Phishing Attack Protection (PAP) Approaches for Fairness in Web Usage

Mohiuddin Ahmed[1], Jonayed Kaysar[2]

[1] Department of Computer Science and Information Technology, Islamic University of Technology Board Bazar, Gazipur-1704, Bangladesh

[2] Department of Computer Science and Information Technology, Islamic University of Technology Board Bazar, Gazipur-1704, Bangladesh

Abstract

Phishing scams are considered as a threat issue to all web users. But still the web users are not consciously aware of this fact. Many research works have been done to increase the phishing awareness among the users but it is not up to the mark till to date. We have conducted a survey among a diversified group of people who are active user of internet. And then analyzed the existing phishing warnings provided by the web browsers and protection schemes, in this paper we have suggested new approaches i.e. sending notifications to user, checking URL, creating user alarms and security knowledge to ensure fairness in web usage.

Keywords: *Phishing, Design, Warnings, Usable Privacy & Security, Spoof, Phisher.*

1. Introduction

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy and America Online[9]. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait.

Suppose you check your e-mail one day and find a message from your bank. You've gotten e-mail from them before, but this one seems suspicious, especially since it threatens to close your account if you don't reply immediately. What do you do? This message and others like it are examples of phishing, a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses and convince people to participate unwittingly in money laundering.

2. A Statistics of Scams

In 2010, RSA[3] witnesses a total of 203,985 phishing attacks launched. As compared to the total in 2009, this marks a 27 percent increase in phishing attack volume over the past year.

Top Ten Countries by Attack Volume

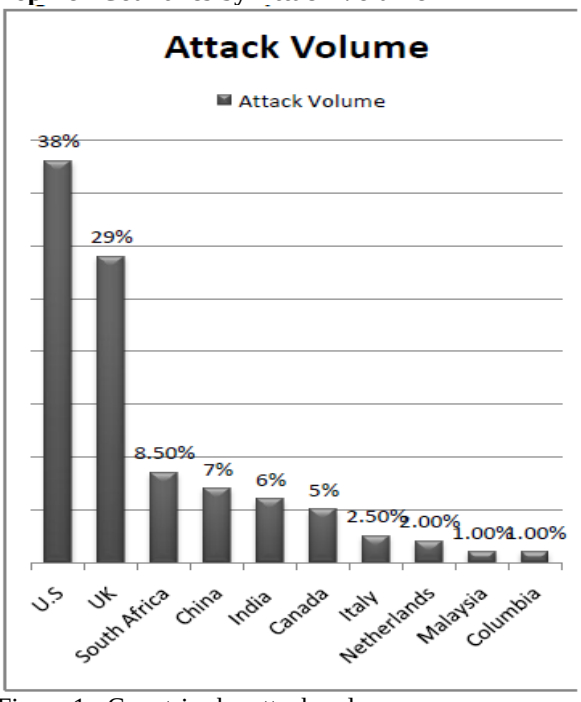

Figure 1 : Countries by attack volume

3. State-of-the-art Web Browsers

The state-of-the-art web browsers have included active warnings, which coerce users to notice the warnings by interrupting. We will consider most favorite browsers i.e. Microsoft's Internet Explorer and Mozilla Firefox. IE 9 includes both active and passive warnings. Upon observing a confirmed phishing site the browser will display an active warning message in full screen with URL bar colored red[10]. For passive indication IE 9 will show a popup dialog box while sensing the site as suspicious[10].

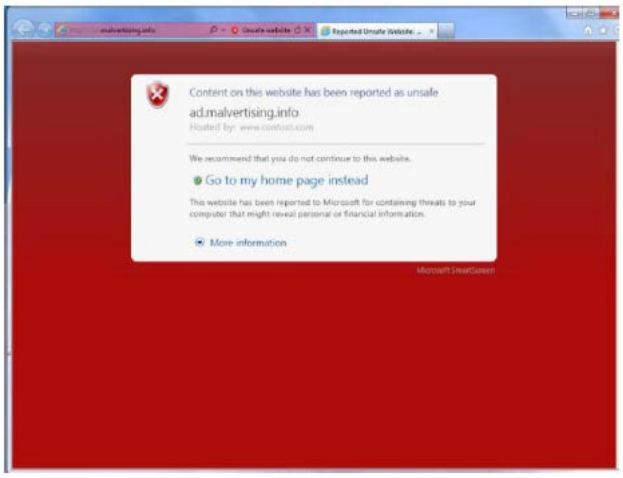

Figure 2 : The active Internet Explorer 9.0 phishing warning[10]

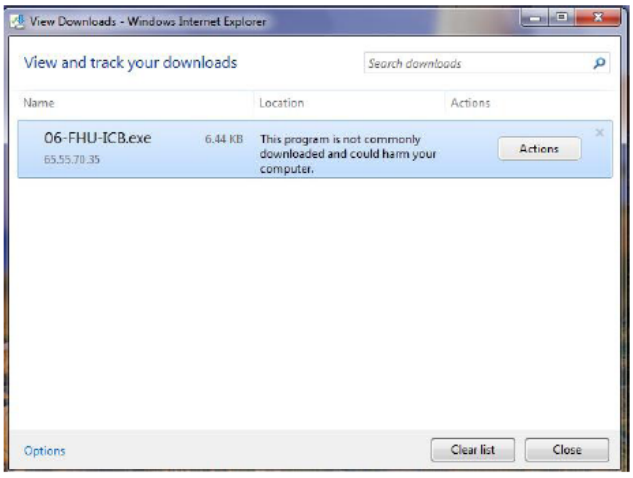

Figure 3 : The passive Internet Explorer 9.0 phishing warning[10]

Firefox 6.0 also includes active cautionary. When a user confronts a phishing site, a non-interactive dimmed version of the site is shown with a dialog box given choices for continuing or leaving the site[11].

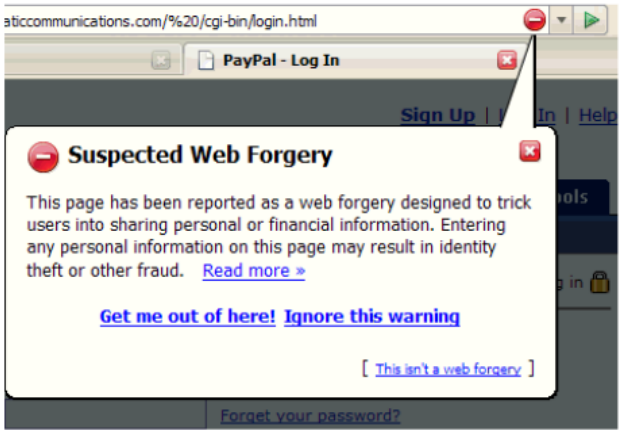

Figure 4 : The active Firefox 6.0 phishing warning[11]

This paper has two contributions. At first, the phishing awareness level of web users is surveyed. And then analyzing the stat-of-the-art web browsers phishing warnings and other approaches it recommends phishing attack protection (PAP) approaches to help users handling the online frauds.

4. Related Works

There have been extensive surveys about phishing awareness to identify the user knowledge on phishing. In [1] the work has simulated a spear phishing attack to expose users to browser warnings. But interestingly enough 97% of the participants fell for at least one of the phishing messages sent to them. And then they used active and passive warnings to find out how the users reacting on that situation. Basically they have used a model form warning science to identify the user reaction and offered suggestion for making more efficient phishing warnings. Another study in [2] shows that the users after having training are less likely to fell for the attacks. The study evaluated the effectiveness of PhishGuru training in field trails and found that generic training materials are more effective than spear phishing training materials.

Even the unaware users of web can be helped not to be in a trap by Client Side Phishing Protection[4]. In this paper they have provided two approaches by which user will be able to identify whether phishing attack is there or not. Their work focused on browser extension which has a limited range and valid for online-banking.

Another approach was based on visual cue. The solution provided by Dhamija et al.[5] consists of dynamic security

skin in the web browser. Here a remote server has to prove its identity in a way that is efficient for human users to examine and cumbersome for phishers. The problem with this approach is that the users must be educated enough about phishing scams.

We considered the last approach in our related work is flow of information based approach. PwdHash[6,7] has been considered as a favorite anti-phishing solution. Which creates passwords for domains like, a password for www.yahoomail.com will be different if it is input to www.attacker.com. Comparing this approach with AntiPhish[8], which keeps eye on sensitive information. Whenever classified information is used in mistrusted websites then a warning is generated and consequent operations are canceled, that means the user should be always vigilant about the information being input in various websites.

5. Questionnaire

We used a set of questions to know that how much knowledge web users are possessing and based on that we work toward designing new approaches. We collected feedback from one hundred users to identify the specific arena where to emphasize for developing new phishing attack protection approaches.

- **What is your internet usage per day?**

We wanted to know how much time a user spends on the web to measure how vulnerable one individual is.

- **Do you prefer online shopping?**

Most of the phishing attacks are placed on online shopping and credit card transaction based. So, this question helped us understanding the scope of a user being cheated.

- **What is your favorite browser?**

Browsers are also creating protection approaches where a user having no idea about phishing might help him/her from being ripped off.

- **Phishing awareness level**

We extracted the level of knowledge about phishing in this question to judge the real life scenario of web users.

- **Do you feel insecure to use internet for phishing attack?**

This question let us know how much a user is worried about phishing attacks and whether users feel insecure over web space or not.

- **Is your browser able to defense phishing attack?**

This tells us whether user is known about phishing or not and whether his/her browser is able to notify any phishing.

- **Did you face any phishing attack?**

This is to know how experienced a user is about being jockeyed.

- **Do you know someone who has financial loss due to phishing attack?**

Awareness of financial losses claimed the information about phishing attacks are disseminated among peer groups and thus being aware of it.

6. PAP Approaches

Here we are suggesting some approaches considering the user knowledge on phishing and the state-of-the-art web browsers. Our proposed approaches will help the users to be more aware of phishing and thus ensure fairness in web usage.

6.1 Sending Notification to User

When a mail or any message from bank or any other financial organization or any credit card payment gateway is sent to the client that organization needs to send a notification to the client's cell phone as a sms. In this era of smart phones, sending notification by sms is the most simple and reliable solution. For this reason, the client phone number should be synchronized with the organization. Whenever there is a mail sent from the organization, the automated system sends a sms momentarily. This will help the clients to understand that the mail is generated by the original organization. And for attackers, it is not possible to send automated notification to the targeted victim's cell phone.

6.2 Checking the URL

An extension can be developed which will check the URL on behalf of the user. It will check the URL and search for the matches of the URL with default search engine of the browser. If the URL matches, then it checks the domains

and sub domains. Now if the sub domain and other part of the URL matches with another domain, then it will generate a message. Most of the time, sub domain is used to create attack. So, if there is a notice, user will check the sub domain itself.

6.3 Creating User Alarm

There should be database of the phishing sites and browsers should always sync with the database. Currently, an alert is given if a site contains malware and same alerts can be created for those phishing sites. When there is an alert, user have to be cautious about the site.

6.4 Check the Redirection

Most of the users are not aware about the redirection. Although browsers like Firefox have the option to show an alert during redirection, nobody cares. This is a vulnerable thing. Redirection should be checked and if the redirected site is not trustworthy, then an alert will also appear and closes the window as well as adding the site with the central phishing database.

6.5 Increase Security Knowledge

The users are the victim and from our survey we found that many of them have heard the term "phishing" but they don't have any clear concept about it. This situation can be improved by increasing security knowledge. Financial organizations like Banks, Insurance companies can organize some weekly/monthly event for their clients where the latest news and views of internet security will be presented. Beside these events, there must be some tutorial(written/video) with the browsers which will teach the users about phishing. As many people will not find enough time to check that tutorial, it can be made mandatory while installing the browsers to watch the tutorials first.

7. Conclusion

Phishing attacks are causing huge financial losses to individual and group. A number of professional and academic protection approaches have been proposed to date. But still there are very less improvement. So, it's the only way when the users are cautious about this issue and thus oriented approaches provided by us in this paper can help to block this burgeoning problem in today's IT world. In our future work, we will be implementing more novel approaches which will supersede the existing approaches for combating phishing attack.

References

[1] Serge Egelman, Lorrie Faith Cranor, Jason Hong. You 've Been Warned: An empirical Study of the Effectiveness of Web Browser Phishing Warnings. CHI 2008,April 5-10,2008,Florence,Italy.
[2] Lesson From a Real World Evaluation of Anti-Phishing Training. ACM Conference'04,Month 1-2,2004.
[3] RSA online fraud report,2011. www.rsa.com
[4] Venkata Prasad Reddy, V.Radha,Manik Jindal. Client Side Protection from Phishing Attack,IJAEST 2010, vol-3,issue-1.
[5] R.Dhamija and J.D Tygar. The battle against phishing: Dynamic Security skins. In Proceedings of the 2005 symposium on Usable Privacy and security,Newyork,NY,pages 77-88. ACM press, 2005.
[6] B.Ross, C.Jackson,N.Miyake,D.BBoneh and J.C.Mitchell. Stronger password Authentication Using Browser Extensions. In 14th Usenix Security Sumposium,2005.
[7] B.Ross, C.Jackson,N.Miyake,D.BBoneh and J.C.Mitchell. A Browser Plugin Solution to the Unique Password Problem. http://crypto.stanford.edu/PwdHash/,2005.
[8] E.Kirda and C.Kruegel. Protecting Users against Phishing Attacks. Yhe Computer Journal,2006.
[9] www.yahoo.com, http://www.aol.com/, www.bestbuy.com, www.msn.com, www.paypal,com, www.ebay.com
[10]http://windows.microsoft.com/en-US/internet-explorer/products/ie/home
[11] http://www.mozilla.org/en-US/firefox/fx/

Mohiuddin Ahmed is a final year undergraduate student in Islamic University of Technology, OIC at Computer Science & Information Technology Department. Research interest includes Human Computer Interaction, Artificial Intelligence, Data Mining and Knowledge Management.

Jonayed Kaysar is also a final year undergraduate student in Islamic University of Technology, OIC at Computer Science & Information Technology Department. Research interest includes Web Engineering, Wireless Network, Human Computer Interaction and Peer to Peer overlay networks.