Investigation of Phishing Attacks and Means to Utilize Anti Phishing Techniques

T. Venkat Narayana Rao[1] and Sreeja Reddy [2]
Professor[1], Student[2], Department of C.S.E, SNIST
Sreenidhi Institute of Science and Technology
Yamnampet,Hyderabad, T.S,India.

Abstract: Advancement of technology have both positive and negative impacts. Some of the negative impacts are cyber crimes. Cyber crimes have become more dangerous. Phishing is one of the cyber crime which results in exploitation of data. There are many phishing attacks which are identified every day. There are different techniques in phishing attacks. We have to reduce those attacks by employing suitable anti-phishing techniques. Some of the anti-phishing techniques and algorithms are discussed in this paper. History of phishing and the lifecycle are also discussed in this paper. People should be aware of all such phishing and the anti-phishing techniques. They have to be careful while checking their mails and should not click on any links or downloadable malware files.

***Keywords**: Cyber,hackers,theft,attacks,phishing.*

*****

I. Introduction

Cyber crimes are the most powerful attacks which are growing rapidly. Now-a-days every information between any organisation, company or even person is shared through internet. Internet is growing rapidly. The information shared should be secured and it should not be exploited by hackers.But there are many ways through which some illegitimate users (hackers) attempt to steal our information or personal credentials. Among all the cyber crimes, Phishing is a way through which a person can get the information such as usernames, passwords using emails and links etc. For example, usually people may have secured and strong passwords but whenever an attacker sends a mail usually with a link (hyper text transfer protocol) which asks them to update their passwords for any security reasons, then the user clicks on the given link and resets the password and in such cases the information is sent directly to the attacker. This is how phishing attack is processed. With these types of thefts, there are huge losses to different organisations.This usually costs many million dollars. Every day, there are many attacks which are launched with the aim of getting the information like passwords, login credentials, banks passwords, credit card numbers etc. by sending emails with links to spoofed websites. Paypal, ebay are some of the commonly spoofed websites[4]. When a user click on the link, a malicious malware is also installed on the computer and this malware affects our computer badly and this malware helps in exploiting the system vulnerabilities. Due to this attack, there will be compromised systems, which are attacked by the malware and the files or information on this system are not trusted. Figure 1.1 shows the report of phishing attack impacts. The attackers create some fake websites and lure the innocent users. There are many fake websites which are created every day. Phisher is a person who is involved in phishing activity and generally who initiates the attack.The statistics of phishing attack 2018 shows that major phishing attack is done in airlines, followed by banks and then online stores. Some other categories which are affected by phishing are global internet portals, payment systems, IMS, IT companies, telecommunication companies, government taxes, social network and blogs etc.

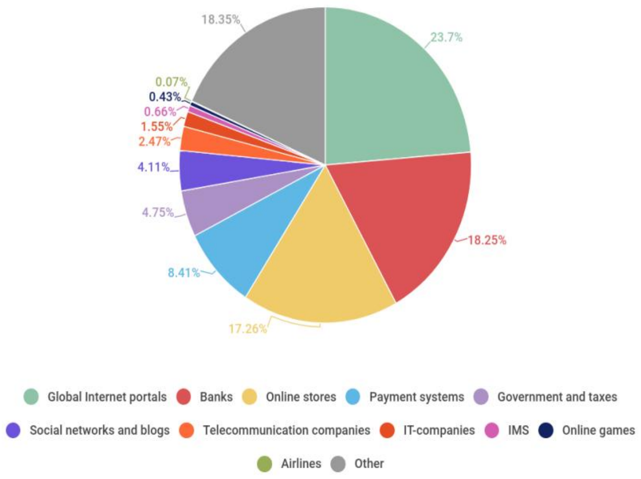


Figure 1.1 Phishing Attacks Impact

The most popular phishing sites hosting countries are Vietnam, united states, china, India ,Germany, France ,brazil, Russia , Spain and many others as shown in figure 1.2.

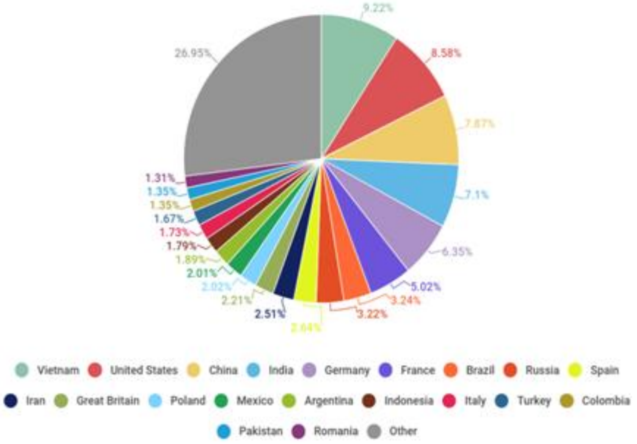


Figure 1.2: Popular Phishing Sites Hosting Countries

.

II. History of Phishing

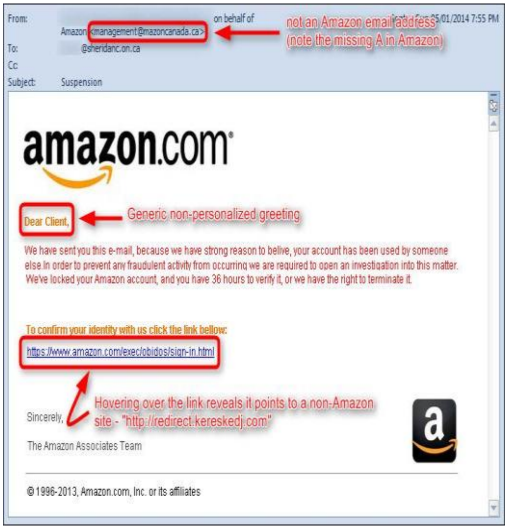
The term phishing is derived from two words Phreaking and fishing. Phreaking means making phone calls for free call back in late 70's and fishing is a method which uses abait to lure the target[6].

Phishingin 1995: The main target of phishing in 1995 is AOL users. The purpose of the attack is to steal sensitive information like passwords. The threat level is low. The techniques used is social engineering.

Phishing in 2001: The main target of phishing in early the 2000s is Ebayers and major banks. The purpose of the attack is to get credit card numbers and bank accounts details. The threat level is medium. The techniques used is social engineering and keyblogger.

Phishingin 2007: The main target of phishing in late 2000s is Paypal, banks,ebay. The purpose of the attack is to get bank accounts details.The threat level is very high. The techniques used is browser vulnerabilities and link obfuscation.

Examples of Phishing:



From: on behalf of
Amazon <management@mazoncanada.ca>
To: @sheridanc.on.ca
Cc
Subject: Suspension

not an Amazon email address
(note the missing A in Amazon)

Sent: 25/01/2014 7:55 PM

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

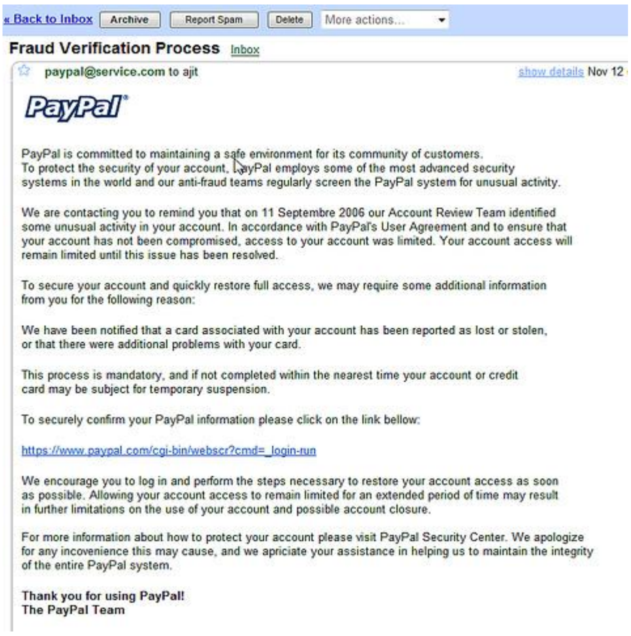
Sincerely,

The Amazon Associates Team

©1996-2013, Amazon.com, Inc. or its affiliates

Figure 2.1: example showing the phishing mail

In the above figure 3.1, there is an example showing the phishing mail which looks exactly like an original mail sent from an amazon website. Here, we can identify it as a fake mail using some techniques like, general non personalised greetings and when we point mouse to the link it reveals the point to a non- amazon site. We should be careful before clicking such mails[3].



Fraud Verification Process Inbox

paypal@service.com to ajit show details Nov 12

PayPal is committed to maintaining a safe environment for its community of customers.
To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We are contacting you to remind you that on 11 Septembre 2006 our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

To secure your account and quickly restore full access, we may require some additional information from you for the following reason:

We have been notified that a card associated with your account has been reported as lost or stolen, or that there were additional problems with your card.

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject for temporary suspension.

To securely confirm your PayPal information please click on the link bellow:

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account closure.

For more information about how to protect your account please visit PayPal Security Center. We apologize for any incovenience this may cause, and we apriciate your assistance in helping us to maintain the integrity of the entire PayPal system.

Thank you for using PayPal!
The PayPal Team

Figure 2.2:Example of Phishing Attack.

The above example a shown in Figure 2.2 is the phishing attack using paypal. It asks the users to click on the link and then assists the user to enter all the personal information related to bank accounts.

III. Life Cycle of Phishing

The life cycle of phishing involves some major stages. First the phishing scam begins and then some phishing message arrives at the users system and the message bears a deceptive view which is being sent from a authorised user[2]. Then the user interacts with the message by giving the users personal information as requested by the phishing message. If the user performs the required action, then phishers payload execution takes place, otherwise there will be no payload execution.This is the lifecycle of phishing attack as shown in figure 3.

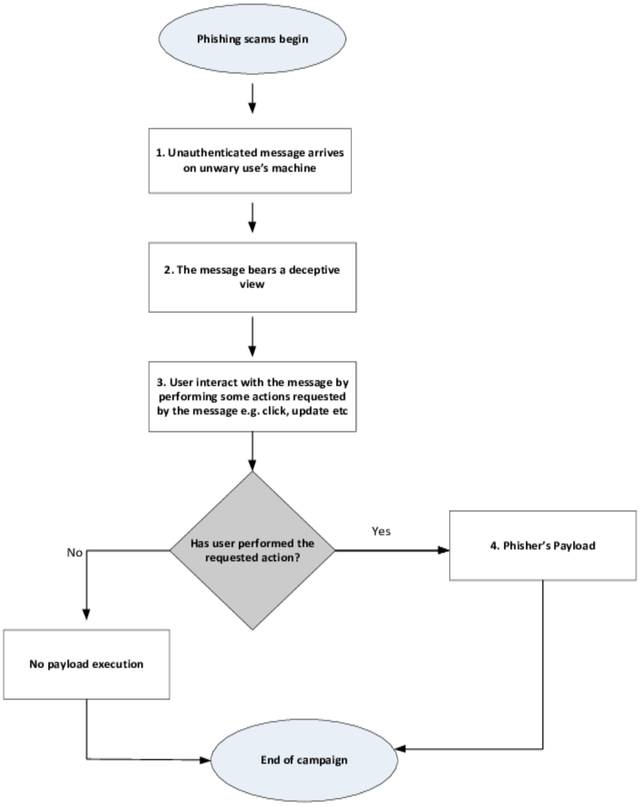

Phishing scams begin
1. Unauthenticated message arrives on unwary use's machine
2. The message bears a deceptive view
3. User interact with the message by performing some actions requested by the message e.g. click, update etc
Has user performed the requested action?
Yes
No
4. Phisher's Payload
No payload execution
End of campaign

Figure 3: Life Cycle of Phishing

IV. Types of Phishing Attacks

Phishing attacks are the most trending and dangerous attacks in these days. The phishers employ technically advanced methods for attacking or for getting the users sensitive information[5]. People should always be aware of these techniques. Some of the types of phishing attacks are:

A) Deceptive Phishing:This is the most common type of phishing attack. In this attack, the attacker sends a fake mail that exactly looks like mail which is sent from legitimate website. The mail requests the user to click on a link and enter all the information of the user, the attacker gets thesensitive information like account credentials. This is how attacker gathers the user information[11].

B) Malware–Based Phishing: In this type of attack, a malware is sent to the user computer in forms of attachment to mail or any downloadable file form any fake websites. When clicked on file or attachment, a malware is installed on computer and it slow down the victims computer and steals the sensitive information from the computer.

C) System Reconfiguration: In this attack, the attacker changes the settings or configuration on users computer. For example: the attacker changes the url name of the favourite file like for example "bankofindia.com" to "bankcfindia.com"

D) Host file Poisoning: In this type of attack, whenever a user enters a url to visit a website, it must be translated into an IP address and then redirect to the respective website. Here, the attacker poisons the IP address and redirects to another fake website which exactly looks like original website[8].

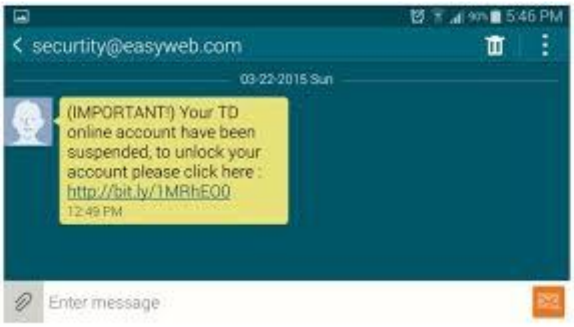
E) Data theft: Usually, all the sensitive information of a person is stored in the user computer. Data theft refers to the attack in which the attacker steals the sensitive information like account details, bank passwords, corporate records and other credentials.

F) DNS –Based Phishing: DNS based phishing refers to the type of phishing in which the attacker changes the hosts-id and returns a bogus address of the fake website and asks the users to enter the information and which is sent directly to the attacker. Unknowingly, user enters all the information trusting the original website. This is also called as "Pharming".

G) Content-Injection: This attack refers to the theft in which the attacker mislays the fake information with original content in the website and fakes an user to enter all the personal details.

H) Phishing through search engines: In this type of attack, the phisher creates a fake website for some products which are usually sold with low prices when compared to the original prices. Unsuspected users generally enter their information and bank account details for order placement and signup[9].

I) Phone Phishing: Phone phishing refers to the type of attack in which a phisher calls a user and they assists the people to dial a number. Through this the phisher gets the sensitive information related to bank accounts. These calls are usually done from fake caller ids as shown in figure 4.1.


5:46 PM

securtity@easyweb.com

03-22-2015 Sun

(IMPORTANT!) Your TD online account have been suspended, to unlock your account please click here : http://bit.ly/1MRhEO0
12:49 PM

Notice the sender's email above. Easyweb is the name of the online tool that is used to login to my bank account

Figure 4.1: Phone phishing

K) Man in the Middle Phishing: MIM phishing is the phishing in which the phisher will be in between the user and the original website.When the user is in active state, the phisher takes the information which is shared between the user and the website without any interruption.After the user is in inactive state, the phisher uses these information. It is shown in Figure 4.2.

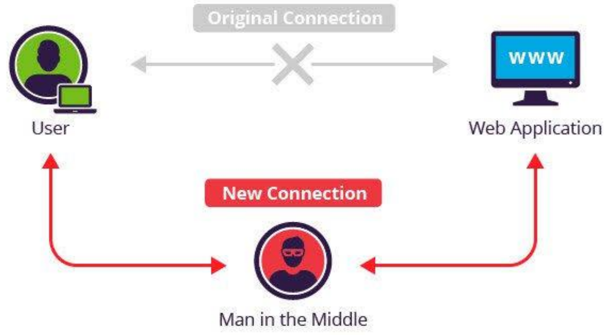


Figure 4.2 : Man in the Middle Phishing

L) Web trojans: These are usually used to steal the information of the user and sends to the attacker. This generally runs at the time of login.

M) Key loggers and Screen loggers: This is usually called key stroke logging. The attacker records the key strokes which are entered by the user without having the knowledge that someone is monitoring the user actions as shown in figure 4.3. It can generally be either a software or hardware[3][4].

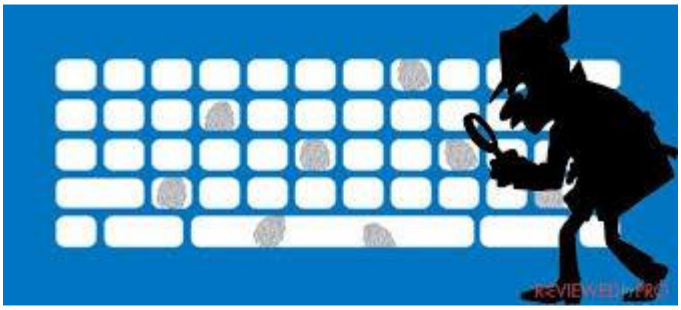


Figure 4.3: Key loggers and Screen loggers Phishing

V. Causes , Steps and ways to avoid of Phishing

Phishing attack is caused due to some general reasons. Some of them are :

1. Due to misleading emails.

2.Source address is not checked properly by the user.

3. There are some vulnerabilities in browser.

4.There is no strong authentication at the bank websites or at any other institutional websites.

5. Digital signatures usage is very limited.

6.There are no secured desktop tools available and lack of user knowledge on phishing attacks and some vulnerabilities in websites causes the attack of phishing.

The steps involved in Phishing attack:

Phishing attack is a procedure to get the users sensitive information. There are five major steps involved in phishing attack.They are:

1.Planning: In this step the phisher plans the attack. The outline of the attack is clearly prepared in this phase.

2.Setup:The phisher set up the attack according to the sketched plan and follows as per the plan.

3.Attack:In this stage, the phisher executes the attack and some code or message is sent to the victims computer through different techniques which have been discussed in this paper.The victim without having any knowledge responds to the fake message and enters all his personal information.This information is directly sent to the phisher.

4.Collection: The information which have been sent from the victims computer is collected in this stage.

5.Fraud: The information which have been collected from the user is used by the phisher in different ways like blackmailing the user etc. This stage is called Fraud.

Protection from the Phishing Attack:

1) Awareness:

The user should be aware of all the updated and latest phishing attack techniques.They should be careful while creating passwords and these passwords should not shared with others. Users must be in a position to identify the fake websites from the original websites. User education is very important.

2) Network layer protection:

Some protection at the network level is very protective against the phishing attack. Some set of domain names or IP address should not be allowed to enter into the network which is done by DNS protocol[1].This should be frequently updated by monitoring the network traffic.

3) Authentication mechanisms:

This is usually done at domain level. This authentication based mechanisms checks whether the received message is sent from an authorised user. Email communication systems use these authentication mechanisms and these mechanisms improve security also[5][6].

To avoid the phishing attacks:

At first the users should be aware of these phishing attacks. Some of the ways to avoid these attacks are:

1) Do not click without thinking on a link.
2) Use antimalware software.
3) Firewalls installation in the computer.
4) Usage of anti-phishing tools.
5) Be aware of pop ups and donot click unnecessarily.
6) Personal information should not be revealed.
7) Regularly examine your online accounts.
8) Verification of a sites security.
9) Frequently change passwords[8][9].

VI. Anti-Phishing and Anti-Phishing Detector

Anti phishing is a process which detects and prevents phishing attacks[7]. There are many anti-phishing tools. These tools should be installed in every user computer so that the phishing attacks will be reduced to a greater extent. This protects the user computer from phishing attacks. Scientists named, Lakshmi Rajamani and Mahmood Ali discovered and implemented a technique called Association rule mining especially for deceptive phishing attacks. This attack protects the users system from these phishing attacks by identifying instant messengers.Whenever messages are exchanged between users of some instant messaging system, this anti –phishing detector detects any phishing attacks if implemented. Another algorithm named, Apriori algorithm is also used to detect the deceptive phishing attack[10].

VII. Techniques for detection of Phishing

A. Email detection

Generally when a phisher sends some phishing mails, this approach is used. Jemal, isredzarahmi and kim introduced this hybrid feature selection technique to discover the phishing mails. This technique identifies the mail by extracting some information from the mail like message id field, email header which helps to detect the behaviour of the sender.

B. Link algorithm

This algorithm is usually used to detect and prevent the phishing attacks in web. This is implemented by Umeshwarade, Nilkeshsurana and Nehasabe. Whenever a phisher sends a link. This algorithm examines the link using the characteristics of links to detect the phishing attacks which are done using these links. This algorithm is used not only for detecting the phishing links but also prevents the malware from installing into the users system.

C.Hadoop Approach

Hadoop is actually used to divide an application into many small parts which are called fragments. It generally deals with large data. Hadoop kernel, hive, hbase and Mapreduce , these constitute a Apache hadoop ecosystem. Whenever a phisher sends a spoofed website, this system examines the entire website and finds out whether the website examined by the system is phished or not. This approach generally takes less time and offer more security.

D. Honey pots

This approach detects the phishing attacks using Honey pots. Honey pots are the traps that are set to detect the phishing attacks.These are most powerful anti phishing techniques. These collect the critical and most important details or the information about the phishing attacks activities which are being involved[10]. Some honeytokens are being sent to the phisher to confuse the phisher and extract the information of the phisher.These honey pots provides greater security and usually discourages phishers by detecting them. But the major drawback of this honeypots approach is, its applicability to online banking systems[11].

VIII. Conclusion

Phishing attacks are rapidly increasing day by day.We have to prevent these phishing attacks so that our information will be confidential and there will be no loss. This paper, is emphasized on phishing attack types and its statistics. The different techniques of phishing attacks and examples have been discussed. There should be awareness among the users about the phishing attacks and the different techniques. The information shared between the people should be secure enough hence, anti phishing techniques and different anti phishing tools are being narrated. Some algorithms like link algorithm,APD and apriopri algorithms are also discussed to avoid phishing attacks.

References

[1]. P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, andE. Nunge, “Protecting people from phishing: the design and evaluationof an embedded training email system,” in Proceedings of the SIGCHIconference on Human factors in computing systems, ser. CHI ’07. NewYork, NY, USA: ACM, 2007, pp. 905–914.

[2]. A. Alnajim and M. Munro, “An anti-phishing approach that uses trainingintervention for phishing websites detection,” in Proceedings of the2009 Sixth International Conference on Information Technology: NewGenerations. Washington, DC, USA: IEEE Computer Society, 2009,pp. 405–410.

[3]. “Learning to Detect Phishing Emails” Ian Fette Schoolof Computer Science Carnegie Mellon UniversityPittsburgh, PA, 15213,

[4]. ”A survey on phishing detection and prevention technique”ArchitShukla, LalitGehlod, 2International Journal Of Engineering And Computer Science ISSN: 2319-7242Volume 3 Issue 5 may, 2014 Page No. 6255-6259.

[5]. ”STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS”Dr.RadhaDamodaram International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056Volume: 03 Issue: 01 | Jan-2016

[6]. ”A Review on Phishing Attacks and Various Anti Phishing Techniques V. Suganya International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016.

[7]. Aanchal Jain and Prof. VineetRichariya 2011,”Implementing a Web Browser with Phishing Detection Techniques” World of Computer Science and Information Technology Journal, Vol. 1, No. 7, 289-291.

[8]. “Phishing Detection and Prevention Techniques & Analysis of Various Recent Phishing Attacks” Prof. Gayathri Naidu International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 8 August 2017, Page No. 22322-22326.

[9]. NilkeshSurana, Prabhjot Singh, UmeshWarade, NehaSabe 2015,‖ Detection and Prevention of Phishing Attacks in Web International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04, Issue.08, April-2015.

[10]. MatherAburrous, M.A. Hossain, KeshavDahal, FadiThabtah “Prediction phishing websites using classification mining techniques with experimentalcase studies” in proceedings of Seventh International Conference on Information Technology, Las Vegas, NV, pages 176-181, 2010.

[11]. Huajun Huang Junshan Tan Lingxi Liu “Countermeasure Techniques for Deceptive Phishing Attack” International Conference on NewTrends in Information and Service Science.NISS'09.June-2009.