Chapter 4: Success Factors of Phishing

4.1 Introduction

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

4.2 Human Factor

Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized "lures." For instance, a phisher misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. In a study by Gartner, about 19% of all those surveyed reported having clicked on a link in a phishing email, and 3% admitted to giving up financial or personal information.[89]

According to Gunter Ollmann, Professional Services Director of NGS Software Ltd in his paper, "The Phishing Guide, Understanding and Preventing Phishing Attacks" [90] stated that in the majority of cases the Phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information. Communication channels such as email, web-pages, IRC and instant messaging services are popular. In all

[89] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer School of Informatics Indiana University, Bloomington, "Social Phishing", (2005) at p.1

[90] See NGSSoftware Insight Security Research, The Phishing Guide, Understanding and Preventing Phishing Attacks at p.5

cases the Phisher must impersonate a trusted source (e.g. the helpdesk of their bank, automated support response from their favourite online retailer, etc.) for the victim to believe.

To date, the most successful Phishing attacks have been initiated by email – where the Phisher impersonates the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos). For example, the victim receives an email supposedly from *support@mybank.com* (address is spoofed) with the subject line 'security update', requesting them to follow the URL *www.mybank-validate.info* (a domain name that belongs to the attacker – not the bank) and provide their banking PIN number.

However, the Phisher has many other nefarious methods of social engineering victims into surrendering confidential information. In the real example below, the email recipient is likely to have believed that their banking information has been used by someone else to purchase unauthorized services. 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 (such as address, credit card number and security code, etc.), to reverse the transaction – thereby verifying the live email address (and potentially selling this information on to other spammers) and also capturing enough information to complete a real transaction.

According to study conducted by Gartner Inc in 2003, 57 million of US Internet users have identified the receipt of email linked to phishing scams, and about 1.7 million of them are thought to have yielded to the convincing attacks and tricks them into divulging personal information. In addition, data analysts by the Anti Phishing Working Group have concluded that phishers are likely to succeed with as much as 5 percent of all message recipients to respond to them.[91]

According to Rachna Dhamija, J.D Tygar and Marti Hearst had tested hypotheses in a usability study which they showed 22 participants 20 web sites and asked them to determine which ones were fraudulent, and why. Their key findings are:

- Good phishing websites fooled 90% of participants.
- Existing anti-phishing browsing cues are ineffective. 23% of participants in our study did not look at the address bar, status bar, or the security indicators.
- On average, our participant group made mistakes on our test set 40% of the time.[92]
- Popup warnings about fraudulent certificates were ineffective: 15 out of 22 participants proceeded without hesitation when presented with warnings.
- Participants proved vulnerable across the board to phishing attacks. In our study, neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing.

The study identifies three main factors that contribute to the success of a phishing attack:-

Lack of Knowledge

a) Lack of computer system knowledge. Many users lack the 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. For example, some

[91] APWG, Phishing Activity Trends Report January 2005
[92] Rachna Dhamija, J.D Tygar and Marti Hearst, “Why Phishing Works”, (2006) at p.1

users do not understand the meaning or the syntax of domain names and cannot distinguish legitimate versus fraudulent URLs (e.g., they may think www.ebay-members-security.com belongs to www.ebay.com). Another attack strategy forges the email header; many users do not have the skills to distinguish forged from legitimate headers.

b) Lack of knowledge of security and security indicators.

Many users do not understand security indicators. For example, many users do not know that a closed padlock icon in the browser indicates that the page they are viewing was delivered securely by SSL. Even if they understand the meaning of that icon, users can be fooled by its placement within the body of a web page (this confusion is not aided by the fact that competing browsers use different icons and place them in different parts of their display). More generally, users may not be aware that padlock icons appear in the browser "chrome" (the interface constructed by the browser around a web page, e.g., toolbars, windows, address bar, status bar) only under specific conditions (i.e., when SSL is used), while icons in the content of the web page can be placed there arbitrarily by designers (or by phishers) to induce trust.[93]

Attackers can also exploit users' lack of understanding of the verification process for SSL certificates. Most users do not know how to check SSL certificates in the browser or understand the information presented in a certificate.

In one spoofing strategy, a rogue site displays a certificate authority's (CA) trust seal that links to a CA webpage. This webpage provides an English language description and verification of the legitimate site's certificate. Only the most informed and diligent users

[93] For user convenience, some legitimate organizations allow users to login from non-SSL pages. Although the user data may be transmitted securely, there is no visual cue in the browser to indicate if SSL is used for form submissions. To "remedy" this, designers resort to placing a padlock icon in the page content, a tactic that phishers also exploit.

would know to check that the URL of the originating site and the legitimate site described by the CA match.[94]

Visual Deception

Phishers use visual deception tricks to mimic legitimate text, images and windows. Even users with the knowledge described in (1) above may be deceived by these.

a) Visually deceptive text.

Users may be fooled by the syntax of a domain name in “typejacking” attacks, which substitute letters that may go unnoticed (e.g. www.paypai.com uses a lowercase “i” which looks similar to the letter “l”, and www.paypa1.com substitutes the number “1” for the letter “l”). Phishers have also taken advantage of non-printing characters and non-ASCII Unicode characters in domain names.

b) Images masking underlying text.

One common technique used by phishers is to use an image of a legitimate hyperlink. The image itself serves as a hyperlink to a different, rogue site.

c) Images mimicking windows.

Phishers use images in the content of a web page that mimic browser windows or or dialog windows. Because the image looks exactly like a real window, a user can be fooled unless he tries to move or resize the image.

d) Windows masking underlying windows.

A common phishing technique is to place an illegitimate browser window on top of, or next to, a legitimate window. If they have the same look and feel, users may mistakenly believe that both windows are from the same source, regardless of variations in address or security

[94] Ibid

indicators. In the worst case, a user may not even notice that a second window exists (browsers that allow borderless pop-up windows aggravate the problem).

e) Deceptive look and feel.

If images and logos are copied perfectly, sometimes the only cues that are available to the user are the tone of the language, misspellings or other signs of unprofessional design. If the phishing site closely mimics the target site, the only cue to the user might be the type and quantity of requested personal information.[95]

Bounded Attention

Even if users have the knowledge described in (1) above, and can detect visual deception described in (2) above they may still be deceived if they fail to notice security indicators (or their absence).

a) Lack of attention to security indicators.

Security is often a secondary goal. When users are focused on their primary tasks, they may not notice security indicators or read warning messages. The image-hyperlink spoof described in (2b) above would thwarted if user noticed the URL in the status bar did not match the hyperlink image, but this requires a high degree of attention. Users who know to look for an SSL closed-padlock icon may simply scan for the presence of a padlock icon regardless of position and thus be fooled by an icon appearing in the body of a web page.

b) Lack of attention to the absence of security indicators.

Users do not reliably notice the absence of a security indicator. The Firefox browser shows SSL protected pages with four indicators. It shows none of these indicators for pages not protected by SSL. Many users do not notice the absence of an indicator, and it is sometimes possible to insert a spoofed image of an indicator where one does not exist.[96]

[95] Ibid
[96] Ibid

A May 2005 consumer survey by First Data confirmed the widespread nature of the problem. It found that 43 percent of respondents had received a phishing contact, and of those, 5 percent (approximately 4.5 million people) provided the requested personal information. Nearly half of the phishing victims, 45 percent, reported that their information was used to make an unauthorized transaction, open an account, or commit another type of identity theft.[97]

Behind these raw numbers, the consumer experience of the Internet is being profoundly affected by phishing, identity theft, and other types of fraud. The Ponemon Institute National Consumers League conducted a survey 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:

• Most people are vulnerable to spoofing. Over 60 percent of online users had inadvertently visited a fake or spoofed site.

• Many people are tricked into providing sensitive personal information such as checking account information or Social Security numbers. Over 15 percent of respondents admitted to having provided personal data to a spoofed site.

• Most people expect organizations to do a better job in addressing phishing problems. A full 96 percent agreed with the statement that "the organization should install technology that allows customers to know the differences between authentic emails and Web sites from fake emails and spoofed Web sites."

• Economic loss from spoofing had touched only about 2 percent of respondents, with an average reported cost of $115. Extrapolated to the full U.S. population, the result would be direct monetary loss from phishing fraud of approximately $480 million[98]

[97] *Http://news.firstdata.com/media/ReleaseDetail.cfm?ReleaseID=163659.*
[98] US National Consumers League Report (2006) at p.10

Therefore, consumer education is deemed to be very important. According to Prof Abu Bakar Munir (UM)[99], banks cannot afford to be complacent in their defence strategy to protect themselves and their customers from the threat of the criminal. 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, recognized them when they occur, and not to give the information that these attacks seek to obtain. He also stressed that, the purpose is to avoid the customers from being tricked or fooled by the criminals.

But it is also important to understand that customer education is unlikely to be a complete solution to the problem. The Anti-Phishing Working Group 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"[100].

4.3 Technical Factor

Besides human factor, this chapter also will look into the technical aspect of the reason why phishing succeed. 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:[101]

[99] Abu Bakar Munir and Siti Hajar Mohd Yassin , "*Would the Phishers get hooked*?"(2007), at p.9
[100] APWG, "Proposed Solutions to Address the Threat of Email Spoofing Scams," December 2003, *at p*. 4.
[101] Federal Deposit Insurance Corporation (FDIC), "Putting an End to Account-Hijacking Identity Theft", December 14, 2004,

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.

Authentication is the means of verifying the identity of a person or entity. It can also be used to verify that information received has not been altered. Closely associated and often confused with authentication is authorization, which determines the level of rights and privileges available to the authenticated user. Tying authentication and authorization together is referred to as identity management.

Generally the way to authenticate the user is to have the user present some sort of credential to prove his or her identity. A credential is generally one or more of the following:[102]

- Something a person knows—most commonly a password. If the user types in the correct password, access is granted.
- Something a person has—most commonly a physical device referred to as a token. The user must physically connect the token to the computer in order to be granted access. Thus, tokens often require the user's computer to be outfitted with specific hardware to accept the token.
- Something a person is—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye.

This type of authentication is referred to as biometrics and often requires the installation of specific hardware on the system to be accessed.

Single-factor authentication involves the use of one of the three authentication credentials listed above, most commonly a password. Single-factor authentication is very common and

[102] Ibid

is the method used by the vast majority of financial institutions for granting customers access to Internet-banking applications and by the vast majority of businesses for granting employees access to computer networks. The main problem with single-factor authentication is that passwords, the most commonly used factor, are often easy to guess, steal, or crack, and once a password is compromised the thief has the same access rights as the legitimate user. In addition, the legitimate user may not even know that his or her password has been compromised, since usually no physical evidence of the compromise exists. [103]

The initial section of this study has documented the monetary damage that can be inflicted when passwords are compromised. The rise in account hijacking suggests that traditional single-factor authentication may not be adequate in today's online world.

Two-factor authentication has the potential to eliminate, or significantly reduce, account hijacking. Two-factor authentication uses two of the three types of credentials mentioned above (something a person knows or has or is) for establishing the user's identity. Two-factor authentication is most widely used today in connection with ATMs. To withdraw money from an ATM, the user must present both an ATM card (something the person has) and a password or PIN (something the person knows). A fraudster who succeeds in stealing just one or the other will not be able to pose as the legitimate account owner and access the ATM. Two-factor authentication can also involve the combination of a password (something a person knows) and a biometric (something a person is). Biometric authenticators (as well as tokens, which are something you have) are unique and not easily duplicated and can be disabled, so their ability to serve as an authentication device can be quickly revoked.[104] Two-factor authentication is significantly more secure than single-

[103] Ibid

[104] Rainbow Technologies (2002).

factor authentication because the compromise of one factor would not be enough to permit a fraudster to access the system and the additional factor (usually a token or biometric identifier) is extremely difficult to compromise. Almost all the phishing scams in use today could be thwarted by the use of two-factor authentication. Most two-factor authentication systems use shared secrets, tokens (USB token devices, smart cards, or password-generating tokens), or biometrics.

In addition, the FDIC in its supplements stated that two-factor authentication—a term that can encompass a wide variety of specific technologies—should not be considered a panacea for the problem of account hijacking and that a one-size-fits-all solution will not work. 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.[105]

The Federal Financial Institutions Examination Council also shared the same view like FDIC Study. 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. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk

[105] Federal Deposit Insurance Corporation, "Putting an End to Account-Hijacking Identity Theft: Study Supplement", June 17, 2005, 9

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.[106] 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 as the guidance 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[107]

Hence, 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.[108] 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.[109]

As Ken Young puts it,

"…any system that relies on a single unchanging password is inherently insecure".[110]

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. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something

[106] Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment" (2001), 1.

[107] 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

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

[109] Ibid

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

the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band" controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

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.[111] 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.

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

[111] Federal Deposit Insurance Corporation , "Putting an End to Account Hijacking Identity Theft; Study Supplement", June 17, 2005, 9

enough to permit fraudster to access the system…"[112] In the similar vein, the Australian Securities & Investments Commission states:[113]

"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."

Some of the country is aware the importance of the two-factor authentication for example the regulatory authorities in Singapore and Hong Kong require banks and financial institutions to implement the two-factor authentication for Internet banking services. The Monetary Authority of Singapore (MAS) in its Circular of 25 November 2005 states:[114]

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 the 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

[112] Ibid

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

[114] Monetary Authority of Singapore, Circular No. SRD TR 02/2005.

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.[115]

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."[116]

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".[117]

4.4 Conclusion

As the conclusions, financial institutions have made, and should continue to make efforts to educate their customers. Because human factor- through customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and periodically evaluate its

[115] Hong Kong Monetary Authority, Circular 23 June 2004, *Strengthening Security Controls for Internet Banking Services*.
[116] Deloitte, "Identity theft- a view from the financial services industry", at 6.
[117] *See* OUT-LAW News, 19/10/2005, "UK Law Will Demand Better Authentication for Online Banking", available at http://www.out-law/page-6241

effectiveness. This is due to phishing is the art or practice of manipulating people in order to obtain confidential or sensitive data. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their stronger authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. 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. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.