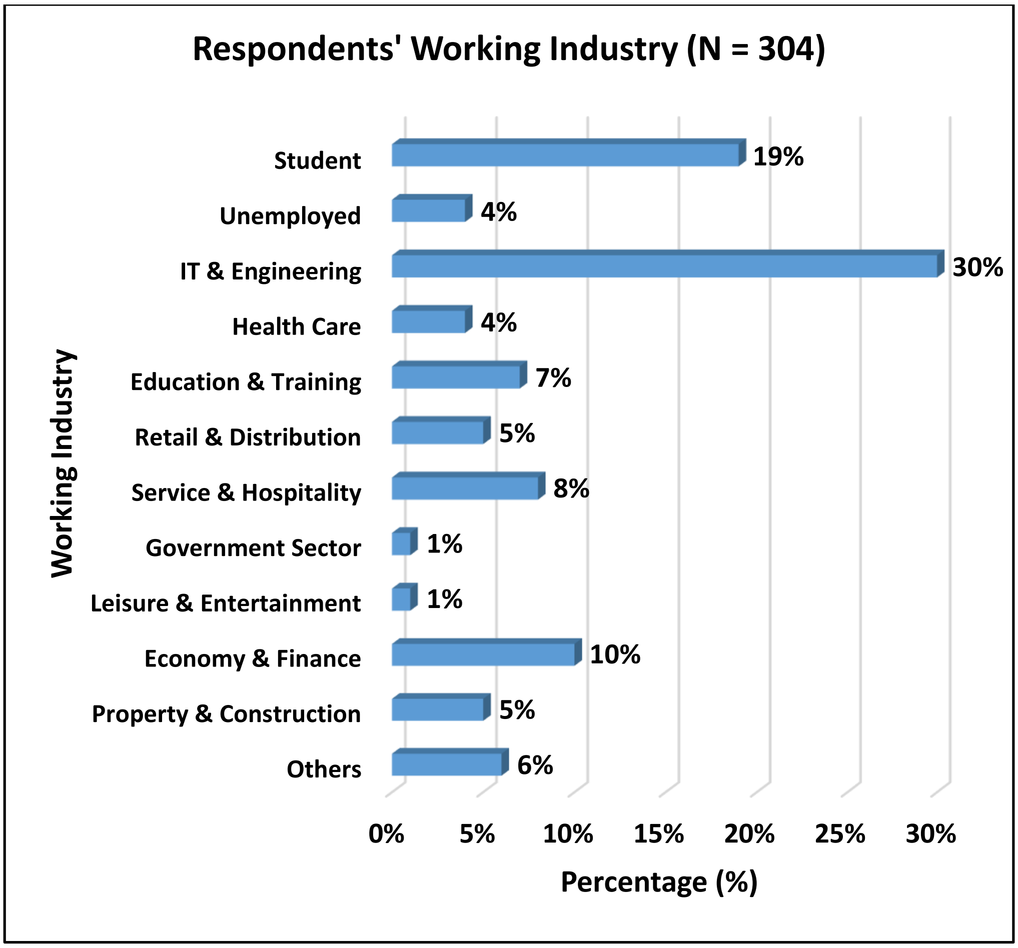


Figure 4.5: Respondents’ Demographic Data – Working Industry

Figure 4.5 shows the industry where the respondents came from. The respondents were allowed to state the industry which they are working in if the industries listed above do not fit theirs. Other industries that were specified by 6% of the respondents are: agriculture, creative design, gems and jewellery, legal, machining, manufacturing, marine, marketing, professional service, sales, publishing and secretarial.

4.3 Results of Data Analysis Using Descriptive Statistics

This section demonstrates the analysis results of all data collected from the questionnaire using descriptive statistics. The findings are categorized into five sections (Section A, B, C, D and E) and are presented as follows:

- Section A presents data about the actual usage of Facebook.
- Section B presents data about the usage characteristics of respondents on certain Facebook features, including the usage frequency.
- Section C presents data about respondents' Facebook privacy and security settings.
- Section D presents data about the respondents' perception on cyberstalking.
- Section E presents data about cyberstalking attacks received by the respondents.

4.3.1 Section A: Actual Usage of Facebook

This section displays data in regards to respondents' actual usage of Facebook, which includes: the number of times they browse Facebook per day, total amount of friends they have on their Facebook profile, reasons for using Facebook, and what information have they revealed on their Facebook profile.

4.3.1.1 Data about Number of Times Browsing Facebook

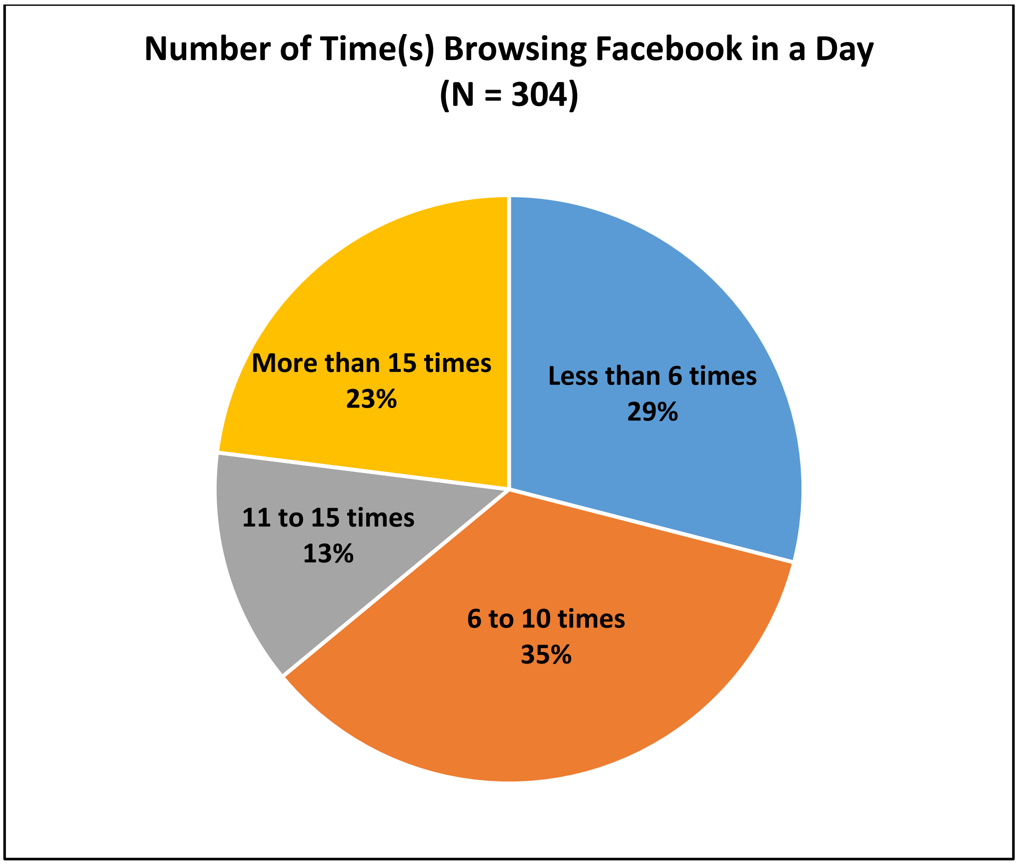


Figure 4.6: Number of Times Browsing Facebook per Day

Respondents were asked to select how many times they browse or check their Facebook in a typical day, using either computers or smartphones. The finding in Figure 4.6 shows that out of 304 respondents, 71% of them browse Facebook at least 6 times per day. 35% of them browse Facebook 6 to 10 times per day whereas 13% of respondents check their Facebook 11 to 15 times per day. Lastly, 23% respondents said that they browse Facebook more than 15 times per day.

Table 4.1 below shows that the mean value for this question is 2.30, which means that young Malaysian Facebook users check their Facebook approximately 7 times a day averagely using either their computers or smartphones. This finding clearly indicates that Facebook has indeed become a major part of life among young Malaysians. It also proved that most of the respondents are very addicted in using Facebook on a daily basis.

Table 4.1: Mean Value for Number of Times Browsing Facebook

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
NoOfTimesBrowsingFB	304	1	4	2.30	1.122
Valid N (listwise)	304				

4.3.1.2 Data about Total Amount of Friends on Facebook

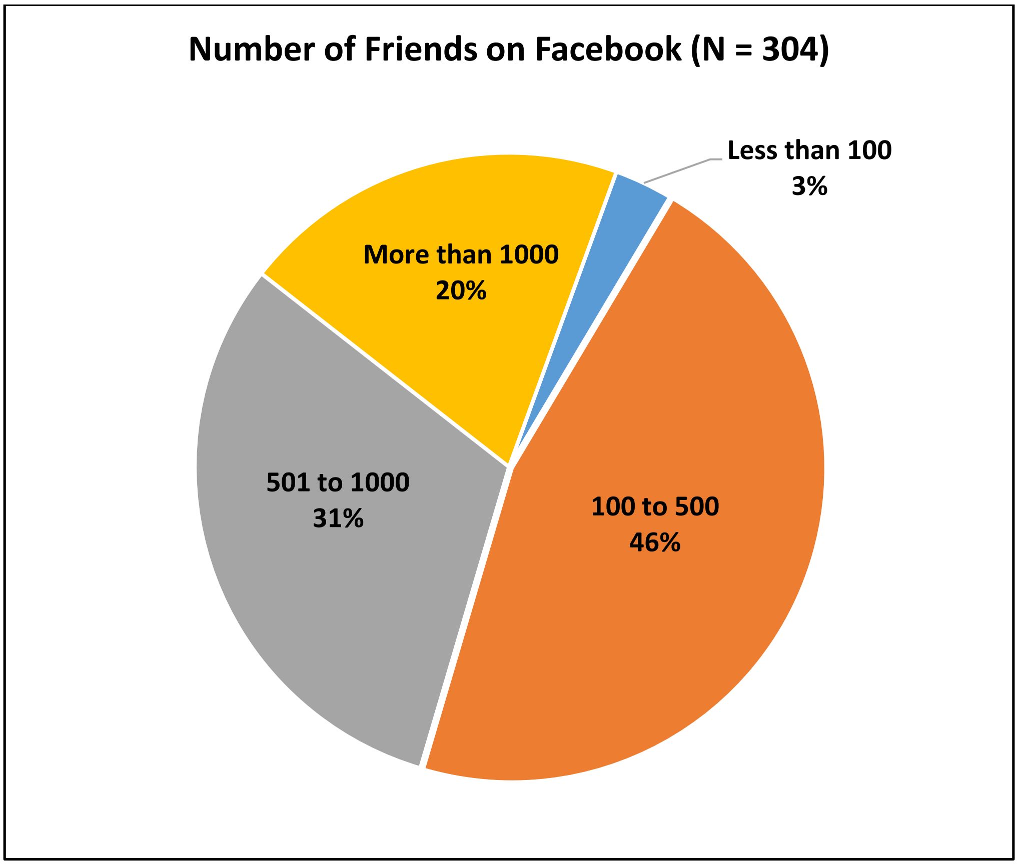


Figure 4.7: Total Amount of Friends on Facebook

Respondents were asked to select the amount of friends they have on their Facebook profile from four categories. The largest portion of the pie chart shows that 46% of respondents have 100 to 500 friends on their Facebook profile. This is followed by 31% respondents who have 501 to 1,000 friends on Facebook. Thirdly, one-fifth of the respondents have number of friends that amounted over 1,000. On the contrary, there is only a mere 3% of respondents that have less than 100 friends on Facebook. The chart in Figure 4.7 also indicates that 51% of the respondents have more than 500 friends on Facebook, and the amount will most probably be increased as time passes.

4.3.1.3 Data about Reasons for Using Facebook

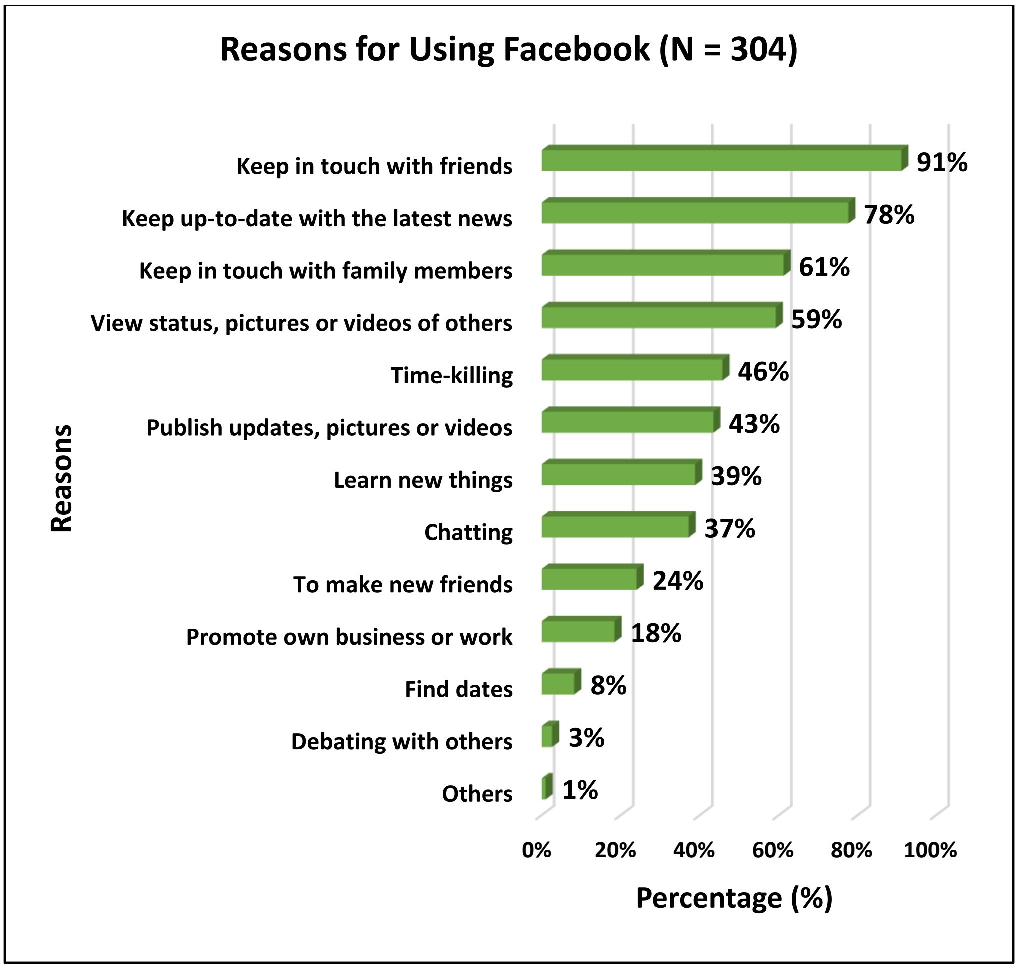


Figure 4.8: Reasons for Using Facebook

Respondents were asked to tick on all the reasons that contributed to their use of Facebook. It can clearly be seen from Figure 4.8 that 91% of respondents chose “keep in touch with friends” as the primary reason they use Facebook. This is closely followed by “keep up-do-date with the latest news” at 78%. This finding shows that besides using it to keep in touch with friends, a lot of respondents used Facebook as a source of latest news, the contributing factor to this trend can be due to the fact that there are quite a substantial amount of news agencies, both domestic (e.g., The Star Online) and international (e.g., CNN and Reuters) publishing latest news as it happens on their official Facebook page.

The third most picked reason for using Facebook is to “keep in touch with family members” at 61%, the percentage is very close to that of “view status, pictures or videos of others” at 59%. “Chatting” (37%), “time-killing” (46%), “learn new things” (39%) and “publishing new updates, pictures or videos” (43%) were among the reasons picked by respondents for using Facebook. Interestingly, only a small percentage of respondents (24%) stated that they use Facebook to “make new friends”, even less people at 8% who actually used Facebook to “find dates”. Lastly, only 3% of respondents indicated that they actually used Facebook to “debate with others”.

Besides the listed reasons, respondents were also encouraged to state whatever reasons that led to Facebook usage. Three responses were received, first respondent stated he used Facebook to “build networking” to improve his or her social intercourse. Second respondent indicated the reason as using

Facebook to “perform research”, without specifying what kind of research it was used for. Interestingly, the last respondent said he or she actually used Facebook as a platform to “cyberstalk” other people.

The finding from this is slightly different from the study conducted in Norway by Brandtzæg and Heim (2009). In their study, they found that the top reason for Norwegians to use social networking sites is to seek new relations or the opportunity to meet new people. As opposed to that, the result for this study indicated only a small percentage (24%) of young Malaysians that used Facebook to make new friends, and even less people (8%) who actually used Facebook to find dates. Thus, it seems that young Malaysians are less interested when it comes to making new friends on social networking sites. However, there is a similarity between both studies as respondents from both countries actually ranked “keep in touch with friends” as one of the top reasons for using social networking sites.

4.3.1.4 Data about Types of Information Revealed on Facebook Profile

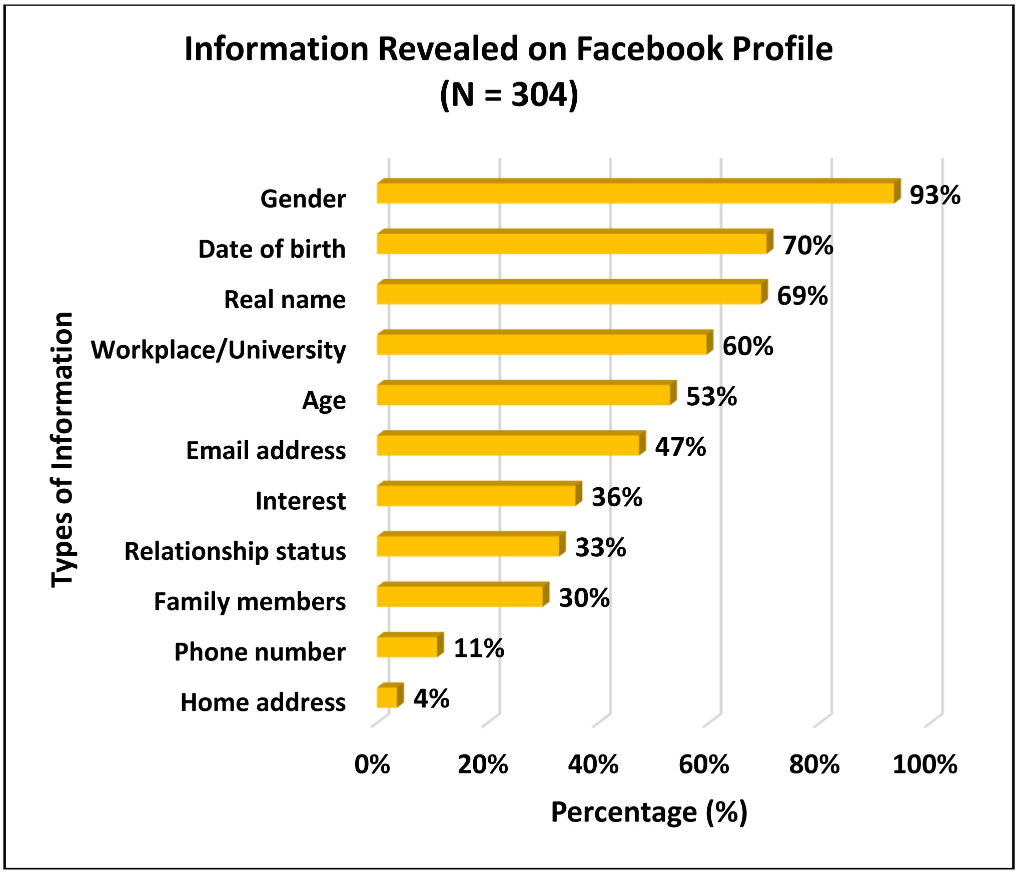


Figure 4.9: Types of Information Revealed on Facebook Profile

Respondents were asked to select from a list in regards to what types of information have they revealed on their Facebook profile. From the finding (see Figure 4.9), the most commonly revealed personal information on Facebook is gender, which was indicated by 93% of respondents. Date of birth and real name are the second and third most revealed information on Facebook profile, which were selected by 70% and 69% respondents respectively.

Surprisingly, more than half of the respondents willingly revealed information regarding to their current workplace or university and their actual age, which are 60% and 53% correspondingly. Interest (36%), family members

(30%) and relationship status (33%) are also among the types of information revealed on respondents' Facebook profile. It was also found that 47% (144 respondents) are willing to disclose their email addresses on Facebook profile, however, they are more reluctant in revealing their phone number (11%) and home address (4%), which are the two least revealed information on Facebook profile.

4.3.2 Section B: Usage Characteristics of Facebook Features

This section displays data in regards to the usage frequency of Facebook features which include location tagging features, Facebook messenger app and friend requests approval.

4.3.2.1 Data about Respondents' Frequency of Accepting Strangers' Friend Requests

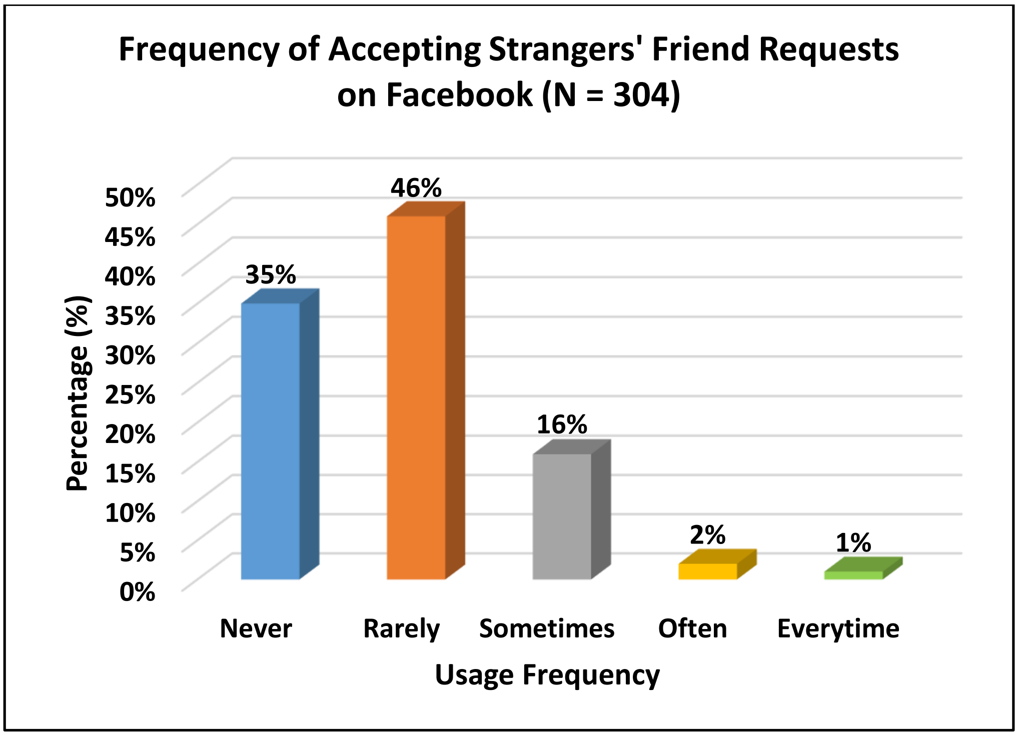


Figure 4.10: Frequency of Accepting Strangers' Friend Requests

Respondents were asked to select their frequency of accepting friend requests from people they do not know. Five options were listed for this question, ranged from Never, Rarely, Sometimes, Often to Every time. From Figure 4.10, it can be seen that “Rarely” represented the highest amount with 46% of the respondents selected this option. Then, it followed by “Never” at 35% and “Sometimes” at 16%, only 2% of the respondents chose “Often”. Lastly, 1% of the respondents chose “Every time” as their frequency of accepting strangers’ friend requests, this indicates that the 2 respondents are eager to accept friend requests from anyone, every single time.

Despite the fact that many of the respondents stated they rarely accept friend requests from people they do not know, yet, this also indicates that they had indeed added strangers as friends previously, albeit “rarely”. This finding revealed that 65% of the respondents had actually accepted friend requests from strangers. This percentage is slightly higher than the study conducted in UK by Wrenn (2012), which was reported at 51%; and even higher than the 36% reported by Norton (2012). It seems that young Malaysian Facebook users are less cautious when it comes to accepting friend requests from people they do not know.

4.3.2.2 Data about Respondents' Frequency of Using Check-in Feature

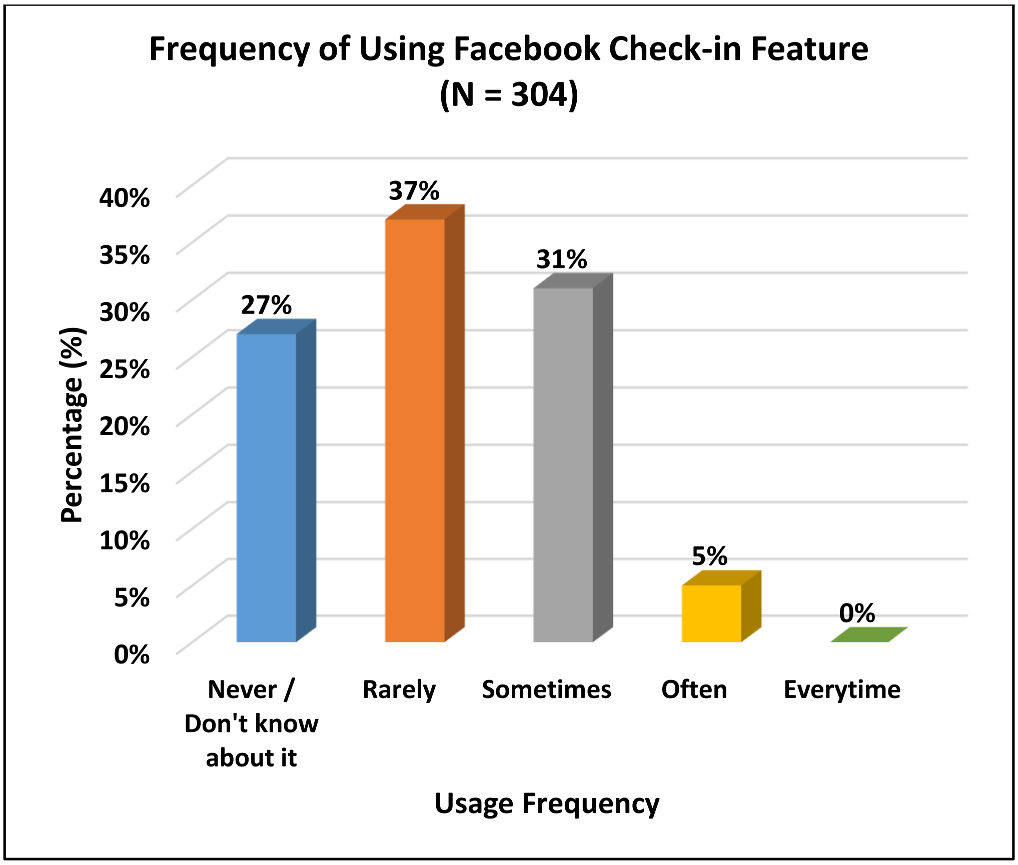


Figure 4.11: Frequency of Using Facebook Check-in Feature

When the respondents were requested to select their usage frequency on Facebook check-in feature from a scale of five, only 27% of them said that they never use or do not know about Facebook check-in feature (see Figure 4.11). Majority of them selected "rarely" (37%) and "sometimes" (31%). There is only a minor portion of respondents that selected "often" (5%). Surprisingly, there is not a single respondent that selects "every time".

4.3.2.3 Data about Respondents' Frequency of Adding Location to Photos

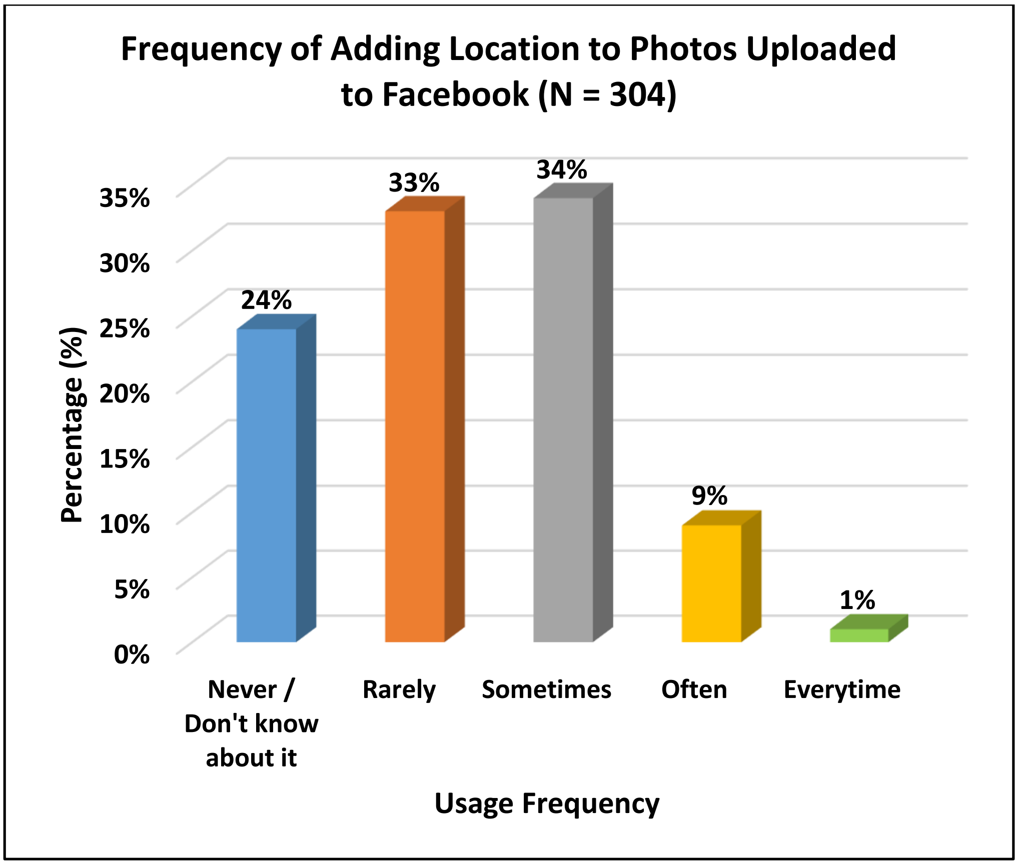


Figure 4.12: Frequency of Adding Location to Photos

The finding of the usage frequency for this Facebook feature (see Figure 4.12) is similar to that of check-in feature. The two highest percentage are still "sometimes" (34%) and "rarely" (33%), however it is noticed that there are slightly more respondents who chose "sometimes" over "rarely" for this case. There are also less respondents that indicated they never use or know about this Facebook feature. Furthermore, 9% respondents stated they "often" add location to photos when uploading it to Facebook, as compared to only 5% for check-in feature. Last but not least, 1% of the respondents selected "every time", meaning they tend to add location to every photos of theirs when uploading it to Facebook.

4.3.2.4 Data about Respondents' Frequency of Using Facebook Messenger App

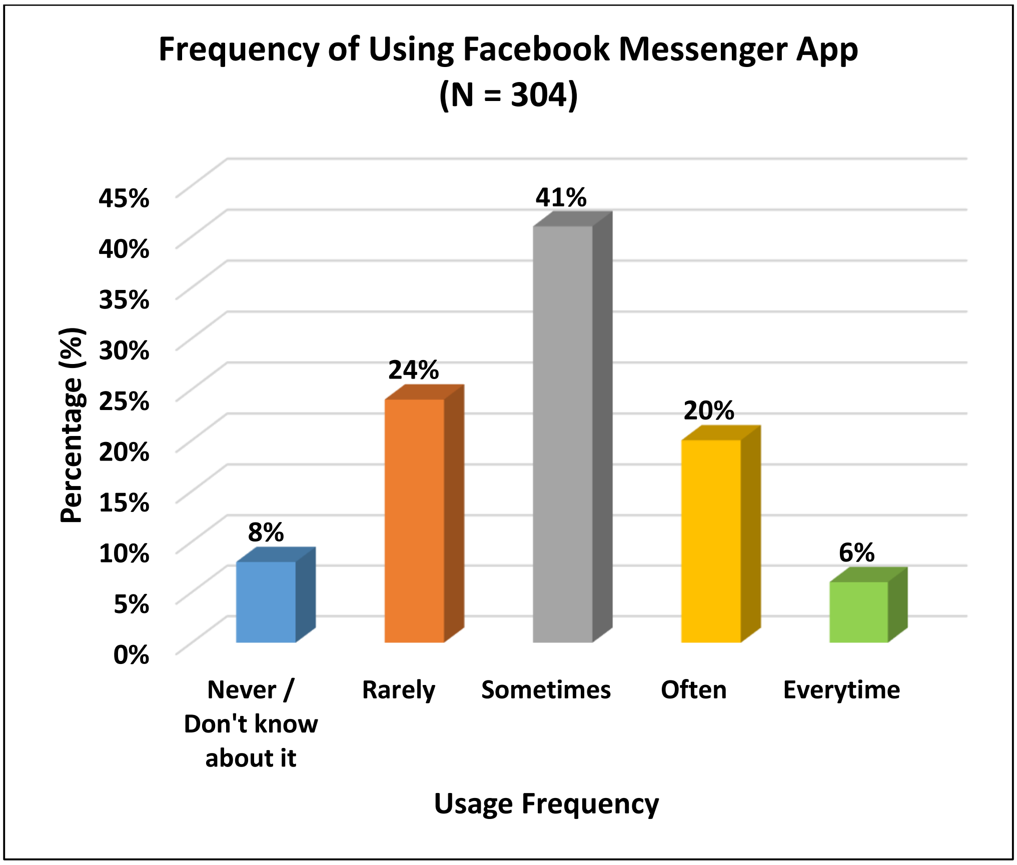


Figure 4.13: Frequency of Using Facebook Messenger App

Respondents were asked to select their usage frequency on Facebook Messenger app in which they used to chat with others. Figure 4.13 depicts that 41% respondents stated they use it sometimes, 24% stated rarely, and 20% stated often. The chart also shows that the percentage of respondents who never use Facebook Messenger app and those who used it all the time are almost equal, which is at 8% and 6% respectively.

4.3.2.5 Data about Respondents’ Awareness Regarding Location Sharing by Facebook Messenger App

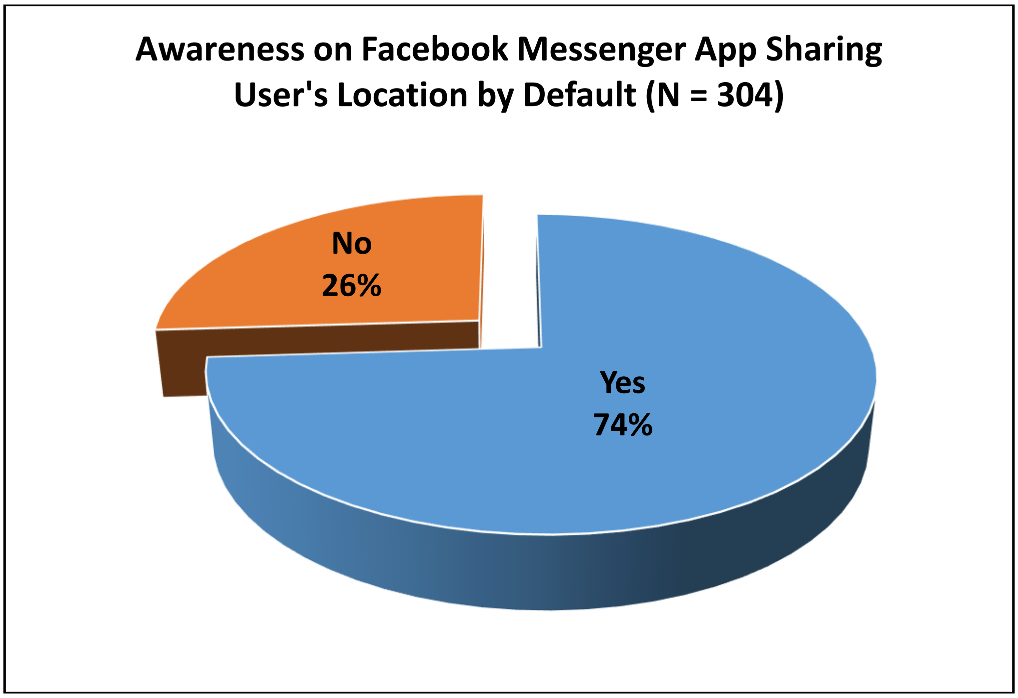


Figure 4.14: Awareness on Facebook Messenger App Sharing User’s Location by Default

According to the result (see Figure 4.14), 74% respondents said that they are aware that Facebook Messenger app on their smartphones automatically shares their precise location on a map, to the person they are chatting with by default. In contrast, only 26% of the respondents stated they do not know about this. From the finding, it is evident to conclude that majority of young Malaysian Facebook users are conscious about the privacy risk posed by Facebook Messenger app.

4.3.2.6 Data about Respondents' Location Sharing Setting for Facebook Messenger App

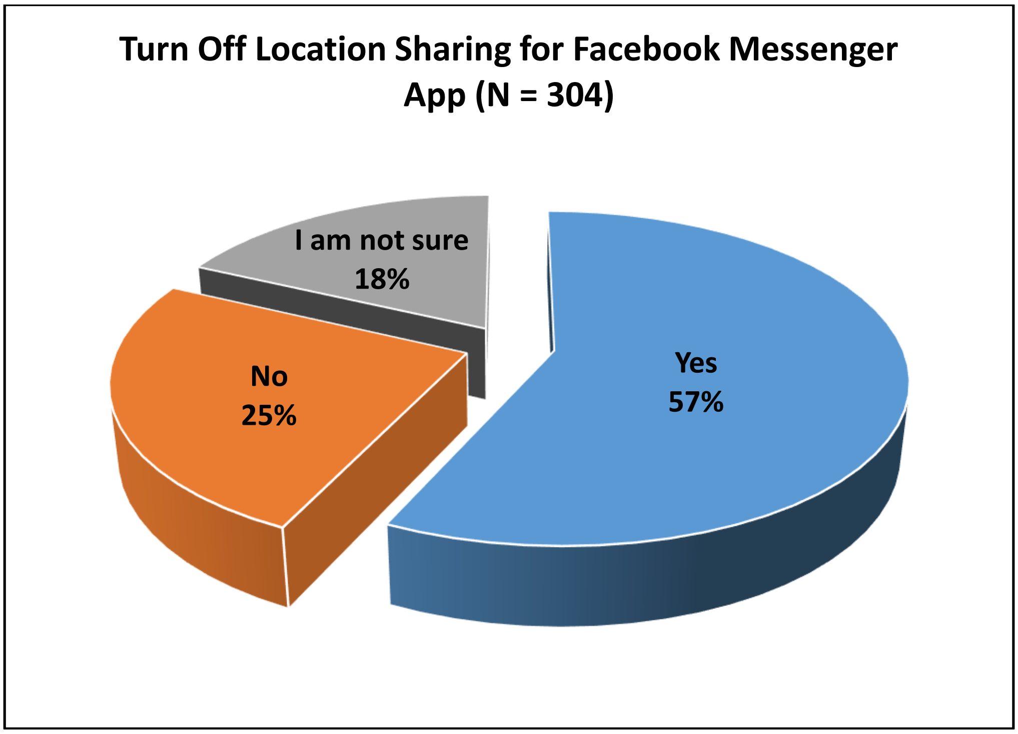


Figure 4.15: Location Sharing Setting for Facebook Messenger App

As shown in Figure 4.15, when asked whether they have turn off the location sharing setting for Facebook Messenger app, 57% respondents said "Yes", whereas 25% said no. On the other hand, 18% stated they are not sure what setting is their Facebook Messenger app currently set to. Nevertheless, it was found during the literature review that the location sharing setting is turned on by default for Facebook Messenger app during installation, therefore, those who chose "I am not sure" are actually unwittingly sharing their location to the person they are chatting with.

It was observed from previous chart (Figure 4.14) that 74% respondents said they knew about the privacy risk posed by Facebook Messenger app, however, there are only 57% respondents that had turned off the location sharing setting. There are three possibilities arise from this finding. First, respondents knew about the privacy threat of Facebook Messenger app but chose to ignore it by leaving the setting on. Second, respondents knew about the privacy risk but purposely chose to on it anyway because they wanted to share their location to others. Third, the respondents accidentally chose the wrong answer or they did not take the survey seriously.

4.3.3 Section C: Facebook Privacy and Security Settings

This section presents data associated with the privacy and security settings of respondents' Facebook account. At the same time, it also revealed the motives behind the modification of Facebook privacy and security settings by the respondents.

4.3.3.1 Data about Respondents' Current Privacy Settings

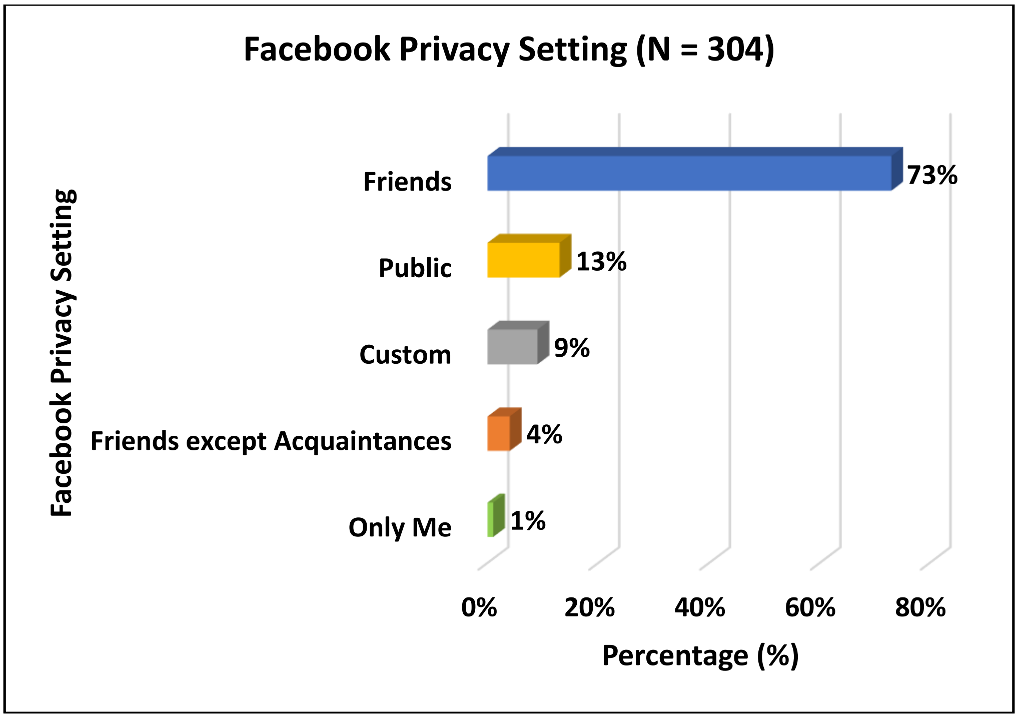


Figure 4.16: Facebook Privacy Settings

The main privacy settings on Facebook are divided into five selection of visibility: public, friends, friends except acquaintances, only me and custom. Out of 304 respondents who participated, 73% had “friends” as their privacy option, 13% chose “public”, 9% chose “custom”, and 4% selected “friends except acquaintances” (see Figure 4.16). The custom option allows the user to specifically set what content is visible on their profile to a particular group of friends. Only 1% of respondents chose “only me” as their privacy option. Nonetheless, it is still highly unlikely for someone to choose “only me” as his privacy option because this would mean that all his future posts on Facebook would only be visible to himself.

The result from current study is closely similar to that of Hoffmann (2012) (see Table 4.2). However, it is important to keep in mind that Hoffmann’s study only included three selections of privacy options as opposed to five in the current study.

Table 4.2: Comparison of Results between Current and Hoffmann’s Study

Results		
	Hoffmann’s Study (2012)	**Current Study**
Public	17%	13%
Friends	67%	73%
Custom	16%	9%

4.3.3.2 Data about Modification of Facebook Privacy Settings by Respondents

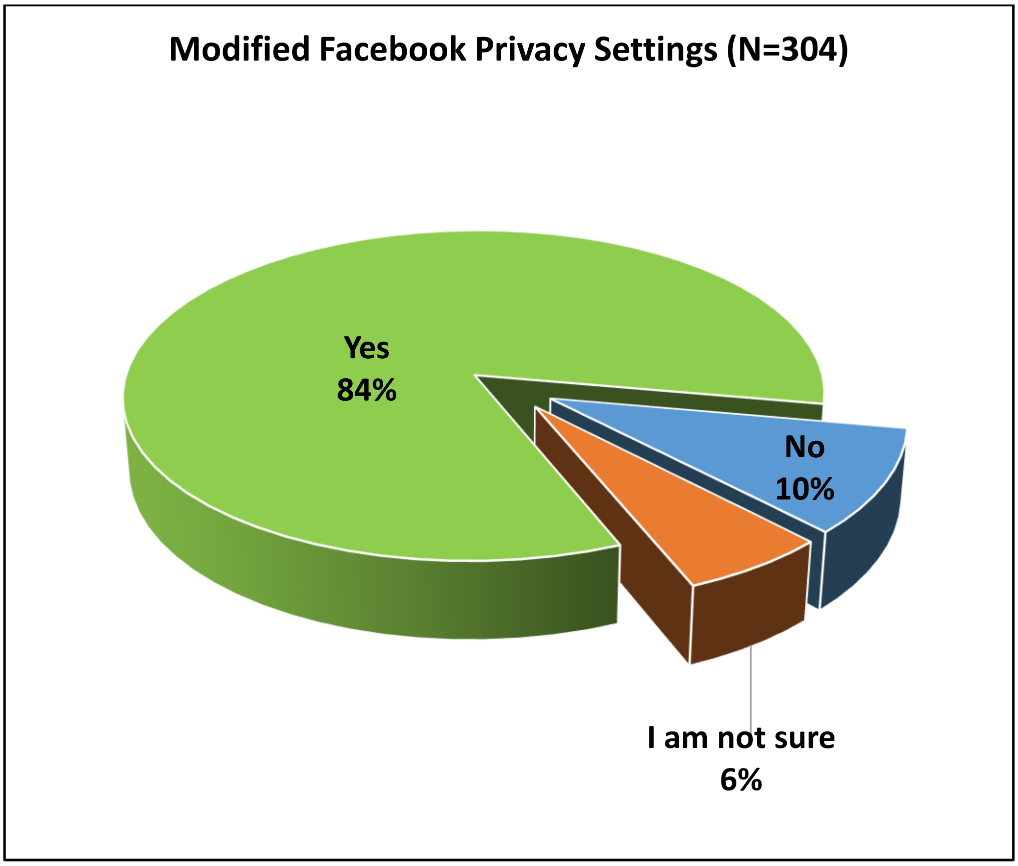


Figure 4.17: Modification of Facebook Privacy Settings

When asked if users ever modified their privacy settings on Facebook profile, 84% respondents said yes, 10% said no, while 6% said they were not sure (see Figure 4.17). Those that answered "Yes" were then directed to answer an additional question that explores on the reasons why respondents modify their privacy settings.

4.3.3.3 Data about Reasons for Modifying Facebook Privacy Settings

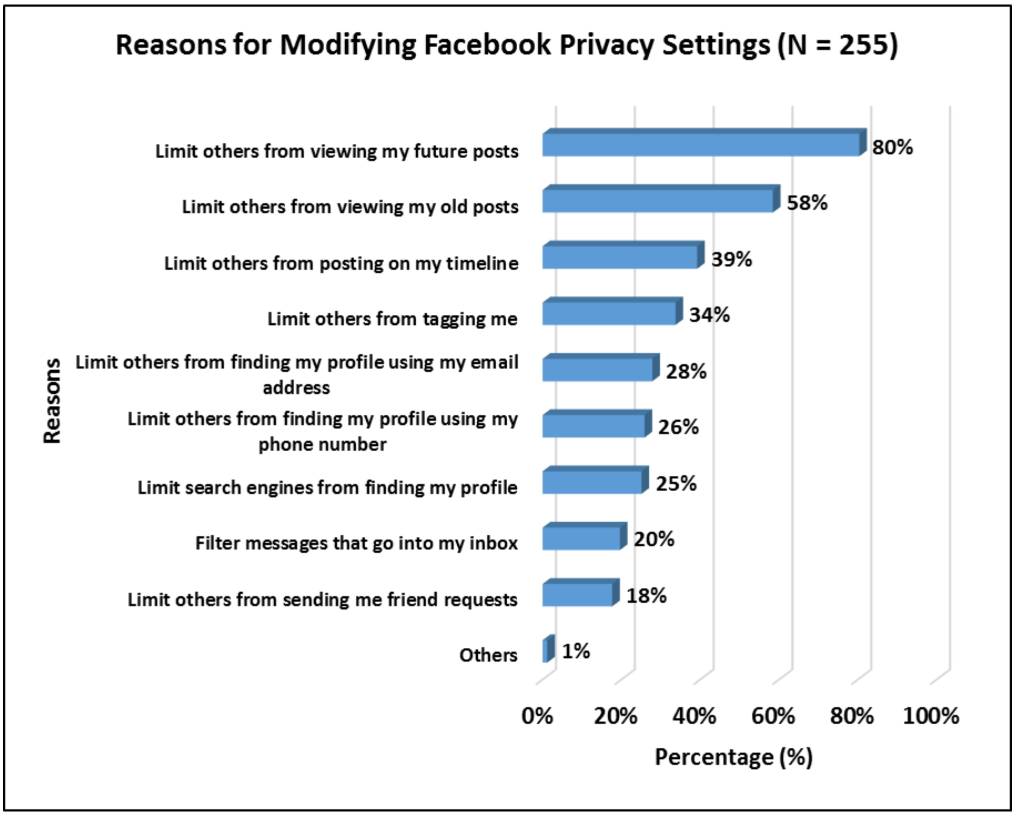


Figure 4.18: Reasons for Modifying Facebook Privacy Settings

Respondents were allowed to select more than one reason for this question. Out of the 255 respondents that stated they had modified their privacy settings before, 80% of them cited “limit others from viewing my future posts” as the top reason for modifying their privacy settings. The second most selected reason “limit others from viewing my old posts” was chosen by 58% respondents. 39% respondents indicated that they wanted to limit their friends from posting on their timeline, whereas 34% respondents wanted to prevent others from tagging them.

It can also be seen respectively from Figure 4.18 that 28%, 26% and 25% respondents wanted to avoid others from finding their Facebook profile through various ways. On the other hand, 18% respondents mentioned the reason for modifying their privacy setting is to limit others from sending them friend requests, while 20% respondents said they wanted stricter filtering on messages that goes into their Facebook inbox. Besides the above, three open ended responses were received saying "to have better control on contents flowing throughout the network", "Facebook app testing", and "prevent others from viewing my profiles".

4.3.3.4 Data about Modification of Facebook Security Settings by Respondents

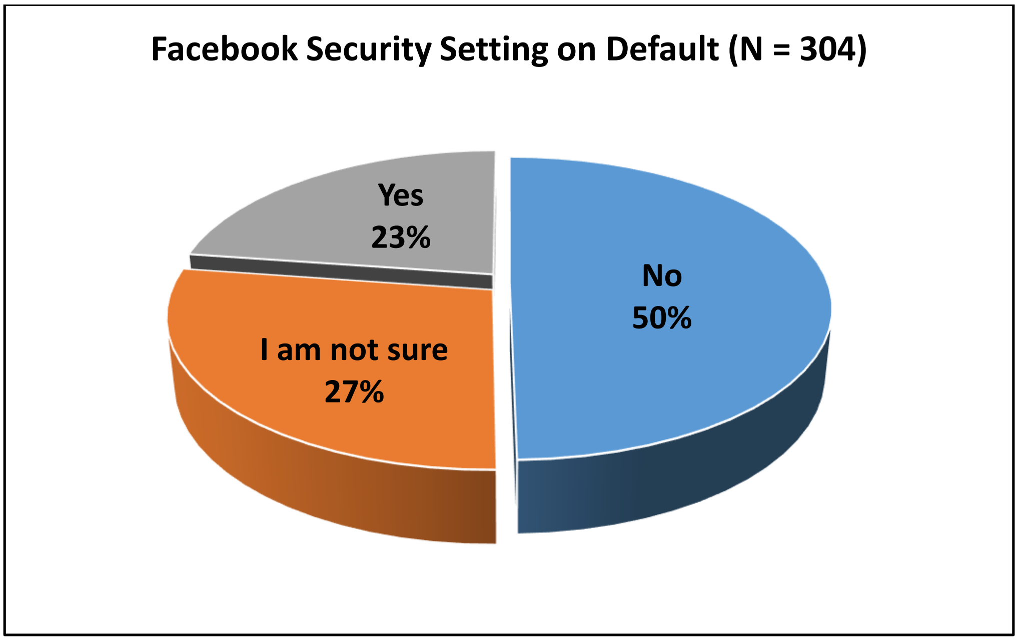


Figure 4.19: Modification of Facebook Security Settings

Respondents were asked if they have left their Facebook security settings on default. From the finding (see Figure 4.19), 23% admitted that they left their security settings on default, while 50% said they made changes to it. Alternatively, 27% mentioned they were not sure. The 151 respondents who had answered "No" for this question were then directed to answer an additional question that further explores on the changes made to their Facebook security settings. It was also found that the percentage of people who left their Facebook security settings on default from current study (22.7%) is slightly higher than the finding from Hoffmann's (2012) study, which is at 15%.

4.3.3.5 Data about Changes Made by Respondents on Facebook Security Settings

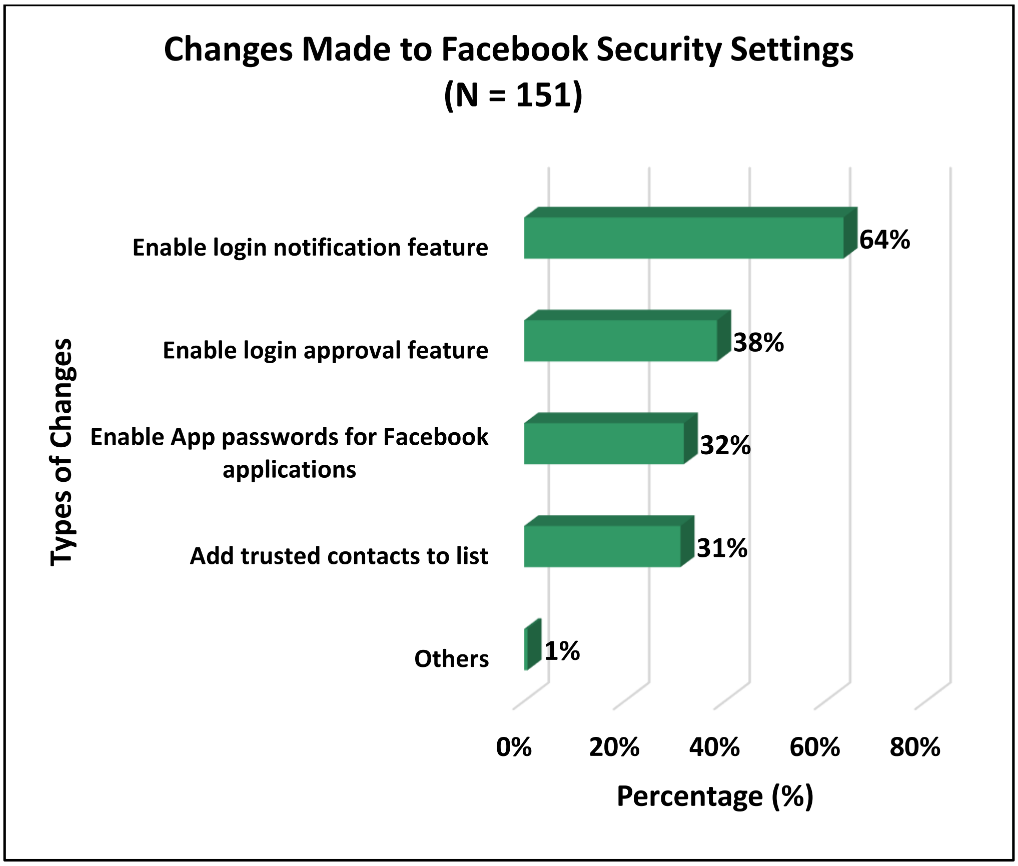


Figure 4.20: Types of Changes Made on Facebook Security Settings

Respondents were allowed to select more than one item for this question. From the 151 respondents who said they had made changes to their security settings, 64% stated they had enabled login notification feature while 38% enabled login approval feature. 32% respondents have indicated they enabled app passwords for their Facebook applications while another 31% stated they added trusted contacts to list (see Figure 4.20). There is one open ended response which the respondent indicated that he or she used Facebook security settings to “review trusted browsers”.

4.3.4 Section D: Perception on Cyberstalking

This section displays data in regards to respondents’ perception on the behaviours of cyberstalking.

4.3.4.1 Data about Respondents’ Awareness on Cyberstalking

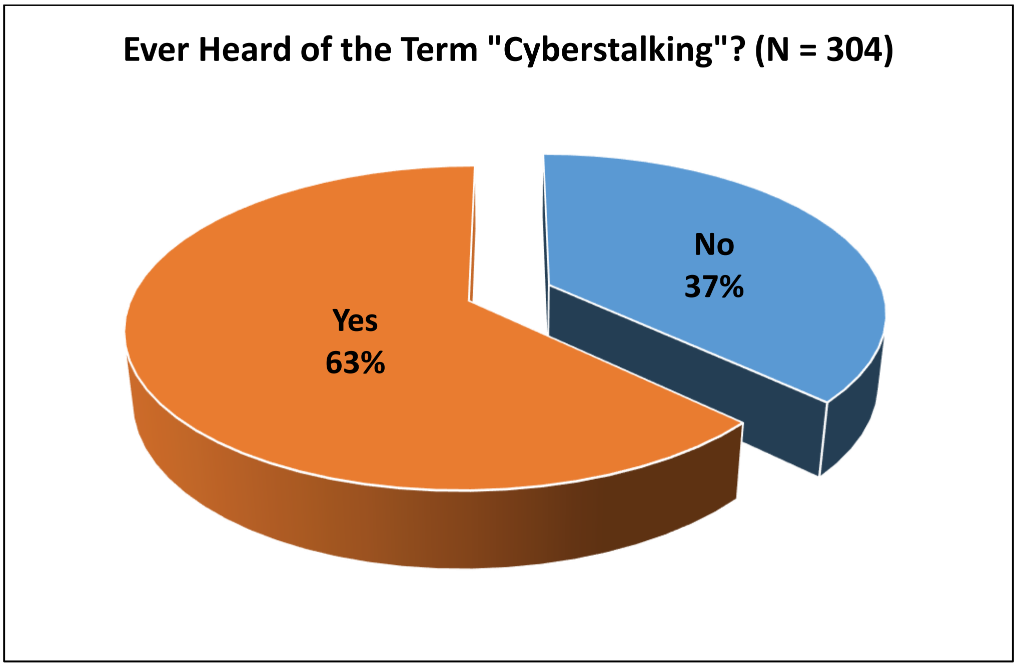


Figure 4.21: Awareness on Cyberstalking

As displayed in Figure 4.21, 63% of the respondents stated they had heard of the term “cyberstalking” prior to the survey, whereas 37% stated they have never heard of the term cyberstalking in the past. However, it is not certain whether those respondents who mentioned they heard of the term “cyberstalking” before actually understood the real definition behind the term.

4.3.4.2 Data about Respondents' Opinions toward Cyberstalking

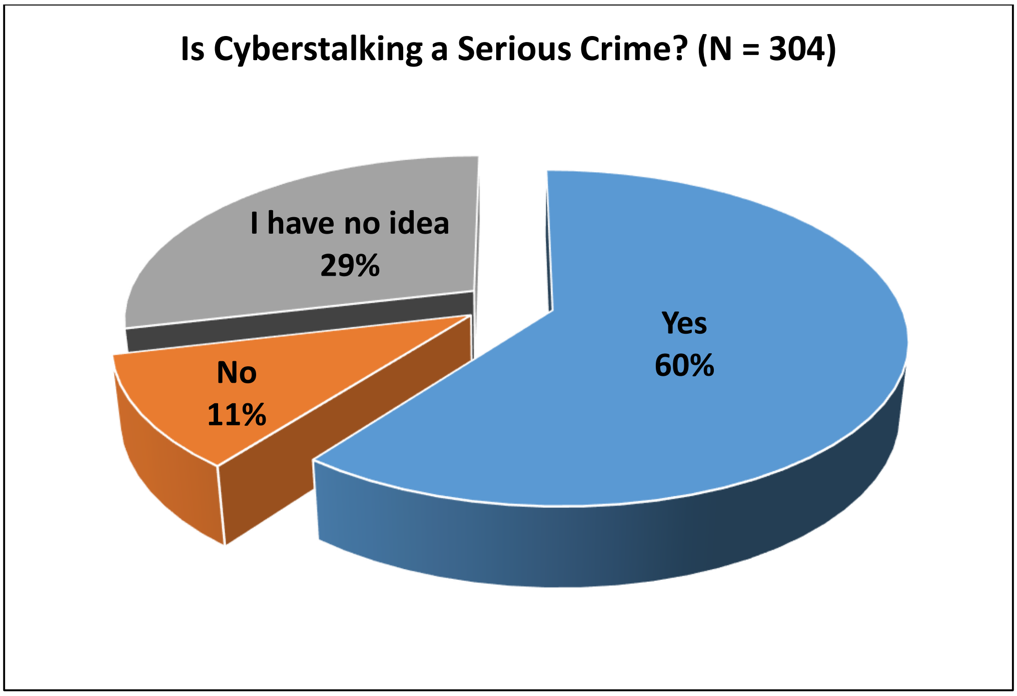


Figure 4.22: Opinions of Respondents toward Cyberstalking

With regards to the severity of cyberstalking behaviours in terms of crime, 29% respondents had no idea with it. Apart from that, 60% of respondents agreed that cyberstalking is a serious crime, whereas 11% classified cyberstalking as a non-serious crime (see Figure 4.22). From this finding, it can be seen that majority of the respondents viewed cyberstalking as a serious threat to their online privacy.

4.3.5 Section E: Cyberstalking Attacks

This section exhibits data in regards to types of cyberstalking attacks the respondents had faced in the past.

4.3.5.1 Data about Cyberstalking Attacks Received by Respondents

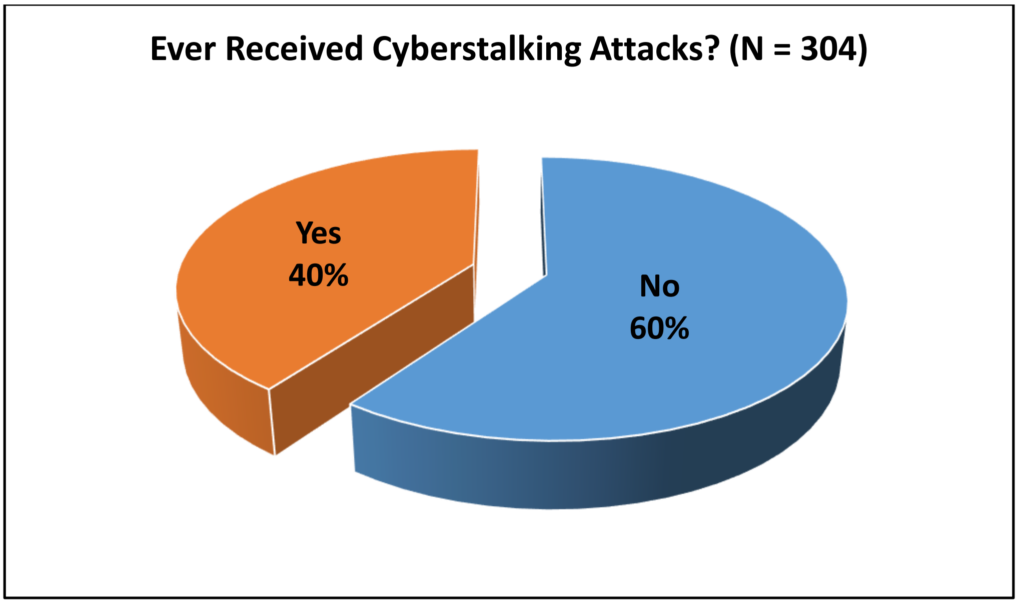


Figure 4.23: Received Cyberstalking Attacks

As cited previously in the literature review, the researcher had clearly defined several types of cyberstalking attacks one might faces from cyberstalkers. The attacks were then listed in the survey and respondents were asked if they had ever experienced these attacks through Facebook or resulting from the use of Facebook. From Figure 4.23, it can be seen that out of 304 respondents, 60% have stated they never received or experienced any of the attacks listed in the questionnaire. The other 40% respondents who stated they had previously received attacks were then requested to select what type of attack they had received beforehand and the results are shown in Table 4.3 below.

Table 4.3: Types of Attacks Received by Respondents

Respondents who had experienced cyberstalking attacks (N = 121)	
Received viruses or malware	47%
Received sexual messages	35%
Received threat or hostile messages	31%
Account hijacked or password stolen	25%
Account used to send false accusations	16%
Someone spread vicious rumours about you	16%
Account pretending to be you (identity theft / impersonation)	16%
Real life physical attack	6%
Vandalism of private property	5%

Table 4.3 shows types of attacks faced by the 121 respondents on Facebook. Respondents were allowed to select more than one item. Significant results include 47% who claimed they received viruses or malware attacks, 35% received sexual messages, 31% received threat or hostile messages before, and 25% had their account hijacked or password stolen previously. There are three types of attacks that were experienced by the same amount of respondents at 16%, in which their account were used to send false accusations, also, someone spread spiteful rumours about them on Facebook, and impersonation of fake account by cyberstalkers. Interestingly, a relatively small percentages of survey respondents reported they had experienced real life attacks by cyberstalkers (i.e., vandalism or private property, real life physical attack).

In conclusion, the finding from the current study indicated approximately 40% of young Malaysian Facebook users experienced some kind of cyberstalking victimization before. This percentage is similar to the study of Henson et al. (2011), in which the authors reported approximately 42% of social network users had experienced some kind of interpersonal victimization while online.

4.4 Results of Hypotheses Testing Using Inferential Statistics

As described in chapter 1, five hypotheses were formulated and used to verify the research objectives. The purpose of hypotheses testing in this study is to uncover and describe the relationship between the dependent variable and independent variable (see section 3.7). And so, this section presents the results of each hypothesis testing. For full analysis results, kindly refer to Appendix D.

4.4.1 Hypothesis One

The following null hypothesis was tested:

- $H_0$1: There is no significant relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users

From the first main null hypothesis 1 ($H_0$1), the following two sub hypotheses were formed:

- $H_0$1a: There is no significant relationship between the use of location tagging features and cyberstalking victimization among young Malaysian Facebook users

- $H_0$1b: There is no significant relationship between the use Facebook Messenger app without turning off location sharing and cyberstalking victimization among young Malaysian Facebook users

4.4.1.1 Testing $H_0$1a

- $H_0$1a: There is no significant relationship between the use of location tagging features and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Used Location Tagging Features” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.4. The objective was to test the relationships between the two variables. Results show that there was no significant relationship between the independent and dependent variables as the p-value (p = 0.456) was larger than the set 0.05 level of significance. Therefore, there was not enough evidence to reject the null hypothesis of $H_0$1a.

Table 4.4: Binary Logistic Regression Results of Hypothesis $H_0$1a

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	UsedLocationTaggingFeatures(1)	-.218	.293	.555	1	.456	.804
	Constant	-.238	.262	.827	1	.363	.788

a. Variable(s) entered on step 1: UsedLocationTaggingFeatures.

4.4.1.2 Testing $H_0$1b

- $H_0$1b: There is no significant relationship between the use Facebook Messenger app without turning off location sharing and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Used Facebook Messenger App without Turning off Location Sharing Setting” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.5. The objective was to test the relationships between the two variables. Results show that there was no significant relationship between the independent and dependent variables as the p-value (p = 0.466) was larger than the set 0.05 level of significance. Therefore, there was not enough evidence to reject the null hypothesis of $H_0$1b.

Table 4.5: Binary Logistic Regression Results of Hypothesis $H_0$1b

Variables in the Equation							
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	UsedFacebookMessenger App(1)	.175	.240	.531	1	.466	1.191
	Constant	-.482	.151	10.209	1	.001	.617

a. Variable(s) entered on step 1: UsedFacebookMessengerApp.

4.4.2 Hypothesis Two

The following null hypothesis was tested:

- $H_0$2: There is no significant relationship between accepting strangers’ friend requests and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Accepted Strangers’ Friend Requests” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.6. The objective was to test the relationships between the two variables. Results show that there was a statistically significant relationship between the independent and dependent variables as the p-value (p = 0.045) was smaller than the set 0.05 level of significance. Hence, there was enough evidence to reject the null hypothesis of $H_0$2. The finding implies Facebook users who accept strangers’ friend requests is significantly and positively related to cyberstalking victimization. Furthermore, the odds ratio (i.e., Exp(B)) shows that Facebook users who accept strangers’ friend requests are 1.7 times more likely to experience cyberstalking attacks, as opposed to those who do not.

Table 4.6: Binary Logistic Regression Results of Hypothesis $H_0$2

Variables in the Equation							
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	AcceptStrangerFriendRequests(1)	.507	.253	4.024	1	.045	1.660
	Constant	-.750	.208	13.001	1	.000	.472

a. Variable(s) entered on step 1: AcceptStrangerFriendRequests.

4.4.3 Hypothesis Three

The following null hypothesis was tested:

- $H_0$3: There is no significant relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Used Default Security Settings” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.7. The objective was to test the relationships between the two variables. Results show that there was no significant relationship between the independent and dependent variables as the p-value (p = 0.167) was larger than the set 0.05 level of significance. Therefore, there was not enough evidence to reject the null hypothesis of $H_0$3.

Table 4.7: Binary Logistic Regression Results of Hypothesis $H_0$3

Variables in the Equation							
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	DefaultSecuritySetting(1)	-.325	.235	1.906	1	.167	.723
	Constant	-.253	.164	2.378	1	.123	.776

a. Variable(s) entered on step 1: DefaultSecuritySetting.

4.4.4 Hypothesis Four

The following null hypothesis was tested:

- $H_0$4: There is no significant relationship between the use of “Public” privacy settings and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Used Public Privacy Setting” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.8. The objective was to test the relationships between the two variables. Results show that there was a highly significant relationship between the independent and dependent variables as the p-value (p = 0.007) was a lot smaller than the set 0.05 level of significance. Hence, there was strong evidence to reject the null hypothesis of $H_0$4. The finding implies Facebook users who used “Public” privacy setting is significantly and positively related to cyberstalking victimization. Furthermore, the odds ratio (i.e., Exp(B)) shows that Facebook users who used “Public” privacy setting are 2.6 times more likely to experience cyberstalking attacks, as compared to those who do not.

Table 4.8: Binary Logistic Regression Results of Hypothesis $H_0$4

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PublicPrivacySetting(1)	.966	.355	7.395	1	.007	2.629
	Constant	-.539	.127	17.981	1	.000	.583

a. Variable(s) entered on step 1: PublicPrivacySetting.

4.4.5 Hypothesis Five

The following null hypothesis was tested:

- H_05: There is no significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users

Binary logistic regression was used for analysis and the SPSS output for the relationship between the variables of “Gender” (independent variable) and “Received Cyberstalking Attacks” (dependent variable) is shown in Table 4.9. The objective was to test the relationships between the two variables. Results show that there was no significant relationship between the independent and dependent variables as the p-value (p = 0.626) was larger than the set 0.05 level of significance. Therefore, there was not enough evidence to reject the null hypothesis of H_05.

Table 4.9: Binary Logistic Regression Results of Hypothesis H_05

Variables in the Equation							
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	-.115	.235	.238	1	.626	.892
	Constant	-.351	.173	4.131	1	.042	.704

a. Variable(s) entered on step 1: Gender.

4.4.6 Summary of Binary Logistic Regression

The results of binary logistic regression for each independent variables on the dependent variable (Received Cyberstalking Attacks) are summarized in Table 4.10.

Table 4.10: Summary of Binary Logistic Regression of all Independent Variables on Cyberstalking Victimization

	Cyberstalking Victimization			
Variables	**Scale / Coding**	**Coefficient**	**Sig.**	**Exp(B)**
Used Location Tagging Features	(0 = No, 1 = Yes)	-0.218	0.456	0.804
Used Facebook Messenger App without Turning off Location Sharing Setting	(0 = No, 1 = Yes)	0.175	0.466	1.191
Accepted Strangers' Friend Requests	(0 = No, 1 = Yes)	0.507*	0.045	1.660
Used Default Security Settings	(0 = No, 1 = Yes)	-0.325	0.167	0.723
Used Public Privacy Setting	(0 = No, 1 = Yes)	0.966**	0.007	2.629
Gender	(0 = Male, 1 = Female)	-0.115	0.626	0.892
Received Cyberstalking Attacks	(0 = No, 1 = Yes)	-	-	-
N	304			

**. Correlation is significant at the 0.01 level
*. Correlation is significant at the 0.05 level

4.5 Summary of Hypotheses Testing

Overall, the results of hypotheses testing showed that out of the five null hypotheses tested, two null hypotheses (i.e., $H_0 2$ and $H_0 4$) were successfully rejected. Both $H_0 2$ ($p = 0.045$) and $H_0 4$ ($p = 0.007$) were rejected because the obtained p-values were smaller than 0.05 level of significance. This means that there is a significant relationship between Facebook users who accepted strangers’ friend requests and them receiving attacks from cyberstalkers. On the other hand, there is also a significant relationship between Facebook users who used public privacy setting and them receiving attacks from cyberstalkers.

The three null hypotheses which the researcher failed to reject are $H_0 1$, $H_0 3$, and $H_0 5$. The reason for the failure to reject the null hypotheses is due to the p-values obtained for all three $H_0 1$ ($p = 0.456$), $H_0 3$ ($p = 0.167$), and $H_0 5$ (p

= 0.626) were larger than 0.05 level of significance. Hence, there was not enough statistical evidence to reject the null hypotheses of the study.

The overall results and decisions to reject or failure to reject of all five hypotheses tested are summarized in Table 4.11 below.

Table 4.11: Summary of Hypotheses Testing Results

Null Hypothesis	**Decision**
$H_0$1: There is no significant relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users	**Fail to reject $H_0$1** The findings showed that there was no significant relationship between young Malaysian Facebook users who use location disseminating features and cyberstalking victimization
$H_0$2: There is no significant relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users	**Rejected $H_0$2** The findings indicated that there was indeed a significant relationship between young Malaysian Facebook users who accept strangers' friend requests and cyberstalking victimization
$H_0$3: There is no significant relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users	**Fail to reject $H_0$3** The findings showed that there was no significant relationship between young Malaysian Facebook users who left their security settings on default and cyberstalking victimization

Table 4.11 (Continued)

Null Hypothesis	Decision
H$_0$4: There is no significant relationship between the use of “Public” privacy settings and cyberstalking victimization among young Malaysian Facebook users	**Rejected H$_0$4** The findings indicated that there was indeed a highly significant relationship between young Malaysian Facebook users who have their privacy settings set to “Public” and cyberstalking victimization
H$_0$5: There is no significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users	**Fail to reject H$_0$5** The findings showed that there was no significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users

4.6 Conclusions

In conclusion, this chapter presents all the major findings of the study, including the demographic profile of respondents, results of data analysis on data collected from the online survey using descriptive statistics, and the results of hypotheses testing using binary logistic regression. From the results of hypotheses testing, it was found that of the five null hypotheses, two were successfully rejected, whereas there was not enough statistical evidence to reject the other three. The outcomes presented and outlined in this chapter provided inputs for further discussion in the next chapter, which is the last chapter of this dissertation.

CHAPTER 5

DISCUSSION AND CONCLUSIONS

5.1 Introduction

This chapter covers the following topics:

- Discussion of the research outcomes
- Research contributions
- Limitations and recommendations for future study
- General recommendations on cyberstalking prevention
- Conclusion

5.2 Discussion of the Research Outcomes

The emergence popularity of social media have irrevocably transformed the nature of human communication, creating social networks which are unprecedentedly broad and divergent from normative, interpersonal relationships in numerous ways. Nowadays, social network users all around the world can share their views, thoughts or information with their friends and families instantaneously, regardless of different time zones and geographic locations.

However, it has become an ecosystem of friends upon friends who have no initial relation to the target user and the spread of information is no longer contained to a small group – it become international, global and exponential in the manner that it can be shared. For this reason, the ease of information dissemination comes at a cost. As it can be seen from the research findings, 40% (see Table 4.23) of young Malaysian Facebook users had previously experienced some kind of cyberstalking attacks while using Facebook, or resulting from the use of Facebook. Besides, two out of the six factors (independent variables) have been proven as statistically significant predictors of cyberstalking victimization on Facebook.

As mentioned in chapter 1, five research objectives were identified for this study. Overall, all the identified research objectives have been achieved. The following subsections further discussed the research outcomes obtained from each hypothesis testing, at the same time verified each of the findings against the research objectives.

5.2.1 Objective 1

- To determine the relationship between the use of location disseminating features and cyberstalking victimization among young Malaysian Facebook users

The hypotheses testing results described in section 4.4.1.1 and 4.4.1.2 revealed that there was no significant relationships between young Malaysian Facebook users who use location disseminating features and cyberstalking victimization. Contrary to popular belief, the finding implies that Facebook users who use Facebook features to share their current locations to others is not significantly related to them receiving cyberstalking attacks.

A plausible explanation for this could be that respondents who shared their locations to others did not previously added people they do not know to their Facebook account. Another possibility is that they were not using public privacy settings which would reveal all their Facebook status, including their shared locations, to all people around the world. All things considered, there is a probability that it is not what the users shared that increase the likelihood of receiving cyberstalking attacks, instead, it is whether or not the people who have access to the shared information are trustworthy.

The above explanation is supported by a study done by Wolak et al. (2008), in which the authors studied the relationship between online behaviours of youths and the odds of them receiving online related victimization (i.e., solicitation for sexual purposes or harassment). They found that posting private information on social network, by itself, has no significant relationship with increased likelihood of online victimization among youths. However, the authors clearly pointed out that youths who interact and added strangers online are 5 to 11 times more likely to fall victim to predators. Thus, it is clear that one of the most essential way of preventing online victimization among youths is to choose the right target audience when posting private information online.

5.2.2 Objective 2

- To determine the relationship between accepting strangers' friend requests and cyberstalking victimization among young Malaysian Facebook users

The hypothesis testing results described in section 4.4.2 revealed that there was a significant and positive relationship between young Malaysian Facebook users who accept strangers' friend requests and cyberstalking victimization. The finding implies that Facebook users who allow strangers into their friend list increases the odds of them receiving attacks from cyberstalkers by approximately 1.7 times. In other words, individuals who accept strangers' friend requests on Facebook are 1.7 times more likely to be victimized by cyberstalkers.

This finding is consistent with a study by Henson et al. (2011) about online interpersonal victimization. They found that individuals who added strangers as friends on their social networks are 2.6 times more likely to experience online interpersonal victimization. Likewise, the finding from this hypothesis testing is also consistent with the study of Pinchot and Paullet (2012), which the authors cite that "In general, participants did not seem to be aware that limiting the number of friends that they accept within Facebook can directly affect the level of security for their private data". The authors were concerned as their results found that 40% of respondents had accepted friend requests from people they do not know and a small percentage of them had experiences with cyberstalking attacks.

Similarly, a study by Legal & General into the habits of UK Facebook users found that online criminals are increasingly setting up fake profiles to hunt potential victims, cottoning on the fact that 51% of UK Facebook users accepted friend requests from people they do not know (Wrenn, 2012). Lastly, a real life incident which happened in the United States further supported the outcome of the hypothesis testing. The news article claimed that the victim was harassed both physically and mentally by a cyberstalker, who happened to be a stranger the victim had previously accepted on Facebook (Silva, 2014).

5.2.3 Objective 3

- To determine the relationship between the use of default security settings and cyberstalking victimization among young Malaysian Facebook users

The hypothesis testing results described in section 4.4.3 revealed that there was no significant relationship between young Malaysian Facebook users who left their security settings on default and cyberstalking victimization. The finding implies that Facebook users who use default security settings for their Facebook account is not significantly related to them receiving cyberstalking attacks. The reason for the large p-value acquired (p = 0.167) is because respondents who had made changes to their Facebook security settings also received amount of cyberstalking attacks similar to those who used default settings (see Table 5.1).

Table 5.1: Cross-tabulation Results of Default Security Settings and Received Cyberstalking Attacks

DefaultSecuritySetting * ReceivedCyberstalkingAttack Crosstabulation

Count

		ReceivedCyberstalkingAttack		
		No	Yes	Total
DefaultSecuritySetting	No	85	66	151
	Yes	98	55	153
Total		183	121	304

This finding is identical to that of Hoffmann (2012), which the author also failed to reject the hypothesis that indicates “Facebook users who adjust their security setting are far less likely to fall victim to privacy attacks”, as he found that users who adjusted their security settings were also receiving amount of attacks similar to that of user who do not.

5.2.4 Objective 4

- To determine the relationship between the use of “Public” privacy settings and cyberstalking victimization among young Malaysian Facebook users

The hypotheses testing results described in section 4.4.4 revealed that there was a highly significant and positive relationship between young Malaysian Facebook users who have their privacy settings set to “Public” and cyberstalking victimization. The finding also indicates that Facebook users who use public privacy setting are approximately 2.6 times more likely to be victimized by cyberstalkers.

This finding is consistent with a study by Hoffmann (2012) about user’s Facebook privacy settings. They found that individuals who utilize custom privacy settings on Facebook have lower chances of receiving privacy attacks whereas individuals that use public privacy settings have higher chances of receiving privacy attacks. Both Williams et al. (2011) and Mathiyalakan et al. (2013) further supported this by claiming that Facebook default privacy options permit too-open access to user profiles and promote vulnerability for the users who use them. Mathiyalakan et al. (2012) further mentioned that public privacy settings on Facebook can easily lead to unwanted information disclosure that can be harmful to the user, especially when the user is unwittingly sharing his or her private information to the whole world.

5.2.5 Objective 5

- To determine the relationship between gender and cyberstalking victimization among young Malaysian Facebook users

The hypothesis testing results described in section 4.4.5 revealed that there was no significant relationship between gender and cyberstalking victimization among young Malaysian Facebook users. Reason for the failure in rejecting the null hypothesis was due to the large p-value (p = 0.626) obtained from the hypothesis testing result. However, if the level of significance is ignored, the coefficient shows there is a negative relationship between female users and cyberstalking victimization (see Table 4.9). In simple words, it was found that males have higher odds of experiencing cyberstalking attacks than females, which is an interesting result. This is contrary to expectations that females are more attractive targets for cyberstalkers.

It can be seen from Table 5.2 that even though there are more females who had experienced cyberstalking attacks when compared to males, however, it is important to take note that there are more female respondents who had participated in the study. Considering that, the result of cross-tabulation reported that there are 41% male respondents who had received cyberstalking attacks, as opposed to a lower 39% for female respondents. This situation is similar to the finding by Garlik (2007), an online security firm. They found that UK men are at greater risk of being cyberstalked than their female counterparts with male victims outnumbering female victims by three to one. More than 394,000 men have fallen victim to cyberstalkers as compared to just under 135,000 women victims, the reason given is that men typically are less guarded than women when they operate online, rendering themselves easier targets for cyberstalkers.

Table 5.2: Cross-tabulation Results of Gender and Received Cyberstalking Attacks

Gender * ReceivedCyberstalkingAttack Crosstabulation

Count

		ReceivedCyberstalkingAttack		
		No	Yes	Total
Gender	Male	81	57	138
	Female	102	64	166
Total		183	121	304

5.3 Research Contributions

The research is anticipated to make four contributions to the area of user’s privacy in social networking sites. First, the research outcomes will be of great benefit to users of Facebook or other online social networking sites to better engage themselves in privacy settings, as it clearly demonstrates how technological advancements have changed the manner in which their information is disseminated to a nearly exponential audience.

Second, the findings of the current study also contribute to the cyberstalking victimization literature by addressing the relationship of certain Facebook usage characteristics and the likelihood of victimization by cyberstalkers.

Third, the research can help to promote healthier privacy and security mechanisms for social networking sites to ensure more protection for user’s information.

Lastly, the research can pave way for further research whereby companies or individuals can develop applications for both computers and smartphones to counter the issues of cyberstalking.

5.4 Limitations and Recommendations for Future Study

As mentioned previously in chapter 3 that this study is bounded by both resource and time constraints, thus, it is important to point out several limitations of the current study. Correspondingly, in light of these limitations, this section also provides relevant recommendations for future research.

First of all, this research utilized purposive sampling, which is a type of non-probability sampling technique. This means that the samples were gathered in a manner that does not ensure each member of the population has an equal chance of being selected. For that reason, many researchers tend to question the confidence in generalizability of a research's findings that utilized non-probability sampling. For future study, it is highly recommended to use random sampling method to conduct similar research as it would greatly increase the confidence in the generalizability of the study.

Secondly, it is noticed that majority of the respondents came from developed states of Malaysia (i.e., Penang, Selangor, Kuala Lumpur) (see Figure 4.4). The significance of this limitation is that the outcomes of the study might be different if more respondents were sought from less developed states as their computer and internet literacy might differ enormously. Future research should seek to acquire the same amount of respondents from each states in Malaysia as this would provide a more accurate and complete results for the study.

Thirdly, the research method employed in this study is a quantitative research approach that utilized self-administered questionnaire to collect data from targeted respondents. Although convenient and cost effective, this method does not allow the respondents to provide more in-depth thoughts, comments or information (e.g., why do they like to use check-in feature so much, what kind of physical attacks have they faced, any psychological or physical trauma resulting from being cyberstalked) which might be useful for the study. Future research should cover both quantitative and qualitative research methods as this would help to obtain clearer understanding of the findings.

The last limitation of the study is the use of only English language for the questionnaire. Even though English is one of the primary languages in Malaysia, there may still be some respondents who have lower English proficiency that might possibly miscomprehend the meaning of the questions. Thus, future research may consider to translate the questionnaire into other languages which include English, Chinese and Malay to increase the accuracy of data collected.

5.5 General Recommendations on Cyberstalking Prevention

Fighting cybercrime is no longer only a responsibility of legal bodies, government, and IT experts. It is time for average users to learn to protect themselves from cyber threats. This study has evidenced that no one is absolutely safe from cyber threats in today’s technology-driven world. The researcher has come up with a list of recommendations in the hope of aiding Facebook users to better protect themselves from cyberstalking threats:

- Avoid adding strangers to your friend list. This is vital as it was found from the research outcome that accepting strangers' friend requests is significantly related to cyberstalking victimization. However, if you are using Facebook to make new friends, be sure to move those newly added strangers into a separate friend list and use custom privacy option which limit their viewing privileges whenever you want to share private information on your Facebook.
- Avoid using public privacy setting for your personal Facebook account, at the minimum, choose "Friends" as the privacy option. This is essential as it was found from the research outcome that using public privacy setting is significantly related to cyberstalking victimization.
- Lessen the use of location tagging feature and do not reveal your daily itineraries if you have previously added strangers to your friend list, as this would let cyberstalkers the opportunity to know where and when you are planning to be at. To be on the safe side, remember to share only with those who are within your trusted circle.
- Turn off location sharing settings for Facebook Messenger app on your smartphones as the app is known for sharing your precise location to the person you are chatting with by default.
- Use Facebook security settings to better safeguard your account from cyberstalkers. For example, by turning on login approvals settings, the cyberstalker is unable to log into your Facebook account

even he or she has your passwords, as Facebook will require an additional security code that is only accessible via your phone.

- Avoid sharing confidential data such as home or work addresses and mobile number on your Facebook profile.
- Practice good password management by never sharing your credentials with others.

On top of that, Symantec Corporation has come up with a list of anti-stalking tips and highly recommends all social network users to follow suit to protect not only themselves, but also their family members from cyberstalking threats (Merritt, 2014):

- Make sure you logout your computer whenever you move away and use a strong password for your user account, the same applies to your smartphones.
- Perform an online search for names of you or your family members, and be sure to remove anything private or inappropriate that you find from the search results.
- If you suspect that you are being monitored daily by someone using spyware, use only public computers or phones to seek help, if not, the cyberstalker might find out that you are actually trying to get help and this will put you in even greater danger.
- Always use updated security software to prevent someone from infecting your computer with spyware, the same goes for your smartphones. Security software can help to detect existing spyware

and also help to prevent spyware from infecting your devices in the future, this will greatly reduce the likelihoods of being stalked.

5.6 Conclusions

The changing nature of social networks in the twenty-first century has warranted that privacy and security protections be enhanced in order to combat new forms of criminal behaviour such as cyberstalking. As social network has become such a standard part of life, it comes upon the user to gain control over the information they share and upload online.

Through the literature review, it has been made known that cyberstalking is very real and the number of cases are on the rise every year. Cyberstalking is also a threat that most people are not aware of until it is too late as users generally only pay close attention and begin to take initiatives to protect themselves after they have fallen victim to an attack, which is usually too late. In addition, the popularity and rapid growth of smartphones also played a significant role in making personal information easier to disseminate through Facebook.

This study has examined the relationship between several usage characteristics on Facebook in affecting cyberstalking victimization. The findings suggest that there are indeed two usage characteristics that stand out as statistically significant predictors of cyberstalking victimization. First, by accepting strangers' friend requests on Facebook. Second, by using public privacy settings for Facebook profile. There are also other key findings from the study, which found that young Malaysian Facebook users:

- Check Facebook 7 times a day on average
- The top reasons for using Facebook is to keep in touch with friends and to keep up-to-date with latest news
- Gender is the most revealed information on Facebook profile
- 51% of users have more than 500 friends on Facebook
- 65% had previously accepted friend requests from people they do not know on Facebook
- 13% are using public privacy settings
- 60% view cyberstalking as a serious crime
- 40% had experienced some kind of cyberstalking victimization resulting from the use of Facebook

As a final point, the future of social networks depend critically on combating cyberstalking through external and internal regulations, with the default settings on Facebook a particularly salient concern. Newly registered users of social networks should have mandatory privacy settings that protect them from cyberstalkers, with readily available information for new users regarding how to report and block unwanted communications.

REFERENCES

Acock, A.C., 2005. SAS, Stata, SPSS: A comparison. *Journal of Marriage and Family*, 67(4), pp. 1093 - 1095.

Adler, E. and Clark, R., 2007. *How it's done: An invitation to social research*. 3rd ed. Stamford: Cengage Learning.

Agosto, D.E., Forte, A., and Magee, R., 2012. Cyberbullying and teens: What YA librarians can do to help. *Young Adult Library Services*, 10(2), pp. 38 - 43.

Alexa, 2014a. *The top 500 sites on the web* [Online]. Available at: http://www.alexa.com/topsites [Accessed: 15 June 2014].

Alexa, 2014b. *Top sites in Malaysia* [Online]. Available at: http://www.alexa.com/topsites/countries/MY [Accessed: 15 June 2014].

Anderson, J.A., 1982. Logistic regression. In: Krishnaiah, P.R., and Kanal, L.N. (eds.). *Handbook of statistics*. New York: North-Holland, pp. 169 – 191.

Anderson, S., 2001. *Logistic regression* [Online]. Available at: http://schatz.sju.edu/multivar/guide/logistic.pdf [Accessed: 15 July 2014].

Andrew, D.P., Pedersen, P.M. and McEvoy, C.D., 2011. *Research methods and design in sport management*. Illinois: Human Kinetics.

Ardito, S.C., 2003. Information brokers and cyberstalking. *Information Today*, 20(5), pp. 17 - 23.

Arora, R. and Mahankale, N.R., 2012. *Marketing research.* Delhi: PHI Learning Pvt. Ltd.

Asadoorian, M.O. and Kantarelis, D., 2005. *Essentials of inferential statistics*. Maryland: University Press of America.

Baines, P., Fill, C. and Page, K., 2010. *Marketing*. Oxford: Oxford University Press.

Bajrektarevic, A.H., 2012. Is there life after Facebook? - Addendum the cyber gulag revisited & debate reloaded. *Review of Contemporary Philosophy*, 11, pp. 125 - 134.

Banerjee, N. and Dey, A.K., 2013. Identifying the factors influencing users' adoption of social networking websites: A study on Facebook. *International Journal of Marketing Studies*, 5(6), pp. 109 - 127.

Basu, S. and Jones, R., 2007. *Regulating cyberstalking* [Online]. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/basu_jones/basu_jones.pdf [Accessed: 30 June 2013].

Bocij, P., 2004. *Cyberstalking: Harassment in the internet age and how to protect your family.* Connecticut: Greenwood Publishing Group.

Brandtzæg, P.B. and Heim, J., 2009. Why people use social networking sites. *Online Communities and Social Computing*, pp. 143 – 152.

Burnham, K, 2011. *Four Facebook security tips to stay safe in 2012* [Online]. Available at: http://www.cio.com/article/696212/4_Facebook_Security_Tips_to_Stay_Safe_in_2012_ [Accessed: 15 January 2014].

CNN, 2014. *Is the new Facebook friend-tracking feature a potential stalking tool?* [Online]. Available at: http://fox6now.com/2014/04/17/facebook-launches-friend-tracking-feature-but-is-it-a-potential-stalking-tool/ [Accessed: 30 August 2014].

Cocheo, S., 2009. Shred your marketing beliefs at the door: As community banks explore social media like Twitter, Facebook, and Linkedin, fresh thinking helps. Social media marketing is different. *ABA Banking Journal,* 101(6), pp. 12 - 19.

Cutlack, G., 2014. *Facebook's compulsory messenger push angers the commenting horde* [Online]. Available at: http://www.techradar.com/news/world-of-tech/facebook-s-compulsory-messenger-push-angers-the-commenting-horde-1260017 [Accessed: 11 September 2014].

Cyber Security Malaysia, 2014a. *Information security best practice series: Cyberstalking* [Online]. Available at: http://www.cybersecurity.my/data/content_files/11/573.pdf [Accessed: 19 February 2014].

Cyber Security Malaysia, 2014b. *MyCERT incident statistics* [Online]. Available at: http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html [Accessed: 29 January 2014].

Daily Mail, 2011. *Facebook founder Mark Zurkerberg is stalked by obsessed fan on his own website* [Online]. Available at: http://www.dailymail.co.uk/news/article-1354789/Facebook-founder-Mark-Zuckerberg-stalked-online-obsessive-fan.html [Accessed: 1 January 2014].

DeGusta, M., 2012. *Are smart phones spreading faster than any technology in human history?* [Online]. Available at: http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any/ [Accessed: 17 June 2013].

Delaney, P.M., 2012. Sorry Linus, I need your security blanket: How the smartphone, constant connectivity with the Internet, and social networks act as catalysts for juror misconduct. *St. Thomas Law Review*, 24(3), pp. 473 - 480.

Discovery Communication, 2012. *Top 10 social networking sites* [Online]. Available at: http://news.discovery.com/tech/apps/top-ten-social-networking-sites.htm [Accessed: 15 June 2013].

Do, T.M.T., Blom, J. and Perez, D.G., 2011. Smartphone usage in the wild: a large-scale analysis of applications and context. *In Proceedings of the 13th international conference on multimodal interfaces*, 2011 New York, NY. New York: ACM, pp. 353 - 360.

EBiz MBA, 2014. *Top 15 most popular social networking sites* [Online]. Available at: http://www.ebizmba.com/articles/social-networking-websites [Accessed: 2 November 2014].

ECU, 2012. *Cyberstalking* [Online]. Available at: http://www.ecu.edu/cs-itcs/itsecurity/cyberstalking2.cfm [Accessed: 10 June 2013].

ESD, 2011. *Readability for job orders* [Online]. Available at: http://www.wa.gov/esd/training/elearning/business/02-05.pdf [Accessed: 7 September 2014].

Etherington, J.D., 2011. *Why are smartphones so popular?* [Online]. Available at: http://uberarticles.com/computers-and-technology/mobile/why-are-smartphones-so-popular/ [Accessed: 6 July 2013].

Facebook, 2014a. *Newsroom: Statistics* [Online]. Available at: http://newsroom.fb.com/company-info/ [Accessed: 5 November 2014].

Facebook, 2014b. *Extra security features* [Online]. Available at: https://www.facebook.com/help/413023562082171 [Accessed: 20 May 2014].

Flinders University, 2013. *What is SPSS?* [Online]. Available at: http://www.flinders.edu.au/library/research/eresearch/statistics-consulting/spss-licenses-and-technical-support/ [Accessed: 15 August 2014].

Garlik, 2007. *UK men fall victim to online stalking* [Online]. Available at: http://www.garlik.com/press/Garlik%20Press%20Release%20-%20Cyberstalking.doc [Accessed: 25 September 2014].

Gay, L.R. and Airasian, P., 2003. *Educational research: Competencies for analysis and applications*. 7th ed. New Jersey: Pearson/Merrill Prentice Hall.

Gideon, L., 2012. *Handbook of survey methodology for the social sciences*. Berlin: Springer Science & Business Media.

Gilchrist, R., 2010. *Danger of new Facebook apps* [Online]. Available at: http://www.channel4.com/news/articles/science_technology/danger+of+new+facebook+app+aposplacesapos/3769677.html [Accessed: 9 June 2013].

GO-Gulf, 2012. *Smartphone users around the world - statistics and facts [Infographic]* [Online]. Available at: http://www.go-gulf.com/blog/smartphone [Accessed: 19 June 2013].

Goodman, M., 2012. *How technology makes us vulnerable* [Online]. Available at: http://edition.cnn.com/2012/07/29/opinion/goodman-ted-crime [Accessed: 16 June 2013].

Göritz, A.S., 2006. Incentives in web studies: Methodological issues and a review. *International Journal of Internet Science*, 1(1), pp. 58 – 70.

Gross, D. and Hanna, J., 2010. *Facebook introduces check-in feature* [Online]. Available at: http://edition.cnn.com/2010/TECH/social.media/08/18/facebook.location/index.html [Accessed: 25 June 2013].

Hane, P.J., 2012. Facebook in the spotlight. *Information Today*, 29(7), pp. 8.

Haron, H. and Yusof, F.B.M., 2010. Cyber stalking: The social impact of social networking technology. *In Education and Management Technology (ICEMT), 2010 International Conference on*, IEEE, pp. 237 - 241.

Hensler-McGinnis, N.F., 2008. *Cyberstalking victimization: Impact and coping responses in a national university sample.* Michigan: ProQuest UMI Dissertation Publishing.

Henson, B., Reyns, B.W. and Fisher, B.S., 2011. Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal justice review*, 36(3), pp. 253 - 268.

Hillier, Y. and Jameson, J., 2003. *Empowering researchers in further education.* Staffordshire: Trentham Books.

Hoffmann, B.C., 2012. *An exploratory study of a user's Facebook security and privacy settings.* MSc Thesis, Minnesota State University, United States.

Ibrahim, I.H., 2001. *Differences between statistical software packages (SAS, SPSS and MINITAB): As applied to binary response variable* [Online]. Available at: www.ats.ucla.edu/stat/mult_pkg/library/CompBinary.doc [Accessed: 22 July 2013].

Jones, H. and Soltren, J.H., 2005. Facebook: Threats to privacy. *Massachusetts Institute of Technology*. Available through Massachusetts Institute of Technology website http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf [Accessed: 5 July 2013].

Kennesaw State University, 2013. *Reference manual for statistical software: A gentle overview of Excel, SPSS, Minitab, SAS* [Online]. Available at: http://science.kennesaw.edu/~jpriestl/STAT3010/Reference%20Manual%20for%20Statistical%20Software.pdf [Accessed: 23 July 2013].

Lafferman, M., 2012. Do Facebook and Twitter make you a public figure?: How to apply the gertz public figure doctrine to social media. *Santa Clara Computer & High Technology Law Journal*, 29(1), pp. 199 - 202.

Landau, H.B., 2011. *Winning library grants: A game plan.* Chicago: American Library Association.

Leary, M.R., 2008. *Introduction to behavioral research*. 5th ed. New Jersey: Pearson Education.

Lee, C.F., Lee, J.C. and Lee, A.C., 2000. *Statistics for business and financial economics, Volume 1*. Singapore: World Scientific.

Leedy, P.D. and Ormrod, J.E., 2005. *Practical research: Planning and design.* 8th ed. New Jersey: Pearson/Merrill Prentice Hall.

Leong, F.C., 2014. *Bread and kaya: Cyberstalking, harassment and road rage* [Online]. Available at: http://foongchengleong.com/2014/07/bread-kaya-cyberstalking-harassment-and-road-rage-see-more-at-httpwww-digitalnewsasia-cominsightsbread-and-kaya-cyberstalking-harassment-and-road/ [Accessed: 28 October 2014].

Leroy, G., 2011. *Designing user studies in informatics*. Berlin: Springer Science & Business Media.

Levitas, D., 2013. *Always connected: How smartphones and social keep us engaged* [Online]. Available at: https://fb-public.box.com/s/3iq5x6uwnqtq7ki4q8wk [Accessed: 20 June 2013].

Lewis, S.F., Fremouw, W.J., Del Ben, K. and Farr, C., 2001. An investigation of the psychological characteristics of stalkers: Empathy, problem-solving, attachment and borderline personality features. *Journal of Forensic Sciences*, 46(1), pp. 80 - 84.

Lin, J.Y., Le, A.N., Khalil, S. and Cheng, J.M., 2012. Social media usage and work values: The example of Facebook in Taiwan. *Social Behavior and Personality: An International Journal,* 40(2), pp. 195 - 202.

Mahadi, N., 2013. *13.3 million M'sians are Facebook users* [Online]. Available at: http://www.theborneopost.com/2013/06/16/13-3-million-msians-are-facebook-users/ [Accessed: 7 August 2013].

Maple, C., Short, E. and Brown, A., 2011. *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey* [Online]. Available at: http://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf [Accessed: 18 June 2013].

Mathiyalakan, S., Heilman, G. and White, S., 2013. Gender differences in student attitude toward privacy in Facebook. *Communications of the IIMA,* 13(4), pp. 35 - 44.

Matyszczyk, C., 2013. *Man can't stop ex from stalking him online after years* [Online]. Available at: http://www.cnet.com/news/man-cant-stop-ex-from-stalking-him-online-after-years/ [Accessed: 17 August 2014].

McClure, A., 2010. Friend or foe? Network security in the social media age. *University Business,* 13(10), pp. 50 - 61.

McCue, C., 2006. *Data mining and predictive analysis: Intelligence gathering and crime analysis.* Oxford: Butterworth-Heinemann.

MCMC, 2012. *Statistical brief number fourteen: Hand phone users survey 2012* [Online]. Available at: http://www.skmm.gov.my/skmmgovmy/media/General/pdf/130717_HPUS2012.pdf [Accessed: 1 January 2014].

MCMC, 2014. *Annual report 2012* [Online]. Available at: http://www.skmm.gov.my/skmmgovmy/media/General/pdf/MCMC_RET523-667P_ENGLISH_COMPLETE.pdf [Accessed: 1 May 2014].

McVeigh, K., 2011. *Cyberstalking now more common than face-to-face stalking* [Online]. Available at: http://www.guardian.co.uk/uk/2011/apr/08/cyberstalking-study-victims-men [Accessed: 16 June 2013].

Mensch, S. and Wilkie, L., 2011. Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), pp. 91 - 110.

Merritt, M., 2014. *Straight talk about cyberstalking* [Online]. Available at: http://us.norton.com/cyberstalking/article [Accessed: 7 October 2014].

Minitab, 2013. *Company overview* [Online]. Available at: http://www.minitab.com/en-GB/company/company-info/default.aspx [Accessed: 23 July 2013].

Moo, K., 2013. Review: face2face: Using Facebook, Twitter, and other social media tools to create great customer connections. *Journal of Library Innovation*, 4(1), pp. 71 - 89.

Muijs, D., 2004. *Doing quantitative research in education with SPSS.* California: Sage Publication.

Mullen, P.E., Pathé, M. and Purell, R., 2004. Stalking: Defining and prosecuting a new category of offending. *International Journal of Law and Psychiatry*, 27, pp. 157 – 169.

Murphy, D., 2012. *Facebook adds locations, read receipts to messenger app* [Online]. Available at: http://www.pcmag.com/article2/0,2817,2404031,00.asp [Accessed: 29 January 2014].

Neville, C., 2007. *Introduction to research and research methods* [Online]. Available at: http://www.brad.ac.uk/management/media/management/els/Introduction-to-Research-and-Research-Methods.pdf [Accessed: 30 August 2014].

Nobles, M.R., Reyns, B.W., Fox, K.A. and Fisher, B.S., 2012. Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, pp. 1 - 29.

Norton, 2012. *2012 Norton cybercrime report* [Online]. Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf [Accessed: 17 June 2013].

NWCCC, 2013. *Cyberstalking* [Online]. Available at: http://www.nw3c.org/docs/whitepapers/cyberstalking__(10-09)DEA10B7727C80144B56E5500.pdf?sfvrsn=8 [Accessed: 10 June 2013].

O'Brien, D. and Torres, A.M., 2012. Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 31(2), pp. 63 - 76.

Ogilvie, E., 2000. Cyberstalking. *Trends and issues in crime and criminal justice*, 166, pp. 1 - 16.

Page, C., 2014. *Facebook messenger now mandatory for mobile chat on iOS and Android* [Online]. Available at: http://www.theinquirer.net/inquirer/news/2357668/facebook-messenger-now-mandatory-for-mobile-chat-on-ios-and-android [Accessed: 11 September 2014].

Pannoni, A., 2014. *Facebook's messenger app shares your location by default* [Online]. Available at: http://busterandellie.com/facebooks-messenger-app-shares-your-location-with-everyone-you-message-by-default/ [Accessed: 10 June 2014].

Perez, S., 2010. *Nearby friends: New cyber-stalking app for tracking Facebook places check-ins* [Online]. Available at: http://readwrite.com/2010/08/30/nearby_friends_new_cyber-stalking_app_for_tracking_facebook_places_checkins#awesm=~ocBJc7iaibe7Ea [Accessed: 15 June 2013].

Perry, J., 2012. *Safer-settings.com secures social media for stalking victims* [Online]. Available at: http://www.eyepat.org/login/uploaded/Safer_Settings_launch_release_Final.pdf [Accessed: 20 May 2014].

Pettinari, D., 2002. *Cyberstalking investigation and prevention* [Online]. Available at: http://www.crime-research.org/library/Cyberstalking.htm [Accessed: 20 May 2014].

Pickard, A.J., 2007. *Research methods in information*. London: Facet.

Pinchot, J.L. and Paullet, K.L., 2012. What's in your profile? Mapping Facebook profile data to personal security questions. *Issues in Information Systems*, 13(1), pp. 284 – 293.

Piotrowski, C. and Lathrop, P.J., 2012. Cyberstalking and college-age students: A bibliometric analysis across scholarly databases. *College Student Journal*, 46(3), pp. 533 - 544.

Purcell, R., 2012. *Stop the trolls: how to prevent cyber stalking happening to you* [Online]. Available at: http://theconversation.com/stop-the-trolls-how-to-prevent-cyber-stalking-happening-to-you-5460 [Accessed: 27 June 2013].

Radhakrishna, R.B., 2007. Tips for developing and testing questionnaires/instruments. *Journal of Extension*, 45(1), pp. 1 - 4.

Reardon, M., 2008. *Smartphones drive demand for Web browsing* [Online]. Available at: http://news.cnet.com/8301-1035_3-10096614-94.html [Accessed: 18 June 2013].

Richardson, S., Guru, B.K., Yu, C.M., Wei, K.K. and Pointon, L., 2005. *How to research: A guide for undergraduate and graduate students*. Connecticut: Thomson Learning.

Riedel, C., 2008. The fight against cyberbullying: As tales of online cruelty mount, districts are trying a mix of prevention and punishment, incorporating internet safety into curriculum and tightening student conduct codes. *THE Journal (Technological Horizons in Education)*, 35(5), pp. 20 - 34.

Rouse, M., 2007. *Cyberstalking definition* [Online]. Available at: http://searchsecurity.techtarget.com/definition/cyberstalking [Accessed: 20 May 2014].

Sharon, M.E., 2010. *Checking in with friends* [Online]. Available at: https://blog.facebook.com/blog.php?post=418175202130 [Accessed: 25 June 2013].

Silva, G., 2014. *Facebook cyberstalking: The dark side of social media* [Online]. Available at: http://www.myfoxla.com/story/24044124/facebook-cyberstalking-the-dark-side-of-social-media [Accessed: 12 June 2014].

Singel, R., 2010. *Facebook launches 'check-in' service to connect people in real space* [Online]. Available at: http://www.wired.com/business/2010/08/watch-facebooks-location-sharing-announcement-live/ [Accessed: 25 June 2013].

Smith, A., 2011. *Smartphone adoption and usage* [Online]. Available at: http://www.pewinternet.org/Reports/2011/Smartphones/Summary.aspx [Accessed: 20 June 2013].

Song, H., 2013. *Here's how to turn off location sharing for Facebook messenger by default and why you should do it right away* [Online]. Available at: http://www.lowyat.net/2014/01/heres-how-to-turn-off-location-sharing-for-facebook-messenger-by-default-and-why-you-should-do-it-right-away/ [Accessed: 9 January 2014].

SPSS, 2009. *Corporate history* [Online]. Available at: http://www.spss.com.hk/corpinfo/history.htm [Accessed: 23 July 2013].

Stuart, R., 2014. Science of social media: The prevalence and ever-changing nature of social media is both a benefit to and problem for students and universities. *Diverse Issues in Higher Education*, 31(6), pp. 18 - 23.

The Star, 2010. *Survey: Malaysians have most Facebook friends* [Online]. Available at: http://www.thestar.com.my/story/?file=%2f2010%2f10%2f13%2fnation%2f7212273 [Accessed: 10 May 2014].

The Week, 2012. *The future of smartphone growth: By the numbers* [Online]. Available at: http://theweek.com/article/index/224535/the-future-of-smartphone-growth-by-the-numbers [Accessed: 20 June 2013].

THR, 2011. *Mark Zuckerberg obtains restraining order against Facebook stalker* [Online]. Available at: http://www.hollywoodreporter.com/news/mark-zuckerberg-obtains-restraining-order-97234 [Accessed: 1 January 2014].

Tuffery, S., 2011. *Data mining and statistics for decision making.* New Jersey: John Wiley & Sons.

Vogt, W.P., Gardner, D.C., Vogt, E.R. and Haeffele, L.M., 2014. *Selecting the right analyses for your data: Quantitative, qualitative and mixed methods*. New York: Guilford Publications.

Williams, J., Feild, C. and James, K., 2011. The effects of a social media policy on pharmacy students' Facebook security settings. *American Journal of Pharmaceutical Education*, 75(9).

Wimmer, R. and Dominick, J., 2013. *Mass media research*. 10th ed. Stanford: Cengage Learning.

Wolak, J., Finkelhor, D., Mitchell, K.J. and Ybarra, M.L., 2008. Online predators and their victims. *American Psychological Association*, 63(2), pp. 111 – 128.

Wrenn, E., 2012. *Half of Facebook users accept 'friend requests' from strangers, while 13m U.S. users have never opened their privacy settings* [Online]. Available at: http://www.dailymail.co.uk/sciencetech/article-2139424/Half-Facebook-users-accept-friend-requests-strangers-13m-U-S-users-NEVER-opened-privacy-settings.html [Accessed: 15 August 2014].

Yap, J., *Malaysia has most online friends globally* [Online]. Available at: http://www.zdnet.com/malaysia-has-most-online-friends-globally-2062203590/ [Accessed: 10 May 2014].

Zikmund, W. and Babin, B., 2006. *Exploring marketing research*. 9th ed. Stanford: Cengage Learning.

Appendix A

Survey Questionnaire

Cyberstalking on Facebook

Dear Valued Respondent,
I am Alan Chew, a postgraduate student currently pursuing my Master of Information Systems at Universiti Tunku Abdul Rahman (UTAR). In partial fulfillment of my dissertation, I am required to conduct a survey which aims to study the incidents of cyberstalking on Facebook in Malaysia.

The participating respondents for this study must be a MALAYSIAN CITIZEN, AGED between 20 to 30 years old, and also a REGISTERED USER of FACEBOOK.

I would be grateful if you could spend 10 minutes of your precious time to complete this survey. The validity of this study highly depends on your ingenuous and truthful response.

Please be assured that all information collected for this survey will be kept confidential and would be used strictly for academic purpose only. Your time and cooperation is highly appreciated.
Thank you.

Definition of Cyberstalking

By definition, cyberstalking is described as “a group of behaviours in which individual or group of people use information and communication technology (ICT) to harass another individual or group of people".
These behaviours include but not limited to:

1) Transmission of threats
2) False accusations
3) Identity theft
4) Data theft
5) Electronic sabotage (sending viruses or malware)
6) Damage to data or equipment
7) Computer monitoring
8) Solicitation for sexual purposes
9) Any form of aggression

* Required

Section A – Actual Usage of Facebook

This section of the questionnaire explores your habits and preferences, if any, with regard to the usage of Facebook.

1. In a typical day, how many times do you browse your Facebook using either your computers or smartphones? *

   ○ Less than 6
   ○ 6 to 10
   ○ 11 to 15
   ○ More than 16

2. How many friends do you have on your Facebook account? *

   ○ Less than 100
   ○ 100 to 500
   ○ 501 to 1000
   ○ More than 1000

3. Why do you use Facebook? (Please tick all that apply) *

   □ To make new friends
   □ Keep in touch with friends
   □ Keep in touch with family members
   □ Keep up-to-date with the latest news
   □ Debating with others
   □ Find dates
   □ Chatting
   □ Time-killing
   □ Learn new things
   □ Publish updates, pictures or videos
   □ View status, pictures or videos of others
   □ Promote own business or work
   □ Other: ___________________________

4. Which of the following information have you revealed on your Facebook profile? (Please tick all that apply) *

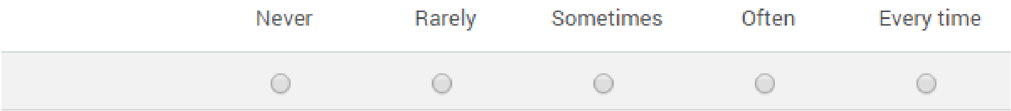
   □ Real name
   □ Age
   □ Date of birth
   □ Gender
   □ Email address

❑ Phone number
❑ Home address
❑ Workplace / University
❑ Interest
❑ Family members
❑ Relationship status
❑ Other: ____________________________

Section B – Usage Characteristics of Facebook Features

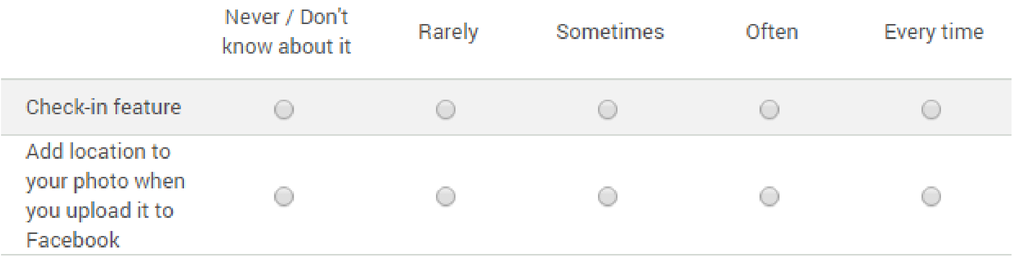
This section of the questionnaire captures your usage frequency of certain Facebook features.

5. How often do you accept friend requests from people you DO NOT know in Facebook? *



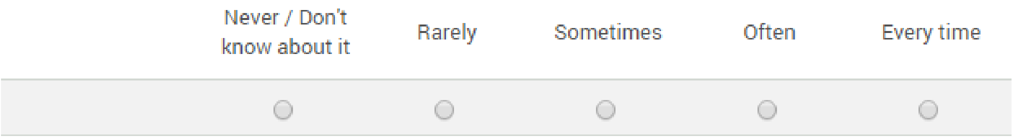
	Never	Rarely	Sometimes	Often	Every time
	○	○	○	○	○

6. How often do you use Facebook location tagging features listed below? *



	Never / Don't know about it	Rarely	Sometimes	Often	Every time
Check-in feature	○	○	○	○	○
Add location to your photo when you upload it to Facebook	○	○	○	○	○

7. How often do you use Facebook Messenger app on your smartphone to chat with your friends? *



	Never / Don't know about it	Rarely	Sometimes	Often	Every time
	○	○	○	○	○

8. Are you aware that Facebook Messenger app on your smartphone automatically shares your precise location on a map, to the person you are chatting with (this feature is enabled by default)? *

○ Yes
○ No

9. Did you turn off the location sharing setting for Facebook Messenger app in your smartphone? *

○ Yes
○ No
○ I am not sure

10. Have you ever received attacks listed below on Facebook or resulting from the use of Facebook? (Please tick all that apply) *

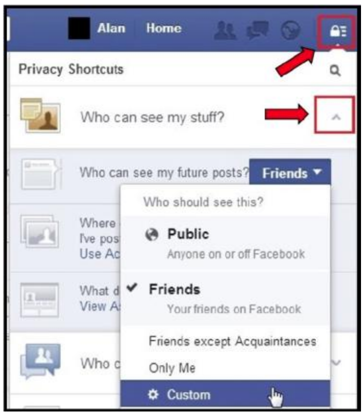
□ Received threat or hostile messages
□ Received sexual messages
□ Received viruses or malware
□ Account hijacked or password stolen
□ Account used to send false accusations
□ Someone spread vicious rumors about you
□ Account pretending to be you (identity theft / impersonation)
□ Vandalism of private property
□ Real life physical attack
□ Never received above-mentioned attacks

Section C – Facebook Privacy and Security Settings

This section of the questionnaire explores your Facebook privacy and security settings.

11. What PRIVACY setting is your Facebook currently set to? (Please refer to the picture below) *

○ Public
○ Friends
○ Friends except Acquaintances
○ Only Me
○ Custom



12. Have you ever modified your PRIVACY settings in Facebook? *

○ Yes *Skip to question 13.*
○ No *Skip to question 14.*
○ I am not sure *Skip to question 14.*

13. What is the reason for modifying your PRIVACY settings in Facebook? (Please tick all that apply) *

❑ Limit others from viewing my future posts
❑ Limit others from viewing my old posts
❑ Limit others from sending me friend requests
❑ Limit others from finding my profile using my email address
❑ Limit others from finding my profile using my phone number
❑ Limit search engines from finding my profile
❑ Limit others from posting on my timeline
❑ Limit others from tagging me
❑ Filter messages that go into my Facebook Inbox
❑ Other: ___________________________

14. Do you leave your Facebook SECURITY settings on default? *

○ Yes *Skip to question 16.*
○ No *Skip to question 15.*
○ I am not sure *Skip to question 16.*

15. What changes have you made to your Facebook SECURITY settings? (Please tick all that apply) *

❑ Enable login notification feature (receive notification when your Facebook account is accessed)
❑ Enable login approval feature (require a security code in order to log in to your
Facebook account)
❑ Enable App passwords for Facebook applications
❑ Add trusted contacts to list (in case you have trouble accessing your Facebook account)
❑ Other: ___________________________

Section D – Perception on Cyberstalking

This section of the questionnaire gathers your perception of cyberstalking.

16. Have you heard of the term “cyberstalking” prior to this survey? *

○ Yes
○ No

17. In your own opinion, is cyberstalking a serious crime? *

○ Yes
○ No
○ I have no idea

Section E – Demographic Information

This section of the questionnaire refers to background or biographical information. Although we are aware of the sensitivity of the questions in this section, the information will allow us to combine your responses with those of the other people taking part in this study. Once again, we assure you that your response will remain anonymous and will be kept strictly confidential.

18. Please select your age: *

○ 20
○ 21
○ 22
○ 23
○ 24
○ 25
○ 26
○ 27
○ 28
○ 29
○ 30

19. Please select your gender: *

○ Male
○ Female

20. Which state of Malaysia do you currently live in? *

○ Johor

○ Kedah
○ Kelantan
○ Melacca
○ Negeri Sembilan
○ Pahang
○ Penang
○ Perak
○ Perlis
○ Sabah
○ Sarawak
○ Selangor
○ Terengganu
○ Federal Territory of Kuala Lumpur
○ Federal Territory of Labuan
○ Federal Territory of Putrajaya

21. Which of the following categories best corresponds with your last completed year in school: *

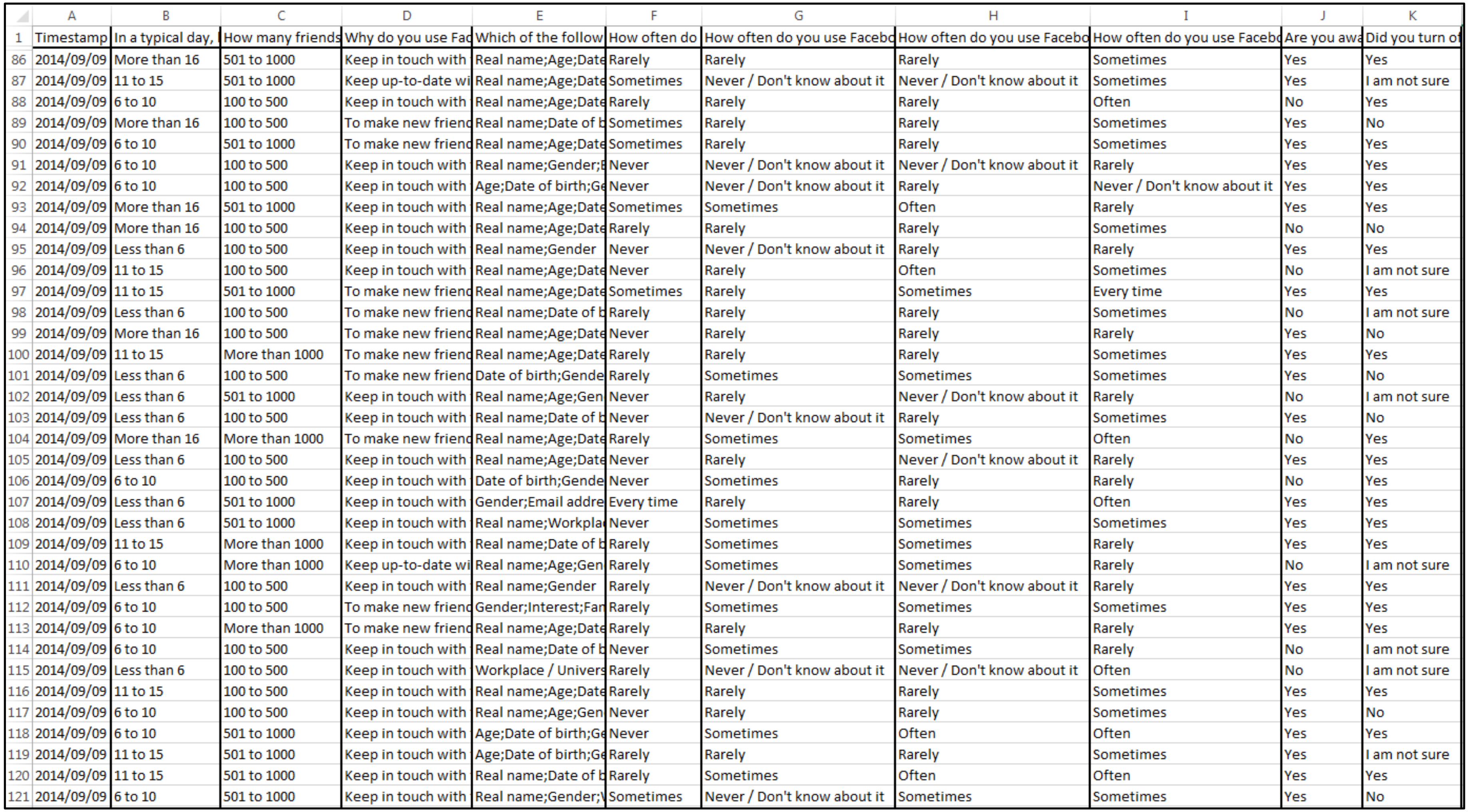
○ High school or equivalent
○ Completed some college
○ Diploma
○ Bachelor's degree
○ Master's degree
○ Doctoral degree
○ Professional degree (MD, JD, etc.)
○ Other: ___________________________

22. Which of the following categories best describes the industry you work in:*

○ Student
○ Unemployed
○ Retiree
○ IT and Engineering
○ Health Care Industry
○ Education and Training
○ Retail and Distribution
○ Service and Hospitality
○ Government Sector
○ Leisure and Entertainment
○ Economy and Finance
○ Property and Construction
○ Other: ___________________________

Appendix B

Sample Data from Respondents



	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	In a typical day,	How many friends	Why do you use Fac	Which of the follow	How often do	How often do you use Facebo	How often do you use Facebo	How often do you use Facebo	Are you awa	Did you turn of
86	2014/09/09	More than 16	501 to 1000	Keep in touch with	Real name;Age;Date	Rarely	Rarely	Rarely	Sometimes	Yes	Yes
87	2014/09/09	11 to 15	501 to 1000	Keep up-to-date wi	Real name;Age;Date	Sometimes	Never / Don't know about it	Never / Don't know about it	Sometimes	Yes	I am not sure
88	2014/09/09	6 to 10	100 to 500	Keep in touch with	Real name;Age;Date	Rarely	Rarely	Rarely	Often	No	Yes
89	2014/09/09	More than 16	100 to 500	To make new friend	Real name;Date of b	Sometimes	Rarely	Rarely	Sometimes	Yes	No
90	2014/09/09	6 to 10	501 to 1000	To make new friend	Real name;Age;Date	Sometimes	Rarely	Rarely	Sometimes	Yes	Yes
91	2014/09/09	6 to 10	100 to 500	Keep in touch with	Real name;Gender;E	Never	Never / Don't know about it	Never / Don't know about it	Rarely	Yes	Yes
92	2014/09/09	6 to 10	100 to 500	Keep in touch with	Age;Date of birth;Ge	Never	Never / Don't know about it	Rarely	Never / Don't know about it	Yes	Yes
93	2014/09/09	More than 16	501 to 1000	Keep in touch with	Real name;Age;Date	Sometimes	Sometimes	Often	Rarely	Yes	Yes
94	2014/09/09	More than 16	100 to 500	Keep in touch with	Real name;Age;Date	Rarely	Rarely	Rarely	Sometimes	No	No
95	2014/09/09	Less than 6	100 to 500	Keep in touch with	Real name;Gender	Never	Never / Don't know about it	Rarely	Rarely	Yes	Yes
96	2014/09/09	11 to 15	100 to 500	Keep in touch with	Real name;Age;Date	Never	Rarely	Often	Sometimes	No	I am not sure
97	2014/09/09	11 to 15	501 to 1000	To make new friend	Real name;Age;Date	Sometimes	Rarely	Sometimes	Every time	Yes	Yes
98	2014/09/09	Less than 6	100 to 500	To make new friend	Real name;Date of b	Rarely	Rarely	Rarely	Sometimes	No	I am not sure
99	2014/09/09	More than 16	100 to 500	To make new friend	Real name;Age;Date	Never	Rarely	Rarely	Rarely	Yes	No
100	2014/09/09	11 to 15	More than 1000	To make new friend	Real name;Age;Date	Rarely	Rarely	Rarely	Sometimes	Yes	Yes
101	2014/09/09	Less than 6	100 to 500	To make new friend	Date of birth;Gende	Rarely	Sometimes	Sometimes	Sometimes	Yes	No
102	2014/09/09	Less than 6	501 to 1000	Keep in touch with	Real name;Age;Gen	Never	Rarely	Never / Don't know about it	Rarely	No	I am not sure
103	2014/09/09	Less than 6	100 to 500	Keep in touch with	Real name;Date of b	Never	Never / Don't know about it	Rarely	Sometimes	Yes	No
104	2014/09/09	More than 16	More than 1000	To make new friend	Real name;Age;Date	Rarely	Sometimes	Sometimes	Often	No	Yes
105	2014/09/09	Less than 6	100 to 500	Keep in touch with	Real name;Age;Date	Never	Rarely	Never / Don't know about it	Rarely	Yes	Yes
106	2014/09/09	6 to 10	100 to 500	Keep in touch with	Date of birth;Gende	Never	Sometimes	Rarely	Rarely	No	Yes
107	2014/09/09	Less than 6	501 to 1000	Keep in touch with	Gender;Email addre	Every time	Rarely	Rarely	Often	Yes	Yes
108	2014/09/09	Less than 6	501 to 1000	Keep in touch with	Real name;Workpla	Never	Sometimes	Sometimes	Sometimes	Yes	Yes
109	2014/09/09	11 to 15	More than 1000	Keep in touch with	Real name;Date of b	Rarely	Sometimes	Sometimes	Rarely	Yes	Yes
110	2014/09/09	6 to 10	More than 1000	Keep up-to-date wi	Real name;Age;Gen	Rarely	Sometimes	Sometimes	Rarely	No	I am not sure
111	2014/09/09	Less than 6	100 to 500	Keep in touch with	Real name;Gender	Rarely	Never / Don't know about it	Never / Don't know about it	Rarely	Yes	Yes
112	2014/09/09	6 to 10	100 to 500	To make new friend	Gender;Interest;Far	Rarely	Sometimes	Sometimes	Sometimes	Yes	Yes
113	2014/09/09	6 to 10	More than 1000	To make new friend	Real name;Age;Date	Rarely	Rarely	Rarely	Rarely	Yes	Yes
114	2014/09/09	6 to 10	100 to 500	Keep in touch with	Real name;Date of b	Never	Sometimes	Sometimes	Rarely	No	I am not sure
115	2014/09/09	Less than 6	100 to 500	Keep in touch with	Workplace / Univers	Rarely	Never / Don't know about it	Never / Don't know about it	Often	No	I am not sure
116	2014/09/09	11 to 15	100 to 500	Keep in touch with	Real name;Age;Date	Rarely	Rarely	Rarely	Sometimes	Yes	Yes
117	2014/09/09	6 to 10	100 to 500	Keep in touch with	Real name;Age;Gen	Never	Rarely	Rarely	Sometimes	Yes	No
118	2014/09/09	6 to 10	501 to 1000	Keep in touch with	Age;Date of birth;Ge	Never	Sometimes	Often	Often	Yes	Yes
119	2014/09/09	11 to 15	501 to 1000	Keep in touch with	Age;Date of birth;Ge	Rarely	Rarely	Rarely	Sometimes	Yes	I am not sure
120	2014/09/09	11 to 15	501 to 1000	Keep in touch with	Real name;Date of b	Rarely	Sometimes	Often	Often	Yes	Yes
121	2014/09/09	6 to 10	501 to 1000	Keep in touch with	Real name;Gender;\	Sometimes	Never / Don't know about it	Sometimes	Sometimes	Yes	No

Appendix C

Pilot Test Cronbach's Alpha Results

Reliability of the Usage Characteristics of Facebook Location Tagging Features

Case Processing Summary

		N	%
Cases	Valid	20	100.0
	Excluded[a]	0	.0
	Total	20	100.0

Reliability Statistics

Cronbach's Alpha	N of Items
.767	2

Item Statistics

	Mean	Std. Deviation	N
checkIn	1.55	.826	20
addLocationToPhoto	1.95	1.050	20

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
checkIn	1.95	1.103	.641	.
addLocationToPhoto	1.55	.682	.641	.

Scale Statistics

Mean	Variance	Std. Deviation	N of Items
3.50	2.895	1.701	2

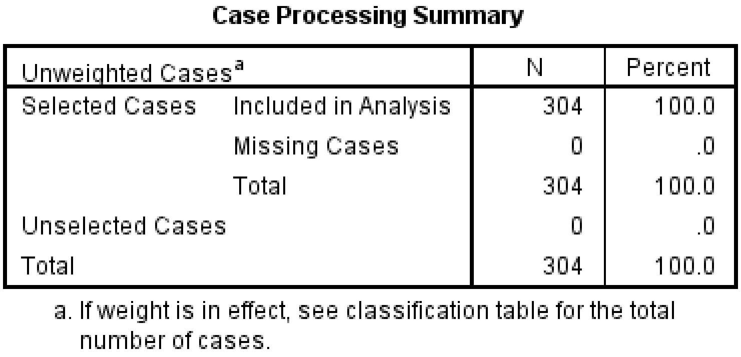
Appendix D

Full Results of Binary Logistic Regression Analysis

Results of Binary Logistic Regression for Hypothesis $H_0$1a

Logistic Regression

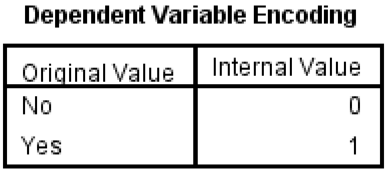
```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```



Case Processing Summary

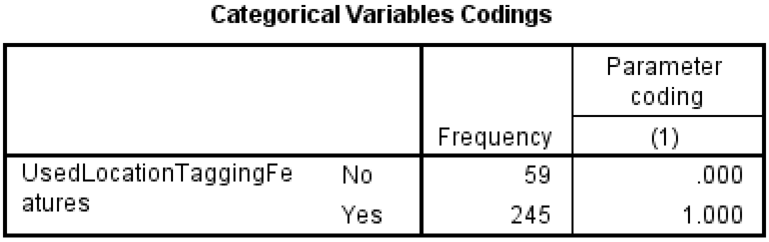
Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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



Dependent Variable Encoding

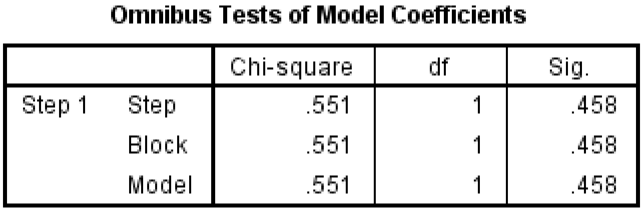
Original Value	Internal Value
No	0
Yes	1



Categorical Variables Codings

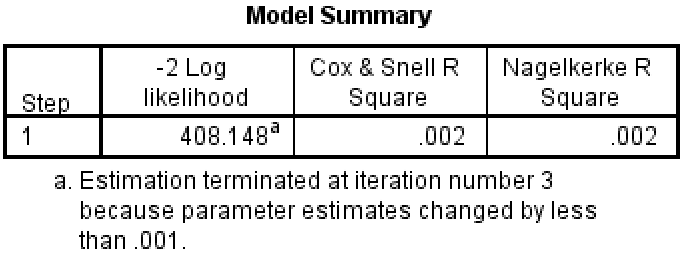
		Frequency	Parameter coding
			(1)
UsedLocationTaggingFeatures	No	59	.000
	Yes	245	1.000

Block 1: Method = Enter



Omnibus Tests of Model Coefficients

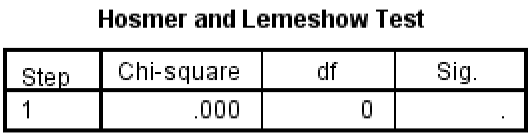
		Chi-square	df	Sig.
Step 1	Step	.551	1	.458
	Block	.551	1	.458
	Model	.551	1	.458



Model Summary

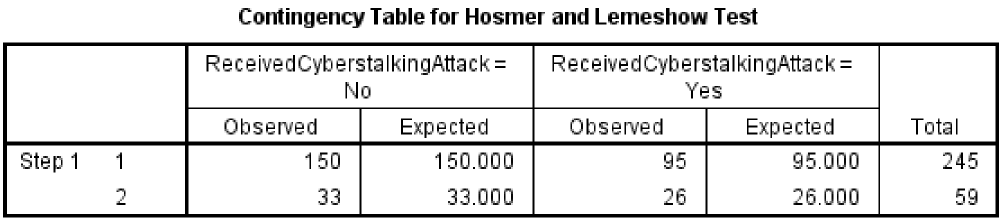
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	408.148[a]	.002	.002

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.



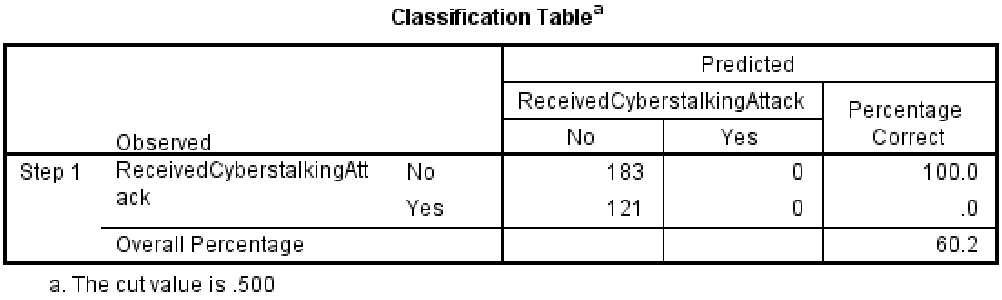
Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	.000	0	.



Contingency Table for Hosmer and Lemeshow Test

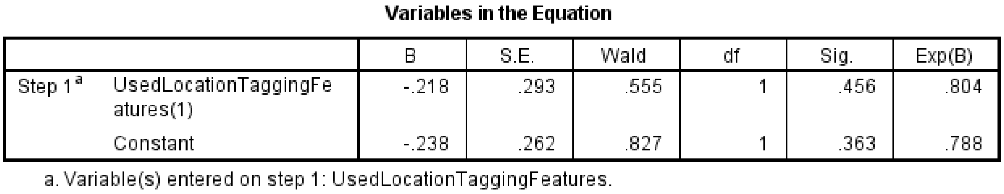
		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		
		Observed	Expected	Observed	Expected	Total
Step 1	1	150	150.000	95	95.000	245
	2	33	33.000	26	26.000	59



Classification Table[a]

			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
	Observed		No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	183	0	100.0
		Yes	121	0	.0
	Overall Percentage				60.2

a. The cut value is .500



Variables in the Equation

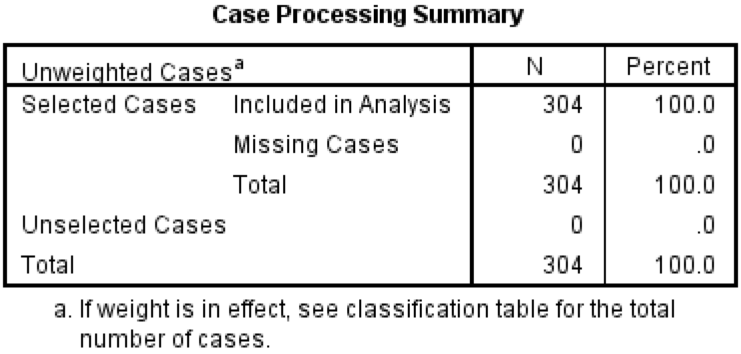
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	UsedLocationTaggingFeatures(1)	-.218	.293	.555	1	.456	.804
	Constant	-.238	.262	.827	1	.363	.788

a. Variable(s) entered on step 1: UsedLocationTaggingFeatures.

Results of Binary Logistic Regression for Hypothesis $H_0$1b

Logistic Regression

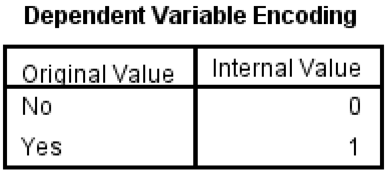
```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```



Case Processing Summary

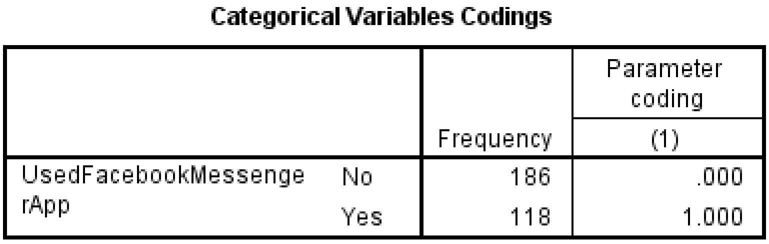
Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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



Dependent Variable Encoding

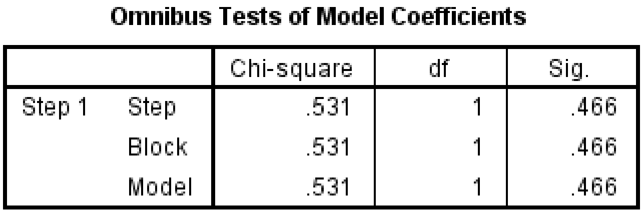
Original Value	Internal Value
No	0
Yes	1



Categorical Variables Codings

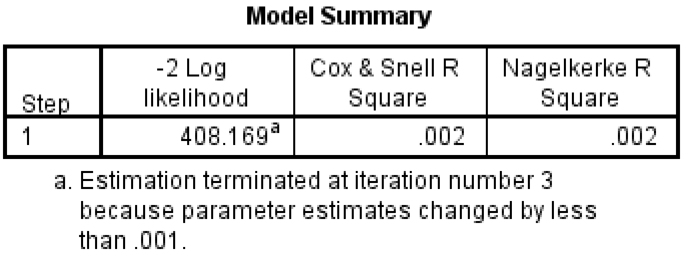
		Frequency	Parameter coding
			(1)
UsedFacebookMessengerApp	No	186	.000
	Yes	118	1.000

Block 1: Method = Enter



Omnibus Tests of Model Coefficients

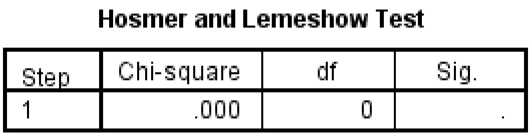
		Chi-square	df	Sig.
Step 1	Step	.531	1	.466
	Block	.531	1	.466
	Model	.531	1	.466



Model Summary

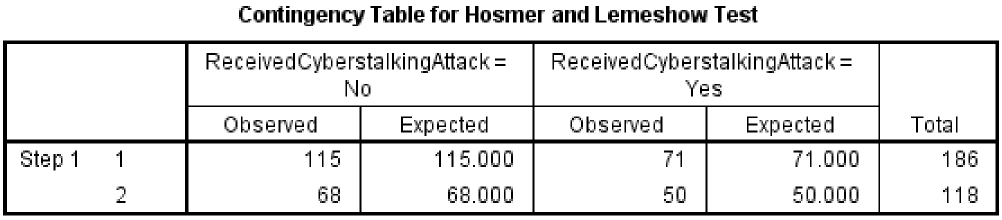
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	408.169[a]	.002	.002

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.



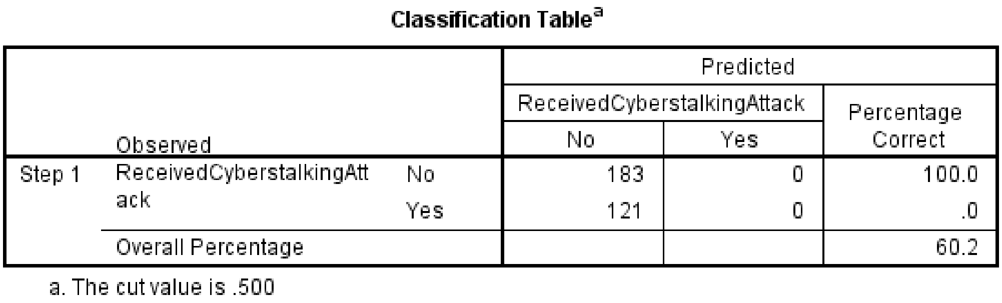
Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	.000	0	.



Contingency Table for Hosmer and Lemeshow Test

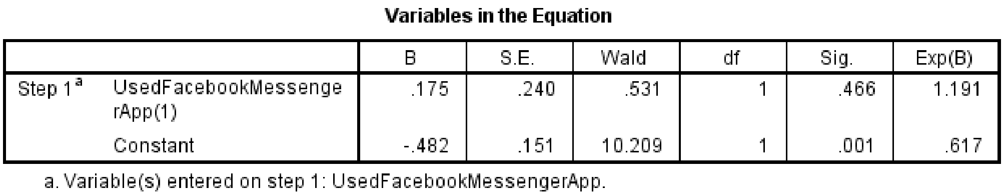
		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		
		Observed	Expected	Observed	Expected	Total
Step 1	1	115	115.000	71	71.000	186
	2	68	68.000	50	50.000	118



Classification Table[a]

Observed			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
			No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	183	0	100.0
		Yes	121	0	.0
	Overall Percentage				60.2

a. The cut value is .500



Variables in the Equation

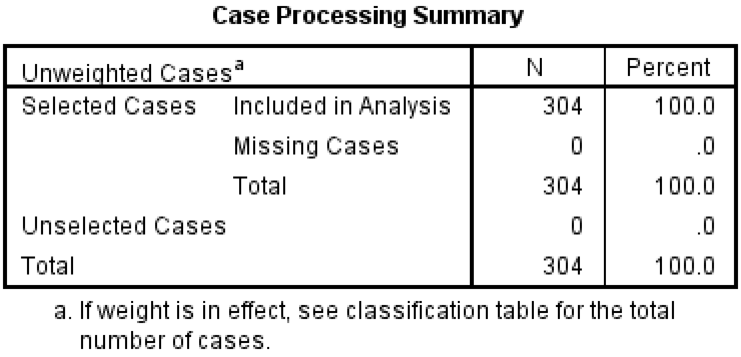
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	UsedFacebookMessengerApp(1)	.175	.240	.531	1	.466	1.191
	Constant	-.482	.151	10.209	1	.001	.617

a. Variable(s) entered on step 1: UsedFacebookMessengerApp.

Results of Binary Logistic Regression for Hypothesis $H_0 2$

Logistic Regression

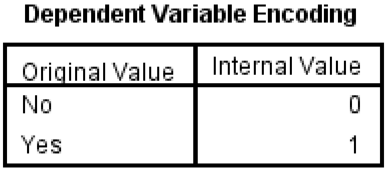
```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```



Case Processing Summary

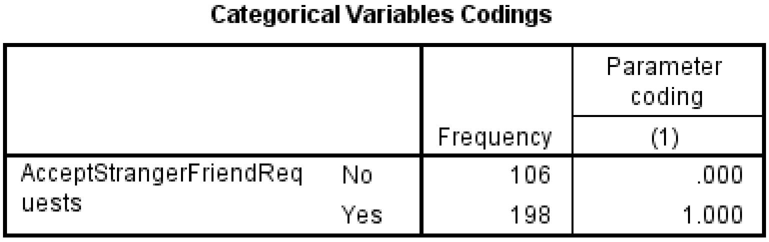
Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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



Dependent Variable Encoding

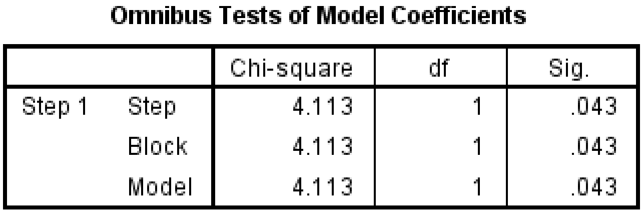
Original Value	Internal Value
No	0
Yes	1



Categorical Variables Codings

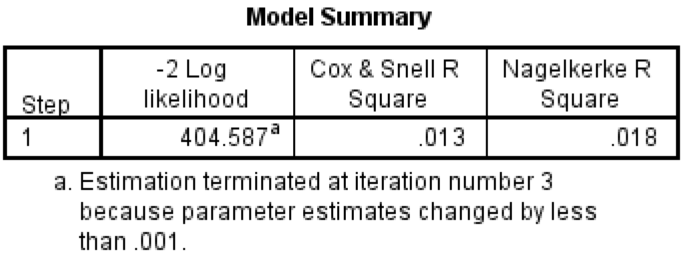
		Frequency	Parameter coding
			(1)
AcceptStrangerFriendRequests	No	106	.000
	Yes	198	1.000

Block 1: Method = Enter



Omnibus Tests of Model Coefficients

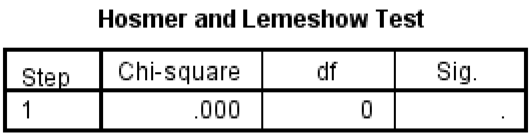
		Chi-square	df	Sig.
Step 1	Step	4.113	1	.043
	Block	4.113	1	.043
	Model	4.113	1	.043



Model Summary

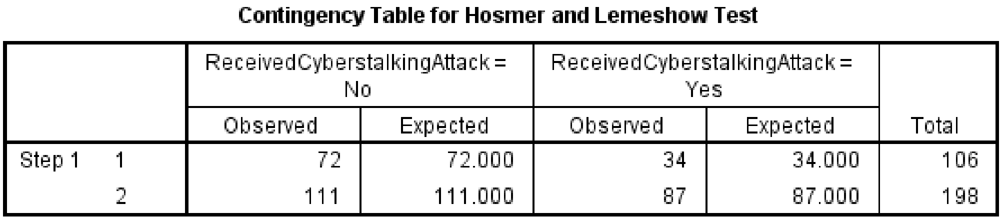
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	404.587[a]	.013	.018

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.



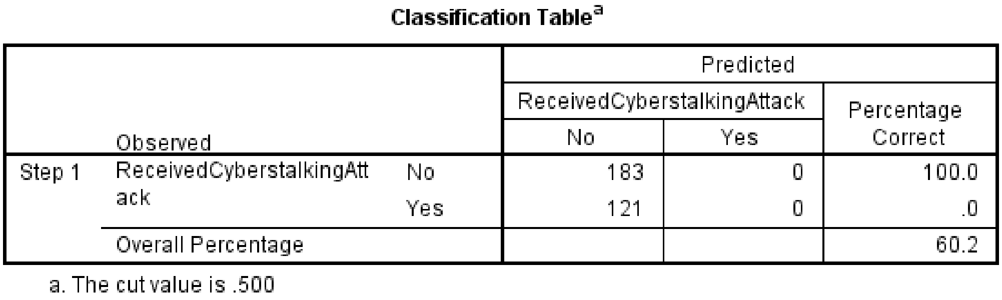
Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	.000	0	.



Contingency Table for Hosmer and Lemeshow Test

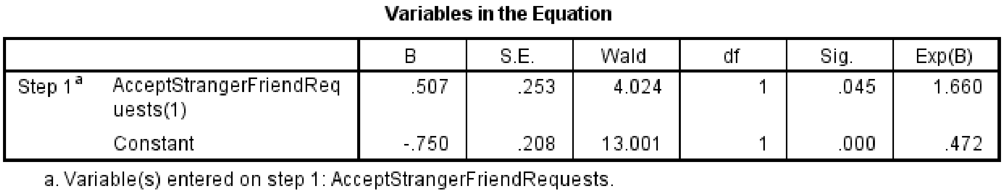
		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		
		Observed	Expected	Observed	Expected	Total
Step 1	1	72	72.000	34	34.000	106
	2	111	111.000	87	87.000	198



Classification Table[a]

			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
	Observed		No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	183	0	100.0
		Yes	121	0	.0
	Overall Percentage				60.2

a. The cut value is .500

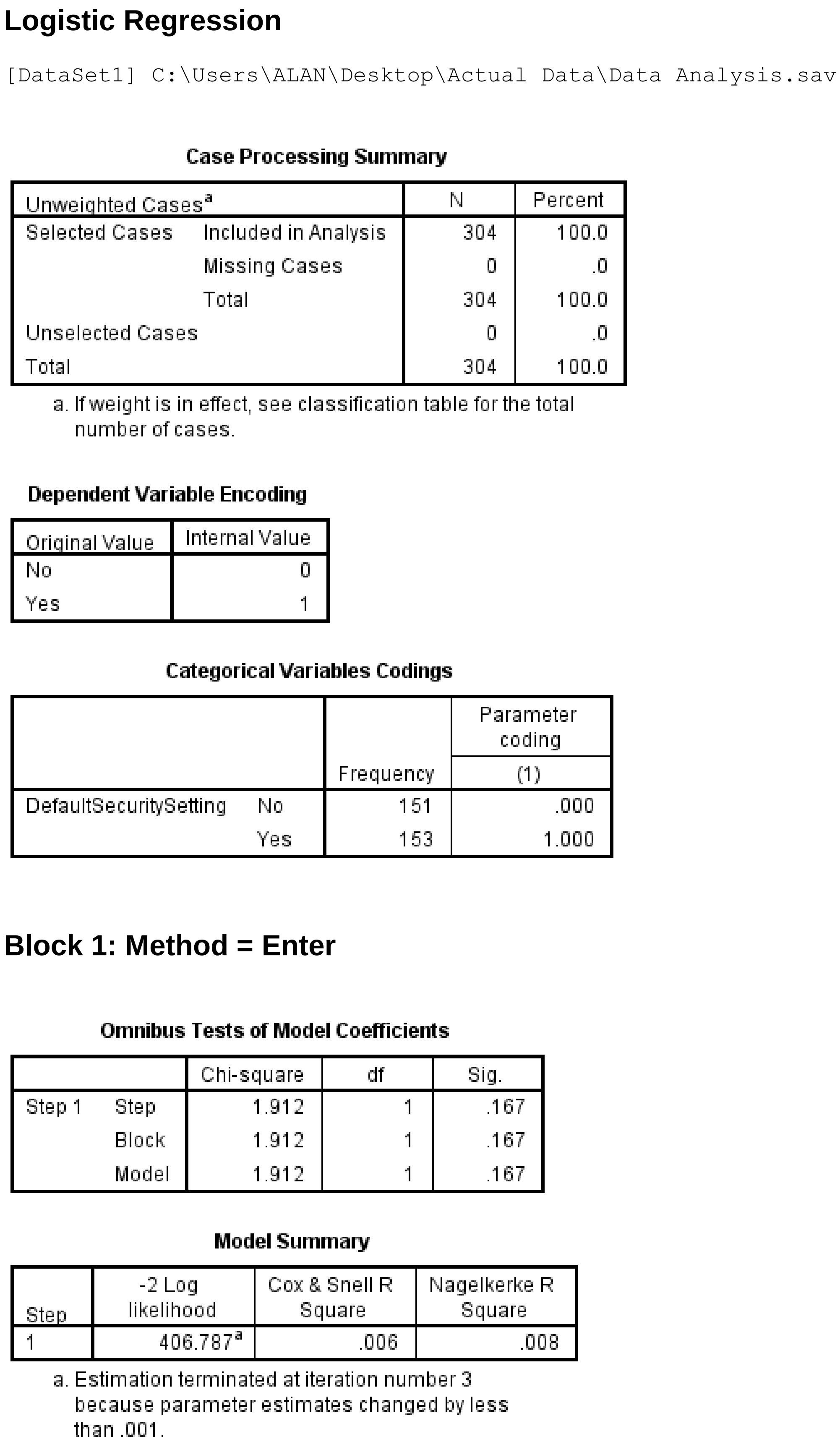


Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	AcceptStrangerFriendRequests(1)	.507	.253	4.024	1	.045	1.660
	Constant	-.750	.208	13.001	1	.000	.472

a. Variable(s) entered on step 1: AcceptStrangerFriendRequests.

Results of Binary Logistic Regression for Hypothesis H_03



Logistic Regression

```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```

Case Processing Summary

Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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

Dependent Variable Encoding

Original Value	Internal Value
No	0
Yes	1

Categorical Variables Codings

			Parameter coding
		Frequency	(1)
DefaultSecuritySetting	No	151	.000
	Yes	153	1.000

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

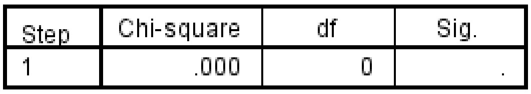
		Chi-square	df	Sig.
Step 1	Step	1.912	1	.167
	Block	1.912	1	.167
	Model	1.912	1	.167

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	406.787[a]	.006	.008

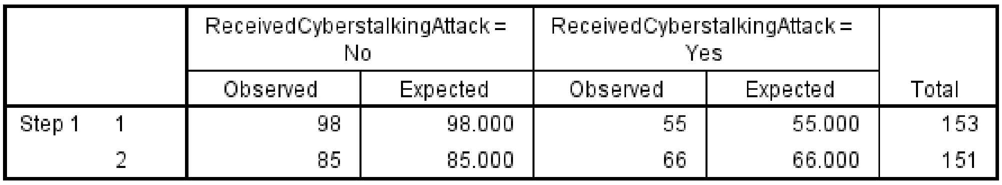
a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.

Hosmer and Lemeshow Test



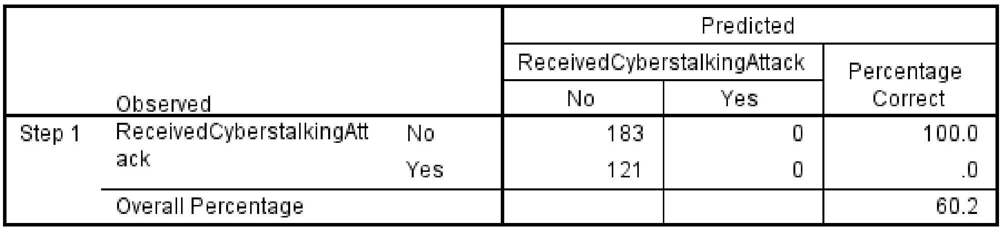
Step	Chi-square	df	Sig.
1	.000	0	.

Contingency Table for Hosmer and Lemeshow Test



		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		
		Observed	Expected	Observed	Expected	Total
Step 1	1	98	98.000	55	55.000	153
	2	85	85.000	66	66.000	151

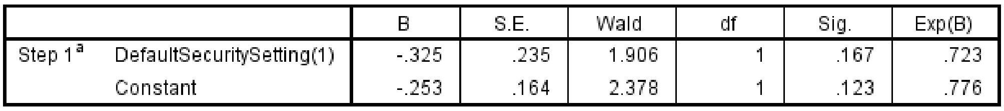
Classification Table[a]



			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
	Observed		No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	183	0	100.0
		Yes	121	0	.0
	Overall Percentage				60.2

a. The cut value is .500

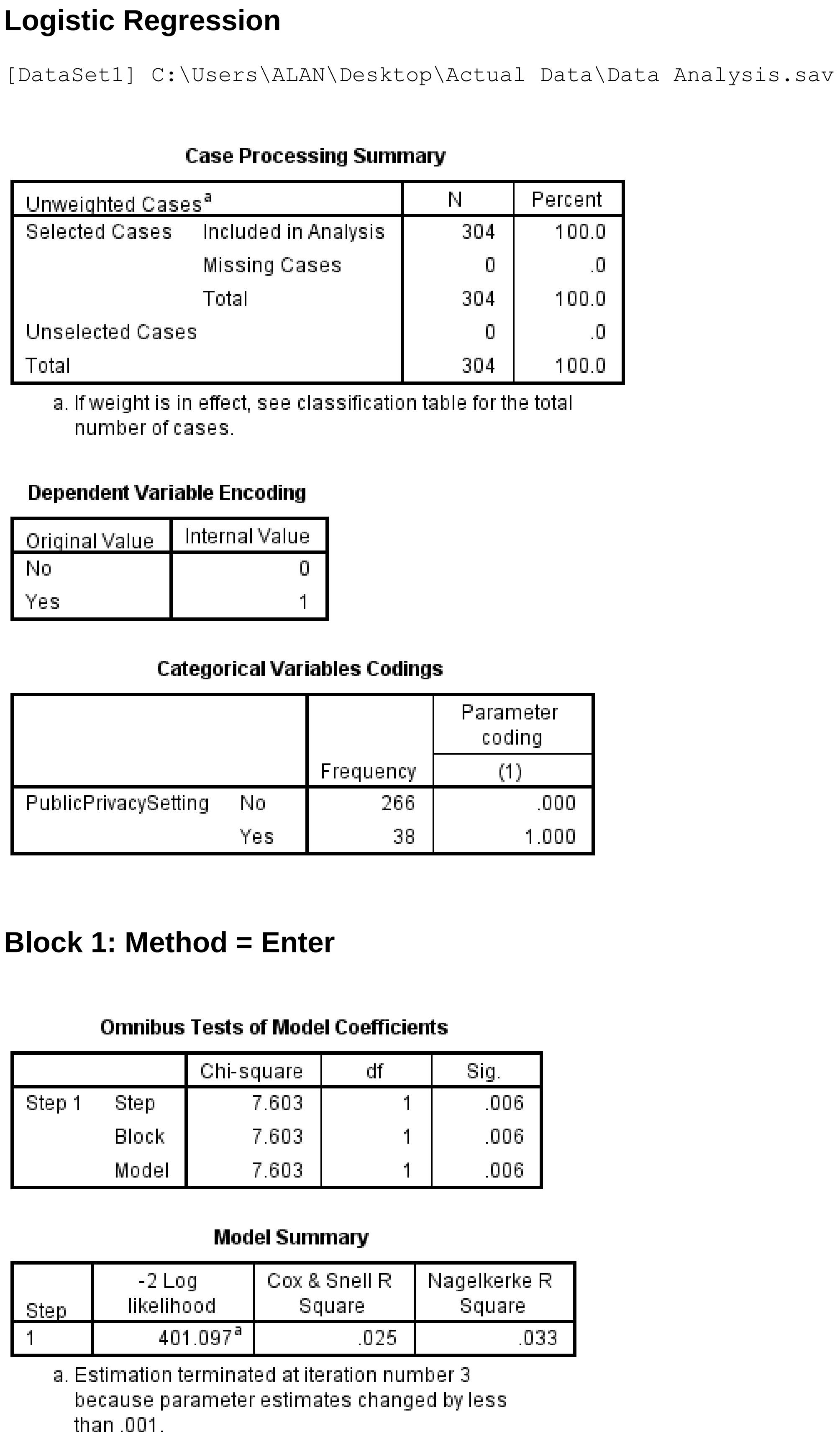
Variables in the Equation



		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	DefaultSecuritySetting(1)	-.325	.235	1.906	1	.167	.723
	Constant	-.253	.164	2.378	1	.123	.776

a. Variable(s) entered on step 1: DefaultSecuritySetting.

Results of Binary Logistic Regression for Hypothesis $H_0$4



Logistic Regression

```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```

Case Processing Summary

Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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

Dependent Variable Encoding

Original Value	Internal Value
No	0
Yes	1

Categorical Variables Codings

			Parameter coding
		Frequency	(1)
PublicPrivacySetting	No	266	.000
	Yes	38	1.000

Block 1: Method = Enter

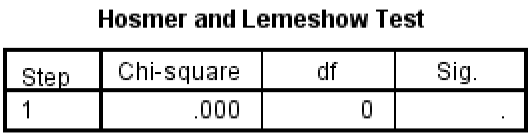
Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	7.603	1	.006
	Block	7.603	1	.006
	Model	7.603	1	.006

Model Summary

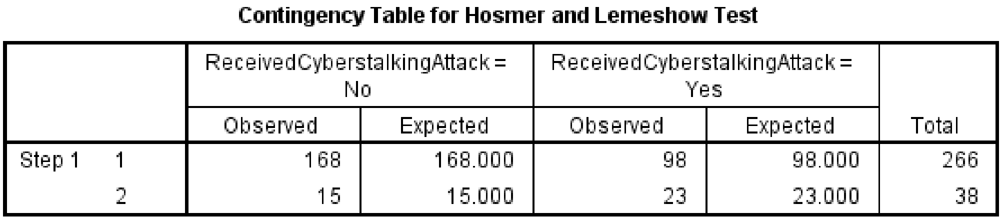
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	401.097[a]	.025	.033

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.



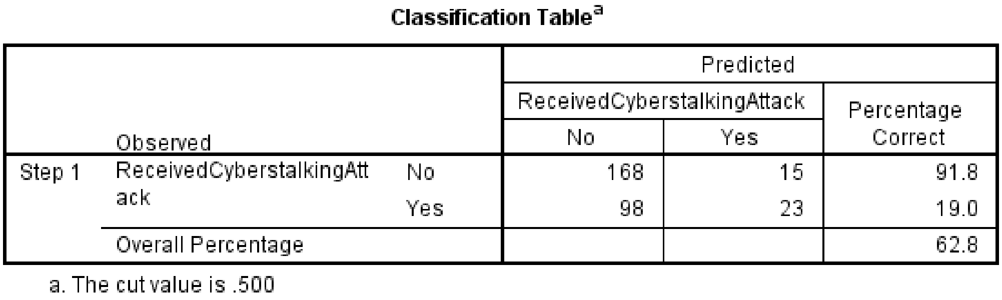
Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	.000	0	.



Contingency Table for Hosmer and Lemeshow Test

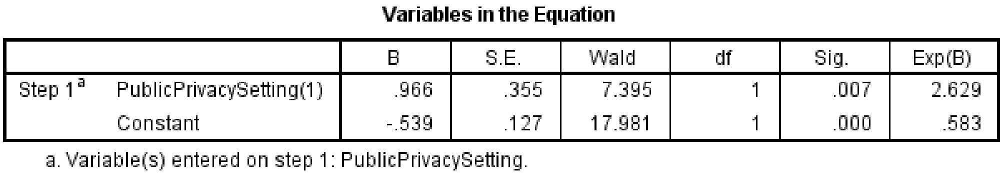
		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		
		Observed	Expected	Observed	Expected	Total
Step 1	1	168	168.000	98	98.000	266
	2	15	15.000	23	23.000	38



Classification Table[a]

			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
	Observed		No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	168	15	91.8
		Yes	98	23	19.0
	Overall Percentage				62.8

a. The cut value is .500



Variables in the Equation

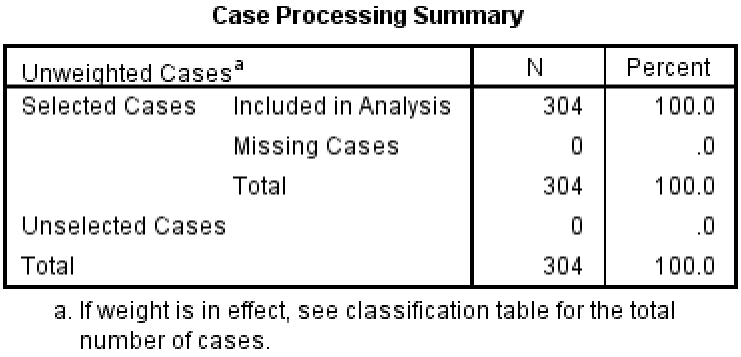
		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PublicPrivacySetting(1)	.966	.355	7.395	1	.007	2.629
	Constant	-.539	.127	17.981	1	.000	.583

a. Variable(s) entered on step 1: PublicPrivacySetting.

Results of Binary Logistic Regression for Hypothesis H_05

Logistic Regression

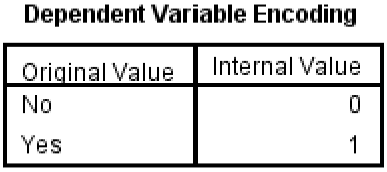
```
[DataSet1] C:\Users\ALAN\Desktop\Actual Data\Data Analysis.sav
```



Case Processing Summary

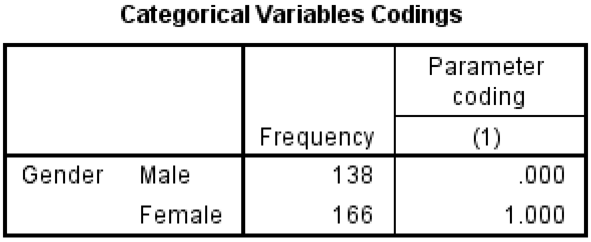
Unweighted Cases[a]		N	Percent
Selected Cases	Included in Analysis	304	100.0
	Missing Cases	0	.0
	Total	304	100.0
Unselected Cases		0	.0
Total		304	100.0

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



Dependent Variable Encoding

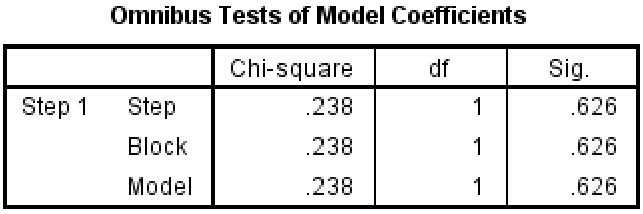
Original Value	Internal Value
No	0
Yes	1



Categorical Variables Codings

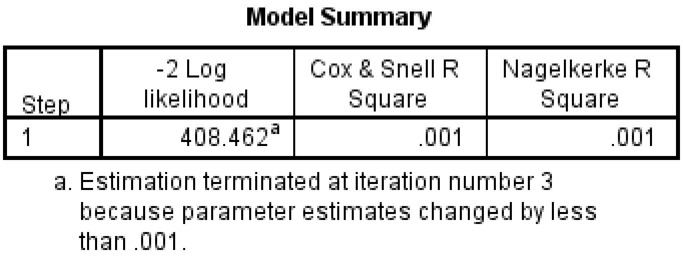
		Frequency	Parameter coding
			(1)
Gender	Male	138	.000
	Female	166	1.000

Block 1: Method = Enter



Omnibus Tests of Model Coefficients

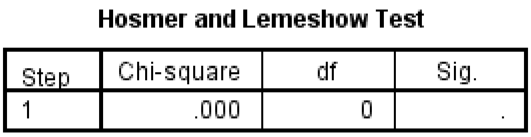
		Chi-square	df	Sig.
Step 1	Step	.238	1	.626
	Block	.238	1	.626
	Model	.238	1	.626



Model Summary

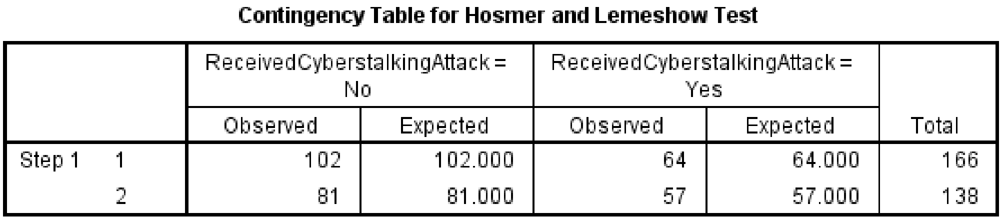
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	408.462[a]	.001	.001

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.



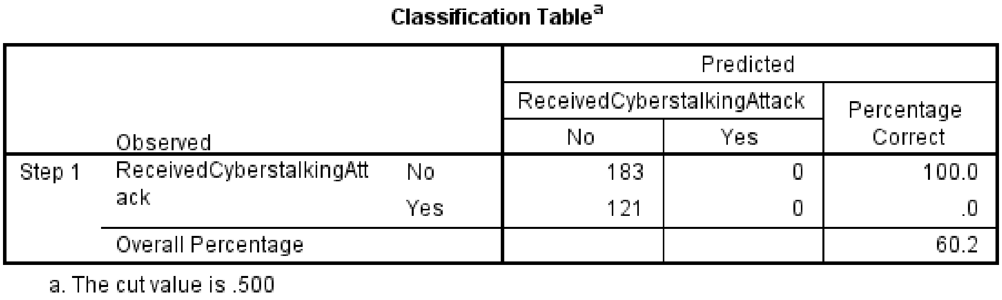
Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	.000	0	.



Contingency Table for Hosmer and Lemeshow Test

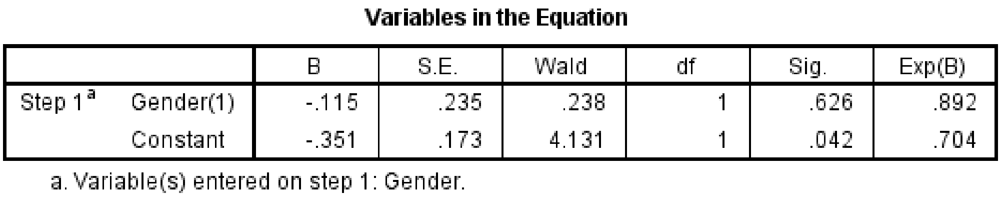
		ReceivedCyberstalkingAttack = No		ReceivedCyberstalkingAttack = Yes		Total
		Observed	Expected	Observed	Expected	
Step 1	1	102	102.000	64	64.000	166
	2	81	81.000	57	57.000	138



Classification Table[a]

			Predicted		
			ReceivedCyberstalkingAttack		Percentage Correct
	Observed		No	Yes	
Step 1	ReceivedCyberstalkingAttack	No	183	0	100.0
		Yes	121	0	.0
	Overall Percentage				60.2

a. The cut value is .500



Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	-.115	.235	.238	1	.626	.892
	Constant	-.351	.173	4.131	1	.042	.704

a. Variable(s) entered on step 1: Gender.