Proposing Awareness Guidelines on Phishing Attempts among Students

Vanisri Nagalingam, Ganthan Narayana Samy, Nurazean Maarop, Nurulhuda Firdaus Mohd Azmi, Bharanidharan Shamugam, Rabiah Ahmad

Abstract

This study mainly focuses on identifying the level of user awareness on phishing attempts among students and to propose appropriate phishing awareness guidelines specifically among students. The research focused on the phishing attempts among four selected academic institutions in Malaysia with a total of 113 students from information technology background. Adopting mixed research design, this study has found that the level of awareness on phishing attempts among students in Malaysia is low through a web based survey that has been conducted. Another important contribution of this study is proposed phishing awareness guideline for students. These guidelines may be useful as a basis reference for researchers and practitioners whom wish to conduct study on phishing awareness especially among students. The guideline was produce based from the factors that is identified from literature review on previous related studies and online survey result. This proposed awareness guidelines on phishing attempts also can be ideal for security awareness programs and training specified for students.

Keywords: Phishing; Phishing Attacks; User Awareness; Students

1. Introduction

According to [1] stated that, during 1st January until 20th, Anti Phishing Alliance of China (APAC) handled 24,535 phishing websites in total and by 20th November 2012, APAC had confirmed and handled 100,402 phishing websites in total. This report has clearly shows that the fast grow of internet attack especially on phishing attack within a year.

There are many types of online attacks and one of the famous online attacks is phishing. Phishing attacks exploit emails or malicious websites to seek personal information by posing as a truthful party. In this case, an attacker may send email allegedly from a trustworthy organization or financial institution that requests account information and when users act in response with the requested information, attackers can use it to gain access to the account [15].

Basically, phishing involved with two time scam, firstly it steals a company’s identity and then use it to victimize consumers by stealing their credit identities. The term Phishing (also called spoofing) comes from the fact that Internet scammers are using increasingly sophisticated lures as...
they "fish" for user’s financial information and password data [8]. Surprisingly many of the phishing attack victims may never realise that they have been attacked. Moreover, countless of these refined attacks are targeted on small scale and thus it is expected that they have not reported and captured.

Besides that, according to [2] notifies that there are total of 9,986 cybercrime incident reported for the first 3 months of the 2013 itself. Thus, this had led to a problem where the safety of the online user being questionable. Secondly, a phishing awareness research was done among participants aged between 18 to 46 and the results showed that the participants in the 18-25 age groups were more likely to fall for phishing than those in older age groups [3]. Hence, an effective awareness guideline specifically for phishing attacks for students are needed to secure a healthy internet environment our next generation. Therefore, this paper focuses on identifying the level of user awareness on phishing attempts among students and proposed appropriate phishing awareness guidelines specifically among students.

This paper is organized into five sections. The next section describes the related works in this research. Section 3 explains a research method that is used in this research. Section 4 presents the results of the studies followed by conclusions in section 5.

2. Related Works

Studies on related works are broken down into three categories, which are the overview of phishing attempts, user awareness on phishing attempts and about the existing phishing awareness guidelines.

2.1 Definition and Description of Phishing

“Phishing” refers to mass amounts of spam e-mails that typically includes urgent language or a persuasive offer, and are sent by cyber criminals in an attempt to elicit a response from recipients [4]. In this statement the author defines that phishing appears in a form of spam to trick the user to become a victim. Moreover, phishing can be in any electronic form where it will trap the victim by imitating as the original thing. Phishing also known as a form of electronic deception in which an attacker tries to cause the recipient to do something or disclose data that they likely would not normally do by mimicking a trustworthy entity [5]. Phishing can be a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information [6].

Phishing attacks were described more precisely by [7] in six ways as listed below:

1) A malicious email (or an instant message) which pretends it is from a legitimate company but it contains some links which are from the attacker website. In most cases, the attacker manipulates the email header to change the sender to a legitimate one.

2) A malicious email (or an instant message) that deceives people into sending their information for the attacker.

3) A fake website which accepts donation for charities but it is actually the phisher’s website.

4) A fake website with the similar content as the legitimate website and a homogeneous domain name address such as “payepal.com” or “secure-paypal.com” instead of “paypal.com”.

5) A malicious message which guides the victim to one page of the legitimate website which has vulnerability such as “XSS4”. And by using that page, the attacker steals the victim’s confidential information.

6) Attacker fools the victim to setup a malware which is called “crimeware”. This program redirects the important websites, such as “ebay.com”, to the attacker website (for instance by changing the local DNS) or steals the user’s information via the web browsing directly (for instance by adding a small JavaScript to all of the web pages).
### 2.2 User Awareness on Phishing Attempts

Awareness focuses concentration on security and is intended to permit individuals to be familiar with security concerns and respond accordingly. Therefore to make the users to be aware of the threat they are about to deal with and in order to encourage them in avoiding those risks, users must be initially exposed with awareness in the information security.

Besides that, trust was one of the main factors that trapped the user whereby they believe the phishing email that they received is from genuine person/organization. Trust, like risk, has been discussed for several decades and has been analyzed in such social science literatures as psychology, sociology, political science, anthropology, history, socio-biology and economic [8]. It is basically an action done without hesitation or no awareness.

Apart from that, [9] conducted a web based survey where they developed 50 phishing and legitimate website survey scenarios which were collected from the APWG’s archive. Only 30 out of the 50 were phishing websites and the rest were legitimate. The main intention of their survey was to identified regular phishing hints and signs that become visible in the scenarios, to determine what aspects of a website effectively express authenticity to their employees, and to try to classify which malicious strategies and attack techniques are doing well at misleading general users, and why (Alnajim and Munro, 2008) [10].

From their experiment, they tried to conclude the efficiency and the importance of implementing security training awareness and phishing courses or classes about phishing threats and detection expertise. They have outlined 27 phishing website factors and features which were all deliberately circulated randomly across the 30 phishing website scenarios. One phishing scenario could have more than one factor or feature and one phishing factor could appear in many phishing scenarios.

From the research, they concluded that most of the participants that are untrained on security awareness fail to recognize some of the very noticeable phishing clues or indications like address bar contents, page contents, domain name, page style, URL and security indicators like SSL certificate or logos. The majority of their choices and decisions determined on the interface of the website and its colors, pictures and animation style, as a consequence taking sides the influences.

Besides that [11], conducted a study to investigate the impact of Saudi Arabian users’ individual factors on their ability to detect phishing emails. The findings propose that there are a range of individual factors based on the four modal studies they used. These factors are users’ personality traits and susceptibility levels. Users with extraversion, openness, and high susceptibility are more likely to execute the action in the phishing email. This may be for the reason that these types of users have more confidence in themselves. [12] also found four important factors in the vulnerability to phishing emails namely: involvement, email load, knowledge, and computer self-efficacy.

[13] highlight same studies among student which are in military academics. In this academic all the new cadets are required to attend a four hours class on information security. To experiment the success of the class, randomized phishing email were sent out to cadets whereby it included the senior cadets as well. The phishing email states that they have a problem in their grade and required the cadets to click on a links to view their grade. The result of the experiment shows that eighty percent of all cadets clicked on the attached link, while ninety percent of the victims were the freshmen. This clearly shows that the factor of urgency blind their knowledge on avoiding the phishing links. The cadets were basically worried that there was a problem on their grade and without further thoughts they click on the link. Therefore it is important to have a proper exposure
on phishing attempt awareness and it clearly shows that a four hour class on information security will not guarantee the safety of online users.

### 2.3 Existing Phishing Awareness Guidelines

There are many security awareness guidelines available for internet users and these guidelines are easily accessible through online. Users are able to view all the available guidelines that are proposed all around the world. This section presents on few selected existing phishing awareness guidelines as shown in Table 1.

<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
</table>
| CYBERSECURITY MALAYSIA - Guidelines on Computer Security [14] | • Type the URL of your Internet Banking or Online Shopping website (instead of clicking the link from an unsolicited email).  
• Check the lower right-hand corner of the browser for a lock icon. (This lock icon will appear when the site is using a secure HTTP and is verified to be legitimate. You can double-click the lock icon to verify the website.)  
• Install an anti-phishing toolbar. (These toolbars are freely available to help combat phishing scams. These tools usually come in the form of web browser extensions. Some examples are Mozilla Firefox 2, Internet Explorer 7, and Netcraft.)  
• Install anti-virus software and enabled the ‘automatic update’ option.  
• Report the incident to MyCERT and the respective banking institution/online shopping website. |
| THE FEDERAL TRADE COMMISSION UNITED STATES OF AMERICA - Phishing Action Steps [15] | • Don't email personal or financial information. Email is not a secure method of transmitting personal information.  
• Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.  
• Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.  
• Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. |
| INFORMATION SECURITY EDUCATION & AWARENESS, DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA - Guidelines for using e-Mail safely [16] | • Use e-mail filtering software to avoid spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.  
• Do not open attachments coming from strangers, since they may contain a virus along with the received message.  
• Be careful while downloading attachments from e-mails into your hard disk. Scan the attachment with updated antivirus software before saving it.  
• Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.  
• Avoid sending personal information through e-mails.  
• Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-mail.  
• Do not click on the e-Mails that you receive from untrusted users as clicking itself may execute some malicious code and spread into your system. |

From these three guidelines sources, the main issues stressed are on avoiding sharing personal information via online to untrusted parties, clicking on the link embedded in the email and install anti-virus as well as anti-phishing toolbar.

### 3. Research Methodology

In this research mixed method which both qualitative and quantitative method are used.
3.1 Phase I: Quantitative Method

Quantitative research requires that one either simply study the counts of events/people/things or that numeric labels be created for meaningful events, experiences and actions [17]. In this research, the data gathering will be done by survey which is expected to provide an immense research and feedback information.

Survey is one of a method of data gathering which is easy on the pocket, and express. Therefore it would be very appropriate method for small to medium research. Furthermore, survey has a flexibility of gathering vast information in a very short of time.

Therefore for this research, an online survey will be conducted rather than hard copy survey. Online survey is an elucidation which solves the allocation and collecting the result in a good approach. Therefore, in order to identify users’ level of awareness in handling phishing attempts among students, a total of 120 online surveys were distributed randomly among students from four higher institutions in Malaysia.

3.2 Phase II-Qualitative Method

The second data gathering that has been chosen is qualitative method which is interview method. Qualitative research methods provides more emphasis on interpretation and providing consumers with complete views, looking at contexts, environmental immersions and a depth of understanding of concepts [17]. Just as in everyday life, one of the most productive way to learn about a person, place, or set of activities is to actually ask questions of people who have knowledge about that topic [17].

Therefore, interview data is more affluent than quantitative data in a way the researcher will know how the interviewees interpret something. Moreover, a clear view on the topic discussed can be gained. In short, while quantitative methods produce data that can be aggregated and analyzed to describe and predict relationships, qualitative research can help to probe and explain those relationships and to explain contextual differences in the quality of those relationships [18].

This method of data gathering would be so valuable and essential since this interview will be done with Information Security Officer who is an expert in dealing with phishing attempts. Experts, the highest rank users have the illusion of always making the correct decision, and effortlessly master the problems in their area of specialization [19].

Therefore in these context, the Information Security Officer expert are those who handles phishing attempts and making decision to overcome it on their daily work. There are many ways an interview can be done such as via phone, email, live chat and face to face chat. In this research face to face interview will be conducted with three information security officer expert. These three Information Security Officer are a Security Consultant, a Security Engineer and a Security Analyst whom have faced, deal and come up with proper solution on phishing attempts. This face to face interview will help in the planning of appropriate awareness guidelines for targeted users. The interviewee can share their ideas and knowledge about the phishing attempt and the perceptive or even the feedback gain through the interview can be helpful to design appropriate proposed guidelines.

3.3 Research Procedures

This research is conducted according to the process as follows, it contains five stages namely literature review, formulation of questionnaire, data collection and analysis, evaluation and documentation as shown in Figure 1.
Stage 1: Conduct the literature review
A literature review will be carried out to understand the prior researches and issues that related to user awareness on phishing attempt among students. During phase is the general information about phishing and user awareness are collected, the review should illustrate, recapitulate and estimate, based on literature review, it should give an idea for the research and conclude the scope and track of the research.

Stage 2: Formulation of Questionnaire
During this phase the formulating and designing of questionnaire will take place. A study will be conducted on previous existing studies and related questionnaire to identified criteria needed for the questionnaire on phishing attempts. Finally, a proper questionnaire will be formulated based on candidate’s criteria.

Stage 3: Data collection and Analysis
Data will be collected with mixed method. First through a survey by online based questionnaire, the data will be collected among students in four different academic institutions, these data involves in understanding user’s response on phishing attempt, how they compare between legitimate and illegitimate phishing website/email/URL and the factors that influence them to get trapped. The feedback of the questionnaires will be analysed. The result data will be analysed in this phase. It is necessary to have an analysis on the result, through the analysis, we can illustrate a practical
understanding to the proposed guidelines, and moreover, the analysis result is essential for the future research.

Stage 4: Evaluation

The data collected from the web based survey will create a baseline to propose appropriate awareness guidelines in order to prevent phishing attempts. These guidelines will be evaluated by second types of data collection method which is through interview. Three experts in handling phishing attempts from selected Security Analyst will be interviewed and possible suggestion given throughout the interview will be used in the development of the proposed guidelines.

Stage 5: Documentation

This is the last process to be done. Every bit of information starting from phase 1 to phase 5 will be documented in a complete report. It will record all the information, process, methods, data, analysing result and other related parts of the research.

4. Result

In order to identify users’ level of awareness in handling phishing attempts among students, a total of 120 online surveys were distributed randomly among students from four higher institutions in Malaysia. Out of these 120, one hundred thirteen (113) had responded to the survey. The respondents were from Information Technology (IT) background. Based from the questionnaire results, it was clearly showed that almost half of users are unaware about phishing. Although more than half of the respondent answered that they heard about phishing but they failed to identify the illegitimate website, email and URL (Uniform Resource Locator).

The level of user’s awareness on phishing attempts or in this case the level of student’s level of awareness towards phishing awareness is low. This is because from overall result on identifying the legitimate and illegitimate website and emails for the six images, more than half of the respondents on average were able to detect the correct answer.

Moreover, for the URLs detection on average more than half (66.4%) of the respondent are able to response correctly. At the same time, based from the six images only two of the images have more than half respondent detect correctly. Besides that 49.5% of total respondents admit that they are unaware on new phishing threats. Finally, the proposed guidelines as shown in Table 2.
Table 2. Proposed Phishing Awareness Guidelines.

<table>
<thead>
<tr>
<th>AWARENESS GUIDELINES ON PHISHING ATTEMPTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td>1) Do not respond to any email asking for personal and private information such as User Id, Password, Account Number and so on.</td>
</tr>
<tr>
<td>2) Do not click on the link in the email message if you suspect the message might not be authentic. Instead, contact the company on the telephone, or log onto the website directly by typing in the Web address in your browser.</td>
</tr>
<tr>
<td>3) Do not cut and paste the link that came in the email message.</td>
</tr>
<tr>
<td>4) Avoid filling out forms in email messages that ask for personal confidential information.</td>
</tr>
<tr>
<td>5) Always be suspicious of any email with urgent request for personal confidential information.</td>
</tr>
<tr>
<td>6) Do not fall for a phishing scam just because you trust the &quot;sender&quot; of the email, as it is easy for a spammer to forge the sender's name.</td>
</tr>
<tr>
<td><strong>Website</strong></td>
</tr>
<tr>
<td>1) Always be aware that a phishing website will have the same layout or design which looks like the genuine website.</td>
</tr>
<tr>
<td>2) Always check for a lock symbol in the browser bar.</td>
</tr>
<tr>
<td>3) Make sure the website URL starts with &quot;https.&quot;</td>
</tr>
<tr>
<td>4) Make sure the website URL are the correct and does not contain any suspicious link.</td>
</tr>
<tr>
<td><strong>Other Important Notes</strong></td>
</tr>
<tr>
<td>1) Regularly update and patch your Web browser(s).</td>
</tr>
<tr>
<td>2) Never download software or files from an unknown source; they might contain phishing Trojans.</td>
</tr>
<tr>
<td>3) Manage well configured personal anti-virus and anti-spam software on the computers.</td>
</tr>
<tr>
<td>4) Regularly log into your online accounts, and check your statements.</td>
</tr>
<tr>
<td>5) Do report to your respective bank or credit card providers if you see any suspicious transactions.</td>
</tr>
</tbody>
</table>

5. Conclusion

Education in online security plays a key role in increasing user’s awareness towards security threats. Thus, good user security education should not only increase users’ alertness, but also teach them how to distinguish threats from non-threats [3]. Therefore, this research highlighted the importance of a student’s getting proper awareness education on online security threats and how to guide them in raising their awareness.

Hence, from these guidelines students are expected to have a basic knowledge on this phishing attempts and are able to identify legitimate and illegitimate website or email. Furthermore, the
education institution also should pay more attention in educating the students on online threats. A simple training or awareness program is essential for the students. As a conclusion, students should be more aware on phishing attempts. In order to do so, students should be exposed to awareness program or training and must always be updated on the current online threats.

References