2009 Sixth International Conference on Information Technology: New Generations

# A Proactive Approach to Preventing Phishing Attacks Using a Pshark

Ripan Shah, Jarrod Trevathan, Wayne Read and Hossein Ghodosi
*James Cook University, Townsville, QLD, Australia – 4811*
*E-mail: ripankumar.shah@jcu.edu.au*

## Abstract

*Phishing is an online scam used to dupe people out of their personal information for the purpose of defrauding them. This paper presents a conceptual design for removing phishing pages that have been uploaded on a website, potentially without knowledge of the website owner or host server. Initially the system is alerted to the presence of a phishing page upon receiving the Phisher's solicitation e-mail. Next the system retrieves the location, IP address and contact information of the host server using a tracking program. Finally, the system sends notification to the Administrator about the phishing page on its server. It is then up to the host server Administrator to remove the phishing page from its server, or face the possibility of criminals continuing to use their site. This approach acts as the basis for further development into proactively (or aggressively) attacking Phishers directly, rather than being a reactionary approach that is common to most email filters and anti-virus software.*

## 1. Introduction

The Internet is now a popular means for providing entertainment, communicating with friends, conducting e-commerce, and delivering teaching materials. However, some people around the globe are taking advantage of the anonymity provided by the Internet to fool individuals with fake offers, or by misrepresenting themselves as legitimate companies. *Phishing* is an online scam that attempts to defraud people of their personal information such as credit card/bank account information, and username and password credentials, using social engineering or technical subterfuge attacks [1]. These online criminals are known as *Phishers*. Phishing scams either try to swindle money out of people, disrupt someone's computer account, or attempt to get an individual to unsuspectingly download malicious software. Conventionally, mass e-mailing with a phishing link is the most popular way to lure the victims. However, SMS messages, chat rooms, fake add banners, fake job offers, and fake browser tools have emerged as a new platform among phishers [2]. More recently, social networking sites (such as Facebook) have become the target of phishing attacks. Phishing-style attacks can also use technical subterfuge strategies that involve deploying crimeware, spyware, and key-stroke loggers into a target computer to directly steal a victim's credentials.

In January 2006 alone 9,715 unique phishing websites were detected [3]. The number of unique phishing websites detected in August 2007 was 32,079 [4]. In the first quarter of 2008, the number of phishing websites detected was 81,215 and more than 90% of the attacks were targeted at financial services [5]. In the first half of 2008, the website infection rate has increased to three times compare to 2007. On average, Sophos detects 16,173 malicious web pages everyday [6].

Although researchers have proposed techniques to prevent phishing attacks, Phishers are becoming increasingly sophisticated in their approaches. Phishing attacks often involve rigorous planning and incorporate strategies to bypass existing anti-phishing tools. The shear volume of phishing attacks suggests that existing anti-phishing tools are insufficient. This is primarily due to fact that they only take a reactive or *passive* approach to stemming the problem. That is, they only filter suspect emails, but don't actually do anything to shut down the problem at its source.

This paper proposes a *proactive* approach to remove a phishing page from the host server. Rather than just filtering email and flagging suspect messages as 'spam', our approach actively seeks out Phishers in an attempt to disconnect them at the source. To use an analogy, our system introduces sharks (or *Psharks* as

978-0-7695-3596-8/09 $25.00 © 2009 IEEE
DOI 10.1109/ITNG.2009.302

we refer to them) that lie in wait for a Phisher to dangle his/her line in the water. Once the presence of a Phisher has been confirmed, the Pshark moves in to bite the Phisher back (by continually taking its baits) and essentially stop them from phishing.

Initially the system is alerted to the presence of a phishing page upon receiving the Phisher's solicitation e-mail. Next the system retrieves the location, IP address and contact information of the host server using a tracking program. Finally, the system sends notification to the Administrator about the phishing page on their server. It is then up to the host server Administrator to remove the phishing page from its server, or face the possibility of criminals continuing to use its site. This approach acts as the basis for further development into proactively (or aggressively) attacking Phishers back, rather than being a reactionary approach that is common to most email filters and anti-virus software.

This paper is organized as follows: Section 2 provides a brief summary of the types of phishing attacks and the anti-phishing techniques that currently exist. Section 3 presents our proposed approach to proactively attacking Phishers directly. Section 4 presents some practical results we have obtained using the proactive approach, and Section 5 provides some concluding remarks.

## 2. Related work

This section provides background on the phishing process, the various strategies employed by Phishers, and the style of phishing attack considered by this paper. It also presents the existing mechanisms that are currently being used to combat phishing.

Generally, most phishing attacks begin with *spam*. Spam is mass unsolicited email. The email message typically contains some sort of socially engineered message enticing the recipient to venture to a web site or to reply to the message. It is usually at this point phishing attacks start to differ in their approach. In this paper, we will primarily be concentrating on phishing attacks that attempt to lure a recipient to a website by providing a link within an email. Upon reaching the website, the user is either asked to enter personal details as they believe it to be a legitimate company (such as his/her bank), or the user is conned into believing that s/he must install a critical update for his/her computer (which is in fact a virus). A variation on this style of phishing attack is for the victim to reply directly to the Phisher's email address rather than following a link to a website. This style of attack will not be considered in this paper, but will be the focus of future work.

The majority of the anti-phishing tools use an email filtering process to separate legitimate emails from suspected spam in the inbox. It is then up to the individual to decide whether to discard the message. If an individual doesn't have the latest anti-phishing tools installed, or has failed to install the most recent update for his/her anti-phishing program, then they lose this layer of protection. We refer to this as a *passive* anti-phishing approach. This is because the approach only attempts to locally protect an individual from a phishing attack, but does not actively make any effort to remove or shut down the Phisher at the source. In effect, the Phisher is free to continue with his/her operation and can potentially accrue further victims.

There are several spam filters, browser tools, anti-spyware and anti-virus software [7, 8] available to protect online computers from various attacks. However, there were very few research efforts have been entirely focused to protect online users from phishing attacks in the past. Existing anti-phishing and anti-spam techniques suffer from one or more limitations and they are not 100% effective at stopping all spam and phishing attacks [9]. Phishers are able to find ways to bypass existing rule-based and statistical-based filters without much difficulty. Major e-mail service providers such as Yahoo, Hotmail, Gmail, and AOL filter all incoming emails separating them into Inbox (legitimate email) and junk (illegitimate email) email folders. However, these e-mail service providers do not actually attempt to remove the phishing page associated with the illegitimate email. Furthermore, Phishers have readily available tools to bypass such spam filters [9].

There have been efforts made to compare performance of various machine learning techniques such as fuzzy logic and neural network theory to detect phishing emails. However, these attempts still require improvement to achieve a higher accuracy rate [8]. Many researchers have attempted to detect the structure, properties and technical subterfuge of the typical phishing emails in order to design more effective anti-phishing tools [1, 9, 10]. The ultimate problem with only using detection as a defense is that the final decision rests with the user as to whether s/he should access a website or not. The extremely convincing nature of phishing emails makes this a dangerous approach for the occasional or non-technical Internet user.

Other defensive techniques involve the use of Secure Sockets Layer (SSL), digital signatures, and

digital certificates. The security of information is very important where the confidential data transferred on public Internet such as online shopping, banking transactions, government and corporate email communications, etc. SSL, digital certificates and digital signatures provide a level of information security while data travels across the public Internet. While such cryptographic techniques are quite reliable and robust in mathematical terms, however they suffer from weak implementation or incorrect use of technique [11].

People are familiar with the SSL icon and padlock on the browser and they believe that the communication is secure. However, phishers can exploit this perceived protection by using fake SSL padlock images on their phishing pages to create confidence and lure Internet users. Some Phishers also use a low-quality certificate or trial certificate on their phishing pages. Furthermore, there are technical subterfuge mechanisms in which malware can suppress any security errors and create false security indicators [11, 10].

Another popular approach for anti-phishing techniques is flooding the Phisher's database with fake information [12]. This approach significantly minimizes the probability of distinguishing the correct data from the flooded database in order to protect people who have submitted their personal credentials already. However, this approach does not prevent other Internet users from supplying their personal credentials to the phishing website. Raising awareness through training and enforcing policies for suspect emails is also popular approach among corporations and institutions for preventing the damage caused by phishers. However, researchers have found that best phishing sites have fooled 90% of the people during their experiment on various groups of people including academic staff and students at a prestigious American university [13].

## 3. Our Proposed Approach

This section describes our approach to detecting and shutting down Phishers using a *Pshark* (shark). Effectively a Pshark lies in wait for a Phisher to dangle his/her line in the water. When the Pshark detects the Phisher's presence it aggressively attacks the Phisher by continually taking his/her baits, thereby preventing him/her from phishing any further.

Figure 1 presents the conceptual design of the Pshark technique to remove a phishing page from its host server. Firstly, the system detects a phishing email and records the phishing page's URL. The WHOIS query is then used to retrieve information regarding the host server's IP address, location of the host server and contact information of the Server Administrator. Based on this information, the Pshark sends notification to the host Server Administrator to raise awareness that a phishing page resides on its server.

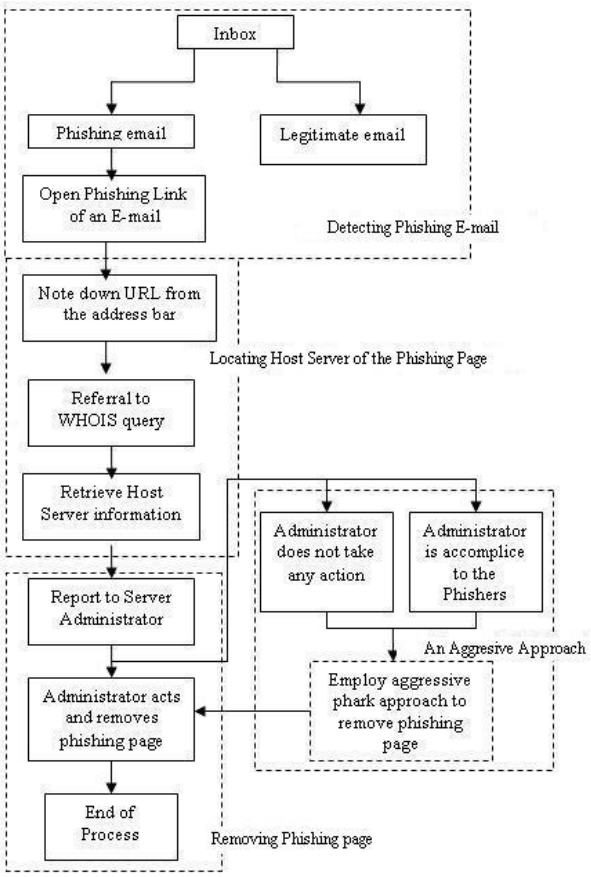


**Figure 1: Pshark process to remove phishing page**

Finally the Administrator removes the phishing page from its server. If the Administrator fails to remove the page, the Pshark becomes more aggressive in its notifications and/or actions. Specific details of each stage in the process are as follows:

### 3.1. Detecting a Phishing Email

Many researchers have proposed anti-phishing tools that examine the structural properties, SMTP (Simple Mail Transfer Protocol) pathways or layouts of suspect emails to detect phishing e-mails [14]. In this research we have largely ignored this stage to integrate with the proposed Pshark approach and we are more concerned with how to deal with the Phisher once a phishing email has been detected.

For the experiments conducted with this approach, we used our own judgment to decide what phishing emails were. There are obvious give-aways, such as a generic salutation and subject heading, an unrealistically lucrative offer, a request for personal details, etc. See [1] for more information on common phishing email traits.

The majority of the phishing emails we found were targeted at leading financial institutions. We also noticed that phishers have spoofed sender's email address and ask the victims not to reply to the email. Instead they have requested users to click on the link sent within the email.

### 3.2. Locating the Host Server of Phishing Page

The Pshark technique locates the host server of a phishing page using a WHOIS query [15]. WHOIS is a query/response protocol that is widely used for querying an official database. The WHOIS database contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources, and related Points of Contact on the Internet. Traditionally, WHOIS lookups were made using command line interface, but now many simplified web based tools are available. In this technique http://www.domaintools.com web based WHOIS tool is implemented.

A WHOIS server listens on (Transmission Control Protocol) TCP port 43 for requests of the host server and related contact information sent through web-based referrals. The WHOIS server closes its connection as soon as the output is finished. The closed TCP connection is the indication to the client that the response has been received.

To locate the phishing page's host server, the Pshark technique runs the WHOIS query on the URL that is contained within the phishing email. While phishing emails may give erroneous FROM emails addresses, this type of attack requires that they provide a genuine/legitimate website address for the victim to interact with. This therefore is the vulnerability in a Phisher's attack which a Pshark can exploit.

### 3.3. Removing the Phishing Page

Upon receiving the notification of the phishing page existence on the host server through the Pshark technique, the host Administrator confirms the phishing page by testing the legitimacy of the phishing link and its genuineness. Once the Administrator confirms the phishing page, the infected or hacked website is quickly shut down to protect Internet users from further phishing. The host Administrator then notifies the website owner about the existence of the phishing page within their website. Once the phishing page is removed, if no notification has been sent to the Pshark, the Pshark periodically checks to for evidence that it has been removed.

This technique assumes that website owner and host Administrator are absolutely unaware of the presence of the phishing page within their website or server until our technique notifies them. This means Phishers are taking control of the legitimate website to upload their phishing page. By doing so phishing pages are able to bypass anti-virus securities installed on the user's computer.

### 3.4. An aggressive approach to remove a phishing page upon non-responsive Pshark notification

In the situation where an Administrator does not act upon the Pshark notification, the technique becomes more aggressive with regard to its notifications or actions.

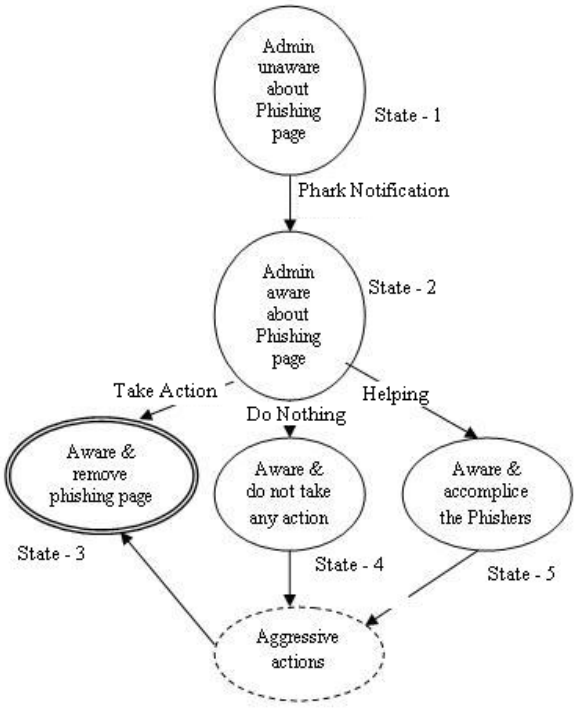


**Figure 2: State Diagram of an aggressive approach implementation**

Figure 2 presents a state diagram illustrating the various stages an Administrator can be in with respect to the Pshark defense.

Initially, the Pshark assumes that an Administrator is unaware about the existence of a phishing page (i.e., innocent until proven guilty), even though the

Administrator could actually be harboring a Phisher, or actively involved in phishing.

Once the Pshark has sent notification to the Administrator, the Administrator can then be assumed to be in state 2. That is, the Administrator is now aware of the existence of a phishing page on its server. Once the Administrator is in this state, it makes it difficult for him/her to ignore that criminal activity is occurring, and its next actions dictate how the Pshark should proceed.

Ideally, the Administrator will shut down the phishing page so that is no longer a threat (state 3). Once the Pshark confirms the phishing page is removed, this is the end of the process. It is the Pshark's goal to get all Administrators to this state.

However, if the Administrator does not shut down the phishing page, the Pshark must take further action. As the Administrator has been notified, the Pshark can now assume that it is aware of the phishing page. There are now two possible cases the Administrator has moved to:

Case 1 (state 4): The Administrator is not in a league with the Phishers but is aware about the presence of the phishing page. The Administrator does not act to remove the phishing page indifference, or another reason. If this is the case, then the Administrator essentially is *harboring a Phisher*.

Case 2 (state 5): The Administrator is actively involved in the phishing crime. That is, they are either responsible for the phishing page, or are in league with the Phisher to help perpetrate the attack. Obviously, this is more serious than Case 1.

Given the aforementioned possibilities when a Pshark notification has been ignored, the Pshark must become more aggressive (illustrated by the dashed state) to force the Administrator into state 3 (i.e., page removal). Some of the avenues for aggressive action are aimed at either the Administrator or the Phisher itself. These include:

1. Inform legal authorities about the accomplice of the host server in the phishing crime. Regardless of whether an Administrator is in state 4 or 5, as they have been notified about the crime, they now have an obligation to take action otherwise they will be incriminated along with the Phisher.

2. Execute anti-phishing attacks such as flooding phishing page with misleading information [12] which minimizes the chances of distinguishing actual data and fake data. Alternately the Pshark might take the bait and delay the phisher with false information. This and other similar approaches force the phisher to spend time and money following up false leads – they catch Psharks instead of Phish.

Fleshing out the details of the more aggressive Pshark attacks is beyond the scope of this paper at this time. However, we are actively involved in designing the aggressive Pshark approach and will document it in future work.

## 4. Real World Test Experiment

This section presents an experiment using the Pshark technique to actually shut down phishing pages at their source. We used phishing emails that arrived in our personal email inbox as test subjects.

The following outlines how the Pshark technique operated with one specific phishing example.


Access To Your Account(s) Have Been Blocked Due To Third Party Activities
From: HSBC Bank PLC (error#8122@secure.hsbc.co.uk)
Sent: Sunday, 26 October 2008 7:41:24 AM
To: ripan@hotmail.com

You have 1 new Security Message Alert!

Log In into your account and resolve the problem.

HSBC Internet Banking

Yours Sincerely
HSBC Holdings plc Security Department

**Phishing e-mail arrived in personal Inbox**

When we received the above email, we realized it was a phishing email as we never had an account with HSBC bank. To test our technique we clicked on the link (*HSBC Internet Banking*) sent in the email. The link opened the HSBC online login page straight away which was an exact copy of the legitimate HSBC login page. Mozilla browser or anti-virus software did not detect the webpage as a phishing forgery. We noted down the web address of the HSBC login page: http://www.kirmes-forum.de/documentation.IBlogin.html. From this web address it is clear that a Phisher had hacked the plausible legitimate website www.kirmes-forum.de and uploaded the HSBC phishing page on the website without the knowledge of the website owner or host server. Actually tracking the source of the above web address with a WHOIS query returned the following details:

Whois Record

| | |
|---|---|
| Domain: | kirmes-forum.de |
| Domain-Ace: | kirmes-forum.de |
| Nserver: | ns5.kasserver.com |
| Nserver: | ns6.kasserver.com |
| Status: | connect |
| Changed: | 2008-01-22T12:41:05+01:00 |
| [Admin-C] | |
| Name: | Michael Martens |
| Address: | Schulenburgstr. 21 |

Pcode: 26129
City: Oldenburg
Country: DE
Changed: 2008-01-22T12:41:10+01:00
[Tech-C][Zone-C]
Name: Werner Kaltofen
Organisation: Neue Medien Muennich GmbH
Address: Hauptstrasse 68
Pcode: 02742
City: Friedersdorf
Country: DE
Phone: +49 35872 35310
Fax: +49 35872 35330
Email: info@all-inkl.com
Changed: 2007-10-09T21:15:45+02:00

IP Information: 85.13.134.29
IP Location: Germany Berlin
Neue Medien Muennich
Resolve Host: dd11712.kasserver.com
IP Address: 85.13.134.29 [Whois] [Reverse-Ip] [Ping] [DNSLookup]
Reverse IP: 40 other sites located on this server.
Blacklist Status: Clear

From the above WHOIS record we can gather very important information including:

- The actual IP Address of the infected website or phishing page website;
- The physical location from which this phishing page has been uploaded. In this case, the website/phishing page is hosted from Berlin, Germany;
- The name of the actual host Administrator is provided; and
- The contact phone and email address of the host server.

From the above information, it is possible to notify the host Administrator about the existence of phishing page on their server. Below is the actual copy of the email sent to the Administrator.

Date: Sun, 26 Oct 2008 12:59:59 +1000 4 of 65
From: Ripankumar Shah <ripankumar.shah@jcu.edu.au>
Subject: Phishing page found on your server
To: ip@all-inkl.com , info@all-inkl.com

Hello Admin,

We have found HSBC Phishing page located on your server on following link.

http://www.kirmes-forum.de/documentation/IBlogin.html

Regards,
Ripan Shah
Department of Maths,Physics & IT
James Cook University
Townsville - 4811
Ph: (O) 07 47815525

**Pshark Notification to the host Administrator**

Within short period of time (less than 24 hours) the Administrator replied acknowledging that this was a phishing page. They informed us that the infected website had been closed and phishing page was now removed. Below is the actual copy of the host Administrator's email:

Subject: Re: Phishing page found on your server
To: ripankumar.shah@jcu.edu.au
From: support@all-inkl.com
Date: Sun, 26 Oct 2008 04:46:10 +0100

Hallo,
the site has been closed.

Mit freundlichen Grüßen
Jens Lehmann
Support Team

Bitte geben Sie bei einer Anfrage stets die Kundennummer oder die Domain im Betreff Ihrer E-Mail an, damit wir Ihre Anfrage schneller bearbeiten können.
Neue Medien Münnich
Inhaber René Münnich -
Hauptstraße 68, D-02742 Friedersdorf
Ust-ID: DE212657916

Tel: +49 35872 353-10
Fax: +49 35872 353-30
E-Mail: info@all-inkl.com
Web: www.all-inkl.com

Bitte helfen Sie uns mit, die Qualität unseres Supportes zu verbessern. Nehmen Sie sich einen kleinen Moment Zeit um uns zu sagen, wie Sie mit der E-Mail zufrieden waren.
Unter der URL:

http://all-inkl.com/?cna=mail_bewertung&nummer=662452&m=cmlwYW5rdW1hci5zaGFoQGpjdS5lZHUuYXU=

können Sie diese E-Mail bewerten.

**Reply of Server Admin informing the removal of Phishing page from the server**

## 5. Experiment Results

In our experiment, we investigated phishing emails sent to Inboxes on Yahoo mail, Hotmail, Gmail, James Cook University Webmail, and Face book.

| Phishing emails | Browser detected | Traced server info. | Removal of phishing page | Time Taken |
|---|---|---|---|---|
| 12 | 3 | 11 | 11 | < 24 Hrs |

**Table 1: Experiment Results of Phishing Removal**

Table 1 presents the results of the experiments performed during October – November 2008. The Pshark technique achieved a 91.67% success rate in removing the phishing pages from their host servers. The time taken to remove the phishing page is typically less than 24 hours once the host Administrator had been notified. While there are only a small number of test experiments, the success rate is encouraging and indicates that the approach is sound.

It is important to mention here an exceptional case in which the host Administrator did not respond to the

initial Pshark notification, and the phishing page still remains online (for more than a week time at the time of writing this paper). This appears to suggest that the host Administrator either doesn't care, or is helping the Phisher. Therefore, this warrants the development of a more aggressive Pshark attack to shut down such phishing pages and to punish the host Administrators that do not do the right thing. Essentially the longer a phishing page is available, the more victims it can accrue. Therefore a non-responsive host Administrator becomes more culpable for every minute they allow phishing to continue.

## 6. Conclusions

This paper presented a proactive method to shut down a Phisher's operation by using a Pshark. This effectively stops a phishing attack at its source thereby protecting a significant number of other innocent users from being duped in the future. This is in contrast to the existing passive approach that only attempts to filter suspect email and allows the Phisher to continue his/her operations. While this technique does not prevent an initial phishing email from being sent, once the phishing page has been removed, all future victims are essentially protected from the Phisher.

Experimental results show that this approach can be an effective way to remove phishing pages hosted on servers around the world. The Pshark technique achieved a 91.67% success rate with minimal delay in removal time. While the experiment data was limited in size, it nevertheless shows that this approach can work and lays a sound framework for future development involving a larger number of test subjects.

Furthermore, there is scope to undertake development on more aggressive techniques to address the problem of a non-responsive host Administrator that fails to shut down a phishing site. This could inform legal authorities, or baiting the Phisher back with fake information that makes it spend a significant amount of time chasing up bad leads (thereby distracting it from legitimate targets).

At present our proactive approach to shutting down a Phisher is performed manually in our laboratory. Future work involves automating this technique. This would involve firstly integrating our approach with an email filtering program to initially detect a potential phishing email. The next step would be to automate the tracing and web host email notification process. The final stage would be to devise a method to tangibly check to see whether a phishing web page has been removed, and if not, what means of action then must take place. Furthermore, we plan to significantly increase the number of phishing subjects used in the experimentation to test the Pshark techniques effectiveness.

## 7. References


[1] C. E. Drake, J. J. Oliver, and E. J. Koontz, "Anatomy of Phishing Email", *MailFrontier Inc*., CA, USA

[2] http://computer.howstuffworks.com/phishing.htm

[3] Y. Zhang, S. Egelman, L. Cranor, J. Hong, "Phinding Phish: Evaluating Anti-phishing Tools", *Annual Network and Distributed System Security Symposium*, USA, February 2007

[4] S. Abu-Nimeh, D. Nappa, X. Wang, S. Nair, "A Comparison of Machine Learning Techniques for Phishing Detection", *Anti Phishing Working Group: eCrime Research Summit*, 2007, USA, pp: 60-69

[5] Anti Phishing Working Group, "Phishing Activity Trend Report", 2006

[6] Anti Phishing Working Group, "Phishing Activity Trend Report", Jan-March 2008

[7] Sophos, "Security Threat Report", July – 2008,

[8] J. Milletaty, "Technical Trends in Phishing Attacks", *US-CERT, http://www.us-cert.gov/reading_room/*

[9] M. Chandrashekaran, K. Narayana, S. Upadhyaya, "Phishing Email Detection Based on Structural Properties", *Symposium on Information Assurance: Intrusion Detection and Prevention*, New York, 2006

[10] P. Ducklin, "Can Strong authentication sort out phishing and fraud", *Virus Bulletin Conference*, , Australia, Oct 2006

[11] Anti Phishing Working Group, "Phishing Activity Trend Report", 2007

[12] D. Geer, "Security Technologies go Phishing", *Computer*, June-2005, Vol. 38, no.6, pp. 18-21,

[13] R. Dhamija, J.D. Tygar, M. Hearst k, "Why Phishing Works", *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, January, 2006, Canada, pp: 581-590

[14] L. Wenyin, G. Huang, L. Xiaoyue, Z. Min, X. Deng, "Detection of Phishing Webpages based on Visual Similarity", *14th international conference on World Wide Web*, Chiba, Japan, 2005, pp: 1060-1061

[15] "WHOIS Protocol Specification," http://www.rfc-editor.org/rfc/rfc3912.txt, August 2005