BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Would the Phishers get Hooked?

Abu Bakar Munir
Associate Professor, Faculty of Law, University of Malaya, Kuala Lumpur, Malaysia.
Email: abubmunir@yahoo.com
Siti Hajar Mohd. Yasin,
Faculty of Law, University Technology MARA, Shah Alam, Selangor, Malaysia.
Email: smohdyasin@yahoo.com

1. Introduction

Phishing and identity theft is emerging as one of the crimes of the 21st century. It is one of the fastest growing forms of Internet fraud. According to the U.S Federal Bureau of Investigation, phishing has become the hottest, and most troubling, new scam on the Internet. Credible estimates of the direct financial losses due to phishing alone exceed a billion dollars per year.[1] Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions.[2] According to the Anti-phishing Working Group (APWG), in January 2007 alone, it received 29,930 unique phishing reports – the highest recorded number. There are 27,221 phishing websites and 135 brands were hijacked in that month.[3] In the U.S, it was estimated that between May 2004 and May 2005, 1.2 million Internet users were victims of phishing, totalling approximately USD 929 million. Meanwhile, in the U.K, losses from phishing almost doubled to 23.2 million pounds in 2005, from 12.2 million pounds in 2004.[4] It is a multimillion pound problem. The BBC News on 13 December 2006 reported that the UK has seen an 8,000 percent increase in fake internet banking scams in the past two years.[5]

Banks and financial institutions, around the world, are the prime target. They have been and they will be.[6] The list of phishing attacks in 2003 and 2004 reads like a "Who's Who," including the Bank of America, Bank One, Citizens Bank, U.S Bank, Sun Trust, MBNA, Wells Fargo, and Visa, to name a few.[7] Phishing attacks have become a sobering reminder of the vulnerability of the Internet banking. Trust in online payment systems and the ability of financial institutions to mitigate fraud are diminished by successful attacks. The magnitude of the problem has prompted the Australian Prudential Regulation Authority (APRA) to issue an advice entitled "Emerging

---

[1] *See* the Joint Report of the US Department of Homeland Security-SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, *The Crimeware Landscape: Malware*, *Phishing, Identity Theft and Beyond*, (October 2006), at 4.
[2] Ibid.
[3] See the Anti-Phishing Working Group, "August Phishing Trends Report" , available at http://www.antiphishing.org/reports/apwg_report_january_2007.pdf
[4] According to the U.K Home Office Identity Fraud Steering Committee, a collaboration between the U.K financial bodies, government and the police to combat the threat of identity theft, the latest estimate is that identity fraud costs the U.K economy 1.7 billion pounds. Available at http://www.identitytheft.org.uk/
[5] BBC News, "Online Banking Fraud 'up 8,000%' ", available at http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/61775.
[6] The 2006 Global Security Survey by Deloitte finds that the threat that respondents most anticipated over the coming years was phishing and pharming. The APWG in its January 2007 report states that financial services continue to be the most targeted sector at 88.9 percent of attacks in the month of January, *supra* n. 3.
[7] *See* Frederick W. Stakelbeck Jr, "Phishing: A Growing Threats to Financial Institutions and E-Commerce", at 2.

Threats to Internet Banking" on 26 August 2004.[8] As Avivah Litan, Vice President and Research Director of Gartner Inc., puts it, "The whole promise of e-commerce-lower costs, increased revenue and quicker launches of marketing campaigns-all goes out the window if consumers cannot trust email communications."[9]

2. From AOL To Tsunami and From Malaysia To America

Phishing refers to luring techniques used by identity thieves to fish for personal information in a pond of unsuspecting Internet users.[10] The U.K 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. [11] The U.S Department of Justice defines it 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."[12] The APWG defines phishing as the use of spoofed emails and fraudulent web sites to fool a recipient into divulging personal financial data such as credit card numbers, account usernames and passwords, and social security numbers.[13]

Phishing, also known as "brand spoofing" or "carding", is 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.[14] "Ph" is a common hacker replacement for "f", and is a nod to the original form of hacking, known as "phreaking". [15] 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.[16]

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 U.S, U.K, Australia, Germany, and in other parts of the globe have been hit by phishing attacks. The FSA in its 2004 report states, "Phishing attacks aimed at identity theft are an increasing financial crime risk. Firm cannot afford to be complacent in their defence strategy to protect themselves and their customers from the threat of such fraudsters."[17] It is not only banks and financial institutions that are coming under attack from online cyber crooks. AT&T, AOL, eBay, Paypal, Microsoft, Yahoo,

---

[8] Australian Prudential Regulation Authority, *Emerging Threats to Internet Banking*, 26 August 2004.
[9] Alice Dragoon, "Fighting Phish, Fakes, and Frauds," CIO, September 22, 2004.
[10] *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*, October 2006, 3.
[11] Financial Services Authority, Countering Financial Crime Risks in Information Security: Financial Crime Sector Report, (2004), at 12
[12] United States Department of Justice, Special Report on Phishing (2004), p.3, available at http://www.usdoj.gov/criminal/fraud/Phishing.pdf
[13] The Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of Email Spoofing Scams*, (2003), at 3.
[14] Ibid
[15] Ibid

[16] Ibid
[17] Supra n. 11, at 4.

the FDIC, the FBI, IRS, Monetary Authority of Singapore (MAS)[18] and even the Tsunami charity organisation[19] have all been the victims of phishing assaults. The entire world is a pond for phishers. No one, large or small, anywhere, is immune. In fact, the U.S military has also become a favourite target of phishers.[20]

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.[21] 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.[22] 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".[23] 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.[24] This is reiterated by the Deputy Prime Minister, when he reminds the banks to enhance the security of Internet banking services.[25]

3. Techniques and Variants of Phishing

Phishing is a particularly invidious attack on the Internet community because it almost always involves two separate acts of fraud.[26] The phisher first "steals" the identity of the business it is personating and then acquires the personal information of the unwitting customers who fall for the impersonation.[27] This has led commentators to refer to phishing as a "two-fold scam" and a "cybercrime double play".[28] Phishing involves sending customers a seemingly legitimate email request for account information, often under the guise of asking the customer to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the email, the perpetrator uses various means to convince customers that they are receiving a legitimate message from someone whom the customer may already be doing business with, such as a bank.[29]

Techniques such as a false "from" address or the use of seemingly legitimate bank logos, web links, and graphics may be employed to mislead the customer. After gaining the customer's trust, the perpetrator attempts to convince the customer to provide personal information and provides one or more methods for the customer to communicate that information back. For example, the email might include a link to the perpetrator's web site that contains a form for entering personal information.[30] Like the email, the web site is designed to trick the customer into believing that it

---

[18] The MAS has issued Public Statement on Internet Security on 28 July 2006 indicating that it has become the target of the phishers, Available at http://www.mas.gov.sg/masmcm/bin/ptlPublic_Statement_on_Iternet_Security.htm

[19] In January 2005, Mathew Schmeider was charged in the U.S District Court for the Western District of Pennsylvania for sending more than 80,000 emails purporting to be from a charity appealing for funds for the victim of the Asian tsunami.

[20] Supra n. 7.

[21] See Utusan Malaysia 10 October 2006.

[22] Theedgeasia.com, available at http://www.theedgedaily.com/cms/contentPrint.jsp?id=om.tms.cms.article.rticle_4216

[23] Ibid

[24] Utusan Malaysia, 12 October 2006.

[25] Ibid.

[26] *See* Robert Louis B. Stevenson, "Plugging the Phishing Hole: Legislation versus Technology" (2005) Duke L. & Tech. Rev. 2.

[27] Ibid.

[28] Ibid.

[29] Comptroller of the Currency Administrator of National Banks, OCC Alert 2003-11.

[30] Ibid.

belongs to the bank. Alternatively, the email might simply include an embedded form for the customer to complete.[31]

3.1. Classic/Unique Attacks

Under this method, it begins with the phisher sends spam with bait. Most often, the bait is an email claiming to be from a trusted organisation, such as a bank or an online retailer. The email often claims that the consumer must urgently take action, or else bad thing would occur such as the closure of the account, for example. This most common way, also known as "dragnet method" or "deceptive phishing", is like a fisherman casting a large net to catch as many fish as possible. It is designed to elicit responses from unsuspecting email recipients. The next step is that the email provider delivers bait to consumer. Next, the user reads bait. A user might respond directly to the email, shown as "user enters info". More often, the user clicks on spoofed link.[32]This link is typically to a web site controlled by the phisher. The web site is designed to seem like the site of the trusted company. The consumer then enters personal information, such as account number, password, or username for the Internet banking. Once this is done by the consumer, the phisher has all the information, which allows the phisher to impersonate the victim to transfer funds from the victim's account, or purchase merchandise, etc.

This is the most successful phishing attacks to date; initiated by emails. However, the phisher has many other nefarious ways to entice the victims into surrendering confidential information.[33] The phisher has also been able to convince the email recipient to have believed that their banking information has been used by someone else to purchase unauthorised services.[34] The victim would then attempt to contact the email sender to inform them of the mistake and cancel the transaction. Depending upon the specifics of the scam, the phisher would ask (or provide an online "secure" web page) for the recipient to type-in their confidential details, to reverse the transaction -thereby verifying the live email address and also capturing enough information to complete a real transaction.[35]

3.2 Spear Phishing

Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack.[36] Spear phishers send spurious e-mails that appear genuine to a specifically identified group of Internet users such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website.[37] Much like a standard phishing e-mail, the message appears to come from a trusted source, such as employer or a colleague who would be likely to send e-mail message to everyone or a select group in the company.[38] Because it comes from a known and trusted source, the request for valuable data such as user names or passwords may appear more plausible.[39]

3.3 Vishing

"Vishing" or "voice phishing" is relatively new tactic that phishers adapted to fish in the ocean of the Internet. This has been described as follows; "Vishing can work in two different ways. In one

---

[31] Ibid.
[32] U.S National Consumers League, A Call for Action: Report from the National Consumers League Anti-Phishing Retreat (March 2006), Part One, at 5.
[33] *See* NGS/NISR, "The Phishing Guide: Understanding & Preventing Phishing Attacks", at 5.
[34] Ibid.
[35] Ibid.
[36] Supr*a* n. 10 at 8.
[37] Ibid.
[38] Ibid.
[39] Ibid.
.

version of the scam, the consumer receives an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and then prompted to "log-in" using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account."[40]

Vishing operate slightly differently. Rather than asking the receivers to reply by clicking on a link, the "visher" ask the receivers of the e-mail to call a number and provide confidential details over the phone. Victims call the number in the mistaken belief it belongs to their bank or credit card company. Instead, they are connected to a Voice over Internet Protocol (VoIP) phone that can recognize, and record, telephone keystrokes.[41]

3.4 Pharming

The U.S Federal Deposit Insurance Corporation (FDIC) describes pharming as the practice of redirecting Internet domain name requests to false websites in order to capture personal information, which may later be used to commit fraud and identity theft. It is the redirection of an individual to an illegitimate website through technical means.[42]

Pharming, like other types of phishing, aims to gather personal information from the unsuspecting victims; the difference is that pharming does not rely on email solicitation.
Instead, this attack method redirects the victims to a malicious website. Chris Risley said, "Phishing is to pharming what a guy with a rod and a reel is to a Russian trawler. Phishers have to approach their targets one by one. Pharmers can scoop up many victims in a single pass."[43] Another commentator, distinguishing pharming from phishing, states, "Phishing is throwing the bait out and hoping to get a bite. Pharming is planting the seeds and not trusting to chance."[44]

Pharming can occur in four different ways. First, static domain name spoofing-the pharming attempts to take advantage of slight misspellings in the domain names to trick users into inadvertently visiting the pharmer's web site. Second, malicious software (malware) -viruses and Trojans on a consumer's personal computer may intercept the user's request to visit a particular site and redirect the user to the site that the pharmer has set up. Thirdly, domain hijacking -a hacker may steal or hijack a company's legitimate web site, allowing the hacker to redirect all legitimate traffic to an illegitimate site.[45] Fourthly, domain name server (DNS) poisoning - when a user types a name into the web browser's address bar, a Domain Name System server reads the name, finds the corresponding numeric address and directs the user to the official website. In a DNS poisoning scheme, a hacker will alter a company's IP address on a domain server so that when a user enters the correct web address, the server will direct the user to a different address that contains a bogus website, built to steal passwords and other data.

3.5 Man-in-the-middle Attacks

A man-in-the-middle (MiM) attack is a form of phishing in which the phisher positions himself between two communicating parties, the user and the legitimate site, and gleans information to which he should not have access. Messages intended for the legitimate site are passed to the

---

[40] Ibid, 10.
[41] *See* Privacy Commissioner of Canada, "Recognizing Threats to Personal Data: Four Ways That Personal Data Gets Hijacked Online', p 3. Available at http://www.privcom.gc.ca/id/phishing_e.asp
[42] Federal Deposit Insurance Corporation, "Guidance on How Financial Institutions Can Protect Against Pharming Attacks," July 18, 2005, at 1.
[43] Cited in Michelle Delio, "Pharming Out-Scams Phishing", Wired News, available at http://www.wired.com/news/infostructure/1,66853-1.html
[44] Scott Chasin, cited in William Jackson, "Is a New ID Theft Scam in the Wings?", GCN, available at http://www.gcn.com/online/vo11-no1/34815-1.html
[45] *See* FDIC, supra n. 42.

attacker instead, who saves valuable information, passes the messages to the legitimate site, and forwards the responses back to the user.[46]Man-in-the-middle attacks are difficult for user to detect, because the site will work properly and there may be no external indication that anything is wrong.[47] Man-in-the-middle attacks may be performed using many different types of phishing. Some forms of phishing are inherently man-in-the-middle attacks. However, man-in-the-middle attacks may be used with many other types of phishing, including DNS-based phishing and deception-based phishing.[48]

4. Why Phishing Succeeds and Phishers are Rarely Caught

4.1 Single-factor Authentication

The current single-factor authentication of customers, which typically rely on shared secret of passwords and user ID are more susceptible to phishing schemes rather stronger authentication methods. The U.S Federal Deposit Insurance Corporation (FDIC) in its 2004 report, states:[49]

> Major reasons why phishing and other types of attacks have been used more and more, and with growing success, to perpetrate identity theft, particularly account hijacking [is that] the user authentication by the financial services industry for remote customer is insufficiently strong.

The FDIC was quite blunt on this issue, noting that "almost all phishing scams in use today could be thwarted by the use of two-factor authentication".[50] The U.S Federal Financial Institutions Examination Council (FFIEC) seems to have the same view. The FFIEC states, "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties…Financial institutions offering Internet- based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services…Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation".[51] The FFIEC further suggested that where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.[52]

The FDIC, in its 2005 report, which supplements the 2004 report, agrees that the two-factor authentication should not be considered a panacea for the problem of account hijacking and that a one-size-fits-all solution will not work. The FDIC, however, states, "The Study suggested that two-factor authentication will reduce the risk of account hijacking, not that it will solve the account-hijacking problem; nor did the Study suggest that two-factor authentication cannot be circumvented in certain circumstances. The FDIC Study stated only that two-factor authentication *can have a substantial positive effect* in reducing the incidence of account hijacking".[53] As a result, on October 13, 2005, the U.S Federal Reserve Board sent a letter to all the banks reinforcing on the need for the financial institutions to use the FFIEC report[54] as the guidance

---

[46] Supra n. 1 at 14.
[47] Aaron Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", (October 3, 2005), at 11.
[48] Ibid.
[49] Federal Deposit Insurance Corporation (FDIC), "Putting an End to Account-Hijacking Identity Theft", December 14, 2004, at p. 38, available at www.fdic.gov/consumers/consumeridtheftstudy/identity_theft.pdf.
[50] Ibid, p26.
[51] Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment" (2001), 1.
[52] Financial institutions are expected to come into compliance with this guidance by end of 2006.
[53] Federal Deposit Insurance Corporation, "Putting an End to Account-Hijacking Identity Theft: Study Supplement", June 17, 2005, 9.
[54] Supra n. 51.

when evaluating and implementing authentication systems and practices. The Federal Reserve informed the banks that they have until year- end 2006 to conform to authentication guidance.[55]

Thus, in developing a security programme that addresses the threat of phishing, it may be important to consider whether current authentication methods facilitate the success of a phishing attack.[56] For example, the use of IDs and password to authenticate customers means that a simple compromise of this information allows an impostor to access a customer's account. The mere possession of that information will allow complete access to the customer's account. With the advent of phishing, this may be a significant potential vulnerability.[57] As Ken Young puts it, "…any system that relies on a single unchanging password is inherently insecure".[58]

The authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrent.[59] There is, of course, no limit to the "types" of information that a phishing attack can seek to elicit from the targeted individuals. But the "value" of that information is sometimes determined by the spoofed company. Reducing the value of that information reduces both the incentive to engage in phishing conduct and the likelihood that significant damages will result. It may also eliminate a significant point of vulnerability.[60] For example, changing the company's security procedures so that two factor authentication is required to access online customer accounts (e.g., a password, ID plus a physical token) reduces the value of customer passwords obtained via phishing attacks. A customer may still be tricked into disclosing his password during a phishing attack, but it is no longer sufficient to gain access to his account, as something else (e.g., a token) that cannot be acquired via a phishing attack is also required.[61]

The US FDIC 2004 report states, "Two-factor authentication has the potential to eliminate, or significantly reduce, account hijacking….Two-factor authentication is significantly more secure than single-factor authentication because compromise of one factor would not be enough to permit fraudster to access the system…"[62] In the similar vein, the Australian Securities & Investments Commission states:[63]

> The use of two or more factors of authentication-such as a combination of something the user knows (a password) with either something the user has (a token), or something the user is (a biometric indicator)-is generally regarded as providing a significantly higher level of security than single factor authentication. On the other hand, using additional single factor authentication, such as requiring the user to enter more than one piece of secret information before the transaction can proceed will also enhance online security.

Realising its importance, the regulatory authorities in the U.S, Singapore and Hong Kong require banks and financial institutions to implement the two-factor authentication for Internet banking

---

[55] Federal Reserve Board, Supervisory Letter SR 05-19 on Interagency Guidance on Authentication in an Internet Banking Environment, available at http://www.federalreserve.gov/boarddocs/srletters/2005/sr0519.htm

[56] See Thomas J. Smedinghoff, "Phishing: The Legal Challenges for Business", World Internet Law Report, Vol. 5, No. 12, December 2004, 3.

[57] Ibid.

[58] Ken Young, "Phishing Phobia" Guardian, available at http://money.guardian.co.uk/print/0,,5064989-111609,00.html

[59] Supra n. 51 at 3.

[60] Supra n. 53.

[61] Ibid.

[62] FDIC, supra n.53 at 3-4.

[63] *See* the Australian Securities & Investments Commission (ASIC), "Reviewing the EFT Code: ASIC Consultation Paper" (January 2007), 26.

services. The Monetary Authority of Singapore (MAS) in its Circular of 25 November 2005 states:[64]

> Given the surge in security incidents involving the capture or misappropriation of customer PINs by cyber hackers, criminals and terrorists, there are serious doubts about the security of single-factor PINs.

To further enhance Internet banking security, MAS expects banks to implement two-factor authentication at login for all types of Internet banking systems by December 2006.

In February 2004, the Hong Kong Monetary Authority (HKMA) issued a guidance note on Supervision of Electronic banking which suggested, *inter alia*, that banks should employ stronger customer authentication for transactions with higher risk. The E-banking Working Group of the Hong Kong Association of Banks has reached a general consensus that, as minimum standard, banks should offer two-factor authentication for high-risk transactions to all retail Internet banking customers as an option. In June, the HKMA endorses the group's consensus and recommend banks to adopt the minimum standard. The HKMA expects banks to complete the implementation of two-factor authentication within one year from the date of the Circular.[65] The Australia's authority, APRA, too, strongly encourages the adoption of two-factor authentication on an industry-wide basis.[66]

The financial institutions in the U.K have acknowledged that two-factor authentication can be part of the solution to the problem of phishing. The interview conducted by Deloitte on Association for Program Administrators of CSTEP and STEP (APACS) (UK's payments association), the FSA and the leading financial services institutions headquartered in the UK finds, "the use of two-factor authentication was selected as the most popular technology to address identity theft. Some Chief Information Security Officers interviewed saw this as the inevitable standard for the future; "Two-factor authentication will become an industry standard, both for the investment banking sector as well as retail banking."[67] In 2005, the APACS issued this statement, "In view of the growing incidence of Trojans and phishing attacks directed at Internet users, banks are recommended to move towards stronger authentication for online banking customers".[68] The FSA, however, is sending a confusing signal. In its 2006 Financial Risk Outlook, the regulatory authority states:[69]

> With phishing losses relatively low, providing direct security measures, such as anti-virus software or two-factor authentication, *may not yet be cost effective for banks*. Firms may choose to provide such products as a way to maintain confidence in online banking or may market them as unique selling points. In the longer term firms may provide these security features with conditions attached or provide discounted fees for 'careful' customers as a way to encourage consumers to protect themselves against fraud.

4.2 Human Factor

Phishing attacks rely upon a mix of technical deceit and social engineering practices. Social engineering is the art or practice of manipulating people in order to obtain confidential or sensitive data.[70] Social engineering uses influence and persuasion to deceive people by convincing them

---

[64] MAS, Circular No. SRD TR 02/2005.
[65] HKMA, Circular 23 June 2004, *Strengthening Security Controls for Internet Banking Services*.
[66] Supra n. 8.
[67] Deloitte, "Identity theft- a view from the financial services industry", at 6.
[68] *See* OUT-LAW News, 19/10/2005, "UK Law Will Demand Better Authentication for Online Banking", available at http://www.out-law/page-6241
[69] Financial Service Authority*, Financial Risk Outlook 2006*, at 92.
[70] *See* Privacy Commissioner of Canada, "March is Fraud Prevention Month", available at http://www.privcom.gc.ca/id/phishing_e.asp.

that the social engineer is some he isn't, thus manipulating them into divulging personal information.[71] In majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.[72] Communication channels such as email, web pages, IRC and instant messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe.[73] To date, the most successful phishing attacks have been initiated by email- where the phisher impersonates the sending authority.[74]

According to 2003 study conducted by Gartner, 57 million U.S Internet users have identified the receipt of email linked to phishing scams, and about 1.7 million of them are thought to have succumbed to the convincing attacks and tricked them into divulging personal information. Studies by the APWG have concluded that phishers are likely to succeed with as much as 5 per cent of all message recipients. The APWG states, "Data suggests that phishers are able to convince up to 5 per cent of recipients to respond to them".[75] By contrast, the estimated response rate for regular spam is 0.01%.[76] As the FSA puts it, "Because 'phishing' scams are sent to thousands of people, even a small success rate in obtaining a person's online account and personal details encourages more 'phishing' attacks".[77]

A study by Rachna Dhamija, J.D. Tygar and Marti Hearst finds that: (1) good phishing websites fooled 90 per cent of participants; (2) existing anti-phishing browsing cues are infective. Twenty-three per cent of participants did not look at the address bar, status bar, or the security indicators.[78] The study identifies three main factors that contribute to the success of a phishing attack; lack of knowledge, visual deception and bounded attention. On the lack of knowledge, these researchers from Harvard University and University of California Berkeley state that, "Many users lack underlying knowledge of how operating systems, applications, email and the web work and how to distinguish among these. Phishing sites exploit this lack of knowledge in several ways".[79] Phishers use visual deception tricks to mimic legitimate text, images and windows. Even users with knowledge may be deceived by the deception tricks. Even if users have the knowledge, and can detect visual deception, they may still be deceived if they fail to notice security indicators.[80]

The Ponemon Institute conducted a survey in the U.S in the summer of 2004, at a time when phishing attacks were running at less than half the rate of October 2005. This survey had the following major findings: (1) most people are vulnerable to spoofing. Over 60 per cent of online users had inadvertently visited a fake or spoofed site; (2) many people are tricked into providing personal information such as checking account information or social security numbers. Over 15 per cent of respondents admitted to having provided personal data to a spoofed site.[81] In this respect, consumer education is crucially important. Banks cannot afford to be complacent in their defence strategy to protect themselves and their customers from the threat of the criminals. Banks' education of consumers plays an important role in preventing phishing attacks. Education and even greater education is needed. The ultimate aim of phishing attacks is to trick the customer into voluntarily providing information. Thus, a key defensive measure is to educate customers so that they will be on guard for these attacks, recognised them when they occur, and

---

[71] Ibid.
[72] *See* NGSSoftware Insight Security Research, "The Phishing Guide: Understanding & Preventing Phishing Attacks", at 5.
[73] Ibid.
[74] Ibid.
[75] Anti-Phishing Working Group, Phishing Activity Trends Report, January 2005, available at http://antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf
[76] Laura Sullivan cited in Robert Louis B. Stevenson, supra n. 27 at 2.
[77] FSA, supra n. 11 at 11.
[78] Rachna Dhamija, J.D. Tygar and Marti Hearst, "Why Phishing Works", (2006), at p 1.
[79] Ibid, 2.
[80] Ibid, 3.
[81] Cited in the U.S National Consumers League Report, *supra* note 33, *at*. 10.

not to give the information that these attacks seek to obtain. Simply put, the purpose is to avoid the customers from being tricked or fooled by the criminals.

In its 2004 report, the FSA states, "Phishing attacks are increasing and will probably grow to include the smaller banks as well as the major ones. Although losses to date are low, effective *customer education and good corporate communication* is needed to minimise loss".[82] The need for greater consumer education results from the large and growing nature of the phishing problem. The number of phishing attacks has arisen rapidly. The nature of such attacks also keeps shifting. Baits emails have become far more convincing in appearance. And the bad grammar and English usage of earlier attacks -helpful hints to consumers that something was amiss -are less common.[83]

Anything that will reduce the likelihood that a customer will provide information to a phisher is helpful. But it is also important to understand that customer education is unlikely to be a complete solution to the problem. The APWG has noted, "A solution to phishing cannot simply rely on millions of users being trained to check the details of email routing headers and to scrutinise the minutia of Internet URL web links to ensure that email communications are genuine, and not from a phisher. In fact, with the URL masking vulnerability in the Internet Explorer Web browser that was disclosed on Dec 10, 2003, even the URL web address cannot be relied upon to be correct".[84]

The next question to be asked is why phisher are rarely caught. Special Agent John Curran, Supervisory Special Agent with the FBI's Internet Crime Compliant Center, commented about the elusiveness and unpredictable nature of phishing attacks, "I've been to meetings of industry experts where it's taken them minutes of studying an email from a phisher site to determine that it's not the actual site. You can't expect the average person surfing the Internet or doing online banking to be suspicious of an e-mail that convincing."[85]

Besides, the fraud can be perpetrated very quickly, and afterward, the phishers can "vanish" into cyberspace. The phony websites typically migrate from one server to another very rapidly -in an effort to stay a step ahead of ISPs and law enforcement.[86] In one scam documented by the APWG, the perpetrators operated a spoofed web page on seven different servers over a period of just 12 days. And the servers were all over the globe-including four in Korea, two at the American ISPs, and one in Uruguay.[87] According to the APWG, the average phishing web site is online for only about 54 hours. Some sites, however, have been able to remain online for more than two weeks before being shut down or abandoned.[88] The 2005 APWG's report finds that the average life span for phishing sites, measured by how long they continue to respond with content, is 5.8 days. Accordingly, law enforcement personnel have, on average, 5.8 days from the time the phisher first initiates the scam to track him down and compile sufficient evidence to bring charges.

5. Legislative Bait

5.1 Existing U.S Laws and the Enforcement

The U.S Department of Justice states that, "because they use false and fraudulent statements to deceive people into disclosing valuable personal data, phishing schemes may violate a variety of federal criminal statutes. Existing legislation, such as, Identity Theft Penalty Enhancement Act,

---

[82] FSA, *supra* note 10, *at*. 14.
[83] *Supra* note 33 *at*.14.
[84] APWG, "Proposed Solutions to Address the Threat of Email Spoofing Scams," December 2003, *at p*. 4.
[85] Cited in Frederick W. Stakelbeck, Jr, *supra* note 7.
[86] Ramasastry: Hooking Phisherman, CNN.com, available at http://cnn.com.printthis.clickability.com/pt/cpt?action=cpt&title=CNN.com+-+Ramasatr...
[87] *Id*.
[88] *Id*.

Identity Theft and Assumption Deterrence Act, Fair and Accurate Credit Transactions Act, USA PATRIOT Act, Gramm-Leach Bliley Act, CAN-SPAM Act, Wire Fraud Act, Credit-Card Fraud Act, Bank Fraud Act and Computer Fraud Act - all contain provisions related to identity theft and/or fraud.

The Identity Theft Penalty Enhancement Act which was signed by President Bust in July 2004 establishes a new crime of "aggravated identity theft." The new law carries mandatory minimum sentences for using a stolen identity to commit crimes such as phishing. In signing the law, President Bush said, "Identity theft undermines the basic trust on which our economy depends." Committing identity theft while engaged in major criminal offences such as terrorism will carry an extra, automatic prison term of up to five years. This law supplements the Identity Theft and Assumption Deterrence Act 1998, which makes it a federal crime when "someone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.

In many phishing schemes, the participants in the scheme may be committing identity theft, for examples, (18 U.S.C. S1028 (a) (7)), Wire Fraud (18 U.S.C. S.1343), Credit-Card Fraud (18 U.S.C. S.1029), Bank Fraud (18 U.S.C. S 1344), Computer Fraud (18 U.S.C. S 1030(a)(4)), and the newly enacted criminal offences in the CAN-SPAM Act (18 U.S.C. S 1037). When a phishing scheme also uses computer viruses or worms, participants in the scheme may also violate other provisions of the computer fraud and abuse statute relating to damage to computer systems. Finally, phishing may violate various state statutes on fraud and identity theft".[89] There have been some prosecutions under these federal legislations.[90] Some of the accused pleaded guilty to the charge. Thus, existing federal laws do criniminalise phishing-but mainly after the damage is done, when a consumer has already been defrauded as a result of phishing.[91] As explained by a member of Senator Leahy's staff:

> [P]hishing scammers already violate a host of identity theft and fraud laws, but prosecuting them under those statutes can be challenging…To charge scammers now, law enforces need to prove that a victim suffered measurable losses. By the time they do that…the scammer has often disappeared.[92]

Section 1028(a)(7) provides that it is unlawful for anyone who knowingly transfers or uses, without lawful authority, a means of identification of another person with intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. While the wire fraud act in section 1343 prohibits "whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretences, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

In *Forcellina*, a husband accessed chat rooms, used a device to capture screen names of chat room participants and then sent emails pretending to be the ISP requiring correct billing information, including current credit-card number. He used the credit-card numbers and other personal data to arrange for wire transfers of funds via Western Union. The husband and his wife were charged with conspiracy to commit access device fraud. In *Hill* the defendant operated AOL and PayPal phishing schemes to fraudulently obtain credit-card numbers to purchase goods and

---

[89] Department of Justice, Special Report on "Phishing".
[90] *See,* e.g., United States *v. Forcellina* (D. Conn., sentenced April 30 and June 18, 2004), United States v. Hill, United States v. Carr (E.D. Va. 2003), United States v. Guevara (W.D. Wash. 2003), FTC v. ---- (C.D. Cal. 2003), United States v. Gebrezihir (S.D. N. Y. 2003), United States v. Kalin (D.N.J., Nov. 2003
[91] *Supra* note 86.
[92] David McGuire, "Senate Bill Targets Phishers", Newsbytes News Network, July 12, 2004.

services costing more than USD 47,000. The defendant pleaded guilty in February 2004 to possession and use of access devices and was sentenced to 46 months imprisonment. In *Carr*, Helen Carr was accused of sending fake email messages to AOL customers in the U.S and several foreign countries. The emails advised the customers that they must update their credit card and personal information on file with AOL to maintain their accounts. She was found guilty of conspiracy to possess unauthorised access devices and sentenced in January 2004 to 46 months imprisonment.

In *Guevara* a young man created false email accounts with Hotmail and an unauthorised website with the address www.msnbilling.com through Yahoo!. He then sent MSN customers email messages, purporting to come from MSN, which directed customers to the fraudulent website and asked them to verify their accounts by providing name, MSN account, and credit-card data. The website automatically forwarded each customer's data to one of the defendant's false Hotmail accounts. He pleaded guilty in September 2003 to wire fraud and was sentenced to 5 years probation and 6 months home confinement.

In *Kalin*, the defendant allegedly registered four websites with domain name deceptively similar to the website operated by DealerTrack, Inc. Dealer Track provides services via Internet to auto dealerships located throughout the United States, including dealers' ordering credit reports on prospective automobile buyers. The defendant's website was designed to be practically identical to the main page of DealerTrack. He then allegedly got a number of dealership employees mistakenly to enter usernames and passwords at his sites and consequently managed to obtain unauthorised access to DealerTrack for personal data.

5.2 New State Laws

Several states in the U.S have enacted specific legislation to combat phishing. The State of California was taking the lead when she passed Anti-Phishing Act in 2005. Under the California's Act, it is illegal for any person, through the Internet or other electronic means to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the approval or authority of the business. The State of Connecticut "prohibits using Internet or an email message to solicit or induce another to provide identifying information by pretending to be an online Internet business and provides civil and criminal penalties".

The Anti-Phishing Act of Florida prohibits inducing, requesting, or soliciting identifying information with an intent to engage in conduct involving the fraudulent use or possession of another person's identifying information. The Act also prohibits the fraudulent use of a web page or Internet domain name to obtain personal identifying information from a resident of Florida; prohibits the fraudulent use of electronic mail to obtain personal identifying information from a resident of Florida. The Act provides a civil action for injunction and damages.

In 2006, Louisiana, New Jersey, New York, Oklahoma, Tennesse have passed state anti-phishing legislation. Many states are considering having similar one. The Tennesse Anti-Phishing Act of 2006 penalises persons, who, without authorisation or permission of subject of identifying information, obtain, record, access or distribute identifying information of another person through use of Internet, email or wireless communication.

There are two common features of the anti-phishing legislation. Firstly, they criminalise the bait. They make it illegal to knowingly send out spoofed email that links to sham websites with the intention of committing a crime. Secondly, they criminalise the sham websites that are the true scene of both types of crime.

It is interesting to note, as indicated above, the law also provide for civil penalties against phishers. Individuals who are victims of identity theft have a cause of action against those who have violated the statute-the phishers. Perhaps, it is too early to assess the efficacy of these

legislations. However, some commentators have already voice scepticism about the ability of the law to phish the phishers. Camille Calman wrote; "Bills that define phishing and attempted phishing as crimes are good public relations moves for legislators, since they give an impression of government taking active steps to wipe out a dangerous new crime. But such legislation ignores the fact that phishing and attempted phishing are already crimes. Fraud and identity theft have never been legal activity; the only factor that makes phishing "new" is the particular electronic method used to con the target out of his or her personal information. By declaring that phishing is now a crime, legislators do little more than state the obvious. Such measures should not reassure consumers, since phishers often operate offshore and are not available for criminal prosecutions in state courts. Criminal penalties will have little deterrent effect if they cannot be enforced. As long as phishing remains a low-cost, low-risk crime, criminals will continue to phish".[93]

5.3 Proposed Federal Law

On February 28, 2005, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005 ("APA") in the United States Senate. The APA targets the entire scam process from the sending of the email to the creation of fraudulent website. As mentioned earlier, if passed, the APA will add two crimes to the current federal law. First, it would criminalise the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages. Second, it criminalises the sham websites.

In this respect, the APA criminalises the bait. This 'poisoned bait' approach criminalises the conduct engaged in before the actual commission of the fraud. It makes it illegal to knowingly send out spoofed email that links to false websites, with the intention of committing a crime.[94] It is also criminalises the operation of such websites that are locus of the wrong doing. This creates an opportunity to prosecute before the actual fraud takes place, not just to successful phishing occurrences.[95]

5.4 Phishing under the U.K Fraud Act

The Home Office acknowledges that fraud is a growing problem in the U.K. The Government has passed a new Fraud Act in November 2006 which will come into force in early 2007. The new law aims to close a number of loopholes in preceding anti-fraud legislation, which the Government said was unsuited to modern fraud. The Act seeks to simplify the criminal law by creating a general offence of fraud, which may be committed in three different ways. The Attorney General, Lord Goldsmith commented, "This reform is needed to enable prosecutors to get to grips with the increasing abuse of new technology, particularly in relation to fake credit cards scams and personal identity theft, which cost millions of pounds every year".[96] In the similar vein, the Home Office official said, "The introduction of a general fraud offence will improve the criminal law in a number of respects. It will simplify the law, making it clearer to juries and the general public as well as making the prosecution process more effective by providing a clear definition of fraud. Our aim is to encompass all forms of fraudulent conduct, with a law that is flexible enough to deal with developing technology, allowing us to bring more offenders to justice".[97]

---

[93] Camille Calman, "Bigger Phish to Fry: California's Anti-Phishing Statute and its Potential Imposition of Secondary Liability on Internet Service Providers", Richmond Journal of Law & Technology, Vol. XIII, Issue I, *at*. 3.

[94] Warren B. Chik, "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore", *at*. 16.

[95] *Id*.

[96] *See* finextra.com, "UK Government Cracks Down on Phishers", available at http://www.finextra.com/fullstory.asp?id=13735

[97] *See* ZDNet.co.uk, "Government Moves to Tackle Phishing", available at http://www.zdnet.co.uk/misc/print/0,000000169,39201079-39001093c,00.htm

Earlier, in its consultation paper the Home Office rejected calls for a specific offence to cover phishing, maintaining that this, "is an offence, or an attempted offence, of fraud under the current law" and that it would be caught by the proposed new offence created by the Bill. Section 1 of the Bill sets out a new general offence of fraud, the maximum penalty for which will be ten years' imprisonment and a fine. There will be three different ways of committing the new offence and these are set out in Sections 2, 3 and 4 of the Act. They are fraud: (1) by false representation (Section 2); (2) by failing to disclose information (Section 3); and (3) by abuse of position (Section 4).

Section 2 covers phishing. Under this section, it will be an offence for a person to commit fraud by making a false representation dishonestly. Section 2(2) defines a representation as being "false" if it is untrue or misleading and the person making it knows that it is, or might be, so. "Representation" is defined in Section 2(3) as any representation as to fact or law, including a representation as to a person's state of mind. The representation may be expressed or implied. Section 2 is drafted broadly so as to encompass fraudulent Internet and other activities such as phishing. The Act requires that the representation must be made dishonestly and it must be made with the intention of making a gain or causing loss or risk of loss to another, regardless of whether the gain or loss actually takes place. The prosecution will not have to show that actual gain or loss took place. There is no limitation on the way in which the words must be expressed and that it could therefore be written, spoken or posted on a website. The explanatory notes states," This offence would also be committed by someone who engages in phishing…."

Section 6 of the Fraud Act can be used against the phishers as well. This clause seeks to make it an offence, punishable by up to five years' imprisonment and a fine, for a person to have in his possession or under his control any article for use in the course of or in connection with any fraud. Under this clause, it is an offence for phishers to have in his possession or under his control any software or trojan to be used to intercept communication between parties to glean information which he should not have access. This is relevant in relation to pharming and man-in-the-middle-attack. As stated in the explanatory notes, the intention of section 6 is to cover a situation where the defendant had the article for the purpose of or with the intention that it be used in the course of or in connection with the offence, and that a general intention to commit fraud will suffice.

Another provision of the new law which is applicable to phishing is section 11. It is designed to make it an offence, punishable by up to five years imprisonment and a fine, for a person, by dishonest act, to obtain services for himself or another person, for which payment is required, with intent to avoid paying the full amount required. For a prosecution to succeed it will have to be proved that the person knew when he obtained the services that payment was required or that it might be. Deception is not required under this new offence. The explanatory notes comments that the new offence will be committed only where the dishonest act was done with the intention of avoiding the expected payment for the services concerned. The explanatory notes states:

> The offence is not inchoate; it requires the actual obtaining of the service. For example, data or software may be made available on the Internet to a certain category of person who has paid for access rights to that service. A person dishonestly using false credit card details or other false personal information to obtain the service would be committing an offence under this clause.

6. Conclusion

Phishing shows no sign of abating. It is, indeed, likely to continue in newer and more sophisticated forms. The continuing growth of phishing is a serious concern for the entire Internet community. It represents one aspect of the increasingly complex and converging security threats

facing businesses today. The effect and impact of phishing on businesses and Internet as an effective mechanism to do business is far-reaching. As Frederick W. Stakelbeck wrote:[98]

> From a risk assessment perspective, phishing attacks can create significant long-term pressures on financial institutions, which could permanently damage their reputation in the marketplace. If permitted to continue unabated, phishing has the potential to transform a dynamic conduit for legitimate commerce, the Internet, into an instrument of consumer scorn and scepticism.

Some governments and regulatory bodies have done or are doing their bit. Banks and financial institutions, more importantly, must do their parts.[99] A study by Next Generation Security, released in September 2004, found that 90 per cent of financial and commercial websites contained flaws that, if exploited, could result in successful phishing attacks. These include site configuration problems that would allow the redirection of information from a legitimate site to a fraudulent site.[100] Professor Bill Caelli, an Internet expert, is of the view that financial institutions have been lucky so far not to have suffered more serious attacks. He asserts, "IT risk assessment is generally outdated. Banks are underestimating the number of phishing attacks. A number of banks conducting online transactions are using insecure operating systems. We haven't had a massive attack yet. All I'm saying is that we have been warned."[101]

But not all is doom and gloom. In some parts of the world, steps have been taken in the areas of consumer education and in the improvement of technology available to detect and defeat phishing attacks.[102] However, not enough has been or being done in some countries.

---

[98] *Supra* note 7.

[99] A recent survey of U.S Internet users by the Ponemon Institute finds that over three-fifths of the survey respondents believed it "unacceptable" for a bank to not respond to phishing schemes that use the bank's identity as the means of gaining the victim's trust. Nearly 96 percent of the respondents said that banks need to use technology to provide protection to their banking customers. In other words, customers blame the banks, not just the criminals. See Gene J. Koprowski, "Phishing Liability Concerns Online Banks", E-Commerce Times, available at http://www.ecommercetimes.com/story/45890.html

[100] Cited in Frederick W. Stakelbeck, *supra* note 7 at p. 4.

[101] Andrew Colley, "Banks Dismissive of Phishing Losses," *ZDNET*, March 11, 2004.

[102] *Supra* note 7.