Journal of Scientific Research & Applications (JASRA)
2014 Edition No 1.
A Quarterly Publication of the Faculty of Science, Adeleke University, Ede, State of Osun, Nigeria
www.jasra.adelekeuniversity.edu.ng

Understanding Phishing and Phishing Techniques in Client-Side Web-Based Systems

Okesola, J.O.
School of Computing
University of South Africa, South Africa
48948535@mylife.unisa.ac.za

Adewole, O.A.
Department of Computer Science
The Polytechnic, Ibadan
Ibadan, Nigeria.
Olu_gold@yahoo.com

Sorunke I. I.
Department of Computer Science
University of Ibadan
Ibadan, Nigeria
ismailsorunke@yahoo.com

ABSTRACT

As auspicious as the technology is, the bane of the internet has always been the constant threats of online identity theft and other forms of fraud prevalent on the information highway. Phishing is a form of internet fraud in which emails and websites that are purportedly from legitimate organisations and agencies are used to deceive users into disclosing personal or financial information. Despite the plethora of anti-spam filters that are readily available today, phishing emails are still able to bypass such measures and find their ways into users' inboxes. This challenge at the client side of the web-based infrastructure is prevalent as clients are at varying levels of usage and knowledge of internet infrastructure. This paper takes a look at the phishing scenario by examining why it works. We provide extensive insights into extant literature in the subject domain as a basis for the development of tools to mitigate phishing and assisting users understand phishing attacks.

Keyword: Phishing, computing, clients, web systems, internet, security, fraud and filters.

1. INTRODUCTION

Just a few years ago, phishing attacks were primarily seen by researchers as just one of several threats found in email spam. For some time, phishing remained relatively primitive from a technical point of view. It was relatively rare and it typically posted a threat only to the most naïve and inexperienced users. But today, the scale of these attacks and the technologies used are such that phishing has been elevated to a category of its own, meriting a separate study. There are different theories of where the "ph" in phishing (pronounced same as fishing) comes from. G. Ollmann believes that it originally comes from the early hacker naming terminology such as "Phreaks" who often were involved in "phreaking" i.e. hacking telephone systems [1]. D. Watson and his colleagues on the other hand states that the "ph" stand for "password harvesting fishing".

Phishing is common method for hackers and other malicious people to collect different kinds of sensitive information. Phishing is a kind of "social engineering" attack, where the attacker extracts sensitive information by tricking the user, instead of extracting it directly from the computer system [2] [3]. The collected information is often personal information or authentication credentials used to login to different sites, however it can also be sensitive financial data. Harvested credentials can thereafter be used by hackers or other malicious people to impersonate the victim to pursue a crime in near anonymity. The collected information, called "phish", can either be used directly by the people who collected it or be traded as a form of electronic currency, for example against a piece of hacking software or warez (pirated copyrighted content such as applications or games) [1].

1.1 A Phishing Attack Scenario

A phishing attack involves an attacker, a victim, a phishing website and a target website, as shown in Figure 1. According to Huang et al., [3] a phishing attack involves 5 steps:

1. Attacker sets up a phishing website.
2. Attacker sends the link of the phishing website to the victim via email or instant message.
3. Victim follows the link and enters personal details on the website thinking it is a legitimate website.
4. Attacker retrieves user's personal details from the phishing website.
5. The attacker uses details of the user on the respective legitimate website.

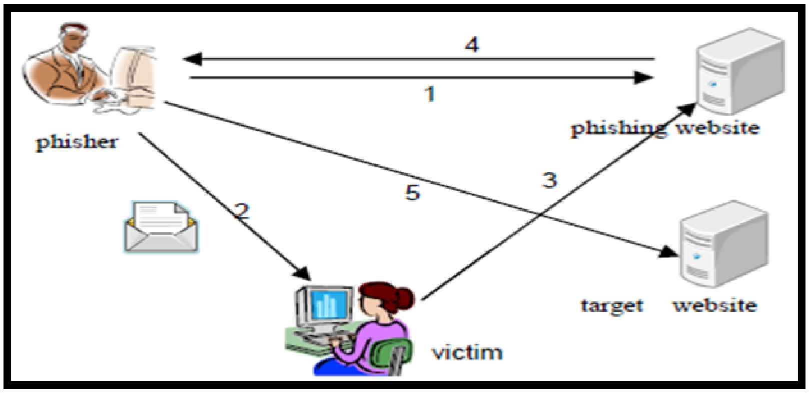


Figure 1: Steps involved in a phishing attack [4]

1.2 Why Phishing Works

Phishing attacks target human users. A number of user studies have been done in order to find out why phishing works and how effective phishing is. In some studies, users were attacked by simulated phishing attacks. Phishing is an attack that directly targets the human being in the security system. Simulating these kinds of attacks for study purposes raises some special problems. Chief among them is the secondary goal property articulated by Whitten and Tygar [4]: in real life, security is rarely user's primary goal. The user is primarily concerned with other tasks, such as reading mail, buying a book, or editing a document. Avoiding disclosure of passwords or personal information may be important, but it isn't foremost in the user's mind. Anti-spam firm MailFrontier Inc did a web survey on how well people can distinguish phishing emails from legitimate ones. The user's goal is to identify five phishing emails from the screenshots of ten emails. Users could not interact with the emails, e.g., clicking their embedded links. About 28% of the time, subjects incorrectly identified the phishing emails as legitimate. [5]

Whalen and Inkpen used an eye tracker to study the user's attention to browser security indicators when doing secure online transactions. Their study [6] found that subjects often looked at the lock icon in the status bar, but rarely clicked on the lock and thus didn't learn anything about the site's certificate. In this study, the subjects were explicitly told to pay attention to the security indicators in the browser to find faking web sites. Security was their primary goal. The experimenter's own passwords and credit card information were used in this study. A web proxy was used to simulate financial transactions with the tested sites. Dhamija et al did a study [7] to find out why phishing works. The subjects were shown 20 web sites and asked to determine which sites (12 of them) were fraudulent.

The study found out that 40% of the subjects made errors, either thinking good sites as fraudulent or thinking phishing sites as legitimate. 23% of them only paid attention to the web page content but not look at browser-based cues such as the address bar and status bar. Security is again the subject's primary goal. In April 2005, an interesting study [8] was done at Indiana University Bloomington that showed that social context can make phishing attacks far more effective. The researchers sent out phishing emails to university students, claiming to be from a friend, having mined friendship relations from a social networking site used on campus. The email led to a phishing site that asked for the subject's university username and password. 72% of the subjects provided valid usernames and passwords to the phishing site. In this study, the subject's goal is not security. They were not even told before that they will be attacked. There is only one attack per subject. Because of the study design, the result from this study was expected to faithfully reflect how effective social phishing can be. On the other hand, there were a lot of debates about whether this study should be done in this way. And many subjects felt offended when they eventually knew that they had been attacked.

At least two organizations have initiated phishing attacks against their own members, with the goal of teaching them to protect themselves. [9] The US Military Academy at West Point found that more than 80% of its cadets succumbed to a phishing attack by a fictional colonel. The State of New York mounted two attacks on its 10,000 employees: 15% were spoofed by the first attack, but only 8% by the second, which came three months later. This research shows that there is a long way to go to bring user perceptions and design of browsers and security of browsers to a point in which phishing is easily detected and prevented.

1.3 Anti-Phishing Tools

We consider two classes of anti-phishing tools that employ Email Content Analysis - Server side and Client Side Phishing solutions.

Server side Phishing Solutions

Server side phishing solutions involve installing a program or configuring the server to prevent users from being victims to phishing attacks. These programs filter incoming emails and check websites users are trying to connect to etc. Server side solutions mainly use email content analysis or notice and take down methods.

Email Content Analysis

The mechanism of email content analysis method is to analyse incoming emails and filter them on the basis of a set of features. When an email arrives the application installed on the server analyses the content of the email and decides whether the email is ham (legitimate), spam or phishing. There is a difference between spam and phishing email classification. Spam emails are intended only for informing users about some product, whereas in phishing emails there is a certain level of interaction with the receiver. Phishing emails are more harmful and may contain malicious links, deceptive forms etc through which attacker can gain access to personal details of users. Table 2.1 lists the differences between spam and phishing emails

Content based email filtering is done on the basis of a set of features which can be categorised as; structural, Link, Element, Spam filter and Word List [29]. Machine learning techniques are used to extract relevant features by capturing the content and structural properties of a number of illegitimate emails, and data mining techniques are used to find hidden patterns within these phishing emails.

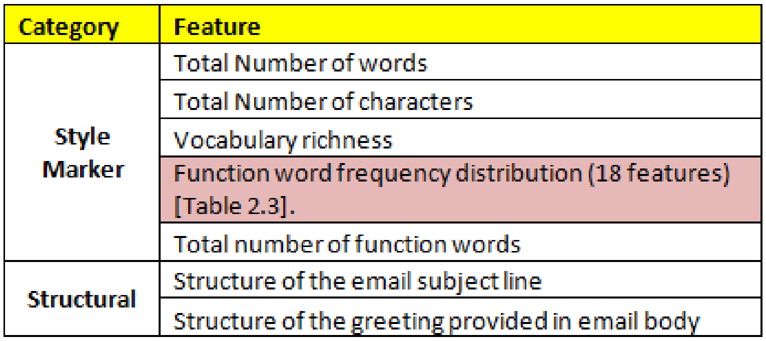
2. RELATED LITERATURE

There has been a lot of research in the past on content based phishing filters; some of which are discussed next.

E-mail Structural Attributes Method

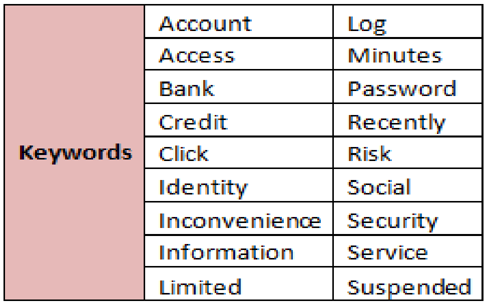
Chadrasekaran et al., [10] proposed a technique which used structural properties of phishing emails to segregate legitimate emails from fake ones. 25 features comprising of style markers and structural attributes were used, as shown in Table 2.2. A total of 200 emails were tested; which included 100 phishing and 100 legitimate emails, with simulated annealing as feature selection algorithm. According to the relevance between features, information gain was used by author to rank the features. Support Vector Machine (SVM) classifier was used to classify phishing emails which yielded a detection rate of 95% with a very low false positive rate. The Table below depicts marker and structural attributes extracted from email documents.

Table 1: Marker and structural attributes extracted from email document.



Category	Feature
Style Marker	Total Number of words
	Total Number of characters
	Vocabulary richness
	Function word frequency distribution (18 features) [Table 2.3].
	Total number of function words
Structural	Structure of the email subject line
	Structure of the greeting provided in email body

Table 2: List of 18 functional words used in experiment [30]



Keywords	Account	Log
	Access	Minutes
	Bank	Password
	Credit	Recently
	Click	Risk
	Identity	Social
	Inconvenience	Security
	Information	Service
	Limited	Suspended

Advantages:

Mails are classified before they reach the user’s inbox which reduces human exposure [30]. The action is also automated.

Limitations:

- Experiment data set is not large enough to draw a broader conclusion.
- Effectiveness of classification depends on the choice of features and keywords. If words outside Table 2.3 are used, the attacker will be able to bypass the filter.
- This technique only focuses on email based attacks and won’t be able to help users against other attacks.

Fette et al., [31] proposed a machine learning based approach PILFER. Random forest is used as a classifier to classify emails as either phishing emails or legitimate emails. A total of 10 features are used: IP based URLs, age of linked-to domain names, Non- matching URLs, “Here” links to non-modal domain, HTML emails, number of links, number of domains, number of dots, JavaScript, and spam filter output. 9 out of 10 features can be extracted from emails directly while WHOIS query can be used to get the “age of linked-to domain” feature. A data set with 713 legitimate emails and 860 phishing emails is used to obtain results.

Advantages:

- PILFER is flexible and can adapt if the nature of phishing attacks changes. New features can be added if they become more important.
- PILFER performs better than a general spam filter [11].

Limitations:

- Less number of features used [31].

Take down method

Another server side technique to counter phishing is to take down a phishing website before it harms anyone. In email content analysis phishing emails were filtered but no action was taken against the attacker. This is both preventive and corrective approach as compared to email content analysis which is a preventive solution. Reported websites and URLs found in phishing emails are harmful websites that are removed from the internet in notice and take down method.

Shah et al., [12] extended email content analysis approach and proposed an improved solution called Pshark. Pshark is a proactive approach against phishing websites and works aggressively against attackers rather than just preventing the user from phishing attacks. Pshark methodology can be divided into 4 steps as shown in Figure 2; detecting phishing emails, locating host server, reporting to server administrator and aggressive Pshark approach. If the administrator fails to respond to the warning given by Pshark and does not remove the phishing website, in step 4 either the server is taken down by reporting to legal authorities or by flooding the page with deceptive information.

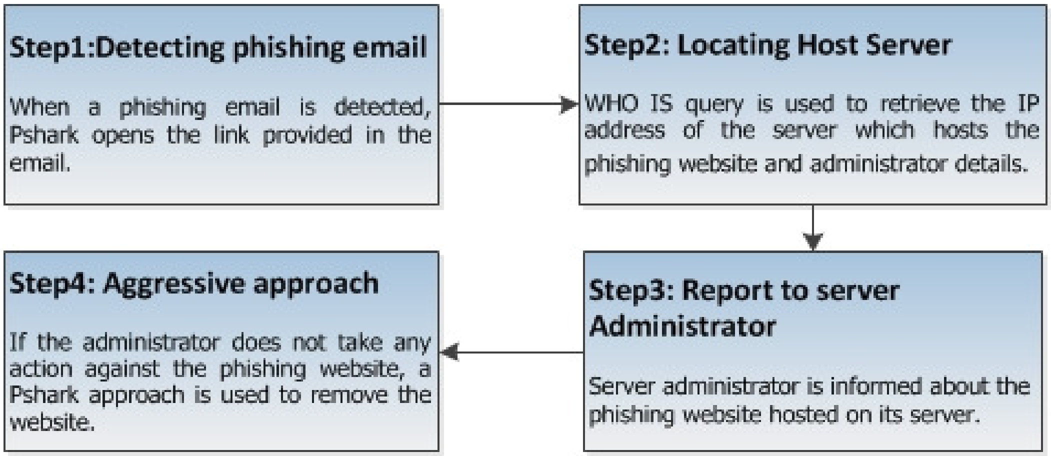

Step1:Detecting phishing email
When a phishing email is detected, Pshark opens the link provided in the email.
Step2: Locating Host Server
WHO IS query is used to retrieve the IP address of the server which hosts the phishing website and administrator details.
Step3: Report to server Administrator
Server administrator is informed about the phishing website hosted on its server.
Step4: Aggressive approach
If the administrator does not take any action against the phishing website, a Pshark approach is used to remove the website.

Figure 2: Shows the basic 4 steps of the methodology used by Pshark

Advantages:

- Pshark is a proactive approach and takes down websites rather than just ignoring phishing attacks.
- Once the phishing website is taken down, all future attacks from that particular website are stopped.

Limitations:

- Most phishing websites have an average age of 3.1 days and many disappear within hours [13]. The attacker might cause damage and remove the website by the time administrator acknowledges the message sent by Pshark.
- Cannot stop an initial phishing email.
- Pshark does not have an email filtering technique.
- Shutting down a fake website is performed manually and still needs to be automated.

Many organizations like Netcraft, BrandProtect, Dell SecureWorks, Cyveillance, PhishLabs, MarkMonitor, Telefónica, VeriSign, FraudWatch International, Easy Solutions, Internet Identity, etc. assist in deactivating fraudulent websites and removing them from the internet. Table 2 shows the list of organizations and the services offered.

Table 2: List of organizations and services against phishing offered

Organization	Services						
	Email authentication	Email filtering	Web filtering	Consumer toolbars	Takedown	Fraud analysis	Forensic Services
Netcraft	✗	✓	✓	✓	✓	✗	✗
BrandProtect	✗	✗	✗	✗	✓	✓	✓
Dell SecureWorks	✗	✗	✗	✗	✓	✗	✓
Cyveillance	✗	✗	✓	✗	✓	✓	✗
PhishLabs	✗	✓	✓	✗	✓	✓	✗
MarkMonitor	✓	✓	✓	✗	✓	✓	✓
Telefónica	✗		✗	✗		✗	✗
VeriSign	✓	✓	✗	✗	✓	✗	✗
FraudWatch International	✗	✗	✗	✗	✓	✓	✗
Easy Solutions	✗	✗	✗	✗	✓	✓	✗
Global Sign	✓	✗	✗	✗	✗	✗	✗
Go Daddy.com	✓	✓	✗	✗	✗	✗	✗
Iconix	✗	✓	✗	✗	✗	✗	✗
Symantec	✗	✓	✗	✗	✗	✗	✗
McAfee	✗	✓	✗	✗	✗	✗	✗

These organizations remove fake websites after a complaint has been made about a specific website or a phishing incident. On receiving a complaint, the reported website is checked whether it is a fraudulent website or not. Once that is confirmed, information about the owner is collected and the website is deactivated. Most of these organizations also ask Microsoft, Google and other major companies to update their blacklist. Figure 3 summarizes the steps taken once a complaint is made.

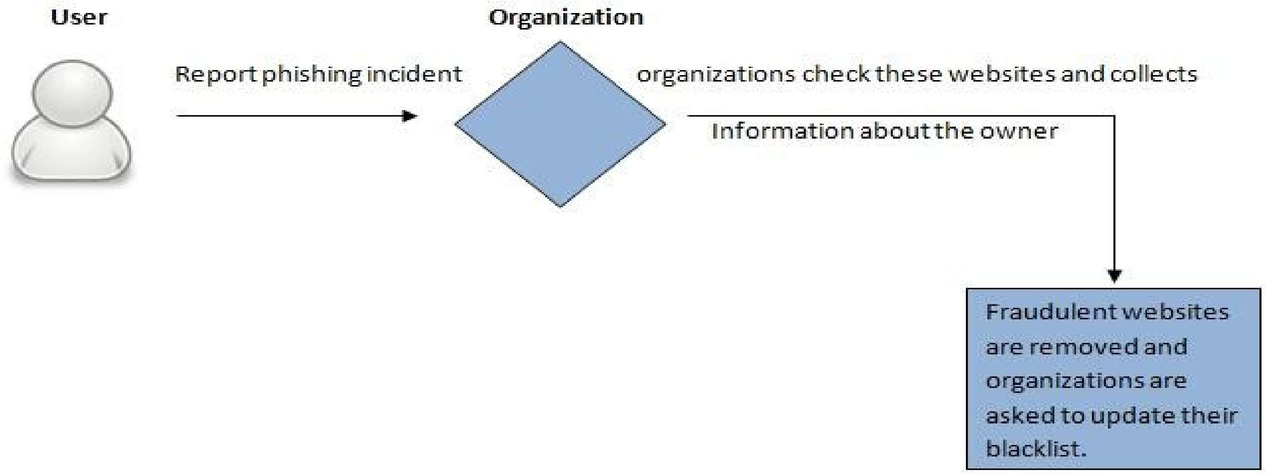

User
Organization
Report phishing incident
organizations check these websites and collects
Information about the owner
Fraudulent websites are removed and organizations are asked to update their blacklist.

Figure 3: Process of taking down a website

Table 3 summarizes the two techniques, email content analysis, notice and takedown discussed in this section.

Table 3: Comparison of Email content analysis and Takedown

Email Content Analysis	Notice-and-Take-down
Preventive approach	Preventive and Corrective approach
Take no action against attacker	Take action against attacker
Fraudulent website may continue to harm many users	Once a fraudulent website is taken down, all future attacks are stopped from that particular website
Prevents phishing emails from reaching the user	First phishing email cannot be prevented from reaching the user

3. CLIENT SIDE PHISHING SOLUTION

Mostly client side solutions are browser plug-ins or extensions that are installed on user's machine. These extensions monitor websites visited by users and informs them if they are about to enter a fraudulent page. There are many different solutions present to help users distinguish a fraudulent page from a legitimate one but each technique has some limitations. Attackers have constantly improved their methods which make the job of detecting phishing websites even harder. Client side phishing solutions fall into two categories: Blacklist based method and heuristic approach.

3.1 Blacklist Based Method

Blacklist approach has been used in many other areas for quite some time and has recently been adopted as an anti-phishing solution. Blacklist is an access control technique that allows access to anything outside the list. An anti-phishing blacklist contains all the entries that are denied access [4]; whereas a whitelist contains entries which are legitimate and denies access to anything outside the list. In blacklist based anti-phishing, creating and maintain the list is the most important task. To create this list, URLs of phishing pages are retrieved from users directly, spam or phishing emails, or from various authentic websites. Anti-Phishing Work Group (APWG), PhishTank, OITC, SURBL, The DNS blackhole, ZeuS Tracker etc. are some of the organizations that serve the anti-phishing cause.

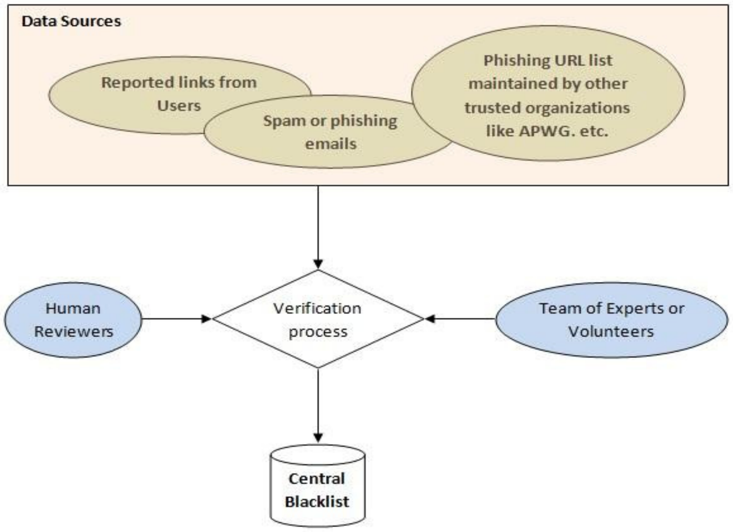
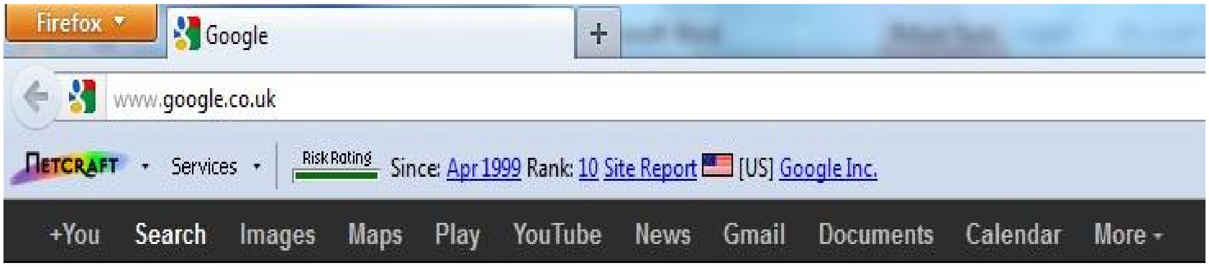

Data Sources
Reported links from Users
Spam or phishing emails
Phishing URL list maintained by other trusted organizations like APWG. etc.
Human Reviewers
Verification process
Team of Experts or Volunteers
Central Blacklist

Figure 4: Steps involved in blacklist compilation

Once a URL is reported, it is verified before added to the blacklist to minimize false positives. Different organizations have different ways of checking a URL; PhishTank classifies a URL as a phishing threat if it has at least 4 votes from users. Figure 4 shows a general model of how a blacklist is formed.

Blacklist of IP addresses can also be used to stop attackers but usually a lot of websites are hosted on one server and this will terminate other legitimate websites on the same IP address as well. Therefore, blacklist of domains is preferred. Organizations like Sucuri, Symantec, Google etc. also maintain a blacklist and inform the users when they are about to visit a blacklisted site. The blacklist method is used by Netcraft Toolbar [14], Cloudmark DesktopOne [15], Microsoft SmartScreen Filter [16], Firefox [17] and many others. Netcraft toolbar helps Internet Explorer and Mozilla Firefox users against phishing attacks. There are 5 labels; Since, Country, Rank, Host and Risk Ratting, through which Netcraft assists a user in differentiating a phishing website from a legitimate one (see Figure 2.5).

Table 4 gives details of the labels and how they contribute in determining the risk rating. Netcraft's designers consider age of the website domain to be the most important factor in determining the risk rating.



Since: Apr 1999 Rank: 10 Site Report [US] Google Inc.

Figure 5: Netcraft Toolbar

Table 4: Labels used by Netcraft and how they contribute in calculating Risk Rating

Label	What is shown in the Toolbar		Risk
Since	The date, when this website was first seen in Netcraft Web Server Survey	Website formation date if the website is available in the Web Server Survey	Low Risk
		"New Website" if it is not available in Web Server Survey	High Risk
Rank	Number of times this website has been visited	most visited pages	Low Risk
		Least visited pages	High Risk
Country	Country where the website is hosted	If the hosting country does not have history of hosting phishing websites	Low Risk
		If the hosting country has history of hosting phishing websites	High Risk
Host	Name of Organization hosting the current site	If the hosting company has no history of hosting phishing websites	Low Risk
		If the hosting company has previously hosted phishing websites	High Risk
Risk Ratting	Calculates the risk involved in visiting this website	Shows how trustworthy this website	

Advantages:

- Netcraft toolbar can deal with DNS poisoning. If a website that is supposed to be hosted in USA is hosted in India, Netcraft Toolbar will highlight this problem and show the country's name in the toolbar.
- Protects users against popup windows which hides the address bar and browser navigations [18].

Limitations:

- ❖ Most phishing sites are hosted on hacked servers which host all legitimate websites and have been active for quite some time which means the attackers will be able to bypass the Since and Host labels.
- ❖ Country label is user dependent and users have to notice the fact that a website is not hosted in a country where it is supposed to be.

3.2 Microsoft SmartScreen Filter

Microsoft SmartScreen Filter is a tool for Internet Explorer 9 (IE9) users which uses blacklist and heuristic analysis to determine whether the page is phishing or legitimate. When a user visits a page using IE9, the contents of the page are compared against heuristic characteristics. If the page fails to pass the heuristic test, a yellow shield will appear warning the user about the contents of the page and will suggest the user not to enter any confidential information. However, if no suspicious properties are found, the tool will check its URL against a blacklist. If a match is found in the blacklist, a red shield will appear informing users about the blacklisted page. It is then up to the users whether they want to proceed or cancel the page. Users can also report to Microsoft about new fraudulent URLs using SmartScreen reporting feature. SmartScreen blacklist verifies URLs before adding them to the blacklist.

Advantages:

- SmartScreen provides additional security in a network as it allows the administrator to set up a group policy which restricts users from ignoring warning shown by SmartScreen Filter [19].
- SmartScreen also provides protection against downloadable malicious files like key-loggers.

Limitations:

- Blacklist needs to be updated regularly and users will be vulnerable to newly created phishing websites.

Firefox, one of the most used browsers available [20]; also uses blacklist-based approach to protect users against phishing. Other major browsers like safari [21] and Internet Explorer also use this approach. Firefox maintains 2 blacklists, remote and local. The local blacklist is downloaded on the user's browser and is updated every 30 minutes from an update server. This reduces network queries but a delay is introduced in blacklist and performance may suffer. The remote blacklist on the other hand is updated and more comprehensive as well because the local blacklist may be pruned due to size limitations. However, the remote blacklist is hosted on a lookup server and each time a query is made, it is encrypted before sending to increase the security. Response time is the main drawback of remote list. When a blacklisted page is detected, the page is disabled and user is notified about it by a warning sign. The user then has the option to either continue or close the page. Firefox also gives its users the option to report false negatives and false positives.

3.3 Heuristic Method

Heuristic approach uses HTML, website content or URL signatures to identify phishing pages. According to Sheng et al., [40], blacklists are less effective as compared to heuristic when protecting users at the start and tools that use heuristic and blacklist together are more accurate than tools with only blacklist. There has been a lot of research in the past on heuristic approach. Phishing websites are analyzed to make heuristics which are then later used to classify websites as either phishing or legitimate using machine learning models. Garera et al. [22] discovered heuristics by analyzing existing phishing URLs, while Ludl et al., [23] analyzed page structure.

The technique proposed by Garera et al., [22] relies on analyzing URLs to differentiate between a benign and phishing URL. A logistic regression classifier classifies a URL as either benign or phishing on the basis of 18 URL features selected. These features can be categorised into 4 groups; page based, domain based, type based and word based. The model was trained using a data set which consisted of a blacklist and a whitelist. 1220 URLs from the blacklist maintained by Google were used as training blacklist along with 113 most popular URLs as training white list. Experiments performed with the dataset and logistic regression algorithm yielded coefficients of the URL features, which showed that "White Domain Table" and "host obfuscated with IP" are the most informative features in determining phishing URLs.

Advantages:

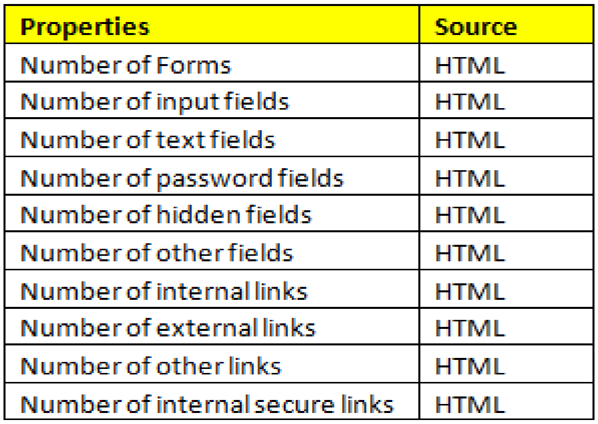
- No need to maintain a blacklist.
- Can identify and report an attack as soon as it is launched, no need to wait for an updated blacklist.

Limitations:

- High false positive rate.

According to Ludl et al. [23], the structure of a page can be used to distinguish between a legitimate and phishing website. 18 page properties are defined that can be extracted from the HTML and URL of a page. Table 5 shows the features and their sources. C4.5 decision tree is used as a classifier with a dataset that comprises of 680 phishing and 4149 legitimate pages. This model correctly classified 284 phishing websites but misclassified the other 396. The experiment shows that structural properties of websites can be used to determine their nature but the selection of these properties is very important and a larger number of properties will yield better results.

Table 5: Page properties and their source



Properties	Source
Number of Forms	HTML
Number of input fields	HTML
Number of text fields	HTML
Number of password fields	HTML
Number of hidden fields	HTML
Number of other fields	HTML
Number of internal links	HTML
Number of external links	HTML
Number of other links	HTML
Number of internal secure links	HTML

Advantages:

- Like all heuristic approaches, no need to maintain a blacklist and can identify and report an attack as soon as it is launched.

Disadvantage:

- High true negative rate. Too many phishing websites are classified as legitimate.

Chou et al., proposed and implemented a client side anti-phishing browser plug-in, SpoofGuard [24][25]. SpoofGuard evaluates a spoof index for each page which determines whether a page is legitimate or phishing. The spoof index is computed on the basis of page properties: domain name, link, URL, password, outgoing password, referring page, post data and image checks. If the computed spoof index is greater than a predefined threshold value, the page is classified as phishing and the user is notified about the threat. If the spoof index is less than threshold value, the page is classified and legitimate.

Advantages:

- Minimum or no user input required.
- High true positive rate.

Limitations:

- High false positive rate.
- Not effective against modern phishing attacks.

Mohammed Baihan [25] extended SpoofGuard's functionality and implemented SpoofGuard++. He enhanced the existing SpoofGuard functionality and added new functions as well to counter new phishing attacks. Existing SpoofGuard Image, URL and link check functionality was enhanced. HTML5 threat detection, Cross site scripting, URL shortening threat detection, HTML attachment attack detection and tab-nabbing attack detection functions were added to enhance SpoofGuard. 2 main components of SpoofGuard++ are DOM tree extractor and Phishing assessment manager. The output from DOM tree is used as input to Phishing assessment manager. Unlike SpoofGuard; which was available for both Firefox and Internet Explorer users, SpoofGuard was developed only for Internet Explorer 9 users {27][26].

4. CONCLUDING REMARKS

Most of the anti-phishing solutions discussed have limitations and require some sort of user input. In order to alleviate the growing phishing problem, it is important to identify a fake website and notify users when they encounter one. Users tend to ignore warning messages because extra effort is required. Majority of the existing industry and research solutions rely on either the blacklist model or heuristic based approach. According to Sheng et al. [28], blacklist and heuristic based approach when used together is the most effective approach against phishing.

Direction for Future Works

Based on the foregoing, Research is warranted into hybridizing client side anti-phishing techniques and so devise a solution that not only efficiently identifies fraudulent websites but also ensures that users pay attention to the warning messages displayed on sites being visited.

REFERENCES

[1] Ollman, G. (2004). The Phishing Guide. September, 2004. Available online at www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf

[2] Anderson, R. (2001). Security Engineering. John Wiley & Sons, Inc. New York USA.

[3] Watson D., Holz T. and Mueller S. (2005). Know Your Enemy: Phishing. The Honeynet Project & Research Alliance.

[4] Whitten, A. and Tygar, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In the 8th Usenix Security Symposium.

[5] Sullivan, B. (2004). Consumers Still Falling for Phish. Available Online at http://www.msnbc.msn.com/id/551990/.

[6] Whalen T. and Inkpen K. (2005). Gathering Evidence: Use of Visual Security Cues in Web Browsing. In Graphics Interface.

[7] Rachna D., Tygar J.D. and Marti A.H. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 581–590, 2006.

[8] Jagatic T. Johnson N. Jakobsson M. and Menczer F. (2006). Social Phishing. In Communications of the ACM.

[9] Bank, D. (2005). Spear Phishing Tests Educate People about Online Scams. The Wall Street Journal, August Edition. Available online at http://www.wsj.com/articles/SB112424042313615131

[10] Chandrasekaran M., Narayanan K. and Upadhyaya S. (2006). Phishing Email Detection Based on Structural Properties. In Proceedings of the 2006 International Symposium on World of Wireless, Mobile &

Mulotimedia Networks, Niagara falls, Canada. Available online at https://scholar.google.com/citations?user=9XFx3VMAAAAJ

[11] Fette I., Sadeh N. and Tomasic A. (2007). Learning to Detect Phishing Emails. In Proceedings of the International World Wide Web (WWW) Conference. pp. 649-656

[12] Shah R., Trevathan J., Read W. and Ghodosi H. (2009). A Proactive Approach to Preventing Phishing Attacks Using a Pshark, Sixth International Conference on Information Technology, pp. 1-7.

[13] Bergholz A., Chang J.-H., Paaß G., Reichartz F. and Strobel S. (2008). Improved phishing detection using model-based features. In Proceedings of the Conference on Email and Anti-Spam (CEAS), pp. 1-10.

[14] NETCRAFT INC. (2013). Netcraft Anti-Phishing Toolbar. Available Online at http://toolbar.netcraft.com/

[15] CLOUDMARK INC, (2012). Cloud mark desktop one. Available Online at http://www.cloudmark.com/desktop/download/

[16] Microsoft (2011). SmartScreen Filter. Available Online at http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/smartscreen-filter..

[17] Schneider F., Provos N., Moll R., Chew M. and Rakowski B. (2007). Phishing protection: Design documentation. Available Online at https://wiki.mozilla.org/Phishing_Protection:_Design_Documentation.

[18] Zhang Y., Egelman S., Cranor L. and Hong J. (2010). Phinding Phish: Evaluating Anti-Phishing Tools. In Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007). Available online at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.126.263

[19] Microsoft (2009). SmartScreen Filter and Resulting Internet Communication in Windows 7 and Windows Server 2008 R2. Available Online at http://msdn.microsoft.com/en us/library/ee126149(v=ws.10).aspx

[20] Net Applications. Inc. (2008). Browser market share q4. Available Online at at:http://marketsharehitslink.com/report.aspx?qprid=0&qpmr=15&qpdt=1&qpct=3&qp cal=1&qptimeframe=Q&qpsp=39

[21] APPLE INC. (2013). New Features in Safari. Available Online at http://www.apple.com/safari/features.html#security

[22] Garera S., Provos N., Chew M. and Rubin A.D. (2007). A Framework for Detection and Measurement of Phishing Attacks. In WORM '07: Proceedings of the 2007 ACM Workshop on Recurring Malcode, 9 New York, NY, USA. ACM, pp. 1-8.

[23] Ludl C., Mcallister S., Kirda E. and Kruegel C. (2007). On the Effectiveness of Techniques to Detect Phishing Sites. In DIMVA '07: Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer-Verlag, pp. 20-39.

[24] Chou N., Ledesma R., Teraguchi Y., Bonch D. and Mitchell J. (2005) Client-side Defense Against Web based Identity Theft. In 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego.

[25] SpoofGuard (2005). Client-side defense against web-based identity theft. Available online at http://crypto.stanford.edu/SpoofGuard/

[26] Baihan M. (2011) Anti Spoofing tool – Project background report. Unpublished Thesis (Msc.), University of Manchester.

[27] Herley C. (2009) So Long and no Thanks for the Externalities: The Rational Rejection of Security Advice by Users, Association for Computing Machinery, Inc., pp. 1-12

[28] Steve S., Mandy H., Ponnurangam K. and Lorrie C. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Pages 373-382. Available online at http://dl.acm.org/citation.cfm?id=1753383