Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Phishing environments, techniques, and countermeasures: A survey

Ahmed Aleroud [a,*], *Lina Zhou* [b]

[a] *Yarmouk University, Jordan*

[b] *University of Maryland, Baltimore County, MD, USA*

ARTICLE INFO

Article history:
Received 11 February 2017
Received in revised form 19 March 2017
Accepted 10 April 2017
Available online 17 April 2017

Keywords:
Phishing
Social engineering
Phishing detection
Mobile phishing
Social networks phishing
Honeypots
Ontology

ABSTRACT

Phishing has become an increasing threat in online space, largely driven by the evolving web, mobile, and social networking technologies. Previous phishing taxonomies have mainly focused on the underlying mechanisms of phishing but ignored the emerging attacking techniques, targeted environments, and countermeasures for mitigating new phishing types. This survey investigates phishing attacks and anti-phishing techniques developed not only in traditional environments such as e-mails and websites, but also in new environments such as mobile and social networking sites. Taking an integrated view of phishing, we propose a taxonomy that involves attacking techniques, countermeasures, targeted environments and communication media. The taxonomy will not only provide guidance for the design of effective techniques for phishing detection and prevention in various types of environments, but also facilitate practitioners in evaluating and selecting tools, methods, and features for handling specific types of phishing problems.

1. Introduction

Phishing is an attack wherein the attacker exploits social engineering techniques to perform identity theft. Phishing traditionally functions by sending forged e-mail, mimicking an online bank, auction or payment sites, guiding users to a bogus web page which is carefully designed to look like the login to the genuine site (Inomata et al., 2005; Jakobsson and Myers, 2006; Kumar, 2005; Tally et al., 2004; Wu et al., 2006a). Phishing aims to collect sensitive and personal information such as usernames, passwords, credit card numbers, and even money by impersonating a legitimate entity in the cyber space. Ramzan and Wüest (2007) characterize a phishing attack in three ways: 1) a legitimate entity must be spoofed; 2) the spoofing process must involve a website, which distinguishes itself from some scams (e.g., muling); and 3) sensitive information about the entity must be solicited.

Phishing attacks, which are prevalent, could have serious consequences for their victims, such as the loss of intellectual property and sensitive customer information, financial loss and the compromise of national security (Ramzan and Wüest, 2007), as well as general weakening trust (Litan, 2005; Sullins, 2006). According to CYREN report, the first quarter of 2015 witnessed a 51 percent increase in phishing sites (Mclean, 2015). RSA identifies 52,554 phishing attacks in April, 2014, marking a 24% increase from the previous month. Phishing, including spear phishing, has become such a serious problem that

[*] *Corresponding author.*
E-mail address: ahmed.aleroud@yu.edu.jo (A. Aleroud).

[1] https://www.phishtank.com/.

http://dx.doi.org/10.1016/j.cose.2017.04.006

researchers and practitioners strive to look for an effective way to mitigate its impact.

1.1. Scope challenges

Phishing detection remains a challenging problem. This is primarily because phishing is considered a semantics-based attack, which particularly exploits human vulnerabilities, but not system vulnerabilities (Wu et al., 2006b), despite the fact that protection protocols increase the probability of phishing attacks (Alsaid and Mitchell, 2006; Bose and Leung, 2008; Oppliger and Gajek, 2005). Phishing belongs to unsolicited bulk email like spam, but the latter is distinctly different in that it is mainly utilized for marketing or advertising products (Toolan and Carthy, 2010) (see Appendix A). This current survey is focused on phishing. For email phishing, phishers utilize Social Engineering and identity impersonation through spoofing to steal legitimate users' passwords for fraudulent purposes (Jakobsson and Soghoian, 2009).

Social engineering relies heavily on human interaction and often involves using psychological tricks aimed at making victims agree to things they would not have done normally. By exploiting humans' limited security knowledge or awareness, phishers deceive online users into disclosing their sensitive information (e.g., passwords, credit card numbers, and other sensitive information; Gouda et al., 2007), or inject suspicious content into their systems (Berghel et al., 2007; Cova et al., 2008; Jakobsson and Myers, 2006). The key to traditional phishing is to attract users to visit a bogus website, which can be effectively achieved through a fake email. The weaknesses in web applications fuel phishing attempts; for example, attackers can easily modify the "FROM" address in an email to make it look like coming from a legitimate source. Thus, compared to the creation of viruses, worms or other exploits, some phishing attempts are considered simple. However, phishing attack techniques are evolving and becoming more sophisticated (Irani et al., 2008). There has been an increasing trend of launching new phishing attacks through emerging technologies such as mobile and social media (Egele et al., 2013; Marforio et al., 2015). The prevalent use of social media provides fertile ground for phishing attacks due to increasing sharing of personal information but little awareness and action of protecting the information (Borsack and Lifson, 2010). Studies show that phishing attacks increasingly focus on social networks because they offer the greatest possibilities for success (Lemos, 2014). Recent statistics shows that mobile users around the globe download over 67 million apps every day. The large numbers of mobile users and apps are not matched with high levels of security-awareness, and it is a matter of time before online threats such as phishing become a reality on mobile devices (Kessem, 2012). Trend Micro already identified 4000 phishing URLs designed for the mobile web (Pajares and Abendan, 2013). Other channels have also been exploited for phishing such as *Voice over IP* (VoIP) technology (Gupta et al., 2015). For instance, the frequency of unwanted calls has increased at an alarming rate. Telephone phishing can be made at little or no cost at a scale and in an automated fashion similar to email phishing. Therefore, the Federal Trade Commission (FTC) has received millions of complaints from citizens about such unwanted and fraudulent calls. Some studies show that the economics of phishing is far worse than it appears. Rather than sharing a fixed pool of dollars, phishing is subject to the tragedy of the commons – the pool of dollars shrinks as a result of the efforts of phishers (Herley and Florêncio, 2009). One limitation of these studies is that they overlooked uptime – an important metric of the damaging effect of phishing attacks and the success of counter measures (Aaron and Rasmussen, 2013) (see Appendix B). Based on a statistics for different time periods between 2008 and 2013 by anti-phishing Working Group, the average uptime ranges between 23 and 72 hours (Aaron and Rasmussen, 2013). Additionally, at hour zero, only fewer than 20% of phishing attempts were identified by blacklists, and only 47~87% of those phish got updated into the blacklist after 12 hours of occurrences (Sheng et al., 2009). These data suggest that existing countermeasures remain ineffective and insufficient for detecting phishing attacks. Therefore, providing a systematic survey of countermeasures and phishing techniques can not only help to understand the state of phishing practice but also inform future design of anti-phishing mechanisms.

1.2. Contributions

This survey provides a system review of extensive research on phishing techniques and countermeasures. Previous surveys and taxonomies either concentrate on one specific aspect of phishing such as anti-phishing tools (Abbasi et al., 2010; Zhang et al., 2011a) or fail to provide an integrated overview of research approaches to various phishing techniques (Huajun et al., 2009; Ollmann, 2007a; Wetzel, 2005). The taxonomy proposed in this research is multi-dimensional, which distinguishes itself from the previous ones that are focused on a single dimension. In addition, the phishing environment covered in existing taxonomies is limited to traditional channels such as e-mails and spoofed websites.

However, emerging communication channels in support of phishing, such as mobile apps, online social networks, and Instant Messaging (IM) applications, are yet to be considered by existing taxonomies and surveys (Hong, 2012). To address these limitations, we propose a phishing taxonomy that addresses phishing environments, techniques and corresponding countermeasures. We identify the dimensions of phishing via the process lens. Particularly, we identify the characteristics of phishing attacks in emergent communication media. Moreover, we analyze anti-phishing techniques in relation to the communication media for the first time. In view of the significant practical implications of phishing detection, we introduce a comprehensive comparison between research anti-phishing tool and another comparison between commercial anti-phishing tools. Additionally, we applied the dimensions to analyze anti-phishing tools, and ranked the techniques based on their performance. The analyses revealed several new categories of countermeasures that are missing from the existing taxonomies, including human users, ontology, and search engine-based. For instance, human users play an important part in the loop of phishing attacks, who can potentially serve as the most effective line of defense. Further, we identified a number of phishing problems that require future research and suggested possible solutions.

The rest of this survey is organized as follows. The next section provides a critical review of extant phishing taxonomies.

Table 1 – Comparison of existing phishing taxonomies.

	Wetzel (2005)	Jakobsson and Myers (2006)	Ollmann (2007a)	Huajun et al. (2009)	Zhang et al. (2011a)	Almomani et al. (2013)
Communication media	√		√		√	
Attack initialization techniques		√	√	√		
Data collection techniques		√	√			
System penetration techniques			√			
Target environment						
Countermeasures	√	√		√	√	√

In Section 3, we first examine phishing from the process perspective. Based on each activity of the process, we propose one or more taxonomy dimensions. We introduce our proposed taxonomy and its dimensions in Section 4. In Section 5 we provide a comprehensive review of extant anti-phishing techniques and discuss future research issues in phishing detection. The final section concludes the survey.

2. Existing phishing taxonomies

We adopted the snowballing approach for article selection. The literature search revealed several existing phishing taxonomies and anatomies. Wetzel (2005) provides an anatomy of phishing attacks, but it ignores attack vectors and the environment where attacks occur. Ollmann (2007a) categorizes attack initialization techniques, victim data collection techniques, and the communication media utilized in attack initialization; however, the study makes no attempt at anti-phishing techniques. Zhang et al. (2011a) solely focus on countermeasures and classified them based on where the measures were applied. They also ignore the effect of communication media in their discussion of client–server authentication techniques. Similarly, Huajun et al. (2009) classify anti-phishing strategies into three categories based on the system architecture: server-side, browser-side, and online training anti-phishing strategies. However, the classification of strategies is too generic to be made operational. Almomani et al. (2013) provide a countermeasure classification schema in e-mail but ignore other attack environments. Jakobsson and Myers (2006) provide a comprehensive view of technological countermeasures for phishing without taking into account emergent communication media and evolving attacking techniques over the past decade (see Appendix F). While Jakobsson and Myers (2006) were the first to comprehensively study the problem of phishing and provide a framework for studying the attack and its defenses, the current research analyzes countermeasures with respect to phishing techniques instead of the attack phases. Our literature review reveals that existing studies on countermeasures have focused on phishing problems in specific communication media without systematically examining the distribution of countermeasure categories among communication media. For instance, Chandrasekaran et al. (2008) classify anti-phishing approaches in website communication media into three categories, including browser plug-ins and anti-phishing toolbars, digital signing and trust propagation schemes, and content-based detection techniques. The classification not only ignores countermeasures in other types of media (e.g. e-mail, Online Social Networks), but also overlooks the dependency of countermeasures on the communication environment.

For instance, browser toolbars are not applicable for Voice over IP phishing, as prevention of the latter type of attack requires multiple layers of protection (Griffin and Rackley, 2008). A summary of the coverage of existing phishing taxonomies is shown in Table 1. The current survey aims to address the limitations of previous taxonomies by proposing a new one.

3. The phishing process

To better inform the design of our phishing taxonomy, we anatomize phishing via the process lens. The phishing attack process consists of five phases: *attack planning*, *attack setup*, *attack execution*, *fraud*, and *post attack phases* (Wetzel, 2005).

Similarly, Jakobsson and Myers (2006) divide the phishing process with reference to the information flow of a phishing attack into fundamental step-by-step phases (see Appendix F). They include attack preparation, sending a malicious payload via some propagation vector such as a deceptive email, eliciting the user's reaction which may subject his sensitive information to being stolen, prompting user for his confidential information, compromising the confidential information, transmitting the information to phisher, impersonating the user, and finally eliciting monetary gain by a fraudulent party. Based on the similarities in terms of involved activities (Abad, 2005; Jakobsson and Myers, 2006; Tally et al., 2004), phishing attacks undergo three major phases – *preparation*, *execution*, and *results exploitation* (see Fig. 1). In this study, we refine each phase into its sub-processes by incorporating new phishing trends; for instance, an attacker may perform feasibility analysis that compares alternative communication media to be used to carry out a specific attack material.

- *Attack Preparation*: Attackers initially select *Communication Media* for carrying out the attack. The most frequently targeted medium is e-mail, but there are other targets such as Instant Messengers (IM), mobile apps, social and voice media.

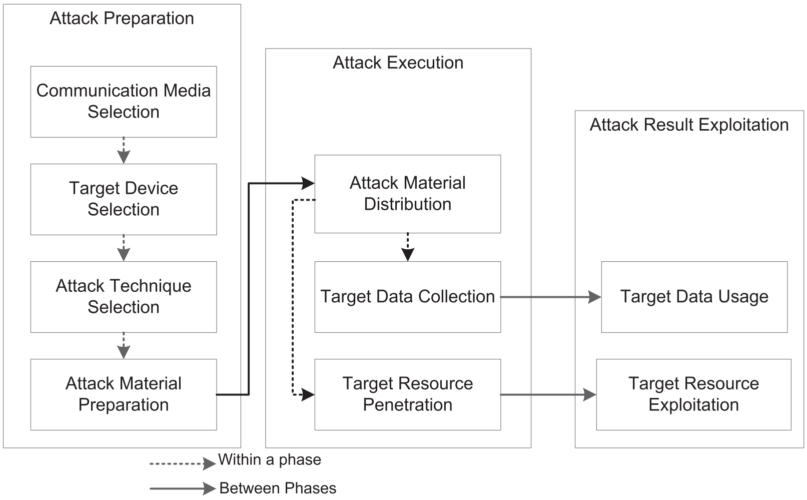

Attack Preparation
Communication Media Selection
Target Device Selection
Attack Technique Selection
Attack Material Preparation
Attack Execution
Attack Material Distribution
Target Data Collection
Target Resource Penetration
Attack Result Exploitation
Target Data Usage
Target Resource Exploitation
Within a phase
Between Phases

Fig. 1 – Phishing process phases.

In addition, the attackers also select *Target Devices* (e.g. smart phones). *Communication Media* and *Target Devices* comprise the environment in which phishing attacks are initialized. Next, the attackers select *attacking techniques*, such as website spoofing, and finally proceed with *attack material preparation* for future distribution. Attack preparation can be performed either manually or with aid of some automated tools such as phishing kits (Sponchioni, 2015). Phishing kits may include pre-designed webpages for popular companies, suspicious scripts for collecting user credentials, and hosting mechanisms for phishing sites. The preparation of attack material depends on the targeted environment. For instance, in case of e-mail, the attack material would be the e-mail text or any other suspicious code embedded in the e-mail.

- *Attack Execution*: This phase consists of three sub-processes – *attack material distribution*, *target data collection*, and *target resource penetration*. The attack material can be distributed to one or more victim depending on the intended scope of attack. The material distribution strategy also depends on the attack material and target device type. For instance, if the attack material is in text and the target is a mobile device (van der Merwe et al., 2005a, 2005b), wireless networks would be the preferred choices (Martinovic et al., 2007). The target's data collection will not start until the victim responds to the sent material as expected by the phishers. Finally, the attackers may compromise system resources to ease the process of collecting user information via means such as injecting client-side script into webpages (Jakobsson et al., 2007).
- *Attack Results Exploitation*: This is the last attack phase, when the data collected from the target victim, such as his/her credentials, are used, usually to impersonate the victim.

Based on the in-depth analysis of the phishing process, we identified four dimensions of phishing – *Communication Media*, *Target Environments*, *Attack Techniques* and *Countermeasures*.

4. A new phishing taxonomy: an integrated view of phishing

Drawing upon existing taxonomies and the process models of phishing attacks, we propose a phishing taxonomy, as shown in Fig. 2.

In the taxonomy, a phishing attack is described in four dimensions: *Communication Media*, *Target Environments*, *Attack Techniques*, and *Countermeasures*. We elaborate on the first three dimensions in this section, and discuss countermeasures separately in the subsequent section.

4.1. *Communication media*

Communication Media are the media of human interaction, with applications targeted by attacks. Communication also covers any intermediate interfaces with which human users interact (e.g. fake webpages).

We identify seven types of communication media from the literature, *E-mails*, *Websites*, *IM*, *Online Social Networks*, *Blogs and Forums*, *Mobile*, and *Voice over IP*. Among them, emails and websites are most frequently studied.

- *Emails*. A common phishing practice in emails is asking users to update their account information. However, when users hover over the link, it does not lead to the organization's actual website but a phishing trap site instead. A phishing email, disguised as an official email from PayPal, is illustrated in Fig. 3.
- *Websites*. The spoofed e-mail may then utilize social engineering and contextual information about targets to direct users to a bogus webpage (Jakobsson and Myers, 2006). A fake webpage and its corresponding legitimate version are illustrated in Fig. 4. Although the two pages are visually similar, the faked version (Fig. 4a) differs from the legitimate one (Fig. 4b) in several aspects: 1) its URL contains HTTP instead of HTTPS, and only the latter transfers data through a secured connection that encrypts data by a secure

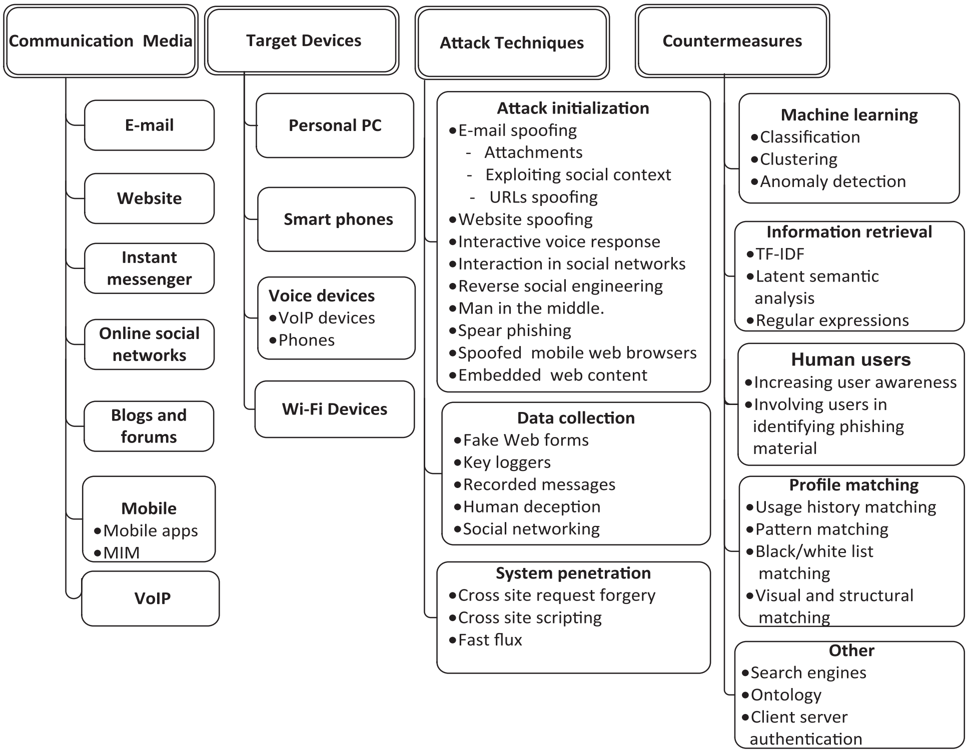
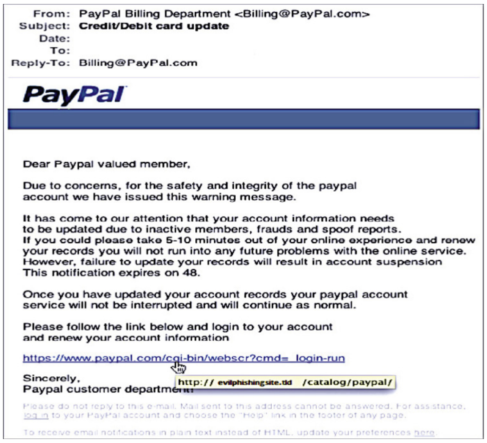


Fig. 2 – The proposed phishing taxonomy.

certificate known as SSL (Secure Sockets Layer). The encryption prevents third-parties from eavesdropping on communications to and from the server; 2) a padlock icon at the beginning of the URL is missing, indicating that the website being accessed is not secure; and 3) the URL itself contains a fake domain (e.g., gmall-imp-info2.com) which is not the real domain.

- *IM.* In IM, phishing attacks are usually accomplished through suspicious URLs (Ying and Xuhua, 2006). In addition, a phisher tries to collect password and security related information through asking questions by pretending to be a trustworthy chat-mate through voice chat, text chat or a combination of both.

  An empirical study of the spread of some "worms" over the social graph of IM users reveals that over 14 million distinct users clicked on suspicious URLs over a two-year period. In addition, 95% of users who clicked on the URLs became infected with malware (Moore and Clayton, 2015). Among the 50~110 malicious URLs gathered per day using a honeypot, 93% of phishing sites were not found in popular blacklists.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date:
To:
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal
account we have issued this warning message.

It has come to our attention that your account information needs
to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew
your records you will not run into any future problems with the online service.
However, failure to update your records will result in account suspension
This notification expires on 48.

Once you have updated your account records your paypal account
service will not be interrupted and will continue as normal.

Please follow the link below and login to your account
and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http:// evilphishingsite.tld /catalog/paypal/

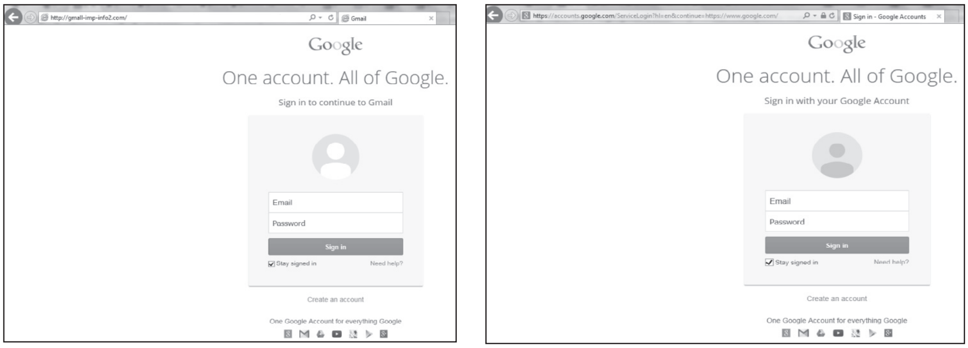
Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Fig. 3 – An illustration of phishing e-mail.

- *Online Social Networks* (e.g. Facebook and Twitter) have witnessed a rapid growth of phishing attacks for several reasons (Yu et al., 2008): 1) ease of impersonating profiles, 2) users' willingness to trust, and 3) popularity of social networking sites. One recent study (Stern, 2014) shows that, 22% of phishing scams on the web target Facebook. Additionally, the phishing sites imitating social networking websites comprised over 35% of all cases that triggered anti-phishing components.
- *Blogs and Forums.* According to Microsoft security and safety center (Microsoft, 2016a), news groups and online-ads scams are exploited in the event of a natural disaster, or a national election. Faked e-card, online job-hunting scams, and donation scams are some examples of phishing attacks that target blogs and forums. For instance, online job-hunting scams are used to collect the credentials of job hunters. In general those ads represent the names of spoofed organizations and are displayed on various job search sites. If a user shows an interest in an ad, he is either requested to provide his credentials, or depending on his interaction, his


http://gmall-imp-info2.com/
Gmail
Google
One account. All of Google.
Sign in to continue to Gmail
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google
https://accounts.google.com/ServiceLogin?hl=en&continue=https://www.google.com/
Sign in - Google Accounts
Google
One account. All of Google.
Sign in with your Google Account
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google

(a) (b)

Fig. 4 – (a) A faked page (Source: phish tank).[1] (b) A legitimate page.

credit card would be charged for a fake job service. Donation phishing exploits social, political, or natural events to request donations using a well-known identity. When users interact with those phishing attempts, they will also be asked to provide information of their credit cards.

- *Mobile Platform*. When using the Internet or downloading mobile apps, mobile users may be targeted by phishing attacks similar to those from personal computers (PC). Phishing attempts on mobile devices are harder to identify by users, because it is difficult to discern whether a page is legitimate or not when looking at devices with small screens where the complete URL is not visible (Canova et al., 2015). *Mobiles Apps* and *Mobile Instant Messaging* (*MIM*) (Goel et al., 2014) are the main media utilized by attackers to initialize mobile phishing attempts. In *Mobile Apps*, the attackers redirect users to fake apps interfaces through which users provide their sensitive information (Felt and Wagner, 2011). Marforio et al. (2015) classify attacks on *Mobile Apps* into five types – *similarity*, *forwarding*, *background*, *notification*, and *floating attacks*.

In *similarity attack* the phishing app has UI features that are similar to the legitimate one. This category of attacks has been reported on both Android and iOS devices. In *forwarding attack*, the attackers take the advantage of the forwarding functionality of Android apps. For instance, a suspicious app may ask the user to share a high score in a game on a social networking site and access the network app through a button on the screen. When the user taps the button, the suspicious app does not initiate the social network app, but instead launches the phishing app. In *background attack*, the phishing app functions in the background and uses Activity Manager on Android to control other running apps. When the user launches the legitimate app, the phishing app triggers itself to the foreground and displays a phishing UI. In *notification attacks*, the attacker presents a spoofed notification and prompts the user to enter his account information. In *floating attacks*, the attackers take advantage of Android functionalities that allow an app to draw an activity on top of the app in the foreground. For instance, a phishing app that has the system alert window permission can present an input field on top of the password input field of the legitimate app. The UI of the legitimate app that remains visible to the user has no way to detect the new input field. When the user taps on the password field, the focus is transferred to the phishing app which obtains the password entered by the user.

- *Voice over IP* (aka Vishing; Ollmann, 2007b) attacks, such as *Automatic Dialing*, *Manual Dialing*, and *Telemarketing Calls*, are utilized to guide callees to a service which does not exist in reality. Overall, vishers exploit vulnerabilities of the Voice over IP infrastructure. Vishing attacks are evolving owing to the growth of mobile technologies, Voice over IP protocols, and the automated Interactive Voice Response (IVR) services (Griffin and Rackley, 2008). Some Security Agencies in the US have identified several techniques that are used to implement vishing attacks (FBI, 2010). Initiating vishing requires relatively less effort compared to other environments. Such attacks are conducted by attackers who utilize vulnerabilities in the integration mechanism between Digital Private Branch Exchange (PBX) tools and Voice over IP technology. If those vulnerabilities exist, the system can be initiated as an auto dialer and it may generate spoofed calls to hundreds of customers on hourly basis. One variant of telemarketing calls in vishing is the callee being directed to dial costly numbers, where he provides his credentials. Another variant is the voice pharming attack (Wang et al., 2008), where an active adversary in the Voice over IP along with one or more accomplices subvert the victims' Voice over IP calls and divert them to a bogus IVR or representative. The voice pharming attack eliminates the bogus phone number used in vishing via transparent call diversion, just as pharming attack eliminates the bogus URL used in phishing via transparent web traffic diversion (Wang et al., 2008).

4.2. *Target environments*

The *target environment* is the physical device by which victims interact online. Device type plays a major role in selecting attacking strategies. For instance if the attacker wants to deceive mobile users he/she has to adapt specific techniques for particular types of devices (e.g. mobile devices; Felt and Wagner, 2011). We classified *Target Environments* of phishing attacks into three categories: *personal computers (PC)*, *smart devices*, and typical *voice devices* such as *desk* or *soft phones*. The targeted environments impose constraints on the types of attacks that could be initiated. For instance, while it is common to attack PCs through spoofed websites, it requires more sophisticated techniques to fake mobile web browsers and mobiles apps (Felt and Wagner, 2011). Likewise, Griffin and Rackley (2008) discuss several steps to initialize Voice over IP (Vishing) attacks. Initially, the attacker must gain unauthorized access to a computer with Internet. Once the attacker has control of host, a Digital Private Branch Exchange (PBX) needs to be installed (e.g. Skype).

Lastly, an attacker needs the ability to record the phone conversation. This functionality is built into most digital PBX software. An attacker cannot utilize an existing phone number but can configure his own number to reflect the entity of his choice. He could employ any number not in use, and make it appear to be a trusted organization calling from that number. This simple configuration within the PBX software could be very convincing to potential victims. At some point the attacker can expand criminal activities by crossing over to the analog phone world. This can be accomplished by purchasing a hardware device that bridges the digital session initiation protocol (SIP) to the public switched telephone network (PSTN).

Phishing attacks have recently targeted the Wi-Fi networks (Song et al., 2010). The attack is initialized through attacker's association with the Wi-Fi clients unknowingly. The users are presented with an authentication interface that looks legitimate (e.g., an interface that is similar to the one used by a legitimate Access Point (AP)). The interface is usually a login page for a free Internet service (e.g., Fake captive portals in airports, hotels, universities, etc.). Information about the targeted network such as the web browser and the operating system of the victim, the encryption type, and the MAC address of the AP are collected from the Beacon Frame and the User-Agent header (application layer). By knowing the router manufacturer, a fake router configuration pages can be presented to the victims.

Target environments have social as well as technical implications for phishing. For instance, mobile users have greater likelihood to fall to phishing attacks than PC users (Niu et al., 2008). Mobile devices are always on and in most cases physically close-by. Their owners tend to check their communications close to real time, and thus become victimized by phishing attacks. Additionally, mobile users are accustomed to entering their credentials into simple interfaces on their devices; in fact, 40% of smartphone users enter passwords into their phones at least once a day. Although modern mobile devices come with first-class web browsers that rival with their desktop counterparts in power and popularity, mobile browsers are particularly susceptible to attacks on web authentication, such as phishing or Touchjacking (Luo et al., 2012).

Baset (2017) introduces a new form of social engineering attacks which utilizes Quick Response Code Login Jacking (QRLJacking) to initialize phishing on the pages that rely on the "Login with QR code" feature such as mobile social networks (Guo et al., 2016). In its simplest form, the victim scans the attacker's QR code instead of the real one, which results in session hijacking. The attack is executed in several steps, which include cloning the Login QR Code into a phishing website, sending the phishing page to the victim, and then scanning the QR Code by the victim using a Mobile App. When these steps are successful, the service exchanges all victim's data with the attacker's session. Braun et al. (2014) have shown that existing countermeasures from desktop computers cannot be easily transferred to the mobile world. However, such the significance of device type on the probability of phishing attack success has not yet been studied.

4.3. *Attack techniques*

Based on the purpose of the techniques, we group attack techniques into three categories: *attack initialization*, *data collection*, and *system penetration*.

4.3.1. *Attack initialization techniques*

Attack initialization techniques, such as those analyzing the social context of the victim, are used in preparing attack material (Jagatic et al., 2007). Attack initialization techniques are categorized by two types: *technical* and *behavioral*. A predominant method in the technical category involves embedding a suspicious URL into spoofed emails (Drake et al., 2004; Ollmann, 2007b). Social engineering exemplifies this behavioral category which is aimed at deceiving users into disclosing their personal information (Chandrasekaran et al., 2008; Drake et al., 2004; Felten et al., 1997; Guan et al., 2009).

We identify several techniques for attack initialization, such as *Spoofed URLs*, *Bogus IVR*, *Social Networking*, *Man in the Middle Attack (MITM)*, *Spear Phishing*, *Spoofing Mobile Browsers*, and *Embedded Web Contents*.

- *Spoofed URLs* most likely target e-mail users. Sample URL spoofing techniques include *bad domain name*, *shortened URL*, *host name obfuscation*, and *encoded URL obfuscation* (Berghel et al., 2007) (see a summary in Appendix G).
- *Bogus IVR* attacking techniques are utilized to initialize voice-based phishing attacks (Wang et al., 2008).
- *Social Networking Techniques* are used in social network phishing. Phishers can gain control of a user's email or social networking account in a number of ways.
  - ■ *First*, sending a genuine-looking email or message from the site that requests the user to "confirm" the username and password for his/her social networking accounts via an attached URL (Wüest, 2010). Once the phisher gains control of the user's account, he/she can change the password. Phishers use this information to send bogus emails or messages that look like they are from the registered user to request money or gain access to other users' accounts.
  - ■ *Second*, the creation of fake profiles, which appear to be from friends of the victims, can be sent to users as spoofed messages (Kontaxis et al., 2011).
  - ■ *Third*, attackers use social networking walls or official pages to post phishing URLs (Chen et al., 2014; Liu et al., 2011; Navarro and Jasinski, 2014)
  - ■ *Fourth*, Reverse Social Engineering (Abawajy, 2014; Irani et al., 2011; Krombholz et al., 2015), one of the new phishing techniques that target social networks. It is implemented through exploiting friends' recommendation list to invite victims to add, as friends, the cloned profiles recommended by the social networks; once added by victims, attackers can exploit such friendships to send

messages including information about the victims' social contexts.

- *Man in the Middle Attack (MITM) techniques* (Bicakci et al., 2014; Joshi et al., 2008). In MITM, phishers position themselves between the victim and the legitimate site. As a result, the messages submitted to the legitimate site are passed to phishers instead, and such information usually represents valuable credentials. Although SSL web traffic is generally not vulnerable to *MITM*, a malware-based attack can modify a system configuration to install a trusted certificate authority in which a *MITM* can create its own certificate for any SSL-protected site, decrypt the traffic and extract confidential information, and re-encrypt the traffic to communicate with the other side. There are two main models of *MITM* (Karapanos and Capkun, 2014): MITM + certificate and MITM + key. In MITM + certificate, the attacker holds a valid certificate for the domain of the target web server, binding the identity of the server to the public key, of which he holds the corresponding private key. The attacker, however, has no access to the private key of the target web server. This can happen if the attacker compromises a Certificate Authority (CA) or is able to force a CA issue such a certificate. In MITM + key, the attacker holds the private key of the legitimate server. While it is not easy to compromise the server key, such attacks are feasible, as demonstrated in the Heartbleed vulnerability in OpenSSL, and can be very stealthy, remaining unnoticed.
- *Spear or Organization Phishing*. The technique is an attempt that mainly targets a specific organization in order to collect the credentials of its users, financial, or other sensetive information (Aycock, 2007; Peterson, 2011). Unlike other phishing attemtps, spear phishing attacks require understanding of the organization's context to create effective phishing emails. Thus, spear-phishing is a directed and under-the-radar attack. According to a report by the APWG (Aaron and Rasmussen, 2013), the year of 2011 shows a significant increase in the rate of spear phishing attacks.

  The report also shows that in 2013, the pro-Assad Syrian Electronic Army (SEA) utilized a spear-phishing approach to obtain the credentials of a domain name reseller. Then they redirected the domains of several well-known media channels. While it has been shown that the number of spear phishing attempts has declined in 2014 and 2015 compared to 2013 (73 emails per day compared to 83 per day), this does not necessarily mean that users are more aware about spear phishing (Infosec-Institute, 2015). It mainly indicates that there is a change in the strategies utilized by attackers to create those attempts and the way they select their campaigns.

  Spear phishing attempts target several types of organizations. According to a recent report by Symantec (Nahorney, 2015), the top industries targeted by spear phishing are mainly finance, insurance and real estate. Spear phishing also has high stakes. A recent study shows that the financial benefit of spear phishing attacks tripled while that of conventional phishing attacks dropped by more than half (Caputo et al., 2014) (see summary in Appendix C). Jagatic et al. (2007) also show that using user profiles from online social networks to prepare phishing emails, improves the success rate to 72% from 16% when social context was not utilized.
- *Spoofing Mobile Browsers* and *Embedded Web Contents*, in which the web content is rendered as part of the interface of a mobile app (Felt and Wagner, 2011; Wu et al., 2016). Those attack initialization techniques are mainly applicable to smart devices.

4.3.2. *Data collection techniques*

Techniques used to collect data from victims occur during and after the victim's interaction with attacks material. Victim's data collection techniques are used in gathering user data during and after the victim's interaction with attacks material (Ollmann, 2007a). The data collection can be carried out either *manually* or *automatically*. Automated data collection techniques mainly rely on creating *Fake Web Forms*, *Key Loggers*, *Recorded Messages*, *Automated Social Engineering Bots*, and *Fake Event Invitations* to gather data.

- *Automated data collection*: *Fake Web Forms* are the most commonly used automated technique for data collection in web spoofing (Wenyin et al., 2005). Other techniques such as *Recorded Messages* gather data from user interaction with IVR when attacks are initialized via phones or other Voice over IP attacks (Wang et al., 2008). In social networks, the *public data* about users are utilized to harvest data necessary to initialize social engineering attacks (Huber et al., 2009). Social engineering process generally starts with collecting background information on potential targets. Despite the several online sources that are typically used to collect the information about potential victims, nowadays attackers increasingly exploit user profiles from social networking sites such as Facebook owing to the explosive use of social networking sites. Additionally, social networking sites facilitate automating attacks by providing data in a machine-readable form. Further, online social networks also serve as communication platforms by offering services such as private messaging and chats which can be exploited by *Automated Social Engineering Bots* for data collection (Huber et al., 2009). *Fake Event Invitations* performs by tailoring to the target users' motivations (Ferrara, 2013). For instance, members of LinkedIn (a professional networking site) who identify themselves as business owners send fake event invitations to target users, asking them to provide private information for fake job positions.
- *Manual data collection* is carried out through *Human Deception* or other simpler techniques such as *Relationships within Social Networks*. Human deception collects sensitive data about victims through direct interaction (Dhamija et al., 2006).

4.3.3. *System penetration techniques*

System penetration techniques are used to exploit system resources for facilitating phishing attack initialization (Emigh, 2005; Jakobsson and Myers, 2006). System penetration techniques are in general used along with other types of cyberattacks but not limited to phishing. We identified two main system penetration techniques: *Fast-Flux and Cross Site Scripting*.

- *Fast Flux* (FF). FF is not a direct attack, but rather a DNS-related technique that protects phishing sites from taking down by hiding the hosting machine of phishing websites. DNS-based phishing refers to any form of phishing that tries to spoof the process of finding the real domain name (Jakobsson and Myers, 2006; McGrath et al., 2009; Moore and Clayton, 2007; Zhou et al., 2008) which includes *host files poisoning*, and *polluting the user's DNS cache* with spoofed location. In FF networks, instead of revealing the addresses of the hosting machine of a phishing sites, front-end proxy hosts are used to transmit requests to another server which is the real host of the phishing site (Hsu et al., 2010). As such, several compromised front-end hosts (bots) are needed. In addition, a mapping of the phishing domain name to front-end proxies is performed. To make the process more ambiguous, FF networks perform domain name resolution over a short duration (see Appendix D). This is important in order to avoid tracing the attack back the hosting machine.
- *Content Injection via Cross Site Scripting* (XSS) *and Request Forgery (CSRF)*. XSS can be initialized using different techniques, for instance, the attacker may inject malicious code into a benign website by loading it onto a valid server as part of a client review or a web-based email. Alternatively, the code may be injected into a URL and sent to user as an email (see Appendix E). When the user taps the URL, the content will be transmitted to the benign sever and then returned as part of a request of user credentials (Ramzan, 2010). CSRF is yet another type of injection attacks that can be initiated as part of phishing campaigns. The attacker sends emails to victims to lure them into visiting a web page that is under attacker control (Blatz, 2007; Nagar and Suman, 2016). The attacker hides several executable elements in his page (e.g., Java scripts blocks) which will make a request to the target application. This automatically appends session token to the request when the victim is logged in to the application at that time. The application will automatically perform whatever action the attacker requested.

5. Countermeasures

Countermeasures aim at preventing/detecting attacks before/after victim data are collected/used. We discuss countermeasures for phishing detection and prevention separately in this section. Based on the underlying techniques, we categorize the countermeasures into five major categories – *Machine Learning*, *Text Mining*, *Human Users*, *Profile Matching*, and *Others*. The others category is further broken down into *Ontology*, *Honeypot*, *Search Engine*, and *Client Server-based Authentication*. In addition to countermeasure techniques, we also discuss communication media where the techniques have been applied. Further, we examine the practical application and performance of countermeasures by anti-phishing tools.

5.1. *Machine learning*

This type of approach focuses on applying machine learning and data mining techniques to phishing detection. These related techniques are classified into three main categories: *Classification, Clustering*, and *Anomaly Detection*.

5.1.1. *Classification techniques*

Classification techniques try to map inputs (features or variables) to desired outputs (response) using a specific function. In the case of classifying phishing emails, a model is created to categorize an email into phishing or legitimate by learning certain characteristics of the email. The classification-based countermeasures rely on using labeled datasets of phishing and legitimate instances (e.g. e-mail or webpages). A training model m learns patterns from the training samples using a vector of relevant features $t = |f_1, \ldots, f_n|$, which consists of content and/or URL-based features. Some quality measures are used to assess classification performance of the trained model m on test samples e. Most phishing detection applies statistical classifiers which use function $f(t, \gamma)$ to classify the instances of e in a way that recognizes the relationship between t and e using some optimization criteria, where γ is a vector of adjustable parameters. The values of γ are determined using the selected optimization criteria. Based on types of features that are used to discover phishing (see Appendix H), phishing classifiers can be grouped into three main categories:

- *Classifiers based on URL features* (Bergholz et al., 2008; Bulakh and Gupta, 2016; Cheng et al., 2011; Choi et al., 2011; Garera et al., 2007; Gyawali et al., 2011; Huh and Kim, 2012; Ma et al., 2009; Xiang et al., 2011; Zhang et al., 2011b) such as domain name, IP address characteristics, and geographic properties. URL related features have been used as inputs to several classification techniques for phishing detection, such as Support Vector Machine, Naïve Bayes, and *k*-Nearest Neighbor. Among them, the *k*-Nearest Neighbor produces the best accuracy in one study (Huh and Kim, 2012).
- *Classifiers based on textual features* (Zhang et al., 2007). These approaches examine the content of suspicious material to determine whether it is legitimate or phishing. For instance, the detection of phishing in a website can operate on features extracted from the textual content of the main page, its component files, and DOM structure.
- *Classifiers based on hybrid features* (Aggarwal et al., 2012; Andre et al., 2010; Khonji et al., 2011; Whittaker et al., 2010). Several classifiers are built on hybrid features that are extracted from both content and URL in webpages for phishing detection (Abu-Nimeh et al., 2007; Basnet et al., 2011; Miyamoto et al., 2008). Some methods within this category focus on creating *dynamic*, *adaptive*, or *ensemble classifiers*. Compared with static classifiers, dynamic classifiers are focused on adapting classification rules. L'Huillier et al. (2009) used an online support vector machine approach that utilizes game theory and previous knowledge to create a phishing detection classifier. A similar adaptive topic model based classification has been proposed for detecting phishing in an e-mail environment (André et al., 2010). Sanglerdsinlapachai and Rungsawang (2010) have explored ensemble methods for phishing detection that relies on the decisions of more than one classifier. Most of classification approaches have been applied to detecting phishing in websites, and some to emails (Gansterer and Pölz, 2009; Saberi et al., 2007) and voice using Gaussian mixture (Chang and Lee, 2010).

5.1.2. *Clustering techniques*

Clustering-based countermeasures partition a set of instances into phishing and legitimate clusters. The objective of clustering is to group objects based on their similarities. If each object is represented as a node, and the similarities between different objects are measured based on their shared common features, then a clustering algorithm can be used to identify groups (of nodes) of similar observations. The number of groups can be chosen so that nodes in the same group have higher similarity than nodes in different groups. The information about such a clustering structure is in turn used to assign new objects to the right cluster. New objects are assigned to a cluster based on their similarity with other instances under analysis.

Formally, assume that $p = |p_1, \ldots, p_n|$ represents a set of webpages, where each page p_i is represented as a feature vector $(f_{i_1}, \ldots, f_{i_m})$, in which f_{i_j} is either a content or URL-based feature. The purpose of clustering is to create a structure that best separates phishing from legitimate pages, and then use such a structure to cluster new pages. Two important components of a clustering method are the similarity (distance) measure between two data samples (e.g. pages p_i, p_j) and the clustering algorithm. Different similarity/distance measures can lead to different clustering results. Domain knowledge can be used to guide the formulation of a similarity/distance measure. For high dimensional data, Minkowski Metric is a popular measure:

$$d(p_i, p_j) = \left(\sum_{k=1}^{m} |p_{i,m} - p_{j,m}|^d \right)^{\frac{1}{d}} \tag{1}$$

where m is the dimensionality of the data. There are several special cases when,

- $d = 2$: Euclidean distance
- $d = 1$: Manhattan distance
- $d - \infty$: Super distance

Several clustering algorithms have been used for phishing detection, such as *DBscan*, *k-means*, and *Self-organizing-maps* (see Jain et al., 1999; Murtagh, 1983 for more details). DBscan has been employed to detect phishing targets by clustering a webpage set consisting of a given webpage p_i and all of its associated webpages (Liu et al., 2010). The relationships between p_i and its associated webpages are determined based on links, ranking, text similarity, and webpage layout similarity, which are used as the input features for clustering. The clustering method aims to discover a cluster shaped around p_i to identify p_i as phishing, which would in turn trigger the process of discovering the legitimate webpage p_i attacked by creating p_i – a fake version of p_i. Otherwise, the page is identified as legitimate. Like classification, clustering based anti-phishing techniques have involved a variety of input features and communication media. In addition to URL-based features (Cheng et al., 2011) and content features (Liping et al., 2009), clustering of phishing has also incorporated features extracted from website images (Kuan-Ta et al., 2009). Clustering has been applied in detecting attacks in several communication media such as phishing e-mails (Yearwood et al., 2009), spoofed websites (Kuan-Ta et al., 2009), and voice-based phishing attempts (Chang and Lee, 2010).

5.1.3. *Anomaly detection techniques*

Anomaly is a pattern in data that is not consistent with the schemes of normal behavior (Chandola et al., 2009). The anomaly-based approaches to phishing detection essentially treat phishing attempts as outliers. Every website claims a unique identity in the cyberspace either explicitly or implicitly. When a phishing site maliciously claims a false identity, it always demonstrates abnormal behaviors compared to a legitimate site, as manifested in some DOM objects in webpages and HTTP transactions (Nguyen et al., 2014). Anomaly detection algorithms discover phishing websites by capturing those anomalies (see Ying and Xuhua, 2006). Anomaly detection methods assign a score to the suspicious material under analysis by comparing the features of phishing material with those of one or more nearest neighbors. If the anomaly score goes above a cut-off point, the webpage would be classified as phishing.

Alternatively, one-class anomaly detection assumes that all training samples belong to a single class (i.e. the legitimate email). Accordingly, it creates a discriminative margin around the instances that correspond to legitimate class. One-Class SVM (Schölkopf et al., 2001) has been applied to phishing detection (Chandrasekaran et al., 2006). It treats the origin as the only member of the second class (the potential phishing email). If $e_1, e_2, \ldots e_n$ are training emails that belong to the legitimate class E, where E is a compact subset of R^E, then $\Phi : E \to H$ is a kernel mapping which transforms the email features in E into feature space H. To separate a dataset from the origin, one needs to solve a quadratic programming problem. The solution parameters set an upper bound on the fraction of phishing emails and a lower bound on the number of trainings from the legitimate emails used as Support Vector.

Most anomaly detection approaches to discovering phishing in spoofed websites focus on identifying abnormal signs that are more likely to be present in the URLs (Chandrasekaran et al., 2006; Guan et al., 2009; Ying and Xuhua, 2006).

Sample clues are shown in Table 2. Anomaly detection techniques have been used in other types of media such as IM. Guan et al. (2009) extract features based on the regularity in patterns of sending messages, the time between instant messages, the anomaly patterns in the URLs, and the temporal regularity of sender behavior to detect phishing.

Table 3 summarizes machine learning based phishing detection approaches, their input features, and application context. It is shown that classification is the dominant method for phishing detection, and the classification models generally draw features from the content and/or URLs of webpages or emails. Moreover, it is interesting to note that the phishing detection in emails mostly relies on content-based features, and the detection in websites on URL-based features. Additionally, it is revealed that a relatively small number of studies have applied clustering techniques to phishing; nevertheless, some features such as image and voice have only been explored in phishing clustering so far. Further, anomaly detection techniques have been used to detect phishing in IM as well as websites and emails. Nevertheless, it is shown from Table 3 that machine learning based countermeasures for phishing in

Table 2 – Anomaly clues in phishing pages.

Clue in the URL	Example
Includes redirection	http://3104.nnu4urye.info?http://c43n34.com?35u3b
The path contains a URL of a known organization	http://108.179.216.140/~bankofamerica/
Confused URL with non-valid pattern	http://sparkleyourcake.com/www.paypal.fr/
Special characters "-" in the host name	http://yj4yb6hmb3.x-cant-bank-you-here-of-my money.cn/ yj4yb6hmb3/Oraliao_show_23Y.
Long domain name	http://31837.9hzaseruijintunhfeugandeikisn.com/5/54878
Hostname is encoded	http://www.%64isc%72%65%74%2done-%6ei%67h%74.%63o%6d
IP is encoded	http://0x42.0x1D.0x25.0xC2/
E-mail address in URL	http://username@hotmail.com.fddcol.com

websites and e-mails are studied much more frequently than IM, voice and social networks.

5.2. *Text mining*

Text mining refers to utilizing data mining and machine learning techniques to discover trends, patterns, or useful knowledge from the text (Berry and Castellanos, 2004). Text mining identifies phishing attempts by analyzing the patterns of suspicious material, which include but are not limited to the content of e-mails, websites, URLs, Instant Messages, and SMS.

Three types of text mining techniques have been applied in phishing detection: *Term Frequency Inverse Document Frequency* (TF-IDF), *Regular Expressions* (RE), and *Latent Semantic Analysis* (LSA) and *Topic Models*. While such techniques could be grouped under the machine learning category, they are usually used as pre- and/or post-processing steps in creating other phishing detection solutions.

Table 3 – Machine learning-based countermeasures and their applied communication media.

Type and features		Media: Article
Classification	URL	Web: Ma et al., 2009; Huh and Kim, 2012; Choi et al., 2011; Garera et al., 2007; Gyawali et al., 2011; Cheng et al., 2011; Le et al., 2011 Email: André et al., 2010; L'Huillier et al., 2010 Social networks: Aggarwal et al., 2012
	Content	Web: Whittaker et al., 2010; Zhang et al., 2007 Email: André et al., 2010; L'Huillier et al., 2010; Bazarganigilani, 2011; Khonji et al., 2011; Sanchez and Duan, 2012 Social networks: Aggarwal et al., 2012 IM: Ding et al., 2011
Clustering	Voice	Voice over IP: Chang and Lee, 2010
	Images	Web: Kuan-Ta et al., 2009
	URL & content	Web: Liu et al., 2010; Liping et al., 2009 Email: Yearwood et al., 2009; Zhuang et al., 2012
Anomaly Detection	URL	Web: Ying and Xuhua, 2006 IM: Guan et al., 2009
	Content	Web: Ying and Xuhua, 2006 Email: Chandrasekaran et al., 2008

Essentially, the *TF-IDF* weighting scheme discovers the weight of a word in a set of documents by finding its relative frequency in one document compared to its inverse proportion over a referenced set of documents. The TF-IDF intuitively determines the weight of a given term with respect to a particular document (e.g., a webpage or an e-mail). For instance, the terms that are commonly used in spoofed e-mails tend to have higher TF-IDF weights than their legitimate counterparts. Given a set of e-mails $E = \{e_1, \ldots, e_n\}$ and terms $T = \{t_1, \ldots, t_k\}$, the TF-IDF weight of term t_i in e-mail e_j is calculated as follows:

$$w_{t_i,e_j} = f_{t_i,e_j} \times log\left(\frac{|E|}{f_{t_i E}}\right) \tag{2}$$

where f_{t_i,e_j} is the number of times term t_i occur in e-mail e_j, $|E|$ is the total number of e-mails, and $f_{t_i,E}$ denotes the number of e-mails that contains term t_i. The TF-IDF approach has been mainly used for websites. Zhang et al. (2007) propose a technique called CANTINA that utilizes TF-IDF instead of the URLs and domain names to discover phishing attempts. Xiang and Hong (2009) use TF-IDF and search engines to discover the actual domain of a page by analyzing the features of its declared identity. The extracted features of the claimed domain are used to run a query on search engines. If the query retrieves results, the two identities would be considered as similar and accordingly the pages would be classified as legitimate. This line of research continues by exploiting other features of the page to determine its identity such as features extracted from the DOM structure, element nodes that represent the site brand name, and page keywords (Xiang et al., 2011).

REs provide flexible means for matching strings of text. In phishing detection, REs have been used to generate patterns of phishing URLs from the existing pages (Fu et al., 2006a; Prakash et al., 2010). These patterns can in turn be used to match the new phishing URLs. REs are helpful to generate blacklist databases and eventually handle frequent minor changes in phishing patterns. *LSA* relies on identifying latent relationships between keywords, such as synonyms and homonyms, and hence it is useful to detect related words in the same context. LSA and topic models have been used in many text mining applications. LSA is based on the principle that words which are used in the same context tend to have similar meanings. Topic modeling treats documents as mixtures of latent topics, and the topics are in turn represented as probability distribution over words in the training dataset. Such topics have

Table 4 – Text mining-based countermeasures and their applied communication media.

Type	Media: Article
TF-IDF	Web: Zhang et al., 2007; Xiang and Hong, 2009; Xiang et al., 2011
Regular Expressions(RE)	Web: Prakash et al., 2010; Fu et al., 2006a; Bartoli et al., 2014 Email: Kerremans et al., 2005
Latent Semantic Analysis(LSA) and Topic Modeling	Email: Ramanathan and Wechsler, 2012; Bhakta and Harris, 2015; L'Huillier et al., 2010 Mobile: Modupe et al., 2014

been used as features in classification-based phishing detection (e.g. L'Huillier et al., 2010; Ramanathan and Wechsler, 2012).

Table 4 summarizes text mining-based phishing detection studies. The table shows that the detection of email phishing has leveraged LSA technique. By contrast, phishing detection in websites has focused on TF-IDF techniques. This may be due to the lack of context in web URLs and the wide diversity of web page content.

5.3. *Human users*

Human-based countermeasures and behavioral factors that characterize who falls in phishing are very significant for preventing phishing attacks. User studies, which aim to measure user response to phishing material, have considered *behavioral factors* (Blythe et al., 2011; Downs et al., 2007; Kumaraguru et al., 2007b; Sheng et al., 2010), and *demographic factors* (Carlson, 2006). These studies typically involve users for phishing identification. Most user studies are conducted using anti-phishing systems; nevertheless, some of them provide mechanisms to either increase user awareness when faced with phishing attacks, or involve them in phishing detection.

5.3.1. *Increasing user awareness*

Our lack of security awareness can be misused by attackers to deceive human victims. A variety of factors have been found to have an effect on human security awareness, including experiential factors such as *user's security knowledge* (Jakobsson et al., 2007), *web experience*, *computer self-efficacy*, and dispositional factors such as *user's disposition to trust*, *perceived risk*, and *suspicion of humanity* (Downs et al., 2007). Sun et al. (2016) and Wright and Marett (2010) suggest that experiential factors such as security knowledge, web experience, and computer self-efficacy lower the likelihood of a person being deceived by phishing e-mails. Out of dispositional factors only suspicion of humanity lowers the likelihood of deception.

There are two main approaches to increase security awareness: *Training and Educating* users and *IQ Test Experiments*.

- *Training and Education* is accomplished by educating users how to detect phishing attacks while they are doing regular activities on their email systems (Kumaraguru et al., 2007a), or avoid becoming a victim of phishing (Arachchilage et al., 2016; Dodge et al., 2007; Garera et al., 2007; Herzberg and Jbara, 2008; Herzberg and Margulies, 2011). One form of such training is to send users certain security notices about phishing attacks. Kumaraguru et al. (2007a) found that training embedded in e-mails with text and graphic notes about phishing is more effective than traditional security notification sent to users. It is noted that human-based approaches to phishing detection have been mainly applied to e-mail and website environments. Felt and Wagner (2011) highlight the need to increase human awareness in emerging communication media such as mobile apps. In view of the security limitations of the mobile environment, mobile apps lack secure identity indicators (e.g. certificate information, lock icons, and cipher selection). Moreover, mobile apps can be linked by attackers with faked content or spoofed websites, which further increases the challenge for users to discriminate between fake and valid URLs. Given the lack of technical solutions to phishing problems on mobile devices, increasing the awareness of stakeholders becomes even more critical to detecting phishing on those devices. Similarly, improving user awareness has also been recommended for preventing voice-based phishing (Griffin and Rackley, 2008). Training users to recognize phishing attacks includes also using PHaaS (Phishing as a Service) techniques in which organizations simulate real-world phishing scenarios on their users to track susceptibility to phishing in an experimental-based safe environment (Hadnagy, 2015; Meijdam et al., 2015; Social Engineer 2017). The main objective of these experiments is to understand how an organization is susceptible to phishing and raise awareness to phishing attacks.
- *IQ Test Experiments* are usually preceded by providing users with training material about phishing in specific contexts. These tests are developed from known services that a group of users employ, while excluding the element of inexperienced services. Robila and Ragucci (2006) introduced an IQ-based strategy for spear phishing education. The proposed technique presents users with both legitimate and phishing emails and ask the users to classify the emails. In particular, the method helps users to recognize and focus on important features when receiving suspicious emails. There have been concerns about the ethical aspects (Jakobsson and Ratkiewicz, 2006) and the performance of IQ tests (Anandpara et al., 2007). No correlation, however, was found between the actual number of phishing emails and the number of emails indicated as phishing by users who had taken the IQ test (Anandpara et al., 2007).

5.3.2. *Involving users in identifying phishing material*

Through participation in identifying legitimate and phishing material users are expected to be able to *manually* identify new phishing attempts (Kirda and Kruegel, 2006). In addition, users, particularly expert users, might even participate in creating phishing datasets, which also contribute to *user voting* based detection.

- *Manual Authentication*. This type of approach notifies users to identify suspicious information about phishing signs. Dwyer and Duan (2010) present an e-mail path in a geographical map using information from e-mail headers. The approach makes users aware of the message path, a scenario in which the e-mail sender claims that the e-mail is

Table 5 – User-based countermeasures and their applied communication media.

Type		Media: Article
Increasing user awareness	User training and education	Email: Kumaraguru et al., 2007a; Chandrasekaran et al., 2008; Wright and Marett, 2010 Web: Jakobsson et al., 2007; Downs et al., 2007; Sheng et al., 2009; Kumaraguru et al., 2010 Mobile: Felt and Wagner, 2011; van der Merwe et al., 2005a, 2005b; Niu et al., 2008; Canova et al., 2015 Voice over IP: Griffin and Rackley, 2008
	IQ tests	Web: Robila and Ragucci, 2006; Anandpara et al., 2007
Involving users in the identification of phishing material	Manual authentication	Web: Dhamija and Tygar, 2005 Email: Dwyer and Duan, 2010
	User voting	Web: Liu et al., 2011

sent from a trusted organization, but the actual IP address might not support such a claim. User participation in detecting phishing attacks has two major benefits: 1) it is effective in increasing human security awareness about phishing, and 2) it is useful in creating phishing datasets through user voting on the suspicious pages.

- *User Voting* (Phish tank, 2015) is the most popular database on reported phishing websites. The database offers a community based phishing verification system, where users submit suspected phishes and other users "vote" for whether such submissions are phishing or legitimate. Similarly, Liu et al. (2011) designed a phishing detection technique by relying on trained participants to vote on suspicious URLs.

Table 5 summarizes user-based approaches to phishing detection. It is shown from the table that, 1) user education is one of the most commonly used countermeasures to prevent mobile phishing; 2) user education, training and voting approaches have yet to be explored in several communication media such as IM and social networks; and 3) user voting could be cross-listed under the user awareness category.

5.4. *Profile matching*

Profile matching countermeasures utilize information about the domain name, URLs of domains recently accessed by users, their credentials in these domains, and other characteristics of the accessed domains (e.g. layout and images) to create feature based profiles and use them to detect phishing. The profile matching components can be simple (e.g. URL matching), or include sophisticated techniques (e.g. image matching). *Browser warnings* and most *phishing toolbars* fall under this category. Several tools are available to manage user profiles in a decentralized manner (Florêncio and Herley, 2006; Lee et al., 2008), and consolidate their identities (e.g. OpenID, Liberty Alliance's SAML, Microsoft's WS). We grouped phishing countermeasures that rely on a profile matching strategy into four categories: *Usage History Matching*, *Pattern Matching*, *Visual and Structural Matching*, and *White- and Black-list Matching*.

- *Usage History Matching*. The user profiles store information about the media and the user's authentication used for each media. When such information is requested in a specific medium claiming to be one of legitimate ones stored in user profile, the anti-phishing component uses information stored in the profile to detect the phishing attempt.

This type of approach, which has been mainly used to detect phishing in websites, is composed of two sub-categories. The *first* category develops *browser extension tools* to track user online activities such as his credentials and the webpages he visited (Chandrasekaran et al., 2008; Kirda and Kruegel, 2006). Those tools generate alerts whenever the user attempts to transmit information in an untrusted path based on historically tracked information (Wu, 2006; Wu et al., 2006b). The *second* category requires users to *manually create their profiles* (Xun et al., 2008), which will in turn be used in phishing detection.

- *Pattern Matching*: Instead of recording information about user activities, this type of approaches creates profiles about other entities (e.g. legitimate webpages, legitimate e-mail patterns). For instance, Spoof Guard browser plug-in (Chou et al., 2004) screens for pages requesting the user's credentials by checking user browsing history. If the user enters his stored credentials on an unknown target page, an anomaly score is calculated through a pattern matching procedure. Based on the score, the page is categorized as phishing or legitimate. Pattern matching techniques have also been used to detect cloned profiles in social networks (e.g., Kontaxis et al., 2011).
- *Visual Matching*: Visual similarity is computed based on the visual aspects of web interfaces such as images, blocks, and layout to discriminate between phishing and legitimate pages. Several approaches introduce visual similarity measures for the detection of phishing attacks, such as Segmentation-based Visual Similarity (Afroz and Greenstadt, 2011; Bozkir and Sezer, 2016), DOM Tree Similarity (Rosiello et al., 2007) which detects phishing web pages by comparing the legitimate and suspicious pages based on graph similarity, Earth Mover's Distance which determines web page similarity based on images (Fu et al., 2006b), Unicode Character Similarity List (Fu et al., 2006a), and Contrast Context Histogram Measure which extract key features for pattern matching at real time (Kuan-Ta et al., 2009). Some visual matching approaches employ more than one type of similarity measure, such as block-level page similarity, layout and overall similarity in comparing webpages (Wenyin et al., 2005), text pieces, web page style, and images embedded in pages (Cheng et al., 2011; Medvet et al., 2008).
- *White and Blacklist Matching*: This type of countermeasure puts emphasis on creating a database of known trusted and suspicious domains. Once anomalies are detected using domain filtering techniques, a matching against a blacklist and/or a whitelist can be carried out. White- and blacklist matching has been argued to be one of the most effective

Table 6 – Profile matching-based countermeasures and their applied communication media.

Type	Media: Article
Usage history Matching	Web: Wu et al., 2006b; Kirda and Kruegel, 2006; Xun et al., 2008; Rosiello et al., 2007 E-mail: Chandrasekaran et al., 2008 Social networks: Kontaxis et al., 2011
Pattern matching	Web: Chou et al., 2004; Kontaxis et al., 2011
White and black list matching	Web: Miyamoto et al., 2005; Cao et al., 2008; Chen and Chuanxiong, 2006; Kang and Lee, 2007; Ludl et al., 2007
Visual matching	Web: Rosiello et al., 2007; Fu et al., 2005; Medvet et al., 2008; Wenyin et al., 2005; Kuan-Ta et al., 2009; Fu et al., 2006b; Afroz and Greenstadt, 2011; Chen et al., 2010 Mobile: Malisa et al., 2016

approaches to phishing detection (Cao et al., 2008; Chen and Chuanxiong, 2006; Kang and Lee, 2007; Ludl et al., 2007). In fact, browser blacklists are the major protection mechanism against phishing attacks (Tsalis et al., 2015; Virvilis et al., 2014). Google provides the Safe Browsing service that allows client application to check suspicious URLs against constantly updated lists of suspicious sites. Based on how blacklists are generated, Virvilis et al. (2015) classified existing browsers into three categories:

1. Browsers that utilize the Google Safe Browsing, such as Chrome, Firefox and Safari.
2. Browsers that utilize their own blacklists such as Internet Explorer and Edge that utilize the SmartScreen – a Microsoft proprietary blacklist.
3. Browsers that aggregate blacklists using third parties'. For instance, Opera utilize Phishtank and Netcraft blacklists to create its own list of suspicious URLs.

The majority of blacklist approaches were not found to be effective for handling zero-day/hour phishing (Sheng et al., 2009). Miyamoto et al. (2005) proposed a blacklist filtering algorithm that can be applied to proxy server with no performance overhead. The idea is to sanitize the proxy system by blocking all parts of webpage content that contains malicious code including username and password forms. One limitation of this approach is that it requires efforts to maintain the blacklist. Another lies in performance overhead incurred when web forms are blocked from the suspicious pages.

Table 6 summarizes profile matching countermeasures for phishing. Usage history matching approaches are shown to have been applied not only to spoofed websites, but also to phishing emails and spoofed user profiles in social networking sites. Nevertheless, the approaches have been predominantly used for detecting phishing in websites. This observation may be explained by the availability and accessibility of tools for tracking user's online activities. Other types of profile matching approaches have not yet been applied beyond website spoofing.

5.5. *Other types of countermeasures*

We identified several emerging anti-phishing techniques, including *Ontology*, *Honeypots*, *Search Engines*, and *Client–server Authentication*.

5.5.1. *Ontology*

Ontology models a set of concepts in a particular area as well as the semantic associations among those concepts (Gruber, 1993).

New terms, phrases or expressions used in phishing e-mails can be identified by modeling them as concepts and semantic relationships in an ontology. Phishing attempts are becoming sophisticated. In particular the textual content utilized to initialize the attacks is morphed, making it difficult to classify them using conventional anti-phishing techniques (Taylor et al., 2011). For instance, phishers usually change phishing e-mail contents to avoid the detection when faced with conventional content-based countermeasures. However, if the semantic relationships among concepts are properly defined, the likelihood of detecting new forms of phishing e-mails may increase (Lundquist et al., 2014). Ontological semantics can enhance natural language understanding by detecting meaning-based clues pointing to phishing and reasoning about phishing. Very few anti-phishing techniques have incorporated ontology to date. Bazarganigilani (2011) proposes an ontology-based approach to improve the accuracy of classifier-based anti-phishing techniques. The method first extracts features from an e-mail by analyzing its text, and if the extracted features match those of the known phishing e-mails, the e-mail is passed to an ontology which then incorporates a set of related concepts in the detection process. On a related note, Kerremans et al. (2005) create a knowledge representation system to differentiate among several types of fraud including phishing.

5.5.2. *Honeypots*

Honeypots are security devices whose value lies in their being probed and compromised. The honeypots usually work as a trap that is configured to collect suspicious data. They are configured to collect data about attackers, create an attacker blacklist databases, and/or block suspicious domains.

Several honeypot-based frameworks have been proposed to counter phishing attacks (Gajek and Sadeghi, 2008; McRae and Vaughn, 2007; Shujun and Schmitz, 2009). The key idea in such approaches is to actively provide phishers with honey tokens that seem to be authentication data (e.g. fingerprinted credentials). Honey tokens can exist in almost any form, from a dead, faked account to a database entry that would only be selected by malicious queries – any use of them is inherently suspicious if not necessarily malicious. Another example of a honey token is a faked email address used to track whether a mailing list has been stolen. Honey tokens-based approaches can help track phishing activities that initiate site shut downs, and thus become a popular proactive phishing countermeasure (Florêncio and Herley, 2006). Nassar et al. (2007) propose a holistic honeypot-based approach for Voice over IP security monitoring. Their approach consists of two key components: a Voice over IP honeypot and a correlation engine. The main advantage of the proposed technique lies in its ability to defend against several types of attacks including phishing. HoneyBuddy is yet another approach for detecting suspicious activities in IM (Antonatos et al., 2010). The method discovers contacts and includes them in its honeypot messengers by submitting queries to search engines to identify new contacts and grow its database. Alternatively, it can utilize contact finder sites to find new potential IM victims. One limitation of honey token approaches lies in their ease of discovery by phishers. Thus, the major challenge of this type of approach is to extend the life span of the honey token.

5.5.3. *Search engines*

Search engines are combined with other techniques to detect phishing. Typically, if a page is legitimate, it should have been indexed and assigned a rank by the search engine (Liu et al., 2010).

In contrast, phishing domains are not popular and accordingly their ranks by the search engine tend to be very low. Even worse, most phishing domains are not indexed by search engines (Xiang et al., 2011; Zhang et al., 2007). Guan et al. (2011) use search engines to validate the URLS posted on social network pages. A heuristic approach is developed by analyzing Facebook wall posts that contain URLs. Several features are extracted to distinguish valid from phishing URLs, such as the dash count in hostname, the existence of domain name when queried in a search engine, and the age of the domain. Huh and Kim (2012) propose to use search engine ranking results as inputs to build phishing classifiers, a technique claimed to be effective in reducing false positives.

5.5.4. *Client–server authentication*

Client–server authentication relies on the mutual authentication between clients and servers. *Site Keys*, *Trusted Devices*, *Identity-based Signature Scheme*, *Dynamic Customized Interface*, and *Channel ID*-based Authentication have been the main authentication techniques used in detecting and preventing phishing attacks. In *Site Keys* interactive validation, the user only needs to perform a single graphic matching to authenticate the images he selected for certain site (Dhamija and Tygar, 2005) (see Appendix I). This approach has advantages in its simplicity and robustness. *Trusted Device* (e.g., a smart phone) has been used to perform mutual authentication (Hart et al., 2011). The approach not only reduces the dependency on users during the validation process but also has the potential to prevent other types of attacks such as MITM attacks. Similarly, an *Identity-based Signature Scheme* has been utilized to make email communication trustworthy (Adida et al., 2005). Unlike typical digital signatures, the approach does not require pre-established public-key infrastructure. Neither does it need collaboration between email domains. Instead, each email domain is independent and an identity-based controlling authority will issue keys. Additionally, master public keys corresponding to each domain need to be distributed and certified.

Unlike typical key pairs, the identity-based secret keys are calculated by a controlling authority and then sent to users. Once the keys are sent, a group-based signature scheme is utilized to allow senders to initiate a signature for a message using a selected signatory group. This authentication scheme requires the sender to be part of a group and other members' public keys to be available. Anyone in the group can confirm that a signature has been computed with revealing the identity of a signer. Therefore, the sender himself and the recipients of his message are supposed to be in a single group. *Dynamic Customized Interface* is another approach that only asks users to recognize an image generated by the server instead of any static security indicators shared with the server. Recent works have addressed the problem of how to securely setup a personalized security indicator in mobile banking (Marforio et al., 2016). Several authentication techniques utilize the Transport Layer Security (TLS) and SSL protocols to provide some assurance that the user is the real instead of a scam website. SSL and TSL are based on public key cryptography (Ying and Xuhua, 2006). During the authentication process, the TLS/SSL client sends a message to a TLS/SSL server. As a result, the server will authenticate itself to the client. Authentication keys are then exchanged between the server and the client. Once the keys are exchanged and the validation completed, a secured connection between the client and the server can be established. *Channel ID-based Authentication* (Karapanos and Capkun, 2014) was designed to thwart both types of MITM attacks, as introduced in Section 4.3. When the user attempts to log into his account for the first time from a browser, the web server requires the user to self-authenticate using a strong second factor authentication device, as in phone authentication and Universal 2nd Factor (U2F) protocols.

As part of the authentication protocol, the second factor device compares the Channel ID of the browser to that of the TLS connection that the server witnesses. If they are equal, then the browser is directly connected to the web server; otherwise, there would be an attack in the middle, and the device aborts the authentication protocol to stop the attack. A server may create a channel-bound cookie to protect subsequent interaction with the server from that browser. There are other categories of authentication mechanisms such as email authentication. AOL has implemented a mechanism called AOL passcode to avoid phishing attempts on user accounts (Garera et al., 2007). Passcode utilizes a device that randomly generates a numeric passcode every minute. Microsoft, on the other hand, implemented SenderID Filter (Microsoft, 2016b), an email authentication protocol, to address the problem of domain spoofing.

Table 7 summarizes four types of countermeasures within the other categories. Among them, only search engine-based solutions have been applied to detect phishing in social networking sites, and ontology to e-mails only.

In contrast, honeypot has been used to collect information about phishers in a variety of media such as IM (e.g., collecting accounts utilized by phishers to send phishing material), Voice over IP (e.g., creating blacklist databases of suspicious voice sources), and websites. Client–server authentication countermeasures have been mainly utilized to prevent phishing in e-mail and website environments.

5.6. *Comparison of anti-phishing tools*

Phishing research guides the development of new phishing detection and education tools that can directly benefit target users. Abbasi et al. (2010) provide a comparison between two types of anti-phishing tools: the Lookup/blacklist systems and the Classifier/pattern matching systems. The *Lookup Systems* include

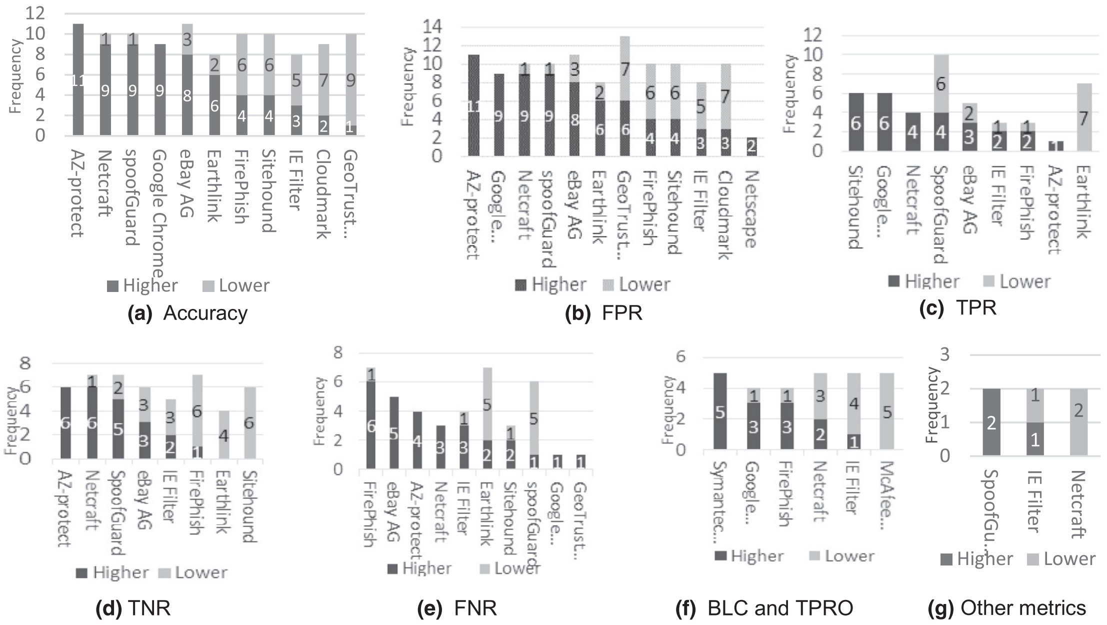
Table 7 – Other types of countermeasures and their applied communication media.

Type	Media: Publication
Ontology	E-mail: Kerremans et al., 2005; Bazarganigilani, 2011
Search engines	Web: Huh and Kim, 2012; Zhang et al., 2007; Xiang and Hong, 2009; Liu et al., 2010 Social networks: Guan et al., 2011
Honeypots	Web: Shujun and Schmitz, 2009; Gajek and Sadeghi, 2008 IM: Antonatos et al., 2010 Voice over IP: Nassar et al., 2007; Gupta et al., 2015
Client server authentication	Web: Dhamija and Tygar, 2005; Parno et al., 2006; Hart et al., 2011 Email: Adida et al., 2005 Mobile: Bicakci et al., 2014 Mobile: Marforio et al., 2016

Microsoft IE phishing filter, the Mozilla Firefox FirePhish, Cloudmark, Earthlink Toolbar, Geotrust Watcher, and the *Classifier Systems* include Calling ID, ebay Account Guard, Netcraft, Site Watcher, and Spoof Guard. However, this comparison schema is limited in that it only focuses on machine learning and statistical anti-phishing tools. Shahriar and Zulkernine (2010) compared anti-phishing tools based on other criteria such as user input it requires, simultaneous testing of several pages, SSL certificate validation mechanism, supporting languages other than English, and detecting XSS phishing attempts. The study compared a list of tools, including BogoBiter (Yue and Wang, 2010; Joshi et al., 2008), AntiPhish (Kirda and Kruegel, 2006), DOM anti-Phish (Rosiello et al., 2007), Cantina (Xiang et al., 2011), SpoofGuard (Chou et al., 2004), PhishTester (Shahriar and Zulkernine, 2010), and the techniques developed by McRae and Vaughn (2007), Wenyin et al. (2006), Ying and Xuhua (2006), Xun et al. (2008), Xiang and Hong (2009), Wenyin et al. (2010), and Ma et al. (2009).

Among the tools, PhishTester, PhishGuard and BogoBiter were ranked highest. This comparison only focuses on the functions provided by tools but it does not utilize performance metrics in comparing them. In addition, tools are not compared based on communication media and attacking techniques. In an effort to understand the state of phishing detection practice, we provide a side-by-side comparison of anti-phishing tools. In addition to the four dimensions drawn from our proposed phishing taxonomy, our comparison is also based on two new dimensions: performance metrics and user evaluation. These dimensions were identified from our systematic survey of existing studies that involve the evaluation of anti-phishing tools. Performance metrics are objective measures, and its most popular examples include *True Positive Rate (TPR)*, *True Negative Rate (TNR)*, *False Positive Rate (FPR)*, *False Negative Rate (FNR)*, *Accuracy*, and *Page Load Delay*. One concern about the performance of most of the phishing detection tools is that they are not fast enough (Moore and Clayton, 2007, 2008). For instance, the statistics of McGrath and Gupta (2008) shows that some phishing domains last for at least 3 days without being discovered by anti-phishing tools. Thus, the time to *take phishing site down* is identified as a significant metric for anti-phishing tools (Yue et al., 2006). Nevertheless, this metric has yet to be used in the evaluation of the phishing detection techniques. In contrast, *user evaluation* involves users' subjective assessment and perception. Our comparison reveals that only a small number of studies have conducted user evaluation of anti-phishing tools (see Appendix J.1). In terms of communication media, spoofed websites predominate in efforts developing anti-phishing tools. Yet, concerns have been raised about the effectiveness of the tools in detecting web spoofing attempts (Downs et al., 2006; Egelman et al., 2008; Geer, 2005). In contrast, research tools in support of phishing detection in other types of media such as mobile, IM, and social networks are still lacking. Despite the fact that several studies have compared phishing detection techniques (Abbasi et al., 2010; Egelman et al., 2008; Li and Helenius, 2007; Sheng et al., 2009), none has yet to rank them and consider system usability.

Using the analytic hierarchy process (AHP), we have provided a ranking of phishing tools based on the findings of extant comparative studies. Given a set of n tools and set of binary comparisons between pairs of tools, AHP infers a total order over the tools by aggregating the given comparison results. Additionally, our ranking considers both performance and usability metrics. The former include accuracy, TPR, FPR, TNR, FNR, *Black list Coverage (BLC)* and *Total Protection (TPRO)*, and the latter include *Visibility of User Interface*, *Matching Real World*, *User Control Freedom*, *Consistency* and *Standards*, *Help Used* and *Error Prevention*, *Flexibility*, *Aesthetic Design*, *Pleasurable Interaction*, and *Privacy*. AHP allows a given pair of tools to receive no comparison due to missing values or to have a tie in ranking. We identified a set of 32 tools from existing studies. The ranking results of the tools are reported in Fig. 5, which are sorted in the descending order of the frequency when the tools are ranked higher in pairwise comparisons. The results show that AZ-protect, Netcraft, SpoofGuard, Google chrome, eBay AG, and EarthLinks receive the highest ranks in accuracy (Fig. 5a) and in FPR (Fig. 5b); Sitehound and Google Chrome are ranked highest in TPR (Fig. 5c); AZ-protect, Net-Craft, and SpoofGuard are the highest in TNR (Fig. 5d); and Firephish and eBay AG outperform other tools in FNR (Fig. 5e). Based on the results of a small number of studies that used BLC, TPRO, and usability metrics, Google Chrome and Symantec toolbars are ranked higher than other tools in terms of BLC and TPRO (Fig. 5f), and SpoofGuard receives the top rank in usability measures (Fig. 5g). The raw ranking results are reported in Appendix J.2. In addition to research tools, we also compared different commercial tools based on their underlying attack detection/prevention techniques and their publicly available information (APWG, 2014). The results are reported in Appendix K. The analysis reveals that these tools emphasize detecting and preventing phishing attempts but have paid insufficient attention to security awareness and training. Instead, the majority of the tools provide algorithmic solutions to prevent phishing such as cousin domains (e.g., cyber-security.com spoofs an actual domain cybersecurity.com and sends emails from the spoofed domain). Additionally, existing commercial tools do not yet have functions to cope with phishing attacks in emerging media such as social networks. There is also limited commercialization of ontology and search engine-based countermeasures. To this end, we have identified the following open research issues that are worthy of exploration in future. These



(a) Accuracy (b) FPR (c) TPR

(d) TNR (e) FNR (f) BLC and TPRO (g) Other metrics

Fig. 5 – Pairwise comparison results.

issues along with their potential countermeasures are also summarized in Table 8.

- *Zero-day Phishing Detection*: Since phishers are constantly adapting their phishing tactics and users would most likely be deceived by unknown phishing attempts, detecting those attempts is very significant to avoid possible financial losses. There is some pioneering work on addressing zero-day phishing (Moghimi and Varjani, 2016; Zhan and Thomas, 2011). Nevertheless, one of the approaches that have been

Table 8 – Future research issues in phishing detection.

Issue	Suggested countermeasure	Counter-measure category	Media*					
			W	E	IM	M	V over IP	S
Zero-day phishing	Contextual relationships with known phishing patterns	Machine Learning		√		√		√
Zero-day phishing	One class-anomaly detection		√	√	√			√
Multi-stage phishing detection	Co-clustering		√	√				√
Deceptive voice phishing	Wavelet clustering				√		√	
Phishing in adaptive environments	Adaptive classifiers		√	√	√			√
Context-based phishing detection and prevention	Graph mining techniques		√		√			√
Multilingual phishing	Latent Semantic Analysis and Semantic nets	Text Mining	√	√	√			√
Detection of profile cloning attacks	Profile trust models	Profile Matching			√		√	√
Multi-stage phishing detection	Multi-layer profiles		√	√				
Context-based phishing detection and prevention	Interactive training and Social Network Analysis	Human User	√	√		√		√
Phishing in adaptive environments	Structure and content mapping	Ontology	√	√				
Detecting phishing farms	Ranking-based phishing detection	Search Engine	√					√
Deceptive voice phishing, profile cloning	Blacklist collector	Honeypot	√	√	√	√	√	√

*W: Web; E: Email; M: Mobile; IM: Instant Messenger; V: Voice; S: Social Networks.

overlooked is contextual similarity with known phishing patterns. Unknown phishing attempts share some common contextual relationships with known ones despite the former's unique characteristics. Thus, contextual similarity can be used in the prediction of unknown patterns of phishing by projecting future possible activities of an adversary and the paths he/she may take. Another promising path for detecting unknown phishing attempts is to combine anomaly detection with contextual similarity. Several anomaly detection approaches can be used in this combination approach such as anomaly-based one class classification approaches that have been recently used in detecting zero-day intrusions (Shon and Moon, 2007).

- *Multi-stage Phishing Detection*: Multi-stage attacks are initialized in one communication media and accomplished in another. Thus, it becomes necessary to implement new phishing solutions that trace and detect phishing attempts at all stages. For instance, when phishing attempts are initiated by e-mails which redirect users to spoofed webpages, appropriate tools are needed to examine phishing patterns in both types of media simultaneously. Co-clustering is one of the clustering approaches that has been used to classify two types of objects simultaneously (Bühler and Hein, 2009; Lei et al., 2012; Long et al., 2007). When applied in phishing detection, co-clustering can be used to create bi-partition graphs by simultaneously clustering similar patterns in phishing e-mail and the corresponding website contents referred to by e-mail URLs.
- *Deceptive Voice Phishing Detection:* Voice phishing detection has received limited attention in phishing research to date. To this end, several machine learning techniques such as wavelet clustering have great potential (El-Wakdy et al., 2008; Sheikholeslami et al., 1998). Wavelet clustering relies on clustering voice waves for speech recognition. Since it is an unsupervised technique, wavelet clustering might be used in detecting unknown patterns of voice phishing attempts. In addition, honeypots can be used to collect suspicious phone numbers to create blacklists (Nassar et al., 2007). Future research approaches need to focus on creating voice-based classification techniques through analyzing patterns of suspicious voices collected by honeypots (Hirschberg et al., 2005). Further, there is a trend of detecting voice phishing in mobile environment.
- *Phishing Detection in an Adaptive Environment:* Adaptive environment is defined as those which are strategically or tactically modified according to their usage (e.g. websites, mobile apps). Existing anti-phishing techniques could lead to high false positive rate when applied in such an environment since most of them are rule-based (Aburrous et al., 2008; Basnet et al., 2011; Ludl et al., 2007). Additionally, they recognize minor changes in these media as phishing attempts. To resolve this problem adaptive classifiers can be utilized (Taninpong and Ngamsuriyaroj, 2009). In addition, as the structure of a web site changes, an ontology consisting of concepts of that particular website can handle the site topology construction and restructuring (Raufi et al., 2009). Specifically, the site ontology can be utilized in mapping between the structure of the site under checking and the stored ontology. Then, based on similarity in terms of structure and content between the site examined and the legitimate site ontology, the website can be classified using appropriate classification functions.
- *Detecting Phishing farms using Ranking-based Phishing Detection:* Ranking based countermeasures can be used in the detection of not only single-page phishing but phishing farms that utilize similar domain names and features as well (Youn and McLeod, 2009). Despite the demonstrated effectiveness of search engines in detecting phishing (Sunil and Sardana, 2012), the validation environment is external and thus inefficient. Specifically, a detection application has to submit suspicious URLs to a search engine, evaluate search results, and pass the results back to the phishing detection engine. Additionally, the robots used to check URLs posted to search engines are usually recognized as spamming attempts by search engines. To address these issues, creating an internal ranking-based mechanism is a promising direction for phishing detection.
- *Multilingual Phishing Detection:* Monolingual phishing attacks in English have increased over time. There have also been some phishing attempts on PayPal accomplished in two languages (English and French) simultaneously (Smustaca, 2011). According to RSA Security's Anti-Fraud Command Center (AFCC), there is an increase in the rate of phishing attacks which target commercial sites in non-English speaking countries. According to a security report (Sullivan et al., 2014), depending on the countries involved, addressing fraud threats means in many cases differences between languages. Those differences complicate the task of researchers and practitioners who would otherwise take advantage of many anti-phishing tools developed for other languages. Several text mining techniques, as introduced in Section 5.2, can be used to create new anti-phishing mechanisms. Multilingual IR is one of the new research areas that focus on creating language-independent IR models. Several other types of semantics-based techniques such as ontology, LSA and semantic networks (Wenyin et al., 2010) have shown success in various applications, which might be extended to phishing detection in different languages.
- *Detection of Profile Cloning Attacks:* One of the many problems inherent in social networking websites is profile cloning. In such attacks, fake user profiles are created as duplicates of an authentic user on the same or across different social networks. The main objective of the cloning attacker is to mislead the user's friends into forming bogus relationships with the faked profile (Lee et al., 2010). The attacker can exploit this trust to collect personal information on the user's friends and perform various types of online frauds. Aside from the manual approach to detect profile cloning by calling every person who sends the message to identify their identities, some social networking sites, such as Facebook, have been trying out social authentication methods. Nevertheless, such methods can be easily breached; as attackers often know a lot about their targets and the user's personal social knowledge is generally shared with people in their social circle (Huh and Kim, 2012). Additionally, photo-based social authentication methods are increasingly vulnerable to automatic attacks such as face recognition and social tagging technologies. To this end, Profile Trust Models are a promising solution, which work by evaluating the material received by users (Chou et al.,

2004; Wang et al., 2010). For instance, the sender's profile can be validated based on the number of friends, social networks usage history, the number of followers, and so on.

- *Context-based Interactive Phishing Prevention:* The design of traditional security training solutions to avoiding security attacks mostly does not take into account contextual factors about users (Wilson and Hash, 2003). Moreover, most users do not pay attentions to warning signs about phishing in their context (Kumaraguru et al., 2007a). Therefore, it has significant practical implications to develop context-aware and interactive phishing detection and prevention solutions. User context includes not only factors directly related to users, but characteristics of communication media and phishing targets as well.

Depending on the types of context, different techniques can be employed. For instance, to identify phishing target communities, some studies are required to identify target social contexts and the phishing patterns utilized to target different types of institutions (Weaver and Collins, 2007). Social Network Analysis and Graph Mining techniques can also be used to group users who have responded to phishing URLs on social networks, news groups, and blogs based on their context (Liu et al., 2011). The objective of all such techniques is to design context-based security awareness solutions.

6. Concluding remarks

This research creates a multidimensional phishing taxonomy based on a comprehensive survey of the related literature. The taxonomy provides an integrated view of phishing that consists of four dimensions: communication media, target environments, attacking techniques, and countermeasures. This research not only identifies traditional and emerging communication channels where phishing attacks take place, but also uses the communication media as lens to analyze phishing countermeasures. Moreover, the research fills a gap in the study of phishing countermeasures through a systematic study by providing a classification consisting of five categories, namely machine learning, text mining, human users, profile matching, and others, and the last category further consists of search engines, ontology, client–server authentication, and honeypot countermeasures. Among them, the first three are most widely studied, whereas semantics-based techniques in the *other* category such as ontology have been overlooked. This study also reveals that anti-phishing research and development has focused on phishing in e-mails and websites, but paid little attention to that in IM, social networks, voice, blogs and web forums; further, phishing in mobile communication has yet to be explored from the technical perspective. In addition, the proposed taxonomy identifies emerging attack vectors such as vishing, spear phishing, fake e-card, online job-hunting and donation scams, mobile apps and online social networks.

These findings lend themselves to a number of open issues for future research and development in phishing detection and prevention of techniques such as zero-day phishing. Going beyond issue identification, we suggest promising solutions based on the proposed categorization of countermeasures.

Acknowledgement

This research effort was supported in part by the National Science Foundation (SES-152768). Any opinions, findings or recommendations expressed here are those of the authors and are not necessarily those of the sponsors of this research.

Appendices

A. *A Comparison between Phishing and Spam*

Table A.1 – Comparison between phishing and spam

Criteria	Spam attempts	Phishing attempts
Difficulty	Easy to initiate/ easy to be identified by spam filters	Harder to initiate/cannot be identified using spam filters
Main objective	Advertise products	Bargain user data
Models	• Pay per click • Affiliate marketing • Promote shady companies	• URLs that direct the recipient to spoofed web pages • Downloading malware that is sent as part of suspicious URL in an email message
Scheme	Implausible	Looks credible
Target*	Sent to as many recipients as possible	Directed to a more targeted audience
Transience*	Sent in frequent and large batches	Short-lived, often occurring for only a few hours
Dynamic*	Advertising products or a service from a known static Web site	More dynamic, moving among servers very quickly, redirecting users to a private site

*Anti-Phishing Working Group (APWG)

B. *Uptime for Phishing Sites*

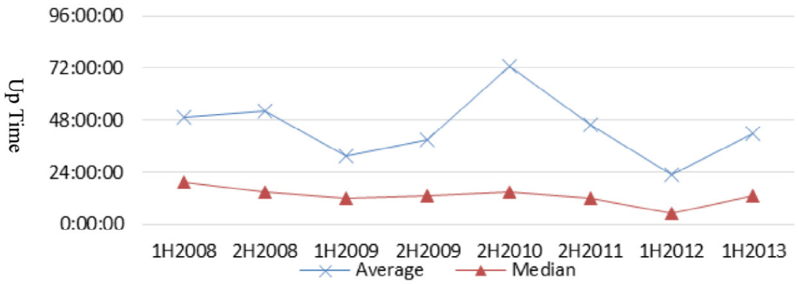


Fig. B.1 – Phishing sites *Uptime* (hh:mm), Anti-Phishing Working Group (APWG).

Fig. B.1 shows the Uptime for phishing sites over different periods of time between 2008 and 2013. The Average Uptime varies from 72 hours in the second half of 2010 to 24:00 hours in the first half 2012. Based on Uptime metric, it is immature to conclude that there is an increase in the success rate of existing countermeasures in detecting phishing attacks.

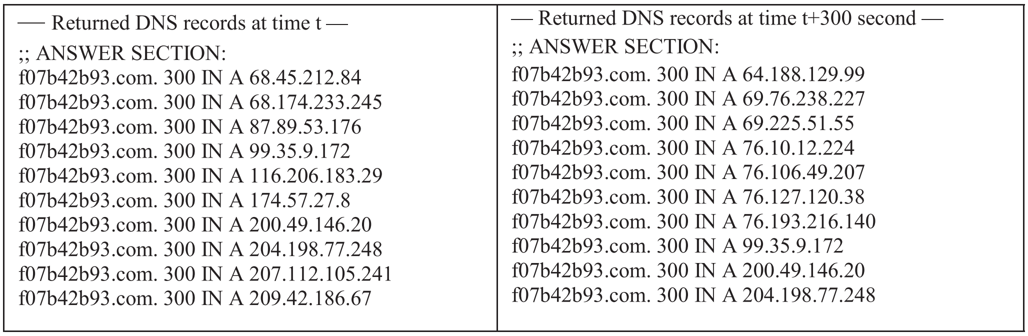
C. *Mass vs. Spear Phishing Attacks*

Table C.1 – Economics of mass vs. spear phishing attacks (a Cisco report).

Example of a typical campaign	Mass phishing	Spear phishing
Total messages sent in campaign	1,000,000	1000
Block rate	99%	99%
Open rate	3%	70%
Click through rate	5%	50%
Conversation rate	50%	50%
Victims	8	2
Value per victim	$ 2,000	$ 80,000
Total value from campaign	$ 16,000	$ 160,000
Total cost for campaign	$ 2,000	$ 10,000
Total profit from campaign	$ 14,000	$ 150,000

Table C.1 shows a comparison between mass and spear phishing based on a security report by Cisco. The report corroborates that spear phishing need not occur on a massive scale for a typical phishing campaign to be effective (Peterson 2011). On the other hand, the costs of a spear phishing attack are five times those of a mass attack, in view of the quality of the list acquisition, botnet leased, email generation tools, malware purchased, website created and campaign administration. Nevertheless, the value and profit of spear phishing are significantly higher. Thus, for an individual campaign, the economics of a spear phishing attack can be more compelling than a mass attack.

D. *Fast Flux Attacks*



```
— Returned DNS records at time t —
;; ANSWER SECTION:
f07b42b93.com. 300 IN A 68.45.212.84
f07b42b93.com. 300 IN A 68.174.233.245
f07b42b93.com. 300 IN A 87.89.53.176
f07b42b93.com. 300 IN A 99.35.9.172
f07b42b93.com. 300 IN A 116.206.183.29
f07b42b93.com. 300 IN A 174.57.27.8
f07b42b93.com. 300 IN A 200.49.146.20
f07b42b93.com. 300 IN A 204.198.77.248
f07b42b93.com. 300 IN A 207.112.105.241
f07b42b93.com. 300 IN A 209.42.186.67
```

```
— Returned DNS records at time t+300 second —
;; ANSWER SECTION:
f07b42b93.com. 300 IN A 64.188.129.99
f07b42b93.com. 300 IN A 69.76.238.227
f07b42b93.com. 300 IN A 69.225.51.55
f07b42b93.com. 300 IN A 76.10.12.224
f07b42b93.com. 300 IN A 76.106.49.207
f07b42b93.com. 300 IN A 76.127.120.38
f07b42b93.com. 300 IN A 76.193.216.140
f07b42b93.com. 300 IN A 99.35.9.172
f07b42b93.com. 300 IN A 200.49.146.20
f07b42b93.com. 300 IN A 204.198.77.248
```

Fig. D.1 – An illustration of a fast-flux botnet rapidly changing the mapping of IP addresses to its domain names (300 s apart).

In Fig. D.1, a malicious service f07b42b93.com hosts a phishing webpage. During a DNS query issued at time *t*, the domain's DNS server replies with 10 records, any of this will lead users to the phishing webpage. The short time-to-live (TTL) value, i.e., 300 s, indicates that the records will expire after 300 s, so a new DNS query will then be required. At t + 300 s, the same query is re-issued and obtained another set of IP addresses.

E. Content Injection Attacks

Table E.1 – The URL sent in the phishing email.

http://www.well-known-financial-institution.com/ ?q=%3Cscript%3Edocument.write%28%22%3C iframe+src%3D%27 http%3A%2F%2Fwww .very-bad-site.com%27 + FRAMEBORDER%3D%270%27+WIDTH %3D%27800%27+HEIGHT%3D%27640%27 + scrolling%3D%27auto%27%3E%3C%2Fiframe %3E%22%29%3C%2Fscript%3E&. . .=. . .&. . .

Table E.2 – Translating URL into human readable form.

http://www.well-known-financial-institution.com/?q=<script>document.write("<iframe src='http://www.very-bad-site.com' FRAMEBORDER ='0'WIDTH='800' HEIGHT='640' scrolling='auto'></iframe>")</script>&. . .=. . .&. . .">

In Table E.1, A phishing email asks the user to click on a URL. The URL is not human-readable, but it can be translated into a readable form after mapping the hexadecimal characters, as shown in Table E.2. Then, the Javascript code embedded into the search query will be executed upon visiting the target website, which will inject the HTML code (fetched from www.very-bad-site.com) into the code the user's browser would normally render.

F. *Countermeasures Classification based on Information Flow of Phishing*

Table F.1 – Phishing and countermeasures (Jakobsson and Myers 2006)

Attack Step	Countermeasure
0-	– Preventing attack • Preemptive domain registration • Providing spoof-reporting service • Monitoring bounced email message • Monitoring account activity for anomalous activity • Monitoring the use of images • Establishing honeypots
1-	– Preventing delivery of phishing payload • Email filtering • Email authentication • Cousin domain rejection • Secure patching
2-	– Preventing a user action • Education(e.g. missing personalized information in phishing email) • Display deceptive content canonically • Interfere with navigation • Detect inconsistent DNS information • Modify referenced images • Prevent navigation and data compromise
3-	– Preventing the transmission of prompt • Filter out cross-site scripting(XSS) • Disable injected scripts
4-	– Preventing transmission of confidential information • Anti-Phishing toolbars • Black listing • Screen-based data entry(e.g. graphical challenges) • Mutual authentication • Rendering data entry and making it useless • Trusted paths
5-	– Tracing transmission of compromised credentials • Take down phishing servers before data transmission
6-	– Interfering with the use of compromised information • Multi-factor authentication(e.g. finger prints) • Password hashing • Transaction confirmation • Policy-based data
7-	– Interfering with the financial benefit • Delay transactions • Detect flow of monetary gain

G. URL Spoofing Techniques

Table G.1 – URL Spoofing techniques

URL spoofing technique	Article
Bad domain name	Moore and Clayton 2007
• **Real domain** http://onlinebanking.realbank.com	Yadav et al. 2010
• **Fake domain**	Felegyhazi et al. 2010
http://realbankS.com	Yee and Sitaker 2006
http://realbamk.com	Herzberg and Jbara 2008
http://onlinebanking.realbankS.com	Prakash et al. 2010
http://onlinebanking.realbamk.com	Ramesh et al. 2014
	Ramzan and Cooley 2014
Shortened URLs	Chhabra et al. 2011
• Real domain http://www.zscaler.com/download-whitepaper_stateofweb-q4-2009.html	McGrath and Gupta 2008
• Short URL	Niu et al. 2008
http://bit.ly/cikl0z	Klien and Strohmaier 2012
• Redirection (fake domain)	Lee and Kim 2012
http://www.zcaler.com/download-whitepaper_stateofweb-b4-2009.html	Gastellier-Prevost et al. 2011
	Chu et al. 2010
	Nikiforakis et al. 2014
Host name obfuscation	Garera et al. 2007
• **Real domain** http://onlinebanking.realbank.com	Chandrasekaran et al. 2006
• **Obfuscated URL**	Tseng et al. 2011
http://realbankS.com (IP: 173.193.212.4)	Rader and Rahman 2013
• **Obfuscated URL as IP Address**	Su et al. 2013
http://173.193.212.4/.	Silva et al. 2015
	Banerjee and Faloutsos 2013
Encoded URL obfuscation	Chandrasekaran et al. 2006
• **Real domain** http://onlinebanking.realbank.com	Cova et al. 2008
• **Obfuscated URL**	Berghel et al. 2007
http://realbankS.com	Liu and Stamm 2007
• **Obfuscated URL (URL encoding)**	Hulten et al. 2014
http%3A%2F%2Frealbank.com+	

H. Features Used in Machine Learning-based Anti-phishing Techniques

Table H.1 – Machine learning-based anti-phishing techniques

Approach		Article	Features
Classification	Naïve Bayes	Bazarganigilani 2011	Email content
		Ma et al. 2009	Lexical features, Host-based features: IP address properties, WHOIS properties, Domain name properties, Geographic properties
		Huh and Kim 2012	Website ranking, Number of results returned in search Engines
		Aggarwal et al. 2012	Tweet content, length, hashtags, mentions, User posting the tweet, Age of the account, Number of tweets, Follower-followee ratio
		Miyamoto et al. 2008	Age of Domain, Known Images, Suspicious URL, IP Address, Dots and dashes in URL, HTML from features
	Random Forest	Fette et al. 2007	Email: IP-based URLs, Age of linked-to domain names, "Here" links to non-modal domain, HTML emails, Number of domains, Number of dots, Contains JavaScript, Spam-filter output. Website: Site in browser history, Redirected site, Term frequency-inverse document frequency(TF-IDF)
	Support Vector Machines	Ying and Xuhua 2006	DoM features and Objects: Keyword/Description (KD), Request URL (RURL), URL of Anchor (AURL), Server Form Handler (SFH), action of FORM
		Choi et al. 2011	Lexical features (LEX), Link popularity features, DNS features (DNS), Webpage content features, DNS fluxiness features (DNSF), Network features (NET)
		L'Huillier et al. 2009	Email Text
	Logistic Regression	Abu-Nimeh et al. 2007	Email header features, Email subject, Email body, Html tags
	K-nearest Neighbor	Choi et al. 2011	-
	Neural Networks	Abu-Nimeh et al. 2007	-
	Rule based	Bergholz et al. 2008	Structural features: Email body, Number of body parts, Discrete and composite body parts, Alternative body parts, Link features: Links contained in an email, Total number of links, Internal and external links, Links with IP-numbers, Deceptive links, Links behind images, Element features: scripting and in particular JavaScript, and whether forms are used, Word list features: A list of words hinting at the possibility of phishing
		Aggarwal et al. 2012	-
	Linear Discriminant Analysis	Huh and Kim 2012	-
Clustering	K-Means	Kuan-Ta et al. 2009	Webpage's image features
	DB Scan	Yearwood et al. 2009; Liu et al. 2010	Size of email, Text content, Number of visible links in an email, Greetings, Signature, Html content, script, Tables, Image, Number of hyperlink in an email, Forms, Fake tags.
	Gaussian Mixture	Jung and Lee 2010	The decoding parameter of the selectable mode vocoder (SMV) extracted from the decoding process of the transmitted speech in the mobile phone
Anomaly Detection	Rule based	Guan et al. 2009	IM Username in text, First URL message, Regular delay time of sender, Regular response time of sender, Fresh domain, IM username in URL + Low reputation of domain, E-mail address in URL, Hostname is encoded, IP is encoded, Confused URL, Domain in Google search result
		Ying and Xuhua 2006	-
		Chandrasekaran et al. 2008	Email content

Table H.1 provides a summary of specific machine learning algorithms and their input features for phishing detection. The table shows that SVM and Naïve Bayes are the most widely used phishing classifiers, and some other classification methods (e.g. Neural Networks) are the least used. Among the clustering based techniques for phishing detection, *k*-means is suitable for simple applications, and other clustering algorithms such as Gaussian Mixture (Sheikholeslami et al. 1998) have been used in more sophisticated voice phishing detection. Approaches such as one-class SVM anomaly detection (Wang et al. 2004) have not been used to detect phishing websites. Nevertheless, one-class anomaly detection techniques seem promising to detect zero-day/hour phishing – a novel phishing attempt.

I. Client Server Authentication

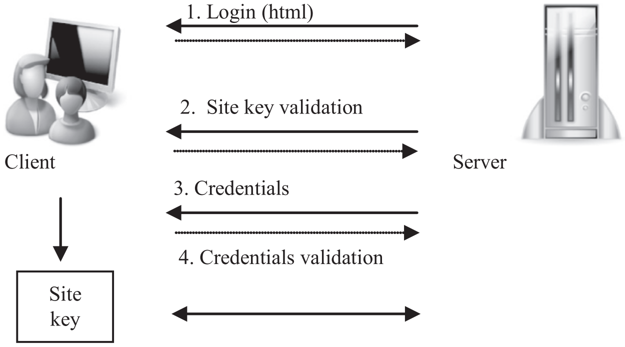


Fig. I.1 – Client server authentication approach.

Fig. I.1 illustrates a site key authentication approach. As shown in the figure, once a user has subscribed to a particular server, the site key (i.e. secret image) is stored in a user machine, which can only be accessible by the corresponding sever. As soon as the user accesses the login page, he is asked to validate his own key before entering his credentials. Once the site key is validated, the user has to provide his credentials which are also validated by server.

J. A Comparison of Anti-phishing Tools

J.1. A comparison of anti-phishing tools in relation to our taxonomy

Table J.1 – A comparison of anti-phishing tools.

Tool	Communication media	Device	Attack technique	Countermeasure type	Performance metrics	User study conducted?
Anti-phish (Kirda and Kruegel 2006)	Website/browser add-on	PC	Website spoofing	Profile matching /usage history	-	-
BogusBiter (Chuan and Haining 2010)	Website/browser add-on	PC	Website spoofing	Client server authentication	Page load delay	No
Cantina+ (Xiang et al. 2011)	Website/browser add-on	PC	Website spoofing	Machine learning /classification	TPR ≈ 0.92 FPR ≈ 0.040	No
Quero (Krammer 2006)	Website/browser add-on	PC	Website spoofing	Text mining /regular expressions	-	-
Itrustpage (Ronda et al. 2008)	Website/browser add-on	PC	Website spoofing	Profile matching/ blacklist	Accuracy=0.98	Yes
SpoofGuard (Chou et al. 2004)	Website	PC	Website spoofing	Profile matching / pattern	TPR≈0.972, Accuracy≈0.67	No
PhishCatch (Weider et al. 2009)	E-mail	PC	E-mail spoofing	Profile matching/ pattern	Accuracy≈ 0.98	No
PhishZoo (Afroz and Greenstadt 2011)	Website	PC	Website spoofing	Profile matching/ pattern	Accuracy≈0.96, FPR≈0.01	No
BayeShield (Likarish et al. 2009)	Website	PC	E-mail spoofing	User based/IQ test	Accuracy ≈ 0.75	Yes
B-APT (Likarish et al. 2008)	Website	PC	Website spoofing	Machine learning/ classification	Page load delay ≈ 51.05ms, TPR≈1,FP≈0.03	No
PhishTester (Shahriar and Zulkernine 2010)	Website	PC	Website spoofing/ Web forms	Profile matching/ pattern	FNR≈0.03, FPR≈0	No
DOM AntiPhish (Rosiello et al. 2007)	Website	PC	Website spoofing	Profile matching/ layout	FNR≈0, FPR≈0.16	No
GoldPhish (Dunlop et al. 2010)	Website	PC	Website spoofing	Search engines	TPR≈0.98,FPR≈0.02	No
PhishNet (Prakash et al. 2010)	Website	PC	Website spoofing	Profile matching /blacklist	FNR≈0.05, FPR≈0.03	No
PhorceField (Hart et al. 2011)	Website	PC	Website spoofing	Client server authentication	Bits of Security Lost per user = 0.2	Yes
PassPet (Yee and Sitaker 2006)	Website	PC	Website spoofing	Profile matching/ usage history	Security and Usability	Yes
PhishGuard (Joshi et al. 2008)	Website	PC	Website spoofing	Client server authentication	-	-
PhishAri (Aggarwal et al. 2012)	Social network	PC	Website spoofing	Machine learning /classification	Precision = 0.95, Recall = 0.92	Yes
MobiFish (Wu et al. 2014)	Mobile	Smart Phone	Website spoofing	Profile matching/ layout	TPR≈1	No
AZ-protect (Abbasi et al. 2010)	Website	PC	Website spoofing	Machine learning /classification	Precision = 0.97, Recall = 0.96	No
eBay AG (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Machine learning /classification	Precision = 1, Recall = 0.55	No
Netcraft (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Profile matching /blacklist	Precision = 0.99, Recall =0.86	No
EarthLink (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Profile matching /blacklist	Precision = 0.99, Recall = 0.44	No
IE Filter (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Profile matching /blacklist	Precision = 1, Recall = 0.75	No
FirePhish (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Profile matching /blacklist	Precision = 1, Recall = 0.77	No
Sitehound (Abbasi et al. 2010)	Website/browser add-on	PC	Website spoofing	Profile matching /blacklist	Precision = 1, Recall = 0.23	No

Table J.2 – Raw ranks of anti-phishing tools: ranking of anti-phishing tools*.

Tool	A	FPR	TPR	TNR	FNR	BLC&TPRO	UM*
AZ-protect	0.164179	0.1486486	0.0357143	0.26087	0.142857	NA	NA
eBay AG	0.119403	0.1081081	0.1071429	0.130435	0.178571	NA	NA
Netcraft	0.134328	0.1216216	0.1428571	0.26087	0.107143	0.142857	0
spoofGuard	0.134328	0.1216216	0.1428571	0.217391	0.035714	NA	0.666667
Earthlink	0.134328	0.0810811	0	0	0.071429	NA	NA
IE Filter	0.059701	0.0405405	0.0714286	0.086957	0.107143	0.071429	0.333333
FirePhish	0.059701	0.0540541	0.0714286	0.043478	0.214286	0.214286	NA
Sitehound	0.059701	0.0540541	0.2142857	0	0.071429	NA	NA
Google Chrome	0.134328	0.1216216	0.2142857	NA	0.035714	0.214286	NA
McAfee Siteadvisor	0	NA	NA	NA	NA	0	NA
Symantec	0	NA	NA	NA	NA	0.357143	NA
Cloudmark	0	0.0405405	NA	NA	NA	0	NA
GeoTrust TrustWatch	0	0.0810811	NA	NA	0.035714	NA	NA
Netscape	0	0.027027	NA	NA	NA	0	NA

NA: missing values. UM: usability measures.

K. A comparison of Commercial Anti-phishing Tools

Table K.1 – Comparison of commercial tools.

Tools aspect	MarkMonitor[1]	VeriSign[2]	Cyveillance[3]	GlobalSign[4]	Internet Identity[5]	GoDaddy[6]	PhishLabs[7]	BrandProtect[8]	FraudWatch International[9]	Websense[10]	Panda[11]	RSA® FraudAction[12]	Telefónica[13]	Easy Solutions[14]	Iconix[15]	Wombat Security[16]	Kaspersky[17]	VASCO Data Security[18]
Detect, analyze attacks	√	√	√				√		√	√	√	√		√				
Takedown	√		√		√		√	√	√			√	√	√				
Fraud analysis	√		√				√	√	√			√		√				
Forensic services	√						√			√								
Email authentication	√	√				√												
Email filtering	√	√				√	√								√	√		
Web filtering	√		√				√			√		√					√	
Hardware based 2-factor authentication			√									√		√				√
Software-based strong authentication				√								√		√				
Mutual authentication			√	√										√				
Law enforcement enablement	√		√					√				√						
Security awareness and training																	√	
Prevent cousin domain	√	√	√	√	√	√	√	√	√									

(continued on next page)

Table K.1 – (*continued*)

Tools aspect	MarkMonitor[1]	VeriSign[2]	Cyveillance[3]	GlobalSign[4]	Internet Identity[5]	GoDaddy[6]	PhishLabs[7]	BrandProtect[8]	FraudWatch International[9]	Websense[10]	Panda[11]	RSA® FraudAction[12]	Telefónica[13]	Easy Solutions[14]	Iconix[15]	Wombat Security[16]	Kaspersky[17]	VASCO Data Security[18]
Communication Media	W, E	E	W	W	W	W, E	W, E	E	W	W, E	W, E	W	W	W, E	E	E	W	W
Device(s)	PC	PC	PC	PC	PC	PC	PC, Phone	PC, Phone	PC	PC	PC	PC	PC, Phone	PC	PC	PC	PC	PC
Attack technique(s)	Fast flux	Spear phishing	Website Spoofing	Website Spoofing	Website Spoofing	Website, email Spoofing	Vishing, spear phishing	Email spoofing	Website	Spear phishing	Website, email Spoofing	Website Spoofing	Website, email Spoofing	Email spoofing	Email spoofing	Spear phishing	Website spoofing	Website spoofing
Countermeasure(s)	Blacklist	Machine learning	Machine learning	Client server authentication	Machine learning	Blacklist	Machine learning	Machine learning	Blacklist	User training	Pattern matching	Machine learning	Machine learning	Client server authentication	Client server authentication	User Training	Black List	Client server authentication

[1] http://www.markmonitor.com.
[2] http://www.verisign.com.
[3] http://www.cyveillance.com.
[4] http://www.globalsign.net.
[5] http://www.internetidentity.com.
[6] http://www.godaddy.com.
[7] http://www.phishlabs.com.
[8] www.brandprotect.com.
[9] http://www.fraudwatchinternational.com.
[10] http://www.websense.com.
[11] http://www.pandasoftware.com.
[12] http://www.rsa.com.
[13] http://www.telefonica.es/.
[14] www.easysol.net.
[15] http://www.iconix.com.
[16] http://www.vasco.com.
[17] http://www.kaspersky.com.
[18] http://www.wombatsecurity.com/training-methodology.

REFERENCES

Aaron G, Rasmussen R. Global phishing survey: trends and domain name use in 2H2013; 2013. Available from: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf.

Abad C. The economy of phishing: a survey of the operations of the phishing market. First Monday 2005;10(9).

Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):237–48.

Abbasi A, Zhang Z, Zimbra D, Chen H, Nunamaker JF Jr. Detecting fake websites: the contribution of statistical learning theory. MIS Q 2010;435–61.

Abu-Nimeh S, Nappa D, Wang X, Nair S. A comparison of machine learning techniques for phishing detection. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, PA: ACM; 2007. p. 60–9 doi:10.1145/1299015.1299021. 1299021.

Aburrous M, Hossain MA, Thabatah F, Dahal K. Intelligent phishing website detection system using fuzzy techniques. In: ICTTA 2008. 3rd international conference on information and communication technologies: from theory to applications. IEEE; 2008. p. 1–6.

Adida B, Hohenberger S, Rivest RL. Fighting phishing attacks: a lightweight trust architecture for detecting spoofed emails. DIMACS Wkshp on theft in E-commerce, April 2005.

Afroz S, Greenstadt R. PhishZoo: detecting phishing websites by looking at them. In: 2011 fifth IEEE international conference on semantic computing (ICSC). Palo Alto, CA: 2011. p. 368–75 18–21 Sept.

Aggarwal A, Rajadesingan A, Kumaraguru P. PhishAri: automatic realtime phishing detection on twitter. In: eCrime researchers summit (eCrime). IEEE: 2012. p. 1–12.

Almomani A, Gupta B, Atawneh S, Meulenberg A, Almomani E. A survey of phishing email filtering techniques. IEEE Commun Surv Tutorials 2013;15(4):2070–90.

Alsaid A, Mitchell CJ. Preventing phishing attacks using trusted computing technology. In: Proceedings of the 6th international network conference (INC'06). 2006. p. 221–8.

Anandpara V, Dingman A, Jakobsson M, Liu D, Roinestad H. Phishing IQ tests measure fear, not ability. In: Financial cryptography and data security. Springer; 2007. p. 362–6.

André B, Gerhard P, Luigi DA, Domenico D. A real-life study in phishing detection. In: Proceedings of the conference on email and anti-spam (CEAS), vol. 1. 2010. p. 1–10.

Andre B, Gerhard P, Luigi D, Domenico D. A real-life study in phishing detection. Paper presented at the Proceedings of the conference on email and anti-spam (CEAS), Redmond, Washington; 2010.

Antonatos S, Polakis I, Petsas T, Markatos EP. A systematic characterization of IM threats using honeypots. In: Proceedings of the network and distributed system security symposium (NDSS). San Diego, CA: 2010.

APWG. APWG phishing solutions directory; 2014. Available from: http://docs.apwg.org/solutions.html#cousin.

Arachchilage NAG, Love S, Beznosov K. Phishing threat avoidance behaviour: an empirical investigation. Comput Human Behav 2016;60:185–97.

Aycock J. A design for an anti-spear-phishing system. In: 7th virus bulletin international conference. Vienna, Austria: Citeseer; 2007. p. 290–3.

Banerjee A, Faloutsos M. Automated identification of phishing, phony and malicious web sites. 2013. Google Patents.

Bartoli A, Davanzo G, De Lorenzo A, Medvet E, Sorio E. Automatic synthesis of regular expressions from examples. Computer 2014;12:72–80.

Baset M. QRLJacking attack; 2017. Available from: https://github.com/OWASP/QRLJacking/wiki/QRLJacking-Attack.

Basnet RB, Sung AH, Liu Q. Rule-based phishing attack detection. In: International conference on security and management (SAM 2011). Las Vegas, NV: 2011.

Bazarganigilani M. Phishing e-mail detection using ontology concept and naïve Bayes algorithm. Int J Res Rev Comput Sci 2011;2(2):249–52.

Berghel H, Carpinter J, Jo Y. Phish phactors: offensive and defensive strategies. Adv Comput 2007;70:223–68.

Bergholz A, Chang JH, Paass G, Reichartz F, Strobel S. Improved phishing detection using model-based features. In: CEAS. 2008.

Berry MW, Castellanos M. Survey of text mining. Comput Rev 2004;45(9):548.

Bhakta R, Harris IG. Semantic analysis of dialogs to detect social engineering attacks. In: IEEE international conference on semantic computing (ICSC). IEEE; 2015. p. 424–7.

Bicakci K, Unal D, Ascioglu N, Adalier O. Mobile authentication secure against man-in-the-middle attacks. In: 2nd IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud). IEEE; 2014. p. 273–6.

Blatz J. CSRF: attack and defense. 2007. McAfee Foundstone Professional Services, White Paper.

Blythe M, Petrie H, Clark JA. F for fake: four studies on how we fall for phish. In: Proceedings of the SIGCHI conference on human factors in computing SYSTEMS. ACM; 2011. p. 3469–78.

Borsack R, Lifson M. The truth about social media identity theft: perception versus reality; 2010. Available from: http://www.businesswire.com/news/home/20100621005370/en/Truth-Social-Media-Identity-Theft-Perception-Reality.

Bose I, Leung ACM. Assessing anti-phishing preparedness: a study of online banks in Hong Kong. Decis Support Syst 2008;45(4):897–912.

Bozkir AS, Sezer EA. Use of HOG descriptors in phishing detection. In: 4th international symposium on digital forensic and security (ISDFS). IEEE: 2016. p. 148–53.

Braun B, Koestler J, Posegga J, Johns M. A trusted UI for the mobile web. In: ICT systems security and privacy protection. Springer; 2014. p. 127–41.

Bulakh V, Gupta M. Countering phishing from brands' vantage point. Paper presented at the Proceedings of the 2016 ACM on international workshop on security and privacy analytics, New Orleans, Louisiana, USA; 2016.

Bühler T, Hein M. Spectral clustering based on the graph p-Laplacian. In: Proceedings of the 26th annual international conference on machine learning. ACM; 2009. p. 81–8.

Canova G, Volkamer M, Bergmann C, Borza R, Reinheimer B, Stockhardt S, et al. Learn to spot phishing URLs with the android NoPhish app. In: Information security education across the curriculum. Springer; 2015. p. 87–100.

Cao Y, Han W, Le Y. Anti-phishing based on automated individual white-list. In: Proceedings of the 4th ACM workshop on digital identity management. ACM; 2008. p. 51–60.

Caputo DD, Pfleeger SL, Freeman JD, Johnson ME. Going spear phishing: exploring embedded training and awareness. IEEE Secur Priv 2014;12(1):28–38.

Carlson EL. Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow. Elder Law J 2006;14:423.

Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM Comput Surv 2009;41(3):15.

Chandrasekaran M, Narayanan K, Upadhyaya S. Phishing email detection based on structural properties. In: NYS cyber security conference. Albany, NY: 2006. p. 1–7.

Chandrasekaran M, Sankaranarayanan V, Upadhyaya S. CUSP: customizable and usable spam filters for detecting phishing emails. In: 3rd annual symposium on information assurance (ASIA'08). Albany, NY: Citeseer; 2008. p. 10.

Chang J-H, Lee K-H. Voice phishing detection technique based on minimum classification error method incorporating codec parameters. Signal Process IET 2010;4(5):502–9. doi:10.1049/iet-spr.2009.0066.

Chen C, Dick S, Miller J. Detecting visually similar web pages: application to phishing detection. ACM Trans Internet Technol 2010;10(2):5.

Chen C-M, Guan D, Su Q-K. Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. Inf Sci (Ny) 2014;289:133–47.

Chen J, Chuanxiong G. Online detection and prevention of phishing attacks. In: 2006 first international conference on communications and networking in China. IEEE; 2006. p. 1–7.

Cheng H, Wang P, Pu S. Identify fixed-path phishing attack by STC. In: Proceedings of the 8th annual collaboration, electronic messaging, anti-abuse and spam conference. ACM; 2011. p. 172–5.

Chhabra S, Aggarwal A, Benevenuto F, Kumaraguru P. Phi. sh/$ oCiaL: the phishing landscape through short URLs. In: The 8th annual collaboration, electronic messaging, anti-abuse and spam conference. Perth, WA: ACM; 2011. p. 92–101.

Choi H, Zhu BB, Lee H. Detecting malicious web links and identifying their attack types. Paper presented at the Proceedings of the 2nd USENIX conference on web application development, Portland. 2011.

Chou N, Ledesma R, Teraguchi Y, Boneh D, Mitchell JC. Client-side defense against web-based identity theft. In: 11th annual network and distributed system security symposium (NDSS'04). San Diego, CA: 2004.

Chu Z, Gianvecchio S, Wang H, Jajodia S. Who is tweeting on Twitter: human, bot, or cyborg? In: Proceedings of the 26th annual computer security applications conference. Austin, TX: ACM; 2010. p. 21–30.

Cova M, Kruegel C, Vigna G. There is no free phish: an analysis of ″free″ and live phishing kits. WOOT 2008;8:1–8.

Dhamija R, Tygar JD. The battle against phishing: dynamic Security Skins. Paper presented at the Proceedings of the 2005 symposium on usable privacy and security, Pittsburgh, Pennsylvania; 2005.

Dhamija R, Tygar JD, Hearst M. Why phishing works. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM; 2006. p. 581–90.

Ding Y, Meng X, Chai G, Tang Y. User identification for instant messages. In: International conference on neural information processing. Berlin, Heidelberg: Springer; November 2011. p. 113–20.

Dodge RC, Carver C, Ferguson AJ. Phishing for user security awareness. Comput Secur 2007;26(1):73–80.

Downs JS, Holbrook MB, Cranor LF. Decision strategies and susceptibility to phishing. In: Proceedings of the second symposium on usable privacy and security. ACM; 2006. p. 79–90.

Downs JS, Holbrook M, Cranor LF. Behavioral response to phishing risk. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, PA: ACM; 2007. p. 37–44.

Drake CE, Oliver JJ, Koontz EJ. Anatomy of a phishing email. In: Proceedings of CEAS the first conference on email and anti-spam (CEAS), vol. 11. Mountain View, CA: 2004.

Dunlop M, Groat S, Shelly D. Goldphish: using images for content-based phishing analysis. In: Fifth international conference on internet monitoring and protection (ICIMP). IEEE; 2010. p. 123–8.

Dwyer P, Duan Z. MDMap: assisting users in identifying phishing emails. In: Proceedings of 7th annual collaboration, ELECTRONIC messaging, Anti-ABUSE and spam conference (CEAS). Redmond, WA: 2010.

Egele M, Stringhini G, Kruegel C, Vigna G. COMPA: detecting compromised accounts on social networks. In: NDSS. 2013.

Egelman S, Cranor LF, Hong J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM; 2008. p. 1065–74.

El-Wakdy M, El-Sehely E, El-Tokhy M, El-Hennawy A. Speech recognition using a wavelet transform to establish fuzzy inference system through subtractive clustering and neural network (ANFIS). Paper presented at the Proceedings of the 12th WSEAS international conference on systems, Heraklion, Greece. 2008.

Emigh A. Online identity theft: phishing technology, chokepoints and countermeasures. Washington, DC: Identity Theft Technology Council; 2005.

FBI. Smishing and vishing; 2010. Federal Bureau of Investigation. Available from: https://www.fbi.gov/news/stories/2010/november/cyber_112410/cyber_112410.

Felegyhazi M, Kreibich C, Paxson V. On the potential of proactive domain blacklisting. LEET 2010;10:6.

Felt AP, Wagner D. Phishing on mobile devices. In: Web 2.0 security and privacy workshop. Oakland, CA: 2011.

Felten EW, Balfanz D, Dean D, Wallach DS. Web spoofing: an internet con game. In: Proceedings of NISSC '97, vol. 28. Baltimore, MD: 1997. p. 6–8 Vol. 2.

Ferrara J. Social engineering and how to counteract advanced attacks. 2013. Available from: http://pittsburgh.issa.org/Social%20Engineering%20ISSA_May%202013_Final.pdf.

Fette I, Sadeh N, Tomasic A. Learning to detect phishing emails. In: Proceedings of the 16th international conference on world wide web. ACM; 2007. p. 649–56.

Florêncio D, Herley C. Password rescue: a new approach to phishing prevention. Paper presented at the Proceedings of the 1st USENIX workshop on hot topics in security, Vancouver, BC, Canada; 2006.

Fu AY, Deng X, Liu W. A potential IRI based phishing strategy. In: International conference on web information systems engineering. Springer; 2005. p. 618–19.

Fu AY, Deng X, Wenyin L. REGAP: a tool for unicode-based web identity fraud detection. J Digit Forensic Pract 2006a;1(2):83–97.

Fu AY, Wenyin L, Deng X. Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD). IEEE Trans Depend Secure Comput 2006b;3(4):301–11.

Gajek S, Sadeghi A-R. A forensic framework for tracing phishers. The future of identity in the information society. In: Fischer-Hübner S, Duquenoy P, Zuccato A, Martucci L, editors. IFIP international federation for information processing, vol. 262. Boston, MA: Springer; 2008. p. 23–35.

Gansterer WN, Pölz D. E-mail classification for phishing defense. In: Advances in information retrieval. Springer; 2009. p. 449–60.

Garera S, Provos N, Chew M, Rubin AD. A framework for detection and measurement of phishing attacks. In: Proceedings of the ACM workshop on recurring malcode. VA, USA: ACM; 2007. p. 1–8.

Gastellier-Prevost S, Granadillo GG, Laurent M. Decisive heuristics to differentiate legitimate from phishing sites. In: Network and information systems security conference (SAR-SSI). IEEE; 2011. p. 1–9.

Geer D. Security technologies go phishing. Computer 2005;38(6):18–21.

Goel N, Raman B, Gupta I. Mobile worms and viruses. Information security in diverse computing environments. In:

Advances in information security, privacy, and ethics (AISPE). IGI Global; 2014.

Gouda MG, Liu AX, Leung LM, Alam MA. SPP: an anti-phishing single password protocol. Comput Netw 2007;51(13):3715–26.

Griffin SE, Rackley CC. Vishing. In: Proceedings of the 5th annual conference on information security curriculum development. Kennesaw, GA: ACM; 2008. p. 33–5.

Gruber TR. A translation approach to portable ontology specifications. Knowl Acquis 1993;5(2):199–220.

Guan D, Chen CM, Lin JB. Anomaly based malicious URL detection in instant messaging. In: In Proceedings of the joint workshop on information security (JWIS). Kaohsiung, Taiwan: 2009.

Guan D, Chen CM, Su QK, Wang TY. Malicious URL detection on Facebook. Paper presented at the 6th joint workshop on information security, Kaohsiung, Taiwan; 2011.

Guo D, Cao J, Wang X, Fu Q, Li Q. Combating QR-Code-based compromised accounts in mobile social networks. Sensors (Basel) 2016;16(9):1522.

Gupta P, Srinivasan B, Balasubramaniyan V, Ahamad M. Phoneypot: data-driven understanding of telephony threats. In: NDSS. 2015.

Gyawali B, Solorio T, Montes-y-Gómez M, Wardman B, Warner G. Evaluating a semisupervised approach to phishing URL identification in a realistic scenario. In: Proceedings of the 8th annual collaboration, electronic messaging, anti-abuse and spam conference. ACM; 2011. p. 176–83.

Hadnagy CJ. Phishing-as-a-service (PHaas) used to increase corporate security awareness. U.S. Patent Application 14/704,148. 2015.

Hart M, Castille C, Harpalani M, Toohill J, Johnson R. PhorceField: a phish-proof password ceremony. In: Proceedings of the 27th annual computer security applications conference. ACM; 2011. p. 159–68.

Herley C, Florêncio D. A profitless endeavor: phishing as tragedy of the commons. In: Proceedings of the 2008 workshop on new security paradigms. Lake Tahoe, CA: ACM; 2009. p. 59–70.

Herzberg A, Jbara A. Security and identification indicators for browsers against spoofing and phishing attacks. ACM Trans Internet Technol 2008;8(4):16.

Herzberg A, Margulies R. Forcing Johnny to login safely. In: Computer security – ESORICS 2011. Springer; 2011. p. 452–71.

Hirschberg J, Benus S, Brenier JM, Enos F, Friedman S, Gilman S, et al. Distinguishing deceptive from non-deceptive speech. In: INTERSPEECH. 2005. p. 1833–6.

Hong J. The state of phishing attacks. Commun ACM 2012;55(1):74–81.

Hsu C-H, Huang C-Y, Chen K-T. Fast-flux bot detection in real time. In: Recent advances in intrusion detection. Springer; 2010. p. 464–83.

Huajun H, Junshan T, Lingxi L. Countermeasure techniques for deceptive phishing attack. In: NISS '09. International conference on new trends in information and service science. Gyeongju, Korea: IEEE; 2009. p. 636–41 doi:10.1109/niss.2009.80.

Huber M, Kowalski S, Nohlberg M, Tjoa S. Towards automating social engineering using social networking sites. In: International conference on computational science and engineering, vol. 3. IEEE; 2009. p. 117–24.

Huh J, Kim H. Phishing detection with popular search engines: simple and effective. Found Pract Secur 2012;6888:194–207. doi:10.1007/978-3-642-27901-0_15.

Hulten GJ, Rehfuss PS, Rounthwaite R, Goodman JT, Seshadrinathan G, Penta AP. Finding phishing sites. 2014. Google Patents.

Infosec-Institute. Spear-phishing statistics from 2014–2015; 2015. Available from: http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/.

Inomata A, Rahman SMM, Okamoto T, Okamoto E. A novel mail filtering method against phishing. In: IEEE pacific rim conference on communications, computers and signal processing (PACRIM. 2005). Victoria, BC: IEEE; 2005. p. 221–4.

Irani D, Webb S, Giffin J, Pu C. Evolutionary study of phishing. In: eCrime researchers summit, 2008. Cambridge, MA: IEEE; 2008. p. 1–10.

Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C. Reverse social engineering attacks in online social networks. In: Proceedings of the 8th international conference on detection of intrusions and malware, and vulnerability assessment. Amsterdam, The Netherlands: Springer-Verlag; 2011. 2026653. p. 55–74.

Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Commun ACM 2007;50(10):94–100.

Jain AK, Murty MN, Flynn PJ. Data clustering: a review. ACM Comput Surv 1999;31(3):264–323.

Jakobsson M, Myers S. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons; 2006.

Jakobsson M, Ratkiewicz J. Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In: Proceedings of the 15th international conference on World Wide Web. Edinburgh, UK: ACM; 2006. p. 513–22.

Jakobsson M, Soghoian C. Social engineering in phishing. Inf Assur Secur Priv Serv 2009;4:195.

Jakobsson M, Tsow A, Shah A, Blevis E, Lim Y-K. What instills trust? A qualitative study of phishing. In: Financial cryptography and data security. Springer; 2007. p. 356–61.

Joshi Y, Saklikar S, Das D, Saha S. PhishGuard: a browser plug-in for protection from phishing. In: 2nd international conference on internet multimedia services architecture and applications. IEEE; 2008. p. 1–6.

Jung C, Lee K. Voice phishing detection technique based on minimum classification error method incorporating codec parameters. Signal Processing, IET 2010;4(5):502–509. doi:10.1049/iet-spr.2009.0066.

Kang J, Lee D. Advanced white list approach for preventing access to phishing sites. In: International conference on convergence information technology, 2007. IEEE; 2007. p. 491–6.

Karapanos N, Capkun S. On the effective prevention of TLS man-in-the-middle attacks in web applications. In: 23rd USENIX security symposium (USENIX security 14). 2014. p. 671–86.

Kerremans K, Yan T, Temmerman R, Gang Z. Towards ontology-based E-mail fraud detection. In: Portuguese conference on artificial intelligence, 2005. epia 2005. Covilhã, Portugal: 5–8 Dec 2005. p. 106–11.

Kessem L. Rogue mobile apps, phishing, malware and fraud; 2012. Available from: https://blogs.rsa.com/rogue-mobile-apps-phishing-malware-and-fraud/.

Khonji M, Jones A, Iraqi Y. A study of feature subset evaluators and feature subset searching methods for phishing classification. In: Proceedings of the 8th annual collaboration, electronic messaging, anti-abuse and spam conference. ACM; 2011. p. 135–44.

Kirda E, Kruegel C. Protecting users against phishing attacks. Comput J 2006;49(5):554–61.

Klien F, Strohmaier M. Short links under attack: geographical analysis of spam in a URL shortener network. In: Proceedings of the 23rd ACM conference on Hypertext and social media. ACM; 2012. p. 83–8.

Kontaxis G, Polakis I, Ioannidis S, Markatos EP. Detecting social network profile cloning. In: 2011 IEEE international conference on pervasive computing and communications workshops (PERCOM workshops). Seattle, WA: 21–25 March 2011. p. 295–300.

Krammer V. Phishing defense against IDN address spoofing attacks. In: Proceedings of the international conference on privacy, security and trust: bridge the gap between PST technologies and business services. ACM; 2006. p. 32.

Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. J Inf Secur Appl 2015;22:113–22.

Kuan-Ta C, Jau-Yuan C, Chun-Rong H, Chu-Song C. Fighting phishing with discriminative keypoint features. IEEE Internet Comput 2009;13(3):56–63.

Kumar A. Phishing – a new age weapon. Technical report. Open Web Application Secuirtry Project (OWASP); 2005.

Kumaraguru P, Rhee Y, Acquisti A, Cranor LF, Hong J, Nunge E. Protecting people from phishing: the design and evaluation of an embedded training email system. In: Proceedings of the SIGCHI conference on human factors in computing systems. San Jose, CA: ACM; 2007a. p. 905–14.

Kumaraguru P, Rhee Y, Acquisti A, Cranor LF, Hong J, Nunge E. Protecting people from phishing: the design and evaluation of an embedded training email system. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, San Jose, California, USA. 2007b.

Kumaraguru P, Sheng S, Acquisti A, Cranor LF, Hong J. Teaching Johnny not to fall for phish. ACM Trans Internet Technol 2010;10(2):7.

Le A, Markopoulou A, Faloutsos M. Phishdef: URL names say it all. In: INFOCOM, 2011 proceedings IEEE. IEEE; 2011. p. 191–5.

Lee H, Jeun I, Chun K, Song J. A new anti-phishing method in OpenID. In: Second international conference on emerging security information, systems and technologies. IEEE; 2008. p. 243–7.

Lee K, Caverlee J, Webb S. Uncovering social spammers: social honeypots + machine learning. Paper presented at the Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval, Geneva, Switzerland. 2010.

Lee S, Kim J. WarningBird: detecting suspicious URLs in Twitter stream. In: Network & distributed system security symposium (NDSS). San Diego, CA: 2012.

Lei T, Huan L, Jianping Z. Identifying evolving groups in dynamic multimode networks. IEEE Trans Knowl Data Eng 2012;24(1):72–85. doi:10.1109/tkde.2011.159.

Lemos R. Phishing attacks increasingly focus on social networks, studies show; 2014. Available from: http://www.eweek.com/security/phishing-attacks-increasingly-focus-on-social-networks-studies-show.html.

L'Huillier G, Weber R, Figueroa N. Online phishing classification using adversarial data mining and signaling games. In: Proceedings of the ACM SIGKDD workshop on CyberSecurity and intelligence informatics. ACM; 2009. p. 33–42.

L'Huillier G, Hevia A, Weber R, Rios S. Latent semantic analysis and keyword extraction for phishing classification. In: 2010 IEEE international conference on intelligence and security informatics (ISI). Vancouver, BC: 2010. p. 129–31 23–26 May 2010.

Li L, Helenius M. Usability evaluation of anti-phishing toolbars. J Comput Virol 2007;3(2):163–84.

Likarish P, Jung E, Dunbar D, Hansen TE, Hourcade JP. B-apt: Bayesian anti-phishing toolbar. In: 2008 IEEE international conference on communications. IEEE; 2008. p. 1745–9.

Likarish P, Dunbar DE, Hourcade JP, Jung E. BayeShield: conversational anti-phishing user interface. In: SOUPS, vol. 9. 2009. p. 1.

Liping M, John Y, Paul W. Establishing phishing provenance using orthographic features. In: eCrime researchers summit, 2009. eCRIME'09. IEEE; 2009. p. 1–10.

Litan A. Increased phishing and online attacks cause Dip in consumer confidence. Gartner Study. June 2005.

Liu C, Stamm S. Fighting unicode-obfuscated spam. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, PA: ACM; 2007. p. 45–59.

Liu G, Qiu B, Wenyin L. Automatic detection of phishing target from phishing webpage. In: 20th international conference on pattern recognition (ICPR'10). IEEE; 2010. p. 4153–6.

Liu G, Xiang G, Pendleton BA, Hong JI, Liu W. Smartening the crowds: computational techniques for improving human verification to fight phishing scams. In: Proceedings of the seventh symposium on usable privacy and security. Pittsburgh, PA: ACM; 2011. p. 8.

Long B, Zhang ZM, Yu PS. A probabilistic framework for relational clustering. Paper presented at the Proceedings of the 13th ACM SIGKDD international conference on knowledge discovery and data mining, San Jose, California, USA; 2007.

Ludl C, McAllister S, Kirda E, Kruegel C. On the effectiveness of techniques to detect phishing sites. In: International conference on detection of intrusions and malware, and vulnerability assessment. Springer; 2007. p. 20–39.

Lundquist D, Zhang K, Ouksel A. Ontology-driven cyber-security threat assessment based on sentiment analysis of network activity data. In: International conference on cloud and autonomic computing (ICCAC). IEEE; 2014. p. 5–14.

Luo T, Jin X, Ananthanarayanan A, Du W. Touchjacking attacks on web in android, iOS, and windows phone. In: International symposium on foundations and practice of security. Berlin Heidelberg: Springer; October 2012. p. 227–43.

Ma J, Saul LK, Savage S, Voelker GM. Beyond blacklists: learning to detect malicious web sites from suspicious URLs. In: Proceedings of the 15th ACM SIGKDD international conference on knowledge discovery and data mining. ACM; 2009. p. 1245–54.

Malisa L, Kostiainen K, Och M, Capkun S. Mobile application impersonation detection using dynamic user interface extraction. In: European symposium on research in computer security. Springer International Publishing; September 2016. p. 217–37.

Marforio C, Masti RJ, Soriente C, Kostiainen K, Capkun S. Personalized security indicators to detect application phishing attacks in mobile platforms. arXiv preprint arXiv:1502.06824. 2015.

Marforio C, Masti R, Soriente C, Kostiainen K, Capkun S. Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. Paper presented at the Proceedings of the 6th workshop on security and privacy in smartphones and mobile devices, Vienna, Austria; 2016.

Martinovic I, Zdarsky FA, Bachorek A, Jung C, Schmitt JB. Phishing in the wireless: implementation and analysis. In: IFIP international federation for information processing. Springer; 2007.

McGrath DK, Gupta M. Behind phishing: an examination of phisher Modi Operandi. In: Proceedings of the 1st Usenix workshop on large-scale exploits and emergent threats (LEET'08), vol. 8. San Francisco, CA: 2008. p. 4.

McGrath DK, Kalafut A, Gupta M. Phishing infrastructure fluxes all the way. IEEE Secur Priv 2009;(5):21–8.

Mclean V. CYREN: cyber threats report the growing risk to business data 2015 q1; 2015. Available from: http://pages.cyren.com/TrendReport_2015Q1.html?utm_campaign=ALL_ALL_2015_Q1_Trend_Report&utm_medium=press_release&utm_source=press_release.

McRae CM, Vaughn RB. Phighting the phisher: using web bugs and honeytokens to investigate the source of phishing attacks. In: 40th annual Hawaii international conference on system sciences. IEEE; 2007. p. 270c.

Medvet E, Kirda E, Kruegel C. Visual-similarity-based phishing detection. In: Proceedings of the 4th international conference on security and privacy in communication networks. ACM; 2008. p. 22.

Meijdam KC, Pieters W, van den Berg J. Phishing as a service: designing an ethical way of mimicking targeted phishing attacks to train employees. TU Delft; 2015.

Microsoft. Phishing scams that target activities, interests, or news events, Microsoft security and safety center; 2016a. Available from: https://www.microsoft.com/en-us/safety/online-privacy/phishing-interests.aspx.

Microsoft. Sender ID filtering; 2016b. Available from: https://technet.microsoft.com/en-us/library/cc526541.aspx.

Miyamoto D, Hazeyama H, Kadobayashi Y. SPS: a simple filtering algorithm to thwart phishing attacks. Paper presented at the Proceedings of the first Asian Internet engineering conference on technologies for advanced heterogeneous networks, Bangkok, Thailand; 2005.

Miyamoto D, Hazeyama H, Kadobayashi Y. An evaluation of machine learning-based methods for detection of phishing sites. In: Advances in neuro-information processing. Springer; 2008. p. 539–46.

Modupe A, Olugbara OO, Ojo SO. Filtering of mobile short messaging service communication using latent Dirichlet allocation with social network analysis. In: Transactions on engineering technologies. Springer; 2014. p. 671–86.

Moghimi M, Varjani AY. New rule-based phishing detection method. Expert Syst Appl 2016;53:231–42.

Moore T, Clayton R. Examining the impact of website take-down on phishing. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. ACM; 2007. p. 1–13.

Moore T, Clayton R. The consequence of non-cooperation in the fight against phishing. In: 2008 eCrime researchers summit. IEEE; 2008. p. 1–14.

Moore T, Clayton R. Which malware lures work best? Measurements from a large instant messaging worm. In: APWG symposium on electronic crime research (eCrime). IEEE; 2015. p. 110.

Murtagh F. A survey of recent advances in hierarchical clustering algorithms. Comput J 1983;26(4):354–9.

Nagar N, Suman U. Prevention, detection, and recovery of CSRF attack in online banking system. In: Online banking security measures and data protection. 2016. p. 172.

Nahorney B. Symantec intelligence report; 2015. Available from: https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence-report-01-2015-en-us.pdf.

Nassar M, Niccolini S, Ewald T. Holistic VoIP intrusion detection and prevention system. In: 07 Proceedings of the 1st international conference on principles, systems and applications of IP telecommunications. New York, NY: ACM; 2007. p. 1–9.

Navarro JN, Jasinski JL. Identity theft and social networks. In: Social networking as a criminal enterprise. CRC Press; 2014. p. 69–90.

Nguyen D, Le N, Vinh T. Detecting phishing web pages based on DOM-tree structure and graph matching algorithm. In: Proceedings of the fifth symposium on information and communication technology. ACM; 2014. p. 280–5.

Nikiforakis N, Maggi F, Stringhini G, Rafique MZ, Joosen W, Kruegel C. Stranger danger: exploring the ecosystem of ad-based URL shortening services. In: Proceedings of the 23rd international conference on world wide web. Seoul, Republic of Korea: ACM; 2014. p. 51–62.

Niu Y, Hsu F, Chen H. iPhish: phishing vulnerabilities on consumer electronics. In: UPSEC'08 proceedings of the 1st conference on usability, psychology, and security, USENIX association, Berkeley, CA. 2008.

Ollmann G. The phishing guide understanding & preventing phishing attacks. IBM Internet Security Systems; 2007a.

Ollmann G. The vishing guide; 2007b. Available from: http://www.iss.net/documents/whitepapers/IBM_ISS_vishing_guide.pdf, IBM, Tech. Rep.

Oppliger R, Gajek S. Effective protection against phishing and web spoofing. In: Proceedings of the 9th IFIP TC-6 TC-11 international conference on communications and multimedia security (CMS'05). Salzburg, Austria: Springer; 2005. p. 32–41.

Pajares P, Abendan G. 2013. Available from: http://blog.trendmicro.com/trendlabs-security-intelligence/author/paulpgeloabendan/.

Parno B, Kuo C, Perrig A. Phoolproof phishing prevention. Paper presented at the Proceedings of the 10th international conference on Financial Cryptography and Data Security, Anguilla, British West Indies. 2006.

Peterson P. Email attacks: this time it's personal; 2011. Available from: http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf.

Phish tank. 2015. Available from: http://www.phishtank.com/.

Prakash P, Kumar M, Kompella RR, Gupta M. Phishnet: predictive blacklisting to detect phishing attacks. In: IEEE Proceedings of the 29th conference on Information communications. San Diego, CA: IEEE; 2010. p. 1–5.

Rader MA, Rahman SSM. Exploring historical and emerging phishing techniques and mitigating the associated security risks. Int J Netw Secur Its Appl 2013;5(4):23.

Ramanathan V, Wechsler H. Phishgillnet – phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training. EURASIP J Inf Secur 2012;2012(1):1–22.

Ramesh G, Krishnamurthi I, Kumar KSS. An efficacious method for detecting phishing webpages through target domain identification. Decis Support Syst 2014;61:12–22.

Ramzan Z. Phishing attacks and countermeasures. In: Handbook of information and communication security. Springer; 2010. p. 433–48.

Ramzan Z, Cooley S. Method and apparatus for resolving a cousin domain name to detect web-based fraud. 2014. Google Patents.

Ramzan Z, Wüest C. Phishing attacks: analyzing trends in 2006. In: Fourth conference on email and anti-spam. Mountain View, CA: Citeseer; 2007.

Raufi B, Ismaili F, Zenuni X. Modeling a complete ontology for adaptive web based systems using a top-down five layer framework. In: ITI. 2009. p. 511–18.

Robila SA, Ragucci JW. Don't be a phish: steps in user education. ACM SIGCSE Bull 2006;38(3):237–41. doi:10.1145/1140123.1140187.

Ronda T, Saroiu S, Wolman A. Itrustpage: a user-assisted anti-phishing tool. ACM SIGOPS Oper Syst Rev 2008;42(4):261–72.

Rosiello APE, Kirda E, Kruegel C, Ferrandi F. A layout-similarity-based approach for detecting phishing pages. In: Third international conference on security and privacy in communications networks and the workshops, 2007. SecureComm 2007. Nice, France: 2007. p. 454–63 17–21 Sept.

Saberi A, Vahidi M, Bidgoli BM. Learn to detect phishing scams using learning and ensemble methods. In: Proceedings of the IEEE/WIC/ACM international conferences on web intelligence and intelligent agent technology-workshops. IEEE Computer Society; 2007. p. 311–14.

Sanchez F, Duan Z. A sender-centric approach to detecting phishing emails. In: ASE international conference on cyber security (CyberSecurity). IEEE; 2012. p. 32–9.

Sanglerdsinlapachai N, Rungsawang A. Web phishing detection using classifier ensemble. In: Proceedings of the 12th international conference on information integration and web-based applications & services. ACM; 2010. p. 210–15.

Schölkopf B, Platt JC, Shawe-Taylor J, Smola AJ, Williamson RC. Estimating the support of a high-dimensional distribution. Neural Comput 2001;13(7):1443–71.

Shahriar H, Zulkernine M. PhishTester: automatic testing of phishing attacks. In: Fourth international conference on secure software integration and reliability improvement (SSIRI). IEEE; 2010. p. 198–207.

Sheikholeslami G, Chatterjee S, Zhang A. Wavecluster: a multi-resolution clustering approach for very large spatial databases. In: Proceedings of the 24th VLDB conference. New York, NY: Institute of Electrical & Electronics Engineers; 1998. p. 428–39.

Sheng S, Wardman B, Warner G, Cranor LF, Hong J, Zhang C. An empirical analysis of phishing blacklists. In: Proceedings of sixth conference on email and anti-spam (CEAS). Mountain View, CA: 2009.

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI conference on human factors in computing systems. Atlanta, GA: ACM; 2010. p. 373–82.

Shon T, Moon J. A hybrid machine learning approach to network anomaly detection. Inf Sci 2007;177(18):3799–821. doi:10.1016/j.ins.2007.03.025.

Shujun L, Schmitz R. A novel anti-phishing framework based on honeypots. In: eCrime researchers summit, 2009. eCRIME '09. Sept. 20–Oct. 21 2009. p. 1–13 doi:10.1109/ecrime.2009.5342609.

Silva SM, Zhang Y, Winsborrow E, Wu JL, Schultz CA. Network infrastructure obfuscation. 2015. Google Patents.

Smustaca. Multilingual Paypal phishing; 2011. Available from: https://aviratechblog.wordpress.com/2011/02/01/multilingual-paypal-phishing/.

Social Engineer. Phishing as a service (PHaaS) understand susceptibility to phishing & raise awareness; 2017. Available from: https://www.social-engineer.com/phishing-service/.

Song Y, Yang C, Gu G. Who is peeping at your passwords at Starbucks? To catch an evil twin access point. In: IEEE/IFIP international conference on dependable systems and networks. IEEE; 2010. p. 323–32.

Sponchioni R. The phishing economy: how phishing kits make scams easier to operate; 2015. Available from: http://www.symantec.com/connect/blogs/phishing-economy-how-phishing-kits-make-scams-easier-operate.

Stern A. Social networkers beware: Facebook is a major phishing portal, Kaspersky Lab Research; 2014. Available from: https://blog.kaspersky.com/1-in-5-phishing-attacks-targets-facebook/5180/.

Su K-W, Wu K-P, Lee H-M, Wei T-E. Suspicious URL filtering based on logistic regression with multi-view analysis. In: Eighth Asia Joint conference on information security (Asia JCIS). IEEE; 2013. p. 77–84.

Sullins L. Phishing 'For a solution: domestic and international approaches to decreasing online identity theft' (2006). Emory Int Law Rev 2006;397.

Sullivan B, Dito B, Contreras B, Klopfenstein N, McGuire C. Cybersecurity trends in Latin America and the Caribbean; 2014. Available from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.

Sun Y, Yu J, Lin S, Tseng S. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. Comput Human Behav 2016;59:249–57.

Sunil ANV, Sardana A. A pagerank based detection technique for phishing web sites. In: 2012 IEEE symposium on computers & informatics (ISCI). IEEE; 2012. p. 58–63.

Tally G, Thomas R, Van Vleck T. Anti-phishing: best practices for institutions and consumers. Technical report # 04-004. McAfee Research, Mar 2004. Available from: http://docs.apwg.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf.

Taninpong P, Ngamsuriyaroj S. Incremental adaptive spam mail filtering using naive Bayesian classification. In: 10th ACIS international conference on software engineering, artificial intelligences, networking and parallel/distributed computing, 2009. SNPD '09. 27–29 May 2009. p. 243–8. doi:10.1109/snpd.2009.45.

Taylor JM, Raskin V, Spafford EH. Ontological semantic technology goes phishing, CERIAS security seminar presentation. Purdue University; 2011. Available from: http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/7b9klvhc5urgkocuqblb1pohl0.

Toolan F, Carthy J. Feature selection for spam and phishing detection. In: eCrime researchers summit (eCrime), 2010. Dallas, TX: IEEE; 2010. p. 1–12.

Tsalis N, Virvilis N, Mylonas A, Apostolopoulos T, Gritzalis D. Browser blacklists: the Utopia of phishing protection. Paper presented at the 11th International Joint Conference on E-Business and Telecommunications, Cham. 2015.

Tseng S-S, Chen K-Y, Lee T-J, Weng J-F. Automatic content generation for anti-phishing education game. In: International conference on electrical and control engineering (ICECE). Beijing, China: IEEE; 2011. p. 6390–4.

van der Merwe A, Seker R, Gerber A. Phishing in the system of systems settings: mobile technology. In: IEEE international conference on systems, man and cybernetics, vol. 1. Waikoloa, HI: IEEE; 2005a. p. 492–8.

van der Merwe A, Seker R, Gerber A. Phishing in the system of systems settings: mobile technology. In: IEEE international conference on systems, man and cybernetics, vol. 1, Vol. 491. Corti, France: 10–12 Oct 2005b. p. 492–8.

Virvilis N, Tsalis N, Mylonas A, Gritzalis D. Mobile devices – a phisher's paradise. In: 11th international conference on security and cryptography (SECRYPT). 2014. p. 1–9.

Virvilis N, Mylonas A, Tsalis N, Gritzalis D. Security Busters: web browser security vs. rogue sites. Comput Secur 2015;52:90–105.

Wang W, Zeng G, Tang D. Using evidence based content trust model for spam detection. Expert Syst Appl 2010;37(8):5599–606. doi:10.1016/j.eswa.2010.02.053.

Wang X, Zhang R, Yang X, Jiang X, Wijesekera D. Voice pharming attack and the trust of VoIP. In: Proceedings of the 4th international conference on security and privacy in communication networks. ACM; 2008. p. 24.

Wang Y, Wong J, Miner A. Anomaly intrusion detection using one class SVM. In: Information assurance workshop, 2004. Proceedings from the fifth annual IEEE SMC. 2004. p. 358–64 doi:10.1109/iaw.2004.1437839. 10–11 June.

Weaver R, Collins MP. Fishing for phishes: applying capture-recapture methods to estimate phishing populations. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, PA: ACM; 2007. p. 14–25.

Weider Y, Nargundkar S, Tiruthani N. Phishcatch – a phishing detection tool. In: 2009 33rd annual IEEE international computer software and applications conference, vol. 2. IEEE; 2009. p. 451–6.

Wenyin L, Huang G, Xiaoyue L, Min Z, Deng X. Detection of phishing webpages based on visual similarity. In: Special interest tracks and posters of the 14th international conference on World Wide Web. Chiba, Japan: ACM; 2005. 1062868. p. 1060–1. doi:10.1145/1062745.1062868.

Wenyin L, Xiaotie D, Guanglin H, Fu AY. An antiphishing strategy based on visual similarity assessment. IEEE Internet Comput 2006;10(2):58.

Wenyin L, Fang N, Quan X, Qiu B, Liu G. Discovering phishing target based on semantic link network. Future Gen Comput Syst 2010;26(3):381–8.

Wetzel R. Tackling phishing. Bus Commun Rev 2005;35(2):46–9.

Whittaker C, Ryner B, Nazif M. Large-scale automatic classification of phishing pages. In: NDSS, vol. 10. 2010.

Wilson M, Hash J. Building an information technology security awareness and training program. NIST Spec Publ 2003;800:50.

Wright RT, Marett K. The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. J Manage Inf Syst 2010;27(1):273–303.

Wu L, Du X, Wu J. MobiFish: a lightweight anti-phishing scheme for mobile phones. In: 2014 23rd international conference on computer communication and networks (ICCCN). IEEE; 2014. p. 1–8.

Wu L, Du X, Wu J. Effective defense schemes for phishing attacks on mobile computing platforms. IEEE Trans Vehicular Technol 2016;65(8):6678–91.

Wu M. Fighting phishing at the user interface [PhD dissertation]. Massachusetts Institute of Technology. 2006.

Wu M, Miller RC, Garfinkel SL. Do security toolbars actually prevent phishing attacks? In: Proceedings of the SIGCHI conference on human factors in computing systems. Montreal, QC: ACM; 2006a. p. 601–10.

Wu M, Miller RC, Little G. Web wallet: preventing phishing attacks by revealing user intentions. In: Proceedings of the second symposium on usable privacy and security. ACM; 2006b. p. 102–13.

Wüest C. The risks of social networking; Symantec. 2010. Available from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf.

Xiang G, Hong JI. A hybrid phish detection approach by identity discovery and keywords retrieval. Paper presented at the Proceedings of the 18th international conference on world wide web, Madrid, Spain. 2009.

Xiang G, Hong J, Rose CP, Cranor L. Cantina+: a feature-rich machine learning framework for detecting phishing web sites. ACM Trans Inf Syst Secur 2011;14(2):21.

Xun D, Clark JA, Jacob JL. User behaviour based phishing websites detection. In: International multiconference on computer science and information technology, 2008. IMCSIT 2008. Wisla, Poland: 2008. p. 783–90 20–22 Oct. 2008.

Yadav S, Reddy AKK, Reddy A, Ranjan S. Detecting algorithmically generated malicious domain names. In: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. Melbourne, Vic.: ACM; 2010. p. 48–61.

Yearwood J, Webb D, Ma L, Vamplew P, Ofoghi B, Kelarev A. Applying clustering and ensemble clustering approaches to phishing profiling. In: Proc. of the 8th Australasian data mining conference (AusDM'09), vol. 101. Melbourne, Vic.: CRPIT; 2009. p. 25–34.

Yee K-P, Sitaker K. Passpet: convenient password management and phishing protection. In: Proceedings of the second symposium on usable privacy and security. Pittsburgh, PA: ACM; 2006. p. 32–43.

Ying P, Xuhua D. Anomaly based web phishing page detection. In: 22nd annual computer security applications conference (ACSAC '06). Miami Beach, FL: 2006. p. 381–92.

Youn S, McLeod D. Spam decisions on gray e-mail using personalized ontologies. Paper presented at the Proceedings of the 2009 ACM symposium on Applied Computing, Honolulu, Hawaii. 2009.

Yu WD, Nargundkar S, Tiruthani N. A phishing vulnerability analysis of web based systems. In: IEEE symposium on computers and communications. IEEE; 2008. p. 326–31.

Yue C, Wang H. BogusBiter: a transparent protection against phishing attacks. ACM Trans Internet Technol 2010;10(2):6.

Yue Z, Serge E, Lorrie C, Jason H. Phinding phish: evaluating anti-phishing tools. In: The 14th annual network and distributed system security symposium; 2006.

Zhan J, Thomas L. Phishing detection using stochastic learning-based weak estimators. In: IEEE symposium on computational intelligence in cyber security (CICS'11). IEEE; 2011. p. 55–9.

Zhang J, Luo S, Gong Z, Ouyang X, Wu C, Xin Y. Protection against phishing attacks: a survey. Int J Adv Comput Technol 2011a;3(9):155–64.

Zhang W, Ding YX, Tang Y, Zhao B. Malicious web page detection based on on-line learning algorithm. In: International conference on machine learning and cybernetics (ICMLC), vol. 4. IEEE; 2011b. p. 1914–19.

Zhang Y, Hong JI, Cranor LF. CANTINA: a content-based approach to detecting phishing web sites. In: Proceedings of the 16th international conference on world wide web. Banff, AB: ACM; 2007. 1242659. p. 639–48 doi:10.1145/1242572.1242659.

Zhou CV, Leckie C, Karunasekera S, Peng T. A self-healing, self-protecting collaborative intrusion detection architecture to trace-back fast-flux phishing domains. In: Network operations and management symposium workshops. IEEE; 2008. p. 321–7.

Zhuang W, Ye Y, Chen Y, Li T. Ensemble clustering for internet security applications. IEEE Trans Syst Man Cybern C Appl Rev 2012;42(6):1784–96.

Ahmed AlEroud is an Assistant Professor of Computer Information Systems at Yarmouk University in Jordan. He holds degrees in Information Systems (Ph.D. and M.S.) from the University of Maryland, Baltimore County, and Software Engineering (B.S.) from Hashemite University in Jordan. He was a Visiting Associate Research Scientist at the University of Maryland, Baltimore County working on Cyber Security research projects. His research work focuses on Cyber-security, Data mining for privacy preserving network data analytics, and Detection of Social Engineering Attacks.

Lina Zhou is an Associate Professor of Information Systems, University of Maryland, Baltimore County. Her research aims to improve human decision making and knowledge management through the design of intelligent technologies and understanding of human behavior. Her current research interests include deception detection, natural language processing, mobile web adaptation, ontology learning, and online social networks. Dr. Zhou has authored and/or co-authored over 50 referred articles in journals such as Journal of Management Information Systems, MIS Quarterly, Communications of the ACM, Information & Management, IEEE Transactions on Knowledge and Data Engineering. She is a member of UMBC Center for Cybersecurity.