ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

# A Comparative Analysis of Anti-Phishing Mechanisms: Email Phishing

ShwetaSankhwar and Dhirendra Pandey
BabasahebBhimraoAmbedkar University
Lucknow, U. P., India

***Abstract***: Phishing has created a serious threat towards internet security. Phish e-mails are used chiefly to deceive confidential information of individual and organizations. Phishing e-mails entice naïve users and organizations to reveal confidential information such as, personal details, passwords, account numbers, credit card pins, etc. Phisher spread spoofed e-mails as coming from legitimate sources, phishers gain access to such sensitive information that eventually results in identity and financial losses.In this research paper,aexhaustive study is done on anti-phishing mechanism from year 2002 to 2014. A comparative analysis report of anti-phishing detection, prevention and protection mechanisms from last decade is listed. This comparativeanalysis reports the anti-phishing mechanism run on server side or client side and which vulnerable area is coverd by it. The vulnerable area is divided into three categories on the basis of email structure. The number of vulnerabilties covered by existing anti-phishing mechanisms are listed to identify the focus or unfocused vulnerability. This research paper could be said as tutorial of a existing anti-phishing research work from decade. The current work examines the effectiveness of the tools and techniques against email phishing. It aims to determine pitfalls and vulnerability of anti-phishing tools and techniques against email phishing. This work could improve the understanding of the security loopholes, the current solution space, and increase the accuracy or performance to counterfeit the phishing attack.

***Keywords***: Phishing, E-mail phishing, Information security, web vulnerabilities, cyber-security.

## I. INTRODUCTION

The present day primary hazardisdirected towards online identity&confidentialinformation, primarily because of the boom of internet users. E-mails are economical and are used in increasing number of times by companies and individuals for various means (like e-commerce services, et al). Con artists, throughmasqueradinglegitimate-mails sent from reputable organization(s),phish e-mails,acquiredinformation such as banking accounts, credit card details, etc. to gain access to sensitive personal information and thereby posing a serious threat to internet users. They allure the users to visit their spoofed website and download malicious content, thereby providing access to delicate data. This paper highlights detection and prevention mechanisms (with summarized descriptions) against phishing e-mails from the last ten years (2002-2014).

The mechanisms have been studied,analyzed and theirdescription, along with their year,tool/algorithm used and thrown light on the variousscopes of phish e-mail detection mechanisms. A comparative analysis report of anti-phishing detection, prevention and protection mechanisms from last decade is listed. This comparative analysis reports the anti-phishing mechanism run on server side or client side and which vulnerable area iscoverd by it. The vulnerable area is divided into three categories on the basis of email structure. The number of vulnerabilities covered by existing anti-phishing mechanisms are listed to identify the focus or unfocused vulnerability by researcher. This paper could be said as tutorial of an existing anti-phishing research work from decade. It gives a background and a deep literature on anti-phishing which could lead recent researcher to fill gaps of security breach causing phishing attack and innovate or develop secure anti-phish mechanism. This paper is organized as: Section-IItakes a look at previously developed anti-phishingdetection, prevention and protectionmechanisms; Section III explains almost all thevulnebilities causing email phishng; Section IV. shows thefindings of the paper;and at last VI concludes the paper.

## II. PHISHING

Recent years have witnessed,phished e-mails asafirst-rate tool for deceptionof online users into revealing sensitive information. Firstly phishersgather information by ‘social engineering’ (making laws or using other methods to influence public opinionand solve social problems or improve social conditions). They then createphished e-mails and feastonthem through different service providers like Gmail, Yahoo, Rediffmail, hotmail, etc.Fundamentally, a phished e-mail is a replica of a general, legitimate e-mail from a trusted source (individual or organization).

A phished e-mail can be,

**(a)**Textual, offering special schemes at lucrative rates, lucky winner rewards, etc. to drawpersonalinfo;

**(b)** Embedded with a urlredirectingtheonline user to fake webpages, askingthe recipients to do the same as in point (a);

**(c)**Rooted with a malicious attachments, i.e., infected PDFs or MS Office documents, et al that, upon being downloaded, gain indignifiedaccess to private information .

The subsequent list is drawn on the evolution of e-mail phishingmechanisms through the last decade. This exhaustive study is based one-mails phishing tools or mechanism,primarilyis based on where the anti-phishing mechanism run on server side or client side and also which vulnerable area is coverd by it. The phish e-mails divided in three categories i.e. Page content, Link/domain based, Header based.Vulnerabilities are loopholes, pitfalls, weaknesses which we can experience when the threat occurs more than once in a system or facility holding information, which can be exploited to gain access or violate system integrity. Vulnerabilities can be assessed in terms of the means, by which the attack would be successful. The number of vulnerbilties covered by existing anti-phishing mechanisms are listed in Table.2 to identify the focus or unfocused vulnerability. The naive user is fooled by an imitation of a trusted site but it is directed to some other web site which is perhaps a phishing site. A secure and trusted link is used within the anchor element and the href i.e. the hyperlink reference directs the website to a malicious website which is used by the phishers for performing their activity. This is a deception technique which can be used by the user to understand that the website is not a trusted one because when the mouse pointer is moved it redirects you to an unwanted malicious website. The phishers always send such emails in which the user needs to fill up some details and also provide a well-known legitimate site which is actually malicious and redirects towards a phishing site.There are several contaminated pages and dialog boxes which are used by the phishers. There are some special malware programs that are either connected to the website as a URL or Pop up or as a dialog box and perhaps attempt an imitation of a website which is actually a fake one. This technology is used on websites where sensitive details are shared by the user. The phishers try to collect and use them for further activities.

Table.1 Anti-Phishing E-Mail Mechanisms

| SR.NO. | YEAR | TOOL/APPROACH/ ALGORITHIM | SERVER SIDE / CLIENT SIDE | PAGE CONTENT BASED | LINK OR DOMAIN BASED | HEADER BASED |
|---|---|---|---|---|---|---|
| 1 | 2002 | DOMAIN NAME SYSTEM BLACKLISTS[1] | NETWORK LEVEL | | ✓ | |
| 2 | 2004 | SPOOFGUARD [2] | CLIENT SIDE | | ✓ | |
| 4 | 2006 | PILFER [3] | CLIENT SIDE | ✓ | ✓ | ✓ |
| 5 | 2006 | LINKGUARD [4] | CLINT SIDE | ✓ | ✓ | ✓ |
| 6 | 2006 | STRUCTURAL PROPERTIES[6] | SERVER SIDE | ✓ | ✓ | ✓ |
| 7 | 2006 | NETCRAFT[7] | CLINT SIDE | ✓ | ✓ | ✓ |
| 8 | 2008 | MODEL BASED [8] | SERVER SIDE | ✓ | ✓ | |
| 9 | 2009 | INTEGRATED APPROACH TO DETECT PHISHING E-MAIL ATTACK [9] | SERVER SIDE | ✓ | ✓ | ✓ |
| 10 | 2010 | HYPERLINK INFORMATION[10] | | | ✓ | |
| 11 | 2011 | MACHINE-LEARNING TECHNIQUES;<br>MODULE BASED [11] | CLIENT SIDE | | ✓ | |
| 12 | 2011 | PECM ,-WITH FOOT PRINT CONSUME MEMORY HIGH SPEED[12] | SERVER SIDE | ✓ | ✓ | ✓ |
| 13 | 2012 | PENFF TO PREDICT DYNAMICALLY THE ZERO DAY PHISHING E-MAILS[13] | SERVER SIDE | ✓ | ✓ | ✓ |
| 14 | 2012 | LATENT SEMANTIC ANALYSIS [14] | SERVER SIDE | ✓ | ✓ | ✓ |
| 15 | 2013 | PDENFF TO DETECT AND PREDICT DYNAMICALLY THE ZERO DAY PHISHING E-MAILS [15] | SERVER SIDE | ✓ | ✓ | ✓ |
| 16 | 2014 | NATURAL LANGUAGE PROCESSING TECHNIQUES [16] | CLIENT SIDE | ✓ | | |

## III. VULNERBILITIES CAUSING EMAIL PHISHING

The most common ways to become susceptible to phishing attacks are: online shopping, through email and out breaking social media networks. With the advancement in technology and web security, new ways of phishing are emerging to break the web security and get access to services and personal information of users. The number of ways adopted and innovated by phishers to trick the users. An exhaustive literature review is done here and through this a report on a slew of email phishing vulnerability created.This report list is categorized into three partsvulnerabilitieson the basis email structure i.e. Page Content vulnerability (PV), Domain vulnerability (DV) and Code-Scripting vulnerability (CV). All Vulnerability are explained in detail to understand how malicious users exploit these vulnerabilities and trick email or online users.

A. ALL PAGE CONTENT VULNERABILITY (PV)

1. Page Content Vulnerability (PV1) : The DNS domain name provided by the hyperlink in the anchor text seems to be legitimate. The hyperlink directs the reader to a specific documentand the reader, considering the link to be real, follows the link. However, the hyperlink would actually point at the phisher's webpage. The destination DNS name in the link visible to reader is slightly different than the actual link but the link looks authentic and lures the unsuspecting internet users.
   Illustration:
   <ahref="http://www.profundnet.org/checksessioninfo.php">
   https://Genuine.secureregion.com/EBanking/logon/</a>
   The above link appears to belinked to Genuine.secureregion.com, which directs the user to a bank's website. However, it is actually linked to www.profundnet.org , which is a phishing website. [9]

2. Page Content Vulnerability(PV2) : ASCII have several characters or pair of characters that looks alike but actually are different in origin (also known as Homographs). Phishers could form a hyperlink by encoding alphabets into their corresponding ASCII codes to make it loookauthentic website that is being spoofed. The link seems authentic to online user and he/she follows the link regardless of any suspection.[9]
   Illustration:
   href="http://%69%2E%34%33%2E%35%32%37%2E%65%35:%34%55%34%87/%6C/%39%6E%34%65%68%2E%48%54%6D">www.citibank.com</a>
   The above link seems to be linked to www.citibank.com. however, it actually points to a phishing website http://9.34.195.41:54/l/index.htm. [9]
3. Page Content Vulnerability(PV3) : A malicious party could deceive online users by forminga hyperlink using special characters. Phishers can register a domain name that seems almost identical to an existing domain just by altering little details and adding special characters in it. It appears legitimate to the user and lures him/her but directs them to a bogus site.
   Illustration:
   http://www.paypal.com:fvthsgbljhfcs83infoupdate@193.201.52.175
   The above link appears to be linked to paypal, but actually is linked to a IP address 193.201.52.175. [9]

4. Page Content Vulnerability(PV4) : One of the most desired tactics used by phishers is to use pop-up to open fraudulent pages. When the user clicks the received link in their e-mail, it goes to a fraudulent website and generates a deceitful pop-up and then redirects the user to the original website. This technique is used by the fraudsters to gather information without undermining the credibility of the site and makes the user believe that pop-up is of an authentic website. The pop-up disables the user from saving the page [9].

5. Page Content Vulnerability(PV5) : Fraudsters often disable the right click function on fraudulent web pages in order to deprive the user from getting the context menus that come up after right-click. It prevents the user from saving and viewing the source code. Despite of this suspicious function, user continues to access the website indubitably and becomes the victim of yet another trick used by attacker [9].

6. Page Content Vulnerability(PV6) : Scammers use @ symbol in the URL to baffle the user. This symbol is used in an URL and the browser refers to the text following @ symbol and ignores the text before @ symbol. This trick is used to fool the email receiver using email address and make him think that the link directs to the site viewed before @ symbol. However, it goes to the phishing site after @ symbol [9].
   Illustration:
   In the following format <userinfo>@<host>, the browser will link to the <host> site and ignore the <userinfo>. [9]

7. Page Content Vulnerability(PV7) : Phisher use spelling error as a tool to fool victims and achieve the desired end. They carefully choose the words and make spelling errors on purpose. Such errors could be easily noticed by a smart user who could recognize the scam; however a gullible user could not notice such error and respond [9].
   Illustration:
   Phisher might show google.com as goggle.com to a victim.

8. Page Contentent Vulnerability(PV8): One of the tactics used by phishers is displaying a link that looks genuine but actually links to a phishing site. They exploit HTML emails and create a link in such a way that text of the URL looks authentic however, the HREF of the link belongs to different host. Users fail to notice that and fall for such tricks.
   Illustration: Phisher could display a link as paypal.com that looks genuine but actually links to a spoofing site. [9]

9. Page Content Vulnerability(PV9): Often e-mails contain link with the text "link", "click" or "here" that link to a user agreement, privacy policy and others. These "modal domain" of the e-mail maintains the authentic feel in the e-mail. However, phishing e-mails could also have such links with text "click here". It becomes difficult for a user to understand whether link with the text "click" is linked to a modal domain or a non-modal domain. A non-modal domain links to a phishing site and user being unable to differentiate between the two

(modal domain and non-modal domain) & becomes the victim [9].

10. Page Content Vulnerability(PV10) : Phisher can easily make a number of links in an email using some kind of technical deception that leads to a spoofing website. It is one of the most common tricks used by attackers to collect private information about their target. Users consider such link as a trustworthy entity and the probability of a spoofing trick getting success increases. [17]

11. Page Content Vulnerability(PV11): Phisher use HTML formats to send an email and steal users' credentials. Such kind of phishing attack works in convenient ways to gain trust of users & craft email using HTML format which has an embedded link in it and then online user may asked to fill in their credential details for verification or by urging statement to input the credential by following the embedded link. The link visible to the user in such emails seems legitimate; however it belongs to a spoofing website which is masked such that user is unable to see it.
    Illustration:
    If a spoofed email is sent to a user using HTML format then the link visible in the email will be https://secure.regionsnet.com/ E-Banking/logon/user?a=defaultAffiliate that masks the reference to the phisher's website:
    http://www.club-daich.com/.checking/regions/. [18]

12. Page Content Vulnerability(PV12): Often attackers send emails to the users which do not contain any link and carry out the attack, depending on the victim's response. Such type of emails do not contain name of the recipient in the email and refers to the user as "Dear Friend", "Hi Dear", "Dear Beneficiary" and other such phrases. A legitimate email always has the name of recipients and a smart user instantly recognizes emails without recipient's name as suspicious. However, a gullible or naive user fails to notice that and responds to these emails. As soon as they respond to a spoofed email, phisher gets aware of the fact that the user is enticed and attacks the victim [16].

13. Page Content Vulnerability(PV13) : Phisher lure the users into replying to their email by promising a sum of money. They offer greedy or lucrative schemes like to make them luck winner & renewed handsome reward of money or schemes to double the money in less time etc. This lust for money attracts users; specifically exploit "free money" with no strings attached. They make the victim believe that he/she will get the amount of money as promised and the person making such promise and sending email is authentic. As soon as the victim starts believing that the email is legitimate, the phishers then ask the user to provide their sensitive information or ask them to transfer a certain amount of money to an account before preceding the transaction and giving away the "free money" to user. The user falls for this well-crafted phishing attack and becomes a victim [16].

14. Page Content Vulnerability(PV14): The attackers frame the spoofed emails in every possible way to induce the victim into replying to their email. They portray the email to the user using such sentences that ask the user to respond to a specific email address and induce the recipient to reply. If the user gets influenced by the email and replies then the attackers start mind games. They influence the user by posing the entity they described in the email and gains user's confidence and induce them into replying and providing sensitive information [16].

15. Page Content Vulnerability(PV15): Attackers often use a reply luring sentence in their emails that has a sense of urgency so as to make the victim reply as soon as possible. They do so, so that the user gets less time to think logically and makes the user think that he/she has to reply soon in order to get the information which will not be available otherwise. Such emails have certain pattern in which attackers may offer a large amount of money or tell that the money is trapped in banks due to civil war (often using the name of countries that are currently in the news) or ask the victim to give their account details to transfer the money. They frame a sympathetic email such as; he is in critical condition (severe disease) or struck at foreign and need financial or banking help to place the urgency. Once the victim is lured into confidence, attackers then ask victims to pay fees or charges that start out as a small amount. However, if user pays such amount, the scammers continue asking them to pay for new "fees" and keep making such fake requirements until they achieve their desired amount of money from the user and of course, the victim is never sent the money that was promised [16].

16. Page Content Vulnerability(PV16) : Phisher often use redirection service to hide URL of a phishing site in the e-mail. As a webpage is visited by a user (by typing in a URL or clicking a link) the webpage could redirect to a different page. Attackers confuse the user regarding what website they drop in and send the user to a fraudulent website by using redirection trick. This URL redirection seems legitimate to the user and he continues to visit the website and provide his information without any suspicion.[6]

17. Page Content Vulnerability(PV17): Phisher use embedded HTML formats in emails that appears to be legitimate and steal users' credentials. Phisher send an email to the user in HTML format which has an embedded link in it and then ask the user to fill in their credential details for verification by following the embedded link or ask for their credit card numbers or other sensitive information. The link visible to the user in such emails seems legitimate; however it belongs to a spoofing website which is masked such that user is unable to see it.
    Illustration:
    If a spoofed email is sent to a user using HTML format then the link visible in the email will be https://secure.regionsnet.com/ E-Banking/logon/user?a=defaultAffiliate that masks the

reference to the phisher's website: http://www.club-daich.com/.checking/regions/. [8]

B. ALL DOMAIN VULNERABILITY(DV)

1. Domain Vulnerability ( DV18): Phisher innovated trick to attack the victim issuing IP address in the URL or the anchor text which appears to contain a link to a legitimate site, however, leads to a misleading domain name. The link appears authentic to the user, leverages their confidence and hooks the unwary victim.
Illustration:
http://212.33.67.194/.citibank/accountexpirycheck.net
The above link appears to be linked to a legitimate site of Citibank but is actually linked to phishing website.[9]

2. Domain Vulnerability (DV19): Instead of hyperlinks, DNS names are used in its URL to provide destination information in its anchor text. These DNS names in the URL usually correspond with a famous company or organization. Users often look for legitimate, familiar, reputed websites and are most likely to fall for such tricks. All it takes is just one naive or careless person to fall for a well-crafted phishing campaign.
Illustration:
<a href= "http://www.ebaysecurecgi.us/webscr.php?cmd=LogIn" > Click here to confirm your account</a>
Such a link could be formed which have the text displayed that might not have to be a real destination.[9]

3. Domain Vulnerability (DV20): In the context of phishing, a list of domain names and untrusted URLs or lists of banned websites that are suspicious and known to have intentions of malicious attacks are blacklisted. While using a browser if an IP address or URL of a site matches the blacklist then the user is warned. However, attackers keep changing IP locations and ISPs to avoid detection and prosecution. If the blacklist is not maintained up to date then the chances of attacking user's system increases. On the other hand, there are various white listed DNS names which are simply a list of trusted websites. This list has just the URLs and domains of the sites that can be trusted. User can get access to these sites without being afraid of getting trapped into any phishing attack. [18]

4. Domain Vulnerability (DV21): Hackers use long URL address to attack the victims. A long URL address becomes difficult for the user to read and hard to recall. The attacker lures the victim by showing him the initial text in the URL which shows the original website but hides the real web address which is at the end of the long URL.[9]
Illustration:
http://www.company.com:crafty.....long......string@www.scammer.com
In the above URL, the user assumes that the link directs to www.company.com, however, the URL actually redirects to www.scammer.com which is not seen by the user as it is hidden at the end of the long URL address. [9]

5. Domain Vulnerability (DV22): Phisher replace characters of a genuine URL with the characters which look similar to it. Many characters, symbols or alphabet of English words replaced by other language which seems same but are actually different, phisher exploits this fact and can register a domain name which seems legitimate or identical to an existing domain but actually goes to a phishing website. It confuses the user and makes him unable to understand the difference.
Illustration:
http://www.rnicrosoft.com
The above URL seems to be linked to microsoft.com but is actually a fake website that contains letters "r" and "n" instead of "m". [9]

6. Domain Vulnerability (DV23): Phisher use prefix or suffix to craft domains same like original or legitimate. There are many valid suffix and prefix that are used by legit websites of various organizations but still there are many possible suffixes and prefixes which aren't reserved and are used by scammers to create a phishing website. Users fail to notice the invalid suffix/prefix and become the victim of phishing.[9]
Illustration:
"thehindu.in" is a legit domain whereas the domain thehindu.info and thehindu.org with suffix "info" and ""org" are invalid.

7. Domain Vulnerability (DV24): Hexadecimal character codes are used by various phishing websites to disguise the actual numbers and letters in a URL. Phisher use these hexadecimal character codes in URL by preceding it with a '%' symbol.
Illustration:
http://www.fastvisa.com%00@:%32%34%2e%37%36%2e%38%39%2e%36%34:38/%63%69%74/%69%6E%33
In the above URL format "@:%32%34%2e%37%..." is a fraudulent website's IP address hidden in hexadecimal character code. [9]

8. Domain Vulnerability (DV25): Another tactic used by attackers is creating a website that looks genuine but is actually a fake website. Phishers use a domain name and make a website that looks real and makes the user believe that the website is authentic. [9]

Illustration:
www.indiatour.com is a genuine website that provides information regarding transportation in India. However, website tourtoindia.com appears to be a real site but it is a fake website. [9]

9. Domain Vulnerability (DV26): Phisher often try to attempt name based attacks in which they register a domain name that looks similar to an existing domain name. Such domains have limited life. Attackers register such domains with credit cards obtained fraudulently and often use trademarks of authentic organizations to make it look genuine. Phisher have an urge to use these domain names as quickly after registration because they scare to get trapped or arrested as many organizations watch registrations of domain name that involves their trademarks. Gullible users easily fall for such similar looking domains and fall for a well-crafted phishing attack.
Illustration;
playpal.com or paypal-update.com sounds legitimate but they are spoofing websites. [17]

10. Domain Vulnerability (DV27): Another trick used by phishers to attack the victim is by adding IP address in the URL or the anchor text which appears to contain a link to a legitimate site, however, leads to a misleading domain name. The link appears authentic to the user, leverages their confidence and hooks the unwary victim.
Illustration:
http://212.33.67.194/.citibank/accountexpirycheck.net
The above link appears to be linked to a legitimate site of Citibank but is actually linked to phishing website. [17]

11. Domain Vulnerability(DV27): There could be a number of domains linked to in an email. For instance, the main domain of www.cs.university.edu is ‘university.edu’. However, main domain of www.company.co.jp is ‘company.co.jp’ which has two domains, that is, .jp and .co. Phisher attempt to create a link with number of domains that may appear legitimate but conceals the address of actual website and misleads the user.[17]

12. Domain Vulnerability (DV28): Attackers can construct legitimate looking URLs by using sub-domains that contain a number of dots. It may appear legitimate to a naïve user and would click on the link considering that the link will redirect to a genuine site however the browser is redirected to a bogus site.
Illustration:
http://www.google.com/url?q=http://www.badsite.com
The above link appears to be linked to www.google.com but actually linked to www.badsite.com. [17]

13. Domain Vulnerability (DV29): Spam filters scan the email messages and provide a great solution to prevent malicious attacks. It scans the message content and if found suspicious, it is recognized as a spam. However, spam filters vary in effectiveness and could not be totally relied upon. Phisher modify the message content in such a way that often the spam filters fails to recognize them and lets the malicious emails slip through. In such cases, user fails to notice the spoofed email and becomes the victim of yet another phishing attack. [17]

## C. ALL CROSS-SITE SCRIPTING VULNERABILITY (CV)

1. Cross-site Scripting Vulnerability (CV30): Phisher often use redirection service to hide URL of a phishing site in the e-mail. As a webpage is visited by a user (by typing in a URL or clicking a link) the webpage could redirect to a Phishers page. Phisher confuse the user regarding what website they drop in and send the user to a fraudulent website by using redirection trick. This URL redirection seems legitimate to the user and he continues to visit the website and provide his information without any suspicion. [9]

2. Cross-site Scripting Vulnerability (CV31): Some fraudsters take phishing to the next level and put efforts to redirect the URL twice. This type of service hides the URL completely. Some services like tinyurl.com and cjb.net permits anyone to enter a URL and thus create a shortcut of the URL. It fulfills the malicious purpose of an attacker and hides the actual URL. [9]

3. Cross-site Scripting Vulnerability (CV32): Phishers are using Java script event handler “onMouseOver” to overwrite the address bar with a different URL. When the user reads the status bar, it seems like a legitimate URL even though it is a false URL of a phishing site.[9]

4. Cross-site Scripting Vulnerability (CV33): To increase security and management, many finance and e-business portal need usernames and passwords. A Server from Handler (SFH) is used for this purpose. Phisher try to attain confidential details like username and password by making a SFH with a different domain name. It contains such spoofing pages requesting user inputs and handler. However, such kind of spoofing happens rarely.[9]

5. Cross-site Scripting Vulnerability (CV34): Phisher use JavaScript to perform various malicious activities. They create pop-up window that opens several fraudulent web pages. When the user clicks the received link in their e-mail, it goes to a fraudulent website and generates a deceitful pop-up. They change status bar of web browser. Status bar looks genuine to the user but actually links to a phishing site. Another tactic used by attackers is mailing clients of well-known organizations by using their trademarks. The email seems authentic to the client and falls for the trick.[17]

6. Cross-site Scripting Vulnerability (CV35): Phishers are well aware of using JavaScript and use it to hide information from the user and lure the user by launching a well-crafted attack. They alter the details in such a way that user doesn't get suspicious and follows the link indubitably. [17]

7. Cross-site Scripting Vulnerability (CV36): Phisher create spoofed URL by exploiting the bugs in web browser technology and making the URL look legitimate. URL spoofing vulnerability causes a significant risk to an individual who uses a web unsecure browser to navigate the web. Such URLs seem authentic to the users and they innocently visit the website considering it legitimate, however in reality, sends the information to a totally different location that is monitored by an informative thief. The user is enticed to a false website and leads the attacker in gathering their sensitive information.
Illustration:
http://www.cba.or.th/member/
A phishing email ofeBay website has above URL that redirects the user to a phishing website. [18]

8. Cross-site Scripting Vulnerability (CV37): Phisher attempt to launch denial-of-service attack where they try to hinder legitimate users of a service from reaching or using that service. Perpetrators who try to perform denial-of-service attacks often target high profile web servers like banks, credit card payment gateways. They send emails with URLs of a real domain so that it couldn't be identified and look like the email is received from a legitimate domain and fool the user. [18]

9. Cross-site Scripting Vulnerability (CV38): Phishers use various tactics to entice the user fall for their phishing attack. They create spoofed hyperlinks. The hyperlink directs the reader to a specific document and the reader, considering the link to be real, follows the link. However, the hyperlink would actually point at the phisher's webpage. Many times phishers attack the victim by adding IP address in the URL or the anchor text which appears to contain a link to a legitimate site.They often use hexadecimal code or ASCII code to confuse the user. These codes are used by various phishing websites to disguise the actual numbers, letters and other characters in a URL and make it loook identical to the website that is being spoofed. Attackers also use JavaScript to attempt malicious activities and lure the user by launching a well-crafted attack. They alter the details in such a way that user doesn't get suspicious and follows the link indubitably.[11]

10. Cross-site Scripting Vulnerability (CV39): Browsers have certain security loopholes that make them prone to malicious attacks. Phisher create spoofed URL by exploiting the bugs in web browser technology and making the URL look legitimate. URL spoofing vulnerability causes a significant risk to an individual who uses a web browser to navigate the web. Browsers are vulnerable to homographic attacks and Trojans can be installed in the user's system which can modify the system and request of a legitimate site can be redirected to a phisher's site. The user is enticed to a false website and leads the attacker in gathering their sensitive information. Such vulnerabilities are extremely difficult for a naïve user to recognize and lacks in protecting their system against these attacks.[6]

11. Cross-site Scripting Vulnerability (CV40): Session hijacking is used to achieve unauthorized access to services or information in user's system. Phisher can attack the user by exploiting loopholes in web applications and software and make the user execute malicious scripts without even letting him/her know of it. Phisher redirect the users to a malicious server by embedding malicious scripts in the URL through encoded characters. They are able to hijack user's existing session. These attacks aren't propagated via email messages but by exploiting a web services session and access victim's web services from somewhere else. Such phishing attacks are hard to recognize and traps the users in it. [6]

## V. DISCUSSION AND FUTURE SCOPE

This research paper thrown light on the various dimensions of email phishing.Through this exhaustive study and analysis it is identified that the researchers were focusedmostly onpage content vulnerabilities which was mostly used to trick naïve users. Domain vulnerabilities and code scripting vulnerabilities are prone to bigger scams and uses advanced technology to trick naïve as well as proficient users. It has been noticed that lot of work done with regard to reducing phishing, considerable work is being done to provide a safe and secure email and internet service, the same can also be said to be true for the other the fence but still is required to stop from root. This research paper gives a background and a deep literature study on anti-phishing mechanisms with their covered vulnerabilities which could lead recent researcher to fill gaps of security breach causing phishing attack and innovate or develop secure anti-phish mechanism. Researchers are here recommended to patch all the dimentions of phishing. However, with consistently improving technology and the research that goes into it, the phishing detection and removal techniques might lead to a future where phishing has ceased to exist.

## VI. CONCLUSION

The most common ways to become susceptible to phishing attacks are: online shopping, through email and out breaking social media networks. Email communication focused in this research paper which is one of the most popular means of launching phishing attacks. Existing anti-phishing research work from a decade shows that phishing is serious problem. An exhaustive study is done to make slew of almost all the vulnerabilities causing email phishing attack. Through the brainstorming study and observation all the vulnerabilities are categorized i.e. Page Content, Domain, Cross-site scripting according to email structure. The various vulnerabilities described by some of the authors' shows greater number of Page Content Vulnerabilities and are more susceptible to phishing as shown. Phishers using page content vulnerabilities are most likely to trick naïve users who remain unsuspicious and can easily be fooled. Domain vulnerabilities and code scripting vulnerabilities are prone to bigger scams and uses advanced technology to trick naïve as well as proficient users. With the advancement in technology and web security, new ways of phishing are emerging to break the web security and get access to services and personal information of users. It becomes necessary to develop a mechanism which can combat against the developing new phishing attacks. Researchers should to patch all the dimensions of phishing attack. More steps are needed to be taken to stop phishing so that the identity theft, sensitive information breach and online transactions become safe and secure. A new boom of technology needs to work to save the global platform of E-commerce and hence make it secure.

## VI. REFFRENCES

1. DNSBL. Information Spam Database Lookup. Accessed 28 may 2002,available: http://www.dnsbl.info/
2. N. Chou, et al., "Client-side defense against web-based identity theft," in In Proc. 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, CA., 2004.
3. Adida, B., Hohenberger, S., Rivest, R.L.: Fighting phishing attacks: a lightweight trust architecture for detecting spoofed e-mails, draft (February 2005)
4. Fette, I., Sadeh, N., Tomasic, A.: Learning to detect phishing e-mails. Technical Report CMUISRI- 06-112, Institute for Software Research, Carnegie Mellon University (June 2006), http://reportsarchive.admcs.cmu.edu/anon/isri2006/ abstracts/06-112.html
5. Chen, J., Guo, C.: Online Detection and Prevention of Phishing Attacks. In: IEEE Communications and Networking, ChinaCom 2006, pp. 1–7 (October 2006)
6. Chandrashekaran, M., Narayana, K., Upadhyaya, S.: Phishing E-mail Detection Based on Structural Properties. In: Symposium on Information Assurance: Intrusion Detection and Prevention, New York (2006)
7. Netcraft."Netcraft toolbar",2006,Available: http://toolbar.netcraft.com/
8. A. Bergholz, et al., "Improved phishing detection using model-based features," in Proc. Conference on E-mail and Anti-Spam (CEAS).Mountain View Conf, CA, aug 2008.
9. R. Suriya, K. Saravanan and ArunkumarThangavelu, " An Integrated approach to detect phishing mail attacks A Case Study"
10. J. Yearwood, et al., "Profiling Phishing E-mails Based on Hyperlink Information," in 2010 International Conference on Advances in Social Networks Analysis and Mining,IEEEConf, Odense, Denmark,aug 2010, pp. 120-127
11. 0.Shamal M. Firake, PravinSoni, and B.B. Meshram, Tool for Prevention and Detection of Phishing E-Mail Attacks, advances in network security application
12. A. ALmomani, et al., "An Online Model on Evolving Phishing E-mail Detection and Classification Method," journal of applied science, vol. 11,issue.18, 2011, pp. 3301-3307
13. A. Almomani, et al.,"Evolving Fuzzy Neural Network for Phishing E-mails Detection," Journal of Computer Science, vol. 8,no.7, 2012,pp. 1099-1107.
14. H. W. VenkateshRamanathan, "phishGILLNETphishing detection methodologyusing probabilistic latent semantic analysis,AdaBoost, and co-training," EURASIP Journal on Information Security,springer open journal, march,Vol.1, 2012. pp.1-22.
15. A. ALmomani, et al., "An enhanced online phishing e-mail detection framework based on evolving connectionist system," International Journal of Innovative Computing, Information and Control (IJICIC), Vol.9, No.3,2013.
16. Aggarwal Shivam, Kumar Vishal, SudarsanS.D.: Identification and detection of phishing Emails using Natural Language Processing Techniques.In: SIN'14 Proceedings of the 7th International Conference on Security of Information and Network.
17. Fette Ian, Sadeh Norman, and Tomasic Anthony. : Learning to Detect Phishing Emails.
18. ChandrasekaranMadhusudhanan, ChinchaniRamkumar, UpadhyayShambhu,: PHONEY: Mimicking User Response to Detect Phishing Attacks. In: Proceeding of 2006 International Symposium on a World of Wireless, Mobile and Multimedia Network (WoWMoM'06)