A Study and Performance Analysis of Browser based Anti-Phishing Tools; An Experience Report

Rajendra Gupta[1], Dr. Piyush Kumar Shukla[2]
[1]BSSS Autonomous College, BU, Bhopal (M.P.) India.
[2]University Institute of Technology, RGTU, Bhopal (M.P.) India.

ABSTRACT
The anti-phishing tool is said to be ideal, when it is giving accurate, timely result and conspicuously identify phishing websites that user visit. In this paper, popular anti-phishing filter tools are discussed with their functionality. The performance of the anti-phishing tools can varies on the source of URL used for testing method. A browser based anti-phishing system model is proposed to protect the user from phishing attack. In the proposed system, the Add-on tool sends the collected information to the main server which is again categorised in five assigned servers on their functionality. The outcome of the proposed system is showing around 96 percentage successful results after a series of experiments. The proposed system checks and gives the result for all accessed websites.

Keywords **:** Phishing, Anti-Phishing, Add-on, Classification Algorithm, Anti-Phishing Toolbars

I INTRODUCTION

The web browser provides the facility of development and installation of add-on tool in its framework. The user access any web site by using web browser only, so the web browser based system should be developed to aware the user about phishing attack. Some web browsers are already providing the alert system for possible malicious attacks. If the website is not having HTTPs protocol and the user is feeding their credential information on it, the web browser shows the alert message to the user about the possible phishing attack. If the website is suspicious then the web browser checks the security certificate whether it is present in the website or not. After checking the security certificate, the web browser alerts the user about possible problem in the website.

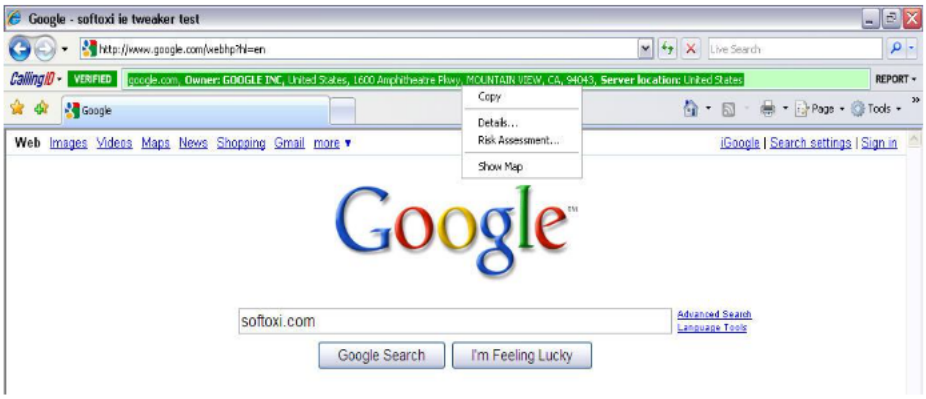
This chapter is based on the anti-phishing tool development, its design and development model. In the proposed anti-phishing tool, the research criteria are based on the URL, content and image matching. All about the add-on development and its working procedure with their screen shots and source code are given for the clear understanding of the anti-phishing tool's working procedure.

II EXISTING ANTI-PHISHING TOOLS

There is a number of anti-phishing approaches proposed earlier to identify a web page as a phishing or not. In this section of study, I have studied the functioning and system details of different earlier proposed anti-phishing tools. Public views and available information related to these tools is collected which is given in the tools downloading web sites. Apart from this, I have observed the basic understanding of how each tool is functioning. The earlier tools are trying to protect the user's confidential information but it is seen that these tools are not completely showing successful results. Mostly tools have defined that legitimated sites are defined as white lists also known as safe sites and the fraudulent sites are defined as blacklists. The proposed method which is used in this research study uses various previously defined concepts. The tool for anti-phishing is developed with the use of publicly available information and the list of phishing and legitimate website details. The description of various anti-phishing tools are described below [1] :

(a) Calling ID Toolbar- CallingID is an anti-phishing tool which focuses on the site ownership details and real-time rating and confirms the user that the site is safe to provide information. This toolbar checks 54 different verification tests for checking the legitimacy of a given site. CallingID directly attacks on the root cause and source of the web usage exposures. The tool uses visual indicators in its toolbar to check the kind of website. These indicators shows different colours for differentiating the web page, just like green colour represent a known-good site; yellow colour represent a site that is "at low risk;"; red colour represent a site that is "at high risk," means most probably be a phishing site. Some of the heuristics used include examining the site's country of origin, length of registration, user reports, popularity of the website and the blacklisted data. The Calling ID Toolbar runs on Microsoft Windows 98 / NT / 2000 / XP with Internet Explorer [2] web browser.
The internet user exposed to fraud and PC damage whenever the user don't know whose site he is visiting. In other words, the user should always know who he is providing information to and

buying from. The snapshot of the Calling ID Anti-Phishing Toolbar is shown below :

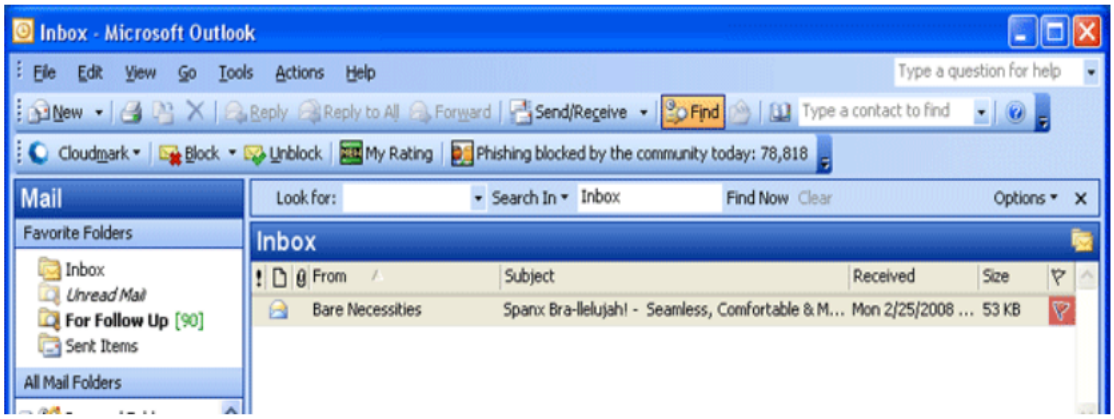


Source : http://www.softoxi.com/callingid-video-trailer-screenshots.html

Calling ID is having extensive data sources record and a delivery model enabling us to ensure our safety without bogging down our system [18].

(b) Cloud mark Anti-Fraud Toolbar- The Cloud mark Anti-Fraud toolbar is one other type of anti-phishing toolbar which is based on the users rating [8]. In this toolbar, the user has a right to report the site that is should be accessible or not. On the basis of this feature, the toolbar display a coloured icon on the web browser for each site visited by the user. The green colour icon indicate that the site has been rated as 'legitimate', red colour icons indicate that the site has been determined to be 'fraudulent', and yellow colour icons indicate that not enough information is known to make a determination. Additionally, the user themselves are able to rated site according to their record of correctly identifying phishing sites. Each site's rating is computed by aggregating all ratings given for that site. Each user's rating of a site weighted according to that user's reputation. In the toolbar, no other heuristics are used in determining a site's rating. The functioning of the toolbar is that the sites determined to be fraudulent are blocked and users are redirected to an information page which gives the option of overriding the block.

The Cloud mark Anti-Fraud Toolbar runs on Microsoft Windows 98 / NT / 2000 / XP operating systems with Internet Explorer web browser. In this study, it is noticed that the Cloud mark is no longer supporting the web browser toolbar. The snapshot of the Cloud mark anti-phishing toolbar is shown below :



Source : http://cloudmark-anti-fraud-toolbar-for-microso.software.informer.com/

(c) EarthLink Toolbar- The EarthLink Toolbar approach is based on two combinations of heuristics, user ratings and manual verification [3]. It shows very little information on the EarthLink website. The toolbar display the suspected phishing sites information to the user. These sites after analysis are then verified and added to a blacklist. The toolbar also focuses on the domain registration

information such as the owner, age and country. The toolbar displays a thumb that changes the colour and position. A green thumb up represents a verified legitimate site whereas a grey thumbs up represent that the site is not suspicious, but it has not been verified. The red thumbs down means that a site has been verified to be fraudulent, whereas the yellow thumbs down means that the site is "doubtful." The tool blocks the sites if it is found to be fraudulent. In this case users are redirected to an information page and given the option of overriding the block.

The EarthLink Toolbar runs on Internet Explorer as well as Firefox [3]. The snapshot of the EarthLink is shown below :

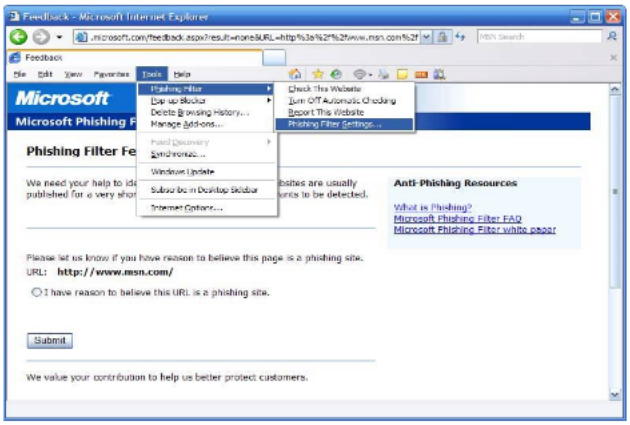
Source : http://www.mccd.edu/myhelp/pop-ups/earth/image001.jpg

(d) eBay Toolbar- The eBay Toolbar is also an anti-phishing tool that uses a combination of heuristics and blacklists [4]. It uses Account Guard indicator that is having three modes: green, red, and grey. If the user operated the eBay (or PayPal) website, the icon is displayed with a green background. The red coloured icon is displayed as a background when the site is a declared phishing site. The icon is displayed with a grey background when the site is not operated by eBay and which is not known to be a phishing site. The information related to known phishing sites blocked and a pop-up appears on the screen which gives the option to the user to override the block. The toolbar also gives users to be able to report phishing sites, which can be verified before being blacklisted. The eBay Toolbar runs under Microsoft Windows 98 / ME / NT / 2000 / XP with Internet Explorer web browser. The snapshot of the ebay toolbar is shown below :

Source : http://download.chip.eu/en/eBay-Toolbar_110514.html

(e) Firefox Toolbar- Firefox toolbar contains a feature that is designed to identify fraudulent web sites. For the Google Safe Browsing Toolbar, system tool is designed which is an optional extension for Firefox. URLs are checked against a blacklist, which Firefox downloads periodically [5]. The toolbar feature displays a popup if it is suspected that the visited site to be fraudulent and present the message to the user to choice leaving the site or ignoring the warning. Optionally, the feature sends each URL to Google to determine the likelihood of it being a scam. According to the Google toolbar downloading site, the toolbar combines "advanced algorithms with reports about misleading pages from a number of sources [6]." The Firefox runs on Microsoft Windows, Apple Mac OS X, and Linux operating systems. The Google Safe Browsing Toolbar on which this functionality is based runs on Microsoft Internet Explorer under Windows XP/2000 SP3+, or Firefox on most platforms.

(f) Microsoft Phishing Filter in Windows Internet Explorer 7- The Microsoft Internet Explorer 7 web browser uses anti-phishing which is based on phishing filter [7]. The tool is basically relies on a blacklist hosted by Microsoft. Apart from this, the tool uses some heuristics when it encounters a site that is not on the blacklist category. If the visiting site is found suspected phishing, website is encountered the user is redirected to a built in warning message and ask the user whether he would like to continue visiting the site or not. Users also have the facility to choose the option to report suspected phishing sites or to report that a site has incorrectly been added to the blacklist. The snapshot of the Microsoft Internet Explorer 7 web browser Anti-Phishing Toolbar is shown below :

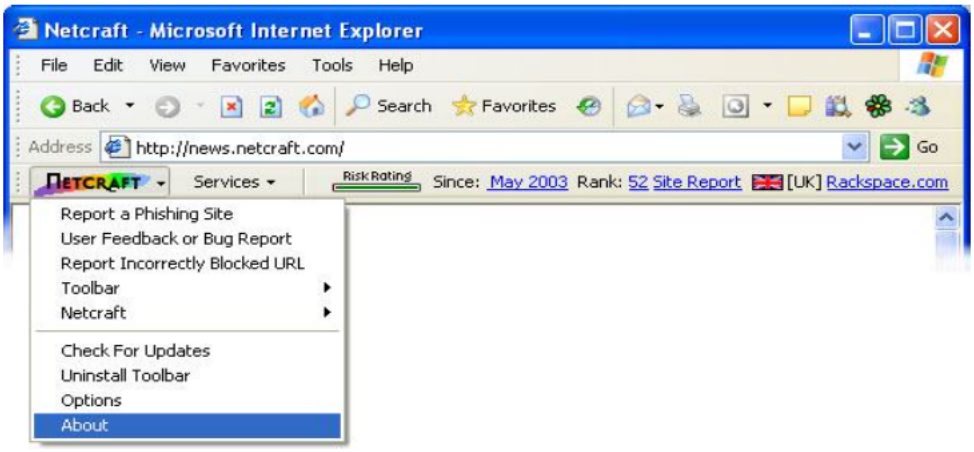


Source: http://winsupersite.com/product-review/internet-explorer-7-beta-1-review

(g) Net craft Anti-Phishing Toolbar - The Net craft Anti-Phishing Toolbar uses several methods to determine the website is legitimate or not [8]. Its website explains that the toolbar (a) clearly depicts sites' hosting location including country which can help you to evaluate spoofing URLs (b) it enforce the display of browser navigation controls (i.e. tool & address bar) in its windows, to defend against popup windows and (c) traps suspicious URLs which contains characters that have no common purpose except to deceive.

The Net craft toolbar also uses a blacklisting, which contains the record of fraudulent sites identified by Net craft and also the sites submitted by users and verified by the company. When a user hit the blacklisted website, a pop-up warning recommends that the access be cancelled, but also provides an override option. The toolbar also displays a 'risk rating' option among the user as well as the hosting location of the site. Users can also use the toolbar to see the more detailed report on a web site.

The Net craft Anti-Phishing Toolbar runs on Firefox mostly and on Microsoft Internet Explorer for Windows 2000/XP operating system. The snapshot of Net craft Anti-Phishing Toolbar is as shown below:

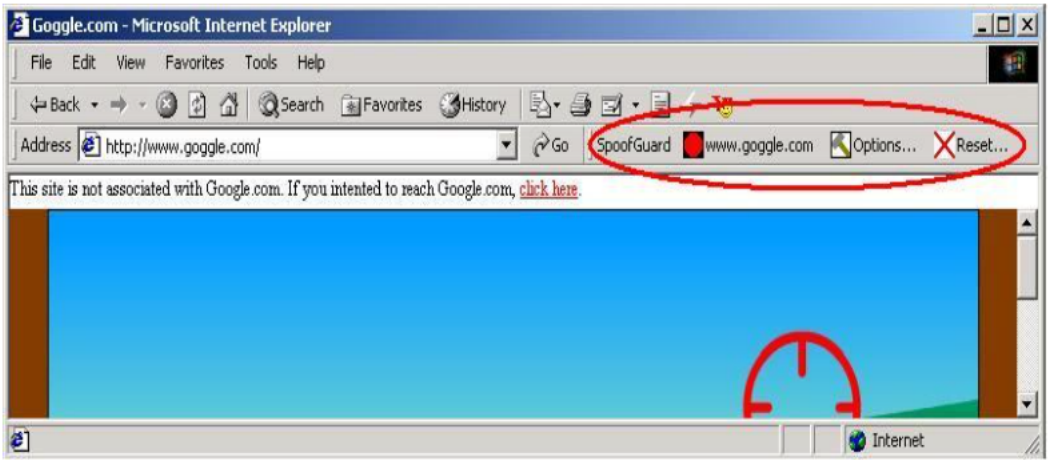


Source : http://www.static.flickr.com/42/123062502_98f75c4f9e.jpg?v=0

(h) Netscape Browser 8.1 - The Netscape Navigator 8.1 web browser uses built-in phishing filter [8,9]. For the testing of the tool as well as the third party reviews, the functionality is the based on blacklisting, which is maintained by AOL and updated frequently [10]. A warning message is appeared on the screen when a suspected phishing site is encountered. The users are shown the original URL and are asked whether or not they would like to precede the website. The Netscape Browser runs under Microsoft Windows, Linux, and Mac OS X. The snapshot of the Netscape Anti-Phishing Toolbar is shown below :

Source: http://www.yevol.com/en/windows/images/browser2.gif

(i) Spoof Guard- Spoof Guard is a tool to which help user to prevent a form of malicious attack called "web spoofing" or "phishing". The phishing attacks generally use deceptive e-mail that looks like a mail coming from a popular commercial site. Generally, the fraudulent e-mail asks the user about account problem or shows some other reason to visit the commercial site and visit the site. The link in the e-mail direct the user to a malicious website that try to collect the user's secret information like account names, passwords and credit card numbers etc. Once the user's information is collected by the spoofing site, the phishing attack may log into the account or cause other serious problems with the account. The snapshot of the Spoof Guard is shown below :



Source: http://crypto.stanford.edu/SpoofGuard/2.jpg

Spoof Guard is a browser plug which is compatible with the Microsoft Internet Explorer. Spoof Guard uses traffic light like symbols in the browser toolbar that turns the colour from green to yellow to red as you access the spoofing site. If the user provides secret information into a form of spoof site, Spoof Guard save the user's data and warn user about the website type. Spoof Guard warn the user it its web browser screen when the alarm indicator reach a level that depends on parameters that are set by the user [11].

The Spoof Guard Toolbar contains three buttons. The first button is Settings Button which brings up the Settings dialog. The second button is Status Button, which display the current domain and a brief representation of the status by using colours. The Status Button brings up a status message when pressed. The third button is Reset Button which removes all the collected data, but do not clear the user's Internet Explorer History.

III DRAWBACK OF BROWSER BASED ANTI-PHISHING SYSTEMS

On the basis of the previous study, some of the drawbacks found in the anti-phishing tool which are needed to solve in further study [12-15]. The earlier proposed and implemented technologies have several limitations, which are as follows:

(a) The proposed blacklist-based technique shows low false alarm rate, but this technique cannot find the websites that are not in the blacklisted database. Because of short life cycle of the phishing websites blacklisted websites are needed to be maintaining systematically.

(b) The heuristic-based anti-phishing system is a higher probability of failed and false alarm method. It is easy for the phishing attack to use technical ideas to avoid the heuristic characteristics detection.

(c) The multi-functioning of the phishing indicators are time-consuming that are not feasible. Also, there is less accuracy rate shows the system for text, images and similarity measurement. Practically, image similarity identification technique is not perfect enough yet for the detection analysis.

(d) The anti-phishing systems take much time to find the type of website.

IV METHODOLOGY

Since the spoofing website remains almost similar to the legitimate website so that the internet user doesn't find at that moment, which website he is accessing. The spoofed website matches almost 90 to 99% of the legitimate website [16-19].

In the study of phishing website detection, a system model is prepared which is based on the phishing criteria [21]. Since when the web user access the website and fill the confidential information into it, the user must be informed instantly about the type of the website. To find the accurate result and instant response, the accessed dataset is categorised at different assigned servers, these are

(a) Group 1 : Character based

- Number of dots ' . ' present in the URL
- Number of dots '@' present in the URL
- Number of dots ' // ' present in the URL
- Existence of IP address in the URL
- Port Number in the URL

(b) Group 2 : Coding based

- Title Tag
- Form Tags on the web page
- Image Tags on the web page
- href Tags on the web page

(c) Group 3 : Identity based

- Country Code present in the URL
- Login/Password evaluation
- Script Tags on the web page
- Link Tags on the web page

(d) Group 4 : Contents based

- The websites which are having HTTPs protocol
- Number of Phishing Keywords present in the URL

(e) Group 5 : Attribute based

- Finding Domain Age
- First Webpage Creation Date
- Snap of Web matching
- Taking declared phishing websites from other authorities

The reason of categorising the system in different groups is to find the spoofed website as quickly as possible when the web user hit the target URL. In the system design, one main server takes care of the functioning of the add-on and sends the received information to five assigned servers. The assigned servers are defined in five different categories; these are *Character based, Coding based, Identity based, Contents based and Attribute based.* All the above mentioned groups are defined on different servers with its database information. When the internet user hit the target, instantly the concerned information about the webpage goes to these servers. On the assigned server, the information is cross checked with the database information. If it is found that the some portion of the webpage information matches with the database information, the server reply to the user system about the matching status.

On the basis of achieved information, Add-on displays a warning message on the web browser screen about the type of website which user is accessing. If user wants to continue accessing the website and feed the confidential information in it, the user can skip this warning message and can continue accessing the website. If the system has tested the user access website is phishing website, the user will be warned again 'Not to access the website'. If user want to discontinue the accessing the website, the website will be blocked for further access. Since the user has already submitted the confidential information like password into the spoofed website, so the user advised to change the password instantly.

The Figure 1 shows the error rate of different anti-phishing tools by collecting the dataset in different days. The proposed system tool is showing less error rate in all the days. The error rate can be calculated by 'No. of phishing websites/No. of legitimate websites [20]. The reason of showing less error rate is that the main server is collecting the data from one of the assigned servers only. This process takes less time to analyse the data and produce accurate result.

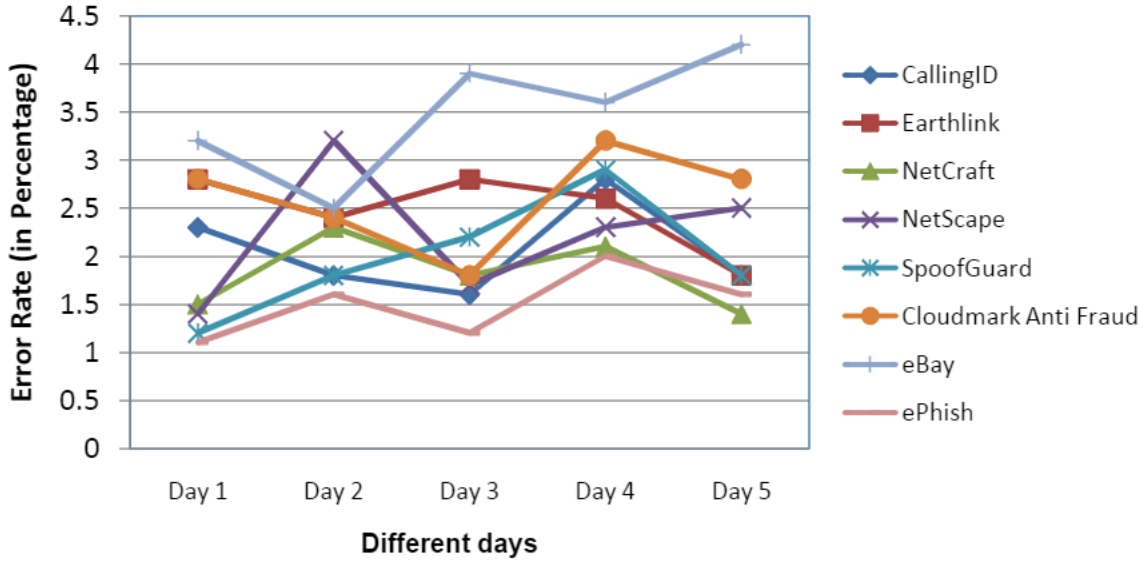


Fig. 1 Error Rate Analysis of Different Anti-Phishing Tools when hitting the websites in different days

V CONCLUSION

In the phishing attack, the user sends their confidential information on mimic websites, so the user should be informed immediately about the type of website. For this, a browser based add-on is prepared and studied with the already declared phishing and legitimate website data sets. To make awareness among of the user about phishing or legitimate website, the web browser should provide the security tools for the user. In the proposed add-on, the system is divided in five different assigned servers and the performance of the system is tested in the form of error rate analysis. The performance evaluation of the proposed anti-phishing add-on is compared with the existing anti-phishing tools and found that if the task is divided into different system, it can give better results. The proposed anti-phishing tool is compared with the anti-phishing tools like Calling ID, EarthLink, Net Craft, Netscape, Spoof Guard, Cloud Mark and ebay.

REFERENCES

[1] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong, Phinding Phish: Evaluating Anti-Phishing Tools, NDSS '07: Proceedings of the 14th Annual Network and Distributed System Security Symposium (February 2007)

[2] Calling ID, Ltd. Accessed: December 1, 2008. http://www.callingid.com/DesktopSolutions/ CallingIDToolbar.aspx.

[3] EarthLink, Inc. EarthLink Tool. Accessed: November 9, 2010. http://www.earthlink.net/software/free/tool/.

[4] eBay, Inc. Using eBay Tool's Account Guard, Accessed: June 13, 2010, http://pages.eBay.com/help/ confidence/accountguard.html.

[5] Kerner, Sean Michael. 2006. Firefox 2.0 Bakes in Anti-Phish Antidote. Internet News. http://www.internetnews.com/devnews/ article.php/3609816.

[6] Google, Inc. Google Safe Browsing for Firefox. Accessed: June 13, 2010. http://www.google.com/tools/firefox/safebrowsing/.

[7] Microsoft Corporation. Internet Explorer7. Accessed: November 9, 2010. http://www.microsoft.com/windows/ie/default.mspx.

[8] Net craft. Net craft Anti-Phishing Tool. Accessed: June, 13, 2010. http://tool.netcraft.com/.

[9] Netscape Communications Corp. "Security Center." Accessed: November 9, 2006. http://browser.netscape.com/ns8/product/security.jsp.

[10] Computer Crime Research Center. "Netscape: Anti-Phishing Bundled." February 2, 2010. Accessed: November 9, 2011. http://www.crimeresearch.org/news/02.02.2005/1024/.

[11] Quick Start : Spoof Guard, A http://crypto.stanford.edu/Spoof Guard/

[12] The Phishing Guide : Understanding & Preventing Phishing Attacks, Gunter Ollmann, Security Strategy - IBM Internet Security Systems

[13] Hansi Jiang, Dongsong Zhang, Zhijun Yan, "A CLASSIFICATION MODEL FOR DETECTION OF CHINESE PHISHING E-BUSINESS WEBSITES", *PACIS 2013 Proceedings*. Paper 152, 2013.

[14] Weiwei Zhuang, Qingshan Jiang, Tengke Xiong, "An Intelligent Anti-phishing Strategy Model for Phishing Website Detection", IEEE Computer Society, 32nd International Conference on Distributed Computing Systems Workshops, 2012.

[15] T. Balamuralikrishna, N. Raghavendrasai, M. Satya Sukumar, "Mitigating Online Fraud by Ant phishing Model with URL & Image based Webpage Matching", International Journal of Scientific & Engineering Research, Volume 3, Issue 3, pp.1-6, March -2012.

[16] Madhuri S. Arade, P.C. Bhaskar, R.K.Kamat, "Antiphishing Model with URL & Image based Webpage Matching", International Conference & Workshop on Recent Trends in Technology, (TCET), Proceedings published in International Journal of Computer Applications® (IJCA), pp 18-23, 2012

[17] Maher Aburrous, M. A. Hossain, Keshav Dahal, Fadi Thabatah, "Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy Data Mining", IEEE Computer Society, International Conference on CyberWorlds, pp. 265-272, 2009

[18] W. Zhuang, Y. Ye, T. Li, Q. Jiang. Intelligent phishing website detection using classification ensemble Systems Engineering Theory & Practice, Volume 31(10), P2008-2020. 2011.

[19] 58.JungMin Kang, DoHoon Lee. Advanced White List Approach for Preventing Access to Phishing Sites. 2007 International Conference on Convergence Information Technology (ICCIT 2007). pp.491–496.

[20] Ahmed Abbasi, Fatemeh "Mariam" Zahedi and Yan Chen, "Impact of Anti-Phishing Tool Performance on Attack Success Rates", 10th IEEE International Conference on Intelligence and Security Informatics (ISI) Washington, D.C., USA, June 11-14, 2012.

[21] A. Abbasi and H. Chen, "A Comparison of Fraud Cues and Classification Methods for Fake Escrow Website Detection," Information Technology and Management, Vol. 10(2), pp. 83-101, 2009.

[22] Mr. Bhushan Yenurkar, Mr. Shrikant Zade "An Anti-Phishing Framework with New Validation Scheme using Visual Cryptography", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 739-744.