Phishing Counter Measures and their Effectiveness – A Review

Swapan Purkait
Indian Institute of Technology
Kharagpur
India
swapan@nettech.in

ABSTRACT: *Phishing is a social engineering crime on the Web. The rapid development and evolution of phishing techniques pose a big challenge for researchers in both academia and industry. The purpose of this study is to examine the available literature on Phishing and its countermeasures to determine how research has evolved in terms of quantity, content, and publication outlets. In addition, the paper identifies important trends in the literature on Phishing and its countermeasures and provides a view of the research gaps and expected topical areas of interest. This paper presents a comprehensive literature study of research conducted in this area, where 16 doctoral theses and 358 papers are analyzed in terms of research focus, empirical basis on Phishing and proposed countermeasures. We found that the current anti-phishing approaches that have seen significant deployments on the Internet can be classified into 8 groups. Our findings reveal that different approaches proposed in past are all preventive by nature. Phishers continually target the weakest link in the security chain, namely consumers, in their attacks. Various usability studies have demonstrated that neither server-side security indicators nor client-side toolbars and warnings are successful in preventing vulnerable users from being deceived. Educating the Internet users about phishing, as well as the implementation and proper application of anti-phishing measures, are critical steps in protecting the identities of online consumers against phishing attacks. Further research is required to evaluate the effectiveness of the available countermeasures against fresh phishing attacks. Also there is the need to find out the factors which influence Internet user's ability to correctly indentify phishing websites.*

Keywords: Phishing, Phishing Counter Measures, Theft Identity, Internet Security, Phishing sites

Received: 22 June 2012, Revised 28 August 2012, Accepted 31 August 2012

1. Introduction

The word phishing is a variation of the word '*fishing*'. The term was coined by hackers who managed to steal America Online (AOL) accounts way back in the year 1995 [92]. Hackers targeted AOL users and coaxed them to provide their username and passwords. At the time, hacked accounts were dubbed '*phish*'; within a year, '*phish*' was actively being traded between hackers as a form of electronic currency that was of value to them. 'Phishers' used to go after compromised e-mail accounts in order to send out spam.

Phishing methodology is very similar to fishing where a bait is thrown with the hopes that an unsuspecting user will grab it and bite into it just like the fish is also known as the bait and hook method [57]. In most cases, bait is either an email or an

instant messaging site [167], which will take the user to hostile phishing websites, mostly to an exact replica of a financial institution's website. The fake website will have similar look and feel of the original one and will be asking for the sensitive information like user name, password, credit card details etc [86]. When the victim (user) enters the information, the data is sent to the phisher who thereby uses the same for his personal gain. Phishing has become the most common channel for thieves to acquire personal information to aid them in identity theft [134, 25, 9, 55]).

Although, in the past, most criminals only aimed their attacks at consumers in English-speaking countries. Phishers are now targeting consumers and companies all over the world [179]. Studies show a steady increase in phishing activities as well as the related cost. APWG in their annual report published in October 2010 reported 48,244 Phishing attacks in last 12 months [10]. PhishTank the online website which collects data on websites engaged in Phishing received 8,468 valid submissions of phishing websites only in the month of October 2010 [151]. In April 2009 Gartner group published results of a survey showing more than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008, a 39.8 percent increase over the number of victims a year earlier [72]. Table (1) gives a year wise summary of Phishing incident handled by Indian Computer Emergency Response Team (Cert-In) in India (CERT, 2011).

Year	2004	2005	2006	2007	2008	2009	2010
Publishing Incidents	3	101	339	392	604	374	508

Table 1. Year wise summary of Phishing incident handled by Cert-In

1.1 Phishing attacks, solutions and requirements

As discussed by [133] the idea of tricking people for financial profit is an old idea, but the easy availability and popularity of Internet allowed criminals to mount an phishing attacks very easily against multiple users with a single attack [69]. They also highlighted that the Phishing attacks are not only problematic for Internet users, but also for organizations that provide financial services online. The reason is that when users fall victim to Phishers, the organization providing the online service such as online banks often suffers an image loss as well as financial damage [69, 64, 173, 22, 36].

There are many techniques for phishing ranging from, code-based key-logger [73], in-session phishing [54], DNS poison, search engine phishing [16] to mass emailing [63]. [158] discussed various phishing technique in comparison to real world fishing such as Dragnet, Rod-and-Reel, Lobsterpot, Gillnet phishing. Most of the phishing attacks trick users into submitting their personal information using a web form. Even though using a web form to submit sensitive information is common practice on genuine sites, it has a few problems that make phishing attacks effective and hard to prevent. More over one of the main reason for the increase of this menace is anybody with a basic knowledge of send mail protocol or free email services can make a spoof email [102], and creating spoof websites is far too easy and cost nothing, which allows even a novice to make and host a Phishing site [100, 128].

Billions of dollars are lost each year due to unsuspecting users entering personal information into phishing websites, more than monetary loss users may lose their confidence in the system and on their banks [8]. To counter this menace software vendors and companies around the globe have released a variety of anti-phishing tools. As on October 2010, the free software download site download.com, listed more than 100 anti-phishing tools.

As concluded by [149] phishing is a significant and growing problem which threatens to impose increasing monetary losses on businesses and to shatter consumer confidence in e-commerce. As highlighted by authors Phishers will become more active and their attacks will become more sophisticated, making user-based protection mechanisms fragile given the user population of non-experts. As stated by [14, 19, 181]. the increase of phishing poses severe threats to legitimate e-mail communications between both business houses and customers.

The rest of the paper is organised as follows. Section '2' describes the method used for identifying relevant research papers. In section '3' overview of the identified papers will be presented and analyzed in terms of research focus, empirical basis, types of antiphishing solutions and their effects, section '4' presents conclusions and future work.

S.N.	Title	Author	Contribution
1	Fighting Phishing At The User Interface	[188]	The work proposes Web Wallet, it is designed and implemented as a new antiphishing solution. It is a dedicated browser sidebar for users to submit their sensitive information online. User studies in this thesis shows that Web Wallet is not only an effective and promising anti-phishing solution but also a usable personal information manager.
2	Web Identity Security: Advanced Phishing Attacks And Counter Measures	[64]	The study proposes Earth Mover's Distance to evaluate the visual similarity of the suspected web pages to the protected ones. The suspected web pages which are similar to the protected ones will be reported as phishing. The work also proposes series of advanced counter measures against the most prominent phishing scams.
3	Mitigating Phishing Attacks: A Detection, Response And Evaluation Framework	[31]	The thesis makes the following contributions to solve the phishing problem: characterizing and formalizing phishing from spamming, using machine learning approaches that identify authorship, extracting significant features require to build efficient and reliable phishing filter that is computationally efficient and performs well.
4	Phishing Detection Using Distributed Bayesian Additive Regression Trees	[1]	The work demonstrates local DNS poisoning attacks in wireless access points to circumvent security toolbars and phishing filters and provide victims with false misleading information about the legitimacy of phishing sites. As a solution the work proposes distributed architectures based on machine learning approaches to detect phishing emails in a mobile environment.
5	Phishing For Answers: Exploring The Factors That Influence A Participant'S Ability To Correctly Identify Email	[129]	This research study sought to determine if consumer education was a solution by exploring specific characteristics such as age, gender, education, knowledge of phishing or online habits impact a participant's ability to correctly identify email messages. Quantitative data was collected by showing participants ten email messages and quizzing their ability to correctly categorize the messages. The impact age, gender, education, knowledge of phishing and online habits had on their ability to identify the emails was measured.

6	Securing Information Assets: Understanding, Measuring And Protecting Against Social Engineering Attacks	[141]	The work address three areas of social engineering attacks: understanding, measuring and protecting. Understanding deals with finding out more about what social engineering is, and how it works. The measuring area is about trying to find methods and approaches that put numbers on an organization's vulnerability to social engineering attacks. Protecting covers the ways an organization can use to try to prevent attacks.
7	The Impact Of Computer Security Policy Content Elements On Mitigating Phishing Attacks	[39]	This study employed empirical research methods on participants to determine the effectiveness of a security policy to mitigate phishing attacks. The research results reveal that a security policy that contains an explanation of the impact of an attack or contains a statement indicating an evaluation for non-compliance or contains a statement from a direct authority provides no significant impact on mitigating phishing attacks.
8	A Policy Analysis Of Phishing Countermeasures	[169]	The work describes the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks. The author explores the relationship between demographics and phishing susceptibility, and the effectiveness of several antiphishing educational materials. Results suggest that women are more susceptible than men to phishing and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups.
9	Anticipating And Hardening The Web Against Socio-Technical Security Attacks	[177]	The work discusses various phishing attacks through case study and investigates the underlying problems in the way data is transferred in and out of browsers and their components by analyzing a variety of security problems and their corresponding solutions.
10	Fighting Internet Fraud: Anti-Phishing Effectiveness For Phishing Websites Detection	[7]	The work concentrates on anti-Phishing training approaches. The study proposes a new anti-phishing approach which uses Training Intervention for Phishing Websites Detection. The results of thework show that technical ability has no effect whereas Phishing knowledge has a positive effect on Phishing website detection.

11	Human Factors In Web Authentication	[96]	The work describes a new attack against Web authentication called dynamic pharming. To resist dynamic pharming attacks, the work proposes two locked same-origin polices for web browsers. They also evaluate the security and deploy ability of their new approach which shows substantially increase in resistance against Pharming attacks.
12	Phishguru: A System For Educating Users About Semantic Attacks	[106]	The work proposes a system called PhishGuru based on embedded training methodology and learning science principles. Author evaluates the proposed methodology through laboratory and field studies. Result shows that the people trained with the proposed system retain knowledge even after 28 days.
13	Enhancing Web Browsing Security	[196]	The work proposed an approach to transparently feed a relatively large number of bogus credential into a suspected phishing site. The idea is to conceal victims real credentials, so the phishers are not able to use the data for their benefit.
14	Motivation For The Avoidance Of Phishing Threat	[40]	This study adopted the protection motivation theory (PMT) as an underlying theoretical model. The results from the survey condcuted during the study with sample consisted of 376 college students indicated that the research model is substantially able to explain the intention to perform recommended phishing protections. The results also showed that to influence an individual's intention to protect him or herself against phishing attempts, the intervention message should persuade the individual to believe that the threat is real and could be severe.
15	Detecting Visually Similar Web Pages: Application To Phishing Detection	[37]	The work proposes a novel approach for detecting visual similarity between two web pages. Author also tested their system using the most popular Web pages to examine its practicality for the real world situation. The result shows accuracy of the proposed method is extremely high, the true positive and false positive rates reached 100% and 0.8%, respectively.

16	Exploring The Identity-Theft Prevention Efforts Of Consumers In The United States	[117]	This study explores how consumers conceptualize identity theft prevention, determines the characteristics of those who take measures to prevent identity theft, and investigates how the threat of identity theft affects consumer exchange.

Table 2. List of Doctoral Thesis included in review

2. Methodology

Based on suggestions given by various authors [154, 182, 77, 116, 125, 11] for writing a literature review paper, the following steps were adopted to search the sources for the review.

2.1.1 Step 1, Keyword Search

The initial reading list for the review covered 16 doctoral theses from various International Universities. We selected theses first as they are the outcomes of rigorous research and have been reviewed at higher exams. We used Proquest online library as source for all doctoral and master theses. Keywords such as "*phishing*", "*phishing countermeasures*" and "*identity theft*" were used to identify relevant theses for the study. The list of thesis included in review and their classification with respect to their topic and contributions are summarised in Table (2).

Source	All fields	Article title Author	supplied abstracts
ACM	1755	113	238
IEEE	344	145	307
Elsevier	1326	54	86
Emerald	82	4	7
Springer	1306	8	100

Table 3. Gives the result summary for the keyword search for selected digital libraries

For our second stage reading leading journals and International conference papers were selected as relevant sources as these have gone through scientific peer reviews in order to be accepted at journals or conference proceedings. Primarily books were not considered relevant in this study since it is uncertain whether or not these have gone through the same level of review. In order to find existing literature in leading journals and related conference papers we focused on the digital libraries of ACM, IEEE, Elsevier, Emerald and Springer. Keywords such as "*phishing*", "*phishing countermeasures*" and "*identity theft*" were used to identify relevant literature by searching all fields, article titles and author supplied abstracts. In order to identify the first set of relevant papers a preliminary screening was performed for keywords in article title only. Papers with Phishing in their article title were selected for abstract reading. Table (3) gives the result summary for the keyword search for selected digital libraries (result as on January 2012) .

2.1.2 Step 2, Backward Search

After the initial keyword search and screening of the papers on the basis of abstract reading, we did a backward search. As discussed by [116] we did the backward reference search of the selected article which lead us to the previous work on the same field. In some cases we followed the path on the basis of the references given of the referred papers for an in-depth study. We also did authors backward search, to find the previous work on the same author on the same field. Personal websites of various authors and various universities faculty profile pages were very helpful for a complete author search.

2.1.3 Step 3, Forward Search

On our last step we did a forward reference search of the article selected. Which lead us to the article which referred the selected article for their work. Our forward search gave us more insight on the follow-up studies or newer developments related to the selected paper.

	Year																			
	1997	2000	2001	2004		2005		2006		2007		2008		2009		2010		2011		2012	
Source	Conference	Conference	Conference	Conference	Journal	Conference	Journal	Conference	Journal	Conference	Journal	Conference	Journal	Conference	Journal	Conference	Journal	Conference	Journal	Journal	**Total**
IEEE	0	1	0	1	0	5	3	6	3	14	1	20	0	29	2	31	2	14	2	0	134
ACM	0	0	1	2	1	10	2	13	1	25	2	12	3	10	1	5	5	10	1	0	104
Others	1	0	0	3	1	2	3	3	7	5	3	1	6	9	0	1	8	0	0	0	53
Elsevier	0	0	0	0	5	0	4	0	1	0	4	0	5	0	6	0	4	0	7	1	37
Springer	0	0	0	0	0	1	1	0	0	0	2	0	1	0	3	0	3	0	0	0	11
Emerald	0	0	0	0	0	0	0	0	0	0	2	0	0	0	1	0	6	0	1	0	10
JIBC	0	0	0	0	1	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	4
Taylor & Francis	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	3
Wiley	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	2
Total	1	1	1	6	8	18	14	22	12	44	17	33	17	48	14	37	29	24	11	1	**358**

Table 4. Classification of papers related to Phishing and its counter measures according to source and publication year and publication outlet

We continued all the three steps repetitively which included initial abstract reading followed by selective full reading till such time we got a common grouping on the basis of the phishing countermeasures proposed. Our search process yielded a total of 358 research papers. Table (4) gives the classification according to source and publication year and publication outlet. For the classification of the available anti-phishing method in the current work we took the Journal papers as the starting point, subsequently we referred the papers from conference proceedings depending on their relevance to the classification.

3. Review and Discussion

The scale of the phishing problem has necessitated a response to help safeguard vulnerable users [70]. As consequence, anti-phishing and wider identity protection features are commonplace within both web browsers and Internet security suites. A huge number of phishing defences are available. Theses solutions range from quick fix changes to more substantial redesigns [172]. [55] in his work examined the information flow in phishing attacks of all types, and provided detail insights on the technologies used by phisher and the available countermeasures that can be used to prevent such attacks. In order to discuss this wide range of defences, first we examine previous research efforts on phishing countermeasures and then provide an insight why we are still not able to stop phishing effectively.

3.1 Phishing Countermeasures

The current anti-phishing systems that have seen significant deployments on the Internet can classified into the following groups:

1. Stop phishing at the email level
2. Security & password management toolbars

3. Restriction list
4. Visually differentiate the phishing sites
5. 2-Factor and multi-channel authentication
6. Takedown, transaction anomaly detection, log files
7. Anti-phishing training
8. Legal solutions

3.1.1 Stop phishing at the email level

Sending an email asking for somebody's bank account login details is a simple idea and its costs almost nothing. Each day more and more emails are sent with the aim of making the web users believe that the same is legitimate and from the trusted institutions, and ask the user to visit a spoofed site where they will be asked to provide their login credentials. And at the end, the same will be used by miscreants for financial and other benefits. As most phishing attackers send email to lure victims to visit spoofed website, one approach can be to stop this email from getting delivered to the end user. According to Viswanath et al., (2011) the more emails one receives, the more likely they are to be deceived, the risk is more higher for the ones who not only receives but also responds to a large volume of emails.

Organisations are not entirely helpless in the face of a phishing attack through email. In order to better protect customers or employees, one can set up filters for classifying e-mails into two categories, legitimate and fraudulent [30]. Cyota's Israel based Anti Fraud Command Centre (AFCC) employs 30 security analysts. Each day, they scan 1 billion incoming e-mails and check for signs of phishing [101]. Using such proactive e-mail scan organisations can filter out suspicious phishing e-mails and prevent them from reaching the destined e-mail recipients. Many companies install spam filters to protect internal employees. As reflected in the study of Kenyon College, introduction of spam filters was able to stop a significant number of attempts to commit identity theft from getting through users' e-mail [139].

In another work [17] describes new approaches including statistical models for the low-dimensional descriptions of email topics, sequential analysis of email text and external links, the detection of embedded logos as well as indicators for hidden salting. Hidden salting is the intentional addition or distortion of content not perceivable by the reader. During experiments of their work authors found that their methods outperform other published approaches for classifying phishing emails.

[32] in their paper proposed a technique to discriminate phishing e-mails from the legitimate emails using the distinct structural features present in them. Their proposed solutions can be used to classify phishing e-mails before it reaches the users inbox, essentially reducing the human exposure. However the experiment base used during the work is not large enough to draw a broader conclusion. Also the classification approach adopted is only one of the many ways that could be employed, thus the choice of features plays an important role for the success of this approach. In another work [60] proposed a machine learning approach to create a specialized filter named PILFER. In the new filter they used ten very specific features that are more directly applicable to phishing emails. They found their solutions to be more effective then available spam filters.

[80] proposed a heuristic method to determine whether a webpage is a legitimate or a phishing page. The solution is a combination of CANTINA [191] method, Anomaly method, and PILFER method [60], with several additions and modifications. The idea is that every website claims a webpage identity, either real or fake. If a website claims a fake identity, abnormality may exist in a network space; therefore the proposed method could detect and differentiate between a legitimate and a phishing website.

[71] suggested that Internet users should adopt digitally signed mail as countermeasures for phishing emails. Digitally signed email makes use of asymmetric key cryptography such as RSA and allows one to clearly distinguish the identity of sender. [3] proposed a method for implementing a Lightweight Public Key Infrastructure (PKI) for email authentication. In another work they proposed Lightweight Trust Architecture [4], a particular identity-based digital signature scheme for making email trustworthy.

Many people have proposed ways to stop spam emails or unsolicited emails [150] in general, which would include phishing emails. [159] proposed to detect and stop phishing email through different learning and ensemble methods. [41] conducted a detail survey of current and proposed spam filtering techniques with particular emphasis on how well they work. The work includes detailed results and limitations of various available spam filtering techniques. Spamato, an open, extendable, and multi-faceted spam filter framework was proposed by [6]. In another work [160] proposed formalism of Bayesian networks to build probabilistic classifiers to detect junk e-mail. [95] in their paper discusses the effectiveness of Domain Names System Black lists (DNSBLs) in tracking active spam sources. The paperhighlights the problem faced due to DNSBLs false

positive rate and miss rate.

[155] proposed Chung-Kwei, a Pattern-discovery-based System for the Automatic Identification of Unsolicited E-mail Messages. Spamguru, a combination of multiple disparate classifiers, which can detect spam at very low false positive rates, was proposed by [165]. In another work [85] compared three predominant email sender authentication mechanisms based on Domain Name System (DNS): Sender Policy Framework (SPF), Domain Keys Indentified Mail (DKIM) and Sender-ID Framework (SIDF). They highlighted the limitations of these mechanisms, identified risks, and made recommendations for future work. [74] in his paper analyzed the adoption ratio of SPF as an anti-phishing mechanism. His finding indicates that the adoption ratio of SPF is very low despite it being designed for easy adoption and being consistently implemented in several popular anti-spam solutions.

As concluded by Leiba and [113] in their work, One has to agree that spam is a large and complex problem today, and there is a significant financial incentive for spammers to learn to defeat any spam-reduction techniques we develop. Because of that, any robust, long-term anti-spam solution must use multiple techniques in several layers, must incorporate social and legal aspects as well as technical ones, must involve cooperation among all parties interested in finding solutions, and must be rooted in open Internet standards. [29] during their survey research with undergraduate students in a private, north eastern U.S. university found that 46% of electronic mail received by students are spam email.

3.1.1.1 Limitation

As discussed by [143], anti-spam techniques as e-mail filtering may not be effective for the specific problem of phishing detection. Filters, which are often used to classify e-mail content based on the occurrence of certain keywords, may evaluate incorrectly words that appear in e-mails that were not previously classified as Spam. More over as the technology gets better at identifying fraudulent email and blocking it, phishers will get better at hiding their intentions and find ways around the technology. In another case the user may choose not to use the spam filer, or forget to update the filter periodically and resulting in becoming a victim of phishing. Filter can also result in a false positive which can affect the trust of the user on the usage of filter. There are plenty of cases where a filter has flagged a legitimate email to be a spam email, resulting inconvenience to the user. Moreover if the Phishers are able to target the group of victims well enough, like spear phishing [25, 110] lot of these spam & phishing filter discussed above will not be effective. As stated by [119] revising email standards could be effective to fight against phishing but changing the way email works could take years and it's not feasible tocompletely depend on this for solving phishing problems.

3.1.2 Security & password management toolbars

HTTP basic authentication protocol is vulnerable to phishing attacks because a client needs to reveal his password to the server that the client wants to login. Most users have multiple accounts on the Internet where each account is protected by a password. To avoid the headache in remembering and managing a long list of different and unrelated passwords, most users simply use the same password for multiple accounts. A Phisher can effectively steal users' passwords for high-security servers, such as an online banking website by setting up a malicious server or breaking into a low-security server, such as a high-school alumni website. [75] proposed anti-phishing single password protocol. Proposed protocol allows a client to securely use a single password across multiple servers, and also prevents phishing attacks. The protocol achieves client authentication without the client revealing his password to the server at any point. Therefore, a compromised server cannot steal a client's password and replay it to another server.

Although password is one of the most commonly adopted means to protect user accounts, most users are used to giving away the same very easily. Most users disregard the security functionality; they do not have the knowledge and/or the motivation to configure or to use the existing security functions correctly. Some software based protection in the client computer can help in user password management. Whenever a user wants to submit login credential in any of the phishing sites, these tools can be useful to prevent such incident. In recent past various client side and browsers based tools have been proposed as solutions to phishing attacks. [94] proposed Identity Manager, a security tool which offers a user interface for security functionality that is compatible with all Internet applications, so even inexperienced users are able to configure and negotiate their security needs in a convenient way. In another work [90] proposed Web Wallet, a browser sidebar. It detects phishing attacks by determining where users intend to submit their information and suggests an alternative safe path to their intended site if the current site does not match it. It integrates security questions into the user's workflow so that its protection cannot be ignored by the user. Authors conducted a user study on the Web Wallet prototype and found that it significantly decreased the spoof rate of typical phishing attacks from 63% to 7%, and it effectively prevented all phishing attacks as long as it was used. In their concluding remarks they also pointed out, there is the possibility of web wallet getting spoofed in addition there is always a human factor involved in understanding the security warnings given by these toolbars.

[98, 99] in their paper presented a browser extension named AntiPhish, that aims to protect end users against spoofed website based phishing attacks. AntiPhish generates warnings whenever the user attempts to submit login credential to any of the untrusted or spoofed websites. But in any case if the users go ahead without heeding the warnings and login to a spoofed website, the job of AntiPhish will be limited.

Passpet, a tool that improves both the convenience and security was proposed by Yee and [194]. It uses combination of techniques such as password hashing as well as user-assigned site labels to help users to identify the secure sites in case of spoofed attacks. But as concluded by the author the tool may not be of much help in case of a pharming attacks or for a non-SSL sites. In another work [83] proposed TrustBar, a browser extension that allows users to assign a name or logo to identify SSL/TLS-protected sites; if users did not assign a name or logo, TrustBar identifies protected sites by the name or logo of the site, and by the certificate authority (CA) who identified the site.

[79] in their paper proposed Password Multiplier, an implementation in the form of an extension to the Mozilla Firefox web browser. They proposed a novel technique that uses a strengthened cryptographic hash function to compute secure passwords for arbitrarily many accounts while requiring the user to memorize only a single short password or master password. This mechanism functions entirely on the client; no server-side changes are needed. As discussed by the authors the password multiplier has shortcoming in respect to account password changes. There are sites which requires user to change their login password frequently, the same will not be possible with the current application and they proposed to add the same feature in their next release.

In another work [93] presented Pvault, it allowed users to outsource personal data to an server which is not trusted. Data confidentiality and Integrity were preserved using cryptographic techniques. Pvault system allowed users seamless mobile access to their personal data. Pvault auto fill feature fill outs passwords/other information on websites, thereby relinquishing users of the responsibility. It also prevents online scams such as Pharming and Phishing. They also listed some of the drawbacks of the proposed system, which included the requirement of installation of the pvault client software in all remote machine from where users need to perform online web activity. Another problem is as all the Pvault entries are guarded by one master password. If the master password is compromised, all the Pvault entries are easily known to the adversary. It is important that users choose a strong password as the master password.

PwdHash, a browser extension that transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks was proposed by [157]. The browser extension applies a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and a private salt stored on the client machine, theft of the password received at one site will not yield a password that is useful at another site. As noted by the authors this approach may not be effective against a pharming or DNS attack or against any spyware or key logger.

[38] introduce a browser plug-in called SpoofGuard. The plug-in monitors a user's Internet activity, computes a spoof index, and warns the user if the index exceeds a level selected by the user. The proposed solution uses a combination of stateless page evaluation (URL check, Image Check, Link check, Password check), stateful page evaluation (Domain check, Referring page, Image-domain association) and examination of outgoing post data to compute a spoof index. When a user enters a username and password on a spoof site that contains some combination of suspicious URL, misleading domain name, images from an honest site, and a username and password that have previously been used at an honest site, it will intercept the post and warn the user with a popup that foils the attack. But the proposed solution can have a very high false alarm rate because of user using the same password in different site or visiting a site for the first time. The frequent false alarm can de-motivate users to use the solution or to give proper attention to the positive notifications.

3.1.2.1 Limitation

In order to prevent phishing attacks some organizations have implemented Internet browser toolbars for identifying deceptive activities. However, the levels of usability and user interfaces are varying. Some of the toolbars have obvious usability problems, which can affect the performance of these toolbars ultimately [118]. More over security is not always the main concern for the user when they are online, we will see under section 3.2 Why phishing works?, that even in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website. Browser security indicators are misunderstood or ignored frequently, and many users have never noticed them. [91] during their work on image-based authentication techniques found that participants preferred "*convenience*", albeit

with an awareness of the "*security*" risks. As discussed by [109], on their work on coping behaviour, it is the cumulative responsibility of government agencies, business houses and mass media to educate and promote good habit oriented coping practice among users to fight against identity theft.

3.1.3 Restriction list

Malicious or the spoofed websites are the core problem of the phishing activities. There have been various efforts to restrict users to visit these sites. Blacklist is one of such effort, where web browsers check the URLs against a list of URLs of known phishing sites. Upon finding the request URL on a blacklist, the system restricts access and/or generates a warning indicating the danger of a phishing sites. These blacklists are constructed by a range of techniques including manual reporting, link analysis, honey pots, and Web crawlers combined with site analysis heuristics [200]. Blacklist approaches have long been used in other areas such as detection of spam email [94]. A spam blacklist of IP addresses can restrict delivery of spam email to large extent, but a similar restriction list is not possible in case of website as there is a possibility that the IP address can have multiple domains hosted on the same. So a blacklist of specific URLs is a better solution in case of phishing or spoofed websites [170].

However, blacklists have a major drawback; it's mainly a reactive approach. Blacklist maintainers learn of phishing websites only after these sites have become active. Thus, a window of vulnerability remains during which users can suffer from malicious exposure because an active entity has not yet appeared on a blacklist [59]. To solve this inherent problem of blacklist [153] proposed Phishnet, which predicts new malicious URLs from existing blacklist entries as well as performs an approximate match of a given URL to the entries in the blacklist. During the evaluation of PhishNet with real-time blacklist feeds, it was found that the proposed approach suffers from low false positives and is remarkably effective at flagging new URLs that were not part of the original blacklist.

To provide better countermeasures against fraudulent and malicious web sites, Obied and [142] proposed a proxy-based method to prevent access to such web sites dynamically and based on the safety ratings set by McAfee SiteAdvisor. They extended the source code for an open source Linux-based proxy server and added features to check the site's safety rating before allowing HTTP requests to be forwarded. [50] proposed user-behaviour based phishing detection system (UBPD). The proposed model constructs a personal white list for the user by adding websites the user has visited more than three times. UBPD sends warning signal to the user if the user wants to visit any web site which is not in the white list.

In another work [28] proposed automated individual white list, which uses a list of sites based on all familiar login user interfaces of web sites for a user. Every time a user tries to login to a particular site, the site information will be verified with the maintained white list, if the site is not present in a white list, user will be warned for a possible attack. But the same approach can have limited results if the user doesn't adhere to the alert given by the white list. As discussed by [17] most users are unclear about what they are expected to do during a system-initiated security warnings or a security prompt. On a similar work [166] proposed PageSafe, which maintains a white list of URLs with the mapping of corresponding IPs. This list prevents accesses to phishing sites through URL validation and also detects DNS poisoning attacks.

3.1.3.1 Limitation

In case of white list the problem is that same is user specific, change of computer or devices can produce different results if the list is not synchronised with a centrally maintained data base. The restriction list will not be effective for a relatively newer site. As we know that the average age of any phishing site varies from few hours to few days only [170].

3.1.4 Visually differentiate the phishing sites

Detecting phishing Web pages is similar to the problem of detecting duplicate documents and plagiarism, except that these focus on text-based features in similarity measurement, whereas phishing-page detection should focus more on visual similarities [120]. To differentiate the legitimate website from the phishing one, Dynamic Security Skins (DSS) a new class of Human Interactive Proofs (HIPs) that allow a human to distinguish one computer from another has been proposed which requires user to verify visual content from the server [45, 44]. DSS that allows a remote web server to prove its identity in a way that is easy for a human user to verify and hard for an attacker to spoof. If user interfaces elements are customized in a way that is recognizable to the user but very difficult to predict by others, attackers can not mimic those aspects that are unknown to them. It assigns each user a random photographic image that will always appear in the password window, the image will be personal to the user. The user should easily be able to recognize the personal image and should only enter his password when this image is displayed. The personal image is also transparently overlaid onto the textboxes (login form and password form). This ensures that user focus is on the image at the point of text entry and makes it more difficult to spoof the password entry boxes. However, users do not normally bother to look at such indicator before inputting their passwords because DSS in not in the critical path of user's workflow [189].

Third party certification includes hierarchical trust models, like Public Key Infrastructure (PKI), which has long been proposed as a solution for users to authenticate servers and vice-versa. In PKI, chains of Certificate Authorities (CAs) vouch for identity by binding a public key to a entity in a digital certificate. The Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, both rely on PKI. [12] proposed TLS-PSK (Transport Layer Security – Pre Shared Key) instead of only TLS based-certificate which can cause problem during certificate verification process with the designated Certificate Authority (CA). TS-PSK is a way to establish a mutual authentication using a pre shared key between the client and the server. This method avoids the need for public key operations and the certificates. This protocol was designed to avoid the public key operations and to reduce the TLS overhead when used with performance-constrained environments.

Man-in-the-middle (MITM) attacks pose a serious threat to SSL/TLS-based web applications. [144, 145, 146, 147, 148], proposed the notion of SSL/TLS session-aware user authentication (TLS-SA) to protect SSL/TLS-based e-commerce applications against MITM attacks. The main idea behind TLS-SA is to make user authentication depend not only on the user's credentials, such as his password or personal identification number, but also on state information related to the SSL/TLS session in which the credentials are transferred to the server. The rationale is that the server should have the possibility to determine whether the SSL/TLS session in which it receives the credentials is the same as the one the user employed when he sent out the credentials in the first place. If the two sessions are the same, then the session is directly established between the user and the server, whereas if they are different, then an MITM attack is likely taking place. With the help of TLS-SA the server can recognize this and drop the session.

Sakilkar and [161] presented a CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart) solution as phishing defence which embed public key information inside CAPTCHA that client side can verify the public key as well as the destination server. However, if user is such unconscious, force validation is needed; their design requires client side installation. As their CAPTCHA challenges are customized for each user in database and create a specific image list pair for each client, it also further induce database storage issue for growing number of customers, as well as client image list revoke or recovery issues after attack.

[114] in his work demonstrates the limitation of CAPTCHA as well as visual security in securing online banking with a series of test on a CAPTCHA implementation of a local bank. The study shows how CAPTCHA can be bypassed. In his other work [115] he proposed an Extended CAPTCHA Input System to depress phishing by utilizing the properties of CAPTCHA combining the time restriction of One-Time-Password.

[175] introduced dynamic analysis and template matching, that tries to systematically prove, whether a given page is phished or not, using the corresponding original page as the basis of the comparison. It analyzes the layout of the pages under consideration to determine the percentage distortion between them, indicative of any form of malicious alteration. The system design represents an intelligent system, employing dynamic assessment which accurately identifies brand new phishing attacks and will prove effective in reducing the number of false positives. As concluded by the author a success rate of 81% bring this design close to the ideal solutions but leaves lot of scopes for improvements.

In another work [34] proposed an image based antiphishing scheme based on discriminative key point features in Web pages. Their invariant content descriptor, the Contrast Context Histogram (CCH), computes the similarity degree between suspicious and authentic pages. Proposed method takes a snapshot of a suspect Web page and treat it as an image throughout the detection process. It uses CCH to capture invariant information around discriminative key points on the suspect page and then match the descriptors with those of authentic pages that are often targeted by phishers.

[36] proposed a new approach based on for Gestalt theory detecting visual similarity between two Web pages. To evaluate their approach they tried to group twelve legitimate web pages and twelve phishing pages each targeting one of these pages together in pairs. Based on the argument that a legitimate page and a phishing page targeting it are highly similar to one another. After analyzing the result of their experiment they found twelve pairs have been successfully paired together as the most similar to one another, for all twelve pairs.

In another work how server operators might automatically detect fraudulent sites [65] proposed detection of phishing web pages based on visual similarity, which can be utilized as a part of an enterprise solution for anti-phishing. A legitimate webpage owner can use this approach to search the Web for suspicious webpage which is visually similar to the true web page. The

approach first decomposes the web pages into salient blocks according to visual cues. The visual similarity between two web pages is then measured in three aspects: block level similarity, layout similarity, and overall style similarity. A webpage is reported as a phishing suspect if any of these similarities to the true webpage is higher than a threshold.

[190] introduced a new anti-phishing solution, the Web Wallet. The Web Wallet is a browser sidebar which users can use to submit their sensitive information online. It detects phishing attacks by determining where users intend to submit their information and suggests an alternative safe path to their intended site if the current site does not match it. It integrates security questions into the user's workflow so that its protection cannot be ignored by the user. However, the study also found that spoofing the Web Wallet interface itself was an effective attack. Moreover, it was not easy to completely stop all subjects from typing sensitive information directly into web forms.

[197] proposed BogusBiter, a client-side anti-phishing tool to automatically protect vulnerable users by injecting a relatively large number of bogus credentials into phishing sites, these bogus credentials hide victim's real credentials and force phisher to verify the collected credentials at the legitimate web sites. The mechanism has two key design objectives. First offensive, it tries to inject as many as possible bogus credentials on the phishing site. Second defensive, it enables legitimate web site to exploit the filtering process initiated by the phisher for detecting user's stolen credentials in a timely manner. Author also concluded that should BogusBiter become widely deployed, phishers may explore its limitations to circumvent it with offline evasions and online evasions to filter harvested passwords.

In recent work [198] proposed a new content-based anti-phishing system based on Bayesian theory. The proposed framework includes a text classifier, an image classifier, and a fusion algorithm. Based on the textual content, the text classifier is able to classify a given web page into corresponding categories as phishing or normal. Based on the visual content, the image classifier, which relies on Earth Movers Distance (EMD), is able to calculate the visual similarity between the given web page and the protected web page efficiently. The matching threshold used in both text classifier and image classifier is effectively estimated by using a probabilistic model derived from the Bayesian theory.

3.1.4.1Limitation

As discussed by [175] their solution can provide success rate of 81%, but the same leaves other 19% which will be vulnerable for phishing attacks. [148] in their work sites that their method is a visual method and assumes the phishing Web pages are visually similar to their attacking targets. The method could not detect those which are not visually similar. More over as discussed earlier as the technology gets better at identifying fraudulent phishing sites or visually differentiating it, phishers will get better at hiding their intentions and find ways around the technology. Also as mentioned earlier visual security indicators are misunderstood or ignored frequently, and many users have never noticed them.

3.1.5 2-Factor and multi-channel authentication

Traditionally passwords are used for authentication in any online websites. One has to memorise the password for the site and provide the same on demand by the website. If a third party gets to know the password then the said account is compromised [21]. In order to solve the problem faced with the usage of passwords researches have proposed 2-factor authentication. In 2-factor authentication process, user should prove "*what he knows*" and "*what he has*". Here what he knows is the password, and what he has is something that only the genuine user will have. This something can be a hardware token given by the institutions which can generate Personal Identification Numbers (PIN) [140], or a One Time Password (OTP) [136, 192] or some Personal certificate or documents which only the user can have. Though the cost of implementation will be very high one can consider biometrics based authentication also [201]. With the help of OTP and separate Boot USB or CD, [130] proposed multi-factor mutual authentication. First, the server is authenticated and next, if the result of the server authentication is successful, the user will provide his credentials. In this manner user credentials are prevented from being stolen by a hijacking server.

In another work [5] proposed BeamAuth, a two-factor web authentication technique where the second factor is a specially crafted bookmark. While using BeamAuth user will be required to select a preconfigured bookmark in his client browser to authenticate himself. Many banks have altered their authentication mechanisms, suggesting a willingness to adapt and go beyond traditional and simple passwords [82].

[127] proposed to use mobile phone network to authenticate services on internet through an un-trusted computer. On a similar line [135] proposed user authentication using multiple communication channels. Their solution enables on-line service providers to strongly authenticate their users on a non-trusted communication channel via trusted communication channels. Their method to utilize a mobile phone network based authentication onto services on the Internet that can strongly authenticate

users without loosing usability, can expand the usage of a mobile phone network to the Internet services which can lead to an application convergence of the mobile and the fixed networks.

As hardware token based methods are quite expensive because every user has to get his own token, also the costs for training and administration are higher than for password based methods because the users have to be taught how to use the tokens. [152] proposed paper-based challenge-response-approach where users needs a single sheet with the challenge-response-pairs for every service he wants to use, which is a compromise between security and costs.

3.1.5.1 Limitation

The biggest hurdle for the same will be is ease of use as discussed by [122]. Most Internet users won't adopt security processes that are too cumbersome, and most online businesses don't want to burden their users. Sending a one-time password or authentication code by SMS text message is also not very secure, because they are often sent in clear text. Mobile phones are easily lost and stolen and if another person has possession of the user's phone, they could read the text message and fraudulently authenticate. SMS text messages can also be intercepted and forwarded to another phone number, allowing a cybercriminal to receive the authentication code. With more businesses relying on mobile phones authentication, cybercriminals will increasingly target this channel for attack. However, the challenge for consumer-facing websites is to balance strong security with usability. Complicated security schemes will not achieve widespread adoption among Internet users. As discussed by [152] cost of implementation of such system will also be hurdle for many institution.

3.1.6 Takedown, transaction anomaly detection, log files

Banks and other organisations deal with fraudulent phishing websites by pressing hosting service providers to remove the sites from the Internet so that there is nothing there for a misled visitor to see, the procedure is commonly known as take-down [137]. Most banks and specialist take-down companies maintain their own feed. PhishTank the online website asks the end users to visit their site and contribute to their source list [151]. Users are invited not only to provide the content but also to verify that the entries are correctly classified. In another work [138] gathered phishing reports from the PhishTank. After analysing the data received from PhishTank authors concluded that any crowd-based decision mechanism link PhishTank remains susceptible to vote rigging and manipulation that could undermine its credibility.

[137] studied the empirical data on phishing website removal times and the number of visitors that the websites attract, and concluded that website removal is part of the answer to phishing, but it is not fast enough to completely mitigate the problem. Until they are removed, the fraudsters learn the passwords, personal identification numbers (PINs) and other personal details of the users who are fooled into visiting them.

In order to detect potentially fraudulent transactions, transaction anomaly detection systems are available. [20] in his paper outlines a framework for Internet banking security using multi-layered, feed-forward artificial neural networks. Such applications utilise anomaly detection techniques which can be applied for transaction authentication and intrusion detection within Internet banking security architectures. It can combine user profiling with business rules to detect suspicious account activity. Suspicious transactions are alerted to the bank's professionals so appropriate reactive measures can be taken. [56] in his report discusses the log analysis approach, which is analysis of audit trails in order to detect phishing lures, hooks and catches. According to his report these mechanisms can dramatically improve a bank's responsiveness to phishing attacks. Indeed, if logs are monitored in real-time, extremely quick response times could be reached.

Tracking the source of phishing attacks is a difficult challenge for investigators. The attacks are frequently launched from botnets comprised of infected, innocent users and web servers compromised by malware. Steel and [122] proposed Automated Impersonator Image Identification System (AIIIS), which allows investigators to track images used in impersonation attacks back to the original download from the source. AIIIS accomplishes this by digitally encoding the IP address, server, and time of the image download into the image itself through a digital watermark. If the image appears on any site the same can be identified.

3.1.6.1 Limitation

Take down effort is not be effective against Fast Flux [131]. Web site using Fast flux typically resolves to many IP addresses, each with a short validity. Successive site resolutions often lead to a new set of IP addresses, which increases availability. At the same time, the addresses' short validity ensures that the sites' operators can provide a new, up-to-date list of machines to host the sites. Without appropriate legal implication and support, takedown will be difficult to implement. With easy available of free hosting sites, takedown will not be an effective deterrent for phishers. Transaction anomaly and log detection both of these comes are reactive in nature. We can only analyze and take appropriate action only after the incident has occurred. Which keeps

the phishers always ahead of us. In case of detecting phishing attacks through log files, the same may not stop the theft of credentials, but it might allow to least detect their subsequent use [184].

3.1.7 Anti-phishing training

Core idea of Anti-phishing training is that users can be trained to actively protect themselves from phishing threats. The United States Military Academy (USMA) has been very active in implementing hands-on exercises such as the Cyber Defence Exercise [47]. Typically, these exercises involve participation by knowing participants and involve a network attack/defence scenario. The use of exercises to reinforce concepts in an education setting has been proposed by [48]. In another work [49] stated that user security education and training is one of the most important aspects of an organisations security postures. [103] conducted lab experiments contrasting the effectiveness of standard security notices about phishing with two embedded training designs they developed. They found that embedded training works better than the current practice of sending security notices. They concluded embedded training interventions helped teach people about phishing and to avoid phishing attacks.

In another paper [104] studied an embedded training methodology using learning science principles in which phishing education is made part of a primary task for users. The goal is to motivate users to pay attention to the training materials. In embedded training, users are sent simulated phishing attacks and trained after they fall for the attacks. They tested users to determine how well they retained knowledge gained through embedded training and how well they transferred this knowledge to identify other types of phishing emails. They concluded that users learn more effectively when the training materials are presented after users fall for the attack (embedded) than when the same training materials are sent by email (non-embedded).

[107] and [108] conducted research works which focuses on educating users about phishing and helping them make better trust decisions. They identified a number of challenges for end-user security education in general and anti-phishing education in particular. They developed an email-based anti-phishing education system called "*PhishGuru*" and an online game called "*Anti-Phishing Phil*" that teaches users how to use cues in URLs to avoid falling for phishing attacks. Their test result suggests that, while automated detection systems should be used as the first line of defence against phishing attacks, user education offers a complementary approach to help people better recognize fraudulent emails and websites.

[168] have shown that people can be trained about phishing URLs through an online game called Anti-Phishing Phil. They found the game to be effective in both a laboratory setting and in the real world. They found that the participants who played the game were better able to identify fraudulent web sites compared to the participants in other conditions. They concluded that their work can be an effective way of educating people about phishing and other security attacks. In another work Srikwan and [176] proposed a cartoon-based online training approach aimed at improving the understanding of risk among typical Internet users. [108] conducted a role-play survey among 1001 online respondents to study both the relationship between demographics and phishing susceptibility and the effectiveness of several antiphishing educational materials. Their work shows that educational materials reduced users' tendency to enter information into phishing web pages by 40% percent, however, some of the educational materials they tested also slightly decreased participants' tendency to click on legitimate links.

Another method for educating users is to send fake phishing emails to test users' vulnerability, and then follow up with training. Subsequent fake phishing emails can be used to measure improvements in phishing detection abilities. This approach has been used by [88] and has shown that education can improve participants' ability to identify phishing emails. They concluded that people can become less vulnerable by a heightened awareness of the dangers of phishing, the importance of reporting attacks to which they fall victims, the ease of spoofing, and the possible misuses of personal information posted on the Web. Lungu and [123] in their work underline the need for a higher degree of awareness related to safe network use and practices. They concluded good user education is a key component for building the trust necessary to overcome the the phishing fears.

Phishing education can also be conducted in class room settings with a good result. [156] applied this strategy in Introduction to Computing courses as part of the computer security component aimed at students pursuing a non-computer science education. Class assessment indicates an increased level of awareness and better recognition of attacks. However, it is not a easy job to train a large number of end users through class room teaching sessions. [26] in his paper listed some of the anti-phishing precautionary measures to educate the internet consumer, who may be a potential phishing victim. The paper also lists some of the measures that can be applied when consumers have responded to phishing emails.

It is evident that the problem of phishing is not going away in the near future. Therefore, the need stands for organizations to

take proactive steps in educating their consumers about the potential risks of phishing. [14] explored the organisational publicrelationship with customers to prevent phishing attacks. Authors concluded that public relations professionals will have a better understanding of their online consumer relationships and will likely establish better relationships among consumers and potential consumers alike. As technology increases and becomes more prevalent, the human factor remains the most viable target for would-be attackers. In recent times the attack has moved seamlessly back and forth between e-mail to one of our most trusted utilities, the telephone system, now combining the two. Criminals are now using vishing [33] a technique which uses convenience of Voice over Internet Protocol (VoIP) combined with electronic mail phishing techniques. As concluded by [78] Vishing exploits the consumer's trust in landline telephone services, educating users about the different types of threats that are present, and training them on how best to respond to these attacks, can greatly reduce the success rate attackers currently enjoy.

3.1.7.1 Limitation

It would be interesting to study longer periods (more than 6 months) of retention for a training program. Previous studies on users training has shown significant improvement on phishing detection but none has tested the retention for a longer period. More importantly training involves cost, not many business houses are keen to spent extra on users training. Users training is not a onetime cost. To get benefit out of that, one has to keep periodical training program which will ask for cost-benefit analysis. It is not physically possible to train the entire population. It is also not certain that after proper training user will behave on ideal manner or follow all instructions. Finding shows that education is effective and needed but not a cure all.

3.1.8 Legal solutions

It is clear that phishing is part of our social and technological reality. Active development of the necessary legislation is desperately required. [111] in their work stated that the law, however, must take proper notice of current technical risks as well as measures taken to counter them. [76] conducted a detail study on phishing experience & available legal frame work in both the developing and the developed world. [132] is his paper examines the existing state laws in USA aimed at stopping phishing as well as proposed federal legislation. He concluded that adequate legal solutions would enable severe punishment of those caught phishing; the law also would allow both the victims of a phishing scam, and companies whose information was fraudulently used, to collect damages. [23] found that in Hong Kong government advocacy for adoption of antiphishing measures influenced the adoption of two-factor authentication by banks.

[112] in his paper recommended that courts should consider either large scale damages against individual phishers or secondary liability against Internet Service Providers (ISP) under the areas of either Intellectual Property (IP) or unfair competition law. The addition of secondary liability to anti-phishing efforts might motivate ISPs to become actively involved in anti-phishing efforts, the least cost avoider since ISPs are best positioned to prevent of phishing schemes [27]. Additionally, trademark holders are also well positioned to deter phishing by asserting their IP rights against trademark infringing phishers and those engaging in unfair competition. The trans-national nature of the phishing or the overall cyber crime is the most accepted characteristics. [121] in his work highlights the judicial challenges and recommends for expedient international cooperation and harmonization of cyber criminal offences amongst legal systems beyond borders.

3.1.8.1 Limitation

As analyzed by [46], the legal scaffold of Malaysia, Unites States and United Kingdom and concluded that inadequacy of current legal framework is the main challenge to govern phishing. Nevertheless, until effective anti-phishing strategies are implemented, the cat-and-mouse game is likely to continue, as the law and law enforcement continue to struggle keeping up with technology and technology-related crimes. As stated by [97] the security model includes many participants with dissimilar interests: users, browser vendors, developers, CAs, Web server vendors, Websites, regulators, and standards committees. It is not easy to reach timely agreement among them. Keeping gullible computer user in mind [163] concluded that before we can think about regulatory tools to curb practices like phishing and identity theft we need a better understanding of the interactions between data, devices and networks. With the advance of technology, phishing attacks are becoming very sophisticated and difficult to identify, even for the experts. As stated by [174] it is not clear that the law would impose on the customer the primary obligation for defending against phishing attacks, especially where the success of the attack may depend on the phished company's choice of security.

These different approaches discusses above are all preventive by nature. Recent usability studies have demonstrated that neither server-side security indicators nor client-side toolbars and warnings are successful in preventing vulnerable users from being deceived [196]. This is mainly because;

a). Phishers can convincingly imitate the appearance of legitimate web sites.

b). Users tend to ignore security indicators of warnings.

c). Users do not necessarily interpret security cues appropriately.

3.2 Why phishing works?

Security is not always the main concern for the user when they are online and submitting confidential login credential in any website they are visiting. [45] in their paper addresses the question of why phishing works. They analyzed a set of phishing attacks and developed a set of hypothesis about how users are deceived. They tested the same in a usability study with 22 participants, and found out good phishing websites fooled 90% of participants. They also found the majority of the participants ignore the available security indicators. Their work illustrates that even in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website. The authors concluded that browser security indicators are misunderstood or ignored frequently, and many users have never noticed them.

[15] conducted an e-mail-based experiment, in which 152 staff members were sent a message asking them to follow a link to an external web site and install a claimed software update. The message utilised a number of social engineering techniques, but was also designed to convey signs of a deception in order to alert security-aware users. The external web site, to which the link was pointing, was intentionally badly designed in the hope of raising the users' suspicions and preventing them from proceeding with the software installation. The results revealed that 23 per-cent of recipients were fooled by the attack, suggesting that many users lack a baseline level of security awareness that is useful to protect them online.

[168] conducted a similar lab study in which they showed 42 participants 20 web sites and asked them to determine which were fraudulent. However, in this study participants took a break after reviewing half the sites. During the break, one group of participants played an anti-phishing game, one group read an anti-phishing tutorial, and one group played solitaire and did other unrelated activities. Similar to [45], the authors found that users have difficulty determining which sites are legitimate. However, after less than 15 minutes of training via the antiphishing game, study participants improved their ability to distinguish legitimate and fraudulent sites considerably. The participants in the tutorial condition also improved, although not as much as those in the game condition.

In another work [2] created an exact replica of the original Jordan Ahli Bank website www.ahlionline.com.jo and sent deceptive phishing email to 120 employees of the Bank after attaining the necessary authorizations from the management. They found most of the employees did not check the certificate that was presented to their browser during the study since they do not know what it means; those that do know occasionally check them out. Some employees pointed out that the content details of the website and its fancy design and style were one of the main reasons for their opinion about the legitimacy of the website. They assumed that the site would be legitimate if it contained high-quality images and lots of animations.

In another work [84] highlights the basic and advance indicators of most web browsers and their usability problems also showed that users often enter their passwords without validating that SSL/TLS is active and that the URL is correct. [53] found that 97% of sixty participants fell for at least one of the phishing messages that the authors sent them. In their laboratory study they examined the effectiveness of browser warnings, and how they fail users. Of the participants who saw the active phishing warnings, 21% of the participants ignore the same and continued their browsing. As many as 99% of the participants ignore passive warnings and submitted personal login credential in a fraudulent website. [87] in his article in Computer Fraud & Security points out though the day of the amateur hacker has gone, but there are still plenty of amateur users.

In another work [185] conducted a field study at a large services organization involved in the insurance and financial industries in the Unites studies. A total no. of 588 employees participated. The work investigated whether the factors that account for how people are persuaded in marketing campaigns to make purchases may apply as well to social engineering to give up confidential information. The study reveal that people feel obligated to reciprocate social engineering gestures and favours such as receiving free software or gift certificates by giving up company e-mail addresses, employee identification numbers, financial and insurance data, and other confidential and sensitive information.

[51] conducted an interview study with 20 non expert computer users to reveal their strategies and understand their decision when encountering possible suspicious emails. They found that merely being aware of phishing or of cues is not enough to

protect people form scams, especially new ones about which they might not be aware. One of the reasons that people may be vulnerable to phishing schemes is that awareness of the risks is not linked to perceived vulnerability or to useful strategies in identifying phishing emails. Their work suggested that people can manage the risks that they are most familiar with, but don't appear to extrapolate to be wary of unfamiliar risks.

[164] conducted a study to evaluate how effectively website authentication indicators protect users from fraudulent sites. They concluded that users ignore HTTPS indicators, during their study 23 of the 25 participants entered their passwords when security indicators where removed.

The credibility of the websites is becoming an increasingly important area in phishing. [62] in a large quantitative study on what makes web sites credible, found out the following five types of element such as real-world feel, ease of use, expertise, trustworthiness and tailoring increased the credibility perceptions of the websites. With technological advances all these elements can be incorporated in a fraudulent websites by a sophisticated phisher to make the site more credible. In another work [90] reports the highlights of a user study which gauges reactions to a variety of common trust indicators such as logos, third party endorsements, and padlock icons over a selection of authentic and phishing stimuli. In the course of the think-aloud protocol, participants revealed different sensitivities to email messages and web pages. The principal result of the work is the analysis of what makes phishing emails and web pages appear authentic.

[186] and [187] in their work phished 446 subjects for confidential information in order to understand the individual factors that help influence deception detection within a phishing context. Authors interviewed the detectors and elicited a rich account of how the subjects processed and formed a correct behavioural decision upon receiving the phishing email. The result of the study indicated, individuals who are suspicious either through personality-based traits, their knowledge based awareness or past web experience tend to be successful detectors of deception.

[52] conducted a pilot survey with 232 computer users from a diverse group of faculty, staff and students, including people who were concerned about computer security. They found out that deeper understanding of the web environment, such as being able to correctly interpret URLs and understanding what a lock signifies, is associated with less vulnerability to phishing attacks. Perceived severity of the consequences does not predict behaviour. The authors concluded tools that aim to combat phishing attacks must take into account how and why people fall for them in order to be effective. They also suggested that educational effort should aim to increase users' intuitive understanding, rather than merely warning them about risks.

In a large scale study done by [61] on web users password habits, results confirmed the conventional wisdom about the large number and poor quality of user passwords. In addition the passwords are re-used and forgotten a great deal. Authors were able to estimate the number of accounts that users maintain and the number of passwords they type per day also the percent of phishing victims in overall population. In another work [81] emphasises on the amount of low skills required to become a phisher, which in turn lure more and more new entrants in the phishing business.

In order to access the extent to which users are able to spot phishing [68] conducted an online survey with 179 participants. Participants were shown 20 potential phishing messages and were asked to judge the legitimacy of each one. The results from the study were hardly encouraging, and revealed that people are not properly attuned to what to look for in a phishing message. Authors concluded that users are lacking a baseline level of online safety awareness.

[189] conducted two user studies of three security toolbars and other browser security indicators and found them all ineffective at preventing phishing attacks. Even though subjects were asked to pay attention to the toolbar, many failed to look at it; others disregarded or explained away the toolbars' warnings if the content of web pages looked legitimate. They concluded Users fail to continuously check the browser's security indicators, since maintaining security is not the user's primary goal. Although users sometimes noticed suspicious signs coming from the indicators, they either did not know how to interpret the signs or they explained them away. Many users had no idea how sophisticated an attack could be, and do not know good practices for staying safe online.

In another similar study [199] evaluated some of the major Anti-Phishing tools available and demonstrated that many of the tools tested were vulnerable to simple exploits. They concluded that all the tools examined appear to have some usability problems and it is very important that these problems to be resolved if these tools are to be effective. An anti-phishing tool could identify all fraudulent web sites without any false positives, but if it has usability problems, users might still fall victim to fraud. [42]

states, "*Although a number of technology-focussed counter measures have been explored, user behaviour remains fundamental to increased online security. Encouraging users to engage in secure online behaviour is difficult with a number of different barriers to change.*"

As discussed above, an educated, informed, and alert consumer could play an important role in improving online banking security and be better prepared against phishing attacks. Bank and financial institutions plays a major role in online education and informing customers about the security threats. [162] examined website contents of 200 largest US banks for information on phishing and security alerts. Authors found that though more of the larger banks are committed to online education of customers, but smaller banks are completely mute on this issue. They are not involved in any online education about fraud detection. Moreover they found Many consumers are unaware about the extent of loss for which they might be held responsible if a fraudster accessed their account illegally.

4. Conclusion and future work

Over the last decade, social engineering attacks on Internet, such as phishing, have grown considerably. Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter personal information on the same. Phishers usually make web pages visually similar to real web pages to spoof users. The academic work on phishing has been diverse, researchers have tried to understand the psychology of the process, how to block the spam email to reach the end user, and how server operators might automatically detect fraudulent sites. In this work we have tried to identify previous works and important trends in the literature on Phishing and its countermeasures. We found that the current anti-phishing approaches that have seen significant deployments on the Internet can be classified into 8 groups. Our findings reveal that different approaches proposed in past are all preventive by nature. Phishers continually target the weakest link in the security chain, namely consumers, in their attacks. Various usability studies have demonstrated that neither server-side security indicators nor client-side toolbars and warnings are successful in preventing vulnerable users from being deceived. [89] has shown that even with the effects of modern anti-spoofing and antiphishing efforts, more than 11% users will read a spoofed message, click the link it contains, and enter their login information. Although some of the work indicates that the education of online consumers, as well as the implementation and proper application of anti-phishing measures, can reduce the risk of consumers falling victim to phishing attacks. Educating the Internet users about phishing, as well as the implementation and proper application of anti-phishing measures, are critical steps in protecting the identities of online consumers against phishing attacks.

Phishing attacks have severe negative impacts for the web and the end user's trust. In this paper we saw several advanced antiphishing methods. If one has to agree with the effectiveness of all these methods Phishing should have been eradicated by now, but the same is not the case. We saw that all phishing problems are not solved by these methods. In one hand we have users who are complete ignorant about phishing in other hand we have criminals who are manufacturing new ideas everyday for a new phishing methods. Hence it is necessary to have further work on new and effective phishing countermeasures.

As concluded by [124] there is no one solution at any one level that will solve the phishing problem. Stakeholders at each level can and must make greater efforts and institute new practices to prevent this menace. Author also insisted that the stakeholders among the levels also must collaborate with each other to find new solutions which will be cross level involving all parties.

Phishing is a pervasive problem that will not disappear in the near future, but will most likely become even more sophisticated [34]. Further research is also required to evaluate the effectiveness of the available countermeasures against fresh phishing attacks. Everyday newer and innovative attacks are being deployed on the Internet. It is important to continuously As discussed by [193] users often understand security, but rank other things such as aesthetics or ease of use ahead of it. Further work will be useful which measures whether users still understand the security message when they are focused on a stressful deadline, or whether users will leave browsers security features enabled when given the choice to disable them.

Also there is the need to find out the factors which influence Internet user's ability to correctly indentify phishing websites. We need to know why it works rather then what works. We saw many previous works impacts of various factors and identifying phishing websites or spam emails, but doesn't indicate why? If we know why those factors affects the users we can design new training procedure or a new tools to address the same issue.

Further work required to evaluate effectiveness of single domain usage for companies against multiple domain and IP addresses for their sites. Lot many times users confuses with the domain name and the brand or the product in question. Usage of various child domain also adds to the confusion.

Work required to provide a secure path between the end users computer to the intended site. When a users types the desired website address in the browser only the legitimate site or user's intended site should open. Future work is also required on the direction on legal jurisdiction to discourage phishing attacks. Catching criminals would provide a strong deterrent as it shows the determination and capability of law enforcement. Internet has no International boundary, so as the phishers, we need to address the complexity of various political and legal hurdle of various nations to facilitate greater information sharing between law enforcement agencies.

Another avenue of future work is to consider various characteristics of the website that can be identified as the phishing websites. For example IP address as domain name, many dots (.) in the URL address, or the age of the websites as phishing websites are generally registered for few days. Many phishing websites comes from the free hosting sites. Evaluation of all these characteristics can lead to a possible solutions for effective phishing site detection.

References

[1] Abu-Nimeh, S. (2008). Phishing Detection Using Distributed Bayesian Additive Regression Trees. Unpublished doctoral dissertation, Southern Methodist University, Dallas, United States.

[2] Aburrous, M., Hossain, M. A., Dahal, K., Thabtah, F. (2010). Experimental Case Studies For Investigating E-BankingPhishing Techniques And Attack Strategies. *Cognitive Computation*, 2 (3) 242-253.

[3] Adida, B., Hohenberger, S., Rivest, R. (2005a). Lightweight encryption for e-mail. *In*: USENIX steps to reducing unwanted traffic on the internet workshop (SRUTI).

[4] Adida, B., Hohenberger, S., Rivest, R. (2005b). Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails. *In*: DIMACS Workshop on Theft in E-Commerce.

[5] Adida, B. (2007). BeamAuth: two-factor web authentication with a bookmark. *In*: Proceedings of the 14th ACM onference on Computer and communications security, Alexandria, Virginia, USA.

[6] Albrecht, K., Burri, N., Wattenhofer, R. (2005). Spamato - An Extendable Spam Filter System. *In*: Proceedings of CEAS.

[7] Alnajim, A. M. (2009). Fighting Internet Fraud: Anti-Phishing Effectiveness For Phishing Websites Detection. Unpublished doctoral dissertation, Durham University, Durham, Uk.

[8] Altintas, M. H., Gursakal, N. (2007). Phishing Attacks and Perceptions of Service Quality: A Content Analysis of Internet Banking in Turkey. *Journal of Internet Banking & Commerce*, Aug, 12 (2), 1-13.

[9] Anderson, K. B., Durbin, E., Salinger, M. A., (2008). Identity Theft. *Journal of Economic Perspectives*. 22 (2). Spring 2008, 171–192.

[10] APWG (2010). Global Phishing Survey: Trends and Domain Name Use in 1H2010. Anti-Phishing Working Group (APWG), November, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf.

[11] Armitage, A., Keeble-Allen, D. (2008). Undertaking a Structured Literature Review or Structuring a Literature Review: Tales from the Field. *The Electronic Journal of Business Research Methods*, 6 (2)103 - 114.

[12] Badra, M., El-Sawda, S., Hajjeh, I. (2007). Phishing Attacks and Solutions. *In*: Proceedings of the 3rd international conference on Mobile multimedia communications, Mobimedia, Nafpaktos, Aitolokarnanania, Greece.

[13] Baker, E. M., Tedesco, J. C., Baker, W. H. (2006). Consumer Privacy And Trust Online: An Experimental Analysis Of Anti-Phishing Promotional Effects. *Journal of Website Promotion*, 2 (1/2) 89-113.

[14] Baker, E. M., Baker, W. H., Tedesco, J. C. (2007). Organizations Respond to Phishing: Exploring the Public Relations Tackle Box. *Communication Research Reports*, 24 (4) 327–339.

[15] Bakhshi, T., Papadaki, M., Furnell, S. (2009). Social Engineering: Assessing Vulnerabilities in Practice. *Information Management & Computer Security*, 17 (1) 53 – 63.

[16] Bargadiya, M., Chaudhari, V., Khan, M. I., Verma, B. (2010). The Web Identity Prevention: Factors To Consider In The Anti-Phishing Design. *International Journal of Engineering Science and Technology*, 2 (7) 2807-2812.

[17] Bergholz, A., Beer, J. D., Glahn, S., Moens, M., Paa, G., Strobel, S. (2010). New Filitering Approaches For Phishing Email. *Journal of Computer Security*, 18 (1) 7–35.

[18] Bielski, L. (2004). Phishing Phace-Off. American Bankers Association. *ABA Banking Journal*, 96, Sep, 46-54.

[19] Bielski, L. (2005). Security Breaches Hitting Home. American Bankers Association. *ABA Banking Journal*, 97, June, 7-8.

[20] Bignell, K. B. (2006). Authentication in an Internet Banking Environment; Towards Developing a Strategy for Fraud Detection. *In*: Proceedings of International Conference on Internet Surveillance and Protection, 23.

[21] Bose, I., Leung, A. C. M. (2007). Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities, *Communications of the Association for Information Systems*, 19 (1) 544-566.

[22] Bose, I., Leung, A. C. M. (2008). Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decision Support Systems*, 45, 897-912.

[23] Bose, I., Leung, A. C. M. (2009). What Drives The Adoption Of Antiphishing Measures By Hong Kong Banks?. *Communications of the ACM*, 52 (8) 141-143.

[24] Brainbridge, D. (2007). Criminal law tackles computer fraud and misuse. Computer Law and Security Report, 23, 276-281.

[25] Brody, R. G., Mulig, E., Kimball, V. (2007). Phishing, Pharming and Identity Theft. *Academy of Accounting and Financial Studies Journal*, 11, 43-56.

[26] Butler, R. (2007). A Framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*, 25 (5) 517-533.

[27] Calman, C. (2006). Bigger Phish To Fry: California'S Antiphishing Statute And Its Potential Imposition Of Secondary Liability On Internet Service Providers. *Richmond Journal of Law & Technology*, 13 (1) 1-24.

[28] Cao, Y., Han, W., Le, Y. (2008). Anti-phishing based on automated individual white-list. *In*: Proceedings of the 4th ACM workshop on Digital identity management, Alexandria, Virginia, USA.

[29] Case, C. J., King, D. L. (2008). Phsihng For Undergraduate Students. *Research in Higher Education Journal*, 1,100-106.

[30] Castillo, M. D., Iglesias, A., Serrano, J. I. (2007). Detecting Phishing E-Mails By Heterogeneous Classification. H.Yin et al. (Eds.): IDEAL, LNCS 4881, 296–305.

[31] Ceesay, E. N. (2008). Mitigating Phishing Attacks: A Detection, Response And Evaluation Framework. Unpublished doctoral dissertation, University Of California, United StatesCERT (2011), Indian Computer Emergency Response Team (CERT-IN); November, http://www.cert-in.org.in/

[32] Chandrasekaran, M., Narayanan, K., Upadhyaya, S. (2006). Towards phishing e-mail detection based on their structural properties. New York State Cyber Security Conference, USA.

[33] Chang, J. -H., Lee, K. -H. (2010). Voice phishing detection technique based on minimum classification error method incorporating codec parameters. *IET Signal Process*, 4 (5) 502–509.

[34] Chen, K., Chen, J., Huang, C., Chen, C. (2009). Fighting Phishing With Discriminative Keypoint Features. *Internet Computing, IEEE*, 13 (3) 56-63.

[35] Chen, X., Bose, I., Leung, A. C. M., Guo, C. (2010). Assessing the severity of phishing attacks: A hybrid data miningapproach. *Decision Support Systems*, 50 (4) 662-672, March.

[36] Chen, T.-C., Dick, S., Miller, J. (2010). Detecting visually similar Web pages: Application to phishing detection. *ACM Transactions on Internet Technology.* 10 (2), Article 5, 38.

[37] Chen, T.-C. (2011). Detecting Visually Similar Web Pages: Application To Phishing Detection. Unpublished doctoral dissertation, University Of Alberta, Canada.

[38] Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J. C. (2004). Client-side defense against web-based identity theft. *In*: Proceedings of the Network and Distributed System Security Symposium, NDSS 2004, San Diego, California, USA.

[39] Ciampa, M. D. (2008). The Impact Of Computer Security Policy Content Elements On Mitigating Phishing Attacks. Unpublished doctoral dissertation, Indiana State University, Indiana, United States.

[40] Comesongsri, V. (2010). Motivation For The Avoidance Of Phishing Threat. Unpublished doctoral dissertation, The University Of Memphis, Memphis, Tennessee, United States.

[41] Cormack, G. V. (2008). Email Spam Filtering: A Systematic Review. *Foundations and Trends in Information Retrieval*, 1 (4) 335-455.

[42] Davinson, N., Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behaviour*, 26, 1739-1747.

[43] Dhamija, R., Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. Symposium on Usable Privacy and Security (SOUPS) Pittsburgh, PA, USA, 77-88.

[44] Dhamija, R., Tygar, J. D. (2005a) Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks. *In:* Proceedings of the 2nd International Workshop on Human Interactive Proofs (HIP05), Lecture Notes in Computer Science, 3517, Human Interactive Proofs, 127-141.

[45] Dhamija, R., Tygar, J. D., Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI conference on Human Factors in computing systems, New York, NY, USA, ACM Press, 581-590.

[46] Dinna., N. M. M., Leau., Y. B., Habeeb., S. A. H., Yanti., A. S. (2007). Managing Legal, Consumers and Commerce Risks in Phishing. *In*: Proceedings of World Academy of Science Engineering and Technology, 26, 562-567.

[47] Dodge, R., Ragsdale, D. J., Reynolds, C. (2003). Organization and training of a cyber security team. *In:* 2003 IEEE International Conference on systems, Man and Cybernetics, 5, 4306–4311, October.

[48] Dodge, R., Hoffman, L., Rosenberg, T., Ragsdale, D. (2005). Exploring a national cyber security exercise for universities. *Security & Privacy, IEEE*, Sept.-Oct, 3 (5) 27 – 33.

[49] Dodge. R. C., Carver, C., Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26, 73-80.

[50] Dong, X., Clark, J. A., Jacob, J. L. (2010). Defending The Weakest Link: Phishing Websites Detection By Analysing User Behaviours. *Telecommunication Systems*, 45, 215–226.

[51] Downs, J. S., Holbrook, M. B., Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *In*: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, ACM Press, SOUPS'06, 149, 79-90.

[52] Downs, J. S., Holbrook, M. B., Cranor, L. F. (2007). Behavioral Response to Phishing. *In*: Proceedings of the 2007 e- Crime Researchers summit, New York, NY, USA, ACM Press, 37-44.

[53] Egelman, S., Cranor, L. F., Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *In*: CHI '08: Proceeding of the twentysixth annual SIGCHI conference on Human factors in computing systems, New York, NY, USA, ACM, 1065-1074.

[54] Eisen, O. (2009). In-Session Phishing And Knowing Your Enemy. *Network Security*, 3, March, 8-11.

[55] Eisenstein, E. M. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, 61 (11) November, 1160-1172.

[56] Emigh, A. (2005). Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. *In*: ITTC Report on Online Identity Theft Technology and Countermeasures. November. http://www.antiphishing.org/Phishing-dhsreport.pdf

[57] Emm, D. (2006). Phishing update, and how to avoid getting hooked. *Network Security*. 8, August, 13–15.

[58] Featherman, M. S., Miyazaki, A. D., Sprott, D. E. (2010).Reducing online privacy risk to facilitate e-service adoption:the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24 (3) 219 -229.

[59] Felegyhazi, M., Kreibich, C., Paxson, V. (2010). On the potential of proactive domain blacklisting. *In*: Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more, San Jose,California.

[60] Fette, I., Sadeh, N., Tomasic, A. (2007). Learning to detect phishing emails. *In*: Proceedings of the 16th International Conference on World Wide Web, Banff, Alberta, Canada, ACM.

[61] Florencio, D., Herley, C. (2007). A Large-Scale Study of Web Password Habits. *In*: Proceeding of the WWW, Banff, Alberta, Canada, ACM.

[62] Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., Shon, J., Swani S., Treinen, A. (2001). What makes Web sites credible?: a report on a large quantitative study, *In*: Proceedings of the SIGCHI conference on Human factors in computing systems, March, Seattle, Washington, United States, 61-68.

[63] Forte, D. (2009). Anatomy of a phishing attack: A high-level overview. Network Security, April, 17 – 19.

[64] Fu, A. Y. (2006). Web Identity Security: Advanced Phishing Attacks And Counter Measures. Unpublished doctoral dissertation, City University Of Hong Kong, Hong Kong.

[65] Fu, A. Y., Wenyin, L., Deng, X. (2006a). Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Movers Distance (EMD), *Dependable and Secure Computing, IEEE Transactions on*, 3 (4), 301 -311.

[66] Furnell, M. (2004). Getting caught in the phishing net. *Network Security,* Issue 5, May 2004, 14-18.

[67] Furnell, S. (2004a). E-Commerce Security: A Question Of Trust. *Computer Fraud & Security,* 10, October, 10-14.

[68] Furnell, S. M. (2007). Phishing: can we spot the signs?. *Computer Fraud & Security*, 3, 10 – 15.

[69] Furnell, S. (2008). It's a jungle out there: Predators, prey and protection in the online wilderness. *Computer Fraud & Security*, 10, October, 3-6.

[70] Furnell, S. M. (2009). The irreversible march of technology. Information Security Technical Report, 14, 176 – 180.

[71] Garfinkel, S.L., Margrave, D., Schiller, J. I., Nordlander, E. and Miller, R.C. (2005). How to Make Secure E-mail Easier to User. Proceedings of the ACM Conference on Human Factors in Computing Systems. SIGCHI 2005, Portland, OR, USA, p. 701-710.

[72] Gartner (2010), Gartner News Room; Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008. November, http://www.gartner.com/it/page.jsp?id=936913.

[73] Goring, S. P., Rabaiotti, J. R., Jones, A. J. (2007). Anti-keylogging measures for secure Internet login: An example of the law of unintended consequences. *Computers & Security,* 26, 421-426.

[74] Gorling, S. (2007). An Overview Of The Sender Policy Framework (SPF) As An Anti-Phishing Mechanism. Internet Research, 17 (2) 169-179.

[75] Gouda, M. G., Liu, A. L., Leung, L. M., Alam, M. A. (2007). SPP: An anti-phishing single password protocol. *Computer Networks*, 51 (13) 3715-3726, September.

[76] Granova, A., Eloff, JHP. (2005). A Legal overview of Phishing. *Computer Fraud & Security*, 7, 6-7.

[77] Green, B. N., Johnson, C. D., Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: secrets of the trade. *Journal of Chiropractic Medicine*, National University of Health Sciences, Fall, 3 (5), 101 - 117.

[78] Griffin, S. E.,Rackley, C. C. (2008). Vishing. InfoSecCD '08: *In*: Proceedings of the 5th annual conference on Information Security Curriculum Development. September 26-27, Kennesaw, GA, USA.

[79] Halderman, J. A., Waters, B., Felten, E.W. (2005). A convenient method for securely managing passwords. *In*: Proceedings of the International World Wide Web Conference (WWW), 471–479.

[80] He, M., Horng, S., Fan, P., Khan, M.K., Run, R., Lai, J., Chen, R., Sutanto, A. (2011). An efficient phishing webpage detector. *Expert Systems with Applications*, 38 (10) 12018-12027.

[81] Herley, C., Florencio, D. (2008). A profitless endeavor: phishing as tragedy of the commons. *In*: Proceedings of the 2008 workshop on New security paradigms, New York, NY, USA, ACM, 59-70.

[82] Herley, C., Oorschot, P. C. V., Patrick, A. S. (2009). Passwords: If We'Re So Smart, Why Are We Still Using Them?. Lecture Notes in Computer Science, 5628, Financial Cryptography and Data Security, 230-237.

[83] Herzberg, A., Jbara, A. (2008). Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks. *ACM Transactions on Internet Technology,* 8 (4), Article 16.

[84] Herzberg, A. (2009a). Why Johnny can't surf (safely)? Attacks and defenses for web users. *Computer & Security,* 28, 63-71.

[85] Herzberg, A. (2009b). DNS-based email sender authentication mechanisms: A critical review. *Computer & Security,* 28,731-742.

[86] Hinde, S. (2004). All you need to be a phisherman is patience and a worm, *Computer Fraud & Security*, 3, March, 4-6.

[87] Hunter, P. (2006). IT security highlights – the day of the amateur hacker has gone, but there are still plenty of amateur users. *Computer Fraud & Security,* 1, 13-17.

[88] Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. (2007). Social phishing. *Communications of the ACM* 50,10 (October), 94–100.

[89] Jakobsson, M., Ratkiewicz, J. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features. *In*: Proceedings of the 15th international conference on World Wide Web, May 23-26, Edinburgh, Scotland.

[90] Jakobsson, M., Tsow, A., Shah, A., Blevis, E., Lim, Y. K. (2007). What instills trust? A qualitative study of phishing. Lecture Notes in Computer Science, 4886, Springer Verlag (Germany) 2007-02, 356-361.

[91] Jali, M. Z., Furnell, S. M., Dowland, P. S. (2010). Assessing Image-Based Authentication Techniques *In*: A Web-Based Environment. *Information Management & Computer Security*, 18 (1) 43-53.

[92] James, L. (2006). Phishing exposed. Tech target article sponsored by: Sunbelt software. Available from searchexchange.com.

[93] Jammalamadaka, R. C., Mehrotra, S., Venkatasubramanian, N. (2005). Pvault: A Client Server System Providing Mobile Access to Personal Data. *In*: Proceedings of the 2005 ACM International Workshop on Storage Security and Survivability. StorageSS , Fairfax, VA, USA, 123-129.

[94] Jendricke, U., Markotten, D. G. (2000). Usability meets security - the Identity-Manager as your personal security assistant for the Internet. *In*: Proceedings of the 16th Annual Computer Security Applications Conference, 344-353.

[95] Jung, J. and Sit, E. (2004). An empirical study of spam traffic and the use of DNS black lists. *In*: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, Taormina, Sicily, Italy, 370-375.

[96] Karlof, C. K. (2009). Human Factors In Web Authentication. Unpublished doctoral dissertation, University Of California, Berkeley, United States.

[97] Kim, W., Jeong, O., Kim, C. and So, J. (2011). The Dark Side Of The Internet: Attacks, Costs And Responses. *Information Systems*, 36 (3) 675-705.

[98] Kirda, E., Kruegel, C. (2005). Protecting Users against Phishing Attacks with AntiPhish. *In*: Proceedings of the 29th Annual International Conference on Computer Software and Applications. COMPSAC, Edinburgh, Scotland, 517-524.

[99] Kirda, E., Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, 49 (5) 554–561.

[100] Knight, W. (2004). Goin Phishing. *Infosecurity Today*, 1 (4), 36-38, July-August.

[101] Knight, W. (2005). Caught in the Net. *IEEE Review*. 51 (7) 26-30.

[102] Kruck, G. P., Kruck, S. E. (2006). Spoofing - A Look At An Evolving Threat. The Journal of Computer Information Systems. Fall 2006, 47 (1) 95-100.

[103] Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., Nunge., E. (2007a). Protecting People from Phishing:The Design and Evaluation of an Embedded Training Email System. *In*: CHI '07: Proceedings of the SIGCHI conferenceon Human factors in computing systems, 905–914.

[104] Kumaraguru, P., Rhee, Y., Hasan, S., Acquisti, A., Cranor, L., Hong, J. (2007b). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *In*: Proceedings of the APWG 2nd annual eCrime Researchers Summit, Pittusburgh, PA, USA, 70-81.

[105] Kumaraguru, P., Sheng. S., Acuisti, A., Cranor. L., Hong. J. (2008). Lessons from a real world evaluation of antiphishing training. e-Crime Researchers Summit,Anti-Phishing Working Group, Atlanta, GA, 1-12.

[106] Kumaraguru, P. (2009). Phishguru: A System For Educating Users About Semantic Attacks. Unpublished doctoral dissertation, Carnegie Mellon University, Pittsburgh, United States.

[107] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, A. B., Pham, T. (2009a). School of phish: a real-world evaluation of anti-phishing training. *In*: Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, California, USA.

[108] Kumaraguru, P., Sheng. S., Acuisti. A., Cranor. L. F., Hong. J. (2010). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*, 10 (2), Article 7.

[109] Lai, F., Li, D., Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52 (2) 353-363, January, .

[110] Langheinrich, M., Karjoth, G. (2010). Social Networking And The Risk To Companies And Institutions. *Information Security Technical Report*, 15 (2) 51-56, May.

[111] Larcom, G., Elbirt, A. J. (2006). Gone Phishing, *IEEE Technology and Society Magazine*. , 25(3) 52-55.

[112] Larson, J. S. (2010). Enforcing Intellectual Property Rights to Deter Phishing. *Intellectual Property & Technology Law Journal*, 22 (I) 1-8.

[113] Leiba, B., Borenstein, N. S. (2004). A multifaceted approach to spam reduction. *In*:Proceedings of CEAS 2004, first Conference on Email and Anti-Spam.

[114] Leung, C. M. (2009a). Visual security is feeble for anti-phishing. *In*: Proceedings of the 3rd International Conference on Anti-Counterfeiting, security, and identification in communication, 118-123.

[115] Leung, C.M. (2009b). Depress Phishing by CAPTCHA with OTP. *In*: Proceedings of the 3rd international conference on Anti-Counterfeiting, security, and identification in communication, 187-192.

[116] Levy, Y., Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science Journal*, 9, 181-212.

[117] Lewis, J. L. (2011). Exploring The Identity-Theft Prevention Efforts Of Consumers, *In*: The United States. Unpublished doctoral dissertation, Northcentral University, Arizona, United States.

[118] Li, L., Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology*, 3 (2) 163-184.

[119] Liao, Q., Luo, X. (2004).The Phishing Hook: Issues And Reality. *Journal of Internet Banking and Commerce*, December, 10 (3).

[120] Liu, W., Deng, X., Huang, G., Fu, A. Y. (2006). An Antiphishing Strategy Based On Visual Similarity Assessment. *Internet Computing, IEEE*, 10 (2), 58-65.

[121] Lovet, G. (2009). Fighting Cybercrime: Technical, Juridical and Ethical Challenges. *In*: Proceedings of the Virus Bulletin Conference, 63-76.

[122] Lu, H., Hsu, C., Hsu, H. (2005). An empirical study of the effect of perceived risk upon intention to use online applications. *Information Management & Computer Security*, 13 (2) 106-120.

[123] Lungu, I., Tabusca, A. (2010). Optimising Anti-Phishing solutions based on User Awareness, Education and the use of the Latest Web Security Solutions. *Informatica Economica Journal*. 14 (2) 27-36.

[124] Lynch, J. (2005). Identity Theft In Cyberspace: Crime Control Methods And Their Effectiveness *In*: Combating Phishing Attacks. *Berkeley Technology Law Journal*, 20 (259).

[125] Ma, J., Nickerson, J. V. (2006). Hands-on, simulated, and remote laboratories: a comparative literature review. *ACM Computing Surveys*, 38 (3) Publication date: September.

[126] Ma, J., Saul, L. K., Savage, S., Voelker, G. M. (2009). Beyond blacklists: learning to detect malicious web sites from suspicious URLs. *In*: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining, Paris, France, 1245 – 1253.

[127] Mannan, M., Oorschot, P. C. V. (2007). Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. Lecture Notes in Computer Science, 4886, Financial Cryptography and Data Security, 88-103.

[128] Marshall, A. M., Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law & Security Review*, 21(2) 128-137

[129] Martin, T. D. (2008). Phishing For Answers: Exploring The Factors That Influence A Participant'S Ability To Correctly Identify Email. Unpublished doctoral dissertation, Capella University, Minneapolis, United States.

[130] Martino. A. S., Perramon, X. (2010). Phishing Secrets: History, Effects, And Countermeasures. *International Journal of Network Security*, 11 (3) 163-171.

[131] McGrath, D. K., Kalafut, A., Gupta, M. (2009). Phishing Infrastructure Fluxes All The Way. *Security & Privacy, IEEE*, 7 (5) 21 – 28.

[132] Mcnealy, J. (2008). Angling for Phishers: Legislative Responses to Deceptive E-Mail. *Communication Law and Policy*,13 (2), Taylor & Francis, USA, 275-300.

[133] Medvet, E., Kirda, E., Kruegel, C. (2008). Visual-Similarity-Based Phishing Detection. *In*: Proceedings of the 4th international conference on Security and privacy in communication networks, Istanbul, Turkey.

[134] Mercuri, R. T. (2006). Scoping Identity Theft. *Communications of the ACM*, 49 (5) 17-21.

[135] Mizuno, S., Yamada, K., Takahashi, K. (2005). Authentication Using Multiple Communication Channels. *In*: Proceedings of the 2005 ACM Workshop on Digital Identity Management. DIM 2005, Fairfax, VA, USA, 4-62.

[136] Molloy, I., Li, N. (2011), Attack on the GridCode one-time password. ASIACCS '11. *In*: Proceedings of the 6th ACM Symposium on Information, *Computer and Communications Security*, Hong Kong, China, 306 -315.

[137] Moore, T., Clayton. R. (2007). Examining the Impact of Website Take-down on Phishing. *In*: Proceedings of the antiphishing working groups 2nd annual eCrime researchers summit, New York, NY, USA, ACM Press, 1-13.

[138] Moore, T., Clayton. R. (2008). Evaluating The Wisdom Of Crowds In Assessing Phishing Websites. FinancialCryptography and Data Security (FC), LNCS 5143, 16–30.

[139] Murphy, J. M. (2005). The Water Is Wide: Network Security at Kenyon College, 1995-2005. *In*: Proceedings of the 33rd Annual ACM Conference on User Services. SIGUCCS, Monterey, CA, USA, 237-240.

[140] Nilsson, M., Adams, A.,Herd, S. (2005). Building Security and Trust in Online Banking, in Extended Abstracts of the *ACM Conference on Human Factors in Computing Systems*. SIGCHI 2005, Portland, OR, USA, 1701-1704.

[141] Nohlberg, M. (2008). Securing Information Assets: Understanding, Measuring And Protecting Against Social Engineering Attacks. Unpublished doctoral dissertation, Stockholm University, Sweden.

[142] Obied, A., Alhajj, R. (2009). Fraudulent And Malicious Sites On The Web. *Applied Intelligence*, 30 (2) 112-120.

[143] Olivo, K. C., Santin, A. O. Oliveira, L.S. (2011). Obtaining The Threat Model For E-Mail Phishing. *Applied Soft Computing*, *In*: Press, Corrected Proof, Available online 8 July.

[144] Oppliger, R., Hauser, R., Basin, D. (2006).SSL/TLS session-aware user authentication – or how to effectively thwart the man-inthe-middle. *Computer Communications* August, 29 (12) 2238–2246.

[145] Oppliger, R., Hauser, R., Basin, D., Rodenhaeuser, A., Kaiser, B. (2007). A proof of concept implementation of SSL/TLS session-aware user authentication. *In*: Proceedings of the 15th GI/ITG conference on, *Kommunikation in Verteilten Systemen*. KiVS '07, Berne, Switzerland. LNCS. Springer-Verlag, 225–236.

[146] Oppliger, R., Hauser, R., Basin, D. (2008a). 'SSL/TLS session-aware user authentication. *IEEE Computer* 41 (3) 59–65.

[147] Oppliger, R., Hauser, R. (2008b). Protecting TLS-SA implementations for the challenge-response feature of EMVCAP against challenge collision attacks. *Security and Communication Networks*,1 (2) 125–134.

[148] Oppliger, R., Hauser, R., Basin, D. (2008c). SSL/TLS session-aware user authentication revisited. *Computers & Security*, 27, 64-70.

[149] Parno, B., Kuo, C., Perrig, A. (2006). Phoolproof Phishing Prevention. Financial Cryptography and Data Security Lecture Notes in Computer Science, 4107, 1 -19.

[150] Pfleeger, S. L., Bloom, G. (2005). Canning Spam: Proposed Solutions to Unwanted Email. *Security & Privacy Magazine*, *IEEE*, 3 (2) 40-47.

[151] PhishTank (2010), November, http://www.phishtank.com/stats/2010/10/

[152] Plossl, K., Federrath, H., Nowey, T. (2005). Protection Mechanism Against Phishing Attacks. Lecture Notes in Computer Science, 3592, Trust, Privacy, and Security in Digital Business, 20-29.

[153] Prakash, P., Kumar, M., Kompella, R. R., Gupta, M. (2010). Phishnet: predictive blacklisting to detect phishing attacks. *In*: Proceedings of the 29th Conference on Information Communications, San Diego, California, USA, 346-350.

[154] Reed, L. E. (1998). Performing a Literature Review. Frontiers in Education Conference, FIE '98. 28th Annual, 1, 380 - 383.

[155] Rigoutsos, I., Huynh, T. (2004). Chung-Kwei: a pattern-discovery-based system for the automatic identification of unsolicited e-mail messages (SPAM). *In*: Proceedings of the First Conference on E-mail and Anti-Spam.

[156] Robila, S. A., Ragucci, J. W. (2006). Don't be a phish: steps in user education. *In*: ITICSE '06: Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education. ACM Press, New York,NY, USA, 237–241.

[157] Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J. C. (2005). Stronger password authentication using browser extensions. Proceedings of the USENIX Security Symposium, 17–32.

[158] Rusch, J. J. (2005). The compleat cyber-angler: a guide to phishing. *Computer Fraud & Security*, 1, January, 4-6.

[159] Saberi, A., Vahidi, M., Bidgoli, B. M. (2007). Learn to Detect Phishing Scams Using Learning and Ensemble Methods. *In*: Proceedings of the 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops, 311-314.

[160] Sahami, M., Dumais, S., Heckerman, D., Horvitz, E. (1998). A bayesian approach to filtering junk e-mail. AAAI Workshop on Learning for Text Categorization, Madison, Wisconsin, USA.

[161] Saklikar, S., Saha, S. (2008). Public Key-Embedded Graphic CAPTCHAs. *In*: Proceedings of the Consumer Communications and Networking Conference, (CCNC 2008), 262-266.

[162] Sarel, D., Marmorstein, H. (2006) Addressing Consumers Concerns About Online Security: A Conceptual And Emperical Analisys Of Banks Actions. *Journal of Financial Services Marketing*, 11 (2) 99–115.

[163] Savirimuthu, J. (2008). Identity Theft and the Gullible Computer User: What Sun Tzu in The Art of War Might Teach. *Journal of International Commercial Law and Technology*, 3 (2) 120-128.

[164] Schechter, S. E., Dhamija, R., Ozment, A., Fischer, I. (2007). The emperor's new security indicators. SP '07 *In*: Proceedings of the 2007 IEEE Symposium on Security and Privacy, 51-65.

[165] Segal, R., Crawford, J., Kephart, J., Leiba, B. (2004). SpamGuru: An Enterprise Anti-Spam Filtering System. *In*: Proceedings of the First Conference on E-mail and Anti-Spam.

[166] Sengar, P. K. and Kumar, V. (2010). Client-Side Defense Against Phishing With Pagesafe. *International Journal of Computer Applications*, 4 (4) - Article 2, 6 -10.

[167] Shein, E. (2011). The Gods Of Phishing. *Infosecurity*, 8 (2), March–April, 28-31.

[168] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In SOUPS '07: *In*: Proceedings of the 3rd symposium on Usable privacy and security, New York, NY, USA, ACM, 88-99.

[169] Sheng, X. (2009). A Policy Analysis Of Phishing Countermeasures. Unpublished doctoral dissertation, Carnegie Mellon University, Pittsburgh, United States.

[170] Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., Zhang, C. (2009a). An Empirical Analysis of Phishing Blacklists, *In*: Proceedings of CEAS'09, Mountain View, CA, USA.

[171] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *In*: Proceedings of the 28th International Conference on Human factors in computing systems, CHI 2010, Atlanta, Georgia, USA, 373-382.

[172] Singleton, T. (2005). Don't Get 'Hooked' by Phishing Scams. *The Journal of Corporate Accounting & Finance*. Wiley Periodicals, 21-28.

[173] Singleton, T., Singleton, A., Gottlieb, G. (2006). Cyberthreats Facing The Banking Industry. Bank Accounting & Finance, February, 26-32.

[174] Smedinghoff, T. J. (2005). Phishing: The Legal Challenges For Business. Banking & Financial Services Policy Report. 24 (4).

[175] Soman, C., Pathak, H., Shah, V., Padhye, A. and Inamdar, A. (2008). An Intelligent System for Phish Detection, using Dynamic Analysis and Template Matching. World Academy of Science, Engineering and Technology, Issue 42, 321-327.

[176] Srikwan, S., Jakobsson, M. (2008). Using Cartoons to Teach Internet Security. *Cryptologia*, 32 (2), 137-154.

[177] Stamm, S. L. (2009). Anticipating And Hardening The Web Against Socio-Technical Security Attacks. Unpublished doctoral dissertation, Indiana University, Bloomington, United States.

[178] Steel, C. M. S., Lu, C. (2008). Impersonator identification through dynamic fingerprinting. *Digital Investigation*, 5 (1-2), September, 60-70.

[179] Sullins, L. L. (2006). Phishing For A Solutions: Domestic And International Approaches To Decreasing Online Identity Theft. *Emory International Law Review*, 20, 397-433.

[180] Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H. R. (2011). Why Do People Get Phished? Testing Individual Differences In Phishing Vulnerability Within An Integrated, Information Processing Model. *Decision Support Systems*, 51 (3), June, 576-586.

[181] Wang, J., Chen, R., Herath, T., Rao, H. R. (2009). Visual E-Mail Authentication And Identification Services: An Investigation Of The Effects On E-Mail Use, *Decision Support Systems*, 48 (1) 92-102, December.

[182] Webster, J., Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MISQuarterly*, 26 (2).

[183] Wenyin, L., Huang, G. Xiaoyue, L. Min, Z., Deng, X. (2005). Detection of phishing webpages based on visual similarity. *In*: 14th International Conference on World Wide Web (WWW), ACM Press, 1060 -1061.

[184] Wilson, P. (2004). Tips To Stop Your Users From Being Phished. *Network Security* (9), September, 5-9.

[185] Workman, M. (2008). Wisecrackers: A Theory-Grounded Investigation Of Phishing And Pretext Social Engineering Threats To Information Security. *Journal of the American Society for Information Science and Technology*, Wiley Periodicals, 59 (4) 662–674.

[186] Wright, R., Chakraborty, S., Basoglu, A., Marett, K. (2010). Where Did They Go Right? Understanding The Deception In Phishing Communications. *Group Decision and Negotiation*, 19 (4) 391-416.

[187] Wright, R. T., Marett, K. (2010a). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*. 27 (1) 273 – 303.

[188] Wu, M. (2006). Fighting Phishing At The User Interface. Unpublished doctoral dissertation, Massachusetts Institute Of Technology, United States.

[189] Wu, M., Miller, R. C.,Garfinkel, S. L. (2006a). Do security toolbars actually prevent phishing attacks?. *In*: CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems, New York, NY, USA, ACM Press,601-610.

[190] Wu, M., Miller, R. C., Little, G. (2006b). Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. *In*: SOUPS '06: *In*: Proceedings of the second symposium on Usable privacy and security, Pittsburgh, PA, USA, 102-113.

[191] Xiang, G., Hong, J., Rose, C. P., Cranor, L. (2011). CANTINA+: A feature-rich machine learning framework for detecting phishing Web sites. *ACM Transactions on Information and System Security* (TISSEC), 14 (2), Article 21.

[192] Yang, S. S., Choi, H. (2010). Vulnerability analysis and the practical implications of a server-challenge-based onetime password system. *Information Management & Computer Security*, 18 (2) 86-100.

[193] Ye, Z., Smith, S., Anthony, D. (2005). Trusted Paths for Browsers. *ACM Transactions on Information and System Security*, 8 (2) 153–186, May.

[194] Yee, K. P., Sitaker, K. (2006). Passpet: Convenient Password Management and Phishing Protection. *In*: SOUPS '06:Proceedings of the second symposium on Usable privacy and security, Pittsburgh, PA, USA, 32-43.

[195] Yue, C., Wang, H. (2008). Anti-phishing in offense and defense. *In*: Proceedings of the Annual Computer Security Applications Conference (ACSAC), 345 -354.

[196] Yue, C. (2010). Enhancing Web Browsing Security. Unpublished doctoral dissertation, The College Of William And Mary,Williamsburg, Va, United States.

[197] Yue, C., Wang, H. (2010a). BogusBiter: A Transparent Protection Against Phishing Attacks. *ACM Transactions on Internet Technology*, 10 (2) 1-31, Article 6.

[198] Zhang, H., Liu. G., Chow, T. W. S., Liu, W. (2011). Textual And Visual Content-Based Anti-Phishing: A Bayesian Approach. *Neural Networks, IEEE Transactions on* 22 (10) 1532-1546.

[199] Zhang, Y., Egelman, S., Cranor, L. and Hong, J. (2007). Phinding Phish: An Evaluation of Anti-Phishing Tools. *In*: Proceedings of the ISOC Symposium on Network and Distributed System Security, Internet Society.

[200] Zhang, J., Porras, P., Ullrich, J. (2008). Highly predictive blacklisting. *In*: Proceedings of the 17th Conference on Security symposium, San Jose, CA, 107-122.

[201] Zviran, M., Erlich., Z. (2006). Identification and Authentication: Technology and Implementation Issues. *Communications of AIS*. 17 (4) 90-105.

The way that sales effectiveness is measured can vary by company or sales organization depending on which sales metrics are the most important to them. Some other ways to measure sales effectiveness include: Individual quota attainment.Â Review their approach. Are they personalizing their outreach? Using multiple channels (email, calls, voicemail, social media, etc.)? Soundly assessing the effectiveness of these embedded phishing exercises is a challenging problem. 1Only one of these companies provided us with data from their phishing exercise. 2These emails are whitelisted to reduce the likelihood of reused test phishing emails being ltered.Â Embedded phishing exer-cise is well received by companies for training as well as measuring the resiliency of their employees against these attacks. Previous works are limited in measuring the effect of phishing training because of the small sample size, as well as the number of rounds in the exercise, and the types of phishing emails used in experiments. Available methodologies and their relevance for the sector. FAO Fisheries and aquaculture. Technical paper.Â This review builds on previous work and reviews of vulnerability concepts and approaches for assessments. It is based on extensive searches of the published and grey literature.Â The document starts with a review of concepts to help understand what vulnerability is and how it can be studied (Chapter 2). Chapter 3 provides information on available methodologies to measure and evaluate vulnerability. Their application in the context of fisheries and aquaculture is detailed in Chapter 4. Chapter 5 proposes a series of practical steps to assess vulnerability in the sector. Measures of Effectiveness (MOEs) assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. They do not measure task performance. When evaluating a course of action or combat assessment we need to evaluate it based on the impact or MOE it will have. These MOEs should use assessment metrics that are relevant, measurable, responsive, and resourced so there is no false impression of task or objective accomplishment [33]. This can be very complex if we are talking about i COUNTER MEASURES. Anti-phishing filters already exist and. integrated into web browsers.Â We discuss the importance of understanding psychological aspects of phishing, and review some recent findings. Given these findings, we critique some commonly used security prac-tices and suggest and review alternatives, including educational approaches. We suggest a few techniques that can be used to assess and remedy threats remotely, without requiring any user involvement. We conclude by discussing some approaches to anticipate the next wave of threats, based both on psychological and technical insights.