Cybersecurity Awareness: A Critical Analysis of Education and Law Enforcement Methods

Said Baadel
Canadian University Dubai, Dubai, UAE
E-mail: s.baadel@gmail.com

Fadi Thabtah
ASDTests, Auckland, New Zealand
E-mail: fadi@asdtests.co.nz

Joan Lu
University of Huddersfield, Huddersfield, UK
E-mail: j.lu@hud.ac.uk

Keywords: anti-phishing, cyber security, embedded training, law enforcement, spear phishing

Received: October 7, 2020

According to the international Anti-Phishing Work Group (APWG), phishing activities have abruptly risen over the last few years, and users are becoming more susceptible to online and mobile fraud. Machine Learning techniques have potential for building technical anti-phishing models, with a handful already implemented in the real time environment. However, majority of them have yet to be applied in a real time environment and require domain experts to interpret the results. This gives conventional techniques a vital role as supportive tools for a wider audience, especially novice users. This paper reviews in-depth, common, phishing countermeasures including legislation, law enforcement, hands-on training, and education among others. A complete prevention layer based on the aforementioned approaches is suggested to increase awareness and report phishing to different stakeholders, including organizations, novice users, researchers, and computer security experts. Therefore, these stakeholders can understand the upsides and downsides of the current conventional approaches and the ways forward for improving them.

Povzetek: Prispevek preučuje ukrepe proti ribarjenju vključno z izobraževanjem in praktičnim usposabljanjem.

1 Introduction

Phishing is an attempt to gain sensitive personal and financial information (such as usernames and passwords, account details, and social security numbers) with malicious intent via online deception [1][2][3]. Phishing typically employs identity theft and social engineering techniques, such as creating websites that replicate existing authentic ones. Through a seemingly legitimate email that contains a hyperlink, potential users are redirected to the malicious website in order to divulge their private information and credentials [4]. Phishing techniques include *spear phishing*, which is a directed attack where emails that appear legitimate are sent to employees of a certain company in an attempt to access a company's computer system and hence gain their sensitive credentials, or *whaling,* that targets senior corporate executives [5]. These attacks require a proper understanding of the organisational structure in order for the phishing attack to be in its proper context.

Advancements in computer networks and cloud technology in recent years have resulted in an exponential growth of online and mobile commerce, where customers perform substantial online purchases [6]. This online growth has led to phishing activities reaching unprecedented levels in recent months. The Anti-Phishing Work Group (APWG), which aims to minimize online threats (including pharming, spoofing, phishing, malware, etc.) has published there Q4 report about phishing activities of 2019 [7]. The report showed that there were approximately 162,155 unique phishing websites detected in the fourth quarter of 2019, with industries providing software as a service (SaaS) and Webmail followed by payments and financial institutions as the most targeted ones. More and more users become prone to information breaches and identity theft, their trust in e-commerce or mobile commerce platforms will deteriorate, thus resulting in a huge loss of financial gains [8].

So, why is there an alarming increase in phishing activities and more users becoming susceptible to phishing scams? The answer to this can be due to inexperienced users and limited knowledge about the severity of phishing. Since phishing can be seen partly as a social problem, software tools are not able to provide a

permanent solution to it. The problem can be minimised by addressing it in three ways: educating the public on identifying fraudulent phishing websites, enforcing the law to punish scammers, and developing more intelligent intervention techniques. There are claims that anti-phishing solutions that adopt Machine Learning (ML) tend to be more practical and effective in combating phishing [9][10]. Nevertheless, the majority of the ML solutions deal with phishing as a static problem in which they only produce the classification decision from an historical dataset [11]. Continuing, the dynamic nature of phishing that involves users browsing in real time necessitates the decision to be on the fly, which makes ML approaches not fully suitable despite being around for the last decade. There are also needs to educate the online community, especially novice users, on phishing as well as to revise existing legislation.

Existing reviews on website and email phishing, such as [10] [12] [13] [14] [15] [16] have dealt with the problem from a technological solution perspective. Their reviews focused on broad anti-phishing techniques based on data mining, ML, databases, and toolbars, and only briefly discuss solutions such as law enforcement, awareness programs, user education, and training among others. To be clear, there are few discussions and critical analyses on the benefits gained by legislative law and simulated training to combat phishing. Other reviews have dismissed conventional solutions and just reviewed ML solutions [9] [17]. Therefore, the key objective of this paper is to reveal the benefits and drawbacks of the classic anti-phishing countermeasures and provide an in depth discussion on legislation, law enforcement, and user training.

The remainder of this paper is organized as follows: section 2 briefly outlines the phishing attacks procedure. In section 3, adding an anti-phishing preventive layer that includes some of the conventional countermeasures is discussed. In Section 4, some of the pros and cons of each of the countermeasures are analyzed. Section 5 then looks into an emerging phishing threat. Finally, a brief summary and conclusion are provided in Section 6.

2 Phishing attacks procedure

Phishing attacks are often initiated when an attacker sends an email to potential victims with a link that can direct them to a phony website that resembles one that is legitimate. Other initiation processes include online blogs, short message services (SMS), social media websites using web 2.0 services (such as Facebook and Twitter), peer to peer (P2P) file sharing services, and Voice over IP (VoIP) systems where spoofing caller IDs are used by attackers [18]. Each of these phishing methods have a slight variation on how the procedure is done all with the goal of defrauding the unsuspecting user. To see how the phishers design their scheme, Figure 1 below shows an example of the life cycle of a phishing attack by email where the phisher uses a common technique of adding a hyperlink to route unsuspecting users to a phony website. The procedure can be summarized as follows:

1) Phishers set up a phony website resembling a legitimate one.
2) A hypertext link is sent via email to potential victims to take immediate action such as updating their account information, resetting their password, etc. Urgency is a vital element in such an email in order to bait unsuspecting users.
3) Once the link is clicked, this action will route users to the fraudulent phishing website.
4) The fraudulent website collects vital sensitive information such as user name and password.

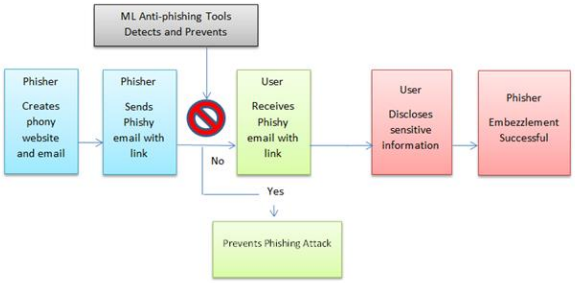

Figure 1: Phishing Attack Life-cycle.

Embezzled information can be used to access other platforms such as ebanks, emails, etc., for financial gain, identity theft, or other cybercrimes. Text of the second section.

Conventional Anti-Phishing Prevention Layer due to the broad nature and severity of phishing scams for individuals, businesses, government entities, and non-profit organisations, there have been different methods proposed in the literature to combat phishing. Among these are technical solutions that address the role of ML techniques to identify phishing features [3] [18] [19] [20] [21] [22] [23] [24] [25].

ML approaches can be seen as the first layer of prevention addressing the menace of phishing attacks. However, ML solutions alone cannot eradicate the problem due to the dynamic nature of it as well as the complexity of the outcomes that ML techniques offer to the end-user. Usually ML technique outcomes are hard to interpret by novice users, and thus are rarely applied when phishing attacks are occurring in real time. These two drawbacks limit the use of ML in commercial anti-phishing tools. There is a need to address other social approaches, such as user training and education, to raise awareness among different types of users. These conventional approaches provide an additional layer in combating phishing, as shown in figures 2 and 3.

Furthermore, developing social online communities' enables rapid data growth through users reporting their phishing experience, and thus similarities between new deceptive scams can be shared by the different stakeholders. Lastly, new legislation that can introduce harsher jail time for cybercrimes can help in reducing phishing attacks. While there is a push by government entities and academic institutions to educate the public and raise awareness about security issues, little research has been done to educate them on how to protect themselves from phishing attacks [26]. These conventional

approaches provide an additional layer in combating phishing, as shown in figures 2 & 3.

In the next section, how government and law enforcement have come around with other conventional anti-phishing approaches are examined.

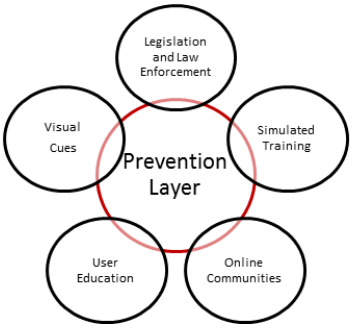

Figure 2: Complete Prevention Layer based on conventional approaches.

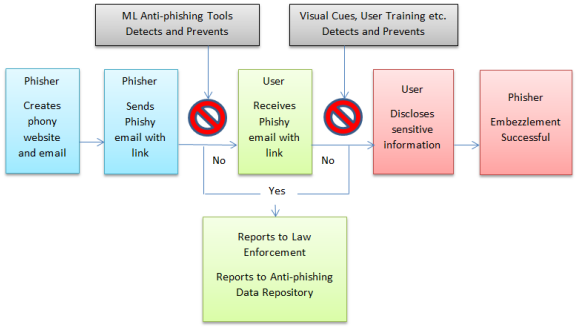

Figure 3: Phishing attack life-cycle with added layer of non-intelligent preventive techniques.

2.1 Legislation and law enforcement

Phishing scammers have the potential to target individual users and businesses, therefore legislative bills must be designed to protect different stakeholders. In the United States of America (USA) and Canada, a joint task force was formed between the U.S Department of Justice (DoJ) and the Public Safety and Emergency Preparedness Canada (PSEPC) in 2004. The primary purposes of the task force were to define the nature and scope of phishing, its impact on cross-border criminality, and to provide the public with information about common phishing techniques [27]. Later that year, the US Senate introduced a bill known as the Anti-Phishing Act of 2004 in order to have legislation at the federal level tackling phishing. After failing to make it through the senate's calendar that year, the bill was re-introduced as the Anti-Phishing Act of 2005. The aim of the bill was to amend the federal criminal code to include phishing and impose an imprisonment of up to five years for anyone found guilty of phishing. However, this bill died in the senate sub-committee reviews and never made it into law. While this legislation tried to address phishing specifically, there are other laws such as "18 U.S.C. section 1028" which do not mention phishing specifically but covers topics such as fraudulency, identity theft, and organized crime, which can be used to address phishing scams [28][29]. Adopting organized crime laws to combat cybercrimes may give law enforcement enhanced investigative powers [30][31].

At the State level, California was able to enact the Anti-Phishing Act of 2005 (named after the failed senate bill) that criminalizes phishing attacks. Businesses under this law are able to sue phishing scammers for financial damages. Individuals can claim the greatest of three times of the actual damages or five thousand dollars for every violation cited. Many other states (such as Arizona, Florida, Connecticut, Michigan, Texas, etc.) followed California's lead and enacted their own cybercrime legislations.

The United Kingdom (UK) strengthened its legal system against cybercrimes, including fraud and identity theft, by introducing a new law in 2006 called the Fraud Act. The act increased prison sentences (up to ten-years) for online fraud offences that included phishing [29][32]. The government also set up *Action Fraud*, a website dedicated to national fraud and cybercrime where users can find educational materials on different cybercrimes and have a forum for reporting any suspicious activities.

Other countries such as Canada passed a broad Anti-Spam law in December of 2010 that included phishing among other cybercrimes. The law allowed three government agencies (Canadian Radio-Television and Telecom Commission, the Competition Bureau, and The Office of the Privacy Commission) to enforce it, and even allowed the agencies to share information with other foreign states if such information is relevant to an investigation. The government of Canada has also posted information online to educate the public on the different cybercrimes, and also encourages them to report any fraud through their website.

Many other countries have enacted similar laws for combatting phishing and other cybercrimes. According to [33] [34], legislation should be designed to provide large-scale damage against individual phishers or secondary liability against Internet Service Providers (ISPs) in hopes that ISPs will be motivated to play their role in fighting phishing. The authors suggested that it can be done under the auspices of intellectual property or unfair competition laws. However, cybercrime is mostly done cross-border, and many phishing attacks have a short life-span. This brings us to two main challenges: locating the phisher and obtaining jurisdiction to enforce the law.

a) Finding and locating the phishing source:

1) Online scammers hide their identities and use secure servers in their activities. Back-tracing the IP of phishers becomes very difficult over the network.

2) Many use fake emails and register malicious domain names for their activities. There are no authentication requirements for any user when opening an email account to verify their identities. Since the internet allows a user to communicate anonymously, it is virtually impossible to locate them.

3) Even when the source is located, it has become increasingly difficult and time consuming for law enforcement to find evidence from their computer systems due to data encryption.

According to the latest APWG report, more than 195,000 domains were used for phishing in 2016, of which

more than half (95,424) were registered maliciously by phishers with 75% of them having top level domains (TLDs) from the Cocos Islands (.cc), pacific island of Palau (.pw), and Tokelau (.tk)[35]. The report also found that many phishing attacks originate from countries such as China and North Korea.

b) Obtaining jurisdiction in order to enforce the law:

1) Many online phishers tend to conduct their activities in countries that have weak cyber laws and law enforcement, and a foreign state may not have jurisdiction over those countries. In the same APWG report, more than half of those phishing domains were registered in China. A country may have strict laws on phishing and other cybercrimes yet enforcing that law will become very difficult if the cybercrime is crossing borders where they do not have any jurisdiction.

2) Phishers and other cyber criminals can simply declare bankruptcy, appeal any conviction, or deny any criminal engagement if the host country is not able to prove so or does not have cybercrime laws.

3) Requesting cyber criminals to be extradited in order to face trial is a lengthy and expensive process that could require years. Since these countries have their own sovereign jurisdiction and borders, internal investigation and prosecution is essential in order to find the culprit guilty of cybercrimes before they can even engage in the extraditing process.

These hurdles have allowed phishers to thrive under the cover of cyber networks while government agencies and law enforcement officials find it difficult to locate and prosecute the perpetrators of cybercrimes. It is therefore imperative that users are better equipped with information and hands-on training to make them aware of this problem.

2.2 Simulated training, visual cues, and user education

Phishers prey on the lack of security knowledge and computer self-efficacy of users. User education, therefore, refers to raising awareness to keep users from becoming victims of phishing attacks [36]. This can be done for instance by providing materials (online, mobile, or hard copy) on how phishing attacks occur, especially during regular work activities. On the other hand, simulated training involves techniques that are used where researchers or organizations simulate real-world phishing scenarios on their users in an experimental, safe, environment in order to track their susceptibility to phishing [37].

Research works by [38] [39] [40] [41] utilize the Elaboration Likelihood Model (ELM), designed by Petty and Cacioppo [42], which suggests that user's cognitive processing is a key reason why many fall victims to deception. How a user pays attention to cues in emails (i.e. initially noticing something fishy, what ELM classifies as "attention") and thus consequently digs deeper to search for more cues (what ELM classifies as "elaboration process"), are key factors for identifying a fraudulent website. In the next sub-section, simulated training, visual cause, and user education techniques are critically analyzed.

a) Simulated Training

A number of research studies have been conducted on simulated user training for phishing awareness [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53]. These studies involved either sending users an email with links and monitoring how they responded or making the participants aware that a simulated phishing experiment was to be conducted and are gauged on their abilities to correctly identify phishing emails. At the end of the training, users were normally given the materials and informed about their vulnerability to phishing.

Harrison, et al. [52], conducted a study at North-eastern University in the USA, where he exposed students to real-world phishing attacks in a safe simulated environment. The study used five measures: elaborations, attention, subjective email knowledge and experience, objective phishing knowledge, and individual personality-based technological innovativeness. After two weeks of students registering their email addresses, they received an email message with a hyperlink that routed them to the phishy webpage where they were asked to log in using their university credentials. Those who did not respond to the initial email were sent a second reminder to participate. The authors wanted to experiment how message factors, elaboration, and attention predicted the participant's susceptibility to phishing attacks. The authors concluded that anti-phishing efforts should focus on refining the quality of initial attention to the e-mail. They suggested that this can be attained and enhanced through educating users to pay attention to just a few key elements in the message, such as noticing red flag elements such as a hyperlink and knowing where to find the actual address that the e-mail was sent from.

Jensen, et al.[53], designed a study at a midwestern university in the USA. A generic and customized phishing message was distributed to students and staff at the university after they were asked to participate in the study. The authors created a fictitious employee email account for the study and sent two types of emails: a generic one that asked the participants to log in and try a new web portal, and a customized one with a similar message but containing the university mascot, displaying a local phone number, etc. A URL in the email directed the participants to a fictitious website where the participant's credentials were collected. The study showed that most of those who fell victim to the attack did so in the first 24 hours of the experiment. The study also concluded that brief online training was effective, and that it should be included as part of a layered set of defences to accompany automated intelligent tools in fighting phishing attacks.

An earlier study by [45], of 921 students from the University of Indiana revealed that students who received an email that was perceived to be from a friend clicked on the link 72% of the time compared to 16% when it was from an unknown address. A similar pilot study was conducted by [43], using embedded training methodology to measure phishing awareness at a university. Malicious emails were urging users to click on a link that would redirect them to a phoney website where they would input their login credentials. During the experiment, the users were interrupted immediately when they clicked the link

and were subsequently provided with training material on phishing.

[47] [48] conducted a study using an embedded training methodology where users were immediately alerted and trained after they fell victim to a simulated phishing attack. The authors argued that users become more motivated to learn about phishing attacks once they have realized that they are victims of such attacks. The authors also wanted to see how effective such a methodology was for user knowledge retention. They concluded that users will be better equipped and can learn more effectively in embedded training simulation as opposed to training sent via regular emails. In their 2009 study using PhishGuru, the authors found that this method allowed users to retain and transfer their knowledge better than with non-embedded training.

An example of a real-life application of simulation training is PhishMe Simulator [54] that was designed to enhance employee awareness and equip them with the proper tools to recognize and report phishing emails by immersing them in simulated phishing scenarios. The tool allows real-time educational opportunities the moment users take the phishing bait.

b) Visual Cues and User Education

In the Elaboration Likelihood Model (ELM), initial notice of something fishy is a crucial first step in how a user pays attention to other cues. Visual cues tend to mimic an alert system where a red flag is raised and a user who picks up on that red flag may dig deeper to search for more cues and potentially identify threats. One of the classical suggestions of human interactive proof (HIP), where online users are required to identify and verify visual cues and contents, was proposed by [55] and is known as dynamic security skins (DSS). In DSS a random image is displayed that is personal to the user prior to the user entering their password. This image can be overlaid on top of the password textboxes, making sure the user sees it and thus making it difficult for phishers to spoof the password entry.

[56] queried users to analyse some emails and gauge whether their understanding of virus attacks gave them a better understanding of web threats. The results indicated that their knowledge of negative consequences resulting from computer related crimes did not prevent the users from being vulnerable to phishing attacks. It was concluded that more specific training should be conducted, focusing on phishing attacks as opposed to providing warnings.

[57] proposed a system that embeds key information on the clients' side for the user to enter, which can then be verified at the server side. The authors introduced what is known as the completely automated public turing test to tell computers and humans apart (CAPTCHA). [58] extended this concept by adding an additional security layer consisting of a time-sensitive restriction of one-time-password (OTP).

[59] developed a game-based tutorial called *Anti-phishing Phil* that trained users on how to avoid phishing scams. The interactive game showed users how to identify phishing URLs, identify other cues on the browser, and how to distinguish between legitimate and fraudulent sites. The study concluded that users who played the game were better equipped to identify a phishing attack. A later study by [60] investigated whether an interactive mobile platform is more effective in educating users in contrast to traditional security training. A comparison of users' responsiveness to phishing was conducted, using a mobile game developed by [61] versus training through a website designed by APWG. Results indicated that users trained through the mobile application had a higher success rate of identifying phishing sites compared to their counterparts who only used the APWG website. In their recent study on phishing threat avoidance using games, [51] concluded that all their participants were convinced that the mobile game was somewhat effective compared to articles and lecture notes for enhancing their avoidance behaviour through motivation to protect themselves from phishing threats. The participants argued that mobile game-based education was fun and gave them immediate feedback, whereas lecture notes or articles provided them with little practical experience.

[50] conducted a study based on the conceptual model of Theoretical Threat Avoidance Theory (TTAT) by [62] to assess the level of computer user's knowledge on how to thwart phishing attacks. Participants were given 5 phishing URL's to assess their procedural knowledge (identify if the given URL is legitimate or suspicious) and another 5 phishing URL's to assess their conceptual knowledge (identify which part of the URL is suspicious). The results of the study concluded that the combination of procedural and conceptual knowledge positively affected self-efficacy, which enhanced the user's avoidance behaviour.

A study by [63], using improved browser security indicators and visual cues to attract attention by users in order to identify phishing websites found that there was a correlation between users gazing at the visual cues and detecting phishing sites. The study showed that users that paid attention to the visual cues had a 53% greater chance of identifying phishing websites.

These visual cues rely solely on human interventions and their abilities to utilize them at the right time. This provides a major challenge as many users tend to ignore the visual cues on the toolbars or fail to interpret some of the security cues appropriately [64][65][66]. Moreover, based on the majority of training and education research, most users are unaware of how phishing attacks start or how to visually recognise and differentiate between a fraudulent and legitimate website [22][64][67]. Many educational and training materials let users become aware of the threats, but do not necessarily provide them with the necessary skills or knowledge for protecting themselves or their organisations from such attacks [9]. While many of the educational materials used to train users on web attacks are readily available online, the vast majority of users ignore them. Some argue that of those who actually train themselves on security and cyber threats, many tend to develop a fear of doing online commerce as opposed to learning how to protect themselves and engage in it [36].

2.3 Online user communities

As users become more aware and are able to identify online scams or fall victim to phishing attacks, they may report their experience in order to prevent others from similar attacks. Users can report fraudulent websites or URL links that can then be stored in online databases. Such accumulated resources can also be used by researchers to study phishing scammers and their evolving ways of devising their scams. These online communities can also be a vital source of information regarding what different types of phishing attacks exist and their potential threats to individuals and organizations. For example, figure 4 below from the user community website Cofense, reveals that more than 90% of IT executives in the US worry about email related phishing [54].

Individuals who recognise phishing activity may report it via public anti-phishing communities. This collection of previously identified and detected phishing domain names, or URLs, is commonly referred to as a "blacklist".

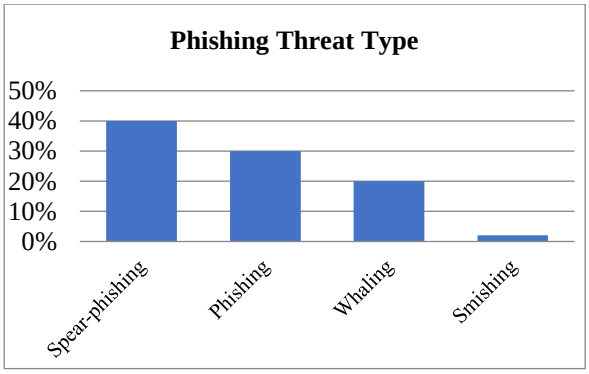

Figure 4: USA IT Executives Concerns Over Phishing Threats [54].

A blacklisted website significantly loses its user traffic and any potential revenues. However, according to [59], effectiveness of blacklists depends on:

a) frequency of the database update,

b) an accurate phishing detection rate (i.e. correctly detecting phishing instances, also known as the True Positive (TP) rate).

Google and Microsoft blacklists are commonly used by marketers, users, and businesses because of their lower false positive (FP) rates (legitimate instances that are incorrectly identified as phishing) compared to other publicly available blacklists and due to their frequency of database updates. Microsoft's blacklist is updated between every nine hours and six days, whereas Google's blacklist gets updated between twenty hours and twelve days [10]. This is a definite limitation on the blacklist approach, as phishing campaigns take significantly lower times to make their attacks before they can be detected and blocked [18] [59][68].

The online communities play an important role in raising anti-phishing awareness and keeping the conversation progressing. However, the vital part of these databases is the ability of the users to identify the fraudulent website before it could be blacklisted. Thus, users are potentially vulnerable until the URL is reported. This also highlights the importance of proactive user education and training.

3 Analysis and discussions

Table 1 below provides a brief summary of the pros and cons of the different approaches identified and discussed in section 3. A thorough analysis and discussion of the table is presented below. Some recommendations are provided as a way forward and are given in the sub-sequent sections.

3.1 Legislation and law enforcement

Many developed countries have adjusted their criminal laws to include online computer fraud, such as phishing. One of the major benefits of legislation and law enforcement is that when phishing activities are criminalized; it brings this problem to the forefront of the public eye as a criminal activity. This in turn facilitates the other two approaches discussed in this paper. Users are therefore able to engage in training in order to become aware of this criminal activity and may participate in reporting any phishing scams to the government run databases or commercial ones. Businesses that suffer from spear phishing may conduct their internal investigations, and if they are able find the perpetrator seek compensation, retribution, or protection of their brands by filing a law suit when such laws exist. Harsh jail terms and steep fines are crucial for deterring potential phishers from initiating an attack. However, some of the negatives to this approach is that many phishers are smart enough to hide their identities by using secure servers. There are no specific laws or requirements that check and verify a users' identity and details when opening an email account or registering a website [69]. Phishers therefore tend to register their websites maliciously and use fake email accounts, making it difficult to locate them. Since many attacks have a short life span, phishers can successfully defraud users and quickly shut down their activities and disappear before law enforcement is able to even begin investigating a phishing attack. While any law enforcement cannot begin before the perpetrator is caught, which as indicated can be very difficult, other issues may arise such as jurisdiction to even implement the law. If such laws cannot be enforced, then they will have little deterrent effect. It can be seen that according to the APWG, many phishing attacks originate from countries that have very lenient or weak cyber laws. Extraditing such criminals would thus be virtually impossible when such treaties do not exist between foreign states.

Countries that do not have cybercrime laws need to act and enact legislation that will criminalize these activities. A globally harmonized policy will be required in order to have a uniform definition of what amounts to cybercrime which can be implemented across all countries with similar legislations. Extradition treaties that can be enforced through law enforcement agents such as the International Police organization (INTERPOL) should then be encouraged among member countries. It is quite obvious that extradition is time consuming, not a cost-

effective process, and may require a lengthy court process in the native countries (even on crimes where the suspects have physical addresses or business), yet nonetheless, is a necessary first step toward combating this menace at a global scale. Information sharing among countries is also critical to fighting cyber criminals.

The following are a few examples of coordinated efforts from different law enforcement agencies, covering different jurisdictions, to indict cyber criminals and phishers.

i) A Florida man was indicted in Pennsylvania for a phishing scam, pretending to be a legitimate Hurricane Katrina relief website [70].

ii) A collaboration between the FBI of the US and law enforcement in Egypt netted around 80 phishers working together in an elaborate banking scam. The FBI made about 33 arrests from phishers based in Southern California, North Carolina, and Nevada [71].

iii) Indian police arrested a ring leader and mastermind of phishers who impersonated agents from the Internal Revenue Service (IRS) and US Citizenship and Immigration Services (USCIS). Following his arrest, the Department of Justice (DoJ) together with the IRS and Department of Homeland Security announced the arrest of 20 individuals in the United States in connection with the same scam and proceeded with extradition requests for the Indian arrests to be charged in the US [72].

3.2 Simulated training and user education

There are many pros as well as cons to user education and training. User training enables the user to identify phishing attacks in a simulated experiment. When the user is well trained, they are better prepared and are aware of phishing scams and other cybercrimes. Users should be trained on specifics, such as phishing attacks and how they work, as opposed to general knowledge of negative consequences to cybercrimes such as identity theft. Specific training will raise awareness and understanding of phishing, and in turn minimise users' vulnerability to phishing attacks. Some of the cons in this approach is that in the general sense, many non-technical users will resist training and learning. Researchers who utilised the Elaboration Likelihood Model (ELM) suggested that attention and elaboration is critical to identifying a fraudulent website. While these are cognitive processes, it requires behavioural adjustment to adapt the two strategies in order for a new user to not continually fall victim to numerous phishing attacks. Changing users' online interactive behaviour is not an easy feat. Users tend to ignore or pay less attention to training materials and visual cues, and many have a difficulty visually recognizing and distinguishing fraudulent sites from legitimate ones.

Awareness can be raised, and users trained on how to identify and appropriately deal with phishing scams in three ways. This can be attained through a traditional medium such as in schools and universities, through the enforcement and participation by the Internet Service Providers, or through a mobile game platform.

i) The traditional medium may raise awareness through the introduction of cybercrimes in high school, university curriculums, or even short courses offered to the community at large.

Technique	Pros	Cons	Reference
Legislation and Law Enforcement	- Incriminate phishers - Harsh jail terms, penalties and fines are a deterrent	- Difficulty in locating phishers - Jurisdiction issues when trying to implement the law	[30] [32] [33] [34]
User Education and Training	- Minimizes susceptibility to phishing attacks - Raises awareness and understanding of phishing attacks and other cybercrimes - Sharing information among organisations, employees, and other stockholders	- Users do not pay attention to visual cues - Users deal with the training as any other annual training conducted - Users ignore training materials - Users do not learn skills on how to combat phishing attacks	[11] [51] [52] [53] [63]
Online social communities approach	- Prevents users from falling victim to identified phishing URLs - Information is shared in a single platform - Data is collected that can be used for further analysis to understand causes of phishing - Past experiences are helpful for other users	- reactive approach and phishers are only blacklisted after an attack has already occurred - lack of real time blacklist update mechanism - Not possessing a high accurate phishing detection rate - Requires user intervention to make it work (users may or may not have proper education and training on phishing attacks)	[18] [10] [35]

Table 1: Summary of Anti-Phishing Countermeasures Pros and Cons.

While this can be a daunting task and require educational institutions to adopt and adjust their curricula, the strategy has proven to be effective.

This approach was partially experimented by [73] in the introduction to computing courses taken by students not pursuing a computer science education. The authors concluded in the class assessment that students had an increased level of awareness and were better able to recognise phishing scams. [74] also concluded that user education is crucial for elevating defences against phishing attacks.

ii) Internet Service Providers (ISPs) are in a position to play a larger role in the prevention of phishing attacks. By putting some of the liabilities on ISPs, [33][34] suggest that this may put pressure on the ISP to take a more proactive stance in training their employees and users and may require them to cascade such knowledge to companies using their services. This can be in the form of embedded training where employees will continuously learn as they conduct their daily work activities. Such training materials can be placed in emails, on company intranet sites, or through simulated text messaging over regular social media platforms.

iii) Mobile game platforms bring an interactive and fun approach to education and training and are somewhat more effective compared to traditional articles or lectures. Users who participated in mobile game studies argued that mobile game-based education was fun and gave them immediate feedback so that they were better equipped to identify a phishing attack after completing the game [59] [60]. Users trained through mobile application had a higher success rate of identifying phishing sites compared to their counterparts who used traditional mediums [61].

3.3 Online communities

The online communities' database approach helps prevent users from falling victim to previously blacklisted sites. This strategy can reduce the amount of people being defrauded by phishers and cut their potential revenues. However, the con for this approach is that it does not protect from zero-hour phishing. New phishing attacks need to be detected first and then blacklisted. This process takes time, and many of the well-known databases have a slow database update rate. The lack of real-time blacklist updating is a major drawback to this approach [10][18] [59][68]. This lag time is enough for the phishers to complete their attacks and move on to something else as the phishing life span is very short. Accuracy in phishing detection is very critical, and failure in this may result in legitimate sites being blacklisted.

These online communities play an important role in raising anti-phishing awareness. It serves the online community in two ways:

i) The accumulated resources can be used by researchers to study phishing scammers and their evolving ways of devising their scams.

ii) It provides a platform for novice users to share experiences and keep the conversation about phishing and other cybercrime progressing.

4 Conclusions and future work

This paper investigated common conventional anti-phishing prevention techniques, including law enforcement, legislative bills, education, simulated training, and online communities. While many countries such as the USA, Canada, and the UK have taken a lead to criminalise phishing attacks and put together harsh legislations, it is still difficult to locate attackers. This is since phishing attacks have a short life span, allowing attackers to change identity or move on before law enforcement agencies can locate them. Despite these limitations, it is still vital that government and other enforcement agencies improve their services to reduce phishing rates by sharing information and removing jurisdiction barriers.

User training and visual cues partially improve users' abilities to identify phishing. However, many novice users are still not paying high enough attention to visual cues when browsing websites, making them vulnerable to phishing attacks. Users need to be exposed, in a repetitive manner, to training about phishing since phishers continuously change their deception techniques. This approach of preventing phishing is useful for novice users, but it has proved to not be cost effective.

Online phishing communities accumulate data repositories that allow users to share useful information about phishing incidents, such as URLs that have been blacklisted and phishing experiences. This does create a knowledge base for users' online communities but requires some computer literacy as well as awareness about security indicators. In addition, due to the nature of the phishing attacks, these blacklists frequently become outdated as updates are only performed periodically rather than in real-time.

While each of the conventional methods has their own deficiencies, as a whole they reinforce each other and provide an additional layer of protection against phishing scams. Novice users can benefit tremendously by combining some of the approaches discussed in order to improve their effectiveness in identifying phishing attacks and should not rely solely on a single method. This paper also provides a clear thorough analysis and discussion on each of the countermeasures proposed as a preventive layer to better equip companies, security experts, and researchers in selecting what can work well and equip individuals with knowledge and skills that may prevent phishing attacks on a wider context within the community.

In future work, it is planned to present an anti-phishing framework in the context of IoT that integrates automated knowledge produced by computational intelligence in visual cues besides using human expert knowledge as a base.

References

[1] Aaron, G., and Rasmussen, R. (2010). *Global phishing survey: trends and domain name use in 2H 2009*. Lexington, MA: Anti-Phishing Working Group (APWG).

[2] Ramanathan, V., and Wechsler, H. (2013). Phishing detection and impersonated entity discovery using conditional random field and latent Dirichlet allocation. *Computers & Security*, 34, 123-139.

[3] Abdehamid, N. (2015). Multi-label rules for phishing classification. *Applied Computing and Informatics* 11 (1), 29-46.

[4] Atkins, B., and Huang, W. (2013). A study of social engineering in online frauds. *Open J Soc Sci*, 1(03):23-32.

[5] Afroz, A., and Greenstadt, R. (2011). PhishZoo: Detecting Phishing Websites by Looking at Them. Proceedings of the Fifth International Conference on Semantic Computing. Palo Alto, California, USA. IEEE.

[6] Abdelhamid, N., and Thabtah F. (2014). Associative Classification Approaches: Review and Comparison. *Journal of Information and Knowledge Management (JIKM)*, 13(3).

[7] Aaron, G., and Manning, R. (2020). APWG Phishing Activity Trends Reports. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf [Accessed March 10th 2020].

[8] Nguyen, L., To, B., and Nguyen H. (2015). An Efficient Approach for Phishing Detection Using Neuro-Fuzzy Model. *Journal of Automation and Control Engineering*, 3(6).

[9] Abdelhamid, N., Thabtah, F., and Abdeljaber, H. (2017). Phishing detection: A recent intelligent machine learning comparison based on models content and features. Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI), China. IEEE.

[10] Mohammad, R., Thabtah, F., and McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review Journal*, 17, 1–24.

[11] Baadel, S., Thabtah, F., Majeed, A. (2018). Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users. Proceedings of the 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference. Vancouver, Canada.

[12] Khonji, M., Iraqi, Y., and Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Surveys and Tutorials*, 15(4).

[13] Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, 20(5): 382-420.

[14] Aleroud, A., and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computer and Security*, 68: 160-196.

[15] Baadel, S., Lu, J. (2019). Data Analytics: intelligent anti-phishing techniques based on Machine Learning. Journal of Knowledge and Information Management. 18 (1) 1950005.

[16] Jain, A., Gupta, B (2017). Phishing Detection: Analysis of Visual Similarity Based Approaches. Security and Communication Networks, Volume 2017, pp. 1-20.

[17] Varshney, G., Misra, M., and Atrey, P. 2016. A survey and classification of web phishing detection schemes. *Security and Communication Networks*, 6266–6284.

[18] Abdelhamid, N., Thabtah, F., Ayesh, A. (2014). Phishing detection based associative classification data mining. *Expert systems with Applications Journal*, 41, 5948–5959.

[19] Aburrous, M., Hossain, M., Dahal, K., and Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Journal of Cognitive Computation*, 2(3): 242-253.

[20] Medvet, E., Kirda, E., and Kruegel, C. (2008). Visual-similarity-based phishing detection. Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, pp. 22:1-22:6

[21] Ma, J., Saul, L., Savage, S., and Voelker, G. (2009). Beyond blacklists: Learning to detect malicious web sites from suspicious urls. Proceedings of the 15th ACM SIGKDD, 2009, pp. 1245-1254.

[22] Mohammad, R., Thabtah, F., and McCluskey L. (2014). Predicting Phishing Websites based on Self-Structuring Neural Network. *Journal of Neural Computing and Applications*, 25 (2): 443-458.

[23] Qabajeh, I., Thabtah, F., Chiclana, F. (2015). Dynamic Classification Rules Data Mining Method. *Journal of Management Analytics*, 2(3):233-253.

[24] Thabtah, F., Mohammad, R., and McCluskey, L. (2016). A Dynamic Self-Structuring Neural Network Model to Combat Phishing. Proceedings of the 2016 IEEE World Congress on Computational Intelligence. Vancouver, Canada.

[25] Marchal, S., Saari, K., Singh, N., and Asokan, N. (2016). Know your phish: Novel techniques for detecting phishing sites and their targets. Proceedings of the IEEE 36th International Conference on Distributed Computing Systems (ICDCS).

[26] Kirlappos, I., and Sasse, M. (2012). Security education against phishing: a modest proposal for a major rethink. *Security & Privacy*, 10: 24-32.

[27] Department of Justice (2004). Report on Phishing. United States Dept. of Justice, p. 3. https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf [Accessed August. 22, 2020].

[28] Pike, G. (2006). Lost data: The legal challenges. *Information Today*, 23 (10): 1–3.

[29] Granova, A., and Eloff, J. (2005). A legal overview of phishing. *Computer Fraud & Security*, Vol. 20(7):6-11.

[30] Leukfeldt, E., Lavorgna, A., and Kleemans, E. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, 23(3):287-300.

[31] Calman, C. (2006). Bigger phish to fry: California's antiphishing statute and its potential imposition of

secondary liability on internet service providers. *Richmond Journal of Law & Technology*, 13(1): 1-24.

[32] Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law & Security Review*, 23(3):276-281.

[33] Larson, J. (2010). Enforcing intellectual property rights to deter phishing. *Intellectual Property & Technology Law Journal*, 22(1):1-8.

[34] Cassim, F. (2014). Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing. *The Comparative and International Law Journal of Southern Africa*, 47(3):401-428.

[35] Aaron, G., and Manning, R. (2020). APWG Phishing Activity Trends Reports. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf [Accessed March 10th 2020].

[36] Arachchilage, N., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: an empirical investigation. *Computers in Human Behaviour*, 60: 185–197.

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

[38] Harrison, B., Vishwanath, A., Yu, J., Ng, and Rao, R. (2015). Examining the impact of presence on individual phishing victimization. 48th Hawaii International Conference on System Sciences (HICSS), pp. 3483-3489.

[39] Vishwanath, A., Harrison, B., and Ng, Y. (2015). Suspicion, cognition, automaticity model (SCAM) of phishing susceptibility. Proceedings of the Annual Meeting of 65th International Communication Association Conference, San Juan.

[40] Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model. *Decision Support Systems*, 51(3): 576-586.

[41] Workman, M. (2008). A test of intervention for security threats from social engineering. *Information Management & Computer Security*, 16(5): 463-483.

[42] Petty, R., and Cacioppo, J. (1986). The elaboration likelihood model of persuasion. L. (Ed.), *Advances in Experimental Social Psychology, Vol 19*. New York: Academic Press, 123-205.

[43] Arachchilage, N., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L., and Hong, J. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit. Pittsburgh, PA, USA. ACM.

[44] Ronald, D., Curtis, C., and Aaron, F. (2007). Phishing for user security awareness. *Computers & Security*, 26(1): 73-80.

[45] Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10):94-100.

[46] Downs, J., Holbrook, M., and Cranor, L. (2007). Behavioral response to phishing risk. 2nd annual eCrime researcher's summit. Pittsburgh, PA. USA.

[47] Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L., et al. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. 2nd annual eCrime researchers summit, Pittsburgh, PA. USA.

[48] Kumaraguru, P., Cranshaw, J., et al. (2009). School of phish: a real-world evaluation of anti-phishing training. Proceedings of the 5th Symposium on Usable Privacy and Security Article No. 3, ACM.

[49] Aburrous, M., Hossain, M., Dahal, K., and Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Journal of Cognitive Computation*, 2(3): 242-253.

[50] Arachchilage, N., and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, 38: 304-312.

[51] Arachchilage, N., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: an empirical investigation. *Computers in Human Behaviour*, 60: 185–197.

[52] Harrison, B., Svetieva, E., and Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, 40(2):265-281.

[53] Jensen, M., Dinger, M., Wright, R., Thatcher, J. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. Journal of Management Information Systems 34(2):597-626.

[54] Cofense Report (2019). 5 Uncomfortable Truths About Phishing Defense. https://cofense.com/ [Accessed March 10th, 2020]

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

[56] Downs, J., Holbrook, M., and Cranor, L. (2007). Behavioral response to phishing risk. 2nd annual eCrime researcher's summit. Pittsburgh, PA. USA.

[57] Saklikar, S., and Saha, S. (2008). Public key-embedded graphic CAPTCHAs. Proceedings of the Consumer Communications and Networking Conference (CCNC 2008), pp. 262-6.

[58] Leung, C. (2009). Depress phishing by CAPTCHA with OTP. Proceedings of the 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication. Pp. 187-92.

[59] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., et al. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. Proceedings of the 2007 Symposium On Usable Privacy and Security, Pittsburgh, PA.

[60] Arachchilage, N., and Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3): 706-714.

[61] Arachchilage, N., and Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". International Conference on Information Society (i-Society), 485-489.

[62] Liang, X., and Xue, Y. (2010). Understanding security behaviours in personal computer usage: A

threat avoidance perspective. *Association for Information Systems*, 11(7):394-413.

[63] Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82: 69-82.

[64] Huang, H., Tan J., and Liu, L. (2009). Countermeasure techniques for deceptive phishing attack. International Conference on New Trends in Information and Service Sciences. Pg 636-641.

[65] Wu, L., Du, X., and Wu, J. (2016). Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms. IEEE Transactions on Vehicular Technology, Vol. 65, Issue: 8. IEEE.

[66] Wu, M., Miller, R., and Garfinkel, S. (2006). Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '06, pp. 601–610.

[67] Yue, C., and Wang, H. (2008). Anti-phishing in offense and defense. Proceedings of the Annual Computer Security Applications Conference (ACSAC), pp. 345-54.

[68] Sheng S., Holbrook M., Arachchilage, N., Cranor, L., and Downs, J. (2010). Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the 28th international conference on Human factors in computing systems. New York, NY, USA, 2010. ACM.

[69] Stevenson, R. (2005). Plugging the "Phishing" Hole: Legislation versus Technology. *Duke Law and Technology Review*, 2005(6).

[70] Leyden, J. (2006). Florida Man Indicted over Katrina Phishing Scam. The Register (U.K.), http://www.theregister.com/2006/08/18/hurricane_k_phishing_scam/ [Accessed Oct 10, 2019]

[71] Associated Press (2009). Dozens Charged in Phishing Scam. http://www.independent.co.uk/life-style/gadgets-and-tech/news/dozens-charged-in-phishing-scam-1799482.html [Accessed Oct 8, 2019]

[72] Phillips, K. (2017). Police Arrest Millennial Behind Multi-Million Dollar IRS Phone Scam. Forbes (US). https://www.forbes.com/sites/kellyphillipserb/2017/04/10/police-arrest-millennial-behind-multi-million-dollar-irs-phone-scam/#1bb604206ffc [Accessed Oct 6, 2019]

[73] Robila, S., and Ragucci, J. (2006). Don't be a phish: steps in user education. Proceedings of the 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education. ACM Press, New York, NY, pp. 237-41.

[74] Lungu, I., and Tabusca, A. (2010). Optimising anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. *Informatica Economica Journal*, 14(2): 27-36.