Tutorial and Critical Analysis of Phishing Websites Methods

Rami M. Mohammad
School of Computing and Engineering
University of Huddersfield
Huddersfield, UK.
rami.mohammad@hud.ac.uk

Fadi Thabtah
E-Business Department
Canadian University of Dubai
Dubai, UAE.
fadi@cud.ac.ae

Lee McCluskey
School of Computing and Engineering
University of Huddersfield
Huddersfield, UK.
t.l.mccluskey@hud.ac.uk

1. ABSTRACT

The Internet has become an essential component of our everyday social and financial activities. Internet is not important for individual users only but also for organizations, because organizations that offer online trading can achieve a competitive edge by serving worldwide clients. Internet facilitates reaching customers all over the globe without any market place restrictions and with effective use of e-commerce. As a result, the number of customers who rely on the Internet to perform procurements is increasing dramatically. Hundreds of millions of dollars are transferred through the Internet every day. This amount of money was tempting the fraudsters to carry out their fraudulent operations. Hence, Internet users may be vulnerable to different types of web threats, which may cause financial damages, identity theft, loss of private information, brand reputation damage and loss of customers' confidence in e-commerce and online banking. Therefore, suitability of the Internet for commercial transactions becomes doubtful. Phishing is considered a form of web threats that is defined as the art of impersonating a website of an honest enterprise aiming to obtain user's confidential credentials such as usernames, passwords and social security numbers. In this article, the phishing phenomena will be discussed in detail. In addition, we present a survey of the state of the art research on such attack. Moreover, we aim to recognize the up-to-date developments in phishing and its precautionary measures and provide a comprehensive study and evaluation of these researches to realize the gap that is still predominating in this area. This research will mostly focus on the web based phishing detection methods rather than email based detection methods.

2. INTRODUCTION

Although phishing is a relatively new web-threat, it has a massive impact on the commercial and online transaction sectors. Presumably, phishing websites have high visual similarities to the legitimate ones in an attempt to defraud the honest people. Social engineering and technical tricks are commonly combined together in order to start a phishing attack. Typically, a phishing attack starts by sending an e-mail that seems authentic to potential victims urging them to update or validate their information by following a URL link within the e-mail. Predicting and stopping phishing attack is a critical step toward protecting online transactions. Several approaches were proposed to mitigate these attacks. Nonetheless, phishing websites are expected to be more sophisticated in the future. Therefore, a promising solution that must be improved constantly is needed to keep pace with this continuous evolution. Anti-phishing measures may take several forms including: legal, education and technical solutions. To date, there is no complete solution able to capture every phishing attack. The Internet community has put in a considerable amount of effort into defensive techniques against phishing. However, the problem is continuously evolving and ever more complicated deceptive methods to obtain sensitive information and perform e-crimes on the Internet are appearing. Anti-phishing tools, or sometimes so called fighting phishing tools, are employed to protect users from posting their information through a forged website. Recognizing phishing websites accurately and within a passable timescale as well as providing a good warning technique reflect how good an anti-phishing tool is. Designing a phishing websites has become much easier and much more sophisticated, and that was the motivation behind looking for an effective anti-phishing technique.

Mixed research methodology has been adopted in our study. Since some previous studies suggest applying protection mechanisms without offering clear experimental results. Hence, qualitative methodology is best fits such researches. On the other hand, some researches taking into consideration experimental analysis, data gathering techniques, testing measures and comparing results, thus it is worthy applying quantitative methodology in such cases.

This article is structured as follows: Section 3 discusses what phishing is and how it started. Section 4 introduces different phishing techniques. Section 5 describes the phishing websites life cycle. Section 6 discusses how and why people fall prey to phishing. Section 7 shows some phishing statistics. Section 8 describes phishing countermeasures. Section 9 introduces a detailed discussion of the up to date anti-phishing techniques. Section 10 compares between human and automatic based protection. Finally, we summarize in Section 11.

3. THE STORY OF PHISHING

Deceiving users into giving their passwords or other private information has a long tradition in the cybercrime community. In the early 90's, with the growing popularity of the Internet, we have witnessed the birth of a new type of cybercrime; that is phishing. In 1987 a detailed description of phishing was introduced, and the first recorded attack was in 1995 (James 2005).

In the early age of phishing; phishers mainly designed their attacks to deceive English-speaking users. Today, phishers broaden their attack to cover users and businesses all over the globe (Sullins 2006). At the beginning, phishers acted individually or in small and simple groups.

Usually, phishing is accomplished through the practice of social engineering. An attacker may introduce himself as a humble and respectable person claiming to be new at the job, a helpdesk person or a researcher. An example of using social engineering is urgency; by asking the user to submit his information as soon as possible. Risk of terrible results if the user denies complying is another tactic used to start social phishing, for example warn the user that his account will be closed or the service will be terminated if he doesn't respond. However, some social engineering tactics promise big prizes by showing a message claiming that the user has won a big prize and to receive it he needs to submit his information. Nowadays, as monetary organizations have improved their online investments the economic benefit of obtaining online account information has become much larger. Thus, phishing attacks became more proficient, planned and efficient.

Phishing is an alternate of the word "fishing" (Oxford Dictionaries 1990) and it refers to bait used by phishers who are waiting for the victims to be bitten (James 2005). Surveys commonly depict early phishers as mischief-makers aiming to collect information to make long-distance phone calls (Watson, Holz and Mueller 2005); such attack was called "Phone Phreaking". This name was behind the origin of the "ph" replacement of the character 'f' in the word "fishing" (Oxford Dictionaries 1990).

Phishing websites are designed to give an impression that they came from a legitimate party with the aim to deceive users into divulging their personal information. The phishers may use this information for dishonest intentions, for instance money laundering or illegal online transactions.

While those phishers focus on individual customers, the organizations that phishers are mimicking are also victims because their brand and reputation is compromised.

There are several definitions of the term *“Phishing”*. To have a good understanding of phishing and their attacking strategies, several definitions will be discussed.

Some definitions believe that phishing demands sociological skills in combination with technical skills. As in the definition from the *“Anti-Phishing Working Group”* (APWG, Aaron and Manning 2014): *“A criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials”*. Another definition comes from (Ming and Chaobo 2006): *“A phishing website is a style of offence that network fishermen tempt victim with pseudo website to surrender important information voluntarily”*. A detailed description stated by (Kirda and Kruegel 2005) defines phishing as : *“creating a fake online company to impersonate a legitimate organization; and asking for personal information from unwary consumers depending on social skills and website deceiving methods to trick victims into disclosure of their personal information which is usually used in an illegal transaction”*. Some definitions assumed that the success of phishing websites depends on their ability to mimic a legitimate website, because most Internet-users, even those having a good expertise in Internet and information security, have a propensity to decide on a website’s validity based on its look-and-feel which might be orchestrated proficiently by phishers. An example of such definitions comes from (James 2005), who defines phishing as: *“Attempts to masquerade as a trustworthy entity in an electronic communication to trick recipients’ into divulging sensitive information such as bank account numbers, passwords, and credit card details”*. Since phishing websites request victims to submit their credentials through a webpage, it is necessary to convince these victims that they are dealing with an honest entity, so that a good definition was introduced by (Zhang, Hong and Cranor 2007) where they define phishing as: Phishing website satisfies the following criteria:

- Showing a high visual similarity.
- Containing at least one login form.

We may outline all previous definitions in one sentence: *"Phishing website is the practice of creating a copy of a legitimate website and use social skills to fool a victim into submitting his personal information"*.

4. PHISHING TECHNIQUES

Until recently, phishers relied heavily on spoofed emails to start phishing attacks by persuading the victims to reply with the desired information. These day's social networking websites are used to spread doubtful links to lure victims to visit phishing websites. A report published by (MessageLabs 2009) estimated that one phishing email occurs every 325.2 emails sent through their system every day. Microsoft Research (Florencio and Herley 2007) revealed that 0.4% of email receivers' were persecuted by phishing emails in 2007. A report published by (Symantec Corporation 2013) substantiate that the amount of phishing websites that mimic social networking websites rose by 12% in 2012. If phishers were able to acquire users' social media login information, they can send out phishing emails to all their friends using the breached account. An email that appears to be originated from a well-known person seems much more trustworthy. Moreover, phishers may send out fake emails to your friends using your account telling them that you face an emergent situation. For example, *"Help! I'm stuck overseas and my wallet has been stolen. Please send $200 as soon as possible"*. Nowadays, phishing websites have evolved rapidly, maybe at a faster pace than the counter measures. Compromised identifications and phishing toolkit are widely offered for sale on Internet black-markets at low prices (Franklin and Paxson 2007). These days, innovative phishing techniques are becoming more frequent, such as malware and Man-In-The-Middle attacks (MITM) (Keizer 2007).

Phishers use different tactics and strategies in designing phishing websites. These strategies can be categorised into three basic groups those are:

1. Mimicking attack: In this attack phishers typically send an email to victims asking them to confirm, update or validate their credentials by clicking on a URL link within the email which will redirect them to a phony webpage. Phishers pay careful attention to designing emails that will be sent to the victims using the same logos of the original website, or sometimes using a fake HTTPS protocol. This type of attack undermines the customer confidence in electronic trading.

2. Forward attack: This attack starts once a victim clicks on the link shown within an email. He then redirected to a website asking him to submit his personal information. This information sent to a hostile server, and the victim is then forwarded to the real website using MITM technique.
3. Pop-up attack: Another method used by MITM technique is urging victims to submit their information by means of well-designed pop-up window. The phishers persuade the victims that submitting their information through a pop-up window is considered more secure.

In order to accomplish their job, phishers use a set of intelligent tricks to give the impression to the victims that they are dealing with a legitimate website. Some of these tricks include using IP address in URL, adding a prefix and suffix to a domain name, hiding the true URL shown in the browser address bar, using a fake padlock-icon on the URL address bar and pretending that the SSL is enabled. These tricks make it difficult for the naïve user to distinguish a phishing website from a legitimate one.

Overall, one principle if committed by organizations and customers will guarantee the security of their information; that is: *"Organizations and consumers should be aware of phishing and anti-phishing methods and take safety measure"*. Theoretically, this principle is easy, but in practice, it is very difficult to implement since there are new phishing techniques appearing constantly.

5. PHISHING ATTACK LIFE CYCLE

To combat phishing, we need to thoroughly investigate the nuts and bolts of the phishing attack. Following, we will describe the phishing attack life cycle.

- Planning: Typically, phishers start planning for their attack by identifying their victims, the information to be achieved and which technique to use in the attack. The main aspect considered by the phishers to pick their targets is how to achieve the maximum profit at the lowest cost and least possible risk. A phisher might need to breach the employee list in an organization, the organization news from a social networking website or the organization calendar. Common social networking such as; email, Voice over IP (VoIP) and Instant Messaging (IM) are used to establish communication between the phisher and the potential victims.

A classic phishing attack consists of two components: a trustworthy-looking email and a fraudulent webpage. The phishing emails contents are commonly designed to confuse, upset or excite the recipient. A fraudulent webpage has the look-and-feel of a legitimate webpage that it impersonates, often having a similar logo to the legitimate company, layout, and other critical features.

A survey published in ACM magazine (Jagatic, et al. 2007) showed that Internet users were 4.5 times more likely to be victims of phishing if they received an invitation to visit a fake URL link from a person they knew. That explains why criminals target social networking websites. Efforts made by webmail providers in filtering phishing emails will decrease the extent of the problem and reduce the time needed to stop phishing attacks since they are the first point dealing with phishing emails. However, most webmail providers focus on filtering spam emails and they would be very happy if their spam filter catches phishing emails but without adding any phishing filters that may consume their resources. The main difference between spam emails and phishing emails is that, spam emails are annoying emails sent to advertise goods and services that have not been requested by the user. On the other hand, phishing emails are sent to get your personal information, which will be used later in fraud activities. The authors in (Chandrasekaran, Narayanan and Upadhyaya 2006) recommend stopping phishing attacks at this stage. The authors suggested dividing the email into several parts such as; subject line; email attachments and the salutation line in the email body. Then extracting some structural features from these parts and making some calculation to produce the final decision on the email legitimacy.

- Collection: As soon as the victim takes an action making him susceptible to an information theft, he is then urged to submit his credentials through a trustworthy-looking webpage. Normally, the fake website is hosted on a compromised server, which has been exploited by the phisher for this purpose. A recent survey (Aaron and Rasmussen 2010) revealed that 78% of the servers holding phishing websites are either hacked file transfer protocol (FTP) or comprised of software application susceptibilities. Sometimes, the phishers may use the free cloud applications such as Google spreadsheets in order to host their fake websites (Seltzer 2011). Nobody is going to block *"google.com"* or even *"spreadsheets.google.com"*, thus, not only naïve users will be deceived, but also expert users are less likely to block this website. In general, to reduce the possibility of being caught, phishers will exploit servers that have weak security or process loopholes operating from countries which have insufficient law enforcement resources (APWG 2003).

- Fraud: Finally, and once the phisher has achieved his goal, he then becomes involved in fraud by impersonating the victim. Sometimes, the information is sold on the Internet black-market.

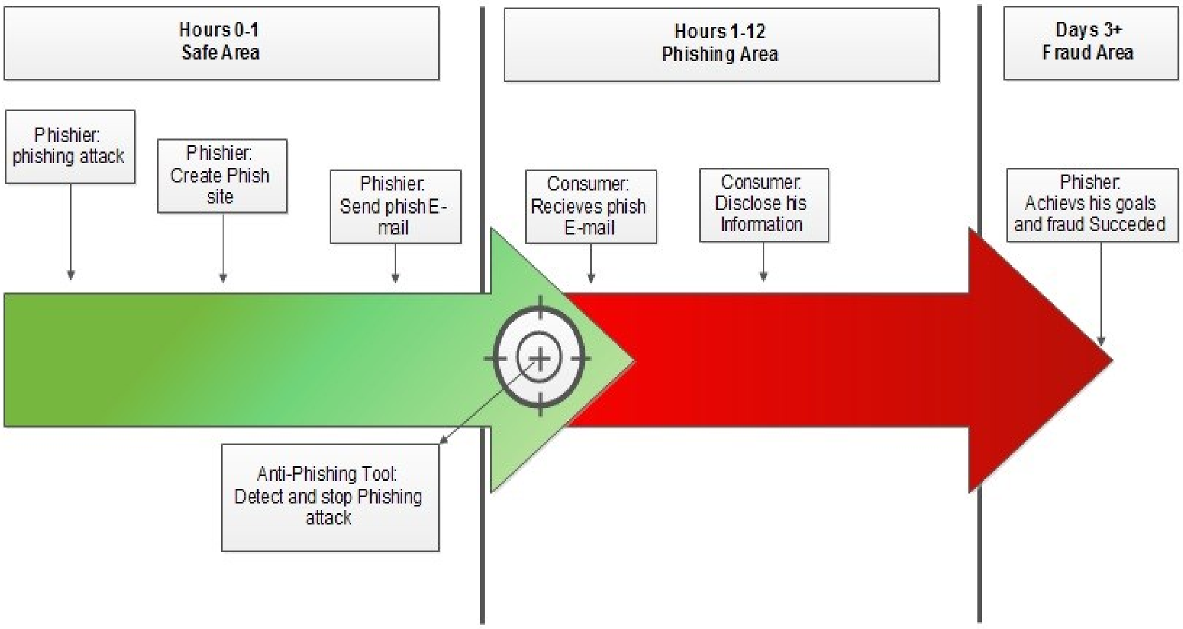
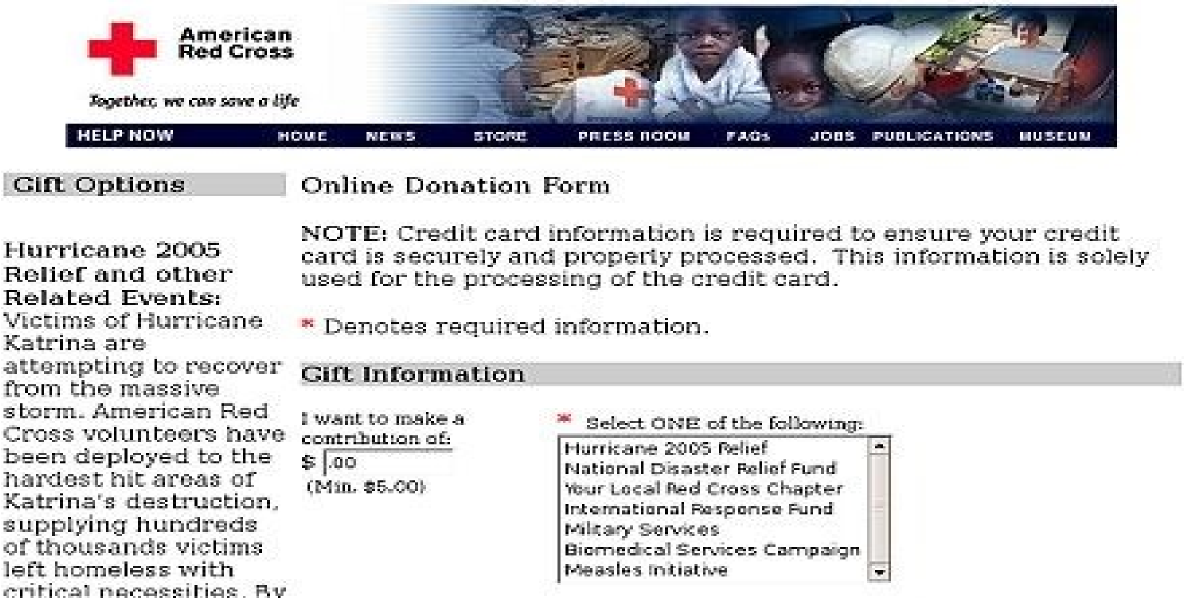

Hours 0-1
Safe Area
Hours 1-12
Phishing Area
Days 3+
Fraud Area
Phishier: phishing attack
Phishier: Create Phish site
Phishier: Send phish E-mail
Consumer: Recieves phish E-mail
Consumer: Disclose his Information
Phisher: Achievs his goals and fraud Succeded
Anti-Phishing Tool: Detect and stop Phishing attack

Fig.1 Phishing Websites Lifecycle

The amounts of activities that take place within the first few hours of a phishing life cycle are the most important aspect of any attack.

Once the phishing website has been created and the phishing email has been sent to consumers, the anti-phishing tool should detect and stop the phishing website before the consumer submits his information as shown in Figure 1. Seconds are important in this situation. Taking down the phishing website is the second line of defence. If we cannot stop the phishing attempt then the spoofed email could reach the victim's mailbox. An example of such an attack strategy happened when eBay costumers received an email claiming to be from the real eBay company asking customers to update their credentials so as not to freeze their accounts (BBC News 2005). The email contained a link that seemed to point to the real eBay's website. As soon as the user clicked on that link, he was then transferred to a webpage that asked for his credentials, including credit card number, expiry date and full name. The phishing website had been designed carefully in an attempt to convince the user that he was dealing with a legitimate website.

Some phishers stay up to date with the news and design their attacks in conjunction with specific approaching events or disasters. This is what happened during *"Hurricane Katrina"* (TREND MICRO 2013). Once the announcement of the hurricane was made, phishers initiated their attacks by registering domain-names which masqueraded as donation and victims-aid websites. Phishers sent fake emails masked as Katrina news updates with links directing users to fake websites hosted in the USA and Mexico, as shown in Figure 2.



Gift Options

Online Donation Form

Hurricane 2005 Relief and other Related Events: Victims of Hurricane Katrina are attempting to recover from the massive storm. American Red Cross volunteers have been deployed to the hardest hit areas of Katrina's destruction, supplying hundreds of thousands victims left homeless with critical necessities. By

NOTE: Credit card information is required to ensure your credit card is securely and properly processed. This information is solely used for the processing of the credit card.

* Denotes required information.

Gift Information

I want to make a contribution of:
$ .00
(Min. $5.00)

* Select ONE of the following:
Hurricane 2005 Relief
National Disaster Relief Fund
Your Local Red Cross Chapter
International Response Fund
Military Services
Biomedical Services Campaign
Measles Initiative

Fig.2 Fake Hurricane Katrina Donation Form

6. Why Fall Prey to Phishing?

Phishing is an example of a bigger category of web threats called semantic attacks. Instead of focusing on the technical vulnerabilities, semantic-attacks focus on how humans interact with computers or how they assign meanings to the message contents (Schneier 2000). A white paper published by Trend Micro (TREND MICRO 2013) which is a worldwide leader in cloud security shows that the victims need on average of about 600 hours to resolve the issue of identity theft. Commonly, users have a tendency to trust email messages and websites based on phony clues that in fact offer superficial trust information.

Several researches (Dhamija, Tygar and Hearst 2006) (Wu, Miller and Gar 2006) (Jakobsson 2007) (Julie S., Mandy and Cranor 2007) (Jagatic, et al. 2007) (Kumaraguru, et al. 2007) (Huang , et al. 2009) (Sheng, Holbrook, et al. 2010) Have revealed that users are susceptible to phishing for quite a lot of reasons among them:

1. Some people may lack essential knowledge of existing online threats.
2. Although some users may have a good understanding of what does computer viruses, hackers and fraud means, and how to protect themselves from these threats; they may not be familiar of what does phishing means. Therefore, they cannot generalize what they knew to unfamiliar threats.
3. Although some users are wary of falling prey to phishing, they have not developed good strategies for recognizing phishing attacks.
4. Users may focus on their main tasks, while paying attention to security clues is considered a secondary task.
5. Some users may ignore some essential security clues in the URL address bar such as the existence of HTTPS protocol, and as an alternative they used the website contents to decide whether the website is a phishing website or not.
6. Some users are unaware of what does SSL protocol and other security indicators mean.
7. Some users may not notice warning messages, while some other users may notice these messages but they expected that the warnings were invalid.
8. Internet users may lack how the organizations that offer online services are formally contacting their consumers in case of maintenance and information update issues.

7. PHISHING STATISTICS

A report disseminated by Anti-Phishing Working Group (APWG, Aaron and Manning 2014) which is a non-profit corporation established in 2003 focuses on reducing the frauds resulting from phishing, crime-ware and email deceiving, shows that 128,387 phishing websites were observed in the second quarter of 2014. This is the second highest number of phishing sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.

The total number of URLs used to host phishing attack increased to more than 175,000 hosts in the second quarter of 2014, while that number was less than 165,000 in the first quarter of the same year. The most affected countries were China with 51% followed by Peru and Turkey with 44%. USA continued the top hosting country of phishing websites. The number of targeted brands decreased to 531 in the second quarter of 2014 after reaching 557 brands in the first quarter of the same year. The average number of phishing URLs per brand decreased to 134 URLs after reaching 147 in the first quarter of the same year. The ratio of IP address based phishing URLs increased in the second quarter to 2.4%. Over 20,000 unique phishing emails were sent monthly during that period. The most industrial sector targeted by phishers was the payment services with 40%, followed by the financial sector with 20%, while the attacks against auctions websites increased from 2.3% in the first quarter to 2.6% in the second quarter. Expert phishers have moved from traditional phishing to a new style of malware attacks in this quarter.

However, Ihab Shraim, the president and Chief Technology Officer (CTO) at MarkMonitor (MarkMonitor 1999) said, *"It is unlikely that traditional phishing will stop since the cost of producing a phishing attack is almost insignificant"*. A survey disseminated by Gartner Inc (Gartner Inc. 2011) which is an advisory and research company, reveals that phishing websites continue to escalate and costs US financial sector an estimated $3.2 billion annually. The same survey estimated that 3.6 million victims fall in such attack. A poll of 2,000 US adults carried out by Harris Poll (2006) showed that 30% of those surveyed have limited their online transactions, and 24% have limited their e-banking transactions because of phishing.

8. PHISHING COUNTERMEASURES

7.1. LEGAL SOLUTIONS

Followed by many countries, the USA was the first to enact laws against phishing activities, and many phishers have been arrested and sued. Phishing has been added to the computer crime list for the first time on January 2004 by Federal Trade Commission (FTC), which is a US government agency aims to promote consumer protection. On May 10, 2006, the US president George W. Bush gave his orders to establish the President's Identity Theft Task Force (Executive Order 13402 2006) which aims to ensure that the efforts of federal authorities become more efficient and more effective in the area of identifying and preventing cybercrime attempts. On January 2005, the General Assembly of Virginia added phishing to its computer crimes act (General Assembly of Virginia 2005).

On March 2005, the Anti-Phishing Act was introduced in the US congress by Senator Patrick Leahy (Gross 2004).

In 2006, the UK government strengthened its legal arsenal against fraud by prohibiting the development of phishing websites and enacted penalties of up to 10 years.

In 2005, the Australian government signed a partnership with Microsoft to teach the law enforcement officials how to combat different cybercrimes. Several prosecutions have been made as in 2006; a Florida man has been indicted with development of a phishing website that aimed to take advantage of the victims of Hurricane Katrina (Leyden 2006).

In 2004, Zachary Keith Hill pleads guilty in Texas Federal Court to law breaking related to phishing activity and was penalized to 46 months (Goldman 2004). Although law enforcement officials successfully arrested, prosecuted and convicted phishers for the past few years (BBC News 2005) (TREND MICRO 2013) criminal act does a poor job of preventing phishing since it is hard to trace phishers. Moreover, phishing attacks can be performed quickly and later the phisher may disappear into cyberspace. Therefore, law enforcement authorities must behave quickly because on average the phishing website lives for 54 hours only (Dhamija, Tygar and Hearst 2006).

7.2. EDUCATION

The key principle in combating phishing and information security threats is consumer's education. If Internet users could be convinced to inspect the security indicators within the website, then the problem would just go away. However, the most biggest advantage for phishers to successfully scam Internet users is that most Internet users lack basic knowledge of current online threats that may target them and how the online sites are formally contacting their consumers in case of maintenance and information update issues.

In general, although education is an effective countermeasure technique, eliminating phishing via education is a difficult and long-winded process and users have to dedicate a substantial amount of their time to studying the phenomenon. Moreover, phishers are becoming more skilled in mimicking legitimate websites, even to the extent of security experts being deceived.

7.3. TECHNICAL SOLUTION

Weaknesses that appeared when relying on previously mentioned solutions led to the emergence to innovative solutions. Several academic studies, commercial and non-commercial solutions are offered these days to handle phishing. Moreover, some non-profit organizations such as APWG, PhishTank and MillerSmiles provide forums of opinions as well as distribution of the best practices that can be organized against phishing. Furthermore, some security enterprises, for example, McAfee and Symantec offered several commercial anti-phishing solutions.

The success of anti-phishing techniques mainly depends on recognizing phishing websites accurately and within an acceptable timeframe. Although a wide variety of anti-phishing solutions are offered, most of these solutions were unable to make decisions perfectly on whether the website is phishing or not, causing the rise of false positive decisions. Even worse, a recent study (KrebsonSecurity 2011) demonstrates that some security providers have fallen victims for phishing attacks.

Hereunder, we preview the most popular approaches in designing technical anti-phishing solutions:

- Blacklist Approach: Where the requested URL is compared with a predefined phishing URLs. The downside of this approach is that the blacklists usually cannot cover all phishing websites since a newly created fraudulent website takes considerable time before it is added to the list. This gap in time between launching and adding the suspicious website to the list may be enough for the phishers to achieve their goals. Hence, the detection process should be extremely quick, usually once the phishing website is uploaded and before the user starts submitting his credentials.
- Heuristic Approach: The second technique is known as heuristic-based approaches, where several features are collected from the website to classify it as either phishing or legitimate. In contrast to the blacklist method, a heuristic based solution can recognize freshly created phishing websites in real time (Miyamoto, Hazeyama and Kadobayashi 2008). The effectiveness of the heuristic based methods, sometimes called features-based

methods, depends on picking a set of discriminative features that could help in distinguishing the type of website (Guang, Jason, et al. 2011).

9. Anti-Phishing Methodologies in Literature

Detecting and preventing phishing websites is an essential step towards shielding users from posting their sensitive information online. Several approaches and comprehensive strategies have been suggested to tackle phishing. Anti-phishing methodologies can be grouped into five categories: blacklist and whitelist based approach, instantaneous based approach, decision supporting tools, community rating based approach, and intelligent heuristic based approaches.

Below, we shed the light on common anti-phishing techniques by evaluating a list of related works and substantiating the need for an automated technique, as oppose to human involvement when fighting against phishing.

8.1. Blacklist and Whitelist Based Approach

A blacklist is a list of URLs thought to be malicious. Blacklist is collected through several methods, for instance heuristics from web crawlers, manual voting, and honeypots. Whenever a website is visited, the browser refers it to the blacklist to examine if the current visited URL is present within the list. If so, this indicates that it is a malicious website and as a consequence, the browser warns users not to submit any sensitive information. Blacklists can be saved either locally on the user's machine or on a server that is queried by the browser for every requested URL.

The main aspects of blacklists are quantity, quality and timing. Quantity refers to the amount of available phishing URLs within the list. On the other hand, quality can be measured in terms of erroneous listing and is commonly known as the false positive rate, which means classifying legitimate websites incorrectly as phishing. This has a negative influence on users as they lose confidence and trust in the blacklist for each false positive reading, thus potentially ignoring the correct warning signals. The third and most significant aspect is timing, which plays a key role to ensure the effectiveness of the blacklist since most phishing websites have a short life span.

If the process of updating the blacklist is slow, this will give website phishers the opportunity to carry out attacks without being added to blacklist. Blacklists are updated at various speeds, in a recent study (Sheng, Wardman, et al. 2009) scholars estimated that approximately 47-83% of phishing URLs are displayed on blacklists almost 12 hours after they launched. The same study ascertained that zero hours defence delivered from most well-known blacklists-based toolbars claimed a TP rate ranges from 15-40%. Therefore, it is necessary for an efficient blacklist to be updated instantly in order to keep users safe from being phished.

A survey published by APWG (Rasmussen and Aaron 2010) found that 78% of phishing domains were hacked domains, and at the same time they were already serving legitimate websites. As a consequence, blacklisting those domains will, in-turn, add legitimate websites to the blacklist. Even if phishing websites are removed from the blacklisted domain, legitimate websites hosted in the same domain may be left on the blacklist for a long period of time, thus causing significant harm to the reputation of the legitimate website or organization.

Some blacklists such as Google's Blacklist needs on average seven hours to be updated (Dede 2011). A range of solutions has been deployed depending on the blacklist approach, one of which is Google Safe Browsing (Google code 2010) . Another solution is Microsoft IE9 anti-phishing protection (Microsoft 2012). Site Advisor (McAfee 1987) is a database-backed measure which is designed essentially to defend against malware-based threats such as Trojan horses and Spyware. Site Advisor comprises automated crawlers which browse websites then carry out tests and build threat assessments for every visited website. Regrettably, like other blacklists, Site Advisor cannot recognize newly created threats.

VeriSign (Symantec 1982) has a commercial phishing detection solution. VeriSign has a web-crawler which collects millions of websites to recognize "clones" in order to discover phishing webpages. One potential drawback with crawling and blacklist approaches might be that anti-phishing parties will always race against attackers.

Netcraft (Netcraft Toolbar 1995) is a small software package that is activated every time a user browses the Internet as shown in Figure 3. Netcraft relies on a blacklist which consists of fraudulent websites recognized by Netcraft and those URLs submitted by the users and verified by Netcraft. Netcraft displays the location of the server where a webpage is hosted and this is particularly helpful for users who are knowledgeable about web server hosting i.e. those who typically know that a URL ending with *".ac.jo"* is not likely to be hosted outside Jordan. When Netcraft comes across a webpage that is present in the blacklist, it shows a warning message, as per Figure 4.

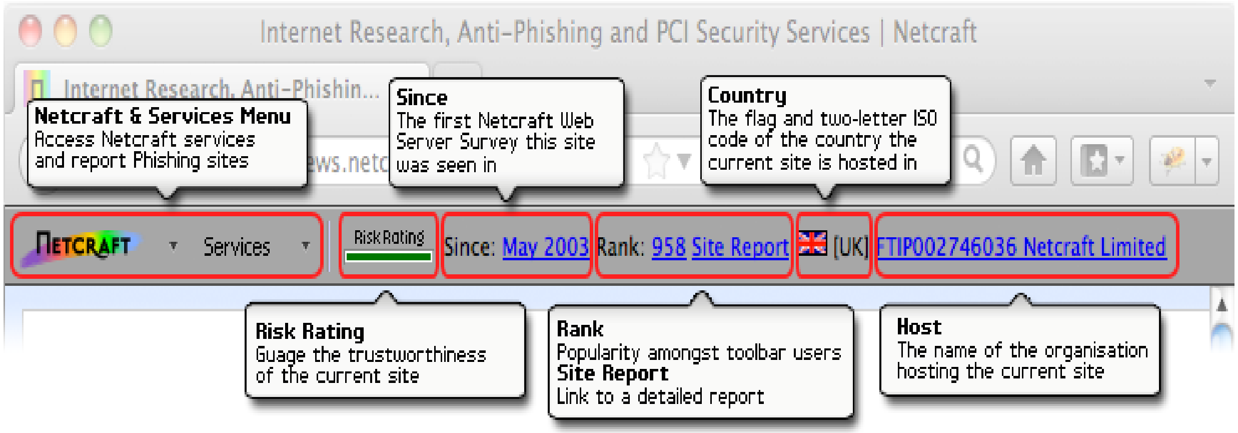
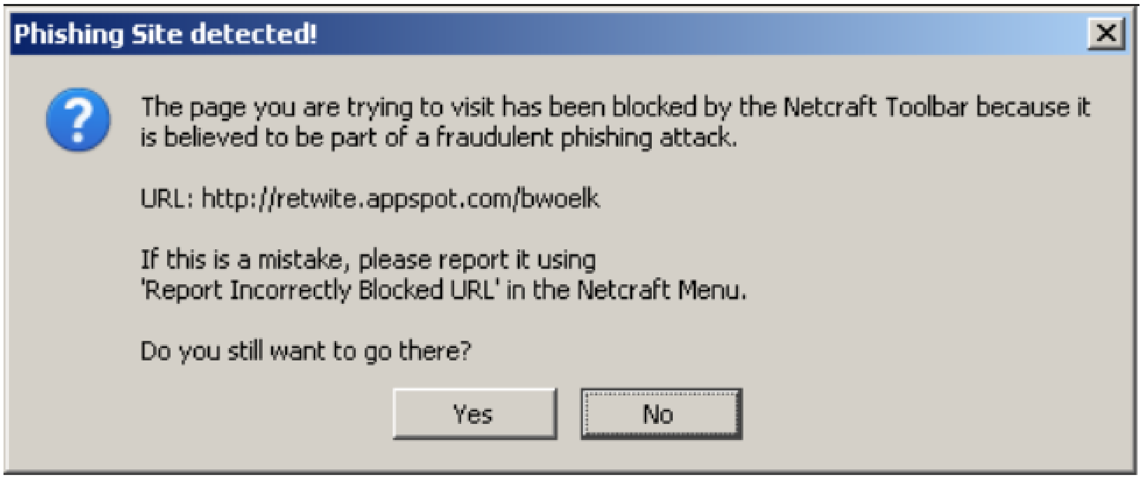

Internet Research, Anti-Phishing and PCI Security Services | Netcraft
Internet Research, Anti-Phishin...
Netcraft & Services Menu
Access Netcraft services and report Phishing sites
Since
The first Netcraft Web Server Survey this site was seen in
Country
The flag and two-letter ISO code of the country the current site is hosted in
NETCRAFT
Services
Risk Rating
Since: May 2003
Rank: 958 Site Report
[UK]
FTIP002746036 Netcraft Limited
Risk Rating
Guage the trustworthiness of the current site
Rank
Popularity amongst toolbar users
Site Report
Link to a detailed report
Host
The name of the organisation hosting the current site

Fig.3 Netcraft Toolbar


Phishing Site detected!

The page you are trying to visit has been blocked by the Netcraft Toolbar because it is believed to be part of a fraudulent phishing attack.

URL: http://retwite.appspot.com/bwoelk

If this is a mistake, please report it using
'Report Incorrectly Blocked URL' in the Netcraft Menu.

Do you still want to go there?

Fig.4 Netcraft warning message

The main features used by Netcraft to calculate the risk rate for each site and decide whether or not to add it to the blacklist are:

- How old is the domain name in which the website is hosted.

- Domain names that are not found in the Netcraft database.
- The existence of any phishing webpages previously hosted in the same domain.
- Using IP addresses or hostnames in the URL.
- History of the country and Internet service provider with regard to hosting phishing webpages
- The history of the top-level domains with respect to phishing websites.
- How popular is the website in the Netcraft Toolbar community.

The main problem with Netcraft is that the final decisions regarding website legitimacy are primarily made by the Netcraft server, rather than the user's machine. Accordingly, if the connection to the server is lost for any reason, then the user will be under threat and vulnerable during this period.

An interesting study (Ludl, et al. 2007) analyses and measures the effectiveness of two popular anti-phishing solutions based on blacklists, those are:

- Blacklist preserved by Google and utilized by *"Mozilla Firefox"*.
- Blacklist preserved by Microsoft and utilized by *"Internet Explorer"*.

The dataset used to conduct the experiments were collected in a three-week period, consisting of around 10,000 phishing URLs. The first experiment was intended to study the effectiveness of both blacklists. This set of experiments started by sending the whole dataset to both servers and saving the answers which could have a definitive result, i.e. the website, is blacklisted, or it is not yet blacklisted. Only Google gives back proper responses for all URLs in the dataset. On the other hand, Microsoft server accurately responded to only 60% of the dataset. Upon further analysis, it was shown that the Microsoft server applying some kind of limiting ratio, which explains the low response rate.

One more experiment was conducted taking into consideration those URLs for which both servers returned a response and which were online at the time of conducting the experiment. For this experiment, the dataset contained 3,592 URLs. The result showed that Google was capable of labelling 90% of the dataset items correctly, whereas Microsoft only labelled around 67%. An additional experiment was conducted to assess the time needed to update the blacklist for both servers by testing URLs that were not initially blacklisted, but added after some period of time to the list. The result showed that Microsoft blacklist has been updated after 9 hours and 7 minutes in best case; however, in worst case it has been updated after 9 days and 6 hours. Google's fastest update took about 20 hours and the slowest update time was almost 12 days. On average, Microsoft needed 6 hours to initially add a non-blacklisted entry. For Google, it took an average of 9 hours.

The authors in (Sharifi, Iran Univ. of Sci. & Technol and Siadati 2008) suggest a method to shape blacklists automatically by making use of search engines, for instance Google. The proposed method starts by extracting the company name from the suspected URL sent through emails, and then the search engine is used to search for the extracted company name. If the suspected URL shown in the first 10 returned results then it is considered a legitimate URL and it is considered phishing otherwise. Once the website is marked as a phishing website it is added to the blacklist. The experimental result on a dataset consisting of 500 legitimate websites and 30 phishing ones shows that all phishing websites were classified correctly whereas 45 legitimate websites were classified incorrectly. However, the same study acknowledges that this method introduces additional delay in the Internet browsing. One possible solution could be by applying this method in mail servers and before the email delivered to the users.

Whitelist is the opposite term to a blacklist, and it is consists of a set of trusted URL's, whereas all others are thought undependable and devious. Whitelisting is an approach that encompasses a new identity problem since a newly visited website is initially marked as malicious. However, to overcome this problem, all websites expected to be visited by the user must be listed within the whitelist. Nevertheless, it is virtually impossible to predict where a user might browse a website. A solution could be achieved by using dynamic whitelisting whereby a user is involved in creating the list independently. For every visited website, the user must decide whether or not to add this website to the whitelist. Regrettably, if phishing websites persuade users to submit their sensitive information, it could also positively persuade them to add it to the whitelist.

A recent work (Han, et al. 2012) proposes an Automated-Individual-Whitelist (AIWL) which is an anti-phishing tool based on an individual user's whitelist of known trusted websites. AIWL traces every login attempt by individual users through the utilization of a Naïve Bayesian classifier. In case a repeated successful login for a specific website is achieved, AIWL prompts the user to add the website to the whitelist. The AIWL whitelist consists of a Login User Interface (LUI) for each trusted website, the website URL, a hash of its security certificate, a hash of the credential to that website, valid IP address for the URL and the HTML DOM path to the username and password input fields. Users are warned once they submit their credentials to a website that does not exist within the whitelist. However, this technique assumes that users only submit their credentials to legitimate sites, whereas all others are considered malicious.

Kang and Lee (2007) suggested a global white-list-based tactic that prevents access to obvious phishing websites with a URL likeness check. As soon as a user request a website, the website's IP and URL pair is passed to the Access Enforcement Facility (AEF) to assess if the website is a phishing website. If the website's URL matches an entry in the trusted website list, then the program assesses the IP address similarity. If the IP also matches, then the protection system permits the user to continue; otherwise, the system warns the user of possible phishing attack.

Another solution that primarily depends on the whitelist technique was presented in PhishZoo (Afroz and Greenstadt 2011). This technique built profiles of trusted websites based on fuzzy hash techniques. A profile of a website is a fusion of several metrics that exclusively identify a specific website. The strength of such whitelisting method allows detecting newly launched phishing websites with the ability of blacklisting and adopting a heuristic approach to alert users.

The same study believes that phishing detection should be completed from a user's point of view since more than 90% of Internet users depend on the website appearance to verify its authenticity.

PhishZoo works as follow:

1. A database containing the profile of trusted websites is loaded.
2. The profile of the currently visited website is compared to the profiles stored at PhishZoo database.
3. If PhishZoo finds an identical copy of the loaded website at PhishZoo database then this website is considered legitimate.
4. Otherwise if PhishZoo finds that the profiles are partially matches then:

A- If the looking-contents does not match, but SSL certificate and addresses do, then PhishZoo will update the profile stored on the PhishZoo database.

B- If the looking-contents match, but SSL certificate or addresses do not, then PhishZoo will assign “phishing” to the loaded website.

C- If PhishZoo does not find any matching, then it will prompt the user to build a new profile.

PhishZoo has been evaluated using 636 phishing websites and 20 legitimate website profiles downloaded from PhishTank (2006). The first experiment was carried out to verify how many phishing websites use the exact or very similar HTML code of the real website. Only the HTML code of a website was considered in the profile content, the result showed that 49% of phishing websites could be detected using HTML code only. However, if the logo of a website is added to the profile content, then the prediction rate will increase to 54%. The second experiment conducted used fuzzy hashing techniques to separate content elements i.e. images, HTML codes and scripts. Matching threshold plays an effective role in detecting phishing websites. When the threshold is set to 0.2, the prediction accuracy was 82% but if the threshold is set to 0.3, PhishZoo gives an accuracy of 67%. The main negative aspect of this approach was when it assumes that most phishing websites are simply copies of real websites. Nonetheless, if the loaded website, which might be a phishing website, does not look like it’s imitated (either by changing the size or position of the website logo) then PhishZoo will ask the user to judge on the legitimacy of the loaded website. It will then ask the user to build a new profile for that website; therefore, user bears the burden of making decisions related to website legitimacy, before building website’s profile.

8.2. INSTANTANEOUS BASED PROTECTION APPROACH

Online transaction systems consist of three components including the users, the websites (from which all transactions are performed), and the stock dataset. We believe that the Instantaneous Based Protection Approach (IBPA) protects the migration of sensitive information during the transaction process by protecting the source or the destination of the information or sometimes protecting both the source and destination. Users are considered the source of information, whereas websites are considered the destination of information. IBPA protects sources of information by either authenticating user's credentials or protecting the input information instantly. However, to protect the destination of information, the IBPA authenticates the website or the server so that the user assures that the website he is dealing with directly corresponds with the website where his credential will migrate to.

A white paper published by Cryptomathic (2012), which is a company providing security solutions to businesses across a wide range of industry sectors, categorizes user authentication mechanisms into three types, as follows:

- Something the user knows such as a password, a secret code or a PIN number.
- Something physical such as a fingerprint or an IRIS scan.
- Something a user owns, for instance a credit card or a Token Generator.

Phishing arises from a reliance on the first category. Strong authentication may be achieved using two completely diverse credentials proof in parallel from different classes. This is often referred to as Two-Factor-Authentication (2FA). Typically, 2FA generates and displays a One-Time-Password (OTP) which is valid for one time use only or sometimes for a specific period of time to ensure that the user not just fill-in his password but also he uses a OTP. However, 2FA is a server-side approach which means if the server breaks down, then the user would not able to access his account. Moreover, although 2FA decreases the risk of phishing attempts, phishers have invented some circumventing techniques such as switching to real-time MITM attacks using malware techniques. Furthermore, sensitive information that is not associated with a particular website, such as a credit card number, cannot be protected by this method. America Online (AOL) distributes RSA SecurID devices (RSA 1982) to all AOL users as per Figure 5. This device produces a unique 6-digit token every minute. The user should fill-in his password along with this token in order to log into his account.

Fig.5 RSA SecurID Device

Hardware token-based technique is considered quite costly since each user should have his own device. Moreover, the training and administration costs are also high, because users should be trained how to use such tokens.

In their article, Mannan and Oorschot (2007) recommend using mobile phones to verify identity on the Internet.

Similarly, (Mizuno, Yamada and Takahashi 2005) propose multiple communication channels to authenticate user identity. Their solution enables Internet Service Providers (ISPs) to use trusted communication channels to verify user's identity on non-trusted modes of communication. The authors also suggest using mobile phones as an example of trusted communication channels.

Most Internet users use one single password for several personal accounts, therefore if phishers were able to break low security websites, then they can obtain thousands of (username, password) pairs and use them on secure e-commerce websites such as Amazon, eBay and PayPal. In their article (Ross, et al. 2005) the authors solve this problem by creating a browser extension called PwdHash which instantly alters a user's password into domains specific password which consists of the pair (Password, Domain-name) and so the user can securely re-use the same password on several websites. PwdHash is activated if the user starts his password with a special prefix "@@", or if he pressed on "F2" on the keyboard. PwdHash ensures that the users can access their accounts from any machine in the world since the hash function utilized can be easily calculated in any machine. Pseudo Random Function (PRF) (Goldreich 2010) has been used to generate the new password. Unfortunately, PwdHash works only for passwords and it is unable to secure other sensitive information, for instance credit card information or social security numbers (SSN). In addition, the safest way to shield users against phishing attacks is to predict phishing websites and warn them, rather than encrypting their passwords.

A browser sidebar used for handling user logins was proposed by (Wu, Miller and Little 2006) as per Figure 6. The users were advised to submit any sensitive information using Web Wallet sidebar and not via website forms directly, which could be achieved by pressing the security key "F2". This, in turn, will disable all input fields in the website and force users to submit their credentials through Web Wallet.

The Web Wallet also has some similarities with Microsoft InfoCard identity meta-system (Brown 2005) since it requires users to enter their information via an authentication interface. However, there are several variations; as websites should be modified to accept InfoCard submissions, whereas Web Wallet is used with web browsers. InfoCard requires support from identity providers, i.e. banks, credit card issuer and government agencies. InfoCard users are compelled to get InfoCard from various identity providers and users should authenticate themselves whenever they choose InfoCard. Lastly, InfoCard users should make correct security decisions depending on website information, as they typically are not reliable.

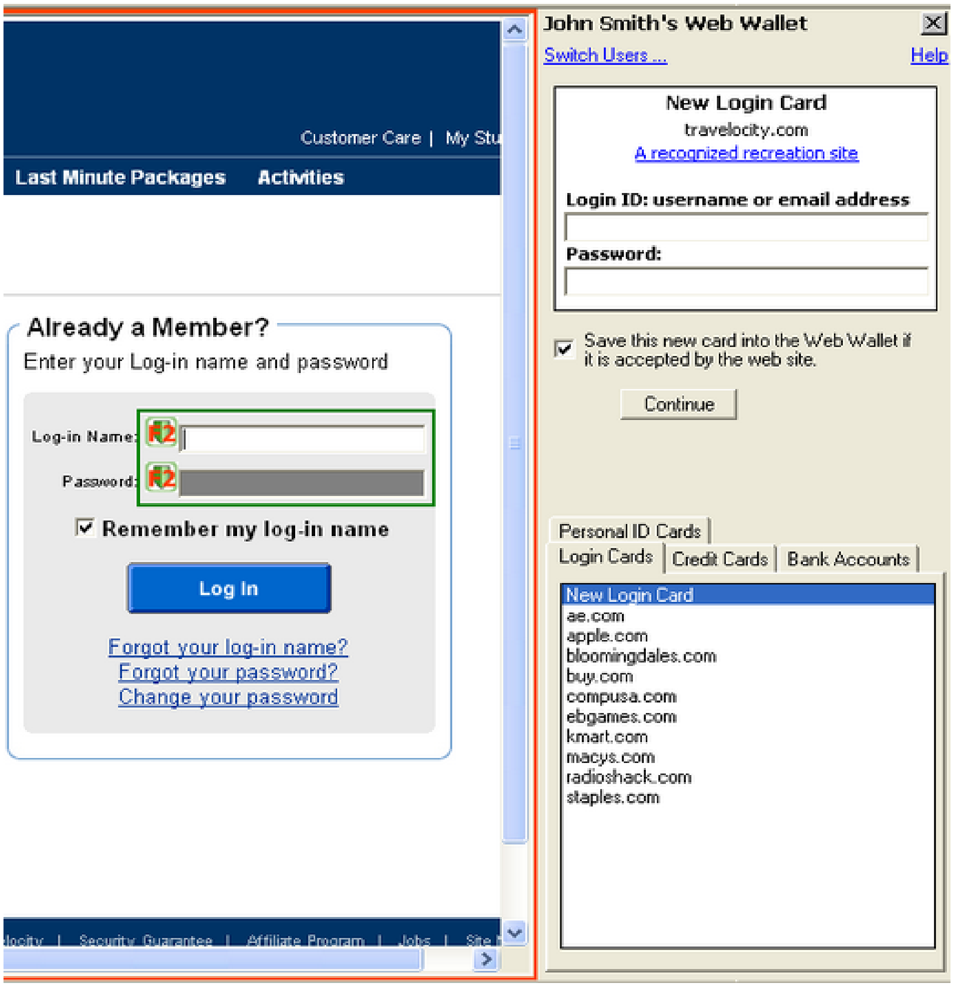
The design of Web Wallet is based on a very interesting principle, which is "integrating security into the user's task workflow". This is something most users do not neglect whilst managing security during their primary activities, and they believe that security systems should provide such a service.

Preventing phishing attacks is a joint effort between users and their respective security systems, since visual appearance is the main clue for users to judge on website legitimacy. Likewise, systems only recognize websites by system properties. Whenever Web Wallet is opened by the users; that usually means secure information is required to be submitted, and they are asked to select a specific card from the card folder which appears in the sidebar. Then, the system recognizes where the user intends to send this information. If Web Wallet detects that the current website does not match the selected one, Web Wallet alerts the user and redirects him to the correct one. Also, if a new card is being filled out, then Web Wallet will use some features i.e. SSL certificate, Trusted-third-party certificates, Website popularity, Website registration information and Website category information, to alert the user that the website is suspicious and help him to find the legitimate site.

The main negative aspect of Web Wallet is that when users visit a website for the first time, and even if Web Wallet warns the user of possible phishing attacks, the user remains able to create a new card for that website.

Several techniques protect user's credentials by adding some random information to the original credentials so that it becomes quite hard for phishers to isolate real credentials. These approaches decide whether a website is valid or not by examining the consistent HTTP response code which could be either “200 Success” or “401 Authentication Failed”. A website is classified as phishing, if the response is always success or failure on all retries.

Bogus Biter (Yue and Wang 2010) is a browser’s built-in client-side anti-phishing tool that is not just warns users about fake websites but also automatically prevents them from phishing attacks. Bogus Biter works by injecting a large number of fake credentials into phishing websites, for confusing phishers. However, the real credentials are still susceptible to phishing since they are also sent along with those fake credentials. An alternative of this technique is to submit fake credentials without submitting the real ones (Joshi, et al. 2008).



Already a Member?

Enter your Log-in name and password

☑ Save this new card into the Web Wallet if it is accepted by the web site.

Fig.6 Web Wallet Interface

A new scheme, called Dynamic Security Skins (Dhamija and Tygar 2005) allows a remote server to prove its identity to the user by showing a secret image. The strength of this schema comes from the difficulty for the phishers to spoof. This method requires the user to make verification based on what image he expects with an image generated by the server. This technique is inspired from the fact that both phishers and anti-phishing systems rely on the user's interface to deceive or protect the users. The authors implement their schema by developing an extension works on Mozilla Firefox. One drawback of this schema is that the user bears the burden of deciding whether the website is phishing or not. Moreover, this approach suggests a fundamental change, for both servers and clients within the web's infrastructure, which therefore can only succeed if the entire industry supports it. In addition, this method does not offer security if the user access his account from a public workstation. The advantage with this approach is that the user does not need to understand what digital certificates are, or any technical aspects of the security mechanisms, the user simply has to verify that the generated image and the received one are identical.

Kirda and Kruegel propose an approach that instantly monitors the data flow such as passwords and credit cards information (Kirda and Kruegel 2005). The authors create a tool referred to as "AntiPhish" which is a Mozilla Firefox extension. This approach posits that each domain is related to only one password on each specific machine, thus if the user visits a website and type in his password, a list of random domain and password pairs is created, AntiPhish then keeps watching the password fields on any visited websites, and searches the domain of that website among a list of previously visited one's, when an identical password is found AntiPhish warns users of potential attacks since the same password is entered on two different places. The main drawback of this tool is that the false positives may increase if identical passwords are used on multiple websites, which is what users usually tend to do. Furthermore, if the user has more than one account on the same website an unwanted warning message will appear.

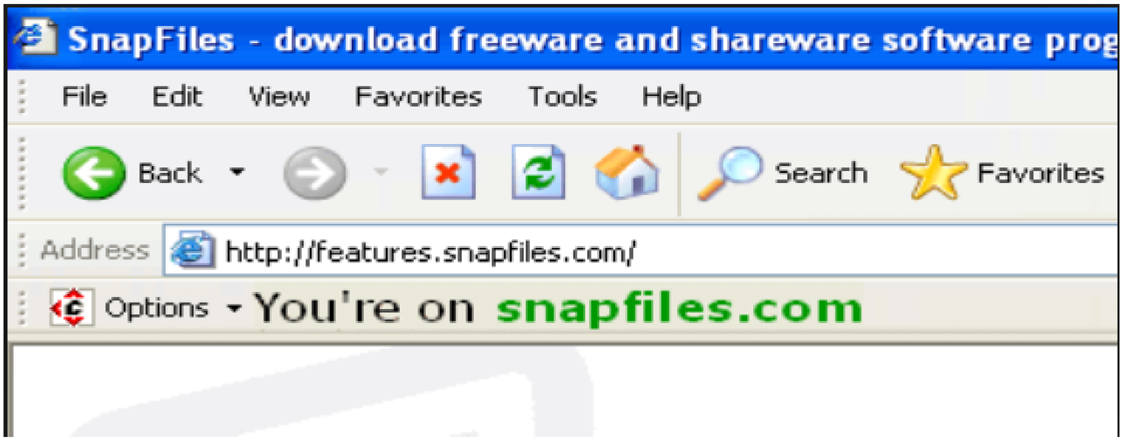
To overcome the problems that arose in (Kirda and Kruegel 2005) a new technique which basically making use of HTML DOM and layout similarity based approach has been proposed in (Angelo, et al. 2007). The new approach suggests adding one extra layer of examination by checking the likeness of the HTML DOM between the currently visited webpage and the previously visited one that have an identical password. However, because of the plasticity nature of the HTML DOM this technique can be easily broken.

(Halderman, Waters and Felten 2005) suggest an innovative method that utilities a reinforced cryptographic hash function to create passwords for several user accounts while expecting the user to remember just one simple password. This method works solely on the client side; not on server side. However, this method has a limitation in case that the user decides to change his password. Some websites ask users to update their password regularly; which will be difficult with the existing version of this application. Moreover, as several user accounts are protected by one master password this means that if this password is disclosed, all the user's accounts will be exposed to the phishers.

8.3. DECISION SUPPORTING TOOLS

Decision supporting tools are a set of tools that support user's decision-making on the website's legitimacy. These tools do not make any decision on the website legitimacy, but they extract various features from the websites and clarify them to the user. However, the final decision on the website legitimacy is made by the user.

The user's experience and attention of the clues displayed by decision supporting tools are the decisive factors on making the final decision. An example of decision supporting tools is SpoofStick (2005) which is a toolbar that can be installed on both Mozilla Firefox and Internet Explorer. SpoofStick shows the website's actual domain name as per Figure 7. An attack would possibly use a valid looking name in the sub-domain part of the URL to fool the users. For instance, if the user visited a URL like *"www.ebay.com.spoofone.ca"* then SpoofStick would consider *"spoofone.ca"* to be the domain of that URL. Moreover, SpoofStick performs reverse DNS query to display the real IP address of the website.



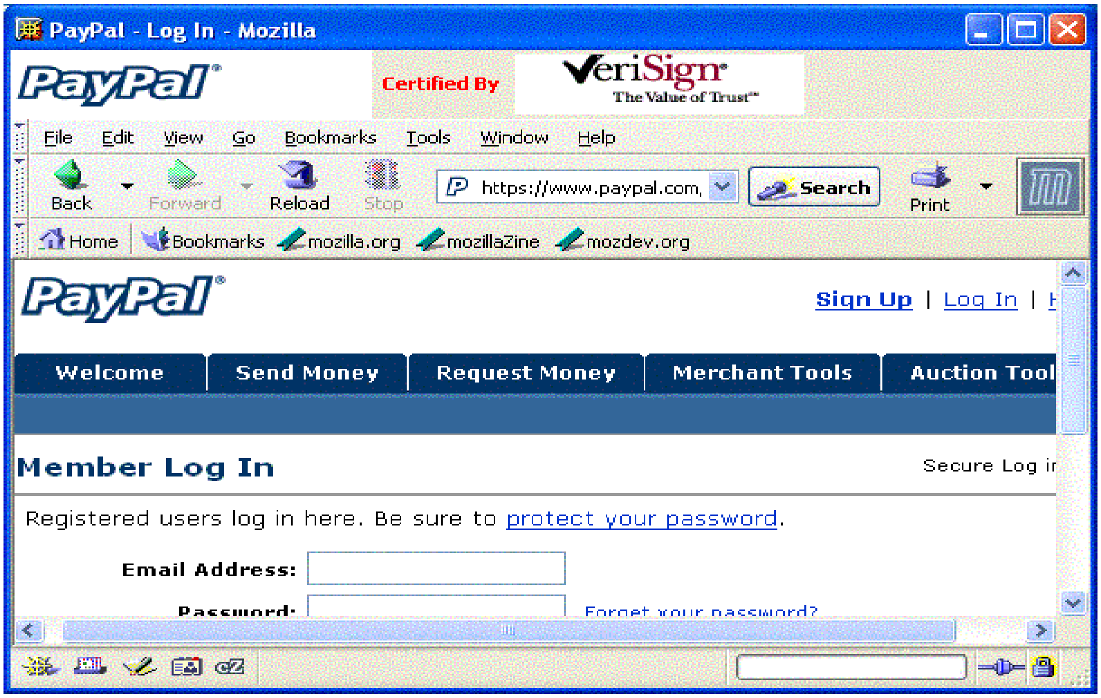
SnapFiles - download freeware and shareware software prog

Address http://features.snapfiles.com/

You're on snapfiles.com

Fig.7 SpoofStick Toolbar

Herzberg and Gbara (2004) develop a Mozilla extension called Trustbar as shown in Figure 8. Trustbar shows some information about the website credentials such as website name, logo, owner, certifying authority, or a warning message for unprotected websites. Trustbar is easy to use even by novice users. The main negative aspect of Trustbar is that it shows the website's Certification Authority (CA) without checking its trustworthiness, and the user has to do such verification. Unfortunately, most Internet users have no idea about how to do such verification.



PayPal - Log In - Mozilla

Certified By VeriSign The Value of Trust

https://www.paypal.com,

Member Log In

Secure Log ir

Registered users log in here. Be sure to protect your password.

Email Address:

Password:

Forget your password?

Fig.8 TrustBar shows the site and its certificate authority logos

iTrustPage (Ronda, Saroiu and Wolman 2008) adopts the same idea of CANTINA *"Carnegie Mellon Anti-phishing and Network Analysis"* (Zhang, Hong and Cranor 2007) since it performs a Google search based on the webpage's key-terms. CANTINA is explained in details in section 8.5. However, iTrustPage is not solely relying on extracting heuristics then judging on the website's legitimacy but it is partially depends on user's input to make the right decision. Unlike CANTINA, the search terms in iTrustPage are provided by the user. When the user encounters a website that does not exists in the iTrustPage's predefined whitelist, they are prompted to a collection of search terms that may be utilized to make a Google search. The authors deployed iTrustPage and picked up statistics on how many times the tool asks for user's intervention. They find that iTrustPage interrupts the users less than 2% after one week of use, 88% of these interruptions were selected to bypass iTrustPage's validation. However, the success of decision supporting tools in detecting and preventing phishing attacks depends on the correct decisions made by the Internet user.

Generally speaking, these approaches eventually depend on the user's skills to take the right decision on the website's legitimacy, which sometimes lacks accuracy.

8.4. COMMUNITY RATING BASED APPROACH

This technique depends on the users' knowledge and experience about a specific website to build a blacklist. This technique does not rely on automatically extracting features from the webpage to make a decision on the website's legitimacy, but on the user's experience to extract such features. Organizations such as APWG (2003), FTC (1903), Phishtank (2006), have introduced cooperative enforcement programs to fight phishing and identity-theft. These organizations offer best practice information, assist law enforcement, and help in capturing and prosecuting persons responsible for phishing and identity theft. Eight of the ten largest US banks have research partners with some of the best global association and e-commerce regulator in the world (TREND MICRO 2013).

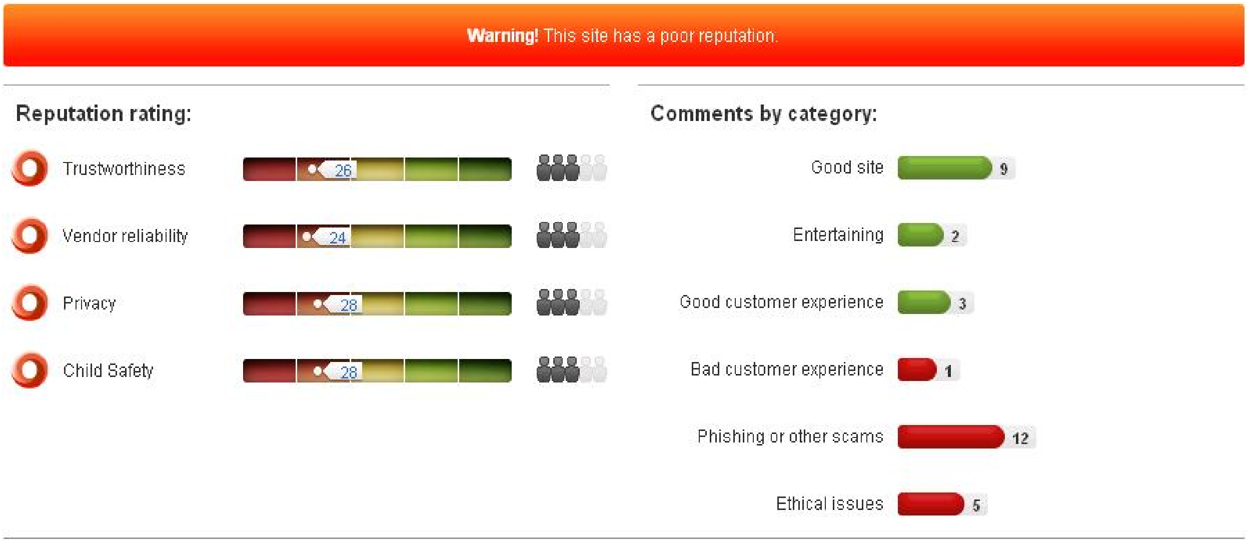
Phishtank (2006) was launched in October 2006. The main goal of Phishtank is to provide the parent company OpenDNS (2006) with a reliable phishing dataset. Phishtank makes all its databases open and accessible, thus developers and organizations such as Yahoo, Mozilla, and Microsoft as well as leading academic institutions can make use of such databases.

Cloudmark (2002) is another community based anti-phishing approach. The fundamental principle in Cloudmark is *"If you visited a website which you recognize to be unsafe, just click the block button to warn other users"*. Whenever a user is browsing the Internet, he can rate the website as "good" or "unsafe". In accordance with the overall users rating, the toolbar displays a coloured icon, where green states a legitimate website; red means a fraudulent one and yellow represents a website with insufficient information. Depending on these colours, the user is warned about phishing websites. However, the users are able to override this warning. The users themselves are also evaluated based on their history of accurately labelling phishing websites to ensure the quality of the tool. The user's reputation increases if he accurately blocks a fraudulent website as well as unblocking legitimate ones. The overall rating of a website consists of user's reputation together with the number of ratings associated with the website. The effectiveness of Cloudmark depends on the honest and active work done by users. In addition, Cloudmark depends on the availability of timely reports evaluating users' performance. If the updating process of the sites or users rating is slow then several phishing websites or users might be unreported. Moreover, some users do not click on the "Unblock" button on every visited website therefore the false positive rate could increase.

Web of Trust (WOT Inc 2006) is a community based safe surfing tool that uses an intuitive rating system to keep users safe while they shop, browse, and search online. For every searching attempt; WOT provides ratings to the searching results. Ratings are updated constantly by various members of the WOT community and from various reliable resources for instance hpHosts (Malwarebytes 2005), Panda Security (1990), LegitScript (2007) and TRUSTe (1997). As soon as the user comes across a website, the colour of the WOT logo will be changed according to the website reputation level determined by WOT community voting. The rating scale ranges from very poor, poor, unsatisfactory, good and excellent as shown in Figure 9. WOT is offered as an add-on for Mozilla Firefox and Internet Explorer and as a bookmarklet for Safari, Google Chrome, Opera and other browsers supporting JavaScript and bookmarks/favourites. WOT uses four classes to assess the website reputation:

- Trustworthiness: The "Poor" rating indicates a high possibility of phishing attacks. The website might achieve a rating of "Unsatisfactory" if it comprises unsolicited advertisements, too much pop-up's, or other contents that make the browser collapse. "Trust" refers to a good website.

- Vendor reliability: Evaluate whether the website is safe enough to perform online transactions. A "Poor" rating might be a sign of fraud possibility.
- Privacy: States whether the website owner is trusted or not.
- Child safety: Indicates whether the website contains age restrictions, sexual restrictions, aggressive nature or any other contents that encourage unsafe or illegitimate activities.



Warning! This site has a poor reputation.

Reputation rating:

Trustworthiness	26
Vendor reliability	24
Privacy	28
Child Safety	28

Comments by category:

Good site	9
Entertaining	2
Good customer experience	3
Bad customer experience	1
Phishing or other scams	12
Ethical issues	5

Fig.9 WOT rating scale.

On the other side, the main drawbacks of WOT are:

- A website may not be rated, thus legitimate website may considered being bad site.
- A website might trick people to believe that it is legitimate, but it is actually not.
- A website could be good, and then becomes bad.
- A website could be bad, and then becomes good.

8.5. Intelligent Heuristics Based Approach

Typically, anti-phishing measures are based either on URL blacklists, or by means of extracting some critical clues (features) from a website. In contrast to blacklist approaches which primarily depend on the user's experiences, the features based approaches are relatively more sophisticated and requires deep investigations.

Feature based techniques firstly collect a set of discriminative features that can separate phishing websites from legitimate ones, then train a machine learning model to predict phishing attempts based on these features, and finally use the model to recognize phishing websites in the real world. Selecting features set is an essential step in order to achieve a good model that has a high true positive rate which occurs when a legitimate website is classified as legitimate, as well as low false negative rate which occurs when a phishing website is classified as legitimate. Several features have been suggested for detecting phishing websites in the literature, nevertheless, some of these features do not seem to be sufficiently discernment, and most of them solely make use of the URL and HTML DOM to examine the webpage legitimacy.

An intelligent approach employed in (Aburrous, M, et al. 2010 c) is based on experimentally comparing associative classification algorithms. The authors have gathered 27 different features from various websites as shown in Table I, these features ranged among three fuzzy set values (Legitimate, Genuine and Doubtful). To evaluate their features the authors conducted experiments using the following data mining algorithms, MCAR (Thabtah, Peter and Peng 2005), CBA (Liu, Hsu and Ma 1998), C4.5 (Quinlan 1996), PRISM (Cendrowska 1987), PART (Witten and Frank 2002) and JRip (Witten and Frank 2002). The results showed an important relation between Domain Identity and URL based features. There was a minor impact of the Page Style on Social Human Factor criteria.

Later, in 2010 the authors used the 27 features to build a model to predict websites type based on fuzzy data mining (Aburrous, et al. 2010 b). Although, their method is a promising solution the authors did not clarify how the features were extracted from the website and specifically features related to human factors. Moreover, this model works on multi-layered approach i.e. each layer should have its own rules; however, it was not clear if the rules were established based on human experiences, or extracted in an automated manner. Furthermore, the authors classified the website as (Very-legitimate, Legitimate, Suspicious, Phishy or Very-phishy) but they did not clarify the fine line that separates one class from another. In general, fuzzy data mining uses approximations; which considered not a good candidate for managing systems that require extreme precision (Sodiya, Onashoga and Oladunjoye 2007).

Table I Features used to create a Fuzzy Data Mining Model

Category	Phishing Factor Indicator
URL & Domain Identity	Using IP Address
	Request URL
	URL of Anchor
	DNS Record
	Abnormal URL
Security & Encryption	SSL Certificate
	Certification Authority
	Abnormal Cookie
	Distinguished Names Certificate (DN)
Source Code & Java Script	Redirect Pages
	Straddling Attack
	Pharming Attack
	Using onMouseOver
	Server Form Handler
Page Style & Contents	Spelling Errors
	Copying Website
	"Submit" Button
	Using Pop-Ups Windows
	Disabling Right-Click
Web Address Bar	Long URL Address
	Replacing Similar Characters for URL
	Adding Prefix or Suffix
	Using the @ Symbol to Confuse
	Using Hexadecimal Character Codes
Social Human Factor	Much Emphasis on Security and Response
	Generic Salutation
	Buying Time to Access Accounts

A literature survey on phishing, Voice Phishing "Vishing" and SMS Phishing "Smishing" has been given by (Salem, Alamgir and Kamala 2010). The authors analysed 600 phishing emails, and they were able to collect a set of features that may discriminate legitimate emails from phishing ones as shown in Table II. An intelligent tool has been created and utilized. The first stage of developing the suggested tool is by creating a set of fuzzy logic rules. Each feature holds "Low, Moderate or High". The experiments conducted over a dataset of 1100 phishing emails shows that 22% of the emails were wrongly classified as suspicious and 78% were correctly classified as phishing. On the other hand, the tool was able to classify 95% of the legitimate emails correctly, and the remaining 5% classified as suspicious. The authors also conducted an experiment aiming to evaluate which feature set is more effective in predicting phishing emails, the result shows that the source code features (IP based URL and Non-matching URLs, Contain scripts, Number of Domains) proved to be more significant in predicting phishing emails.

Table II Awareness Program Features

Layer	Feature
Source code features (Front End)	IP based URL and Non-matching URLs
	Contain scripts
	Number of Domains
Content Features (Back End)	Generic Salutation
	Security promises,
	Requires a fast response
	Links to : https://domain

An innovative model proposed by Pan and Ding (2006) is essentially based on capturing abnormal behaviours demonstrated by phishing websites. The model consists of two components:

- The identity extractor: Which is an abbreviation of the organization's full name and/or a unique string appears in its domain name.
- The page classifier: Which utilizes some website objects i.e. structural feature that cannot be freely fabricated such as the features relevant to website identity.

Structured website consists of W3C DOM objects (W3C 2003). In their experiments, the authors have selected six structural features: Abnormal URL, Abnormal DNS record, Abnormal anchors, Server form handler, Abnormal cookies and Abnormal certificate in SSL. Support Vector Machine classifier (Cortes and Vapnik 1995) was employed to decide on the website legitimacy. Experiments on a dataset consist of 279 phishing websites and 100 legitimate ones showed that the Identity Extractor presents better results when it comes across phishing websites because the legitimate websites are independent, whereas most of the phishing websites are interrelated. Moreover, the Page Classifier performance mainly depends on the result extracted from Identity Extractor. The overall classification accuracy in this method was 84%, which is relatively considered low. However, this method snubs important features that can play a key role in determining the legitimacy of the website, which explains the low detection rate. One solution to improve this method could be by using additional features such as security related features.

The method proposed in (Zhang, Hong and Cranor 2007) suggests utilizing CANTINA which is a content-based technique to detect phishing websites using the term-frequency-inverse-document-frequency TF-IDF measures (Manning, Raghavan and Schütze 2008). CANTINA examines the webpage content then decides whether it is phishing or not by using TF-IDF. TF-IDF produces weights that assess the word importance to a document by counting its frequency.

CANTINA works as follow:

- Calculate the TF-IDF for a given webpage.
- Take the five highest TF-IDF terms and add them to the URL to find the lexical signature.
- Fed the lexical signature into a search engine.

If the N tops searching result contains the current website, it is considered a legitimate website. If not, on the other hand, it is a phishing website. N was set to 30 in the experiments. However, if the search engine returns zero results, thus the website is labelled as phishing; this argument was the main drawback of using such technique, since this would increase the false positive (FP) rate. To overcome this weakness, the authors combined TF-IDF with some other features those are: Age of Domain, Known Images, Suspicious URL, Suspicious Link, IP Address, Dotes in URL and Using Forms. One more limitation of this method is that some legitimate websites contain images; thus, using the TF-IDF may not be right. In addition, this approach does not deal with hidden texts, which might be effective in detecting the type of the webpage.

Another approach that utilizes CANTINA with an additional attributes proposed in (Sanglerdsinlapachai and Rungsawang 2010). The authors have used 100 phishing websites and 100 legitimate ones in their experiments, which are relatively considered limited. According to

CANTINA, there are eight features have been used for detecting phishing websites (Domain Age, Known Image, Suspicious URL, Suspicious Link, IP Address, Dots in URL, Using Forms and TF-IDF). Some changes to the features have been performed during the experiments as follow:

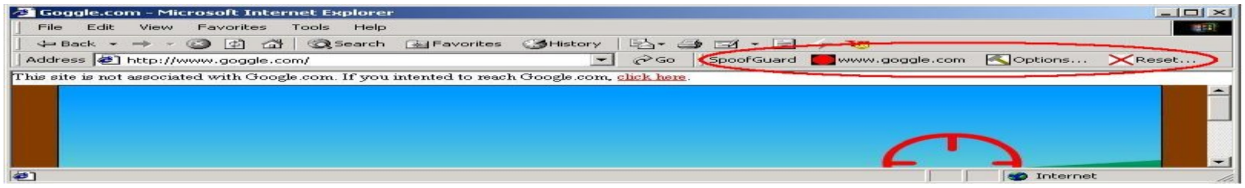
- The Using-Forms feature has been considered as a filter to decide whether to start the classification process or not since fraud websites contain at least one form with input blocks.
- The Known Image and Domain Age features are ignored.
- A new feature that shows the similarity between doubtful webpage and top-page of its domain is suggested.

The authors have performed three experiments; the first one evaluated a reduced CANTINA feature set i.e. dots in the URL, IP address, suspicious URL and suspicious link, and the second experiment involved testing whether the new feature i.e. domain top-page similarity is significant enough to play a key role in detecting website type. The third experiment evaluated the results after adding the new feature to the reduced CANTINA features. By comparing the performance of the new model after adding the new feature the results of all compared classification algorithms showed that the new feature has improved the detection rate significantly. The most accurate algorithm was NN with error rate equal 7.5%, followed by SVM and Random Forest with an error rate equal 8.5%, and AdaBoost with 9.0% and J48 with 10.5%, whereas Naïve Bayes gave the worst result with 22.5% error rate.

Guang and Hong (2009) suggested a hybrid phishing detection method that identifies phishing webpages by determining the inconsistencies between a webpage's true identity and its claimed identity using Information Extraction (IE) and Information Retrieval (IR) methods. These techniques employ the DOM after a webpage has been rendered in a web browser to circumvent intended obfuscations.

He, et al. (2011) implemented a method used by Pan and Ding (2006) and Zhang et al. (2007), using a combination of search engine results to determine whether a webpage is a phishing or not. The fundamental idea is that every website claims a dependable identity, and its activities match to that identity. If a website claims a false identity, then its activities would be anomalous.

Typically, toolbar based and plug-in-based solutions relay on blacklists stored on a server to judge on the website validity. However, some toolbars extract a set of features from the website then make some calculations and finally produce the final decision on the website status. One example of such toolbars is SpoofGuard (Neil, et al. 2004) as shown in Figure 10. SpoofGuard is an open source client-side framework deployed as a browser plug-in. it calculates a spoof index and alerts the user if the index goes beyond a predefined threshold. SpoofGuard does not use blacklists or whitelists; as an alternative, SpoofGuard uses configurable weighted heuristics to determine the likelihood that a website is malicious. Configurable weighted heuristics means that the user is able to configure the algorithmic weights for each feature as shown in the Figure 11. One downside of SpoofGuard is that if a website is classified as a phishing, the user will be warned, and he will be asked: "Do you believe this may be a spoofed site?" if the user selects no then no more warning messages will appear in the future for any webpage have the same domain name, therefore a phisher may create a harmless website and later the clean website is replaced with a malicious one, thus SpoofGuard will not warn the user of possible attacks. This kind of attack is called "Bait and Switch Attack" (Dowd, McDonald and Schuh 2006).

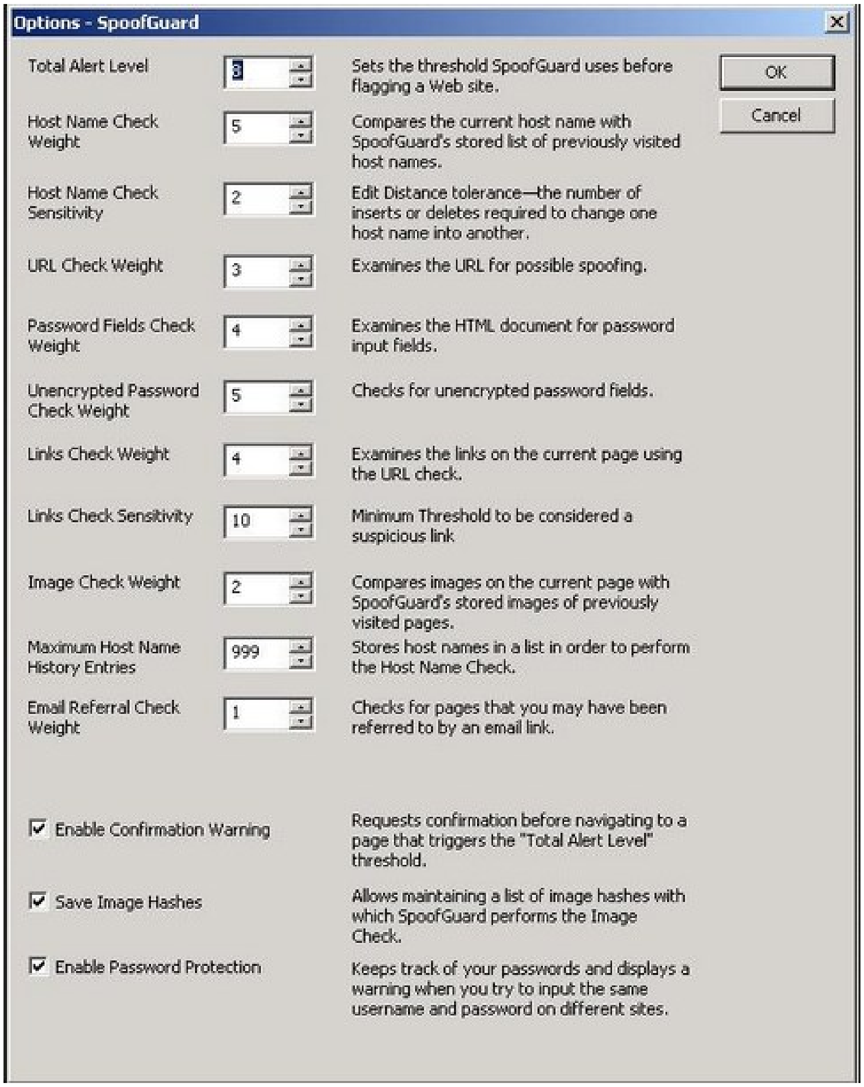


Goggle.com - Microsoft Internet Explorer

Address http://www.goggle.com/

This site is not associated with Google.com. If you intented to reach Google.com, click here.

Fig.10 SpoofGuard Toolbar



Total Alert Level	3	Sets the threshold SpoofGuard uses before flagging a Web site.
Host Name Check Weight	5	Compares the current host name with SpoofGuard's stored list of previously visited host names.
Host Name Check Sensitivity	2	Edit Distance tolerance—the number of inserts or deletes required to change one host name into another.
URL Check Weight	3	Examines the URL for possible spoofing.
Password Fields Check Weight	4	Examines the HTML document for password input fields.
Unencrypted Password Check Weight	5	Checks for unencrypted password fields.
Links Check Weight	4	Examines the links on the current page using the URL check.
Links Check Sensitivity	10	Minimum Threshold to be considered a suspicious link
Image Check Weight	2	Compares images on the current page with SpoofGuard's stored images of previously visited pages.
Maximum Host Name History Entries	999	Stores host names in a list in order to perform the Host Name Check.
Email Referral Check Weight	1	Checks for pages that you may have been referred to by an email link.

☑ Enable Confirmation Warning — Requests confirmation before navigating to a page that triggers the "Total Alert Level" threshold.

☑ Save Image Hashes — Allows maintaining a list of image hashes with which SpoofGuard performs the Image Check.

☑ Enable Password Protection — Keeps track of your passwords and displays a warning when you try to input the same username and password on different sites.

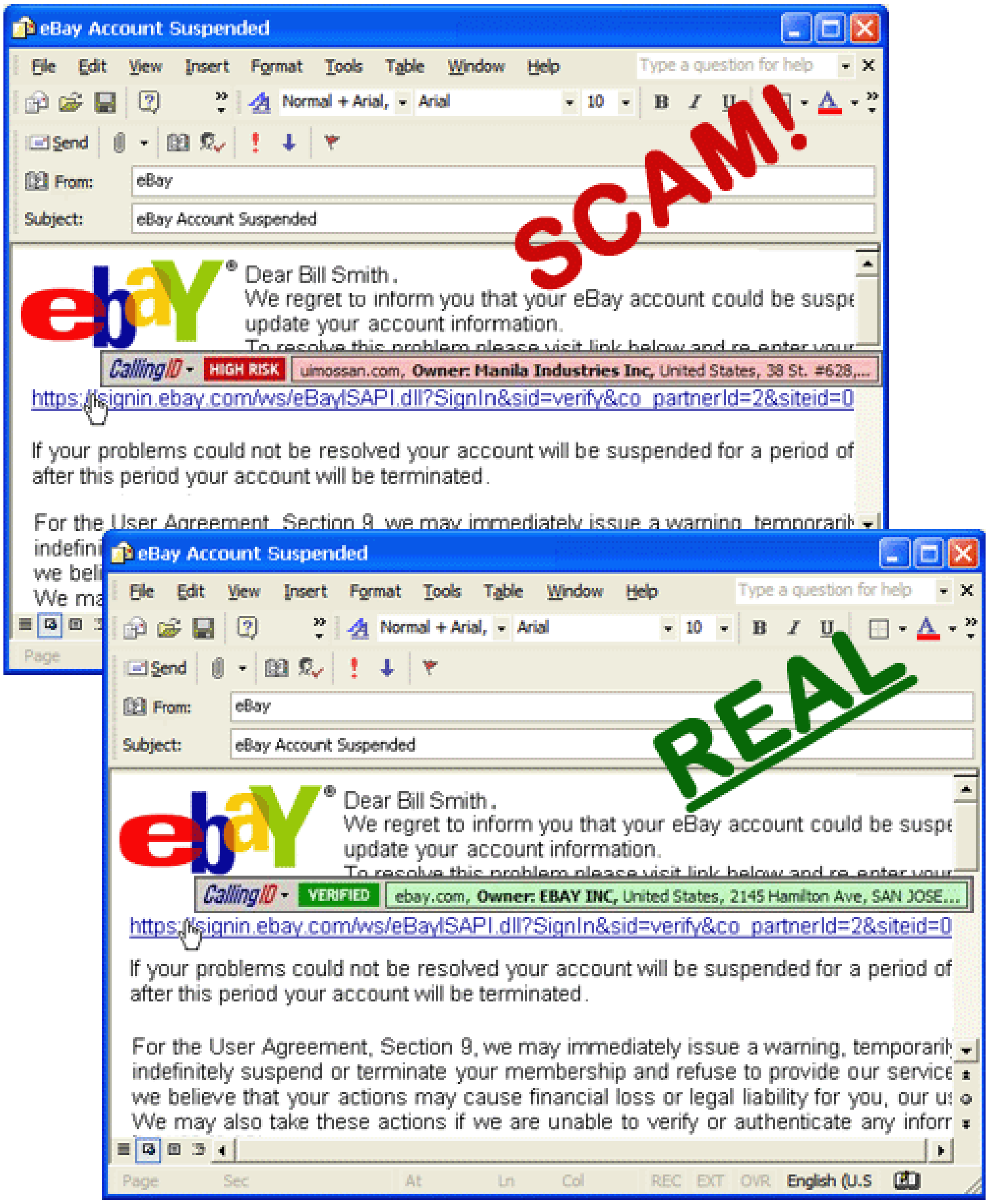
Fig.11 Spoof Guard's configure features weights window

Some organizations offer toolbars to their customers to keep them safe from being phished. An example of such toolbars is the eBay toolbar (1995). The toolbar colour is adjusted according to the website's class. If the colour is red then the website is a phishing, but if the colour is grey then the website is suspicious, whereas a legitimate website takes the green colour. However, this toolbar is solely designed to protect eBay and PayPal user's only. Also, similar to SpoofGuard, this tool is prone to "Bait and Switch" attack, since if the user ignores the warning messages for a specific domain and decides to trust this domain then no more warning messages will appear in the future for any websites hosted in this domain even if the toolbar recognize that the website is a phishing attempt.

Another example of plug-ins that relay on extracting features from a website rather than depending on the white or black lists is CallingID's Link Advisor (2010). This pug-in uses 54 different verification tests divided into five security layers. When the user places the mouse cursor over a link included in an email message the full details of the website owner is shown for the user as in Figure 12. In addition, the CallingID's Link Advisor will make some calculations and warns the user about the website legitimacy level. Green colour means that the website is good; yellow means that the website is low risk; and red means that the website is high risk.

URL and HTML DOM objects are not the only places to extract features from a website; but features might also be extracted from visual related features. The basic idea is that detecting phishing websites is similar to plagiarism and duplicate-document detection, except that phishing detection focuses on visual similarities whereas plagiarism detection focuses on text based features in similarity measurement.

One promising approach proposed by (Wenyin, et al. 2005) suggests detecting phishing websites based on visual similarities between phishing and legitimate websites. This technique initially decomposes the webpage into salient block regions depending on visual clues. The visual similarity between phishing and legitimate webpages is then evaluated in three metrics: block level similarity; layout similarity and overall style similarity. A webpage is considered a phishing attempt if any metric has a value higher than a predefined threshold. The authors collected 8 phishing webpages and 320 official bank webpages, the experimental results show a 100% TP and 1.25% FP. Although the results were impressive, this technique may be instable because of the high plasticity of the webpage layout.



From: eBay

Subject: eBay Account Suspended

Dear Bill Smith.
We regret to inform you that your eBay account could be suspe
update your account information.
To resolve this problem please visit link below and re-enter your

CallingID HIGH RISK uimossan.com, **Owner: Manila Industries Inc,** United States, 38 St. #628,...

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of
after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily
indefini
we beli
We ma

From: eBay

Subject: eBay Account Suspended

Dear Bill Smith.
We regret to inform you that your eBay account could be suspe
update your account information.
To resolve this problem please visit link below and re-enter your

CallingID VERIFIED ebay.com, **Owner: EBAY INC,** United States, 2145 Hamilton Ave, SAN JOSE...

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of
after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily
indefinitely suspend or terminate your membership and refuse to provide our service
we believe that your actions may cause financial loss or legal liability for you, our us
We may also take these actions if we are unable to verify or authenticate any inforr

Fig.12 Calling ID's plug-in

The authors in (Liu, et al. 2006) suggested a phishing detection model using the Earth Mover's Distance (EMD) (Yossi, Tomasi and Leonidas 1998). EMD is a measurement technique to assess the distance between two probability distributions. This approach assesses the similarity between phishing and legitimate websites at the pixel level of the websites without looking at the source code similarities.

Aside from the techniques presented above, a set of literature aims to evaluate the performance of machine learning and data mining algorithms was conducted.

(Miyamoto, Hazeyama and Kadobayashi 2008) evaluate the performance of machine learning based detection methods (MLBDMs) including AdaBoost, Bagging, Support Vector Machines (SVM), Classification and Regression Trees (CRT), Logistic Regression (LR), Random Forests (RF), Neural Networks (NN), Naive Bayes (NB) and Bayesian Additive Regression Trees (BART). A dataset consist of 1500 phishing websites and 1500 legitimate websites were used in the experiments. The evaluation based on 8 heuristics presented in CANTINA (Zhang, Hong and Cranor 2007).

Before starting their experiments a set of decision were made by the authors as follow:

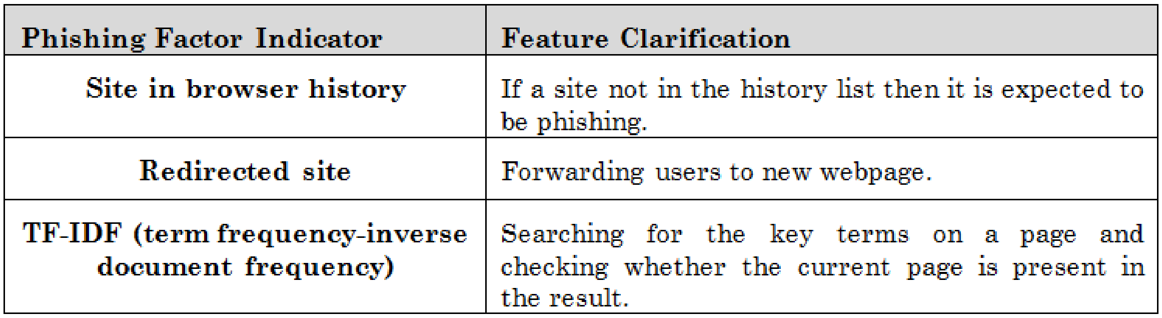
- The number of trees in Random Forest is set to 300.
- For all experiments need to be analysed iteratively the number of iteration was set to 500.
- Threshold value was set to 0 for some machine learning techniques such as BART.
- Radial based function was used in support vector machine.
- The number of hidden neurons was set to 5 in the neural network experiments.

The experiments showed that 7 out of 9 MLBDMs outperform CANTINA’s accuracy and those are: AdaBoost, Bagging, Logistic Regression, Random Forests, Neural Networks, Naive Bayes and Bayesian Additive Regression Trees.

In (Abu-Nimeh, et al. 2007) the authors compare the predictive accuracy of a number of machine learning methods those are Logistic Regression (LR), Classification and Regression Trees (CART), Bayesian Additive Regression Trees (BART), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks (NN). A dataset consist of 1171 phishing emails and 1718 legitimate emails were employed in the comparative experiments. A set of 43 features were used to learn and test the classifiers. The experiments show that RF has the lowest error rate of 7.72%, followed by CART 08.13%, followed by LR 08.58%, followed by BART 09.69%, then SVM 09.90%, and finally NN with 10.73%. However, the results indicate that there is no optimal classifier might be used to predict phishing websites. For instance, the FP rate when using NN is 5.85% and the FN rate is 21.72% whereas the FP rate for RF is 8.29%, and the FN rate is 11.12%, which means that NN outperform RF in term of FN but RF outperform NN in term of FP.

In (Sadeh, Tomasic and Fette 2007), the authors compared a number of commonly used machine learning methods including SVM, Rule-based techniques, Decision Trees, and Bayesian techniques. A random forest algorithm was implemented in “PILFER”. PILFER stands for Phishing Identification by Learning on Features of email Received which essentially aims to detect phishing emails. A dataset consisting of 860 phishing emails and 6950 legitimate one’s have been used in the experiments. The proposed technique correctly detects 96% of the phishing emails with a false positive rate of 0.1%. The authors used 10 features for detecting phishing email’s those are: IP based URL’s, Age of Domain, Non-matching URL’s, Having a Link within the e-mail, HTML emails, Number of Links within the e-mail, Number of Domains appears within the e-mail, Number of Dot’s within the links, Containing JavaScript and Spam filter output. PILFER can be applied towards classifying phishing websites by combining all the 10 features except “Spam filter output” with those shown in Table III. For assessment, the authors utilized exactly the same dataset in both PILFER and SpamAssassin version 3.1.0 (The Apache SpamAssassin Project 1995). One more goal of using SpamAssassin was actually to extract Spam filter output feature. The results revealed that PILFER has a FP rate of 0.0022% if it is being installed without a spam filter. On the other hand if PILFER is joined with SpamAssassin the false positive rate decreased to 0.0013%, and the detection accuracy rises to 99.5%.

Table III Features added to PILFER to classify websites



Phishing Factor Indicator	Feature Clarification
Site in browser history	If a site not in the history list then it is expected to be phishing.
Redirected site	Forwarding users to new webpage.
TF-IDF (term frequency-inverse document frequency)	Searching for the key terms on a page and checking whether the current page is present in the result.

10.HUMAN VS. AUTOMATIC BASED PROTECTION

A phisher uses social engineering practices to defraud honest Internet users into providing their financial and personal information (Yu, Nargundkar and Tiruthani 2008). Phishers know that the Internet users seem to be the weakest link in the protection chain. One strategy for fighting phishing attacks is by educating Internet users to recognize phishing attempts rather than just warning them about possible risks. An example of studies that focus on educating users comes in (Coordination 2005) were a set of phishing emails and booklets defining phishing were circulated to New York State employees. The result shows that employees were less likely to fall victims to phishing if they received good training sessions. Moreover, the authors claimed that digital training booklets are more effective than physical booklets.

In 2006 a usability study conducted to understand how and why phishing works (Dhamija, Tygar and Hearst 2006) showed that the lack of knowledge of computer systems, lack of attention to security indicators and lack of attention to the absence of security indicators are the main reasons why users became victims to phishing attack. The authors introduced 20 different websites to 22 participants and asked them to determine which one is fraudulent and why. The participants' were highly educated members including staff and students at universities; the minimum level of the participants' education was a bachelor degree. The result shows that phishing websites fooled 90% of the participants' despite that some cues warn users of the possibility of exposure to phishing.

This high percentage can be explained by a number of reasons those are:

1. More than 23% of the participants ignored the decisive clues such as the presence of SSL protocol.
2. Some clues were misunderstood since some participants' thought that changing the address bar colour is an aesthetic choice.
3. Many participants were not able to differentiate between an actual SSL in the address bar and a spoofed one.
4. When popup warnings presented of a self-signed certificate, 15 participants accepted the certificate. This means that popup warning is ineffective technique to warn users of possible attack.

In their article (Ronald, Curtis and Aaron 2007) the authors revealed that educating and training Internet users about web security is one of the most essential aspects of an organization's security situations. A study conducted at Indiana University (Jagatic, et al. 2007) showed that the social context of phishing might increase the number of victims. In this study, 487 students were targeted. This research shows that 72% of the students had fallen victims of deception when they emailed by someone they knew, while only 16% have fallen victims when they emailed by a random email address.

In 2007, a survey has been conducted to measure the users understanding of the malicious contents within the websites (Julie S., Mandy and Cranor 2007). The authors gathered data on participants' understanding of URLs and icons related to the browser. The survey finds that although several participants' evinced some technical background; they refused to enter their personal information into legitimate websites due to the potential of severe outcomes like exposing their password or credit card number or social security number.

An interesting education technique was proposed by means of game based learning in (Sheng, Magnien, et al. 2007). This technique offers a close link between action and instantaneous feedback. The authors created an online game called *"Anti-Phishing Phil"* (Cranor, Hong and Sadeh 2008). The main goal of this game is to educate Internet users how to recognize phishing URLs, how to check the cues within the browser and how to find legitimate websites using search engines. This game improved the users' ability to identify phishing websites, since the study shows that a user who played this game became to be more cautious of phishing websites.

An email based education technique called *"PhishGuru"* (Kumaraguru, et al. 2007) that educates Internet users how to use evidences in URLs to evade phishing attacks suggests that alongside with the automated detection systems users education may offer a complementary method to help Internet users to recognize deceptive emails and websites.

A recent study (Sheng, Holbrook, et al. 2010) finds that the users may rely on incorrect heuristics in determining how to reply to emails; for instance, some users believe that since the company they are dealing with already had their information it would be harmless to give it again. The authors conduct an online survey aims to study the relationship between demographics and phishing susceptibility and the effectiveness of several anti-phishing educational materials, the result shows that gender and age are two key demographics to predict phishing vulnerability since women had less technical training and knowledge than men and were more vulnerable to click on email links and exposing their credentials. Moreover, people aged between 18 and 25 are evidently the most vulnerable because they have a lower level of education, fewer years on the Internet experience, less exposure to training materials, and less of an aversion to risks. The study concludes that phishing may be reduced by providing extra instructional material to web users. The same study concluded that the educational materials decreased users' susceptibility to disclose their personal information into a phishing webpage by 40%.

However, some materials have had an adverse impact since to some extent these materials reduced users' susceptibility to click on legitimate links.

Education should focus on the most important features that are most likely associated with less vulnerability to phishing such as; how to interpret URLs, what does SSL protocol means and what does padlock icon signifies. As a result, people can take steps to avoid phishing attempts by slightly modifying their browsing habits.

A research study aims to know why employees are susceptible to phishing, and how the managers should act to protect their organizations (Ohaya 2006) finds that many employees lack the basic knowledge of Internet principles such as what does domain name means, thus they cannot tell the difference between genuine website and a spoofed one. For example, many employees may think that *"http://www.paypai.com"* is the same as *"http://www.paypal.com"*. In addition, many employees do not know that a closed padlock icon in the browser indicates that the webpage is secured with SSL protocol. Even worse, most of the employees do not know that SSL is used is to ensure encryption of any sensitive information sent through the Internet. Furthermore, some employees are not aware of SSL certificate verification process since they focus on their primary tasks and do not pay much attention to security indicators.

Overall, although education is a good method in fighting phishing; this method requires high costs. Not all organizations were able to pay out extra money on users' education, knowing that users' education is not a onetime cost. Moreover, it is not sure that after appropriate education the users will act in an ideal way. As a result, the need for an automatic method has become an urgent need. Nowadays, there are many automated technique proposed in literature to predict phishing attacks, most of them take the form of browser plugins, these plugins are installed as an add-on to the browser. If a website is suspected as a phishing website these plugins warn the users not to submit any personal information through the website. However, browser plugins are not fully able to detect all phishing websites.

A study aimed to evaluate the effectiveness of five toolbars (Wu, Miller and Gar 2006) those are: SpoofStick, Netcraft, Trustbar, eBay Account Guard and SpoofGuard revealed that the users were spoofed 34% of the time; 67% of the users were spoofed by at least one phishing attack; 40% of the spoofed users were tricked due to poorly designed websites. The study concludes that there are two main reasons behind the users falling into these attacks:

Firstly, users discarded what the toolbars display because the content of websites looks legitimate, which means that most Internet users tend to judge on the website class based on its look-and-feel.

Secondly, several companies do not follow sensible practice in designing their websites; thus, the toolbars cannot help Internet users to differentiate between poorly designed websites and malicious websites.

Automated techniques outperform the human based techniques if some improvements are made on the mechanisms of predicting and warning users of possible phishing attacks. Several suggestions were proposed by (Wu, Miller and Gar 2006) to improve the automated technique performance; these suggestions are summarized as follows:

1. Popup warnings should always appear at the right time with the right warning message.
2. Warnings should give an alternative path for the user to finish the tasks they intend to do.
3. Companies need to follow some standard practices to better distinguish their sites from malicious phishing attacks like :
    a. Using single domain name rather than using IP addresses or multiple domain names.
    b. They should use SSL to encrypt every webpage on their sites.
    c. SSL certificates should be valid and from widely used Certificate Authorities (CAs).
4. In addition selecting a set of discriminative features may be the corner stone for any tool to be good enough in predicting phishing attacks.

11.SUMMARY

Internet facilitates reaching customers all over the globe without any market place restrictions and with effective use of e-commerce. As a result, the number of customers who rely on the Internet to perform procurements is increasing dramatically. Hundreds of millions of dollars are transferred through the Internet every day. This amount of money was tempting the fraudsters to carry out their fraudulent operations. Thus, Internet-users were vulnerable to different types of web-threats. Hence, the suitability of the Internet for commercial transactions becomes doubtful.

Phishing is a form of web-threats that is defined as the art of mimicking a website of an authentic enterprise aiming to acquire private information. Presumably, these websites have high visual similarities to the legitimate ones in an attempt to defraud the honest people. Social engineering and technical tricks are commonly combined together in order to start a phishing attack. Typically, a phishing attack starts by sending an e-mail that seems authentic to potential victims urging them to update or validate their information by following a URL link within the e-mail. Predicting and stopping phishing attack is a critical step toward protecting online transactions. Several approaches were proposed to mitigate these attacks. Anti-phishing measures may take several forms including legal, education and technical solutions.

In many perspectives, identifying phishing websites is performed manually. By this means, the Internet-user analyses the webpage and based on the extracted information he takes a decision on the website legitimacy. However, making use of computational technologies to automate the process of predicting phishing websites becoming an urgent need, since phishing websites become more stylish, tactics used become more complicated, and the analysis time increases.

Currently existing filtering methods are far from suitable. For instance, blacklist and whitelist-based detection approaches could not deal with zero-days phishing websites. On the other hand, heuristics-based detection approaches have a possibility to recognize these websites. Yet, most heuristics-based approaches devoted to static environment, where the complete datasets are presented to the learning algorithm. However, the accuracy of the heuristics-based approaches may fall remarkably if some environmental features change. Hence, users would become doubting the protection system and would ignore the warnings raised from detection systems.

We believe that phishing is a continuous problem where the significant features in determining the type of websites are constantly changing. Therefore, we believe that a successful phishing detection model should be able to adapt its knowledge and structure in a continuous, self-structuring, and interactive way in response to the changing environment that characterizes phishing websites.

Bibliography

Aaron, G, and R Rasmussen. *Global Phishing Survey 2H/2009.* Sao Paulo, Brazil.: Counter eCrime Operations Summit IV, 2010.

Abu-Nimeh, Saeed, Dario Nappa, Xinlei Wang, and Suku Nair. "A Comparison of Machine Learning Techniques for Phishing Detection." *The 2nd annual Anti-Phishing Working Groupse Crime researchers, eCrime '07.* New York, NY, USA: ACM, 2007. 60-69.

Aburrous, M, Hossain, M. A., Dahal, K., and Fadi, T. "Predicting Phishing Websites using Classification Mining Techniques." *Seventh International Conference on Information Technology.* Las Vegas, Nevada, USA: IEEE, 2010 c. 176-181.

Aburrous, Maher , M A Hossain, Keshav Dahal, and Fadi Thabtah. "Intelligent phishing detection system for e-banking using fuzzy data mining." *Expert Systems with Applications: An International Journal*, December 2010 b: 7913-7921.

Afroz, Sadia , and Rachel Greenstadt. "PhishZoo: Detecting Phishing Websites by Looking at Them." *Fifth International Conference on Semantic Computing.* Palo Alto, California USA: IEEE, 2011.

Angelo, Rosiello P.E., Engin Kirda, Christopher Kruegel, and Fabrizio Ferrandi. "A layout-similarity-based approach for detecting phishing pages." *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on.* Politecnico di Milano, Italy: IEEE, 2007. 454 - 463.

APWG. 2003. http://www.antiphishing.org/ (accessed December 20, 2011).

APWG, Greg Aaron, and Ronnie Manning. *APWG Phishing Reports.* APWG. 2014. http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf (accessed February 8, 2013).

BBC News. *Jail for eBay phishing fraudster.* 2005. http://news.bbc.co.uk/2/hi/uk_news/england/lancashire/4396914.stm (accessed October 20, 2011).

Brown, Keith. *A First Look at InfoCard.* 2005. http://msdn.microsoft.com/en-us/magazine/cc163626.aspx (accessed January 20, 2012).

Cendrowska, J. "PRISM: An algorithm for inducing modular rule." *International Journal of Man-Machine Studies*, 1987: 349-370.

Chandrasekaran, M., K. Narayanan, and S. Upadhyaya. "Phishing email detection based on structural properties." *NYS Cyber Security Conference.* 2006.

Chen, Juan, and Chuanxiong Guo. "Online Detection and Prevention of Phishing Attacks (Invited Paper)." *First International Conference on Communications and Networking in China. ChinaCom '06.* Beijing: IEEE, 2006. 1-7.

Cloudmark Inc. *Cloudmark.* 2002. http://www.cloudmark.com/en/home (accessed October 12, 2011).

Coordination, New York State Office of Cyber Security & Critical Infrastructure. *Gone Phishing: A Briefing on the Anti-Phishing Exercise Initiative for New York State Government.* 2005. http://www2.ntia.doc.gov/grantee/ny-state-office-of-cyber-security-critical-infrastructure (accessed January 12, 2012).

Cortes, Corinna, and Vladimir Vapnik. "Support Vector Networks." *Machine Learning* 20, no. 3 (1995): 273 - 297.

Cranor, Lorrie, Jason Hong, and Norman Sadeh. *Wombat Security Technologies.* 2008. http://wombatsecurity.com/antiphishingphil (accessed December 20, 2012).

Cryptomathic Co. *Two Factor Authentication for Banking, Building the Business Case.* 2012. http://www.cryptomathic.com/media/11380/cryptomathic%20white%20paper-2fa%20for%20banking.pdf (accessed July 12, 2013).

Dede, David . *Ask Sucuri.* 2011. http://blog.sucuri.net/2011/12/ask-sucuri-how-long-it-takes-for-a-site-to-be-removed-from-googles-blacklist-updated.html (accessed February 17, 2012).

Dhamija, Rachna, and J Doug Tygar. "The battle against phishing: Dynamic Security Skins." *The 1st Symposium On Usable Privacy and Security.* New York, NY, USA: ACM Press., 2005. 77-85.

Dhamija, Rachna, J. D. Tygar, and Marti Hearst. "Why Phishing Works." *The SIGCHI conference on Human Factors in Computing Systems.* New York, NY, USA: ACM, 2006. 581-590.

Dowd, Mark, John McDonald, and Justin Schuh. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities.* Addison Wesley, 2006.

eBay Toolbar's. *Using eBay Toolbar's Account Guard.* 1995. http://pages.ebay.com.au/help/account/toolbar-account-guard.html (accessed March 20, 2012).

"Executive Order 13402." *Presidential Documents.* 2006. http://www.gpo.gov/fdsys/pkg/FR-2006-05-15/pdf/06-4552.pdf (accessed May 12, 2013).

Florencio, Dinei, and Cormac Herley. "Evaluating a trial deployment of password re-use for phishing prevention." *The anti-phishing working groups 2nd annual eCrime researchers summit, eCrime '07.* New York: ACM, 2007. 26-36.

Franklin, Jason, and Vern Paxson. "An inquiry into the nature and causes of the wealth of internet miscreants." *The 14th ACM conference on Computer and communications security, CCS '07.* New York: ACM, 2007. 375-388.

FTC. *Federal Trade Commission.* 1903. http://www.ftc.gov/ (accessed July 26, 2012).

Gartner Inc. *Gartne.* 2011. http://www.gartner.com/it-glossary/data-mining (accessed May 30, 2011).

General Assembly of Virginia. *CHAPTER 827.* 2005. http://leg1.state.va.us/cgi-bin/legp504.exe?051+ful+CHAP0827 (accessed May 2013, 21).

Goldman, Lea. *Cybercon.* 2004. http://www.forbes.com/forbes/2004/1004/088.html (accessed May 2013, 21).

Goldreich, Oded . *Pseudorandom Generators: A Primer.* ULECT series, 2010.

Google code. *Google Safe Browsing.* 2010. http://code.google.com/p/google-safe-browsing/ (accessed December 11, 2011).

Gross, Grant. *Senator introduces 'phishing' penalties bill.* 2004. http://www.informationweek.com/phishers-would-face-5-years-under-new-bill/d/d-id/1030773? (accessed March 18, 2011).

Guang, Xiang, and Jason I Hong. "A hybrid phish detection approach by identity discovery and keywords retrieval." *The 18th international conference on World wide web WWW '09* . Madrid: ACM, 2009. 571-580.

Guang, Xiang, ong Jason, Rose Carolyn P, and Cranor Lorrie. "CANTINA+: A Feature-rich Machine Learning Framework for Detecting Phishing Web Sites." *ACM Transactions on Information and System Security (TISSEC)*, 09 2011: 1-28.

Halderman, Alex J, Brent Waters, and Edward W Felten. "A convenient method for securely managing passwords." *The 14th International Conference on World Wide Web, WWW '05.* NY: ACM, 2005. 471-479.

Han, Weili, Ye Cao, Elisa Bertino, and Jianming Yong. "Using automated individual white-list to protect web digital identities." *Expert Systems with Applications* 39, no. 15 (2012): 11861–11869.

Harris Poll. *Taking Steps Against Identity Fraud.* Harris Pol, 2006.

He, Mingxing , et al. "An efficient phishing webpage detector." *Expert Systems with Applications* 38, no. 10 (2011): 12018–12027.

Herzberg, Amir , and Ahmad Gbara. "Protecting (even) Naive Web Users, or: preventing spoofing and establishing credentials of web sites." *DIMACS*, 2004.

Huang , Huajun, Coll. of Comput. Sci., Central South Univ. of Fore, Junshan Tan, and Lingxi Liu. "Countermeasure Techniques for Deceptive Phishing Attack." *New Trends in Information and Service Science, 2009. NISS '09. International Conference on.* Beijing: IEEE, 2009. 636-641.

Jagatic, Tom N, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. "Social phishing." *Communications of the ACM*, 2007: 94-100.

Jakobsson, Markus. "The Human Factor in Phishing." *Privacy & Security of Consumer Information '07.* 2007.

James, Lance. *Phishing Exposed.* Syngress Publishing, 2005.

Joshi, Y, IIIT-Bangalore, Bangalore , S Saklikar, D Das, and S Saha. "PhishGuard: A browser plug-in for protection from phishing." *The 2nd International Conference on Internet*

Multimedia Services Architecture and Applications, 2008. IMSAA 2008. Bangalore: IEEE, 2008. 1-6.

Julie S., Downs, Holbrook Mandy, and Lorrie Faith Cranor. "Behavioral Response to Phishing Risk." *The Anti-Phishing Working Groups, 2nd annual eCrime researchers summite, Crime '07.* New York, NY, USA: ACM, 2007. 37-44.

JungMin, Kang, and Lee Dohoon. "Advanced White List Approach for Preventing Access to Phishing Sites." *International Conference on Convergence Information Technology, 2007.* Gyeongju: IEEE, 2007. 491-496.

Keizer, Gregg . *Phishers Beat Bank's Two Factor Authentication.* Manhasset, NY: InformationWeek, 2007.

Kirda, Engin, and Christopher Kruegel. "Protecting Users Against Phishing Attacks with AntiPhish." *The 29th Annual International Computer Software and Applications Conference.* Washington, DC, USA: IEEE Computer Society, 2005. 517-524.

KrebsonSecurity. *HBGary Federal Hacked by Anonymous.* 2011. http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/ (accessed May 14, 2013).

Kumaraguru, Ponnurangam, et al. "Getting users to pay attention to anti-phishing education: evaluation of retention and transfer." *The Anti-Phishing Working Groups 2nd annual eCrime researchers summit, eCrime '07.* Pittsburgh, PA, USA: ACM, 2007. 70-81.

LegitScript. *The Leading Source of Internet Pharmacy Verification.* 2007. http://www.legitscript.com/ (accessed February 14, 2012).

Leyden, John. *Florida man indicted over Katrina phishing scam.* 2006. http://www.theregister.co.uk/2006/08/18/hurricane_k_phishing_scam/ (accessed May 21, 2013).

LinkAvisor, CallingID. 2010. http://www.callingid.com/about/press/Press-Releases.aspx (accessed September 1, 2011).

Liu, Bing, Wynne Hsu, and Yiming Ma. "Integrating Classification and association rule Mining." *The 4th international conference on Knowledge Discovery and Data mining, KDD'98.* AAAI Press, 1998. 80--86.

Liu, Wenyin , Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu. "An Antiphishing Strategy Based on Visual Similarity Assessment." *IEEE Educational Activities Department Piscataway.* NJ, USA: IEEE, 2006. 58-65.

Ludl, Christian , Sean Mcallister, Engin Kirda, and Christopher Kruegel. "On the Effectiveness of Techniques to Detect Phishing Sites." *The 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA '07.* Springer-Verlag Berlin, Heidelberg: Springer Berlin / Heidelberg, 2007. 20-39.

Malwarebytes. *hoHosts.* 2005. www.hosts-file.net (accessed January 13, 2012).

Mannan, M, and P.C. van Oorschot. "Using a personal device to strengthen password." *The 11th International Conference and 1st International Workshop on Usable Security, USEC 2007.* Trinidad and Tobago: Springer Berlin Heidelberg, 2007. 88-103.

Manning, Christopher D, Prabhakar Raghavan, and Hinrich Schütze. *Introduction to Information Retrieval.* Cambridge University Press, 2008.

MarkMonitor. *MarkMonitor.* 1999. https://www.markmonitor.com/ (accessed January 14, 2013).

McAfee. *SiteAdvisor.* 1987. http://www.siteadvisor.com/ (accessed December 19, 2011).

MessageLabs. *The MessageLabs Intelligence Annual Security Report: 2009 Security Year in Review.* 2009. http://www.symantec.com/connect/blogs/messagelabs-intelligence-annual-security-report-2009-security-year-review (accessed May 8, 2013).

Microsoft, Support-. *Microsoft IE 9 anti-phishing.* 2012. http://support.microsoft.com/kb/930168 (accessed December 19, 2012).

Ming, Q., and Y. Chaobo. "Research and Design of Phishing Alarm System at Client Terminal." *IEEE - Asian-Pasific conference on services computing, APSCC'06.* Asian, 2006. 597-600.

Miyamoto, Daisuke , Hiroaki Hazeyama, and Youki Kadobayashi. "An Evaluation of Machine Learning-based Methods for Detection of Phishing Sites." *Australian Journal of Intelligent Information Processing Systems*, 2008: 54-63.

Mizuno, Shintaro, Kohji Yamada, and Kenji Takahashi. "Authentication using multiple communication channels." *The 2005 Workshop on Digital Identity Management.* Fairfax, VA, USA: ACM, 2005. 54-62.

Neil, Chou, Robert Ledesma, Yuka Teraguchi, and Dan Bon. "Client side defense against web based identity theft." *The 11th Annual Network and Distributed System Security Symposium, (NDSS '04).* San Diego: SpoofGuard, 2004. 143-159.

Netcraft Toolbar. *Netcraft.* 1995. http://toolbar.netcraft.com/ (accessed December 19, 2011).

Ohaya, Charles. "Managing Phishing Threats in an Organization." *The 3rd Annual Conference on Information Security Curriculum Development.* New York, NY, USA: ACM, 2006. 159-161.

OpenDNS. 2006. http://www.opendns.com/ (accessed February 12, 2012).

Oxford Dictionaries. 1990. http://www.oxforddictionaries.com/definition/english/phishing (accessed October 13, 2012).

Pan, Ying, and Xuhua Ding. "Anomaly Based Web Phishing Page Detection." *The 22nd Annual Computer Security Applications Conference, ACSAC.* Miami Beach, Florida, USA.: IEEE, 2006. 381-392.

Panda Security SL. 1990. http://www.pandasecurity.com/uk/ (accessed Januady 10, 2011).

PhishTank. 2006. http://www.phishtank.com/ (accessed March 12, 2011).

Quinlan, J R. "Improved use of continuous attributes in C4.5." *Journal of Artificial Intelligence Research*, 1996: 77-90.

Rasmussen, Rod, and Greg Aaron. *Global Phishing Survey: Trends and Domain Name Use 2H2009.* Lexington, MA, 2010.

Ronald, Dodge Jr C, Carver Curtis, and Ferguson J Aaron. "Phishing for user security awareness." *Computers & Security* 26, no. 1 (2007): 73-80.

Ronda, Troy, Stefan Saroiu, and Alec Wolman. "iTrustPage: A User-Assisted Anti-Phishing Tool." *The 3rd ACM SIGOPS/ EuroSys European Conference on Computer Systems 2008.* New York, NY, USA ©2008: ACM, 2008. 261-272.

Ross, Blake , Collin Jackson, Nick Miyake, Dan Boneh, and John C Mitchell. "Stronger Password Authentication Using Browser Extensions." *The 14th conference on USENIX Security Symposium, SSYM'05.* Baltimore,USA.: USENIX Association, 2005. 2.

RSA. *RSA SecurID.* 1982. http://www.rsa.com/node.aspx?id=1159 (accessed January 5, 2012).

Sadeh, N, A Tomasic, and I Fette. "Learning to detect phishing emails." *The 16th International Conference on World Wide Web.* New York,NY, USA., 2007. 649-656.

Salem, O, Hossain Alamgir, and M Kamala. "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks." *The 10th International Conference in Computer and Information Technology.* University of Bradford, Bradford, UK., 2010. 1418-1423.

Sanglerdsinlapachai, Nuttapong, and Arnon Rungsawang. "Using Domain Top-page Similarity Feature in Machine Learning-based Web." *Third International Conference on Knowledge Discovery and Data Mining.* IEEE, 2010. 187-190.

Schneier, Bruce. "Inside risks: semantic network attacks." *Magazine Communications of the ACM.* 143, no. 12 (2000): 168.

Seltzer, Larry. *betanews.* 2011. http://betanews.com/2011/06/30/phishers-have-found-a-new-use-for-google-docs-stealing-your-identity/ (accessed October 20, 2012).

Sharifi, M, Iran Univ. of Sci. & Technol, and S H Siadati. "A phishing sites blacklist generator." *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on.* Doha: IEEE, 2008. 840 - 843.

Sheng, Steve , et al. *Anti-Phishing Phil.* 2007. http://cups.cs.cmu.edu/antiphishing_phil/ (accessed December 11, 2011).

Sheng, Steve , Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions." *The 28th International Conference on Human Factors in Computing Systems, CHI '10.* New York, NY, USA: ACM, 2010. 373-382.

Sheng, Steve, Brad Wardman, Gary Warner, Lorrie Faith Cranor, Jason Hong, and Chengshan Zhang. "An Empirical Analysis of Phishing Blacklists." *The 6th Conference on Email and Anti-Spam, CEAS'09.* CA, USA, 2009.

Sodiya, S, S Onashoga, and B Oladunjoye. "Threat Modeling Using Fuzzy Logic Paradigm." *Informing Science: International Journal of an Emerging Transdiscipline.* 4, no. 1 (2007): 53-61.

spoofstick. 2005. http://www.spoofstick.com/ (accessed March 19, 2012).

Sullins, Lauren L. "Phishing for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft." *Emory International Law Review* 20 (2006): 397-433.

Symantec Corporation. *Internet Security Threat Report 2013.* Symantec Corporation, 2013.

Symantec. *Verisign Authentication Services.* 1982. http://www.verisign.com/ (accessed December 19, 2011).

Thabtah, F, C Peter, and Y Peng. "MCAR: Multi-class Classification based on Association Rule." *The 3rd ACS/IEEE International Conference on Computer Systems and Applications.* 2005. 33.

The Apache SpamAssassin Project. *SpamAssassin.* 1995. http://spamassassin.apache.org/ (accessed January 20, 2012).

TREND MICRO. *Threat Reports.* 2013. http://www.trendmicro.com/us/security-intelligence/research-and-analysis/index.html (accessed May 2013, 20).

TRUSTe Co. *TRUSTe.* 1997. http://www.truste.com/ (accessed April 1, 2012).

W3C. 2003. http://www.w3.org/TR/DOM-Level-2-HTML/ (accessed December 2011).

Watson, David, Thorsten Holz, and Sven Mueller. "Behind the Scenes of Phishing Attacks." *Know your Enemy: Phishing.* 2005. http://www.honeynet.org/book/export/html/87 (accessed January 17, 2012).

Wenyin, Liu , Guanglin Huang, Liu Xiaoyue, Zhang Min, and Xiaotie Deng. "Detection of Phishing Webpages based on Visual Similarity." *the 14th international conference on World Wide Web.* New York, NY, USA: ACM, 2005. 1060-1061.

Witten, Ian, H, and Eibe Frank. *Data mining: practical machine learning tools and techniques with Java implementations.* New York, NY, USA: ACM, 2002.

WOT Inc. *Web of Trust.* 2006. http://www.mywot.com/ (accessed January 24, 2012).

Wu, M., R. C. Miller, and S. L. Gar. "Do security toolbars actually prevent phishing attacks?" *The SIGCHI conference on Human Factors in Computing Systems.* NY, USA.: ACM, 2006. 601-610.

Wu, Min, Robert C. Miller, and Greg Little. "Web wallet: Preventing phishing attacks by revealing user intentions." *In Proceedings of the Symposium on Usable Privacy and Security (SOUPS).* New York, NY, USA: ACM, 2006. 102-113.

Yossi, Rubner, Carlo Tomasi, and J Guibas Leonidas. "A Metric for Distributions with Applications to Image Databases." *The Sixth International Conference on Computer Vision ICCV.* Bombay: IEEE Computer Society, 1998. 59-66.

Yu, Weider D., Shruti Nargundkar, and Nagapriya Tiruthani. "A Phishing Vulnerability Analysis of Web Based Systems." *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on.* San Jose, CA: IEEE, 2008. 326-331.

Yue, Chuan , and Haining Wang. "Bogusbiter: A transparent protection against phishing attacks." *ACM Transactions on Internet Technology - TOIT* (IEEE) 10, no. 2 (2010): 1-31.

Zhang, Yue , Jason Hong, and Lorrie Cranor. "CANTINA: A Content-Based Approach to Detect Phishing Web Sites." *The 16th World Wide Web Conference.* Banff, AB, Canada.: ACM, 2007. 639-648.