Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages 17 March 2018
Peer Reviewed Refereed Research Journal

Anti-phishing measures against phishing attack in the state of art

Dr. Raksha Chouhan (Asst Professor)
Swarnjeet Arora (Associate Professor)
Raksha Thakur (Asst Professor)
Anukool Hyde (Associate Professor)
Prestige Institute of Management and Research
Indore, Madhya Pradesh, India

Abstract

Anti phishing measures have been implemented to combat with rising phishing attacks. Most of the cyber attack starts with a phishing email and among all internet scams phishing attacks have become most popular because of their large-scale information capturing behavior. According to statistical data more than 1000 phishing attacks are launched every month and over the last few months phishing attacks have become more effective and complex to track and challenge. An online theft with the intension of stealing sensitive information like credit card information or online banking password is known as phishing whereas anti phishing techniques attempts to protect users against spoofed web site based phishing attacks. Thus development and awareness towards anti-phishing measures and strategies has become demand of the state of the art. Greater number of countermeasures are invented and deployed also in this direction. This study is an examination of the analysis and critique found in the ways adopted at various levels to counter the rise of phishing attacks as well as new techniques being adopted for the same. Comparative study of various anti phishing measures has been done so that suitable technique can be adopted to provide more security as well as researchers can get direction for future work towards anti-phishing strategic development.

Keywords: *phishing, Internet, Hacking tricks, Anti-phishing countermeasures etc.*

1 Introduction

Phishing attacks are increasing in multiple occurrences and complexity has been increased continuously. Now a day's phishing has become serious problem and no corner of the world is unaffected with it. The majority of cyber attacks begin with a user clicking on a phishing email almost all kind of organizations like financial/educational organizations, commercial web sites and end-users are suffering from phishing. Several hundred companies are being targeted regularly, at least every few weeks, while a smaller number of companies are attacked intermittently. According to APWG first half 2017 report, Phishing attacks occurred most frequently in the Payment, Financial, and Webmail sectors. As shown below [19]-

	January	February	March	April	May	June
Number of unique phishing websites detected	42,889	50,567	51,265	50,328	45,327	50,720
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	96,148	100,932	121,860	87,453	93,285	92,657
Number of brands targeted by phishing campaigns	424	423	444	460	457	452
Number of domain names for attacks	13,977	15,877	17,397	21,652	21,373	18,404

Table 1: Statistical Highlights of 1H 2017

As per the APWG 2nd Quarter 2017 report the most targeted industry sectors were financial institutions, logistics and shipping and cloud storage companies[19].

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages 17 March 2018
Peer Reviewed Refereed Research Journal

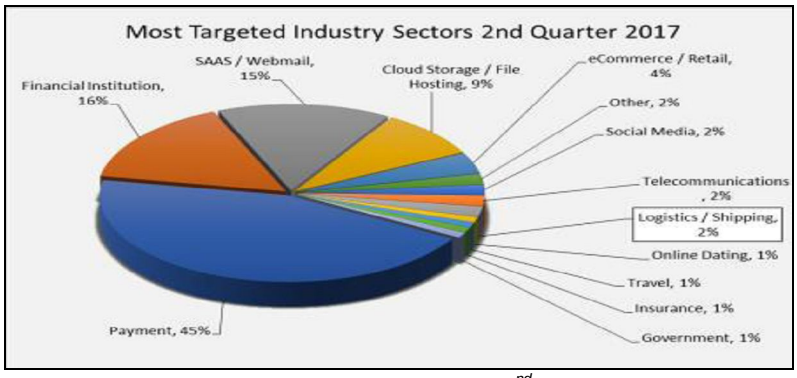


Fig 1: Most targeted industry sectors 2nd quarter 2017

It is a form of social engineering in which an attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking e-communications from a trustworthy or public organization in an automatic fashion is called as phishing [1] or we can say it is the practice of directing users to fraudulent web sites [2]. The word 'Phishing' first appeared in 1996 [3]. It is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information etc from users. The last years have brought a dramatic increase in the number and sophistication of such attacks. Attackers are employing a large number of technical spoofing tricks such as URL obfuscation and hidden elements to make a phishing web site look authentic to the victims. Phishing attacks use a combination of social engineering and technical spoofing techniques to convince users into giving away sensitive information (e.g., using a web form on a spoofed web page) that the attacker can then use to make a financial profit [4]. A method in which hackers capture the trusted brands of well known financial institutions and tactfully asking users personal identification through false/fake website forms. We can define it as "The act of convincing users to provide personal identification information, such as social security numbers or bank information, for explicit illegal use" [5]. A phishing attack is most often initiated with a special type of spam (unsolicited email) containing a link to a misleading domain name, which appears to be a legitimate site. The email tricks the recipient into visiting the spoofed web site. In 2005 David Levi made over $360,000 from 160 people using an eBay Phishing scam. Over 28,000 unique phishing attacks reported in Dec. 2006, about double the number from 2005 [10]. According to Anti-Phishing Working Group (APWG) "Phishing Activity Trends Report-2nd Half 2008' says "Approximately 85% of phishing attacks target financial institutions and payment services" and by Global Phishing Survey says " Over 80% of domains used for phishing are compromised or hacked domains. (Only 3.5% of domain names used for phishing contain or use a brand name or misspelling.)" Most phishing web sites are active for about 20 hours until they are taken down. Actually, the phishing site is designed to install malicious software or acquire personal information, including credit card numbers; personal identification numbers (PINs), social security numbers, banking numbers, and passwords. This information is then used by the phishes for identity theft, to steal money, or to commit other fraudulent schemes [6]. Various stages of cyber attack evolution has been shown below from year 1980 to the year 2000+ [9]:

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages 17 March 2018
Peer Reviewed Refereed Research Journal

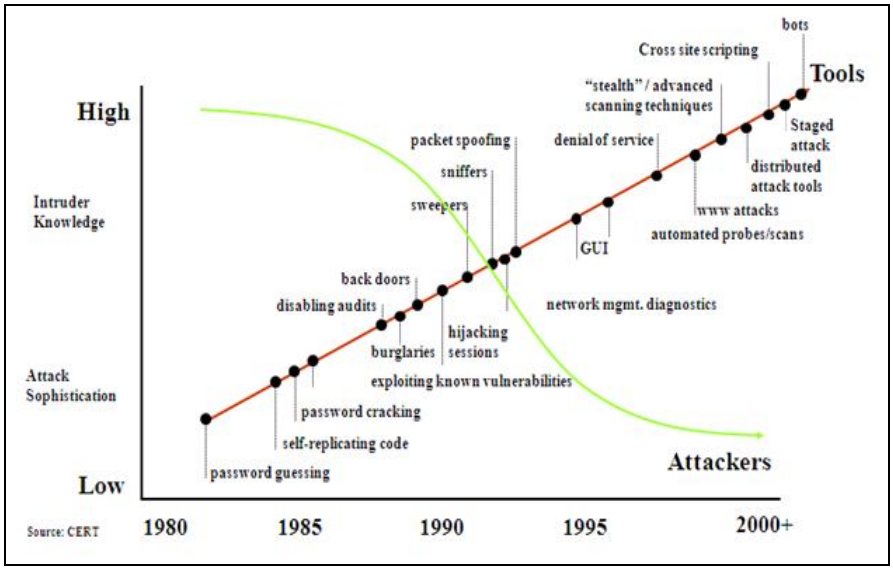


Fig 2: Various stages of cyber attack evolution

Common characteristics of phishing scam emails

1 Spontaneous requests to provide sensitive information
2 Genuine content appearances
3 Disguised hyperlinks and sender address
4 Email consists of a clickable image
5 Generic Greetings
6 Use various ruses to entice recipients to click

1 Rationale and Objectives of The Study

This study provides a proposal to evaluate the completeness and capability of both individual and aggregated anti-phishing controls by identify security and non-security requirements of anti phishing systems. This study explores concepts and working process of phishing by specifying a short summary of the facts and figures related with online and offline fraud when user is busy in performing transactional activities. An attempt towards efficacy of available anti-phishing measures has also been done so that user and companies can take precautions towards phishing attacks to protect their information. A direction has been sketched in which phishing may grow or develop, so that future work and advanced methodologies can be drawn for the same.

Objective of the study is to find phishing vs. anti-phishing scenario in the state of the art, as well as role of available anti-phishing measures and strategic defense techniques used to combat with phishing attacks.

2 Various Stages and Information Flow in a Typical Phishing Attack

Phishing is typically carried out by email or instant messaging, and often directs users to give details at a website, although phone contact has been used as well. Phishes attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishes attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication for example eBay and PayPal are two of the most targeted companies, and online banks are also common targets [11].

Phishing attacks involve following stages [8]:

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages 17 March 2018
Peer Reviewed Refereed Research Journal

A The attacker obtains E-mail addresses for the intended victims from a variety of sources and generates an genuine looking E-mail to the intended victims in a way that appears legitimate and obscures the true source.
B Depending on the content of the E-mail, the recipient performs some action and by the time attacker harvests the victim's sensitive information and may exploit it in the future.

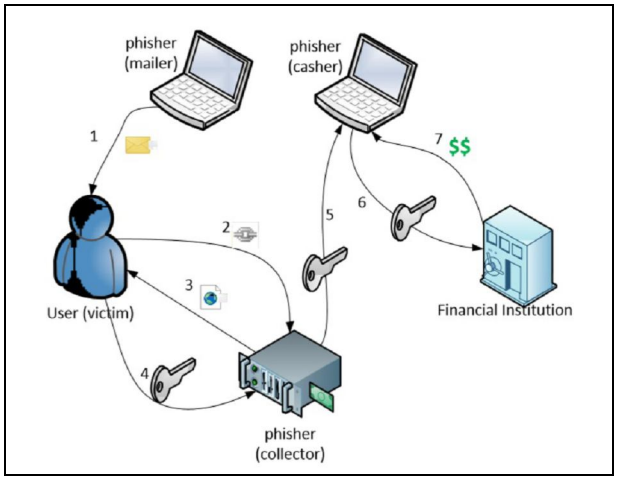


Fig 3: Phishing Information Flow

3 Types of Phishing Attacks and Current Phishing Techniques
Common phishing attacks can be categorized as by Spoofing Emails, By Websites, By Instant Messaging Systems, Exploit-Based Phishing Attacks, Spear Phishing, Wishing, Whaling, Malicious Code / Malware etc [4]. Some examples of top targets of phishing includes: PayPal, eBay, Bank of America, HSBC Group, Google, Alliance Bank, Face book, the Internal Revenue Service, JPMorgan Chase, Wells Fargo and Barclays - http://www.phishtank.com etc [6]. According to phishing e-mail reports and phishing site trends 3rd Quarter 2012, the second and third quarters of 2012 saw a constant decline in the number of unique phishing sites detected by the APWG. This is a return to historical levels after a period of high activity. The decline in traditional phishing is probably due to an increase in malware based attacks. Phishing attacks targeting consumers remained at high levels during the quarter. According to APWG report during the third quarter, there is a constant decline of unique phishing sites detected by the APWG. The drop from April to September was 26 percent [18]. Various types of phishing attacks are shown below [9]-

S. No.	Name of the phishing attack	Examples
1	Impersonate (simple attack)	a. Fake site looks like target b. Mirror or link to images for credibility c. Man in the middle POST login Prevents victim detection.
2	Forward (sophisticated attack)	a. Typically collected via phishing email (not as effective) b. Site collects data; performs meta-refresh to target (HTTP redirect) c. Man-in-the-middle POST login prevents victim detection
3	Popup (creative attack)	a. Real site in back, hostile popup in front b. Real site gives credibility, prevents victim detection c. Not man-in-the-middle d. Mirror or link to images for credibility

Table 2: Types of Phishing Attacks

Few more current phishing techniques have been shown in the following table [10]-

S. No.	Phishing Techniques	Examples
1	JavaScript Attacks	Spoofed Secure Socket Layer lock
2	Certificates	a. Phishes can acquire certificates for domains they own b. Certificate authorities make mistakes
3	Use of visual elements from target site	DNS Tricks like: www.ebay.com.kr, www.ebay.com@192.168.0.5, www.gooogle.com, Unicode attacks

Table 3: Current Phishing Techniques

A common phishing attack tree method has been shown below by including three different concepts/methods of phishing that is worm, Trojan, deceit and spyware [8]:

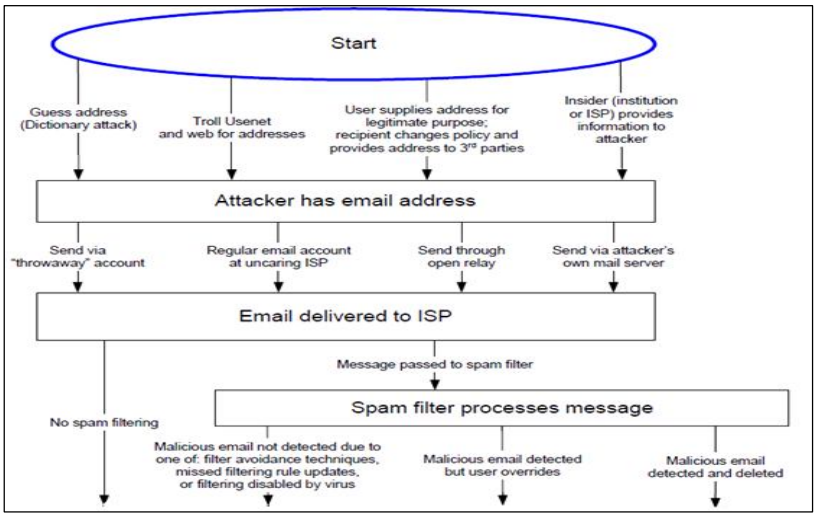
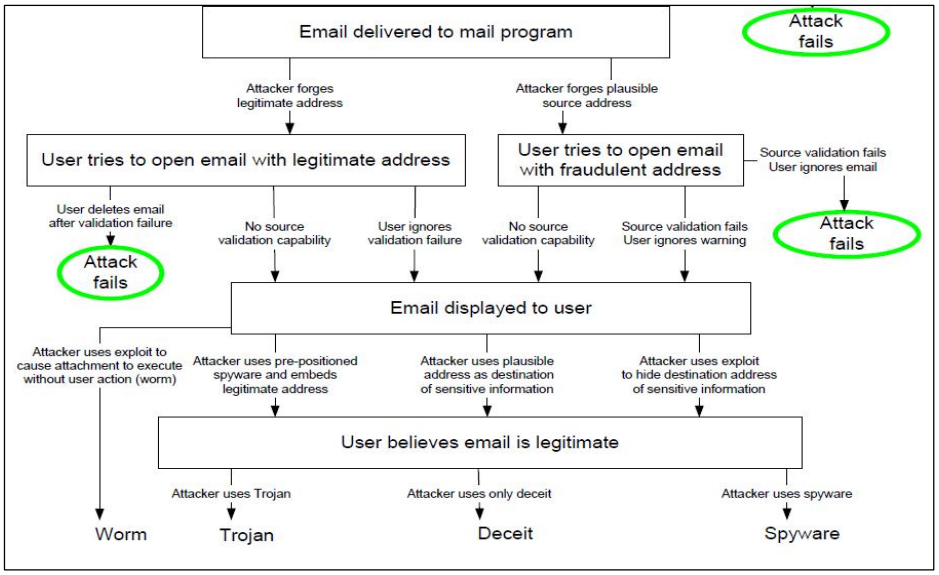


Fig 4- Common phishing attack tree method
(source- McAfee Research Technical Report #04-004)



	Phishing Emails	Phishing Malware / Key loggers
Average number of accounts compromised In a week	100	500,000
Type of information Compromised	Name, address, phone, SSN, credit card, VCC2, bank account numbers, logins and passwords, and even items such as mother's maiden name or the answer to the "forgot your password" prompt. Generally, victims provide All of the information asked.	Account login, or credit card Number with expiration and address. Generally, a single victim only loses A single amount of information. Few victims lose more than one type of information. And the information compromised may not match the information desired by the phishes.
Volume of data Generated	Each victim = < 500 bytes of data. 1 week = < 50 Kbytes. A single person can process the data in minutes.	A single key logging Trojan can generate hundreds of megabytes of data in a week. The data is not processed by hand. Instead, scripts are used to filter the information. Potentially valuable information is frequently ignored due to the filtering process.
How often is the method viable?	Reused regularly for weeks or months before requiring a change. Due to simple changes in the mailing list, a variety of people can be solicited – information is almost never collected from the same person twice.	Most malware is effective for a week before anti-virus vendors develop signatures. Some phishing groups use malware in limited distributions. While these programs may exist for much longer durations, they generally collect less information. A single person that is infected may compromise the same information multiple times.
Total development cost to the phishers?	A single phishing server may take one week to develop. The server may then be applied to hundreds of blind drop servers and reused for weeks or longer. Changes to the phishing email content (bait) can be measured in hours and may not need a change to the phishing server.	A single malware system, including Trojan and receiving server, may take months to develop. Each variant may take a week or longer to develop. When generic anti-virus signatures appear, redevelopment may take weeks or months.

Table 4: Comparisons between Phishing Email and Malware (source-[9])

4 Anti-Phishing: Approach, Strategic Defense Techniques and Working Process

Approach-Anti-phishing is a method or an application which helps to prevent user's personal information from unauthorized access. Anti-phishing services are used to secure variety of information in miscellaneous ways across a variety of platforms. An anti-phishing service deals with a specific type of attempt to obtain personal or other sensitive information and provides tools to help users to recognize phishing attempts. Some anti-phishing tools are available via browsers, through which many phishing attempts occur and some anti-phishing services include sophisticated planning designed to help clients to avoid data theft. Thus an anti-phishing services or tools frequently provides detailed components to analyze how data is stolen, how

data may be recovered or how to close ranks and protect a system from additional hacking [12]. Now a day's emerging latest anti-phishing software's also plays vital roles to identify phishing content contained in websites and emails. 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 software may also be included as a built-in capability of some web browsers [13].

Strategic Defense Techniques- Anti phishing solutions can be divided into server based anti-phishing solutions and client based / browser based (plug-in) anti-phishing solution. The server based anti-phishing solutions try to collect users' credentials to built a black list whereas browser based solution tries to protect users credentials from the client approach. Anti-phishing is an application that is integrated with the web browsers and it is considered as a browser based solution. It is a novel browser extension and it is free for public use with the intension to protect inexperienced users against spoofed web site-based phishing attacks. Examples of both the types have been shown in the following table:

Server Based Technique	Client/Browser Based Technique
Brand monitoring	E-mail Analysis
Behavior Detection	Black Lists
Security Event Monitoring	Information Flow
Strong authentication	Similarity of Layouts
New authentication techniques	

Table 5- Server Based and Client based Anti Phishing Techniques

Anti-Phish is a free, easy and clear reference model for browser based solutions. AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to transmit this information to a web site that is considered un-trusted. The problem with server based solution is that crawling and black listing will find organizations in a race against the attackers. Detecting anomalous behaviors (mainly for banks) means *a-posteriori* solution [14]. The most effective solution to phishing is training users not to follow links to web sites where they have to enter sensitive information such as passwords (unrealistic!). The main challenging factor is to reduce the false-positive warnings when customers use the same password in different websites.

Working process of anti-phishing

After the installation of anti-phish application, when user starts entering input first time into the form, then browser will request to enter new master password to encrypt the sensitive information using DES. The anti-phish menu is used to scan the page (sensitive information entered by user) and to capture and store this information with the domain of the web site. So if the viewing webpage of user is pure HTML, then anti-phish can easily mitigate phishing attacks because attacker will only be able to steal users credential when user submits his form. As soon as anti-phish detects that sensitive information has been entered into a form of an unreliable domain then immediately users operation will be cancelled. Thus for the time being anti-phish temporarily deactivates java scripts in web page with a form [14]. In the following figure execution flowchart of Anti-Phish has been shown to indicate the method of protecting potential victims.[16]

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages 17 March 2018
Peer Reviewed Refereed Research Journal

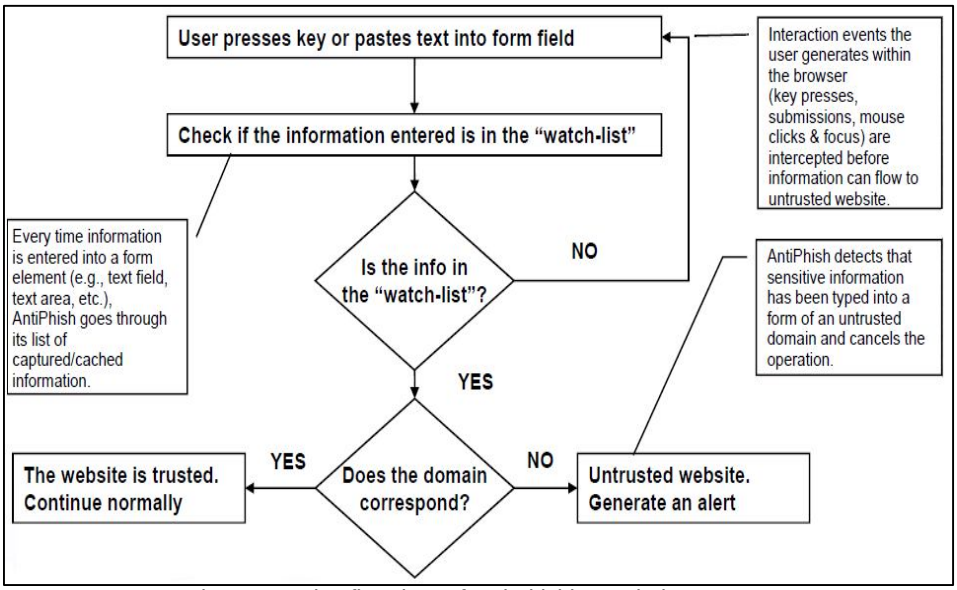


Fig 5-Execution flowchart of anti-phishing techniques

Another popular approach to fighting phishing is to maintain a list of known phishing sites and to check websites against the list. Microsoft's IE7 browser, Mozilla Fire fox 2.0, Safari 3.2, and Opera all contain this type of anti-phishing measure. Fire fox 2 used Google anti-phishing software. Opera 9.1 uses live blacklists from Phish Tank and Geo Trust, as well as live white lists from Geo Trust. Some implementations of this approach send the visited URLs to a central service to be checked, which has raised concerns about privacy [1]. Similarly some browser-based plug-in solutions were provided by Stanford University to mitigate phishing attacks like PwdHash, Spoof Guard, Veri Sign etc [4]. For the purpose of providing complete, worldwide exposure to customers, RSA fraud action committee employs a number of measures to ensure end-to-end protection against phishing like threat detection and alert, forensics and credential recovery, mitigation and site shut-down, countermeasures, intelligence and education etc. An RSA service also offers some key features like accountability, connectivity, expertise and technology to help customers solve their most difficult security and compliance challenges [17]. Phish Tank is a collaborative clearing house for data and information about phishing on the Internet and provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge [15].

6. Conclusion

Phishing is one of the most prevalent threat vectors for cyber attacks. Cybercriminals are using new tools frequently and are becoming more adaptive than ever. In the present scenario the online channels are facing tricky and globally-integrated technological crimes. Some high profile institutions such as Citibank and PayPal are targeted almost continually. In this paper phishing phenomenon strategies have been explored in an elaborated way and current defensive strategy against phishing techniques have been evaluated. This study will increase the understanding and awareness of the internet user about phishing strategy as well as efficacy of available anti-phishing measures and will work as stepping stone for future research in the direction of anti-phishing strategies.

References

1. M. Jakobsson (2007) "Phishing and Countermeasures: Understanding the In-creasing Problem of Electronic Identity Theft", Wiley, ISBN: 978-0-471-78245-2.

2. R. Dhamija, J. D. Tygar, M. Hearst (2006) "Why Phishing Works, in the Proceedings of the conference on Human Factors in Computing Systems" (CHI2006).

3. Tzer-Shyong Chen; Fuh-Gwo Jeng; Yu-Chia Liu (2006);" Hacking tricks toward security on network environments", Seventh International Conference on Parallel and Distributed Computing , Applications and Technologies.
4. Kirda, E.; Kruegel, C.(2005);" Protecting Users Against Phishing Attacks with Anti-Phish", 29th Annual International Computer Software and Applications Conference, COMPSAC, Page(s): 517 524 Vol. 2, Volume 1.
5 Hanaek, P.; Malinka, K.; Schafer, J. (2008); "E-banking security - comparative Study", ICCST 42nd Annual IEEE International Carnahan Conference on Security Technology, PP: 326 – 330.
6. DigiCert Inc. your success is built on trust Phishing (2009), "Phishing A primer on what phishing is and how it works", 355 south 520 west canopy building II Lindon, UT 84042, www.digicert.com
7. Melinda Geist (2008), "Designing Successful Anti-Phishing Applications to Protect Home Computer Users", Intel Corporation applied information management.
8. Gregg Tally, Roshan Thomas, Tom Van Vleck, September 2004, McAfee Research Technical Report #04-004, "Anti-phishing: best practices for institutions and consumers", www.mcafee.com.
9. Lance James ~ CTO, July 2005, "Phishing an evolution", company confidential, copyright 2005 secure science corporation Secure Science Corporation 7770 Regents Rd., Suite 113-535, San Diego, CA. 92122-1967, (877)570-0455, http://www.securescience.net.
10. Dr. Harold L. "Bud" Cothern, "Phishing, Spoofing, Spamming and Security", How To Protect Yourself, downloaded on 10 may 2012 at 1.21 pm
11. "Internet Phishing" downloaded on 10 may 2012 at 2.14 pm from http://en.wikipedia.org/wiki/Phishing
12. Cory Janssen (loaded on 4th march 2013) "what is Anti-Phishing Services? Techopedia", www.techopedia.com/definition/23907/anti-phishing-service.
13. Definition of anti-phishing loaded on 4th march 2013 from (www.websters-online dictionary.org/definitions/Anti-Phishing)
14. Engin Kirda, Christopher Kruegel, Angelo P.E. Rosiello (2007) "AntiPhish: An Anti-Phishing Browser Plug-in based Solution", Technical University of Vienna Politecnico di Milano
15. www.phishtank.com loaded on 5th march 2013 at 12.11 am
16. Angelo P. E. Rosiello "Anti-phishing security strategy" loaded on 5th December 2012 by google through link www.blackhat.com/presentations/bh-europe.../bh-eu-08-rosiello.pdf.
17. RSA Fraud action anti-phishing service (2012 EMC Corporation) "End-to-end protection against phishing threats", published in the USA, FRA DS 0212, www.rsa.com
18. Phishing Activity Trends Report (published on 1, February 2013)3rd Quarter 2012, July- September 2012, www.apwg.org, info@apwg.org.
19. Phishing Activity Trends Report (1H2017) APWG duration January-June 2017, Published October 17,2017, www.apwg.org.