ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Development Review on Phishing: A Computer Security Threat

Gaurav Kumar Chaudhary[1]
BE student, Department of computer science and Engineering, ITM
Gwalior, Madhya Pradesh, India

Abstract: Phishing is kinds of attack in which criminals are use spoofed emails and fraudulent websites to trick people into giving up personal information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. This review looks at the phishing problem holistically by examining various research and review produced till now. . It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. To protect user against phishing, various anti-phishing techniques have been proposed that follow different strategies like client side and server side protection.

In this review we have studied phishing in detail (including attack process and classification of phishing attack) and reviewed some of the existing anti- phishing techniques along with their advantages and disadvantages.

This review also concerned with anti-phishing techniques. There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing. No single technology will completely stop phishing. However a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it.

Keywords: spoofed emails, fraudulent website, phishing, anti-phishing, social engineering.

I. INTRODUCTION

Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion. The word "phishing" appeared around 1995, when Internet scammers were using email lures to "fish" for passwords and financial information from the sea of Internet users; "ph" is a common hacker replacement of "f", which comes from the original form of hacking, "phreaking" on telephone switches during 1960s. Early phishers copied the code from the AOL website and crafted pages that looked like they were a part of AOL, and sent spoofed emails or instant messages with a link to this fake web page, asking potential victims to reveal their passwords.

A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. The information flow is shown in Figure 1.

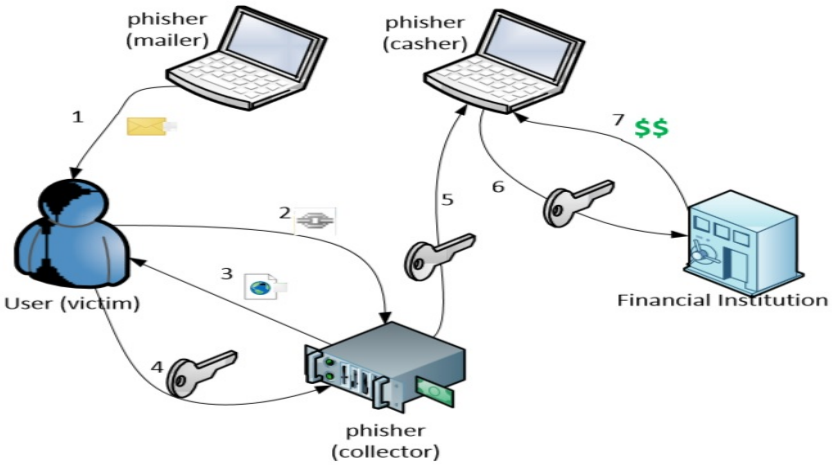


Fig. 1 Phishing information flow

II. TYPES OF PHISHING.

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

Clone phishing

In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.

Spear phishing

Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization. Spear phishing is also being used against high-level targets, in a type of attack called “whaling”. For example, in 2008, several CEOs in the U.S. were sent a fake subpoena along with an attachment that would install malware when viewed. Victims of spear phishing attacks in late 2010 and early 2011 include the Australian Prime Minister’s office, the Canadian government, the Epsilon mailing list service, HBGary Federal, and Oak Ridge National Laboratory.

Phone phishing

This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.

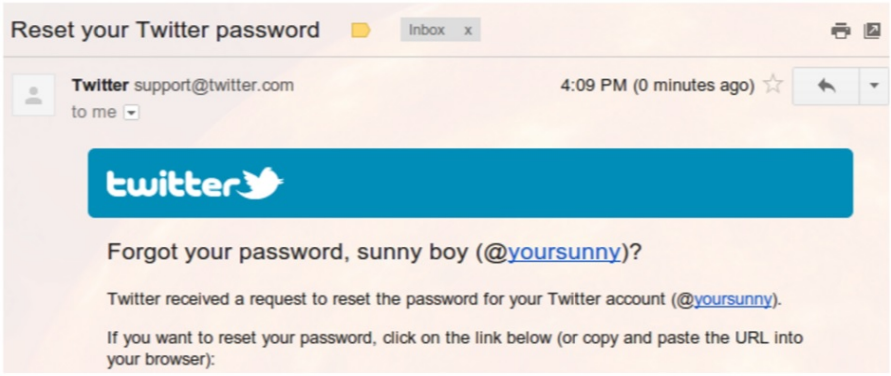
III. PHISHING TECHNIQUES AND COUNTERMEASURES

Various techniques are developed to conduct phishing attacks and make them less suspicious. Some of them are following:

- ***Email Spoofing***

A spoofed email is one that claims to be originating from one source when it was actually sent from another. Email spoofing is a common phishing technique in which a phisher sends spoofed emails, with the sender address and other parts of the email header altered, in order to deceive recipients. Spoofed emails usually appear to be from a website or financial institution that the recipient may have business with, so that an unsuspecting recipient would probably take actions as instructed by the email contents, such as:

- reply the email with their credit card number
- click on the link labelled as "view my statement", and enter the password when the (forged) website prompts for it
- Open an attached PDF form, and enter confidential information into the form.



Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. Since most SMTP servers are mutually-TCP-addressable hosts on the public Internet, receiving and relaying SMTP servers are able to see the IP address of the sending host. SPFv1 protects the envelope sender address, the HELO domain and the MAIL FROM address, by verifying sender IP addresses: SPFv1 allows the owner of a domain to specify a list of IP addresses that are allowed to send emails from their domain, and publish this information in the domain's DNS zone; a receiving server may query DNS to check whether the message comes from one of those whitelisted addresses.

While another technical method to prevent sender address forgery is DKIM. Domain Keys Identified Mail (DKIM) allows an organization to take responsibility for transmitting a message in a way that can be verified by a recipient. The author, the originating sending site, an intermediary, or one of their agents can attach digital signatures onto a message. The message headers and body, including the originator address (the from header field), are signed. The DKIM-Signature header field includes the signature, the signing domain, and information about how to retrieve the public key.

Web Spoofing

A phisher could forge a website that looks similar to a legitimate website, so that victims may think this is the genuine website and enter their passwords and personal information, which is collected by the phisher. Modern web browsers have certain built-in security indicators that can protect users from phishing scams, including domain name highlighting and https indicators. However, they are often neglected by careless users.

Pharming

Pharming is a type of attack intended to redirect traffic to a fake Internet host. There are different methods for pharming attacks, among which DNS cache poisoning is the most common.

Domain Name System (DNS) is a critical piece of Internet infrastructure. Designed as a distributed system, DNS publishes a hierarchical database by a hierarchy of name servers. To improve performance, clients contact local DNS resolvers maintained by local ISPs, which can cache records from name servers. Clients, resolvers, and name servers talk with each other on UDP port 53.

DNS is critical to Internet security. As shown in Section 3.1, SPF, DKIM, and Sender ID all rely on DNS; if DNS is compromised, spoofed emails can get through these signature-based countermeasures. Web spoofing can also be conducted by making DNS respond with the address of phisher's server.

DNS cache poisoning attempts to feed the cache of local DNS resolvers with incorrect records. This is possible because: DNS runs over UDP, and it's easy to spoof the source address of a UDP packet; the DNS packet header contains a 16-bit query ID field, which is relatively short so a birthday attack is feasible.

Google Public DNS, the largest public DNS resolver in the world, mitigates cache poisoning attacks by adding entropy to queries:

- use a random source UDP port
- randomly choose a name server among configured name servers of a zone

IV. Reason of Phishing

Phishing had been widely used at least half a decade ago but it still remains as one of the popular method to scam internet users. Just recently, thousands of Tumbler bloggers were affected by a phishing attack which caused their credentials such as username, passwords, and email addresses to be stolen. Many of us might still be wondering why there are so many victims out there even though we had been taught from time to time to stay aware of a phishing scam. There are five reasons here why phishing is still a popular trick and below are the reasons.

- ***Availability of personal data on social networks***

The explosion of social networks has made it easier than ever to acquire specific information on a targeted victim. The deterrence factor of having to manually obtain the pertinent data could also be alleviated by the use of software that taps into the APIs (Application Programming Interface) offered by most social networks.

- ***Trend of data compromises***

There has been an ongoing trend of data compromises in which email and personally identifiable data have been stolen. To name just a few here, the Epsilon data breach saw hackers gaining illicit access into the company's system and presumably making away with email addresses and contact details of these clients. Beyond five financial organizations that were affected, drug giant GlaxoSmithKline PLC have also issued a warning to customers that their email addresses, names, and the "product website" on which they have registered with the company – may have been stolen.

It is important to remember that not all businesses opt to come clean on data breaches. Moreover, the average hackers endeavour to erase their tracks after gaining what they came for. The bottom line: A wealth of stolen information is floating around out there available for exploitation.

- ***It tricks the victim with fear***

One of the most common method is to trick the victim by sending them an email and tell them that their internet banking account is being compromised and need to click on a link to resolve the issue. Once the user followed the link, the user will be redirected to some forged website that looks similar to the banking website which requires the user to input his/her username and password. Once that form is sent, all the data will be transmitted to the attacker controlled server. Users who have a large

amount of cash in their banking account will be scared to see this mail and some of them will follow the mail to avoid their account being compromised.

- ***It tricks the victim with special interest***

Some scammers use the scenario such as winning lottery or viewing adult material to create a temptation for the victim to click on a link that redirects to the phishing site. Just recently, Tumbler bloggers were asked to re-verify their accounts by entering the username and password in order to continue and view the adult content. At times, it is not always money related issue can relate to phishing scam, but also special interest as mentioned can relate to a phishing scam.

- ***Effectiveness of spam filters against traditional spam***

Spammers have tried practically every trick in the book over the years, including the use of image spam, creative misspelling of words, and even resorted to the use of email attachments. Modern spam filters have the benefit of borrowing from all the lessons learnt since the invention of electronic mail, and employs a plethora of advanced technologies such as cloud-computing to eliminate them. Indeed, one may almost be tempted to consider the problem of spam as one that has already been overcome on some days. As you can imagine, spammers are forced to adopt sophisticated spear phishing techniques in order to reach their victims.

Fig. 3 chart showing the increase in phishing reports from October 2004 to June 2005

V. DAMAGE CAUSED BY PHISHING

The damage cause by phishing ranges from the users who become victim to a phishing site, some of these examples are:

Loss of e-mail accounts

Substantial Financial Loss

Users cannot access accounts that they own

Phishers can use the information they gain to create accounts in their victim's name. They can then also ruin a person's credit or even prevent the user from accessing their account is estimated that, between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing totalling approximately $929 million.

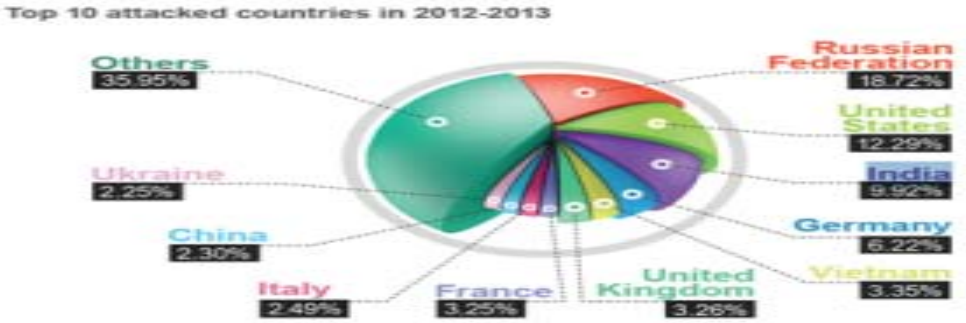


Fig. 4: Kaspersky Lab report: 37.3 million users experienced phishing attacks in the year 2012-2013

VI. ANTI – PHISHING TECHNIQUES

As recently as 2007, the adoption of anti-phishing strategies by businesses needing to protect personal and financial information was low. Now there are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing. These techniques include steps that can be taken by individuals, as well as by organizations. Phone, web site, and email phishing can now be reported to authorities, as described below.

Social Responses

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer phishing tactic, which uses phishing emails targeted at a specific company, known as spear phishing, has been harnessed to train individuals at various locations. In a June 2004 experiment with spear phishing, 80% of 500 West Point cadets who were sent a fake email from a non- existent Col. Robert Melville at West Point, were tricked into clicking on a link that would supposedly take them to a page where they would enter personal information. (The page informed them that they had been lured.)

People can take steps to avoid phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by phishers), it is a sensible precaution to contact the company from which the email apparently originates to check that the email is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message.

Technical Responses

Anti-Phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

a. Helping to identify legitimate sites

b. Browsers alerting users to fraudulent websites

c. Augmenting password logins

d. Eliminating Phishing mail

e. Monitoring and takedown

Legal Responses

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected Phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit

card information. In the United States, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005.Companies has also joined the effort to crack down on Phishing.

Using anti-phishing software

Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate web sites. Anti-phishing functionality may also be included as a built-in capability of some web browsers.

Some of the Client-based anti-phishing programs are:-

avast

Avira Premium Security Suite

EarthLink Scam Blocker (discontinued)

eBay Toolbar

Some of the Cloud-based anti-phishing services are:-

google Safe Browsing API

Web root Real-time Anti-Phishing API

isitphishing.org (http://www.isitphishing.org) - URL analysis service /api

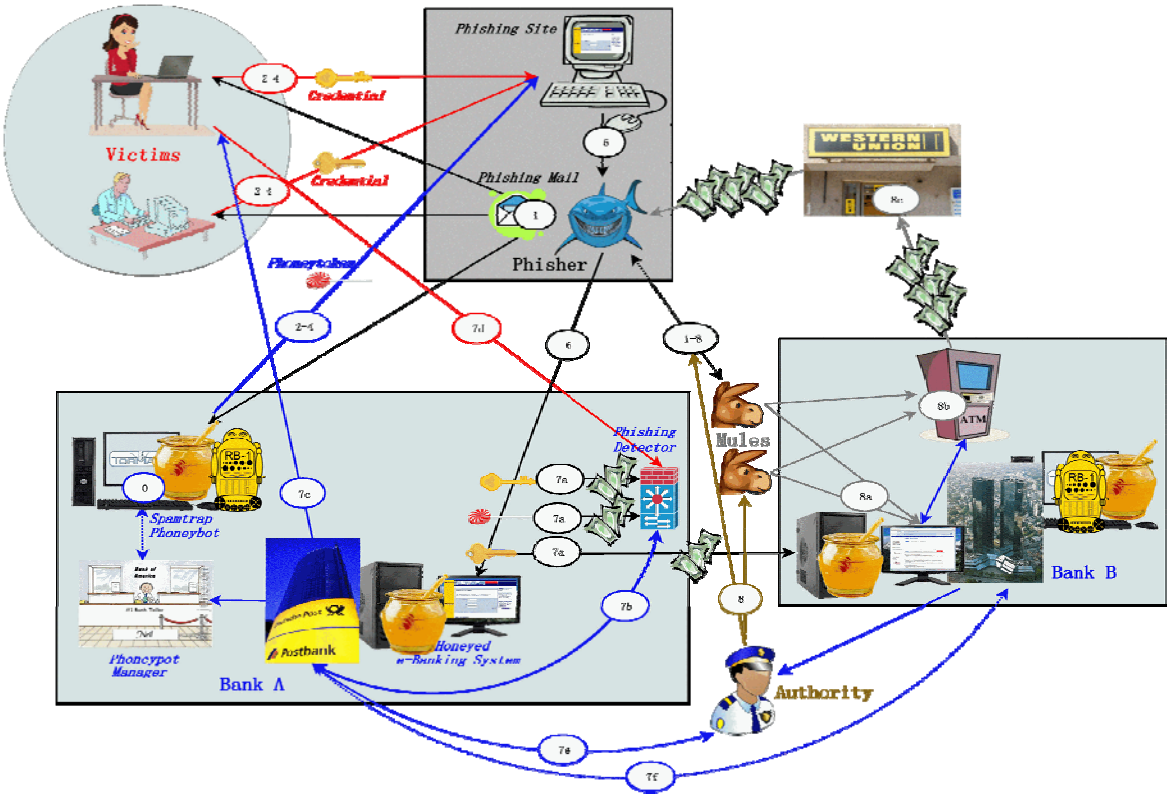


Fig. 5: Anti-phishing framework

VII. ANTI –PHISHING EFFECTIVENESS

A study conducted by 3Sharp released on September 27, 2006 tested the ability of eight anti-phishing solutions to block known phishing sites, warn about phishing sites, and allow good sites. The study, which was commissioned by Microsoft and

titled "Gone Phishing: Evaluating Anti-Phishing Tools for Windows", concluded that Internet Explorer and Netcraft Toolbar were the most effective anti-phishing tools.

A later independent study, conducted by Carnegie Mellon University CyLab titled "Phinding Phish: An Evaluation of Anti-Phishing Toolbars", released November 13, 2006, tested the ability of ten anti-phishing solutions to block known or warn about phishing sites, not block or warn about legitimate sites, as well as usability testing of each solution. Of the solutions tested, Netcraft Toolbar, EarthLink Scam Blocker and Spoof Guard were able to correctly identify over 75% of the sites tested, with Netcraft Toolbar receiving the highest score, without incorrectly identifying legitimate sites as phishing. Severe problems were however discovered using Spoof Guard, and it incorrectly identified 38% of the tested legitimate sites as phishing, leading to the conclusion that "It would seem that such inaccuracies might nullify the benefits Spoof Guard offers in identifying phishing sites." Google Safe Browsing (which has since been built into Firefox) and Internet Explorer both performed well, but when testing ability to detect fresh phishes Netcraft Toolbar scored as high 96%, while Google Safe Browsing scored as low as 0%, possibly due to technical problems with Google Safe Browsing. The testing was performed using phishing data obtained from Anti-Phishing Working Group, Phish Tank and an unnamed email filtering vendor.

The latest study, conducted by Smart Ware for Mozilla, released November 14, 2006, concluded that the anti-phishing filter in Firefox was more effective than Internet Explorer by more than 10%. The results of this study have been questioned by critics, criticising that the testing data was sourced exclusively from Phish Tank, itself an anti-phishing provider. The study only compared Internet Explorer and Firefox, and left out among others Netcraft Toolbar and the Opera browser, both of which use data from Phish Tank in their anti-phishing solutions. This has led to speculations that, with the limited testing data, both Opera and Netcraft Toolbar would have gotten a perfect score had they been part of the study.

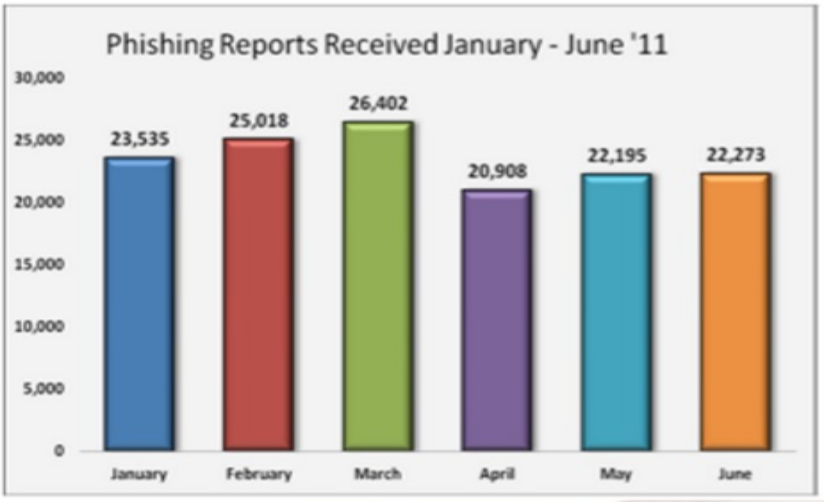


Fig. 6: Phishing activity trend report

The number of unique phishing reports submitted to APWG in H1, 2011 reached a high of 26,402 in March, dropping to the half year low of 20,908 in April as shown in figure 6.

The report depicted that Financial Services continued to be the most targeted industry sector in the first half of 2011as can be seen from figure 7.

VIII. Conclusion and Future Work

In the above study we can conclude that most of the anti- phishing techniques focus on contents of web age, URL and email. Character based anti-phishing approach may result in false positive but content based approach never results in false positive. Attribute based approach consider almost all major areas vulnerable to phishing so it can be best anti-phishing approach that can detect known as well as unknown phishing attack. Identity based anti-phishing approach may fails if phisher gets physical access to client's computer. As a future work on phishing we can do more work on server side security. In the server side security policy we use dual level of authentication for user by which only authentic user can get the access of his account, and to educate the user about this policy will results in avoiding user to give his sensitive information to phished web site.

References

1. Mutton, Paul. "Fraudsters seek to make phishing sites undetectable by content filters". Netcraft. Archived from the original on 2011-01-31. Retrieved July 10.
2. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter.Handbook of Information and Communication Security. Springer. ISBN 9783642041174.
3. "Internet Banking Targeted Phishing Attack".Metropolitan Police Service. 2005-06-03. Archived from the original on 2010-02-18. Retrieved 2009-03-22.
4. "Anti-Phishing Working Group: Vendor Solutions". Anti-Phishing Working Group. Archived from the original on 2011-01-31. Retrieved July 6, 2006.
5. Aryan Chandrapal Singh: Phishing: A Computer Security Threat. Volume 1, Issue 7, December 2013 International Journal of Advance Research in Computer Science and Management Studies.
6. Gaurav, Madhuresh Mishra, Anurag Jain: Anti-Phishing Techniques: A Review International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 2,Mar-Apr 2012, pp.350-355
7. Matthew Dunlop, Stephen Groat, and David Shelly" GoldPhish: Using Images for Content-Based Phishing Analysis", in proceedings of internet monitoring and protection(ICIMP),fifth international conference, Barcelona, Pages 123-128, 2010.
8. V.Shreeram, M.Suban, P.Shanthi, K.Manjula "Anti- phishing detection of phishing attacks using genetic algorithm" in proceedings of Communication control and computing technology(ICCCCT),IEEE international conference, Ramanathapuram , pages 447-450, 2010.
9. Phishing activity trend report 1st half /2011,http://www.antiphishing.org.
10. Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347-352, 2009 .
11. Mitesh Bargadiya, Vijay Chaudhary, Mohd. Ilyas Khan, Bhupendra Verma "the web identity prevention: factors to considers in the anti-phishing design" internation journal of engineering science and technology vol. 2(7), 2010.
12. Huajun Huang Junshan Tan Lingxi Liu "Countermeasure Techniques for Deceptive Phishing Attack" International Conference on New Trends in Information and Service Science. NISS '09. June-2009.
13. http://www.symantec.com/business/resources/articles/article.jsp?aid=phishers_targeting_the_governmen t.
14. Juan Chen, Chuanxiong Guo-"Online Detection and Prevention of Phishing Attacks (Invited Paper)"in proceedings of Communicational and networking in china, first international conference, Beizing, pages 1-7, 2007.

AUTHOR(S) PROFILE

Gaurav Kumar Chaudhary , doing Bachelor of engineering in Computer Science and engineering branch from Institute of Technology and Management(ITM) Gwalior, Madhya Pradesh, India . Recently in the third year of engineering and have a keen interest on study of Research paper published.