Chapter 6: Phishing in Malaysia

6.1 Introduction

"*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. While 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. May bank's Amirsham asserts that customers should not shy from using Internet banking services as the fraud level recorded in the country is "not alarming". 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, when he reminds the banks to enhance the security of Internet banking services."* (*Excerpt Malaysian Media*)

Basically, according to the above statement, the ignorance of the potential of phishing to develop in Malaysia cannot be denied although the problem is still at the early stage.

Efforts to combat phishing attacks that threaten to tackle the local online banking industry are making good progress. The Malaysian Cyber Security Centre (MCSC), which is working closely with the regulator, Internet service providers and Computer Emergency Response Teams (CERTs) - both locally and overseas - have reported some success in bringing down a number of phishing sites hosted across borders.[182]

According to Lieutenant Colonel Husin Jazri, Director of MCSC, the team has been able to bring down phishing sites within several hours, which is commendable. He said the Malaysian CERT (MyCERT), which is a unit within MCSC, has been closely monitoring phishing activities in the country and even issued an advisory on possible phishing attacks on Internet banking users in September 2006. In addition, MyCERT (www.mycert.org.my)

[182] Rozana Sani, "Phished in Troubled Water", Computimes, 16 October 2006

is a unit of the National ICT Security and Emergency Response Team (Niser) and is responsible for tracking and logging security incidents, as well as analysing major security incidents and trends.

Their findings showed that 85 per cent of the phishing sites imitating local banks and other e-commerce Web sites reported were hosted overseas; those hosted in Malaysia mostly involved foreign banks.

"Through our interactions with other National Computer Emergency Response Teams in Australia, Japan and other countries, we are seeing that some cases involving large online payment gateways may involve organised groups with collaboration between spammers and hackers. For smaller-scale targets, they usually involve local players. Most of the banks targeted are not only in Malaysia; similar problems are faced in Europe and other countries," said the Director of MCSC[183].

Husin acknowledged that the battle against phishing is far from over, but advised users not to be overly alarmed, saying that the problem is global and cases in Malaysia are relatively low compared to advanced countries. As of September 2006, MCSC has received a total of 159 phishing reports. It received 132 reports in 2005 and 92 reports in the year 2004

"There is no specific bank targeted. Basically, any bank providing Internet banking would be a target. We believe that the financial sector is aware and putting various measures to curb this activity," Husin said. On why phishing is becoming more rampant, Husin said this is so because of the possibility of identity theft.

[183] Ibid

"Measures to enhance the authentication level such as using two factor authentication, 'what you have' (such as MyKad) combined with 'what you know' (such as password), can reduce the possibility of identity theft. Internet banking users also need to be educated that their banking information should be kept private and confidential despite the many attempts by fraudsters to steal or obtain the information from them."

What's important at this point, Husin advised, is for users to be aware of such threats and to be cautious. "Consumers should not just follow the Internet links provided in e-mail without due diligence. They should retype the URL (uniform resource locator) or use their normal browser bookmarks to access the banking sites. The banks are also providing information on their Web sites to educate users and inform them of the latest phishing scams. Consumers should immediately report to the banks or MCSC upon receipt of potential scam e-mail. Internet banking login ID and passwords should be kept private and confidential at all times[184]."

6.2 Legal Position in Malaysia

Before an analyst is made on the legislation in Malaysia, the writer had communicated with **Ms Haslinda Ariffin, Deputy Public Prosecutor in AG Chambers (Commercial Crime Division)[185]** asking on the current cases dealing with this crime. She mentioned three cases related to identity theft or phishing when she was preparing the prosecution paper:-

a) 1st case (reporting in 2007) without mentioning the name of the party, will be charged under **S.4 Computer Crimes Act**, the accused withdrawn the complainant

[184] Ibid
[185] The interview made on 14 February 2008 via telecommunication.

(client of BCB Bank) using the ID and password without permission via internet banking money transfer.

b) 2nd case (2007) involving RHB Bank, the suspect transfer the victim's money via internet banking and suggest to be charged under **S.403 of the Penal Code –** dishonest misappropriation of properties.

c) 3rd case (2007) dealing with the client of Maybank Berhad, will be charged under **S.4 of the Computer Crimes Act**, the facts that the complainant's money had been withdraw via account transaction at the bank without his knowledge.

Legal actions against cyber criminals and perpetrators of security breaches can be broadly categorized into criminal prosecutions which are commenced by the government (i.e. Attorney General Chamber); and civil actions which are initiated by the victims of the cyber crime or security breach. These 2 distinct categories of legal action are further discussed below.

6.2.1 Criminal Prosecutions

As mentioned earlier, there are various agencies that deal with cyber crime and security breaches. These agencies, in particular MCMC, PDRM and AGC are empowered under various statutes to investigate; charge and prosecute cyber criminals or perpetrators of security breaches.

6.2.2 Computer Crimes Act, 1997 ("CCA")

The principal statute in Malaysia that deals specifically with cyber crime is the CCA. The CCA essentially covers computer misuse such as hacking and cracking; theft of data; and spreading of malicious codes.

Among all cyber laws *Computer Crime Act 1997* is the most relevant legislation to prosecute the chicanery of phishers. But is 'Phishing' included in the definition under Part

II of this act? Under Section 3, the fundamental element for the offence would be that the charge at the time when he/she caused the computer to perform the function, knew that his access was unauthorized. Email Spamming, as bait to consumer's email account without their consent is an unauthorized action based on Section 2 Subsection 5 in this act.

The intention to secure access to any program or data is an important requirement. One may presume that phishers definitely want to secure access to others data in order to obtain personal sensitive data. Their intention could be easily seen in SPAMs they sent to others internet users. Unauthorized access means the phisher is not an entitled person to have control access to the program or data; and he does not have permission or any right to access question to the program or data from any person who is entitled. But there is obviously a doubt on the phrase 'causes a computer to perform any function' could be applicable here when most tricks of phishers only attracts victims to send their personal data and not by installing a computer virus or by hacking into other computers.

Ironically, most cases happened today clearly indicated that the phisher can only achieve his willful aim when the innocent party response to the fraudulent email by sending their personal security data. Therefore, defendant can defend that the incoming bamboozle email is harmless and never automatically caused the computer to perform any function. It is up to the following action of the defendant to respond to the email.

Thus, even though this section could be applied in limited cases, it is not a comprehensive law to protect internet users since some of the phishers may argue that it is a voluntary act of the victim to send their personal data and they did not directly cause a computer to perform any disclosure function. Consequently, this challenging jurisdiction will become the vulnerability of this act to indict the phishing forgery activities.

On the other hand, Section 4 of the *Computer Crimes Act 1997* creates a specific offence of unauthorized access to a computer with intent to commit an offence involving fraud or dishonesty. Obviously, phishers have the intention to commit an offence of fraud or dishonestly by sending the fraudulent email and luring consumers to forged websites in order to disclose confidential data.

However, there is a pre-condition where before Section 4 could be applicable elements in Section 3 must first be proved. Under Section 3, the essential element for the offence to be committed is when the accused knew that his access was unauthorized. This is a subjective test and depends on each individual's state of mind.

Therefore, the court has to decide on the merit of each case. Expectedly, accused may raise thousand of excuses to show that he or she was not aware of the unauthorized access. More complicate is when the case involves bank employees that has rightful access to victim's personal data and thus uses the data for illegal purposes.

Prosecution may need to prove that the phishing scheme is a fraud or dishonesty activity under Section 4 (1) (a). Where fraud means untrustworthy behavior designed to manipulate another person to give something of value by (a) lying, (b) by repeating something that is or ought to have been known by the fraudulent party as false or suspect or (c) by concealing a fact from the other party which may have saved that party from being cheated. The existence of fraud will cause a court to void a contract and can give rise to criminal liability. Thus, cheating others personal data could definitely fall under this particular section.

In addition, luring consumers to forged website and divulge their confidential information are also an arguable indictment under Computer Crime Act 1997. The phisher could be charged under Section 5 for the reason of unauthorized modification of the content of

others computer. Intention or the real motive of the accused will be the main criteria to be ascertain under this section. The Phisher could defend that they did not intentionally modify the real website for their purpose to illegally obtain others personal data. Hence, it is up to the prosecutor to show that the accused has intentionally modified contents of the other computer without real consent.

By this scheme, the prosecutor will find it difficult to convict the perpetrator under this particular section. Therefore, ambiguity of terms in the Computer Crime Act 1997 concerning phishing schemes will be the weakness of the Malaysian Cyber Law in preventing phishing activities. Due to the inadequacy legal framework, Malaysia seems to have a high potential in becoming the target of major organized phisher syndicates.

6.2.3 Communications and Multimedia Act, 1998 ("CMA")

There are specific provisions under the CMA which deal with network related crimes such as unauthorised interception of communications; telecoms fraud; transmission of obscene communications; theft of service; criminal damage or sabotage of networking infrastructure; and sale of counterfeit access devices.

Section 231 CMA - Offence if use apparatus or device without authority. A person who uses any apparatus or device with the intention of obtaining information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency commits an offence and shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding 2 years or to both.

Section 232 CMA - Fraudulent use of network facilities, network services, etc. It is an offence for a person to dishonestly transmit or allows to be transmitted any communication or obtains a service provided by a licensed network facilities provider, network service

provider, applications service provider etc. or content applications service provider. It is an offence to dishonestly receive a content applications service from a place within Malaysia not intended for general reception, with intent to avoid payment of any rate or fee applicable to the provision of that facility or service.

A person also commits an offence if he possesses, obtains or creates a system designed to fraudulently use or obtain any network facilities, network service, applications service or content applications service

A person who commits any of the offences outlined above shall, on conviction, be liable to a fine not exceeding RM300, 000 or to imprisonment for a term not exceeding 3 years or to both

Section 233(2) - Improper use of network facilities or network service, etc. A person who knowingly, by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or permits a network service or applications service under the person's control to be used for an activity described in the latter; is guilty of an offence and shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding 1 year or to both and shall also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction.

This Section can potentially cover the commercial distribution of online pornography.

Section 234 CMA - Interception and disclosure of communications prohibited.

It is a crime for a person without lawful authority under the CMA or any other written law to:

a. Intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications;

b. Disclose, or attempt to disclose, to any other person the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or

c. Use, or attempt to use, the contents of any communications, knowing or having reason to believe that the information was obtained through the interception of any communications in contravention of this section, It is also against the law for a person authorised under the CMA, to intentionally disclose, or attempts to disclose, to any other person the contents of any communications, intercepted by means authorised by this Act:

a. Knowing or having reason to believe that the information was obtained through the interception of such communications in connection with a criminal investigation;

b. Having obtained or received the information in connection with a criminal investigation; or

c. To improperly obstruct, impede, or interfere with a duly authorised criminal investigation. Note also that it is an offence to distribute or advertise any communications equipment or device for interception of communications. A person who commits any of the offences outlined above shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding 1 year or to both.

Section 235 CMA - Damage to network facilities, etc.

A person who, by any willful dishonest or negligent act or omission, extends, tampers with, adjusts, alters, removes, destroys or damages any network facilities or any part of them commits an offence and shall, on conviction, be liable to a fine not exceeding RM300,000 or to imprisonment for a term not exceeding 3 years or to both.

Section 236 CMA - Fraud and related activity in connection with access devices, etc. A person who knowingly or with intention to defraud

a. Produces, assembles, uses, imports, sells, supplies or lets for hire any counterfeit access devices;

b. Possesses any counterfeit access device or unauthorised access device[186];

c. Produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses any device making equipment[187]; or

d. Produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of, or possesses

i. any equipment, device or apparatus that has been modified or altered to obtain unauthorised use of any network service, applications service or content applications service; or

ii. hardware or software used for altering or modifying any equipment, device or apparatus to obtain unauthorized access to any network service, applications services, or content applications service,

A person also commits an offence if he without the authorisation of the issuer of an access device, solicits a person for the purpose of offering an access device; or selling information regarding, or an application to obtain, an access device.

A person who commits any of the offences outlined above shall, on conviction, be liable to a fine not exceeding RM500, 000 or to imprisonment for a term not exceeding 5 years or to both.

• Prosecution under the CMA

The decision of whether to prosecute an offence under the CMA lies with the Public Prosecutor and where consent in writing of the Public Prosecutor is first required.

[186] unauthorised access device" means any access device that is lost, stolen, expired, revoked, cancelled, or obtained with intent to defraud

[187] device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device (Section 236(4) CMA)

6.2.4 Malaysian Penal Code ("the Code") and Other Laws

Although the Code deals with traditional crimes and not specifically with Cyber crime, cyber criminals may also be charged and prosecuted under the Code depending on the nature of the crime. The following are some examples:

a. A bank officer who steals money by making unauthorised transfers via the bank's computer system to his own account may be charged for theft under Section 378 of the Code and criminal breach of trust under Sections 405 or 409 of the Code.

b. A scammer who engages in "phishing" activities may be charged for cheating under Section 415. The section deals with the offence of cheating and reads as follows:

Whoever by deceiving any person, whether or not such deception was the sole or main inducement,-

- *fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property; or*
- *intentionally induces the person so deceived to do or omit to do anything which he would not do or omit to do if he were not so deceived and which act or omission causes or is likely to cause damage or harm to any person in body, mind, reputation, or property,*

is said to 'cheat'.

Explanation 1 - A dishonest concealment of facts is a deception within the meaning of this section.

Explanation 2 - Mere breach of contract is not of itself proof of an original fraudulent intent.

Explanation 3 - Whoever makes any representation through any person acting as an agent, or otherwise, for him, shall be deemed to have made the representation himself.

The appropriate section that attaches criminal liability to the individual if he does use the phishing or identity theft is s415. This section makes it an offence if the fraudster obtains a property from any person by misrepresenting himself. Thus this section could be applicable for instance when the fraudster dishonestly or fraudulently induces the person so deceived to transfer the money or accomplished the transaction or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property." The victim could be the person whose information is stolen, provided that such information can constitute "property" (which shall be an issue to be considered in relation to other property offences), or it could be the person or organization which is deceived or intentionally induced into transacting with the offender on the basis of that information (which can include banking and financial institutions, companies and business, and other forms of organization).

There have been several amendments made to this Act and the Penal Code (Amendment) Act 1993 made fifteen amendments to the Code. One of the amendments related to s415. This section was amended in two ways. Firstly, by including s415 (a) and (b) and secondly, by including a third explanation of the term 'cheat.' Explanation 3 expands the definition of the term because under this explanation, statements made by an agent bind his principal.

6.3 Bank Negara Malaysia (BNM) Minimum Guideline

The Minimum Guidelines on the provision of the Internet Banking Services by Licensed Institutions was issued by Bank Negara Malaysia (BNM). It sets out guidelines that

licensed banking institution in Malaysia should observe in providing internet banking services. It also states that banking institutions are free to implement more stringent measures and are expected to keep abreast not only with technological developments, but also the needs of their customers. The guideline explains, among other things, types of Internet banking and risks. It also provides various aspects of corporate governance such as prudential regulations and supervisions, risks management practices, security requirements, consumer protection and compliance with other requirements

In the online business ecosystem, banks play very important role. Too fit in with the new challenges, banking system today has also transformed itself into survival by engaging in online operation. With borderless nature of business today, Internet banking is a panacea for traditional bureaucracies that had previously defined bank's operations. Thus, in order not to loose this important momentum, the central bank's initiative to issue this guideline is just timely and imperative, that is to ensure the bank plays its traditionally important role in a new ecosystem.

During an interview conducted with the BNM officer (accordingly the Guideline under review), referring to Part 4 under the heading "security" emphasizes the importance of implementing appropriate security measures to combat the risks of internet banking. It is the responsibility of the board of management and the bank to evaluate the costs and benefits of alternative security measures and decide on the best allocation of the banking institution's resources. The Internet security arrangements should achieve the following objectives:

a) Data privacy and confidentiality

b) Data integrity

c) Authentication

d) Access control and System design

The BNM Guidelines further provide that the bank management should place strong emphasis on using monitoring tools to identify vulnerabilities and in real time mode, detect possible intrusions from external and internal parties. In this context, banking institutions are required to conduct penetration testing and administer manual or automated intrusion detection procedures. The aforesaid guidelines under the heading "consumer education" also requires the banks to educate the consumers on their role of maintaining security by not sharing IDs, password, changing passwords regularly and remembering to sign off, as well as the double authentication method provided by banking industry that will be discussed later.

The BNM Guidelines are regulatory in nature as these guidelines are mainly concerned with the proper implementation and operation of the system. If fraud occurs and 'unauthorized transfers' are made without the customers mandate, does the customers have any legal redress?

At this juncture, reference is again made to Part 5, clause 1.2 (ii) of the BNM Guidelines that stipulates 'sharing of risk' in the event of 'unauthorized or fraudulent transactions'. It is submitted that a sharing of risk should only occur if the customer facilitated the fraud (Macmillan's Duty) or if the customer had knowledge of the fraud but did not take any preventive measures, then estoppel acts against him. Otherwise the bank should bear the loss for all fraudulent transactions; it would be onerous to lay responsibility on the customer especially since the customer has no technical expertise of the internet banking activities.

Pertaining to the privacy aspect of internet banking, according to the Guidelines, recognition is given to this principle of secrecy or also known as privacy in Part 5, clauses 4

which is title "Privacy Policy". In clause 4.1, Bank Negara has stressed on the importance of privacy in the following manner;

"Bank Negara Malaysia considers the privacy of consumer personal information to be an important element of public trust and confidence in the Malaysian banking system."

Next clause 4.4 places the responsibility of ensuring privacy on the banks;

"Banking institutions should adopt responsible privacy policies and information practices, disclose policies and practices to increase consumer knowledge and understanding and take other prompt, effective actions necessary to provide consumers with privacy protections in the online environment."

The BNM Guidelines then continue to stipulate the requirement of privacy policy statement in the banks' websites, the aforesaid statement must be displayed prior to or at the time that individually identifiable information is collected or requested.[188]

The banks have to ensure that the 'Privacy Policy Statement' conforms to the following format[189]:

i) Identify the types of information collected about consumers and how it is used

ii) Explain the type of security procedures especially in cases of loss, misuse or alteration of information under the bank's control, including limiting employees access to information, handling of information about customers who have ceased the banking relationship with the institution;

iii) Identify with whom the banking institution shares this information, including agents, affiliates and non-affiliated 3rd parties and how the

[188] Clause 4.5 BNM Guidelines
[189] Clause 4.7 BNM Guidelines

banking institution ensure that the confidentiality of information is maintained;

iv) Explain the choices available to the customer regarding the collection, use and distribution of information including banking institution's opt-out process;

v) Explain how banking institution maintain the accuracy of information and how the customers can correct any inaccuracies in the information, and

vi) Explain how banking institutions handle consumer questions or complaints about the handling of personal information.

Finally, the BNM Guidelines in clause 4.8 – 4.17 provides for the setting up of a customer support services to handle customer queries and complaints, and oversee all internal controls, ensure there are no breaches by own employees, prevent improper disclosure of personal information to 3rd parties and have a meaningful enforcement and redress mechanism.

There are many examples of privacy statements in the entire internet banking websites. The Privacy Policy Statement does try to comply with the BNM Guidelines but when one peruses such statements, several flaws are evident.

i) First, most of the statements on all internet banking sites, allow the dissemination of information to the whole group pf companies, not only to the banking unit per say

ii) Secondly, some of these sites contain cookies that track your activities on the net

iii) Thirdly, a customer will not be protected if you hyperlink to 3rd parties from their websites[190]

iv) Information collected for promotions and contests can be used for marketing purposes, customers are advised to opt-out if you do not desire to compromise on your privacy.

The Guidelines do provide minimum requirements for the privacy policy statements but the banks generally have the freedom to structure such policy to suit their needs, which may not necessarily suit the needs of the customers.

6.4 Case Study on Maybank 2u.com

Despite the rising spam and phishing threats in Malaysia, the demand for Internet banking services is not likely to taper down. A web-based service has become a value proposition for many businesses, especially the banking sector and has become added channel to strengthen customer relationship.

Malayan Banking Bhd senior executive vice-president, head of consumer banking, Lim Hong Tat says the bank is targeting a 50% growth of active users for the financial year ending June 30, 2009.

"The average number of registered users per month is about 90,000, while our active user base stands at 1.1 million. We currently have more than 33 million transactions a month worth over RM3.3bil," he says. Maybank's Internet banking transaction value for the year ended June 30, 2008 grew by 28% to RM27.3bil over the previous year[191].

Maybank Berhad has relaunched its website, Maybank2u.com, introducing new features. With a tagline of "All-New, All-You", the website focuses on being customer-centric rather

[190] See explanation in http://www.bankinginfo.com.my (11 Dec 2006)
[191] The Star, 3 January 2009.

than bank-centric, says Ahmad Shareza Abul Rahman, Maybank's vice president and head of virtual banking.[192]He also mentioned that Maybank 2u.com is a popular target of phishing attempt. He hopes that with Maybank's online education awareness, customers will be able to avoid becoming victims. We get 10 or more phishing attempts a month, the moment we get the reports we bring the website down, said Maybank's Head of Virtual banking. "To check for phishing, key in gibberish in the ID and password boxes. If this takes you through to the next page, you can pretty certain that it is a fraudulent website," he added.

While Malayan Banking Bhd senior executive vice-president, head of consumer banking, Lim Hong Tat says its Internet banking team works closely with MyCERT and the Malaysian Communications and Multimedia Commission to track and shut down phishing sites. He says it is the bank's policy not to request customers to key in or update their personal details or passwords through e-mail, short messaging service or other means.

"Security alerts are highlighted in Maybank2u.com, including pop-up alerts and an updated list of phishing links. These alerts are part of the bank's preventive and educational measures for our customers," he says.

[192] Also can be seen in Personal Money, Dec 2008, pg 12

For example, the customer received an email trying to trick into giving out my Maybank2u login and password over the internet. The content of email:

Subject : Maybank Technical Maintenance

The following are the contents :

Dear Valued Customer,

Due to maintenance during the Sunday 12 November 2006,
The Maybank Technical Department is performing a scheduled software upgrade to improve the quality of the online banking services.
By clicking on the link below you will begin the procedure of the customer details confirmation.

https://www.maybank2u.com.my/mbb/scripts/mbb_update.jsp?do=Update

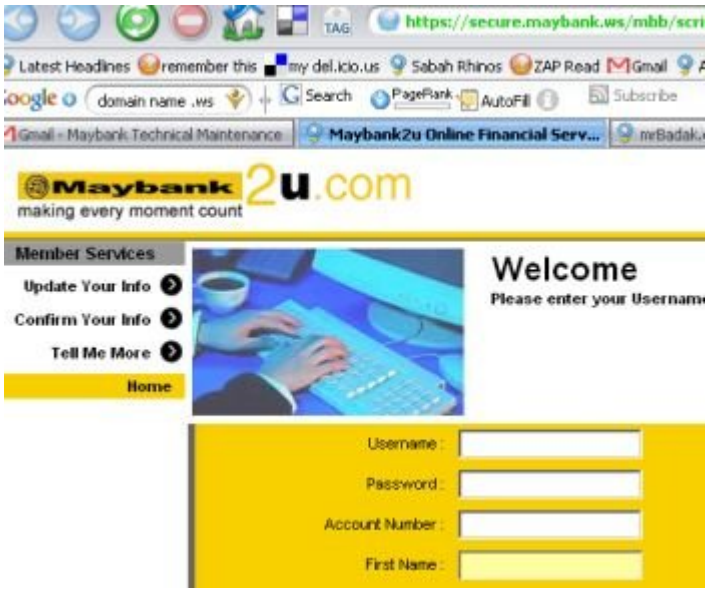
Once you have updated your account records, your Maybank account service will not be interrupted and will continue as normal.

.. ...

Now, for the unsuspecting users, nothing is wrong with the email, the link looks ok. But when you click on it, the site that is actually opens is https://secure.maybank.ws/mbb/scripts/mbb_update.jsp?do=Update.

Notice the domain name? It's not maybank2u.com.my but instead maybank.ws.

WS is the country extension for Western Samoa. On that page, you will see the following page:



Sample of fake website or phishing email.

It looks exactly like Maybank2U's page. Actually, it is the same image taken from the original page. Because of the state of the internet where you can copy almost anything online, imitating pages is too easy. So please do not give out your password on this page. It's like giving out your ATM numbers to some strangers.

How do you prevent being phished? Follow these advices:

- Don't click on any links from any email that says comes from your bank. If you want to check out for any news or information, read the next pointer
- If you want to go to your bank's website, always select from your bookmark or type in your bank's address manually in your browser's address field. If you don't know the bank's address, check it out from their brochures. You can also easily search it from google (just make sure you found the correct bank and not a phishing site).
- If the email says that your account is being terminated unless you click on the link, stay relaxes. They're trying to stir up your emotion and force you to click on the link. Just call up your bank instead for confirmation.
- If you think you've given up your passwords to some bad websites, call your bank immediately and tell them about it. They can reset your password and protect your account.[193]

How do you know if you've been tricked into giving your passwords? Well after trying to login, you will be redirected to the login page again. If you've given the correct password, then the information has been recorded earlier and now they redirected you to the correct website to avoid suspicion.

[193] Ref http://www.maybank2u.com.my

There are several methods of ensuring a more secure Internet banking:

Minimum Requirement: Two Factor Authentication

Based on the above method, the security measures in place are not adequate to prevent fraud. The current method of using only one factor of authentication definitely has its weaknesses. The security aspects of Internet banking need to be strengthened. At minimum, a **two-factor authentication** should be implemented in order to verify the authenticity of the information pertaining to Internet banking services[194].

The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard. MyKAD is a good avenue to introduce the second factor.

The above security measures will greatly minimise incidents of Internet banking fraud. The smartcard here provides a second layer of authentication. This will stop a perpetrator even if he manages to obtain the user's password.

Intercepted passwords cannot be used if fraudsters do not have the Smartcard. Besides addressing fraudulent activities, this can instill customers' confidence in Internet banking.

Additional Requirement: Three Factor Authentication

However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members, but is limited to getting the latest statements of a member.

[194] Ahmad Nasir Mohd Zin and Zahri Yunos, "How to make online banking secure", National ICT Security and Emergency Response Centre (NISER), April 2005

With a three-factor authentication a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. This would be difficult, if not totally impossible.

6.5 Conclusion

The need to enact, pass and thus implement cyber crime laws has been closely linked to assurance of having smooth and secure e-commerce – internet banking activities and thus it is closely associated with a country's determination to speed up development in this information era. The Malaysian Government has indeed reaffirmed this link which they include in their pledge to the international community when initiating Multimedia Super Corridor (MSC) project that Malaysia would become a regional leader in intellectual property protection and cyberlaws. This is because Malaysia believes (like other countries supposedly do) that the existence of cyberlaws in the country means guarantee for the invention, e-commerce as well as consumer protections. This is why the law of e-security is important for the country's growth and development. Based on the nature of the scope of the legislation discussed, cyber law can be categorized into two distinctive categories, firstly, those legislations that address solely the specific electronic environment and applications. Secondly, those legislations that do not solely address on electronic environment, instead they apply as a general law but applicable, in part or in totality, to the cyberspace and online environment. Since their enactment in 1997, specific set of Malaysia's cyberlaws provided ground for establishing legal frameworks for country's e-commerce and information security. As discussed in this chapter, the Computer Crimes

Act, the Communication and Multimedia Act, the BNM Minimum Guidelines, the Penal Code is the legislative bait used in order to combat this scam other than technical solution. Although there are laws provided to overcome the problem, but it is still inadequate. Besides, the consumer awareness and education also should be instilled in order to minimizing the problem of phishing as well as security aspect stressed by the banking industry.