

Chapter 2: Origin of Phishing

2.1 Introduction

In this chapter, the study will be focusing on the beginning of the scam techniques used by identity thieves to fish for personal information in a pond of unsuspecting Internet users. Most popular among the hackers who unauthorized access to the computer material briefly discussed situation in Malaysia. In addition, the definition and concept of phishing described by authority organization such as Anti-phishing Working Group (APWG), and comparatively analyzing with terms like identity theft and account hijacking.

2.2 Historical Review

Although at the earlier stage, we had briefly discussed about computer crime, but the study carried out had been focused on phishing, which is also known as “brand spoofing” or “carding”, a term created by hackers as a play on the word “fishing”. It originally comes from the analogy that Internet scammers are using email lures to “fish” for passwords and financial data from the sea of Internet users.⁶ “Ph” is a common hacker replacement for “f”, and is a nod to the original form of hacking, known as “phreaking”. The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The first mentioned on the Internet of phishing is on the alt.2600 hacker newsgroup in January 1996. However the term may have been used even earlier in the printed edition of the hacker newsletter “2600”. By 1996, hacked accounts were called “phish”, and by 1997 phish were actually being traded between hackers as a form of currency. People would routinely trade 10 working AOL phish for a piece of hacking software that they needed for.

⁶ The Anti-Phishing Working Group, Proposed Solutions to Address the Threat of Email Spoofing Scams, (2003),

Computer hacking and unauthorized access is one of the major problems in the Information Age. Our computers are always at risk of computer hackers. This problem also includes the problem of viruses introduced through computer.

Traditionally, the concept of criminal law in property relates mainly to property of a tangible kind. So, a question arises whether it also includes property which is intangible in its nature like data and software. Under the English law, data and software are not regarded as tangible property or goods as decided in the case of *St. Albans City and District Council v. International Computers Ltd*⁷. This case was concerned with the sale of a computer and software by International Computer Ltd (ICL) to the local authority which wanted the computer to deal with the introduction of the Community Charge and its finances generally. A defect in the program led to an overstatement of the population figure for the council's area and a consequent loss of revenue from central government and from the Community Charge itself. It was held that the computer software does not fall under the category of goods and as such the defect in the computer software cannot be recoverable under the implied terms of UK Sale of Goods Act 1979. In the case of *Boardman v. Phipps*⁸, Lord Upjohn stated that "in general information is not property at all. It is normally open to all who have eyes to read and ears to hear..."

In Malaysia, the Computer Crimes Act 1997 is an Act which provides for offences relating to the misuse of computers⁹. Section 3 of the Act provides for offences of unauthorized access to computer material. It reads:

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

⁷ [1996] 4 All ER 481.

⁸ [1967] 2 AC 46.

⁹ Preamble, Computer Crimes 1997 (Act 563).

(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 unauthorised; and

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

(2) The intent a person has to have to commit an offence under this section need not be directed at –

(a) Any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

The ingredients of the offence under this section may be as follow:-

- i. causes a computer to perform any function (actus reus)
- ii. at the time he causes the computer to perform any function, it must be coupled with intention to secure access to any program or data in any computer (mens rea)
- iii. the access is unauthorised
- iv. he has that knowledge (mens rea)

A person is said to secure access to any program or data held in any computer by causing a computer to perform any function, he alters or erases the program or data, copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held, uses it or causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

So, whether or not the unauthorised access is a success, it is not an issue here since the section requires only an intention. However, if the unauthorised access is not success, it is recommended that the accused to be charged under s.7 under the same Act (i.e under attempt).

However there is a view ¹⁰ that mere physical contact with the computer like reading of computer printout and the reading of data displayed on the monitor cannot be considered as an offence under this Act. It is also the view in UK as to s.1 and 2 of Computer Misuse Act 1990¹¹. The view that s.2 (2)(d) of the Act provides that a person secures access to program or data in a computer by causing it to perform any function where he causes it to be output from the computer in which it is held whether by having it displayed or in any other manner. Referring to section 2(1) of the Act;

“Computer output” or “output” means a statement or representation whether in written, printed, pictorial film, graphical, acoustic or other form produced by a computer, displayed on the screen of a computer...

Thus, it is submitted that the reading of computer printout and reading of data displayed on the screen are also within the offence prescribed under this section.

Another point for contention in this section is the phrase “any program or data held in any computer”. In s.2 (6) of the Act, any data or program held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer. As such, the 3½ inch disk which is considered as a data storage

¹⁰ Sulaiman Azmil, *Crimes on The Electronic Frontier – Some Thoughts On The Computer Crimes Act 1997* [1997] 3 MLJ lxvii

¹¹ Rowland, D., MacDonald, E., *Information Technology Law*, Cavendish, London, 1997 pg 347 - the author viewed that unauthorised reading after printing out in cases where the printing is done by an authorised user, or mere reading of information on computer screen

facility under the definition of “computer” which is outside the computer can be destroyed, erased or modified without being caught under this section.

There is no case reported under this section in Malaysia yet, but reference can be made to the English case of *R v. Cropp* where the accused was charged with an offence under s.2(1) of Computer Misuse Act 1990¹² which requires establishment of an offence under s.1(1) of the Act. The accused visited the premises of his ex-employer. He picked up a machine and a salesperson began to enter the details of the item in the storeroom computer. Then the computer left unattended for a while by the salesperson and the accused being well-acquainted with the operation of the computer in the premises entered a discount of 70% on the item. Subsequently, the accused paid only £204.60 instead of £710.96. At first instance, the court acquitted the accused on the basis that the wording of the section requires the act to be done from **another computer**. On appeal, the Court of Appeal ruled that “there are no grounds whatsoever while implying or importing the word other between any of the computer or accepting the computer which is actually used by the offender from the phrase any computer at the end of s.1(a). So, it does not require the offender to be convicted under this section by using another computer but any computer including the computer that he hacked. This interpretation should be adopted by Malaysian court.

In another case reported in Singapore, a teenage student sentenced to jail for computer hacking, however on appeal, Yong Pung How CJ replaced the lower court ruling, ordering the 17 year old hacker to undergo 30 month probation with a four month jail term¹³. Meanwhile, in a landmark case in Hong Kong a teenager was sentenced to six months in

¹² Similar to s.3 of the Act

¹³ Singapore teenager jailed for computer hacking in landmark ruling. Online www.nstp.com.my/archive (3rd. February 2002).

jail for hacking after pleaded guilty to a total of 49 computer crimes related charges¹⁴. In Beijing, China, a man convicted of destroying computer information systems of China Net, a major Internet service provider, was sentenced to 18 months imprisonment¹⁵.

One of the chaotic cases was the intrusion of Parliament websites by the Brazilian hacker known as "Topeira"¹⁶. Unfortunately, none of these hackers have been brought before any court of justice. It is no doubt that the major hurdles in bringing these criminals before the court are the problem of detection, enforcement and proof or evidence.

In the most highlighted case, concerning Love Bug virus, the former computer student, Onel de Guzman, the accused of releasing the "ILOVEYOU" computer virus where it overwhelmed e-mail systems worldwide causing damages estimated at billions of dollars.

In the United States, David L. Smith, 31, accused in April 1999 of unleashing the "Melissa" computer virus pleaded guilty to both state and federal charges, admitting that he created and spread the virus that caused millions of dollars in damage¹⁷. Smith admitted spreading the Melissa virus, which infected more than one million personal computers in North America and disrupted computer networks in business and government which caused more than \$80 million in damage.

Smith admitted in state and federal court that he created the Melissa virus and disseminated it from his home computer. He said that he constructed the virus to evade anti-virus software and to infect computers using the Windows 95, Windows 98 and Windows NT operating systems and the Microsoft Word 97 and Word 2000 word processing programs.

¹⁴ Hong Kong Computer Hacker Jailed in Landmark Case. Online www.utusan.com.my/archive/ (31st January 2002).

¹⁵ Chinese hacker gets 18 months in prison. Online www.nstp.com.my/archive/ (3rd. February 2002).

¹⁶ Polis mula siasat kes ceroboh laman web Parlimen. Online www.utusan.com.my/archive/ (30th January 2002).

¹⁷ December 9, 1999, Creator of "Melissa" Computer Virus Pleads Guilty to State and Federal Charges. Online www.usdoj.gov/criminal/cybercrime/melissa.htm (3rd February 2002).

Because each infected computer could infect 50 additional computers, which in turn could infect another 50 computers, the virus proliferated rapidly and exponentially, resulting in substantial interruption or impairment of public communications or services. According to reports from business and government following the spread of the virus, its rapid distribution disrupted computer networks by overloading email servers, resulting in the shutdown of networks and significant costs to repair or cleanse computer systems.

2.3 General Background of Phishing

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. The United States Department of Justice defines phishing as criminals' creation and use of e-mails and websites--designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies--in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords.¹⁸

The UK Financial Services Authority (FSA) describes phishing as an attack where criminals send spoof emails misrepresenting corporate identity to trick individuals to disclose personal financial data such as account numbers and PINs. They create websites that mimic the trusted brands of well-known financial firms.¹⁹

The Anti-Phishing Working Group (APWG) defines phishing also known as the spoofing scam has the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers. Phishing is the creation of email messages and web pages that are replicas of existing sites to fool users into submitting personal, financial, or password data.

¹⁸ United States Dept. of Justice, *Special Report on "Phishing,"* p. 3 (2004), available at <http://www.usdoj.gov/criminal/fraud/Phishing.pdf>

¹⁹ Financial Services Authority, *Countering Financial Crime Risks in Information Security: Financial Crime Sector Report*, (2004)

Organized crime operatives typically mount these attacks in order to use the data to execute high-value currency transfers – or to mount sophisticated identity theft schemes and credit-card scams. Typically, a phishing email arrives with the spoofed company’s logo and email layout, requesting the receiver to link to what appears to be a genuine Web site where the victims are instructed to enter their account number and password. If convincing, the scammers will net some customers.²⁰

Phishing attacks are blooming in frequency, scope and rates of success with upwards of 20% of targeted users providing personal information. Recently, Citigroup, Lloyds TSB and Barclays have been subjected to phishing attacks that spoofed their identities in pursuit of customer’s account, debit and credit card data. Within the last year, Wachovia, Bank of Montreal, Bank of America, St. George Bank, and the ANZ Bank of Australia, have been hit by phishing scams. Although financial services firms were obvious initial targets for phishing attacks, highly adept identity theft rings have expanded their operations to exploit a number of Internet consumer brands including Yahoo!, eBay, Paypal, Monster.com, Bestbuy.com, Microsoft MSN and even the FBI.

The deeper the store of data that is held by the enterprise, the more likely it will be targeted for phishing attacks by identity theft rings. Retailers can retain almost any depth of data, depending on the nature of their business. Financial services usually archive substantial amounts of personal data though they are not, as a class, the most data rich source of consumer data. We believe that a highly prized target for identity theft operatives will be health care agencies and health care data processors because they archive rich, deep stores of high quality consumer data including accurate dates of birth, social security numbers and true postal addresses.

²⁰ The Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of Email Spoofing Scams*, (2003)

As mentioned earlier, the word “phishing” comes from the analogy that Internet scammers are using email lures to “fish” for passwords and financial data from the sea of Internet users.²¹ The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The first mention on the Internet of phishing is on the alt.2600 hacker newsgroup in January 1996; however the term may have been used even earlier in the printed edition of the hacker newsletter “2600”. “Ph” is a common hacker replacement for “f”, and is a nod to the original form of hacking, known as “phreaking”. Phreaking was coined by the first hacker, John Draper (aka. “Captain Crunch”). John invented “hacking” by creating the infamous Blue Box, a device that he used to hack telephone systems in the early 1970s.²² This first form of hacking was known as “Phone Phreaking”. The blue box emitted tones that allowed a user to control the phone switches, thereby making long distance calls for free, or billing calls to someone else's phone number, etc. This is in fact the origin of a lot of the “ph” spelling in many hacker pseudonyms and hacker organizations.

By 1996, hacked accounts were called “phish”, and by 1997 phish were actually being traded between hackers as a form of currency. People would routinely trade 10 working AOL phish for a piece of hacking software that they needed. Over the years, phishing attacks grew from simply stealing AOL dialup accounts into a more sinister criminal enterprise. Phishing attacks now target users of online banking, payment services such as PayPal, and online e-commerce sites. Phishing attacks are growing quickly in number and sophistication. In fact, since August 2003, most major banks in the USA, the UK and Australia have been hit with phishing attacks.²³

²¹ Ibid

²² Ibid

²³ Ibid

In October 2004, the Canada-U.S. Cross-Border Crime Forum released a report, prepared jointly by the U.S. Department of Justice (DOJ) and Public Safety and Emergency Preparedness Canada (PSEPC), on Identity Theft²⁴. The report identified, among other methods of committing identity theft, the growing use of a technique known as “phishing”: Consumers will receive "spoofed" e-mails (e-mails that appear to belong to legitimate businesses such as financial institutions or online auction sites). These e-mails will typically redirect consumers to a spoofed website, appearing to be from that same business or entity. Similarly, many consumers receive "pretext" phone calls (phone calls from persons purporting to be with legitimate institutions or companies) asking them for personal information. In fact, the criminals behind these e-mails, websites and phone calls have no real connection with those businesses. Their sole purpose is to obtain the consumers' personal data to engage in various fraud schemes.

The Canada-U.S. Cross-Border Crime Forum determined that it would be appropriate to follow up on the Identity Theft report with a joint report on Phishing and its impact on cross-border criminality. It directed the Canada-U.S. Working Group on Cross-Border Mass-Marketing Fraud, which reports to the Forum annually, to prepare this report. Prepared jointly by the U.S. DOJ and Public Safety and Emergency Preparedness Canada (PSEPC), the report is the result of contributions from the many agency and individual participants in the Working Group from the United States and Canada.

The objective of this report is to define the nature, scope and impact of phishing, to provide the public with information on how to respond to phishing schemes, and to identify current and promising approaches to combating phishing. It includes information on phishing

²⁴ See USA and Canada Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Oct 2006

trends, statistics and a discussion of the principal factors affecting the growing use of phishing by fraudsters.

In the report, the term *phishing* is defined as general term for the creation and use by criminals of e-mails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information. These criminals deceive Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords, or into unwittingly downloading malicious computer code onto their computers that can allow the criminals subsequent access to those computers or the users’ financial accounts.²⁵ Phishing is best understood as one of a number of distinct methods that identity thieves use to “steal” information through deception – that is, by enticing unwitting consumers to give out their identifying or financial information either unknowingly or under false pretenses, or by deceiving them into allowing criminals unauthorized access to their computers and personal data. The United States and some other countries use the term “identity theft,” and the United Kingdom often uses the term “identity fraud,” to refer broadly to the practice of obtaining and misusing others’ identifying information for criminal purposes. Identity fraud also can be used to refer to the subsequent criminal use of others’ identifying information to obtain goods or services, or to the use of fictitious identifying information (not necessarily associated with a real living person) to commit a crime.

Phishing is committed so that the criminal may obtain sensitive and valuable information about a consumer, usually with the goal of fraudulently obtaining access to the consumer’s bank or other financial accounts. According to Federal Deposit Insurance Corporation (FDIC) the term “identity theft” is the use of personal identifying information to commit

²⁵ Ibid

some form of fraud²⁶. Although the range of consumer frauds and criminal acts coming under that definition is quite broad, the focuses on the subset of identity theft that is of particular concern to financial institutions insured by the FDIC and to the institutions' customers: unauthorized access to and misuse of existing financial institution asset accounts primarily through phishing and hacking.²⁷ This form of identity theft is referred to here as "account hijacking." The report examines how technology is used to commit account hijacking and the methods available to help prevent it.

The term "identity theft" means the fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade Commission] may prescribe, by regulation.²⁸

Pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Federal Trade Commission (FTC) has recently proposed a more specific definition of identity theft which describes what is meant by the term "identifying information":

(a) The term "identity theft" means a fraud committed or attempted using the identifying information of another person without lawful authority.

(b) The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any-

(1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

²⁶ FDIC, Putting an End to Account-Hijacking Identity Theft: December 14, 2004 available at [www.fdic.gov/consumers/consumeridtheftstudy/identity theft.pdf](http://www.fdic.gov/consumers/consumeridtheftstudy/identity%20theft.pdf)

²⁷ Phishing attacks use fraudulent or "spoofed" e-mails and Web sites to fool recipients into divulging confidential information, such as account user names and passwords, to criminals. Hacking is the unauthorized intrusion, perpetrated remotely, into a computer or network

²⁸ Ibid

- (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address, or routing code; or
- (4) Telecommunication identifying information or access device. . . .

Although the FTC’s proposed definition refines the statute, both of them cover existing as well as newly created accounts, asset as well as credit accounts, and masquerading as someone else as well as creating a synthetic identity in an effort to obtain services or other benefits fraudulently

In its Identity Theft Survey Report, the FTC included a category of identity theft, described as the “misuse of existing non-credit card account or account number.”²⁹ At least one organization within the financial services industry has created its own definition of identity theft specific to that industry and similar to the FTC’s category: the Identity Theft Assistance Center defines identity theft as either “account takeover” or the creation of a “fraudulent account.” Account takeover—what the present study calls “account hijacking”—is further defined as the “assumption of a customer’s identity on a valid existing account.”

²⁹ ITAC (2004). See Article I, 19.