World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:1, No:11, 2007

Managing Legal, Consumers and Commerce Risks in Phishing

Dinna N. M. N., Leau Y. B., Habeeb S. A. H., and Yanti A. S.

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf

Abstract**—**Phishing scheme is a new emerged security issue of E-Commerce Crime in globalization. In this paper, the legal scaffold of Malaysia, United States and United Kingdom are analyzed and followed by discussion on critical issues that rose due to phishing activities. The result revealed that inadequacy of current legal framework is the main challenge to govern this epidemic. However, lack of awareness among consumers, crisis on merchant's responsibility and lack of intrusion reports and incentive arrangement contributes to phishing proliferating. Prevention is always better than curb. By the end of this paper, some best practices for consumers and corporations are suggested.

Keywords**—**Phishing, Online Fraud, Business risks, Consumers privacy, Legal Issue, Cyber law.

I. Introduction

NOWADAYS, 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 [1] and social engineering that attempts to trick users into revealing their personal private data, particularly financial data [2]. 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-Phishing. Beside internet phishing, a new creature of mobile phishing has been discovered recently, where a number of victims have been cheated by a mobile message mentioning that they had won a lucky draw ticket and to receive the price they need to bank in a certain amount of money to settle foreign taxes. Although the message sounds attractive rather than threatening, the objective is the same: to trick recipients into disclosing their financial and personal data [3].

Phishing can be accomplished anonymously, easily, with a variety of means, and the impact upon the victim can be devastating. The tricks are made by masquerading as a trustworthy authority in an apparently official electronic communication medium such as an email or an instant message or even luring the recipients to a fraud web site.

Recently phishing has emerge into the limelight, whereby cyber criminals will either use a person's details to create fake accounts, ruin a victim's credit or even prevent victims from accessing their own accounts after confidential information are fraudulently acquired. This widespread phenomenon had gradually diminished consumer confidence in e-commerce transaction.

II. Inadequately of Legal Framework

A. Malaysia

In Malaysia, a total of 86 phishing cases were reported in 2006 [4]. The Malaysian Computer Emergency Response Team quarterly report clearly indicated that phishing scams has become a major forgery case which involves local and foreign financial institution [5]. Based on Timothy J. Muris [6], phishing is a two time scam where phishers steal a company's identity and then use it to victimize consumers by stealing their credit identities. Due to the usage of false statements to mislead innocent people into disclosing valuable personal data, phishers may violate a host criminal statue.

In this context, the argument is 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 four new packages of 'cyber-laws': the Computer Crimes Act, Digital Signatures Act, the Copyright (Amendment) Act and the Telemedicine Act.

Manuscript received September 27 , 2007

Dinna Nina Mohd Nizam is with the School of Informatics Science in Universiti Malaysia Sabah, Labuan International Campus, 87000 F.T.Labuan, Malaysia (e-mail: dinna_ninamn@yahoo.com).

Leau Yu Beng is also with the School of Informatics Science in Universiti Malaysia Sabah, Labuan International Campus, 87000 F.T.Labuan, Malaysia (e-mail: leauyubeng@gmail.com).

Habeeb Saleh Al Habeeb is with the Saudi Stock Exchange (Tadawul), NCCI Building, North Tower, King Fahd Rd., P. O. Box 60612, Riyadh 11555, Kingdom of Saudi Arabia (e-mail: habeeb.habeeb@tadawul.com.sa).

Yanti Ahmad Shafiee is with the School of International Business and Finance in Universiti Malaysia Sabah, Labuan International Campus, 87000 F.T.Labuan, Malaysia (e-mail: yanti@ums.edu.my).

TABLE I
BRIEFLY DEFINES ALL ACTS IN THE CURRENT MALAYSIAN CYBER LAW
(SOURCE: HTTP://WWW.MYCERT.ORG.MY/)

Law	Purposes
Copyright Act 1987	To make better provisions in law relating to copyright and for other matters connected therewith.[7]
Computer Crime Act 1997	To provide for offences relating to the misuse of computers.[8]
Digital Signature Act 1997	To make provision for and regulate the use of, digital signatures to provide for matters connected therewith.[9]
Telemedicine Act 1997	To provide for the regulation and control of the practice of telemedicine, and for matters connected therewith.[10]
Communication and Multimedia Act 1998	To provide for and to regulate the converging communication and multimedia industries and for incidental matters.[11]
The Malaysian Communication and Multimedia Commission Act 1998	To supervise and regulate the communications and multimedia activities in Malaysia, and to enforce the communications and multimedia laws of Malaysia and for related matters.[12]

Among all cyber laws shown in Table I, *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 [13]. 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 phiser syndicates. Hence here it is clear that Malaysia does not have any existing Cyber Law that could prevent phishing activities perfectly. Thus this allows

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf

Malaysian to be exposed to phishing attacks without any appropriate protection from the Federal Law.

B. United States

Compared to other developed country such as the United States, similar situation happened before a certain law in governing phishing was existed. Even though there are still some cases where the prosecutor manages to convict the phishers and penalize them with deserver punishments but only in exceptional cases. For instance in a case that happen in Houston, Taxes where a defendant intentionally send phishing emails to AOL and Paypal by spoofing websites and gain consumers credit card numbers was convicted with the legislation under Access Device Fraud 18 U.S.C 1029 (a)(3). The phisher was then sentence to 46 months of imprisonment [14].

Based on the latest report from the Criminal Division, Department of Justice, since phishers uses false and fraudulent statements to mislead people into disclosing valuable personal data, phishing schemes may violate various federal criminal statutes. In many phishing schemes, participants in the scheme may be committed to identity theft, wire fraud, credit-card fraud, bank fraud, computer fraud, or the newly enacted criminal offences in the CAN-SPAM Act. When a phishing scheme involves computer viruses or worms, participants in the scheme may also infringe other provisions of computer fraud and abuse statute related to damage of computer systems and files. Finally, phishing schemes may violate various state statutes on fraud and identity theft [15].

Prosecutions of phishing cases under these existing legislations are very challenging and depend on the intention and action of the perpetrator. Inadequacy of the old legal framework was followed by the enforcement of a new legislation known as the Anti-*Phishing Act of 2005* that specially governs the phishing epidemic in 2005.

Recently, the United States has been the prime mover to enforce the *Anti-Phishing Act of 2005* by Sen. Patrick Leahy (D-Vt.), where the legislation aimed at curbing problems of phishing [16]. The Act focuses on criminalization of two essential parts of phishing attacks which are:

1) The creation and procurement of a web sites that represents itself to be that of a legitimate business, and that attempts to induce the victim to divulge personal information, with the intent to commit a crime of fraud or identity theft.
2) The creation or procurement of e-mail that represents itself as a legitimate business with similar intent.

Based on a view from a member of Senator Leahy's staff, prosecuting phishing scammers under certain existence statutes can be challenging even though they have already violated a host of identity theft and fraud laws. To charge scammers in court, law enforcers need to prove that a victim suffered measurable losses but by the time they do that, the scammer normally disappear [17]. As a result, this new Act will positively allow the prosecution of perpetrator without requirement of showing specific damages to any individual.

But this bill aroused some challenges in its effectiveness to quarantine the thwart phishers. To identify and locate the source of a particular phishing campaign is a main challenge. Lacks of mechanism in the present email system in requiring a sender's identity to be authenticated, allows spammers to conceal their identities freely and causes the process of finding the criminals more complicated.

As the fact that most cyber crimes and phishing attack involves worldwide organizations, the procedures to obtain jurisdiction over the phisher is another impediment in the context. Even if the phisher can be located there is still a high possibility that he/she is located in a foreign country outside of the legislation's jurisdictional reach [18].

C. United Kingdom

Recently, the UK Government's Fraud Bill has been revised to include a new fraud offence that specifically targets the person responsible for phishing attacks. The new offence, which strengthened the current legislation and ease the path of criminal prosecution, covers phishing acts under "Fraud by False Representation". It clarifies that any person disseminating an email to large groups of people with falsely claiming to be a legitimate financial institution in order to gain access to individuals' personal financial information will be committing an offence [19].

For instance in this Fraud Bill [20] a phisher can be convicted under Section 2, a phisher is in breach if he dishonestly makes a false representation in a bogus email or fake website and intends to gain or cause loss to business or consumer.

Besides that, owning a fraud website and sending spurious email to victim by phishers who intent to commit offences involving frauds also will be charged under Section 6 and Section 7 where else websites are classified as an electronic program and email as electronic data under Section 8. In addition, this bill also includes a clause which will allow for extradition in such cases, a clause which will be useful in prosecuting offenders who operate overseas and whose crimes are not hindered by geographical borders.

The United States and United Kingdom both successfully added a new legislation in their existing legal framework to fight phishing, in order to protect their e-commerce consumers and sellers online.

Therefore in this case, Malaysia should follow the steps to enforce a specific legislation for the purpose against phishing in this country since the growth of cyber crime in Asia Pacific had increase dramatically. The new regulation should be a valuable tool to account challenges which have arise the Anti-Phishing Act 2005 and also harmonized with other existing legislations. This is a good first step and will no doubt need to be revisited at some point in the very near future.

Even though it is necessary to use legislation as a deterrence, but legislation alone will not stop the increase of phishing attacks. There are some difficulties in convicting a phisher under particular legislation. First, phishing attacks happen very fast that gives crime forensics difficulty in tracing or suspecting the scam. Addition to that identification of fraudulent website before the scam happens is beyond the scope of most security technologies especially for cases that involves international phishers.

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf

Consequently, due to the profits gain from these attacks and low risk of being caught allows phishing to be an attractive criminal venture.

III. Critical Issues in Phishing Schemes

A. Lack Awareness among Consumers

Focusing on the consumer aspect, a non-educated consumer is basically more vulnerable to phishing attacks. Consumer's confidence towards online security of financial services has decline considerably due to continual reports of identity theft and phishing scams. The substantiation nature of the Internet distributes advantages to phishers. Great number of issues arises due to phishing activities. In general a phishing attack takes place by disguising as an official email which uses the official brand name of a known website to trick customers to disclose their personnel information. Customers can see no visible suspicious object about the email.

Authentication is a main legal issue in this fraudulent activity. Verifying the authenticity of consumers is critical because the phisher acquires sensitive information such as password and credit card details by masquerading as a trustworthy party. In many cases, consumers do not have adequate knowledge to distinguish the disputable email or website. Therefore, lack of particular awareness among consumers will victimize them into these attacks.

Subsequently, consumers can loose their confidentiality when phishers easily gain access to large databanks of email address. Corporations should be responsible for the safeness of consumers' information but unfortunately they tend to neglect this confidential issue by unintentionally divulging customers' information to third parties. As a result, trust towards online payment systems and protection of consumers' personal data by financial institution weakens.

Maintaining integrity of data is another crucial issue raised by the phishing scheme. Data or personal information are maliciously modified, altered or destroyed by an immoral party known as the phishers. Due to these alteration activities and false emails and websites by the phishers causes decline of consumers' confidence on online banking and e-commerce activities.

Availability of accounts is another issue. When consumers' personnel information is in the hands of the phishers', false accounts can be created easily by these wrongdoers. This consequently allows the phishers to ruin the victim's credit card and prevent the victim from accessing their own accounts. This confusion of account accessibility for the consumers provides uncertain security level that chases consumers away from usage of cyber space today.

Overall, phishing attack has become a sobering reminder of the vulnerability of the Internet to consumers. Lack of awareness about relevant issues and natural position to be prepared seems to be the weakness factor. Therefore, the key factor to gain success in the growth of e-commerce activities in Malaysia is to nurture consumers' trust on online transaction by educating consumers' to fight phishing attacks.

B. Merchants' Responsibility Crisis

Some argue that online merchants should be responsible of informing their customers' the current phishing attacks towards the merchant. But a number of merchants pay no attention to this responsibility. Instead, merchants resolve by preventing future occurrences and minimize harm done to their reputation. Priorities are given more to mending security problem, disciplinary action towards the phisher and resume business as soon as possible. This particular incident handling conflict had become a popular argument among e-commerce marketplaces today.

Online merchants have never taken phishing attack seriously because of profits and reputations. This reaction in hiding the truth about the merchants' phishing threats indirectly contributes to the growth of more phishing attacks. There are many reasons why a merchant tries so hard to hide their phishing threats rather then devastating financial losses. One reason that can be considered is the limitation of relevant knowledge of identifying a phishing scam with the current technology. Low awareness and sensitiveness among online merchants regarding latest security issue have exposed themselves to phishing without any protection.

In some extreme cases, corporation will only realize that they are under attack when their customers become victims of phishers. Ethically online merchant should react in advance like implementing integrity management systems to increase customers' awareness and hence help customers to prevent from phishing threats.

However, online merchant should realize that covering phishing threats will only benefit them temporarily. In the long run it is beyond their power to cover the hidden threats because more and more customer will be attacked by phishers. Sooner or later customers will tend to feel betrayed as corporations continue ignoring their social responsibilities in informing them about the merchants' phishing threats. This unethical practice among online merchants' will result to anti-business reaction from the public such as boycotting the merchant until unexpected losses happens to the corporation. For extremely cases, consumers can bring this unethical online merchant issue into court for their losses.

Therefore, one should realize that it might not be secure to do business transaction with merchants that have never undergo any phishing attacks because the phishing threat maybe hidden from customers for the benefit of the company. As a result authorities should draft new laws to force online merchants to inform their customers about any phishing activities. Currently, in Malaysia, United States and United Kingdom have no law addressing this issue.

It is undeniable that there are some companies that are honestly informing their customers about phishing attack towards the company. It is a social responsibility for the company and also the customers' right to know what attacks are happening to their financial institution. This ethical practice will raise dual polar effect, where one is corporation may initially loose their customers trust but will reestablish the trust when the corporation resolve the phishing threat. Second is trust of customer towards the corporation grows stronger because of ethics and honesty of the corporation. As

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf

from the customers' perspective, effort of solving and protecting them from being phishing victims are much appreciated. This also avoids online merchants of the risk of customer's lawsuits and financial losses in the future.

C. Lack of Intrusion Report and Incentive Arrangement

According to Dr Zaitun, National ICT Security and Emergency Response Centre (Niser), only a minority of phishing victims were willing to report the incident. Unwillingness to go through legal process is the reason that hold victims back from reporting. The result of this "under-reporting" was lack of reliable information about cyber-crimes, which hampered action against cyber-criminals and in turn reinforced the idea that there was little to gain by reporting them to the authorities [21]. Generally, the lack of accurate intrusion reports is the main reason why the risk of phishing is not widely recognized. This may increase cost to online merchants and loss of consumers for insuring against phishing risks. In fact, Microsoft Corp., eBay Inc. and Visa International Inc. launched a program - Phish Report Network (PRN) to address the rampant of phishing problem by sharing information [22]. But the country and world are still lack of a set of national and cross-border framework to encourage companies to share information on phishing. Therefore, companies targeted by foxy phisher should not just watch out for dangerous phishing traps, but also need to do more for their unwary consumers.

IV. Legal Remedies

Currently in the United Kingdom legislation to protect consumers' privacy does exist. It is known as the Data Protection Act 1999 [23]. Under this act consumers' data are protected and the balances between the right of individual and usage of personal information for rightful reasons are highlighted. Similar legislation is also found in the United States where the state of California became the first state to enact the law addressing to phishing. Consumers in the States are protected under the Personal Data Privacy and Security Act 2005 [24]. Possibly with emerge of these acts confidence among consumers can be achieved by confronting phishing issues.

In Malaysia, legal action that can be taken by consumers towards the phisher after realizing the attack is limited. The only existing acts that can be used by consumers are the Consumer Protection Act 1999. But this act only focuses on the goods and services that are offered and supplied to consumer in a trade [25]. In Part 1 Section (2) Subsection 2(g), it clearly states that this act shall not apply to any transactions effected by electronic means unless otherwise prescribed by the Minister. Therefore it is a challenge for victims to convict perpetrators whom had steal there personal data via fraudulent schemes.

In 2002, a surprising act was about to be introduce for the consumers data protection known as the Personal Data Protection Act. Unfortunately this act was delayed due to numerous request of exclusion from corporations. This act consist of nine data protection principles covering the collection, use, disclosure, accuracy, retention, access to and security of personal data. If implemented, it will generate a government that officially appoints data protection and will have the power to monitor and enforce compliance, promote public awareness of the law, encourage trade bodies to prepare industry code of practice and corporate with counterparts in foreign countries [26].

V. Best Practices for Consumers and Corporations

Prevention is always better than solution. The particular legislation will only effectively protect consumers and corporations from phishing attacks only after phishing activities occur. Phishing activities can not be solved by legislation only. Therefore, consumers and corporation should take some practices to protect themselves before unsuspicious attack occurs. These are some best practices for:

1) Consumers
   i. Automatically block malicious fraudulent E-mail.
   ii. Automatically detect and delete malicious software.
   iii. Automatically block outgoing delivery of sensitive information to malicious parties.
   iv. Be suspicious.
2) Corporations
   i. Establish corporate policies and share them to consumers.
   ii. Provide a way for the consumer to identify that the E-mail is legitimate
   iii. Stronger authentication in Websites.
   iv. Monitor the Internet for potential phishing web sites.
   v. Implement good quality anti-virus, content filtering and anti spam solutions [27].

VI. Conclusion

When phishing treat is disseminated no one with an Inbox can be immune or protected from the attack. Corporations, financial institutions and consumers will be victimized and thus lead to lost of both time and money. Phishing attacks continue to escalate in terms of complexity, frequency and harshness. Briefly, phishers are the street muggers of this digital era. Even though Malaysia is still in an infant stage, the government, corporations and consumers could not afford to neglect this approaching and frightening fraud. On the contrary, each party must work hand-in-hand to turn the tide against proliferating fraud. Last but not least, solution for phishing is likely to be a combination effort between education, technology, legislation and law enforcement.

Appendix

"Computer Crime Act 1997"

Section 3: Unauthorized access to computer material.

(1) A person shall be guilty of an offence if:

a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

b) the access he intends to secure is unauthorized; and

c) he knows at the time when he causes the computer to perform the function that is the case.

Section 2 (5): For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorized if:

a) he is not himself entitled to control access of the kind in question to the program or data; and
b) he does not have consent or exceeds any right or consent to access by him of the kind in question to the program or data from any person who is so entitled.

Section 4: Unauthorized access with intent to commit or facilitate commission of further offence.

(1) A person shall be guilty of an offence under this section if he commits an offence referred to in section 3 with intent:

a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code [Act 574]

Section 5: Unauthorized modification of the contents of any computer.

(1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

"Access Device Fraud 18"

Definition 1029: Fraud and related activity in connection with access devices

Subsection (a)(3)(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices.

REFERENCES

[1] Sean B. Hoar, (2001). "Identity Theft: The Crime of the New Millennium", USA Bulletin, http://www.cybersafe.gov/criminal/cybercrime/usamarch2001_3.htm
[2] Anonymous, (2007). "Phishing - Nationmaster", http://www.nationmaster.com/encyclopedia/phishing
[3] U.S. Department of Justice, (2004). "Special Report on Phishing", http://www.usdoj.gov/criminal/fraud/docs/phishing.pdf
[4] MyCERT, (2006). "MS-111.112006: MyCert Quarterly Summary (Q3) 2005", http://www.mycert.org.my/
[5] MyCERT, (2005). "MS-093.072005: MyCert Quarterly Summary (Q2) 2005", http://www.mycert.org.my/
[6] Bob Sullivan, (2003). "Look-alike Email Scams on the Rise", http://www.msnbc.msn.com/id/3078451
[7] Laws of Malaysia, (2001). "Copyright Act 1987 – Act 332", http://www.msc.com.my/cyberlaws/act_copyright.asp
[8] Laws of Malaysia, (2002). "Copyright Crime Act 1997 – Act 563", http://www.msc.com.my/cyberlaws/act_computer.asp
[9] Laws of Malaysia, (2002). "Digital Signature Act 1997 – Act 562", http://www.msc.com.my/cyberlaws/act_digital.asp
[10] Laws of Malaysia, (2002). "Telemedicine Act 1997 – Act 564", http://www.msc.com.my/cyberlaws/act_telemedicine.asp
[11] Laws of Malaysia, (2002). "Communications and Multimedia Act 1998 – Act 588", http://www.msc.com.my/cyberlaws/act_communications.asp
[12] Laws of Malaysia, (2002). "Malaysian Communications and Multimedia Commission Act 1998 – Act 589", http://www.msc.com.my/cyberlaws/act_malaysiancomm.asp
[13] Lawyerman, (2005). "Law Dictionary - Fraud", http://www.lawyerment.com.my/scripts/dictionary/?id=362&pr=fraud
[14] Federal Trade Commission, (2004). "FTC v. Zachary Keith Hill", http://www.ftc.gov/os/caselist/0323102/040322info0323102.pdf
[15] United States Department of Justice, (2004). "Internet and Telemarketing Fraud", http://www.usdoj.gov/criminal/fraud/internet/
[16] Steptoe&Johnson, (2004). "Just What Copyright Law Needs", http://www.steptoe.com/publications-3149.html
[17] David McGuire, (2004). " Senate Bill Targets 'Phishers' ", Washingtonpost, http://www.washingtonpost.com/wp-dyn/articles/A44826-2004Jul12.html
[18] Robert Louis, (2005). "Plugging the 'Phishing' Hole: Legislation Versus Technology", http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html
[19] SecurityPark.net, (2005). "Fraud Law strengthened to counter phishing attacks", http://www.securitypark.co.uk/article.asp?articleid=23886&CategoryID=1
[20] House of Lords, (2005). "Fraud Bill [HL]" , http://www.publications.parliament.uk/pa/ld200506/ldbills/007/2006007.pdf
[21] H.Amir Khalid, (2004). "Cyber-crime: Business and the law on different pages", The Star, http://www.niser.org.my/news/2004_03_05_01.html
[22] Symantec Corporation, (2006). "What is the Phishing Report Network?", http://www.phishreport.net/
[23] Office of Public Sector Information, (1998). "Data Protection Act 1998", http://www.opsi.gov.uk/acts/acts1998/19980029.htm
[24] The Library of Congress, (2005). "Personal Data Privacy and Security Act of 2005", http://thomas.loc.gov/cgi-bin/query/D?c109:44:./temp/~c109jCs5pz.
[25] Parlimen Malaysia, (1999). "Akta Perlindungan Pengguna 1999- Akta 599", http://www.parlimen.gov.my/pdf/a599.pdf
[26] Electronic Privacy Information Center, (2003). " Privacy and Human Rights 2003", http://www.privacyinternational.org/survey/phr2003/countries/malaysia.htm
[27] McAfee Inc, (2005). "Anti-Phishing-Best Practices for Institutions and Consumer", http://www.mcafee.com/us/local_content/white_papers/wp_antiphishing.pdf

Open Science Index, Economics and Management Engineering Vol:1, No:11, 2007 publications.waset.org/5717/pdf