Chapter 1: Introduction

1.1 General Background

Many crimes that are not specifically related to computers, however, can be substantially used by criminals to facilitate the act. The borderless nature of the Internet and the easy access of cyberspace can provide a low-cost but high-connectivity way for criminals to reach victims. Computers can be used in a variety of roles in crimes. This can create disaster and chaos in Malaysia if proper legislation is not adequately introduced.

Malaysia has welcomed the coming of the new millennium by introducing the Multimedia Super Corridor (MSC). The government has introduced cyber laws which include the Computer Crimes Act 1997, Digital Signature Act 1997 and Telemedicine Act 1997. However, Internet criminal by the new dimension of rapid advances in computer technology should not be forgotten. This advancement of technology leaves loopholes in some of our present legislations.

The criminal laws of Malaysia, in particular the Penal Code does not specifically provide for any computer-related crimes and our newly legislated Computer Crimes Act 1997 does not cover many areas of computer related crime activities. As such, whether certain types of these acts are unlawful must be determined in the context of the existing laws. The main constraint is that the existing laws were not drafted with computer technology in mind and in most cases are not sufficiently broad to encompass the various types of computer related activities. Consequently, no matter how odious or nefarious such activities may be in the

perception of the policy-makers and the public, they may not constitute unlawful or prohibited behaviour[1]

Internet destroys traditional business transaction in various ways. It creates a cross-borderless marketplace for businessman and consumers to conduct electronic transaction in such a convenient way. Unfortunately, this easy access to cyberspace has been exploited by cyber criminals as another low-cost high connectivity alternative to reach their victims. The exponential growth in online financial transactions has provided criminals with new cyber malice epidemic known as Phishing, which has plagued consumers with increasing frequencies and sophistication.

In general, phishing is a form of online identity theft and social engineering that attempts to trick users into revealing their personal private data, particularly financial data. These data ranged from bank account usernames and passwords, date of birth, credit card details, social security numbers and much more. The everyday activities of a typical Internet user such as checking email, trading online stock, conducting banking transaction and even surfing website may provide tremendous opportunities for an identity thief.

In this context, the general issue is legal and regulatory challenge whether existing Malaysia Cyber law protects internet users from phishing schemes when no specific anti-phishing law has been created by the Parliament. In 1997, the Malaysian Parliament approved a set of cyber-laws to provide a comprehensive framework of societal and commerce-enabling laws, which encompass aspects concerning information security, network integrity and network reliability. It includes packages of 'cyberlaws': the Computer Crimes Act, Digital Signatures Act, the Copyright (Amendment) Act, the Telemedicine Act and Communication and Multimedia Act 1998. The study also analyzing

[1] Khaw Lake Tee, et. al, *Laws and Policies Affecting the Development of Information Technology*, Final Report, National Information Technology Council, 1996.

the legal approach taken by several countries like USA, UK and Singapore in order to tackle the issues.

1.2 Problem Statement

According to Prof Abu Bakar Munir and Siti Hajar Mohd Yassin, phishing and identity theft is emerging as one of the crimes of the 21st century. It is one of the fastest growing forms of Internet fraud. According to the U.S Federal Bureau of Investigation, phishing has become the hottest, and most troubling, new scam on the Internet. Credible estimates of the direct financial losses due to phishing alone exceed a billion dollars per year. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions.[2]

According to the Anti-phishing Working Group (APWG), in January 2007 alone; it received 29,930 unique phishing reports – the highest recorded number. There are 27,221 phishing websites and 135 brands were hijacked in that month. In the U.S, it was estimated that between May 2004 and May 2005, 1.2 million Internet users were victims of phishing, totalling approximately USD 929 million.[3] Meanwhile, in the U.K, losses from phishing almost doubled to 23.2 million pounds in 2005, from 12.2 million pounds in 2004. It is a multimillion pound problem. The BBC News on 13 December 2006 reported that the UK has seen an 8,000 percent increase in fake internet banking scams in the past two years[4]. Banks and financial institutions, around the world, are the prime target especially Internet

[2] See Abu Bakar Munir and Siti Hajar Mohd Yasin, "Would the Phishers get Hooked", (April 2007), Bileta
[3] See the Anti-Phishing Working Group, "August Phishing Trends Report" , available at http://www.antiphishing.org/reports/apwg_report_january_2007.pdf
[4] BBC News, "Online Banking Fraud 'up 8,000%' ", available at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/61775.

banking. Trust in online payment systems and the ability of financial institutions to mitigate fraud are diminished by successful attacks.

This problem is still new in Malaysia. In October 2006, thirteen people were arrested by the Malaysian police, including four university students, reported to be involved in phishing activities. The amount of losses on the part of the customers, according to the police, amounted to RM36, 000. The Association of Banks in Malaysia (ABM) states that a total of 159 online banking fraud cases mainly involving phishing were recorded in the first nine month of the year. Nevertheless the regulatory authority, the Bank Negara Malaysia (BNM) in its reaction, urges that both parties; the customers and financial institutions must take steps to ensure the security of the Internet banking. The BNM also states that all banks are required by the BNM to ensure that their Internet banking systems have appropriate security systems. This is reiterated by the Deputy Prime Minister, Dato Seri Najib Tun Razak when he reminds the banks to enhance the security of Internet banking services.[5]

The study in this paper discussed whether or not there is sufficient existing law in Malaysia to deal with phishing or any forms of developing technology crime such as the Computer Crime Act 1997, the Communication and Multimedia Act 1998, the Penal Code and the Minimum Guideline by Bank Negara. The analyst also been made on several existing laws such as US Laws, new state law passed the California's Anti-Phishing Act in 2005. There was also proposed Anti-Phishing Act in the United States targeting the entire scam process from the sending of the email to the creation of fraudulent websites. The study also been made on the UK Fraud Act which aim to encompass all forms of fraudulent conduct with a law that is flexible enough to deal with developing technology, allowing the law to bring

[5] Refer Abu Bakar Munir and Siti Hajar Mohd Yasin, "Would the Phishers get Hooked", (April 2007), Bileta, also see Utusan Malaysia, 12 October 2006.

more offenders to the justice. In addition, law in Singapore also had been taken into consideration based on its Penal Code and Computer Misused Act (CMA). It also can be proposed that Malaysia will have a set draft bill of law preventing and protecting our system from identity theft and account hijacking specifically. However, the studies determine the solution for phishing is likely to be a combination effort between education, technology measures, legislation and law enforcement.

1.3 Objective of the study

This research aims to study the concept of computer crimes and the forms and the existing law in Malaysia. It will also study and analyse the existence of phishing, and its variants, to identify the factor why phishing succeed.

It also analyzes the existing law in Malaysia and other jurisdictions like in USA, United Kingdom and Singapore dealing with identity theft. Last but not least, to propose recommendations and measures to address the problem of phishing in Malaysia.

1.4 Scope of the study

In fulfilling the above objectives, the following relevant regulations will be analysed:-

i) The Computer Crime Act 1997

ii) The BNM Minimum Guidelines on Internet banking

iii) Licensed banking procedural requirement on internet banking

In the meantime, a comparative study had been carried on the US, UK and Singapore legislations to tackle the problem.

1.5 Importance of the study

The study aims to stimulate awareness and importance among the public especially e-commerce merchant and consumer to taking their role more seriously as they know that they are accountable for the threat caused by phishing.

The researches also determine whether all the existing legislations in Malaysia are sufficient to deal with this matter. The study also analyse comparatively the legislation in Singapore, US and UK.

It also important to know the recommendations taken by industry player such as banking sector in term of technical solution in order to overcome the problems.

1.6 Structure of the study

Chapter 1: Introduction and methodology to the study

This chapter lay out the general background and issues that instigate the research, which it also explain the methodology of the study.

Chapter 2: Origin of Phishing

In this chapter, the study will be focusing on the beginning of the scam techniques used by identity thieves most popular among the hackers. In addition, the definition and concept of phishing described by authority organization and comparatively analyzing with terms like identity theft and account hijacking.

Chapter 3: Threat and magnitude of problems

The chapter discusses the impact of phishing, both domestically and internationally. It also involves the concern to the commercial and financial sectors involving costs and losses. This chapter also examines the variants and technique of phishing.

Chapter 4: Success factors of phishing

This chapter explains how phishing can success. This is because it is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. It will encompass this chapter into two main factor namely human factor and technical factor via authentication in banking sector.

Chapter 5: Legislative baits and technical lures

The chapter highlighted some of the potential solutions through legislation and technical measures. It analyses the approaches adopted by USA, United Kingdom, and Singapore before move to the technical solutions that aim to enhance privacy and provide a secure medium for data transfer in a manner that protects the confidentiality and integrity of personal information.

Chapter 6: Phishing in Malaysia

This chapter discusses approaches adopted by Malaysia via existing legislation and technical authentication to tackle the problems.

Chapter 7: Recommendation and conclusion

The final chapter concludes the study with the recommendation and step proposed by academician and expertise to overcome the issue.

1.7 Methodology of study

In preparation for conducting this study, a combination of various research methods was used. This includes literature review, legislation study, research on web or e-journal, data collection and interviews with the relevant parties including government agencies, lawyer, banking personnel and other interested parties.

1.7.1 Documentary review

In conducting this study, reference was made to various sources of material, including books, journals and articles.

1.7.2 Internet

Searching for and accessing information has been made much easier by using the world wide web of the internet. A lot of valuable, interesting and relevant information were discovered through online research conducted. Visits were made to numerous websites such as the websites of the Malaysia governmental bodies like Bank Negara Malaysia, Malaysia Development Corporation (MDC) as well as corporate sector Maybank Berhad, AM Bank and Bank Islam Malaysia Berhad (BIMB). Information was also found from international websites such as Anti-phishing working group (APWG), the USA and Canada Report on Phishing 2006, the Financial Services Authority Report 2004, the US National Consumer League Report 2006, US Federal Deposit Insurance Corporation report 2004 and others relevant online report related to the study. The information obtained provided for better understanding and answered many questions and some have been reproduced in the study.

1.7.3 Fieldwork

As stated earlier, there is a shortage of written material available that relates towards the topic of study. This has resulted in the decision to seek information and clarification directly from various interested parties. The purpose of undertaking the fieldwork is to require data and considerable amount information from experienced banking personnel, lawyer, government agencies and relevant parties

To supplement the information obtained from the written literature a series of interview were conducted with members of interested parties. This was a very beneficial approach for obtaining material as it provided a reality viewpoint that could be compared to the theoretical views attained from the written literature. Questions were asked in order to find answers to the following issues:-

1. What are the government bodies that have been empowered to implement these laws and ensure proper enforcement is in place?
2. Are existing legislations concerning computer crime especially phishing adequately protecting the interest of online user @ consumer?
3. Is the public in Malaysia aware of the existence of this problem?
4. Who are the interested / relevant parties and what role do they play in Malaysian legislation in combating phishing?
5. What steps have been taken either through legally or technically to ensure proper implementation and enforcement to overcome the problems?

The answer to these questions will provide a better understanding on the situation, problems and issues faced in Malaysia when it comes to the implementation and

enforcement. Specifically listed below are the interviewers/respondents that have been interviewed in the study / research:

1. Ms Haslinda Ariffin, Deputy Public Prosecutor in AG Chambers (Commercial Crime Division)
2. Mr Irman Mohd and Adeebah Jalil, Department of payment system policy, Bank Negara Malaysia
3. Mr Abdul Razak Ahmad, practicing lawyer of Abdul Razak, Zulkifli and partners
4. Mr Ahmad Shahreza Abd Rahman, Head of virtual banking, Maybank Berhad
5. Mr Kamaruzaman Mohamed, personnel executive Bank Islam Malaysia Berhad.

These interviewees has been chosen on the basis that they are person in-charge in certain aspects of fieldwork like Ms Haslinda Ariffin, Deputy Public Prosecutor in AG Chambers (Commercial Crime Division), who preparing the prosecution paper to charge the person suspecting involved in so-called identity theft crime or phishing.

The questionnaire is created to analyze the respondents' opinions towards phishing issues, how the phishing affected their daily operation, how they get to know about phishing, how they react to phishing incident and prevention levels in organizations. The respondents were given a list of questions to answer verbally, the details below:

Phishing Awareness

The awareness towards phishing is covered in question. Majority of the respondents have a good understanding of phishing but majority still felt that their level of knowledge about phishing is very poor.

Phishing Experience and Effect

Question covers the information on respondent's experiences on phishing problem and its impacts on their daily work. The respondent had no experiences in encountering phishing or do not know whether they encounter such attack.

Actions Taken Towards Phishing

Question analyzes respondent actions in confronting, detecting and preventing phishing. The result shows that the respondent just ignore the phishing threat and did not know what action should be done if they encounter such attack .The lack of this action awareness is proven when only five percent of the respondents used tools to detect and prevent phishing. Although respondent did not know the steps should be taken, he agreed that it is possible to prevent the phishing problem. Therefore, researchers should provide more information and steps to combat phishing

Phishing Media Channel

The fourth category, which covered in the question, is to analyze type of respondent's media channel used in receiving information on phishing. The respondent received such information from websites, followed by from newspaper and e-mails.

Responsible Party

The analysis on party responsible for phishing is conducted. The respondent blamed the IT department, the end user and the vendor while the remaining blamed the government The high blame percentage on IT department is due to the highly dependency of the end user to such department in any security matters.

Summary of the Questionnaire Result

From the result obtained, it can be observed that users are aware of phishing threat. However, their knowledge on the identification and prevention of phishing is very poor.

This is one of the reasons why majority of the respondents held the IT department responsible for such cases. Phishing also had caused problems to respondents in performing their daily routine work. The information acquired are used sporadically in the study such as chapter 4 which related to why phishing success.