Knowledge on Phishing and Vishing: An Empirical Study on Thai Students

Pisit Chanvarasuth

***Abstract*—**Technology currently has been developed continuously to facilitate people. It plays a major role to serve social needs in several aspects. Internet becomes one of many technologies most people use in daily life for several purposes, such as Electronic Commerce, Online Internet banking, and other online operations. With all these facilities available to many people, there can also be harm to people as well. Therefore, this study attempts to examine some of the threats people might have experienced by focusing on the comparison between the effectiveness of phishing and vishing techniques. Our samples are 772 Thai undergrad students whose age range between 18 and 23 years old. A survey was conducted and our result suggests that phishing problem tends to get higher success rate than vishing. Some other factors, such as gender also has an impact on the success rate of each technique.

***Keywords*—**phishing, vishing, security, internet threat, experiment.

I. Introduction

THE term phishing is used for a criminal act of using e-mails, websites, or even telephone as a media. Phishers pretend themselves to look like they come from well-known, legitimate, and trusted businesses, financial institutions, and/or government agencies in an attempt to gain personal and sensitive information [1]. When phishers obtain victims' sensitive information, such as credit card numbers, they will commit online activities using obtained information for their own benefits. Phishing can be called as identity theft or identity fraud. In US and some other countries, researchers use the term "identity theft", while researchers in United Kingdom use the term "identity fraud" to refer to the implementation of acquiring and misusing others' identifying information for criminal purposes.

Reference [2] reported that US is the world's top country where people are victims of Phishing. A report from Binational Working Group on Cross-Border Mass Marketing Fraud indicated that there were 3.6 million adults lost money from phishing attacks in 2007. Phishing Activity Trends Report from Anti-Phishing Working Group (APWG) states that US is the top hosting country for phishing in the second quarter of 2010.

Pisit Chanvarasuth is with the School of Management Technology, Sirindhorn International Institute of Technology, Thammasat University, Pathumtahni 12000 Thailand (phone: 662 501 3505 Ext. 2105 ; fax: 662-501-3505 Ext. 2101; e-mail: pisit@siit.tu.ac.th).

The challenge of defending against phishing is underscored by the fact that most of the domains being used for attacks were legitimate sites that had been compromised by bad guys, with only 28 percent of them being registered maliciously by the phishers. Overall, 60 percent of attacks identified by APWG occurred in four top-level domains: .com, .cc, .net and .org; and 89 percent of the malicious domains were registered in .com, .tk, .net and .info.

More than 2,000 phishing attacks were hosted on sites using IP addresses rather than domain names. All of these attacks were in the traditional IPv4 address space with no phishing activity was found using IPv6 addresses.

Following APWG's report of the second quarter in 2010, payment services was the most targeted industry sector in the first half of the year, while the financial service was the second. Many financial institutions have done a research to find the most threat to them and they have found that phishing (or Spoofed e-mails and fraudulent websites) is their most current threat [2].

There are many incidents demonstrated how phishing threaten Thai people. Reference [3] has warned Thai people to aware of the danger of phishing and also told people not to trust or believe any people who arrogate themselves as officers. In Thailand, vishing is the most concerned issues compared to other internet threats.

This paper is focusing on comparing the effectiveness between phishing and vishing (VoIP) techniques. Most of phishing evidences reported in Thailand illustrates the occurrence of both types of threats. Moreover, this was one of many problems most of Thai people had experienced without much help from any institutions until the Telecommunication Consumer Protection Institute of Thailand has established in 2007 to alleviate vishing victims.

The purpose of this paper is two-fold. First, we aim to compare the effectiveness between phishing and vishing techniques on Thai undergraduate students. Secondly, we aim to explore whether human traits could relate to each technique.

II. Literature Review

A. Phishing

Phishing can be defined as the practice of posting a deceptive message as part of an attempt at fraud and/or identity theft, and especially one manipulated to make it look like it comes from a legitimate business or agency [4]. We can consider phishing as a computer crime, the crime which could

not have been committed without the use of a computer. In general, computer crime mainly consists of unauthorized access to computer systems, data alteration, data destruction, or theft of intellectual property. Computer crime is very similar to a normal crime. The only difference is the means in which the act is carried out. An individual can commit theft, trespassing, embezzlement, and fraud using a computer system. The characteristic of computer crime composed of: invisibility/anonymity of offender, a lack of awareness, unwillingness to report, and intangibility of digital goods, evidence, and value.

Recently we have seen a dramatic increase in internet attacks known as "phishing", in which victims get conned by spoofed emails and fraudulent websites. Phishing is the new technique used to steal the sensitive information by using the E-mail messages similar to legitimate businesses that a victim normally use. This technique is designed to fool recipients into divulging personal data such as credit card numbers [5].

It is often assumed that phishing is about finance-related institutions, e.g., banks, credit unions, Paypal, auction sites, etc. However, in practice, target data is not necessary related to the victim's personal finances. This type of attack can be intended to access quite different forms of data. Non-commercial entities may also need to allow clients to volunteer financial information to pay for services electronically. As a result, potential victims are conditioned to share sensitive data with groups masquerading as taxation departments, healthcare and social security agencies, law enforcement agencies, etc.

Phishing activity is not necessarily restricted to short-term exploitation of financial data, but may be extended to full-scale identity theft. Reference [6] explains how phishing attack occurs with the help of internal network attack detection, and also how to defend against them. Phishing not only aim for personal information of the victim but they also aim for despoiling trusted brands of well-known companies which it is very easy for them in persuading victim to response [7].

Vishing, or voice phishing, is the method of using IP-based voice messaging technologies (Voice over Internet Protocol, or VoIP). The word "vishing" is derived from a combination of voice and phishing [8].

Phishing technique can acquire target's information easier than vishing technique because phishing use database to store the target's information but vishing will use paper to collect the data. When phishers want to use their information the database is more preferable than using a paper. On the other hand, information phishers obtained from phishing is more precise than vishing [9].

B. Phishing in Thailand

As internet usage in Thailand keeps increasing, the phishing problem in Thailand is nearly doubled in the last decade. Most phishing victims are people who operate business transactions through an internet or an internet user who need to provide his/her username and password to login in order to get access to some particular websites. Most of the fraud phishers counterfeit websites by imitating the same pattern as the legitimated webpage.

There were 2,612 Phishing victims in 2007 [7]. In the first half of 2008, the victims had increased to 5,088. Most evidences of computer crime reported in Thailand are phishing and vishing. Phishing and vishing occur most in the Government and Banking websites, e.g., Department of Special Investigation (DSI), Bangkok Bank, Kasikorn Bank, etc. The increased popularity of internet banking and online payment lead phishers to increase their focus in order to fraud people online.

Vishing in Thailand currently evolved itself from using simple phone number to VoIP network. They had counterfeited a phone number to be seen by the victims as it actually comes from legitimated government agencies or financial institutions. Sometimes, phishers use private number or non-shown number to block the victim from tracing back and make the victims trusted the call more easily. Most of victims are elders who live in the rural area.

According to the study on psychology, human being has nature to be helpful when people are in real need. They show the tendency to trust people and fear of getting into trouble. Therefore, people need to be trained in order to defend against all fraud. Since this study aims at comparing the effectiveness between Phishing and vishing techniques, we hypothesize:

Hypothesis 1: Phishing technique is more effective than vishing technique.

Hypothesis 1a: People tend to aware more on vishing than phishing technique.

Hypothesis 1b: Response rate of phishing is higher than vishing.

Hypothesis 1c: Success rate of phishing is higher than vishing.

According to [10], the gender does not provide a significant effect on the success rate of phishing. Moreover, reference [11] states that the Internet phishing strongly affects more on women than men. That is, phishers could gain benefit from women easily than men. Therefore, we expect women is become easily phished than women, then:

Hypothesis 2: Women could be phished easier than men.

Hypothesis 2a: Response rate of women is higher than men.

Hypothesis 2b: Success rate of women is higher than men.

Hypothesis 2c: Women tend to aware of phishing more than men.

In addition, academic majors might also have an impact on the effectiveness of phishing. Reference [12] informs that the academic majors did not provide any effect on phishing results. Hence, we hypothesize:

Hypothesis 3: Academic majors have a relationship with both phishing and vishing techniques.

Different types of incoming telephone number could create variety in the results of vishing. Therefore, we also investigate the effect of different types of incoming telephone number on vishing outcome.

Hypothesis 4: The type of incoming telephone number has related to the effectiveness of vishing technique.

Therefore, our conceptual model can be displayed as follows:

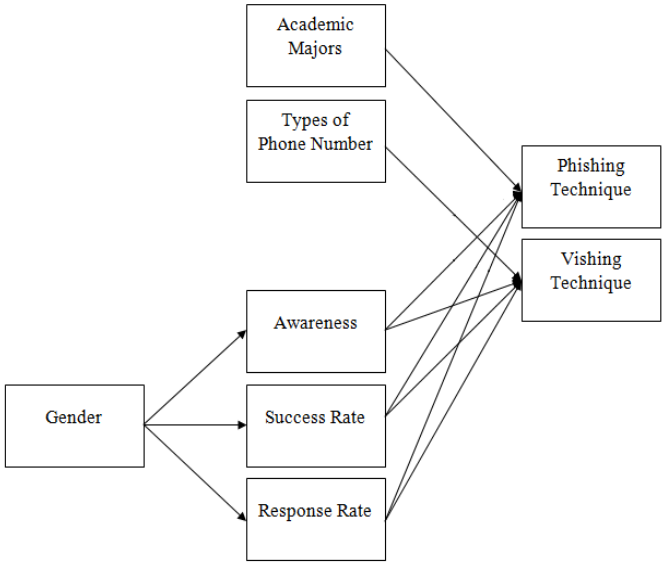

Fig.1 Our Conceptual Model

III. METHODOLOGY

A. Data

In order to capture reliable estimates from a large group of fairly homogenous targets for the phisher, our data collection effort focused on undergraduate students at the institution rather than faculty, staff, and graduate students. Overall, the data collection effort resulted in 772 responses whose age is in the range between 18 to 23 years old. The data was collected by utilizing several tools such as e-mail, web pages, and telephone calls.

B. Data Collection

In a phishing experiment, it is important to make interaction look like it is phishing, without actually compromising credentials. A conductive study such as carrying out phishing attacks, in the academic environment is especially difficult because of reasons that include getting approval from the school and IT personnel to carry out such attacks. In our experiments, we have illustrated methods to avoid having to handle credentials, but still being able to verify whether they were correctly entered. It was achieved by obtaining feedback from a server that the researcher had access to. Undergraduate students in the school of Management Technology, the school of Information Technology, and the school of Engineering were contacted via email asking them to participate in a short-web survey about student e-mail usage and information on their future plan for pursuing graduate studies. Webpage was used to collect the data. We provide a link to webpage that has a misspelled URL (Uniform Resource Locator) to the targets. Web pages were designed similar to the official webpage of their institution. Web pages that replicated from the official institution website were designed. All menus and functions are similar to the official institution website. We decided to use dot com (.com) as a domain which is cheaper than the other host and dot come seems to be the most effective domain for phishing [13].

The step of phishing technique appears when the targets receive phishing e-mail that contains the link to the phisher website. First the targets will see the login page on this page, the targets are asked to login by using their own student ID and password on the registration page. The website also asks each student to fill their information such as name, last name, age, e-mail, and others. Our questionnaire was adapted from [14] which divided their survey into 3 parts; demographic, scale of awareness, and riskiness caused by phishers.

After acquiring the information from both phishing and vishing technique, we use victim's information to analyze and compare the effectiveness of both phishing and vishing techniques. Since this study aims to compare the effectiveness between phishing and vishing techniques then we use paired sample t-test to compare means on the same or related subject for comparison between two sample groups. We use One-Way ANOVA to analyze the data which has more than two groups of sample. Results

We have obtained responses from the total of 772 participants. Then, we divided these responses into two groups separated for each technique (see Table I). In phishing technique, we have sent an e-mail to 433 people and we got 123 (28.4%) respondents. We also made a phone call to 339 students and received 325 (95.9%) success responses.

TABLE I
NUMBER STUDENTS WHO ARE PHISHED

	Percentage	Count
Phishing	28.4%	123
Vishing	95.9%	325

Table II indicates that 224 (51.7%) of the respondents were men and 209 (48.3%) were women. Vishing has 172 (50.7%) of the respondent were men and 167 (49.3%) were women.

TABLE II
NUMBER OF RESPONDENTS CATEGORIZED BY THEIR GENDER

		Percentage	Count	Total
Phishing	Male	51.7%	224	433
	Female	48.3%	209	
Vishing	Male	50.7%	172	339
	Female	49.3%	167	

According to Table III, undergraduate students have been categorized into three groups upon their academic majors, which are: Engineer (20.9%), Technology (26.3%), and Management (52.8%).

TABLE III
NUMBER OF UNDERGRADUATE STUDENTS DIVIDED BY THEIR ACADEMIC MAJOR

Major	Percentage
Engineer	20.9
Technology	26.3
Management	52.8

Table IV illustrates the list of student online activities. These activities include: E-learning (1.4%), gaming (6.9%), e-mail (16.7%), news (15.3%), search engine (23.6), social network (29.1%), e-commerce (2.8%), and others (4.2%), respectively.

TABLE IV
ACTIVITY ON THE INTERNET

Activity	Percentage
E-learning	1.4
Gaming	6.9
E-mail	16.7
News	15.3
Search Engine	23.6
Social Network	29.1
E-Commerce	2.8
Others	4.2

Table V shows all types of media that make the students aware of phishing included internet (53.2%), newspaper (1.3%), television (11.7%), and others such as billboard, radio, or word of mouth (33.8%). Our finding implies that in order to make people more aware of phishing, they should use internet as a major channel because most of the students currently follow the news via internet, radio, billboard, and word of mouth.

TABLE V
MEDIA WHICH STUDENTS LEARN ABOUT PHISHING

Media	Percentage
Internet	53.2
Newspaper	1.3
Television	11.7
Others	33.8

The first hypothesis is focusing on comparing the effectiveness between two techniques; phishing and vishing (see Table VI).

TABLE VI
A COMPARISON BETWEEN AN EFFECTIVENESS OF PHISHING AND VISHING TECHNIQUE

Hypotheses		F Critical	F Statistic	Sig.
H4	Home	1.752	1.36	0.688
	Private	1.437	1.36	0.647
	Mobile	2.716	1.36	0.070**

*$p<0.05$

People tend to aware of phishing more than vishing technique. Hypothesis 1a uses an awareness factor to determine the result. We found that undergraduate students are more familiar with phishing than vishing technique.

Response rate of phishing is higher than vishing response rate. The result of phishing is obtained by the victim response to e-mail and sign up on our website. On the other hand, the result of vishing technique is acquired by the number of times undergraduate students respond to the call. From our finding, it can be concluded that undergraduate students are more vulnerable on phishing than vishing.

Success rate of phishing is higher than vishing success rate. On phishing technique, we obtained students' name, last name, and the mobile phone number to count as success. For vishing technique, the needed information is name, last name, and student ID. On the hypothesis 1c, we found that undergraduate students are vulnerable more on phishing than vishing technique.

Thus, our result reveals that phishing technique is more effective than vishing technique implied by the results of all three sub-hypotheses.

TABLE VII
RESULTS OF THE DIFFERENT GENDER

Hypotheses		SD	Standard error mean	t	Sig.
H2	2a	0.53267	0.02747	- 1.452	0.147
	2b	1.09681	0.05656	-2.210	0.028*
	2c	0.60966	0.04217	1.362	0.175

*$p<0.05$

According to Table VII, only hypothesis 2a is accepted. Therefore, response rate of women is higher than men as $p<0.05$. That is, women seem to get phished easier than men.

For our samples, their academic majors consist of management, technology, and engineering. We found that all three majors are vulnerable to phishing technique (see Table VIII).

TABLE VIII
RESULT OF ACADEMIC MAJORS

Hypotheses		F Critical	F Statistic	Sig.
H3	Technology	1.454	1.36	0.238
	Engineer	1.420	1.36	0.246
	Management	1.426	1.36	0.244

We categorize an incoming telephone number into 3 main types: a household phone number (starting with 02), a private phone number (a no-show number), and a mobile phone number. Our results reveal that the different type of phone number seems to affect the effectiveness of phishing, especially for a mobile phone number that have a fairly low statistic significant. (see Table IX).

TABLE IX
RESULTS OF INCOMING TELEPHONE NUMBER

Hypotheses		SD	Standard error mean	t	Sig.
H1	1a	1.25182	0.11333	0.940	0.349
	1b	0.67081	0.03643	- 9.878	0.00*
	1c	1.37683	-0.07478	- 6.588	0.00*

**p<0.1

IV. CONCLUSION

There has been an increasing in the degree of sophistication in the methods that phishers use to attack consumers. Since phishers are continually designing new ways to execute their attacks on online users, phishing research must stay abreast

and ahead of the scammers in terms of the sophistication and type of phishing strategy, otherwise the knowledge cannot come up with up-to-date approaches to defend against these attacks and protect both users and providers.

In this study, we examine the differences on phishing technique which are spoofing website and vishing. We found that no matter how different of the method in each phishing technique, the results of both techniques are still the same which the target always loses sensitivity information and some of their property. Therefore, user prior education or user awareness appears to be the best weapon to combat against phishing [15].

Our result also reveals that phishing technique is more effective than vishing technique. In general, phishing technique provides higher response rate and success rate. Women are easily to get phished more than men. In addition, an academic major is not a factor affecting the effectiveness of phishing technique. However, we also found that the type of incoming telephone call seems to have an impact on phishing's success rate. Our finding agrees with [11] on the issue that women are phished easier than men, but disagree with the statement of [10] mentioned that gender does not have any effect on phishing. Moreover, our findings also agree with the study by [12] that academic majors do not have any effect on phishing at all.

REFERENCES

[1] Irani, D., Webb, S. and Giffin J., "Evolutionary Study of Phishing", *eCrime Researchers Summit*, 2008, pp. 1-10.

[2] Manning, R., "Phishing Activity Trends Report, 2nd Quarter/2010", *APWG*, 2010, pp. 1-11.

[3] Electronic Publication: APWG's Global Phishing Survey: Trends and Domain Name Use in 1H2009, October 2009: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf

[4] Harley, D. and Lee, A., "Phish Phodder: Is User Education Helping or Hindering?", *Virus Bulletin Conference*, 2007, pp. 1-7.

[5] Kay, R., "Quick Study: Phishing, Computerworld," 2004, http://www.computerworld.com/s/article/89096/Phishing.

[6] Stamm, S., Ramzan, Z., and Jakobsson, M., "Drive-by Pharming," *Technical Report TR641*, Indiana University, December 2006.

[7] Pibulyarojana, K. and Jirawannakool, K., "ThaiCERT Annual Report of 2007,": http://www.ieee.th.org/IEEEConference2008/Proceedings2008/papers/IEEE_Full_Paper_Komain.doc_Paper_5.pdf.

[8] Castiglione, A., De Prisco, R., and De Santis, A., "Do you trust your phone?" In T. Di Noia and F. Buccafurri (Eds.), *E-Commerce and Web Technologies*, 2009, pp. 50-61.

[9] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J., "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", In the *Proceedings of CHI '10, SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 373-382.

[10] Jagatic, T.N, Johnson, N.A., Jakobsson, M., and Menczer, F., "Social Phishing", *Communications of the ACM*, vol. 50, no. 10, 2005, pp. 94-100.

[11] Colley, A. and Maltby, J., "Impact of the Internet on our lives: Male and Female Personal Perspectives", *Computers in Human Behavior*, 2008, vol. 24, no. 5, pp. 2005-2013.

[12] Case, C.J. and King, D.L., "Phishing for Undergraduate Students", *Research in Higher Education Journal*, 2006, pp. 100-106.

[13] Rasmussen, R., "Global phishing survey: Trends and domain name use", 2009: http://web.resourceshelf.com/go/resourceblog/55772.

[14] Wang, J.R.C., Herath, T., Rao, H. R., "An Empirical Exploration of the Design Pattern of Phishing Attacks", in: S.J. Upadhyaya, H.R. Rao (Eds.), *Annals of Emerging Research in Information Assurance, Security and Privacy Services*, Emerald Publishers, 2009.

[15] Baker, E.M., Baker, W.H., and Tedesco, J.C., "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box", *Communication Research Reports*, 2007, vol. 24, no. 4, pp. 327-339.