Phishing: a Field Experiment

Danuvasin Charoen, Ph.D. *danuvasin@nida.ac.th*
NIDA Business School
National Institute of Development Administration
Bangkok, Thailand

Abstract

Phishing is a method that hackers use to fraudulently acquire sensitive or private information from a victim by impersonating a real entity [1]. Phishing can be defined as the act of soliciting or stealing sensitive information such as usernames, passwords, bank account numbers, credit card numbers, and social security or citizen ID numbers from individuals using the Internet [2]. Phishing often involves some kind of deception. The results from a study of Jagatic et al. (2007) indicate that Internet users are four times more likely to become phishing victims if they receive a request from someone appearing to be a known friend or colleague. The Anti-Phishing Work Group indicates that at least five percent of users responded to phishing scams and about two million users gave away their information to spoofed websites [3]. This results in direct losses of $1.2 billion for banks and credit card companies (Dhamija, 2006).

In order to understand how phishing can be conducted, the researcher set up a phishing experiment in one of Thailand's higher education institutions. The subjects were MBA students. A phishing email was sent to the subjects, and the message led the subject to visit the phishing website. One hundred seventy students became victims. The data collection included a survey, an interview, and a focus group. The results indicated that phishing could be easily conducted, and the result can have a great impact on the security of an organization. Organizations can use and apply the lessons learned from this study to formulate an effective security policy and security awareness training programs.

Keywords: Phishing, Computer Crime, Data Security

1. INTRODUCTION

Computers and the Internet have become critical parts of daily life in Thailand, where there has been explosive growth in E-Commerce and in the ICT Market. The total market value for e-Commerce in 2007 was about fourteen billion dollars (National Statistic Office, 2007). Computers and the Internet can provide opportunities for a company to develop competitive advantages, for example, through e-Commerce, online customer services, supply chain management, etc. However, one of the obstacles to e-Commerce growth is the growing concern about computer and Internet-related crimes. Seventy point two percent of E-Commerce customers indicate that they are concerned about the security and privacy of their data when they conduct transactions online [4]. Additionally, customers are worried about giving out their private information on the Internet because of growing concern over computer crime.

In Thailand, computer and Internet-related crimes have become a major concern because the financial loss for the damage can be tremendous. There has been especially strong concern by the industries that utilize computers and the Internet, such as banks and hospitals [5].

In the past, the major concern regarding computer security was malicious software, such as viruses, worms, and spyware. In 2005, this malicious software was a top concern; however, since 2007, the most reported incident was phishing [5]. Phishing is the act or method of tricking users into giving away their private information, including credit card numbers, banking accounts, and usernames and passwords [6]. The methods of phishing include sending phony email messages and duplicating legitimate websites.
In 2010, there were at least 48,244 phishing attacks worldwide[7], and an attack is defined as a phishing website that targets a specific company or brand [7].

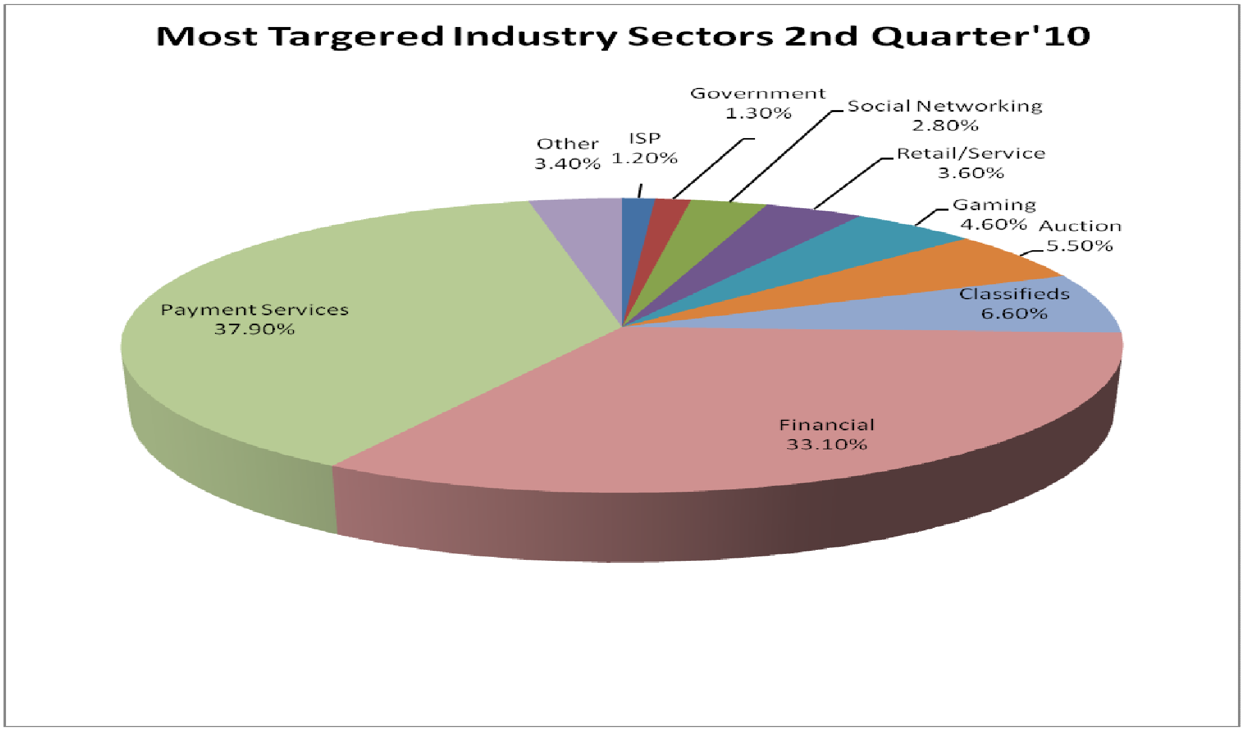


FIGURE 1: Most Targeted Industry Sector [8]

According to the Anti-Phishing Working Group (APWG), the most targeted industry in 2010 was payment services, accounting for 37.9%. The second was financial services, which accounted for 33%, followed by classifieds at 6.6% [8]. Gaming and social networking accounted for 4.6% and 2.8% [8] respectively.

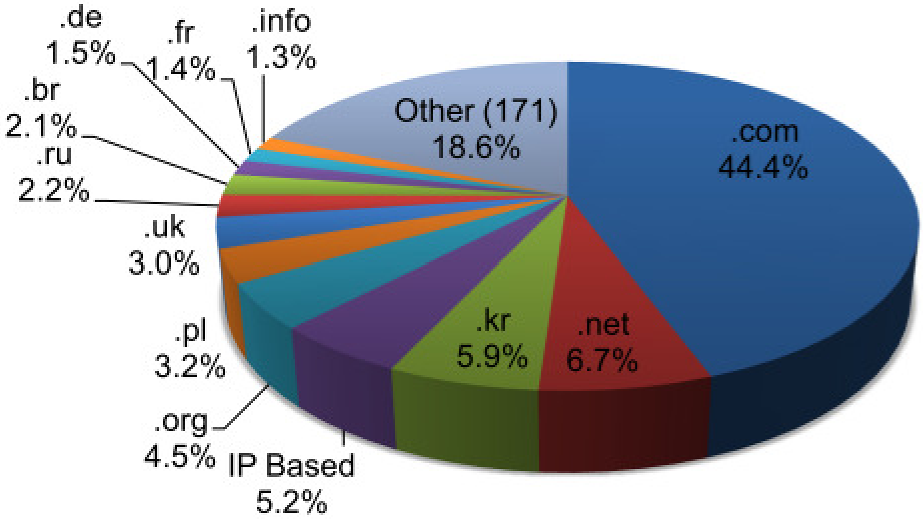


FIGURE 2: Most Targeted Industry Sector [8]

Com was the world largest and most ubiquitous top level domain name. In 2010, .Com contained 44.4% of the phishing domains.

Phishing is now the most common computer crime in Thailand and accounts for 77% of all computer-related crimes [5]. Phishing includes duplicating legitimate Websites such as Ebay, PayPal, and others in order to trick users into revealing their account information.

RANK	TLD	TLD Location	# Unique Phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010
1	th	Thailand	86	62	49,000	12.7	17.6
2	kr	Korea	2,888	989	1,079,298	9.2	26.8
3	ie	Ireland	102	79	145,724	5.4	7.0
4	pl	Poland	1,582	744	1,805,894	4.1	8.8
5	cl	Chile	159	111	282,526	3.9	5.6
6	my	Malaysia	61	39	99,736	3.9	6.1
7	gr	Greece	130	93	260,000	3.6	5.0
8	ro	Romania	324	156	443,700	3.5	7.3
9	vn	Vietnam	64	48	153,002	3.1	4.2
10	cz	Czech Republic	480	207	689,813	3.0	7.0

TABLE 1: Phishing per 10,000 domain names [7]

The above table indicates that phishing has become a serious crime in Thailand. In 2010, Thailand was ranked first in the world for the second consecutive year in terms of the number of phishing websites per 10,000 domains [7]. .Th (Thailand) was at the top of the phishing list between 2009 and 2010. Phishing in .th took place mostly in academic institutions (.ac.th) and governmental organizations (go.th), as well as in commercial organizations (.co.th). These phishing websites dramatically affect consumers' confidence in conducting transactions online.

In the past, the major concern regarding computer security was malicious software, such as viruses, worms, and spyware. Since 2007, the most reported incident has been phishing [5].

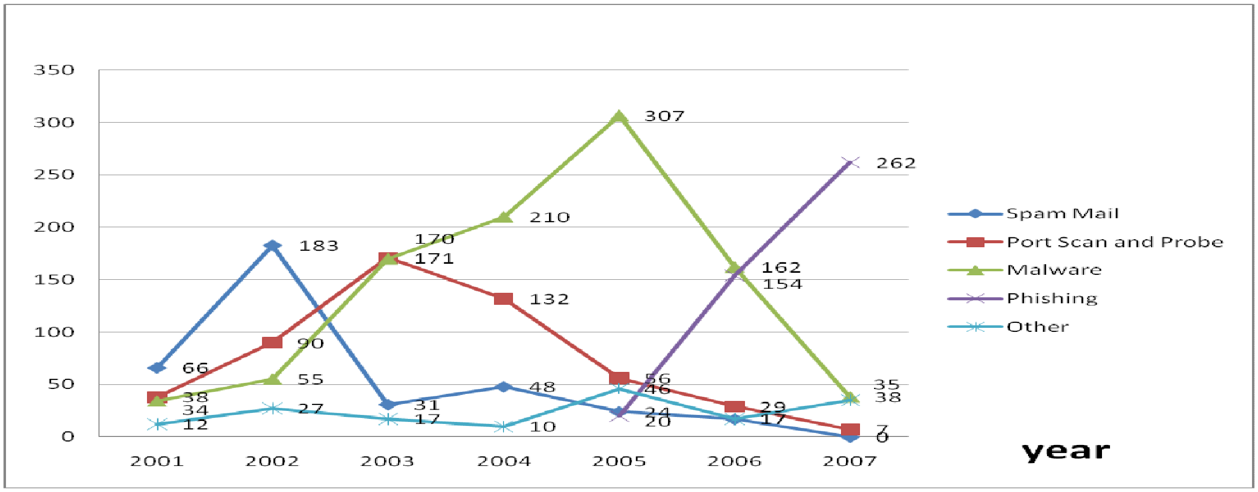


FIGURE 3: Number of Incidents since 2001 categorized based on methods [5]

The phishing problem is now the most frequent computer crime in Thailand and accounts for 77% of all computer-related crimes [5].

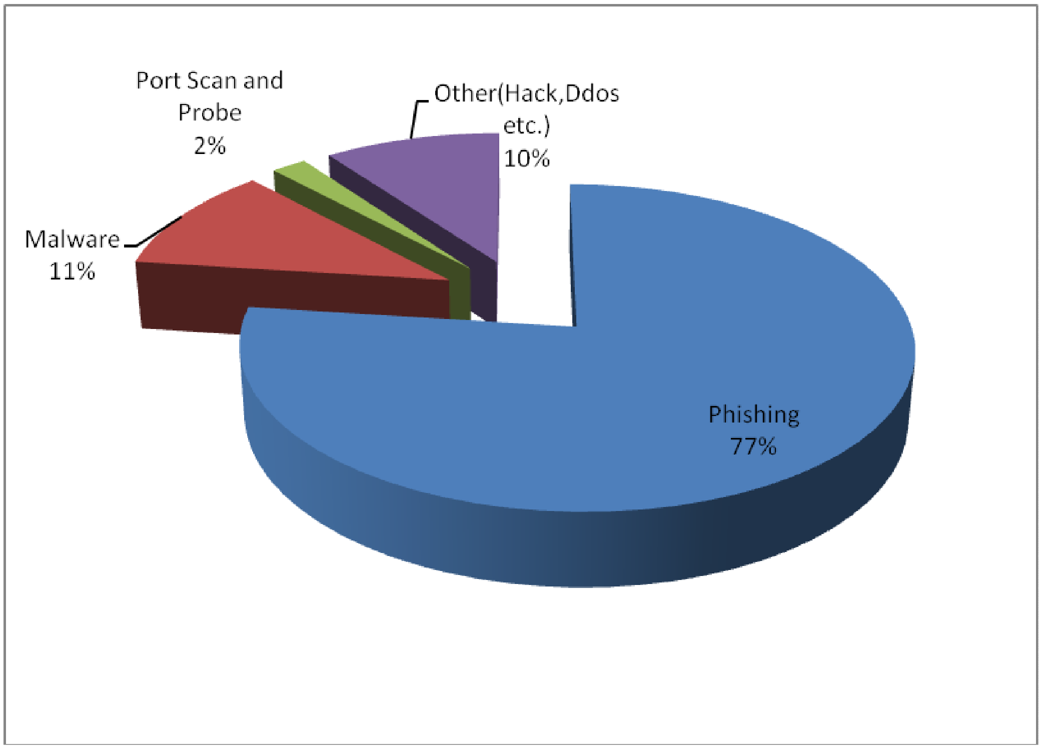


FIGURE 4: Ratio of each type of ThaiCERT- reported incident in the year 2007 [5]

Figure 4 indicates the number of incidents categorized by incident sources. From the figure, it can be seen that phishing is the most frequent computer crime. The survey indicates that government organizations are the main target of computer criminals. In 2007, 170 government organizations in Thailand became victims of computer crimes [5]. This may be because government organizations store a lot of sensitive information, such as citizen information, tax information, etc. This information can be a gold mine for the computer criminal to commit identity theft.

2. RESEARCH OBJECTIVES

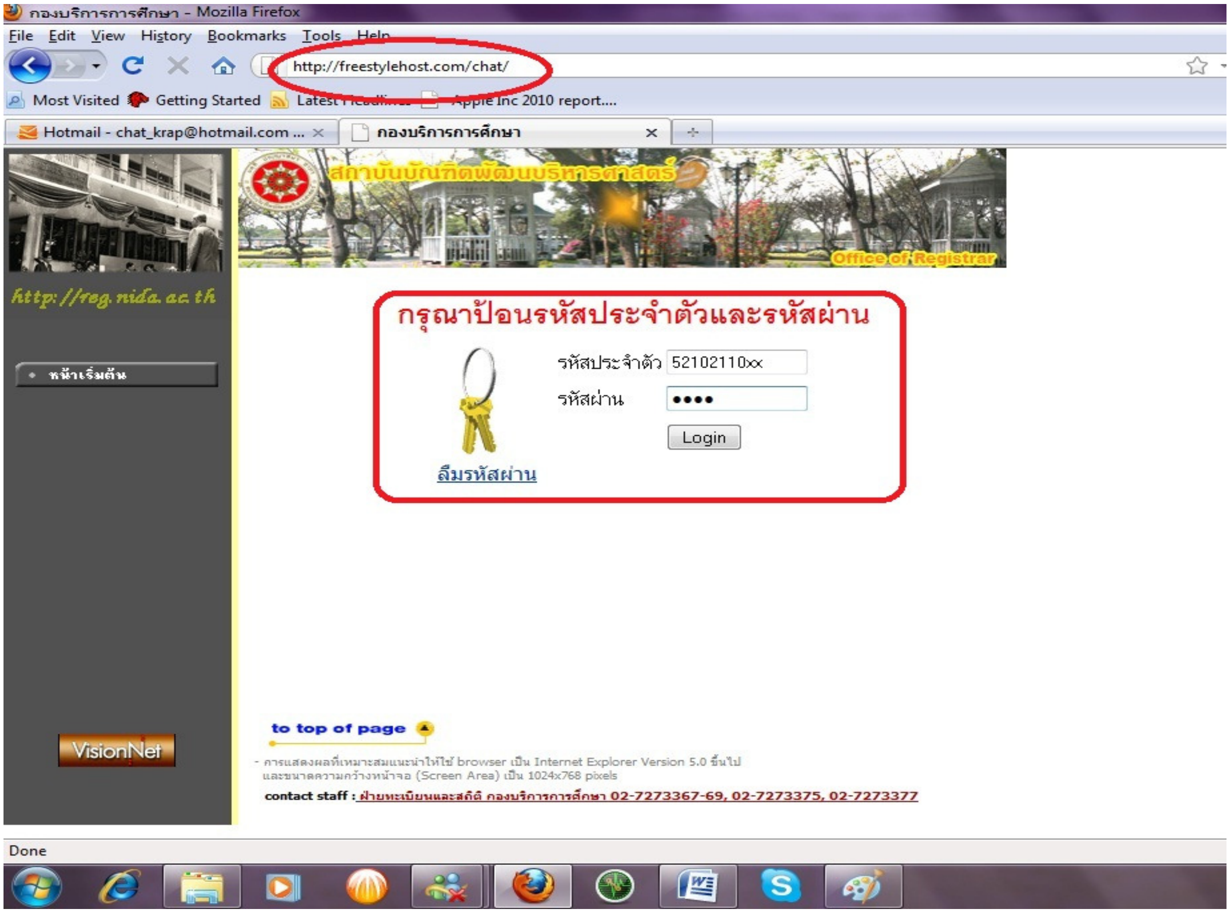
The study is intended to investigate how users become victims of phishing attack. To study how phishing work in the real world, the researcher chose a field experiment approach. The results of the study can potentially explain how phishing works and how people become the victims.

3. RESEARCH SETTING

The researcher recently conducted a phishing experiment at one of the graduate institutions in Thailand. For the purpose of this study, we focused on a subset of the target group. The targets consisted of second year MBA students in the School of Business Administration, the National Institute of Development Administration. The main purpose was to evaluate how social context can increase the success of a phishing attack. The researcher worked closely with the school's institutional review board in designing the research protocol for this study, which can be broken down into four phases.

3.1 Phase 1: Preparation

The researcher identified the target group, which consisted of 174 MBA students. All of them had school accounts to log into the registration system. Their account contained private information, including name, address, student ID, citizen ID, courses taken, and grades. The objective of the experiment was to spoof the student's username and password. In order to do this, a phishing website was created based on the registration website (see figure 5).



กองบริการการศึกษา - Mozilla Firefox

http://freestylehost.com/chat/

Hotmail - chat_krap@hotmail.com ...

กองบริการการศึกษา

กรุณาป้อนรหัสประจำตัวและรหัสผ่าน

รหัสประจำตัว 52102110xx

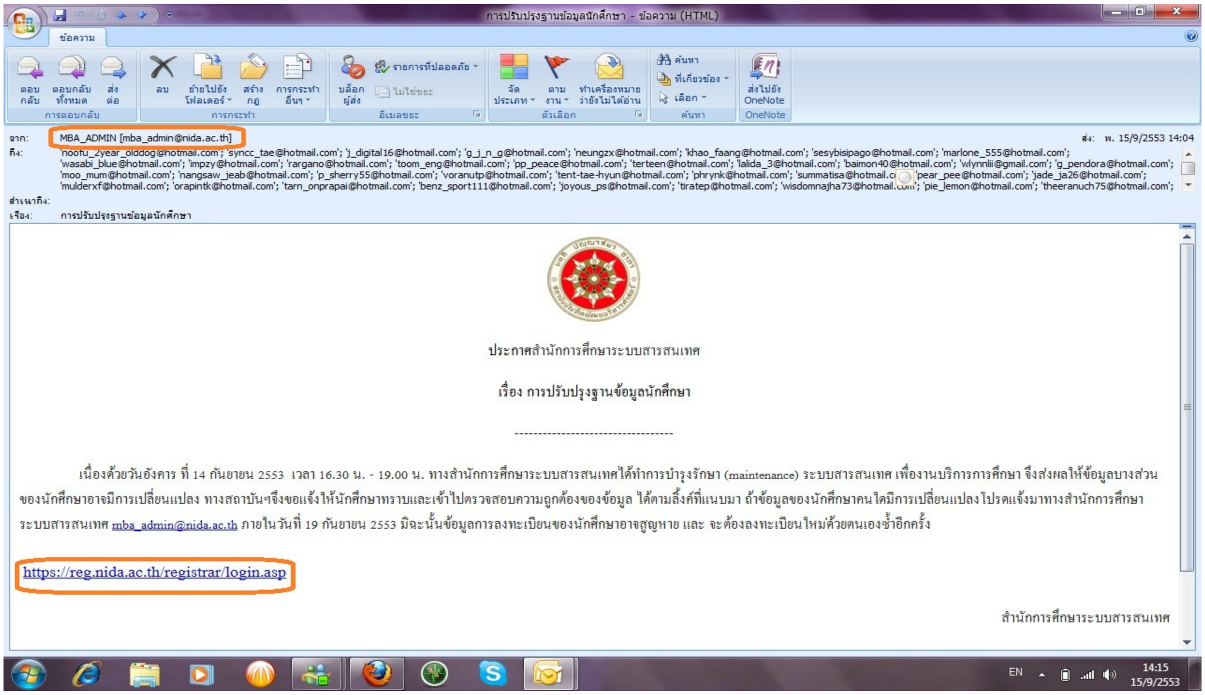
รหัสผ่าน ●●●●

- การแสดงผลที่เหมาะสมแนะนำให้ใช้ browser เป็น Internet Explorer Version 5.0 ขึ้นไป และขนาดความกว้างหน้าจอ (Screen Area) เป็น 1024x768 pixels

contact staff : ฝ่ายทะเบียนและสถิติ กองบริการการศึกษา 02-7273367-69, 02-7273375, 02-7273377

FIGURE 5: The phishing registration website

The experiment created a phishing administrator email account at mba_admin@nida.ac.th by collaborating with the Information Systems Education Center (ISEC) at NIDA (see figure 6). The message indicated that there were some major changes in the registration systems that required students to visit the link (phishing website) and log into it using their student IDs and passwords to update their personal information.



จาก: MBA_ADMIN [mba_admin@nida.ac.th]

ส่ง: พ. 15/9/2553 14:04

ถึง: 'noofu_2year_olddog@hotmail.com'; 'syncc_tae@hotmail.com'; 'j_digital16@hotmail.com'; 'g_j_n_g@hotmail.com'; 'neungzx@hotmail.com'; 'khao_faang@hotmail.com'; 'sesybisipago@hotmail.com'; 'marlone_555@hotmail.com'; 'wasabi_blue@hotmail.com'; 'impzy@hotmail.com'; 'rargano@hotmail.com'; 'toom_eng@hotmail.com'; 'pp_peace@hotmail.com'; 'terteen@hotmail.com'; 'lalida_3@hotmail.com'; 'baimon40@hotmail.com'; 'wlynnlii@gmail.com'; 'g_pendora@hotmail.com'; 'moo_mum@hotmail.com'; 'nangsaw_jeab@hotmail.com'; 'p_sherry55@hotmail.com'; 'voranutp@hotmail.com'; 'tent-tae-hyun@hotmail.com'; 'phrynk@hotmail.com'; 'summatisa@hotmail.c 'pear_pee@hotmail.com'; 'jade_ja26@hotmail.com'; 'mulderxf@hotmail.com'; 'orapintk@hotmail.com'; 'tarn_onprapai@hotmail.com'; 'benz_sport111@hotmail.com'; 'joyous_ps@hotmail.com'; 'tiratep@hotmail.com'; 'wisdomnajha73@hotmail.com'; 'pie_lemon@hotmail.com'; 'theeranuch75@hotmail.com';

สำเนาถึง:

เรื่อง: การปรับปรุงฐานข้อมูลนักศึกษา

ประกาศสำนักการศึกษาระบบสารสนเทศ

เรื่อง การปรับปรุงฐานข้อมูลนักศึกษา

เนื่องด้วยวันอังคาร ที่ 14 กันยายน 2553 เวลา 16.30 น. - 19.00 น. ทางสำนักการศึกษาระบบสารสนเทศได้ทำการบำรุงรักษา (maintenance) ระบบสารสนเทศ เพื่องานบริการการศึกษา จึงส่งผลให้ข้อมูลบางส่วนของนักศึกษาอาจมีการเปลี่ยนแปลง ทางสถาบันฯจึงขอแจ้งให้นักศึกษาทราบและเข้าไปตรวจสอบความถูกต้องของข้อมูล ได้ตามลิ้งค์ที่แนบมา ถ้าข้อมูลของนักศึกษาคนใดมีการเปลี่ยนแปลง โปรดแจ้งมาทางสำนักการศึกษาระบบสารสนเทศ mba_admin@nida.ac.th ภายในวันที่ 19 กันยายน 2553 มิฉะนั้นข้อมูลการลงทะเบียนของนักศึกษาอาจสูญหาย และ จะต้องลงทะเบียนใหม่ด้วยตนเองซ้ำอีกครั้ง

https://reg.nida.ac.th/registrar/login.asp

สำนักการศึกษาระบบสารสนเทศ

FIGURE 6: The spoofed email message

In order to enhance the credibility, the experiment spoofed an email account from the president of the MBA class using an email-spoofer application and used his email to send the link of the phishing website to all MBA students (see figure7).

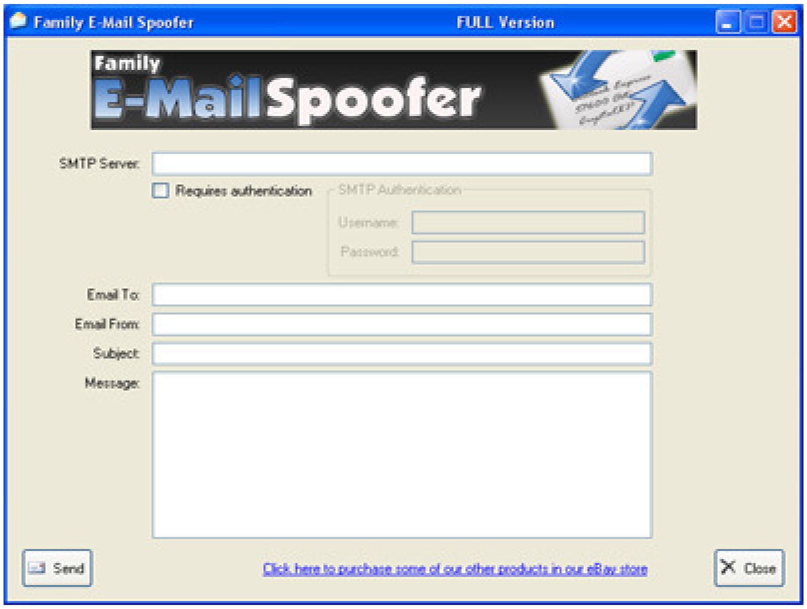
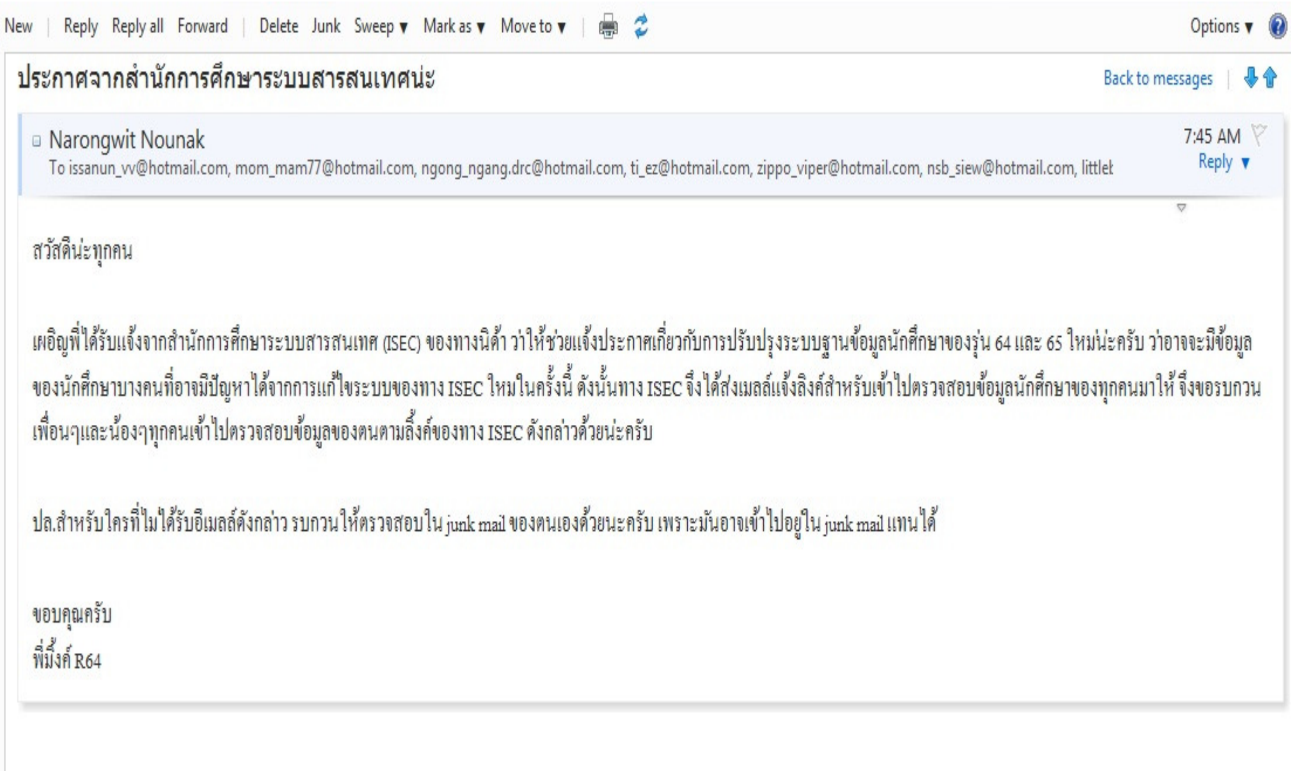


FIGURE 7: E-mail spoofer application



ประกาศจากสำนักการศึกษาระบบสารสนเทศน่ะ

Narongwit Nounak 7:45 AM

To issanun_vv@hotmail.com, mom_mam77@hotmail.com, ngong_ngang.drc@hotmail.com, ti_ez@hotmail.com, zippo_viper@hotmail.com, nsb_siew@hotmail.com, littlel

สวัสดีน่ะทุกคน

เผอิญพี่ได้รับแจ้งจากสำนักการศึกษาระบบสารสนเทศ (ISEC) ของทางนิด้า ว่าให้ช่วยแจ้งประกาศเกี่ยวกับการปรับปรุงระบบฐานข้อมูลนักศึกษาของรุ่น 64 และ 65 ใหม่น่ะครับ ว่าอาจจะมีข้อมูลของนักศึกษาบางคนที่อาจมีปัญหาได้จากการแก้ไขระบบของทาง ISEC ใหมในครั้งนี้ ดังนั้นทาง ISEC จึงได้ส่งเมลล์แจ้งลิงค์สำหรับเข้าไปตรวจสอบข้อมูลนักศึกษาของทุกคนมาให้ จึงขอรบกวนเพื่อนๆและน้องๆทุกคนเข้าไปตรวจสอบข้อมูลของตนตามลิ้งค์ของทาง ISEC ดังกล่าวด้วยน่ะครับ

ปล.สำหรับใครที่ไม่ได้รับอีเมลล์ดังกล่าว รบกวนให้ตรวจสอบใน junk mail ของตนเองด้วยนะครับ เพราะมันอาจเข้าไปอยู่ใน junk mail แทนได้

ขอบคุณครับ
พี่มิ้งค์ R64

FIGURE 8: The message in the spoofed email

The message indicated that the Information Systems Education Center (ISEC) needed to upgrade the system and it needed students to log into the provided link. It was also stated that those students that do not log in might not be able to register for any class (see figure 8).

3.2 Phase 2: Execution

Once the phishing registration website was set up, the email was sent to 174 MBA students. The URL on the phishing registration website was not a real URL, while the interface of the phishing website was the same as the real registration website (see figure 9).

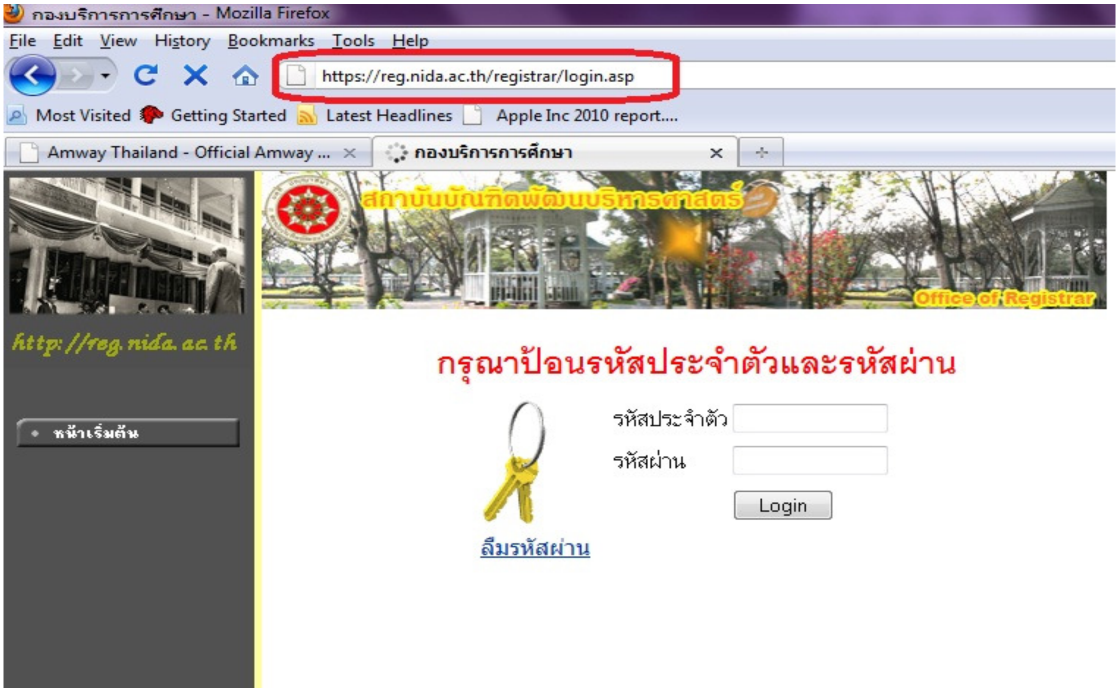

กองบริการการศึกษา - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://reg.nida.ac.th/registrar/login.asp
Most Visited
Getting Started
Latest Headlines
Apple Inc 2010 report....
Amway Thailand - Official Amway ...
กองบริการการศึกษา
สถาบันบัณฑิตพัฒนบริหารศาสตร์
Office of Registrar
http://reg.nida.ac.th
หน้าเริ่มต้น
กรุณาป้อนรหัสประจำตัวและรหัสผ่าน
รหัสประจำตัว
รหัสผ่าน
Login
ลืมรหัสผ่าน

FIGURE 9: The real registration website

When the students received the email from the administrator and the class president, they clicked on the link to the phishing registration website. To log in, they had to provide their student ID and password. When the students clicked login, the page indicated that the system had a problem and asked them to reload the page. Once they reloaded the page, it led them to the real registration website (see figure 9), and once there, they could log into the system. However, the experimenter already had their passwords.

Once they entered their student ID and password, this information was emailed to the researcher. The passwords were encrypted in a way that the researcher cannot see the clear text. All the encrypted passwords were destroyed after the experimentation.

3.3 Phase 3 Results

Out of the 174 MBA students, 170 students logged into the phishing website—79 males (49.3%) and 91 females (50.70%). Although the researcher did not keep the password, the subjects were asked to change their passwords after the experiment. The attack was more successful since it was a spoofed email sent by an influential person, in this case the class president. From the post experimentation survey, 87.3% of the victims indicated that they trusted the content of the email because it was sent from the class president.

3.4 Phase 4 Evaluation

A focus group was conducted after the experiment to evaluate the effectiveness of the phishing attack. The results are the following:

Surprise: all subjects were surprised that they became victims to the phishing website. They believed that the email was actually sent from the class president, and they did not suspect any phishing activity. This might be because the website was made exactly like the real registration website. However, most subjects that became victims did not suspect that it was the wrong URL. Few subjects reported that they saw the wrong URL but still submitted their ID and password because they did not think the website was a fake.

Anger: some subjects were angry to find out that they revealed their ID and password to the phishing website. Some called experiment unethical and illegal. Although no sensitive information about the victims was retained, most victims reported that they were upset to find out they were being tricked to reveal their password. Just like the study of Jagatic et al. (2007), this proves that a phishing attack can result in a tremendous psychology cost for the victims [9].

Mistrust: all victims indicated that the reason they felt victimized was because the email was sent from the class president; they trusted the content of the email to be authentic. The subjects reported that they would never trust any email from an authority asking them to reveal sensitive information.

Misunderstanding: most victims reported that they believed email accounts could not be spoofed. Many subjects did not understand how the researcher was able to spoof the class president's email and most of them believed that the researcher needed to hack into the class president's email. Many subjects believed that the email must have been actually sent from the class leader—they did not know how easy it was for an email to be spoofed.

4. LESSONS LEARNED

The Credibility of a Spoofed Email Plays a Critical Role in the Success of a Phishing Attack

Phishers sometimes send emails that appear to be coming from a legitimate and influential person (IT department, customer support or CEO) within an organization to its employees or customers to update their account passwords. Employees or customers are then directed to a fake website. Since employees or customers believe they are familiar with the sender of the email and the website they are directed to, they are likely to give away sensitive information, such as username, password, and other private information. Today, phishers are more sophisticated with email spoofing. They can easily identify the email of legitimate and influential people through corporate websites and/or social networks such as Facebook.

Phishers Often Use Visual Deception to Imitate Legitimate Websites by Using Text and Images.

Using fraudulent e-mail attachments with a hyperlink that imitates a legitimate website makes the victim believe that it is an official website; he or she then inputs his or her personal information.

Phishers Often Create a Sense of Emergency

Most Phishers create an emergency where the victim needs to react quickly. In this case study, the subjects were notified that they had to log in immediately; otherwise, they could not register for any class. Most victims of this phishing method feel rushed and that they need to respond right away or risk having a negative consequence.

Phishers Often Pretend to be an Authority

In order to gain the trust of the victim, a lot of phishers pretend to be some kind of authority by spoofing email from real authorities. In many cases, phishers have spoofed emails from email administrators and threaten to close an account if the victims do not reply with their username and password. In this case study, the email was made to appear to have been sent from the administrator (mba_admin@nida.ac.th), and lot of students reported that they were duped by the scam because they were afraid of authority.

IT Security Education is Needed to Prevent Phishing

The most effective way to prevent phishing is through security education or a security awareness program. Employees or people in an organization should know about the different methods of phishing and how they can become a victim. Role play can be used as part of the training so that the trainee will understand what phishing methods are used.

An Organization Should Frequently Conduct a Phishing Audit

A phishing audit is an ultimate method to deter and prevent phishing. An internal and external audit should be implemented. An internal audit can be done through an organizational IT department in order to identify weakness and at the same time educate end users. In this study, the process and results of the phishing experiment were shared with the IT department. Because of the results, the IT department considered revising its security policy and training system. An external audit can be done through an outside security consultant.

5. CONCLUSIONS

Phishing is the worst computer crime in Thailand, both in terms of frequency and in terms of impact. This study illustrates how phishing works and how easy it is for people to become a victim of a phishing attack. The researcher conducted a field experiment. A phishing website was created based on a real registration website. The subjects were MBA students. The spoofed email was sent to the subjects and they were asked to visit the phishing registration website. One hundred seventy subjects became the victims by revealing their student IDs and passwords. After the experiment, the subjects were notified to change their passwords, and a focus group was conducted, where the phishing victims expressed feelings of surprise, mistrust, and misunderstanding. The lessons learned from this study indicate that the credibility of a spoofed email plays a critical role in the accomplishment of a phishing attack. The results of the study also indicate that creating a sense of emergency and pretending to be an authority can be an effective method for deceiving victims. From the study, the author suggests that the best way to prevent phishing is through security awareness programs and security audits.

6. REFERENCES

[1] Turban, E., et al., Information Technology for Management: Transforming Organizations in the Digital Economy 7th ed. 2010: Wiley.

[2] Ohaya, C. Managing Phishing Threats in an Organization. in InfoSecCD. 2006. Kennesaw, GA: ACM.

[3] APWG. (2009). Phishing Activity Trends Report: www.antiphishing.org. Available: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf [December 21, 2010].

[4] Office, N. S. (2008). E-Commerce Report Bangkok, Thailand: National Statistical Office Available: http://service.nso.go.th/nso/nsopublish/pocketBook/electThaiRep_52.pdf [November 7, 2010].

[5] ThaiCert, Year 2007 ThaiCERT's handled Incident Response Summary, N. Sanglerdinlapachai, Editor. 2007, Thai Computer Emergency Response Team.

[6] Turban, E., et al., Information Technology for Management: Transforming Organizations in the Digital Economy 6th ed. 2008: Wiley.

[7] APWG. (2010a). Global Phishing Survey: Trends and Domain Name Use in 1H2010 Available: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf [December 25, 2010].

[8] APWG. (2010b). Phishing Activity Trends Report: APWG. Available: http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf [December 25, 2010].

[9] Jagatic, T.N., et al., Social Phishing. Communications of the ACM, 2007. 50(10).