frontiers in Computer Science

REVIEW
published: 09 March 2021
doi: 10.3389/fcomp.2021.563060

Phishing Attacks: A Recent Comprehensive Study and a New Anatomy

Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan*

Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom

With the significant growth of internet usage, people increasingly share their personal information online. As a result, an enormous amount of personal information and financial transactions become vulnerable to cybercriminals. Phishing is an example of a highly effective form of cybercrime that enables criminals to deceive users and steal important data. Since the first reported phishing attack in 1990, it has been evolved into a more sophisticated attack vector. At present, phishing is considered one of the most frequent examples of fraud activity on the Internet. Phishing attacks can lead to severe losses for their victims including sensitive information, identity theft, companies, and government secrets. This article aims to evaluate these attacks by identifying the current state of phishing and reviewing existing phishing techniques. Studies have classified phishing attacks according to fundamental phishing mechanisms and countermeasures discarding the importance of the end-to-end lifecycle of phishing. This article proposes a new detailed anatomy of phishing which involves attack phases, attacker's types, vulnerabilities, threats, targets, attack mediums, and attacking techniques. Moreover, the proposed anatomy will help readers understand the process lifecycle of a phishing attack which in turn will increase the awareness of these phishing attacks and the techniques being used; also, it helps in developing a holistic anti-phishing system. Furthermore, some precautionary countermeasures are investigated, and new strategies are suggested.

Keywords: phishing anatomy, precautionary countermeasures, phishing targets, phishing attack mediums, phishing attacks, attack phases, phishing techniques

OPEN ACCESS

Edited by:
ASM Kayes,
La Trobe University, Australia

Reviewed by:
Gabriele Lenzini,
University of Luxembourg,
Luxembourg
Santiago Escobar,
Universitat Politècnica de València,
Spain

****Correspondence:***
Chaminda Hewage
chewage@cardiffmet.ac.uk

Specialty section:
This article was submitted to
Computer Security,
a section of the journal
Frontiers in Computer Science

Received: *17 May 2020*
Accepted: *18 January 2021*
Published: *09 March 2021*

Citation:
Alkhalil Z, Hewage C, Nawaf L and Khan I (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.
Front. Comput. Sci. 3:563060.
doi: 10.3389/fcomp.2021.563060

INTRODUCTION

The digital world is rapidly expanding and evolving, and likewise, as are cybercriminals who have relied on the illegal use of digital assets—especially personal information—for inflicting damage to individuals. One of the most threatening crimes of all internet users is that of 'identity theft' (Ramanathan and Wechsler, 2012) which is defined as impersonating the person's identity to steal and use their personal information (i.e., bank details, social security number, or credit card numbers, etc.) by an attacker for the individuals' own gain not just for stealing money but also for committing other crimes (Arachchilage and Love, 2014). Cyber criminals have also developed their methods for stealing their information, but social-engineering-based attacks remain their favorite approach. One of the social engineering crimes that allow the attacker to perform identity theft is called a phishing attack. Phishing has been one of the biggest concerns as many internet users fall victim to it. It is a social engineering attack wherein a phisher attempts to lure the users to obtain their sensitive information by illegally utilizing a public or trustworthy organization in an automated pattern so that the internet user trusts the message, and reveals the victim's sensitive information to the attacker (Jakobsson and Myers, 2006). In phishing attacks, phishers use social engineering techniques to redirect users to malicious websites after receiving an email and following an embedded link (Gupta et al., 2015). Alternatively, attackers could exploit other mediums to execute their attacks such as Voice over IP (VoIP), Short Message Service (SMS) and, Instant Messaging (IM) (Gupta et al., 2015). Phishers have also turned from sending mass-email messages, which target unspecified victims, into more selective phishing by sending their emails to specific victims, a technique called "spear-phishing."

Cybercriminals usually exploit users with a lack of digital/cyber ethics or who are poorly trained in addition to technical vulnerabilities to reach their goals. Susceptibility to phishing varies between individuals according to their attributes and awareness level, therefore, in most attacks, phishers exploit human nature for hacking, instead of utilising sophisticated technologies. Even though the weakness in the information security chain is attributed to humans more than the technology, there is a lack of understanding about which ring in this chain is first penetrated. Studies found that certain personal characteristics make some persons more receptive to various lures (Iuga et al., 2016; Ovelgönne et al., 2017; Crane, 2019). For example, individuals who usually obey authorities more than others are more likely to fall victim to a Business Email Compromise (BEC) that is pretending to be from a financial institution and requests immediate action by seeing it as a legitimate email (Barracuda, 2020). Greediness is another human weakness that could be used by an attacker, for example, emails that offering either great discounts, free gift cards, and others (Workman, 2008).

Various channels are used by the attacker to lure the victim through a scam or through an indirect manner to deliver a payload for gaining sensitive and personal information from the victim (Ollmann, 2004). However, phishing attacks have already led to damaging losses and could affect the victim not only through a financial context but could also have other serious consequences such as loss of reputation, or compromise of national security (Ollmann, 2004; Herley and Florêncio, 2008). Cybercrime damages have been expected to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 according to Cybersecurity Ventures (Morgan, 2019). Phishing attacks are the most common type of cybersecurity breaches as stated by the official statistics from the cybersecurity breaches survey 2020 in the United Kingdom (GOV.UK, 2020). Although these attacks affect organizations and individuals alike, the loss for the organizations is significant, which includes the cost for recovery, the loss of reputation, fines from information laws/regulations, and reduced productivity (Medvet et al., 2008).

Phishing is a field of study that merges social psychology, technical systems, security subjects, and politics. Phishing attacks are more prevalent: a recent study (Proofpoint, 2020) found that nearly 90% of organizations faced targeted phishing attacks in 2019. From which 88% experienced spear-phishing attacks, 83% faced voice phishing (Vishing), 86% dealt with social media attacks, 84% reported SMS/text phishing (SMishing), and 81% reported malicious USB drops. The 2018 Proofpoint[1] annual report (Proofpoint, 2019a) has stated that phishing attacks jumped from 76% in 2017 to 83% in 2018, where all phishing types happened more frequently than in 2017. The number of phishing attacks identified in the second quarter of 2019 was notably higher than the number recorded in the previous three quarters. While in the first quarter of 2020, this number was higher than it was in the previous one according to a report from Anti-Phishing Working Group (APWG[2]) (APWG, 2018) which confirms that phishing attacks are on the rise. These findings have shown that phishing attacks have increased continuously in recent years and have become more sophisticated and have gained more attention from cyber researchers and developers to detect and mitigate their impact. This article aims to determine the severity of the phishing problem by providing detailed insights into the phishing phenomenon in terms of phishing definitions, current statistics, anatomy, and potential countermeasures.

The rest of the article is organized as follows. *Phishing Definitions* provides a number of phishing definitions as well as some real-world examples of phishing. The evolution and development of phishing attacks are discussed in *Developing a Phishing Campaign*. *What Attributes Make Some People More Susceptible to Phishing Attacks Than Others* explores the susceptibility to these attacks. The proposed phishing anatomy and types of phishing attacks are elaborated in *Proposed Phishing Anatomy*. In *Countermeasures*, various anti-phishing countermeasures are discussed. The conclusions of this study are drawn in *Conclusion*.

PHISHING DEFINITIONS

Various definitions for the term "phishing" have been proposed and discussed by experts, researchers, and cybersecurity institutions. Although there is no established definition for the term "phishing" due to its continuous evolution, this term has been defined in numerous ways based on its use and context. The process of tricking the recipient to take the attacker's desired action is considered the *de facto* definition of phishing attacks in general. Some definitions name websites as the only possible medium to conduct attacks. The study (Merwe et al., 2005, p. 1) defines phishing as "a fraudulent activity that involves the creation of a replica of an existing web page to fool a user into submitting personal, financial, or password data." The above definition describes phishing as an attempt to scam the user into revealing sensitive information such as bank details and credit card numbers, by sending malicious links to the user that leads to the fake web establishment. Others name emails as the only attack vector. For instance, PishTank (2006) defines phishing as "a fraudulent

[1] Proofpoint is "a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions"(Proofpoint, 2019b).

[2] APWG Is "the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities" (APWG, 2020).

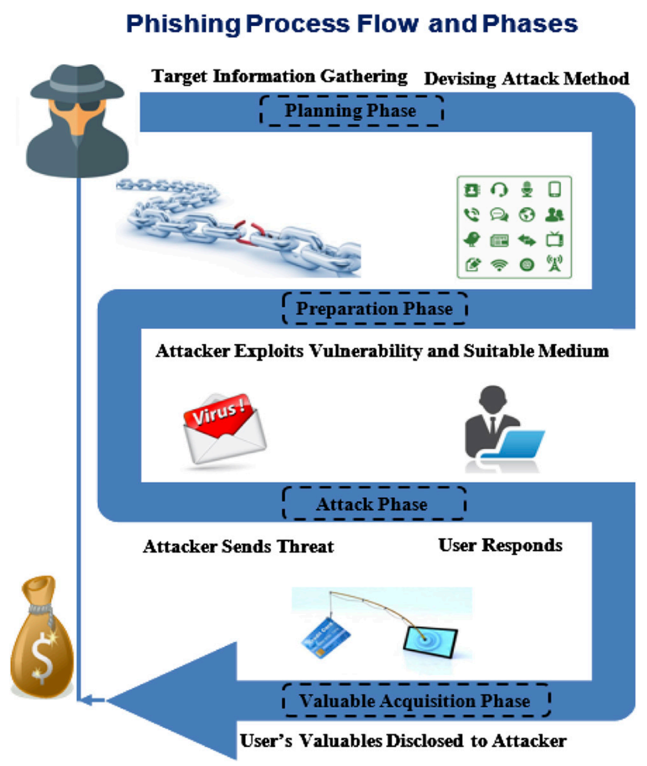

Phishing Process Flow and Phases
Target Information Gathering
Devising Attack Method
Planning Phase
Preparation Phase
Attacker Exploits Vulnerability and Suitable Medium
Virus!
Attack Phase
Attacker Sends Threat
User Responds
Valuable Acquisition Phase
User's Valuables Disclosed to Attacker

FIGURE 1 | General phishing attack process.

attempt, usually made through email, to steal your personal information." A description for phishing stated by (Kirda and Kruegel, 2005, p.1) defines phishing as "a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users." Some definitions highlight the usage of combined social and technical skills. For instance, APWG defines phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (APWG, 2018, p. 1). Moreover, the definition from the United States Computer Emergency Readiness Team (US-CERT) states phishing as "a form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity" (CISA, 2018). A detailed definition has been presented in (Jakobsson and Myers, 2006, p. 1), which describes phishing as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion. Such communications are most frequently done through emails that direct users to fraudulent websites that in turn collect the credentials in question."

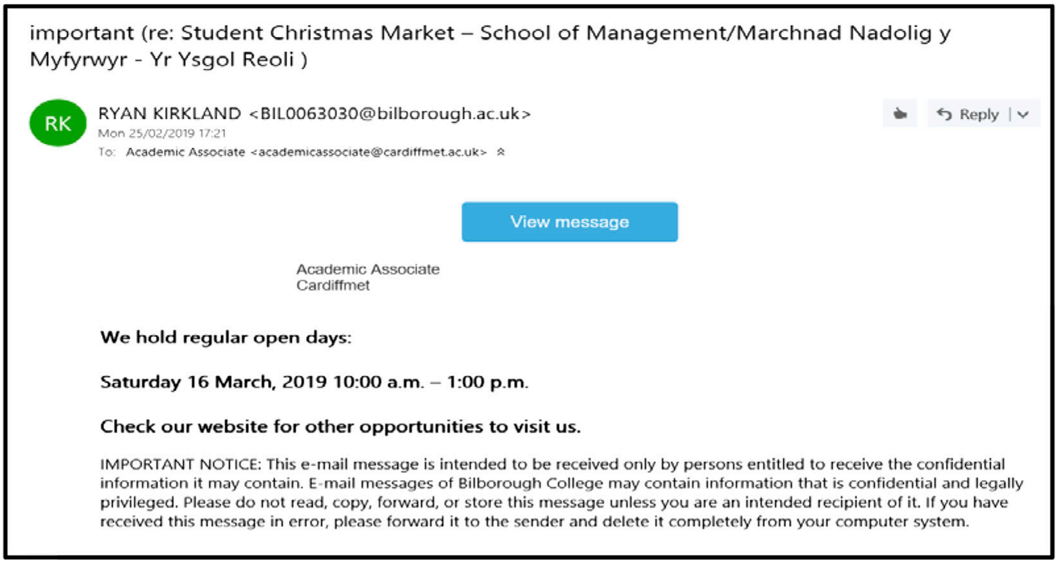
In order to understand the anatomy of the phishing attack, there is a necessity for a clear and detailed definition that underpins previous existent definitions. Since a phishing attack constitutes a mix of technical and social engineering tactics, a new definition (i.e., Anatomy) has been proposed in this article, which describes the complete process of a phishing attack. This provides a better understanding for the readers as it covers phishing attacks in depth from a range of perspectives. Various angles and this might help beginner readers or researchers in this field. To this end, we define phishing as a socio-technical attack, in which the attacker targets specific valuables by exploiting an existing vulnerability to pass a specific threat via a selected medium into the victim's system, utilizing social engineering tricks or some other techniques to convince the victim into taking a specific action that causes various types of damages.

Figure 1 depicts the general process flow for a phishing attack that contains four phases; these phases are elaborated in *Proposed Phishing Anatomy*. However, as shown in **Figure 1**, in most attacks, the phishing process is initiated by gathering information about the target. Then the phisher decides which attack method is to be used in the attack as initial steps within the planning phase. The second phase is the preparation phase, in which the phisher starts to search for vulnerabilities through which he could trap the victim. The phisher conducts his attack in the third phase and waits for a response from the victim. In turn, the attacker could collect the spoils in the valuables acquisition phase, which is the last step in the phishing process. To elaborate the above phishing process using an example, an attacker may send a fraudulent email to an internet user pretending to be from the victim's bank, requesting the user to confirm the bank account details, or else the account may be suspended. The user may think this email is legitimate since it uses the same graphic elements, trademarks, and colors of their legitimate bank. Submitted information will then be directly transmitted to the phisher who will use it for different malicious purposes such as money withdrawal, blackmailing, or committing further frauds.

Real-World Phishing Examples

Some real-world examples of phishing attacks are discussed in this section to present the complexity of some recent phishing attacks. **Figure 2** shows the screenshot of a suspicious phishing email that passed a University's spam filters and reached the recipient mailbox. As shown in **Figure 2**, the phisher uses the sense of importance or urgency in the subject through the word 'important,' so that the email can trigger a psychological reaction in the user to prompt them into clicking the button "View message." The email contains a suspicious embedded button, indeed, when hovering over this embedded button, it does not match with Uniform Resource Locator (URL) in the status bar. Another clue in this example is that the sender's address is questionable and not known to the receiver. Clicking on the fake attachment button will result in either installation of a virus or worm onto the computer or handing over the user's credentials by redirecting the victim onto a fake login page.

More recently, phishers take advantage of the Coronavirus pandemic (COVID-19) to fool their prey. Many Coronavirus-themed scam messages sent by attackers exploited people's fear of contracting COVID-19 and urgency to look for information related to Coronavirus (e.g., some of these attacks are related to Personal Protective Equipment (PPE) such as facemasks), the WHO stated that COVID-19 has created an Infodemic which is



important (re: Student Christmas Market – School of Management/Marchnad Nadolig y Myfyrwyr - Yr Ysgol Reoli)

RK RYAN KIRKLAND <BIL0063030@bilborough.ac.uk>
Mon 25/02/2019 17:21
To: Academic Associate <academicassociate@cardiffmet.ac.uk>

View message

Academic Associate
Cardiffmet

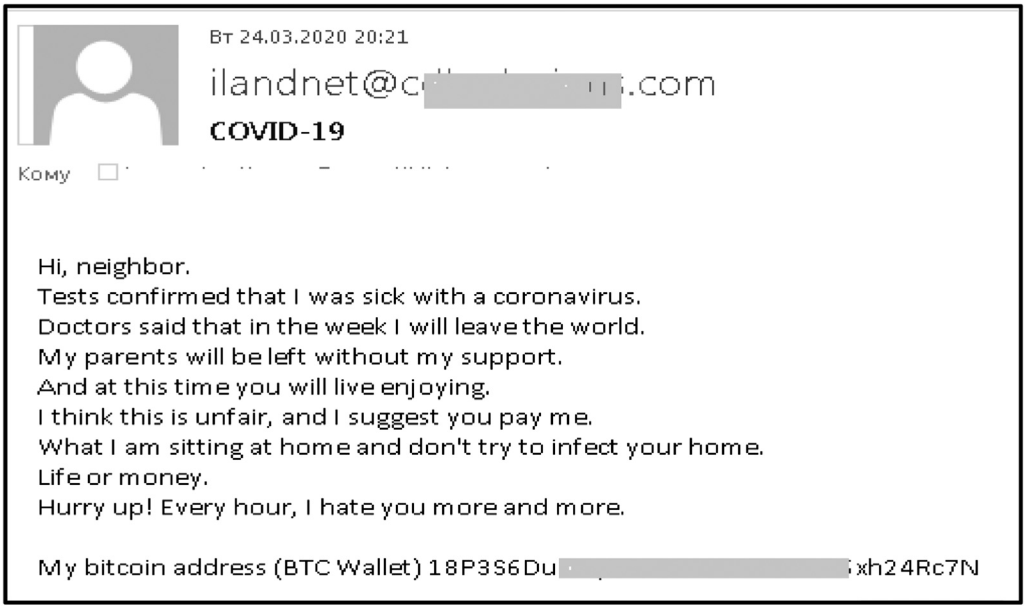
We hold regular open days:

Saturday 16 March, 2019 10:00 a.m. – 1:00 p.m.

Check our website for other opportunities to visit us.

IMPORTANT NOTICE: This e-mail message is intended to be received only by persons entitled to receive the confidential information it may contain. E-mail messages of Bilborough College may contain information that is confidential and legally privileged. Please do not read, copy, forward, or store this message unless you are an intended recipient of it. If you have received this message in error, please forward it to the sender and delete it completely from your computer system.

FIGURE 2 | Screenshot of a real suspicious phishing email received by the authors' institution in February 2019.



Вт 24.03.2020 20:21

ilandnet@c[redacted].com

COVID-19

Кому □ [redacted]

Hi, neighbor.
Tests confirmed that I was sick with a coronavirus.
Doctors said that in the week I will leave the world.
My parents will be left without my support.
And at this time you will live enjoying.
I think this is unfair, and I suggest you pay me.
What I am sitting at home and don't try to infect your home.
Life or money.
Hurry up! Every hour, I hate you more and more.

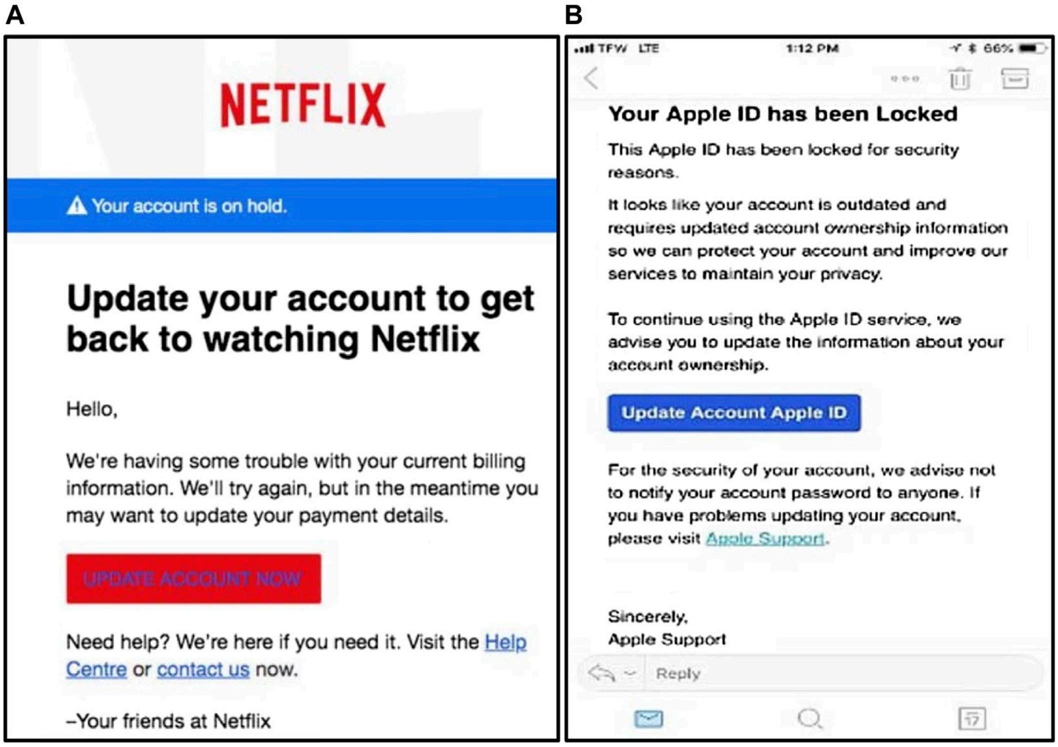
My bitcoin address (BTC Wallet) 18P3S6Du[redacted]xh24Rc7N

FIGURE 3 | Screenshot of a coronavirus related phishing email (Ksepersky, 2020).

favorable for phishers (Hewage, 2020). Cybercriminals also lured people to open attachments claiming that it contains information about people with Coronavirus within the local area.

Figure 3 shows an example of a phishing e-mail where the attacker claimed to be the recipient's neighbor sending a message in which they pretended to be dying from the virus and threatening to infect the victim unless a ransom was paid (Ksepersky, 2020).

Another example is the phishing attack spotted by a security researcher at Akamai organization in January 2019. The attack attempted to use Google Translate to mask suspicious URLs, prefacing them with the legit-looking "www.translate.google.com" address to dupe users into logging in (Rhett, 2019). That attack followed with Phishing scams asking for Netflix payment detail for example, or embedded in promoted tweets that redirect users to genuine-looking PayPal login pages. Although the tricky/bogus page was very well designed in the latter case, the lack of a Hypertext Transfer Protocol Secure (HTTPS) lock and misspellings in the URL were key red flags (or giveaways) that this was actually a phishing attempt (Keck, 2018). **Figure 4A** shows a screenshot of a phishing



NETFLIX

⚠ Your account is on hold.

Update your account to get back to watching Netflix

Hello,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now.

–Your friends at Netflix

Your Apple ID has been Locked

This Apple ID has been locked for security reasons.

It looks like your account is outdated and requires updated account ownership information so we can protect your account and improve our services to maintain your privacy.

To continue using the Apple ID service, we advise you to update the information about your account ownership.

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit Apple Support.

Sincerely,
Apple Support

FIGURE 4 | Screenshot of the **(A)** Netflix scam email and **(B)** fraudulent text message (Apple) (Keck, 2018; Rhett, 2019)

email received by the Federal Trade Commission (FTC). The email promotes the user to update his payment method by clicking on a link, pretending that Netflix is having a problem with the user's billing information (FTC, 2018).

Figure 4B shows a text message as another example of phishing that is difficult to spot as a fake text message (Pompon et al., 2018). The text message shown appears to come from Apple asking the customer to update the victim's account. A sense of urgency is used in the message as a lure to motivate the user to respond.

DEVELOPING A PHISHING CAMPAIGN

Today, phishing is considered one of the most pressing cybersecurity threats for all internet users, regardless of their technical understanding and how cautious they are. These attacks are getting more sophisticated by the day and can cause severe losses to the victims. Although the attacker's first motivation is stealing money, stolen sensitive data can be used for other malicious purposes such as infiltrating sensitive infrastructures for espionage purposes. Therefore, phishers keep on developing their techniques over time with the development of electronic media. The following sub-sections discuss phishing evolution and the latest statistics.

Historical Overview

Cybersecurity has been a major concern since the beginning of APRANET, which is considered to be the first wide-area packet-switching network with distributed control and one of the first networks to implement the TCP/IP protocol suite. The term "Phishing" which was also called carding or brand spoofing, was coined for the first time in 1996 when the hackers created randomized credit card numbers using an algorithm to steal users' passwords from America Online (AOL) (Whitman and Mattord, 2012; Cui et al., 2017). Then phishers used instant messages or emails to reach users by posing as AOL employees to convince users to reveal their passwords. Attackers believed that requesting customers to update their account would be an effective way to disclose their sensitive information, thereafter, phishers started to target larger financial companies. The author in (Ollmann, 2004) believes that the "ph" in phishing comes from the terminology "Phreaks" which was coined by John Draper, who was also known as Captain Crunch, and was used by early Internet criminals when they phreak telephone systems. Where the "f" in 'fishing' replaced with "ph" in "Phishing" as they both have the same meaning by phishing the passwords and sensitive information from the sea of internet users. Over time, phishers developed various and more advanced types of scams for launching their attack. Sometimes, the purpose of the attack is not limited to stealing sensitive information, but it could involve injecting viruses or downloading the malicious program into a victim's computer. Phishers make use of a trusted source (for instance a bank helpdesk) to deceive victims so that they disclose their sensitive information (Ollmann, 2004).

Phishing attacks are rapidly evolving, and spoofing methods are continuously changing as a response to new corresponding

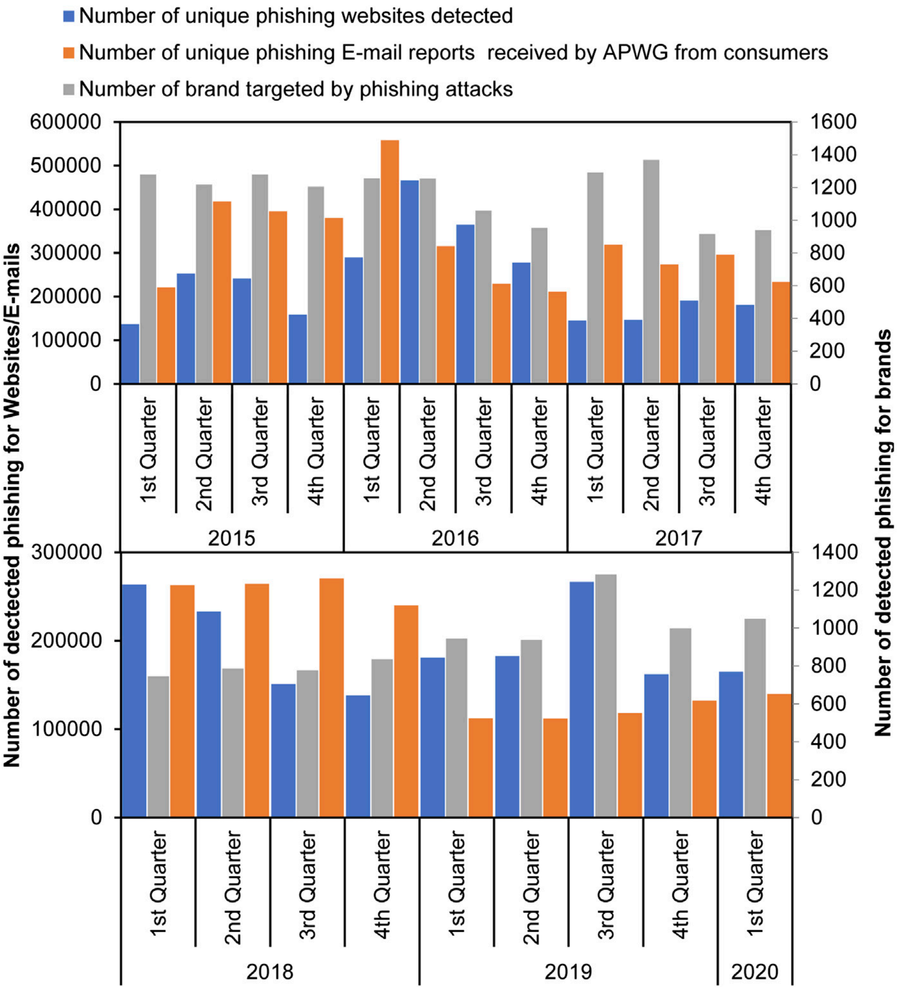


FIGURE 5 | The growth in phishing attacks 2015–2020 by quarters based on data collected from APWG annual reports.

countermeasures. Hackers take advantage of new tool-kits and technologies to exploit systems' vulnerabilities and also use social engineering techniques to fool unsuspecting users. Therefore, phishing attacks continue to be one of the most successful cybercrime attacks.

The Latest Statistics of Phishing Attacks

Phishing attacks are becoming more common and they are significantly increasing in both sophistication and frequency. Lately, phishing attacks have appeared in various forms. Different channels and threats are exploited and used by the attackers to trap more victims. These channels could be social networks or VoIP, which could carry various types of threats such as malicious attachments, embedded links within an email, instant messages, scam calls, or other types. Criminals know that social engineering-based methods are effective and profitable; therefore, they keep focusing on social engineering attacks, as it is their favorite weapon, instead of concentrating on sophisticated techniques and toolkits. Phishing attacks have reached unprecedented levels especially with emerging technologies such as mobile and social media (Marforio et al., 2015). For instance, from 2017 to 2020, phishing attacks have increased from 72 to 86% among businesses in the United Kingdom in which a large proportion of the attacks are originated from social media (GOV.UK, 2020).

The APWG Phishing Activity Trends Report analyzes and measures the evolution, proliferation, and propagation of phishing attacks reported to the APWG. **Figure 5** shows the growth in phishing attacks from 2015 to 2020 by quarters based on APWG annual reports (APWG, 2020). As demonstrated in **Figure 5**, in the third quarter of 2019, the number of phishing attacks rose to 266,387, which is the highest level in three years since late 2016. This was up 46% from the 182,465 for the second quarter, and almost double the 138,328 seen in the fourth quarter of 2018. The number of unique phishing e-mails reported to APWG in the same quarter was 118,260. Furthermore, it was found that the number of brands targeted by phishing campaigns was 1,283.

Cybercriminals are always taking advantage of disasters and hot events for their own gains. With the beginning of the

TABLE 1 | Percentage of respondents understanding multiple cybersecurity terms from different countries.

	US	United Kingdom	France	Germany	Italy	Australia	Japan
What is Phishing	65	72	65	64	70	64	62
What is Ransomware	56	60	40	31	36	58	36
What is SMishing	17	18	39	26	28	17	15
What is Vishing	20	18	15	13	24	20	12

COVID-19 crisis, a variety of themed phishing and malware attacks have been launched by phishers against workers, healthcare facilities, and even the general public. A report from Microsoft (Microsoft, 2020) showed that cyber-attacks related to COVID-19 had spiked to an unprecedented level in March, most of these scams are fake COVID-19 websites according to security company RiskIQ (RISKIQ, 2020). However, the total number of phishing attacks observed by APWG in the first quarter of 2020 was 165,772, up from the 162,155 observed in the fourth quarter of 2019. The number of these unique phishing reports submitted to APWG during the first quarter of 2020 was 139,685, up from 132,553 in the fourth quarter of 2019, 122,359 in the third quarter of 2019, and 112,163 in the second quarter of 2019 (APWG, 2020).

A study (KeepnetLABS, 2018) confirmed that more than 91% of system breaches are caused by attacks initiated by email. Although cybercriminals use email as the main medium for leveraging their attacks, many organizations faced a high volume of different social engineering attacks in 2019 such as Social Media Attacks, Smishing Attacks, Vishing Attacks, USB-based Attacks (for example by hiding and delivering malware to smartphones via USB phone chargers and distributing malware-laden free USBs) (Proofpoint, 2020). However, info-security professionals reported a higher frequency of all types of social engineering attacks year-on-year according to a report presented by Proofpoint. Spear phishing increased to 64% in 2018 from 53% in 2017, Vishing and/or SMishing increased to 49% from 45%, and USB attacks increased to 4% from 3%. The positive side shown in this study is that 59% of suspicious emails reported by end-users were classified as potential phishing, indicating that employees are being more security-aware, diligent, and thoughtful about the emails they receive (Proofpoint, 2019a). In all its forms, phishing can be one of the easiest cyber attacks to fall for. With the increasing levels of different phishing types, a survey was conducted by Proofpoint to identify the strengths and weaknesses of particular regions in terms of specific fundamental cybersecurity concepts. In this study, several questions were asked of 7,000 end-users about the identification of multiple terms like phishing, ransomware, SMishing, and Vishing across seven countries; the US, United Kingdom, France, Germany, Italy, Australia, and Japan. The response was different from country to country, where respondents from the United Kingdom recorded the highest knowledge with the term phishing at 70% and the same with the term ransomware at 60%. In contrast, the results showed that the United Kingdom recorded only 18% for each Vishing and SMishing (Proofpoint, 2019a), as shown in **Table 1**.

On the other hand, a report by Wombat security reflects responses from more than 6,000 working adults about receiving fraudulent solicitation across six countries; the US, United Kingdom, Germany, France, Italy, and Australia (Ksepersky, 2020). Respondents from the United Kingdom stated that they were recipients of fraudulent solicitations through the following sources: email 62%, phone call 27%, text message 16%, mailed letter 8%, social media 10%, and 17% confirmed that they been the victim of identity theft (Ksepersky, 2020). However, the consequences of responding to phishing are serious and costly. For instance, the United Kingdom losses from financial fraud across payment cards, remote banking, and cheques totaled £768.8 million in 2016 (Financial Fraud Action UK, 2017). Indeed, the losses resulting from phishing attacks are not limited to financial losses that might exceed millions of pounds, but also loss of customers and reputation. According to the 2020 state of phish report (Proofpoint, 2020), damages from successful phishing attacks can range from lost productivity to cash outlay. The cost can include; lost hours from employees, remediation time for info security teams' costs due to incident response, damage to reputation, lost intellectual property, direct monetary losses, compliance fines, lost customers, legal fees, etc.

There are many targets for phishing including end-user, business, financial services (i.e., banks, credit card companies, and PayPal), retail (i.e., eBay, Amazon) and, Internet Service Providers (wombatsecurity.com, 2018). Affected organizations detected by Kaspersky Labs globally in the first quarter of 2020 are demonstrated in **Figure 6**. As shown in the figure, online stores were at the top of the targeted list (18.12%) followed by global Internet portals (16.44%) and social networks in third place (13.07%) (Ksepersky, 2020). While the most impersonated brands overall for the first quarter of 2020 were Apple, Netflix, Yahoo, WhatsApp, PayPal, Chase, Facebook, Microsoft eBay, and Amazon (Checkpoint, 2020).

Phishing attacks can take a variety of forms to target people and steal sensitive information from them. Current data shows that phishing attacks are still effective, which indicates that the available existing countermeasures are not enough to detect and prevent these attacks especially on smart devices. The social engineering element of the phishing attack has been effective in bypassing the existing defenses to date. Therefore, it is essential to understand what makes people fall victim to phishing attacks. *What Attributes Make Some People More Susceptible to Phishing Attacks Than Others* discusses the human attributes that are exploited by the phishers.

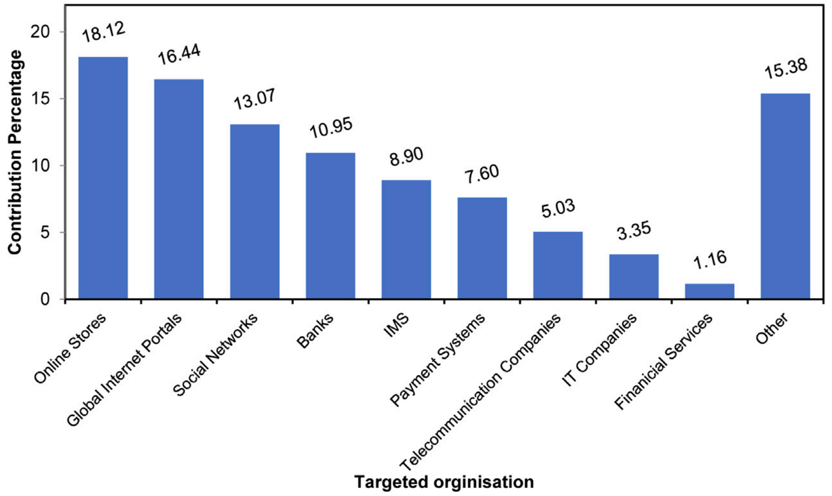
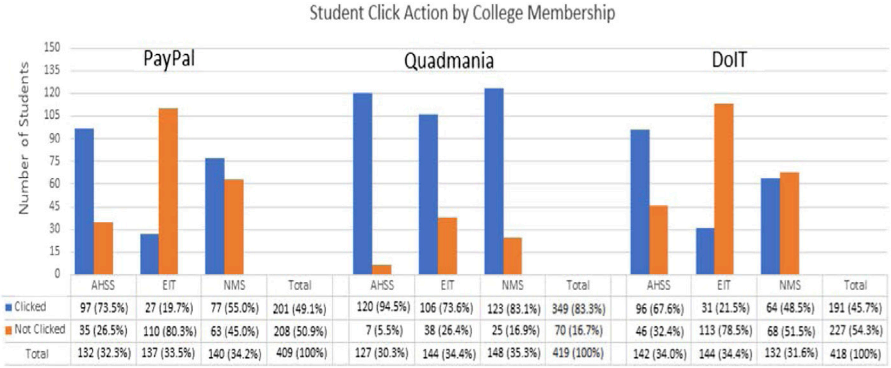


FIGURE 6 | Distribution of organizations affected by phishing attacks detected by Kaspersky in quarter one of 2020.

WHAT ATTRIBUTES MAKE SOME PEOPLE MORE SUSCEPTIBLE TO PHISHING ATTACKS THAN OTHERS

Why do most existing defenses against phishing not work? What personal and contextual attributes make them more susceptible to phishing attacks than other users? Different studies have discussed those two questions and examined the factors affecting susceptibility to a phishing attack and the reasons behind why people get phished. Human nature is considered one of the most affecting factors in the process of phishing. Everyone is susceptible to phishing attacks because phishers play on an individual's specific psychological/emotional triggers as well as technical vulnerabilities (KeepnetLABS, 2018; Crane, 2019). For instance, individuals are likely to click on a link within an email when they see authority cues (Furnell, 2007). In 2017, a report by PhishMe (2017) found that curiosity and urgency were the most common triggers that encourage people to respond to the attack, later these triggers were replaced by entertainment, social media, and reward/recognition as the top emotional motivators. However, in the context of a phishing attack, the psychological triggers often surpass people's conscious decisions. For instance, when people are working under stress, they tend to make decisions without thinking of the possible consequences and options (Lininger and Vines, 2005). Moreover, everyday stress can damage areas of the brain that weakens the control of their emotions (Keinan, 1987). Several studies have addressed the association between susceptibility to phishing and demographic variables (e.g., age and gender) as an attempt to identify the reasons behind phishing success at different population groups. Although everyone is susceptible to phishing, studies showed that different age groups are more susceptible to certain lures than others are. For example, participants with an age range between 18 and 25 are more susceptible to phishing than other age groups (Williams et al., 2018). The reason that younger adults are more likely to fall for phishing, is that younger adults are more trusting when it comes to online communication, and are also more likely to click on unsolicited e-mails (Getsafeonline, 2017). Moreover, older participants are less susceptible because they tend to be less impulsive (Arnsten et al., 2012). While some studies confirmed that women are more susceptible than men to phishing as they click on links in phishing emails and enter information into phishing websites more often than men do. The study published by Getsafeonline (2017) identifies a lack of technical know-how and experience among women than men as the main reason for this. In contrast, a survey conducted by antivirus company Avast found that men are more susceptible to smartphone malware attacks than women (Ong, 2014). These findings confirmed the results from the study (Hadlington, 2017) that found men are more susceptible to mobile phishing attacks than women. The main reason behind this according to Hadlington (2017) is that men are more comfortable and trusting when using mobile online services. The relationships between demographic characteristics of individualls and their ability to correctly detect a phishing attack have been studied in (Iuga et al., 2016). The study showed that participants with high Personal Computer (PC) usage tend to identify phishing efforts more accurately and faster than other participants. Another study (Hadlington, 2017) showed that internet addiction, attentional, and motor impulsivity were significant positive predictors for risky cybersecurity behaviors while a positive attitude toward cybersecurity in business was negatively related to risky cybersecurity behaviors. On the other hand, the trustworthiness of people in some web sites/platforms is one of the holes that the scammers or crackers exploit especially when it based on visual appearance that could fool the user (Hadlington, 2017). For example, fraudsters take advantage of people's trust in a website by replacing a letter from the legitimate site with a number such as goog1e.com instead of google.com. Another study (Yeboah-Boateng and Amanor, 2014) demonstrates that although college students are unlikely to



	PayPal				Quadmania				DoIT			
	AHSS	EIT	NMS	Total	AHSS	EIT	NMS	Total	AHSS	EIT	NMS	Total
■ Clicked	97 (73.5%)	27 (19.7%)	77 (55.0%)	201 (49.1%)	120 (94.5%)	106 (73.6%)	123 (83.1%)	349 (83.3%)	96 (67.6%)	31 (21.5%)	64 (48.5%)	191 (45.7%)
■ Not Clicked	35 (26.5%)	110 (80.3%)	63 (45.0%)	208 (50.9%)	7 (5.5%)	38 (26.4%)	25 (16.9%)	70 (16.7%)	46 (32.4%)	113 (78.5%)	68 (51.5%)	227 (54.3%)
Total	132 (32.3%)	137 (33.5%)	140 (34.2%)	409 (100%)	127 (30.3%)	144 (34.4%)	148 (35.3%)	419 (100%)	142 (34.0%)	144 (34.4%)	132 (31.6%)	418 (100%)

FIGURE 7 | The number of clicks on phishing emails by students in the College of Arts, Humanities, and Social Sciences (AHSS), the College of Engineering and Information Technology (EIT), and the College of Natural and Mathematical Sciences (NMS) at the University of Maryland, Baltimore County (UMBC) (Diaz et al., 2020).

disclose personal information as a response to an email, nonetheless they could easily be tricked by other tactics, making them alarmingly susceptible to email phishing attacks. The reason for that is most college students do not have a basis in ICT especially in terms of security. Although security terms like viruses, online scams and worms are known by some end-users, these users could have no knowledge about Phishing, SMishing, and Vishing and others (Lin et al., 2012). However, study (Yeboah-Boateng and Amanor, 2014) shows that younger students are more susceptible than older students, and students who worked full-time were less likely to fall for phishing.

The study reported in (Diaz et al., 2020) examines user click rates and demographics among undergraduates by sending phishing attacks to 1,350 randomly selected students. Students from various disciplines were involved in the test, from engineering and mathematics to arts and social sciences. The study observed that student susceptibility was affected by a range of factors such as phishing awareness, time spent on the computer, cyber training, age, academic year, and college affiliation. The most surprising finding is that those who have greater phishing knowledge are more susceptible to phishing scams. The authors consider two speculations for these unexpected findings. First, user's awareness about phishing might have been increased with the continuous falling for phishing scams. Second, users who fell for the phish might have less knowledge about phishing than they claim. Other findings from this study agreed with findings from other studies that is, older students were more able to detect a phishing email, and engineering and IT majors had some of the lowest click rates as shown in **Figure 7**, which shows that some academic disciplines are more susceptible to phishing than others (Bailey et al., 2008).

Psychological studies have also illustrated that the user's ability to avoid phishing attacks affected by different factors such as browser security indicators and user's awareness of phishing. The author in (Dhamija et al., 2006) conducted an experimental study using 22 participants to test the user's ability to recognize phishing websites. The study shows that 90% of these participants became victims of phishing websites and 23% of them ignored security indexes such as the status and address bar. In 2015, another study was conducted for the same purpose, where a number of fake web pages was shown to the participants (Alsharnouby et al., 2015). The results of this study showed that participants detected only 53% of phishing websites successfully. The authors also observed that the time spent on looking at browser elements affected the ability to detect phishing. Lack of knowledge or awareness and carelessness are common causes for making people fall for a phishing trap. Most people have unknowingly opened a suspicious attachment or clicked a fake link that could lead to different levels of compromise. Therefore, focusing on training and preparing users for dealing with such attacks are essential elements to minimize the impact of phishing attacks.

Given the above discussion, susceptibility to phishing varies according to different factors such as age, gender, education level, internet, and PC addiction, etc. Although for each person, there is a trigger that can be exploited by phishers, even people with high experience may fall prey to phishing due to the attack sophistication that makes it difficult to be recognized. Therefore, it is inequitable that the user has always been blamed for falling for these attacks, developers must improve the anti-phishing systems in a way that makes the attack invisible. Understanding the susceptibility of individuals to phishing attacks will help in better developing prevention and detection techniques and solutions.

PROPOSED PHISHING ANATOMY

Phishing Process Overview

Generally, most of the phishing attacks start with an email (Jagatic et al., 2007). The phishing mail could be sent randomly to potential users or it can be targeted to a specific group or individuals. Many other vectors can also be used to initiate the attack such as phone calls, instant messaging, or physical letters. However, phishing process steps have been discussed by many researchers due to the importance of understanding these steps in developing an anti-phishing

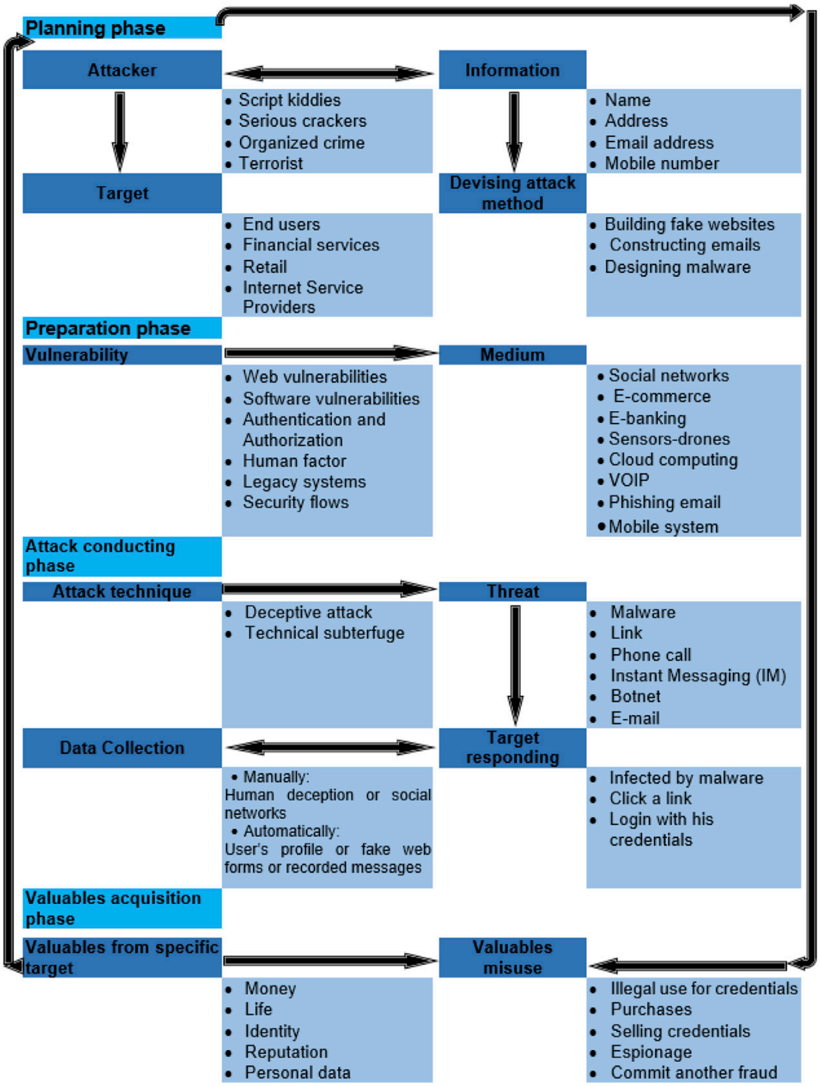


FIGURE 8 | The proposed anatomy of phishing was built upon the proposed phishing definition in this article, which concluded from our understanding of a phishing attack.

solution. The author in the study (Rouse, 2013) divides the phishing attack process into five phases which are planning, setup, attack, collection, and cash. A study (Jakobsson and Myers, 2006) discusses the phishing process in detail and explained it as step-by-step phases. These phases include preparation for the attack, sending a malicious program using the selected vector, obtaining the user's reaction to the attack, tricking a user to disclose their confidential information which will be transmitted to the phisher, and finally obtaining the targeted money. While the study (Abad, 2005) describes a phishing attack in three phases: the early phase which includes initializing attack, creating the phishing email, and sending a phishing email to the victim. The second phase includes receiving an email by the victim and disclosing their information (in the case of the respondent) and the final phase in which the defrauding is successful. However, all phishing scams include three primary phases, the phisher requests sensitive valuables from the target, and the target gives away these valuables to a phisher, and phisher misuses these valuables for malicious purposes. These phases can be classified furthermore into its sub-processes according to phishing trends. Thus, a new anatomy for phishing attacks has been proposed in this article, which expands and integrates previous definitions to cover the full life cycle of a phishing attack. The proposed new anatomy, which consists of 4 phases, is shown in **Figure 8**. This new anatomy provides a reference structure to look at phishing attacks in more detail and also to understand potential countermeasures to prevent them. The explanations for each phase and its components are presented as follows:

Figure 8 depicts the proposed anatomy of the phishing attack process, phases, and components drawn upon the proposed definition in this article. The proposed phishing anatomy explains in detail each phase of phishing phases including attackers and target types, examples about the information that could be collected by the attacker about the victim, and examples about attack methods. The anatomy, as shown in the figure, illustrates a set of vulnerabilities that the attacker can exploit and the mediums used to conduct the attack. Possible threats are also listed, as well as the data collection method for a further explanation and some examples about target responding types and types of spoils that the attacker could gain and how they can use the stolen valuables. This anatomy elaborates on phishing attacks in depth which helps people to better understand the complete phishing process (i.e., end to end Phishing life cycle) and boost awareness among readers. It also provides insights into potential solutions for phishing attacks we should focus on. Instead of always placing the user or human in an accusation ring as the only reason behind phishing success, developers must be focusing on solutions to mitigate the initiation of the attack by preventing the bait from reaching the user. For instance, to reach the target's system, the threat has to pass through many layers of technology or defenses exploiting one or more vulnerabilities such as web and software vulnerabilities.

Planning Phase

This is the first stage of the attack, where a phisher makes a decision about the targets and starts gathering information about them (individuals or company). Phishers gather information about the victims to lure them based on psychological vulnerability. This information can be anything like name, e-mail addresses for individuals, or the customers of that company. Victims could also be selected randomly, by sending mass mailings or targeted by harvesting their information from social media, or any other source. Targets for phishing could be any user with a bank account and has a computer on the Internet. Phishers target businesses such as financial services, retail sectors such as eBay and Amazon, and internet service providers such as MSN/Hotmail, and Yahoo (Ollmann, 2004; Ramzan and Wuest, 2007). This phase also includes devising attack methods such as building fake websites (sometimes phishers get a scam page that is already designed or used, designing malware, constructing phishing emails. The attacker can be categorized based on the attack motivation. There are four types of attackers as mentioned in studies (Vishwanath, 2005; Okin, 2009; EDUCBA, 2017; APWG, 2020):

- Script kiddies: the term script kiddies represents an attacker with no technical background or knowledge about writing sophisticated programs or developing phishing tools but instead they use scripts developed by others in their phishing attack. Although the term comes from children that use available phishing kits to crack game codes by spreading malware using virus toolkits, it does not relate precisely to the actual age of the phisher. Script kiddies can get access to website administration privileges and commit a "Web cracking" attack. Moreover, they can use hacking tools to compromise remote computers so-called "botnet," the single compromised computer called a "zombie computer." These attackers are not limited to just sit back and enjoy phishing, they could cause serious damage such as stealing information or uploading Trojans or viruses. In February 2000, an attack launched by Canadian teen Mike Calce resulted in $1.7 million US Dollars (USD) damages from Distributed Denial of Service (DDoS) attacks on CNN, eBay, Dell, Yahoo, and Amazon (Leyden, 2001).
- Serious Crackers: also known as Black Hats. These attackers can execute sophisticated attacks and develop worms and Trojans for their attack. They hijack people's accounts maliciously and steal credit card information, destroy important files, or sell compromised credentials for personal gains.
- Organized crime: this is the most organized and effective type of attacker and they can incur significant damage to victims. These people hire serious crackers for conducting phishing attacks. Moreover, they can thoroughly trash the victim's identity, and committing devastated frauds as they have the skills, tools, and manpower. An organized cybercrime group is a team of expert hackers who share their skills to build complex attacks and to launch phishing campaigns against individuals and organizations. These groups offer their work as 'crime as a service' and they can be hired by terrorist groups, organizations, or individuals.
- Terrorists: due to our dependency on the internet for most activities, terrorist groups can easily conduct acts of terror remotely which could have an adverse impact. These types of attacks are dangerous since they are not in fear of any aftermath, for instance going to jail. Terrorists could use the internet to the maximum effect to create fear and violence as it requires limited funds, resources, and efforts compared to, for example, buying bombs and weapons in a traditional attack. Often, terrorists use spear phishing to launch their attacks for different purposes such as inflicting damage, cyber espionage, gathering information, locating individuals, and other vandalism purposes. Cyber espionage has been used extensively by cyber terrorists to steal sensitive information on national security, commercial information, and trade secrets which can be used for terrorist activities. These types of crimes may target governments or organizations, or individuals.

Attack Preparation

After making a decision about the targets and gathering information about them, phishers start to set up the attack by scanning for the vulnerabilities to exploit. The following are some examples of vulnerabilities exploited by phishers. For example, the attacker might exploit buffer overflow vulnerability to take control of target applications, create a DoS attack, or compromise computers. Moreover, "zero-day" software vulnerabilities, which refer to newly discovered vulnerabilities in software programs or operating systems could be exploited directly before it is fixed (Kayne, 2019). Another example is browser vulnerabilities, adding new features and updates to the browser might introduce new vulnerabilities to the browser software (Ollmann, 2004). In 2005, attackers exploited a cross-domain vulnerability in Internet Explorer (IE) (Symantic, 2019). The cross-domain used to separate content from different sources in Microsoft IE. Attackers exploited a flaw in the cross-domain that enables them to execute programs on a user's computer after running IE. According to US-CERT, hackers are actively exploiting this vulnerability. To carry out a phishing attack, attackers need a medium so that they can reach their target. Therefore, apart from planning the attack to exploit potential vulnerabilities, attackers choose the medium that will be used to deliver the threat to the victim and carry out the attack. These mediums could be the internet (social network, websites, emails, cloud computing, e-banking, mobile systems) or VoIP (phone call), or text messages. For example, one of the actively used mediums is Cloud Computing (CC). The CC has become one of the more promising technologies and has popularly replaced conventional computing technologies. Despite the considerable advantages produced by CC, the adoption of CC faces several controversial obstacles including privacy and security issues (CVEdetails, 2005). Due to the fact that different customers could share the same recourses in the cloud, virtualization vulnerabilities may be exploited by a possible malicious customer to perform security attacks on other customers' applications and data (Zissis and Lekkas, 2012). For example, in September 2014, secret photos of some celebrities suddenly moved through the internet in one of the more terrible data breaches. The investigation revealed that the iCloud accounts of the celebrities were breached (Lehman and Vajpayee, 2011). According to Proofpoint, in 2017, attackers used Microsoft SharePoint to infect hundreds of campaigns with malware through messages.

Attack Conducting Phase

This phase involves using attack techniques to deliver the threat to the victim as well as the victim's interaction with the attack in terms of responding or not. After the victim's response, the system may be compromised by the attacker to collect user's information using techniques such as injecting client-side script into webpages (Johnson, 2016). Phishers can compromise hosts without any technical knowledge by purchasing access from hackers (Abad, 2005). A threat is a possible danger that that might exploit a vulnerability to compromise people's security and privacy or cause possible harm to a computer system for malicious purposes. Threats could be malware, botnet, eavesdropping, unsolicited emails, and viral links. Several Phishing techniques are discussed in sub-*Types and Techniques of Phishing Attacks*.

Valuables Acquisition Phase

In this stage, the phisher collects information or valuables from victims and uses it illegally for purchasing, funding money without the user's knowledge, or selling these credentials in the black market. Attackers target a wide range of valuables from their victims that range from money to people's lives. For example, attacks on online medical systems may lead to loss of life. Victim's data can be collected by phishers manually or through automated techniques (Jakobsson et al., 2007).

The data collection can be conducted either during or after the victim's interaction with the attacker. However, to collect data manually simple techniques are used wherein victims interact directly with the phisher depending on relationships within social networks or other human deception techniques (Ollmann, 2004). Whereas in automated data collection, several techniques can be used such as fake web forms that are used in web spoofing (Dhamija et al., 2006). Additionally, the victim's public data such as the user's profile in social networks can be used to collect the victim's background information that is required to initialize social engineering attacks (Wenyin et al., 2005). In VoIP attacks or phone attack techniques such as recorded messages are used to harvest user's data (Huber et al., 2009).

Types and Techniques of Phishing Attacks

Phishers conduct their attack either by using psychological manipulation of individuals into disclosing personal information (i.e., deceptive attack as a form of social engineering) or using technical methods. Phishers, however, usually prefer deceptive attacks by exploiting human psychology rather than technical methods. **Figure 9** illustrates the types of phishing and techniques used by phishers to conduct a phishing attack. Each type and technique is explained in subsequent sections and subsections.

Deceptive Phishing

Deceptive phishing is the most common type of phishing attack in which the attacker uses social engineering techniques to deceive victims. In this type of phishing, a phisher uses either social engineering tricks by making up scenarios (i.e., false account update, security upgrade), or technical methods (i.e., using legitimate trademarks, images, and logos) to lure the victim and convince them of the legitimacy of the forged email (Jakobsson and Myers, 2006). By believing these scenarios, the user will fall prey and follow the given link, which leads to disclose his personal information to the phisher.

Deceptive phishing is performed through phishing emails; fake websites; phone phishing (Scam Call and IM); social media; and via many other mediums. The most common social phishing types are discussed below;

Phishing e-Mail

The most common threat derived by an attacker is deceiving people via email communications and this remains the most popular phishing type to date. A Phishing email or Spoofed email is a forged email sent from an untrusted source to thousands of victims randomly. These fake emails are claiming to be from a person or financial institution that the recipient trusts in order to convince recipients to take actions that lead them to disclose their sensitive information. A more organized phishing email that targets a particular group or individuals within the same organization is called spear phishing. In the above type, the attacker may gather information related to the victim such as name and address so that it appears to be credible emails from a trusted source (Wang et al., 2008), and this is linked to the planning phase of the phishing anatomy proposed in this article. A more sophisticated form of spear phishing is called whaling, which targets high-rank people such as CEOs and CFOs. Some examples of spear-phishing attack victims in early 2016 are the

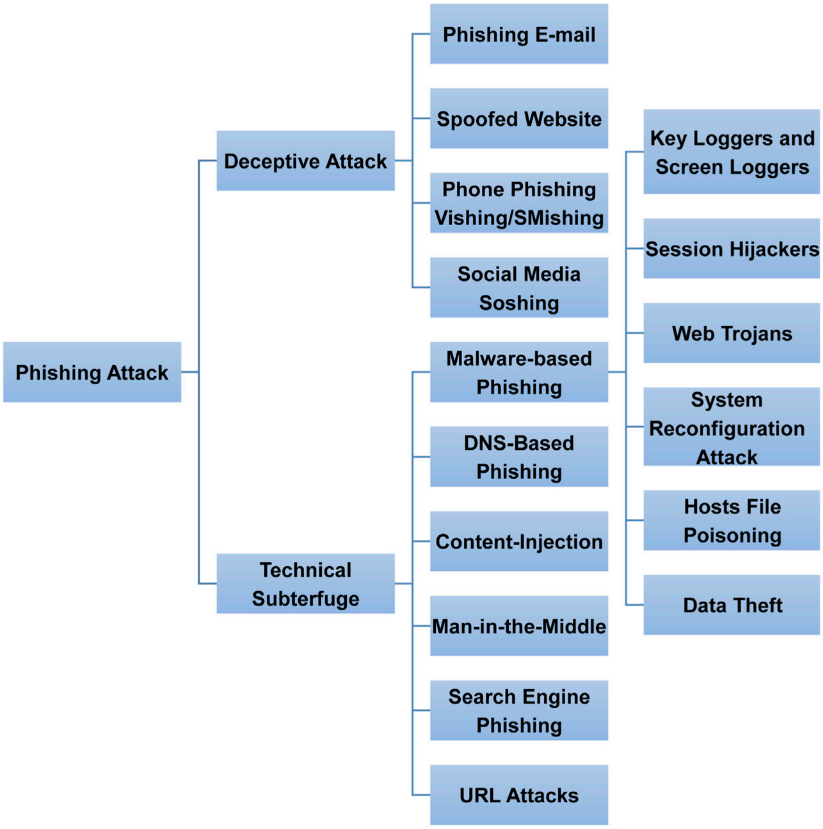


FIGURE 9 | Phishing attack types and techniques drawing upon existing phishing attacks.

phishing email that hacked the Clinton campaign chairman John Podesta's Gmail account (Parmar, 2012). Clone phishing is another type of email phishing, where the attacker clones a legitimate and previously delivered email by spoofing the email address and using information related to the recipient such as addresses from the legitimate email with replaced links or malicious attachments (Krawchenko, 2016). The basic scenario for this attack is illustrated previously in **Figure 4** and can be described in the following steps.

1. The phisher sets up a fraudulent email containing a link or an attachment (planning phase).
2. The phisher executes the attack by sending a phishing email to the potential victim using an appropriate medium (attack conducting phase).
3. The link (if clicked) directs the user to a fraudulent website, or to download malware in case of clicking the attachment (interaction phase).
4. The malicious website prompts users to provide confidential information or credentials, which are then collected by the attacker and used for fraudulent activities. (Valuables acquisition phase).

Often, the phisher does not use the credentials directly; instead, they resell the obtained credentials or information on a secondary market (Jakobsson and Myers, 2006), for instance, script kiddies might sell the credentials on the dark web.

Spoofed Website

This is also called phishing websites, in which phishers forge a website that appears to be genuine and looks similar to the legitimate website. An unsuspicious user is redirected to this website after clicking a link embedded within an email or through an advertisement (clickjacking) or any other way. If the user continues to interact with the spoofed website, sensitive information will be disclosed and harvested by the phisher (CSIOnsite, 2012).

Phone Phishing (Vishing and SMishing)

This type of phishing is conducted through phone calls or text messages, in which the attacker pretends to be someone the victim knows or any other trusted source the victim deals with. A user may receive a convincing security alert message from a bank convincing the victim to contact a given phone number with the aim to get the victim to share passwords or PIN numbers or any other Personally Identifiable Information (PII). The victim may be duped into clicking on an embedded link in the text message. The phisher then could take the credentials entered by the victim and use them to log in to the victims' instant messaging service to phish other people from the victim's contact list. A phisher could also make use of Caller IDentification (CID)[3] spoofing to dupe the victim that the call is from a trusted source or by leveraging from an internet protocol private branch exchange (IP PBX)[4] tools which are open-source and software-based that support VoIP (Aburrous et al., 2008). A new report from Fraud Watch International about phishing attack trends for 2019 anticipated an increase in SMishing where the text messages content is only viewable on a mobile device (FraudWatchInternational, 2019).

Social Media Attack (Soshing, Social Media Phishing)

Social media is the new favorite medium for cybercriminals to conduct their phishing attacks. The threats of social media can be account hijacking, impersonation attacks, scams, and malware distributing. However, detecting and mitigating these threats requires a longer time than detecting traditional methods as social media exists outside of the network perimeter. For example, the nation-state threat actors conducted an extensive series of social media attacks on Microsoft in 2014. Multiple Twitter accounts were affected by these attacks and passwords and emails for dozens of Microsoft employees were revealed (Ramzan, 2010). According to Kaspersky Lab's, the number of phishing attempts to visit fraudulent social network pages in the first quarter of 2018 was more than 3.7 million attempts, of which 60% were fake Facebook pages (Raggo, 2016).

The new report from predictive email defense company Vade Secure about phishers' favorites for quarter 1 and quarter 2 of 2019, stated that Soshing primarily on Facebook and Instagram saw a 74.7% increase that is the highest quarter-over- quarter growth of any industry (VadeSecure, 2021).

Technical Subterfuge

Technical subterfuge is the act of tricking individuals into disclosing their sensitive information through technical subterfuge by downloading malicious code into the victim's system. Technical subterfuge can be classified into the following types:

Malware-Based Phishing

As the name suggests, this is a type of phishing attack which is conducted by running malicious software on a user's machine. The malware is downloaded to the victim's machine, either by one of the social engineering tricks or technically by exploiting vulnerabilities in the security system (e.g., browser vulnerabilities) (Jakobsson and Myers, 2006). Panda malware is one of the successful malware programs discovered by Fox-IT Company in 2016. This malware targets Windows Operating Systems (OS). It spreads through phishing campaigns and its main attack vectors include web injects, screenshots of user activity (up to 100 per mouse click), logging of keyboard input, Clipboard pastes (to grab passwords and paste them into form fields), and exploits to the Virtual Network Computing (VNC) desktop sharing system. In 2018, Panda malware expanded its targets to include cryptocurrency exchanges and social media sites (F5Networks, 2018). There are many forms of Malware-based phishing attacks; some of them are discussed below:

Key Loggers and Screen Loggers. Loggers are the type of malware used by phishers and installed either through Trojan horse email attachments or through direct download to the user's personal computer. This software monitors data and records user keystrokes and then sends it to the phisher. Phisher uses the key loggers to capture sensitive information related to victims, such as names, addresses, passwords, and other confidential data. Key loggers can also be used for non-phishing purposes such as to monitor a child's use of the internet. Key loggers can also be implemented in many other ways such as detecting URL changes and logs information as Browser Helper Object (BHO) that enables the attacker to take control of the features of all IE's, monitoring keyboard and mouse input as a device driver and, monitoring users input and displays as a screen logger (Jakobsson and Myers, 2006).

Viruses and Worms. A virus is a type of malware, which is a piece of code spreading in another application or program by making copies of itself in a self-automated manner (Jakobsson and Myers, 2006; F5Networks, 2018). Worms are similar to viruses but they differ in the execution manner, as worms are executed by exploiting the operating systems vulnerability without the need to modify another program. Viruses transfer from one computer to another with the document that they are attached to, while worms transfer through the infected host file. Both viruses and worms can cause data and software damaging or Denial-of-Service (DoS) conditions (F5Networks, 2018).

Spyware. Spying software is a malicious code designed to track the websites visited by users in order to steal sensitive information and conduct a phishing attack. Spyware can be delivered through an email and, once it is installed on the computer, take control over the device and either change its settings or gather information such as passwords and credit card numbers or banking records which can be used for identity theft (Jakobsson and Myers, 2006).

Adware. Adware is also known as advertising-supported software (Jakobsson and Myers, 2006). Adware is a type of malware that shows the user an endless pop-up window with ads that could harm the performance of the device. Adware can be annoying but most of it is safe. Some of the adware could be used for malicious purposes such as tracking the internet sites the user visits or even recording the user's keystrokes (cisco, 2018).

Ransomware. Ransomware is a type of malware that encrypts the user's data after they run an executable program on the device. In this type of attack, the decryption key is held until the user pays a ransom (cisco, 2018). Ransomware is responsible for tens of millions of dollars in extortion annually. Worse still, this is hard to detect with developing new variants, facilitating the

[3] CalleR ID is "a telephone facility that displays a caller's phone number on the recipient's phone device before the call is answered" (Techpedia, 2021).

[4] An IPPBX is "a telephone switching system within an enterprise that switches calls between VoIP users on local lines while allowing all users to share a certain number of external phone lines" (Margaret, 2008).

evasion of many antivirus and intrusion detection systems (Latto, 2020). Ransomware is usually delivered to the victim's device through phishing emails. According to a report (PhishMe, 2016), 93% of all phishing emails contained encryption ransomware. Phishing, as a social engineering attack, convinces victims into executing actions without knowing about the malicious program.

Rootkits

A rootkit is a collection of programs, typically malicious, that enables access to a computer or computer network. These toolsets are used by intruders to hide their actions from system administrators by modifying the code of system calls and changing the functionality (Belcic, 2020). The term "rootkit" has negative connotations through its association with malware, and it is used by the attacker to alert existing system tools to escape detection. These kits enable individuals with little or no knowledge to launch phishing exploits. It contains coding, mass emailing software (possibly with thousands of email addresses included), web development software, and graphic design tools. An example of rootkits is the Kernel kit. Kernel-Level Rootkits are created by replacing portions of the core operating system or adding new code via Loadable Kernel Modules in (Linux) or device drivers (in Windows) (Jakobsson and Myers, 2006).

Session Hijackers

In this type, the attacker monitors the user's activities by embedding malicious software within a browser component or via network sniffing. The monitoring aims to hijack the session, so that the attacker performs an unauthorized action with the hijacked session such as financial transferring, without the user's permission (Jakobsson and Myers, 2006).

Web Trojans

Web Trojans are malicious programs that collect user's credentials by popping up in a hidden way over the login screen (Jakobsson and Myers, 2006). When the user enters the credentials, these programs capture and transmit the stolen credentials directly to the attacker (Jakobsson et al., 2007).

Hosts File Poisoning

This is a way to trick a user into going to the phisher's site by poisoning (changing) the host's file. When the user types a particular website address in the URL bar, the web address will be translated into a numeric (IP) address before visiting the site. The attacker, to take the user to a fake website for phishing purposes, will modify this file (e.g., DNS cache). This type of phishing is hard to detect even by smart and perceptive users (Ollmann, 2004).

System Reconfiguration Attack

In this format of the phishing attack, the phisher manipulates the settings on a user's computer for malicious activities so that the information on this PC will be compromised. System reconfigurations can be changed using different methods such as reconfiguring the operating system and modifying the user's Domain Name System (DNS) server address. The wireless evil twin is an example of a system reconfiguration attack in which all user's traffic is monitored via a malicious wireless Access Point (AP) (Jakobsson and Myers, 2006).

Data Theft

Data theft is an unauthorized accessing and stealing of confidential information for a business or individuals. Data theft can be performed by a phishing email that leads to the download of a malicious code to the user's computer which in turn steals confidential information stored in that computer directly (Jakobsson and Myers, 2006). Stolen information such as passwords, social security numbers, credit card information, sensitive emails, and other personal data could be used directly by a phisher or indirectly by selling it for different purposes.

Domain Name System Based Phishing (Pharming)

Any form of phishing that interferes with the domain name system so that the user will be redirected to the malicious website by polluting the user's DNS cache with wrong information is called DNS-based phishing. Although the host's file is not a part of the DNS, the host's file poisoning is another form of DNS based phishing. On the other hand, by compromising the DNS server, the genuine IP addresses will be modified which results in taking the user unwillingly to a fake location. The user can fall prey to pharming even when clicking on a legitimate link because the website's domain name system (DNS) could be hijacked by cybercriminals (Jakobsson and Myers, 2006).

Content Injection Phishing

Content-Injection Phishing refers to inserting false content into a legitimate site. This malicious content could misdirect the user into fake websites, leading users into disclosing their sensitive information to the hacker or it can lead to downloading malware into the user's device (Jakobsson and Myers, 2006). The malicious content could be injected into a legitimate site in three primary ways:

1. Hacker exploits a security vulnerability and compromises a web server.
2. Hacker exploits a Cross-Site Scripting (XSS) vulnerability that is a programming flaw that enables attackers to insert client-side scripts into web pages, which will be viewed by the visitors to the targeted site.
3. Hacker exploits Structured Query Language (SQL) injection vulnerability, which allows hackers to steal information from the website's database by executing database commands on a remote server.

Man-In-The-Middle Phishing

The Man In The Middle attack (MITM) is a form of phishing, in which the phishers insert communications between two parties (i.e. the user and the legitimate website) and tries to obtain the information from both parties by intercepting the victim's communications (Ollmann, 2004). Such that the message is going to the attacker instead of going directly to the legitimate recipients. For a MITM, the attacker records the information and misuse it later. The MITM attack conducts by redirecting the user to a malicious server through several techniques such as Address Resolution Protocol (ARP) poisoning, DNS spoofing, Trojan key loggers, and URL Obfuscation (Jakobsson and Myers, 2006).

Search Engine Phishing

In this phishing technique, the phisher creates malicious websites with attractive offers and use Search Engine Optimization (SEO) tactics to have them indexed legitimately such that it appears to the user when searching for products or services. This is also known as black hat SEO (Jakobsson and Myers, 2006).

URL and HTML Obfuscation Attacks

In most of the phishing attacks, phishers aim to convince a user to click on a given link that connects the victim to a malicious phishing server instead of the destination server. This is the most popular technique used by today's phishers. This type of attack is performed by obfuscating the real link (URL) that the user intends to connect (an attempt from the attacker to make their web address look like the legitimate one). Bad Domain Names and Host Name Obfuscation are common methods used by attackers to fake an address (Ollmann, 2004).

COUNTERMEASURES

A range of solutions are being discussed and proposed by the researchers to overcome the problems of phishing, but still, there is no single solution that can be trusted or capable of mitigating these attacks (Hong, 2012; Boddy, 2018; Chanti and Chithralekha, 2020). The proposed phishing countermeasures in the literature can be categorized into three major defense strategies. The first line of defense is human-based solutions by educating end-users to recognize phishing and avoid taking the bait. The second line of defense is technical solutions that involve preventing the attack at early stages such as at the vulnerability level to prevent the threat from materializing at the user's device, which means decreasing the human exposure, and detecting the attack once it is launched through the network level or at the end-user device. This also includes applying specific techniques to track down the source of the attack (for example these could include identification of new domains registered that are closely matched with well-known domain names). The third line of defense is the use of law enforcement as a deterrent control. These approaches can be combined to create much stronger anti-phishing solutions. The above solutions are discussed in detail below.

Human Education (Improving User Awareness About Phishing)

Human education is by far an effective countermeasure to avoid and prevent phishing attacks. Awareness and human training are the first defense approach in the proposed methodology for fighting against phishing even though it does not assume complete protection (Hong, 2012). End-user education reduces user's susceptibility to phishing attacks and compliments other technical solutions. According to the analysis carried out in (Bailey et al., 2008), 95% of phishing attacks are caused due to human errors; nonetheless, existing phishing detection training is not enough for combating current sophisticated attacks. In the study presented by Khonji et al. (2013), security experts contradict the effectiveness and usability of user education. Furthermore, some security experts claim that user education is not effective as security is not the main goal for users and users do not have a motivation to educate themselves about phishing (Scaife et al., 2016), while others confirm that user education could be effective if designed properly (Evers, 2006; Whitman and Mattord, 2012). Moreover, user training has been mentioned by many researchers as an effective way to protect users when they are using online services (Dodge et al., 2007; Salem et al., 2010; Chanti and Chithralekha, 2020). To detect and avoid phishing emails, a combined training approach was proposed by authors in the study (Salem et al., 2010). The proposed solution uses a combination of tools and human learning, wherein a security awareness program is introduced to the user as a first step. The second step is using an intelligent system that detects the attacks at the email level. After that, the emails are classified by a fuzzy logic-based expert system. The main critic of this method is that the study chooses only limited characteristics of the emails as distinguishing features (Kumaraguru et al., 2010; CybintCyberSolutions, 2018). Moreover, the majority of phishing training programs focus on how to recognize and avoid phishing emails and websites while other threatening phishing types receive less attention such as voice phishing and malware or adware phishing. The authors in (Salem et al., 2010) found that the most used solutions in educating people are not useful if they ignore the notifications/warnings about fake websites. Training users should involve three major directions: the first one is awareness training through holding seminars or online courses for both employees within organizations or individuals. The second one is using mock phishing attacks to attack people to test users' vulnerability and allow them to assess their own knowledge about phishing. However, only 38% of global organizations claim they are prepared to handle a sophisticated cyber-attack (Kumaraguru et al., 2010). Wombat Security's State of the Phish™ Report 2018 showed that approximately two-fifths of American companies use computer-based online awareness training and simulated phishing attacks as educating tools on a monthly basis, while just 15% of United Kingdom firms do so (CybintCyberSolutions, 2018). The third direction is educating people by developing games to teach people about phishing. The game developer should take into consideration different aspects before designing the game such as audience age and gender, because people's susceptibility to phishing is varying. Authors in the study (Sheng et al., 2007) developed a game to train users so that they can identify phishing attacks called Anti-Phishing Phil that teaches about phishing web pages, and then tests users about the efficiency and effectiveness of the game. The results from the study showed that the game participants improve their ability to identify phishing by 61% indicating that interactive games might turn out to be a joyful way of educating people. Although, user's education and training can be very effective to mitigate security threats, phishing is becoming more complex and cybercriminals can fool even the security experts by creating convincing spear phishing emails via social media. Therefore, individual users and employees must have at least basic knowledge about dealing with suspicious emails and report it to IT staff and specific authorities. In addition, phishers change their strategies continuously, which makes it harder for organizations, especially small/medium enterprises to afford the cost of their employee education. With millions of people logging on to their social media accounts every day, social media phishing is phishers' favorite medium to deceive their victims. For example, phishers are taking advantage of the pervasiveness of Facebook to set up creative phishing attacks utilizing the Facebook Login feature that enables the phisher to compromise all the user's accounts with the same credentials (VadeSecure). Some countermeasures are taken by Social networks to reduce suspicious activities on social media such as Two-Factor authentication for logging in, that is required by Facebook, and machine-learning techniques used by Snapchat to detect and prevent suspicious links sent within the app (Corrata, 2018). However, countermeasures to control Soshing and phone phishing attacks might include:

- Install anti-virus, anti-spam software as a first action and keep it up to date to detect and prevent any unauthorized access.
- Educate yourself about recent information on phishing, the latest trends, and countermeasures.
- Never click on hyperlinks attached to a suspicious email, post, tweet, direct message.
- Never trust social media, do not give any sensitive information over the phone or non-trusted account. Do not accept friend requests from people you do not know.
- Use a unique password for each account.

Training and educating users is an effective anti-phishing countermeasure and has already shown promising initial results. The main downside of this solution is that it demands high costs (Dodge et al., 2007). Moreover, this solution requires basic knowledge in computer security among trained users.

Technical Solutions

The proposed technical solutions for detecting and blocking phishing attacks can be divided into two major approaches: non-content based solutions and content-based solutions (Le et al., 2006; Bin et al., 2010; Boddy, 2018). Both approaches are briefly described in this section. Non-content based methods include blacklists and whitelists that classify the fake emails or webpages based on the information that is not part of the email or the webpage such as URL and domain name features (Dodge et al., 2007; Ma et al., 2009; Bin et al., 2010; Salem et al., 2010). Stopping the phishing sites using blacklist and whitelist approaches, wherein a list of known URLs and sites is maintained, the website under scrutiny is checked against such a list in order to be classified as a phishing or legitimate site. The downside of this approach is that it will not identify all phishing websites. Because once a phishing site is taken down, the phisher can easily register a new domain (Miyamoto et al., 2009). Content-based methods classify the page or the email relying on the information within its content such as texts, images, and also HTML, java scripts, and Cascading Style Sheets (CSS) codes (Zhang et al., 2007; Maurer and Herzner, 2012). Content-based solutions involve Machine Learning (ML), heuristics, visual similarity, and image processing methods (Miyamoto et al., 2009; Chanti and Chithralekha, 2020). and finally, multifaceted methods, which apply a combination of the previous approaches to detect and prevent phishing attacks (Afroz and Greenstadt, 2009). For email filtering, ML techniques are commonly used for example in 2007, the first email phishing filter was developed by authors in (Fette et al., 2007). This technique uses a set of features such as URLs that use different domain names. Spam filtering techniques (Cormack et al., 2011) and statistical classifiers (Bergholz et al., 2010) are also used to identify a phishing email. Authentication and verification technologies are also used in spam email filtering as an alternative to heuristics methods. For example, the Sender Policy Framework (SPF) verifies whether a sender is valid when accepting mail from a remote mail server or email client (Deshmukh and raddha Popat, 2017).

The technical solutions for Anti-phishing are available at different levels of the delivery chain such as mail servers and clients, Internet Service Providers (ISPs), and web browser tools. Drawing from the proposed anatomy for phishing attacks in *Proposed Phishing Anatomy*, authors categorize technical solutions into the following approaches:

1. Techniques to detect the attack after it has been launched. Such as by scanning the web to find fake websites. For example, content-based phishing detection approaches are heavily deployed on the Internet. The features from the website elements such as Image, URL, and text content are analyzed using Rule-based approaches and Machine Learning that examine the presence of special characters (@), IP addresses instead of the domain name, prefix/suffix, HTTPS in domain part and other features (Jeeva and Rajsingh, 2016). Fuzzy Logic (FL) has also been used as an anti-phishing model to help classify websites into legitimate or 'phishy' as this model deals with intervals rather than specific numeric values (Aburrous et al., 2008).
2. Techniques to prevent the attack from reaching the user's system. Phishing prevention is an important step to defend against phishing by blocking a user from seeing and dealing with the attack. In email phishing, anti-spam software tools can block suspicious emails. Phishers usually send a genuine look-alike email that dupes the user to open an attachment or click on a link. Some of these emails pass the spam filter because phishers use misspelled words. Therefore, techniques that detect fake emails by checking the spelling and grammar correction are increasingly used, so that it can prevent the email from reaching the user's mailbox. Authors in the study (Fette et al., 2007) have developed a new classification algorithm based on the Random Forest algorithm after exploring email phishing utilizing the C4.5 decision tree generator algorithm. The developed method is called

"Phishing Identification by Learning on Features of Email Received" (PILFER), which can classify phishing email depending on various features such as IP based URLs, the number of links in the HTML part(s) of an email, the number of domains, the number of dots, nonmatching URLs, and availability of JavaScripts. The developed method showed high accuracy in detecting phishing emails (Afroz and Greenstadt, 2009).

3. Corrective techniques that can take down the compromised website, by requesting the website's Internet Service Provider (ISP) to shut down the fake website in order to prevent more users from falling victims to phishing (Moore and Clayton, 2007; Chanti and Chithralekha, 2020). ISPs are responsible for taking down fake websites. Removing the compromised and illegal websites is a complex process; many entities are involved in this process from private companies, self-regulatory bodies, government agencies, volunteer organizations, law enforcement, and service providers. Usually, illegal websites are taken down by Takedown Orders, which are issued by courts or in some jurisdictions by law enforcement. On the other hand, these can be voluntarily taken down by the providers themselves as a result of issued takedown notices (Moore and Clayton, 2007; Hutchings et al., 2016). According to PHISHLABS (PhishLabs, 2019) report, taking down phishing sites is helpful but it is not completely effective as these sites can still be alive for days stealing customers' credentials before detecting the attack.
4. Warning tools or security indicators that embedded into the web browser to inform the user after detecting the attack. For example, eBay Toolbar and Account Guard (eBay Toolbar and Account Guard, 2009) protect customer's eBay and PayPal passwords respectively by alerting the users about the authenticity of the sites that users try to type the password in. Numerous anti-phishing solutions rely mainly on warnings that are displayed on the security toolbar. In addition, some toolbars block suspicious sites to warn about it such as McAfee and Netscape. A study presented in (Robichaux and Ganger, 2006) conducted a test to evaluate the performance of eight anti-phishing solutions, including Microsoft Internet Explorer 7, EarthLink, eBay, McAfee, GeoTrust, Google using Firefox, Netscape, and Netcraft. These tools are warning and blocking tools that allow legitimate sites while block and warn about known phishing sites. The study also found that Internet Explorer and Netcraft Toolbar showed the most effective results than other anti-phishing tools. However, security toolbars are still failing to avoid people falling victim to phishing despite these toolbars improving internet security in general (Abu-Nimeh and Nair, 2008).
5. Authentication (Moore and Clayton, 2007) and authorization (Hutchings et al., 2016) techniques that provide protection from phishing by verifying the identity of the legitimate person. This prevents phishers from accessing a protected resource and conducting their attack. There are three types of authentication; single-factor authentication requires only username and password. The second type is two-factor authentication that requires additional information in addition to the username and password such as an OTP (One-Time Password) which is sent to the user's email id or phone. The third type is multi-factor authentication using more than one form of identity (i.e., a combination of something you know, something you are, and something you have). Some widely used methods in the authorization process are API authorization and OAuth 2.0 that allow the previously generated API to access the system.

However, the progressive increase in phishing attacks shows that previous methods do not provide the required protection against most existing phishing attacks. Because no single solution or technology could prevent all phishing attacks. An effective anti-phishing solution should be based on a combination of technical solutions and increased user awareness (Boddy, 2018).

Solutions Provided by Legislations as a Deterrent Control

A cyber-attack is considered a crime when an individual intentionally accesses personal information on a computer without permission, even if the individual does not steal information or damage the system (Mince-Didier, 2020). Since the sole objective of almost all phishing attacks is to obtain sensitive information by knowingly intending to commit identity theft, and while there are currently no federal laws in the United States aimed specifically at phishing, therefore, phishing crimes are usually covered under identity theft laws. Phishing is considered a crime even if the victim does not actually fall for the phishing scam, the punishments depend on circumstances and usually include jail, fines, restitution, probation (Nathan, 2020). Phishing attacks are causing different levels of damages to the victims such as financial and reputational losses. Therefore, law enforcement authorities should track down these attacks in order to punish the criminal as with real-world crimes. As a complement to technical solutions and human education, the support provided by applicable laws and regulations can play a vital role as a deterrent control. Increasingly authorities around the world have created several regulations in order to mitigate the increase of phishing attacks and their impact. The first anti-phishing laws were enacted by the United States, where the FTC in the US added the phishing attacks to the computer crime list in January 2004. A year later, the "Anti-Phishing Act" was introduced in the US Congress in March 2005 (Mohammad et al., 2014). Meanwhile, in the United Kingdom, the law legislation is gradually conforming to address phishing and other forms of cyber-crime. In 2006, the United Kingdom government improved the Computer Misuse Act 1990 intending to bring it up to date with developments in computer crime and to increase penalties for breach enacted penalties of up to 10 years (eBay Toolbar and Account Guard, 2009; PhishLabs, 2019). In this regard, a student in the United Kingdom who made hundreds of thousands of pounds blackmailing pornography website users was jailed in April 2019 for six years and five months. According to the National Crime Agency (NCA), this attacker was the most prolific cybercriminal to be sentenced in the United Kingdom (Casciani, 2019).

Moreover, the organizations bear part of the responsibility in protecting personal information as stated in the Data Protection Act 2018 and EU General Data Protection Regulation (GDPR). Phishing websites also can be taken down through Law enforcement agencies' conduct. In the United Kingdom, websites can be taken down by the National Crime Agency (NCA), which includes the National Cyber Crime Unit, and by the City of London Police, which includes the Police Intellectual Property Crime Unit (PIPCU) and the National Fraud Intelligence Bureau (NFIB) (Hutchings et al., 2016).

However, anti-phishing law enforcement is still facing numerous challenges and limitations. Firstly, after perpetrating the phishing attack, the phisher can vanish in cyberspace making it difficult to prove the guilt attributed to the offender and to recover the damages caused by the attack, limiting the effectiveness of the law enforcement role. Secondly, even if the attacker's identity is disclosed in the case of international attackers, it will be difficult to bring this attacker to justice because of the differences in countries' legislations (e.g., exchange treaties). Also, the attack could be conducted within a short time span, for instance, the average lifetime for a phishing web site is about 54 h as stated by the APWG, therefore, there must be a quick response from the government and the authorities to detect, control and identify the perpetrators of the attack (Ollmann, 2004).

CONCLUSION

Phishing attacks remain one of the major threats to individuals and organizations to date. As highlighted in the article, this is mainly driven by human involvement in the phishing cycle. Often phishers exploit human vulnerabilities in addition to favoring technological conditions (i.e., technical vulnerabilities). It has been identified that age, gender, internet addiction, user stress, and many other attributes affect the susceptibility to phishing between people. In addition to traditional phishing channels (e.g., email and web), new types of phishing mediums such as voice and SMS phishing are on the increase. Furthermore, the use of social media-based phishing has increased in use in parallel with the growth of social media. Concomitantly, phishing has developed beyond obtaining sensitive information and financial crimes to cyber terrorism, hacktivism, damaging reputations, espionage, and nation-state attacks. Research has been conducted to identify the motivations and techniques and countermeasures to these new crimes, however, there is no single solution for the phishing problem due to the heterogeneous nature of the attack vector. This article has investigated problems presented by phishing and proposed a new anatomy, which describes the complete life cycle of phishing attacks. This anatomy provides a wider outlook for phishing attacks and provides an accurate definition covering end-to-end exclusion and realization of the attack.

Although human education is the most effective defense for phishing, it is difficult to remove the threat completely due to the sophistication of the attacks and social engineering elements. Although, continual security awareness training is the key to avoid phishing attacks and to reduce its impact, developing efficient anti-phishing techniques that prevent users from being exposed to the attack is an essential step in mitigating these attacks. To this end, this article discussed the importance of developing anti-phishing techniques that detect/block the attack. Furthermore, the importance of techniques to determine the source of the attack could provide a stronger anti-phishing solution as discussed in this article.

Furthermore, this article identified the importance of law enforcement as a deterrent mechanism. Further investigations and research are necessary as discussed below.

1. Further research is necessary to study and investigate susceptibility to phishing among users, which would assist in designing stronger and self-learning anti-phishing security systems.
2. Research on social media-based phishing, Voice Phishing, and SMS Phishing is sparse and these emerging threats are predicted to be significantly increased over the next years.
3. Laws and legislations that apply for phishing are still at their infant stage, in fact, there are no specific phishing laws in many countries. Most of the phishing attacks are covered under traditional criminal laws such as identity theft and computer crimes. Therefore, drafting of specific laws for phishing is an important step in mitigating these attacks in a time where these crimes are becoming more common.
4. Determining the source of the attack before the end of the phishing lifecycle and enforcing law legislation on the offender could help in restricting phishing attacks drastically and would benefit from further research.

It can be observed that the mediums used for phishing attacks have changed from traditional emails to social media-based phishing. There is a clear lag between sophisticated phishing attacks and existing countermeasures. The emerging countermeasures should be multidimensional to tackle both human and technical elements of the attack. This article provides valuable information about current phishing attacks and countermeasures whilst the proposed anatomy provides a clear taxonomy to understand the complete life cycle of phishing.

AUTHOR CONTRIBUTIONS

This work is by our PhD student ZA supported by her Supervisory Team.

REFERENCES

Abad, C. (2005). The economy of phishing: a survey of the operations of the phishing market. *First Monday* 10, 1–11. doi:10.5210/fm.v10i9.1272

Abu-Nimeh, S., and Nair, S. (2008). "Bypassing security toolbars and phishing filters via dns poisoning," in IEEE GLOBECOM 2008–2008 IEEE global telecommunications conference, New Orleans, LA, November 30–December 2, 2008 (IEEE), 1–6. doi:10.1109/GLOCOM.2008.ECP.386

Aburrous, M., Hossain, M. A., Thabatah, F., and Dahal, K. (2008). "Intelligent phishing website detection system using fuzzy techniques," in 2008 3rd international conference on information and communication technologies: from theory to applications (New York, NY: IEEE, 1–6. doi:10.1109/ICTTA.2008.4530019

Afroz, S., and Greenstadt, R. (2009). "Phishzoo: an automated web phishing detection approach based on profiling and fuzzy matching," in Proceeding 5th IEEE international conference semantic computing (ICSC), 1–11.

Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *Int. J. Human-Computer Stud.* 82, 69–82. doi:10.1016/j.ijhcs.2015.05.005

APWG (2018). *Phishing activity trends report 3rd quarter 2018*. US. 1–11.

APWG (2020). APWG phishing attack trends reports. 2020 anti-phishing work. Group, Inc. Available at: https://apwg.org/trendsreports/ (Accessed September 20, 2020).

Arachchilage, N. A. G., and Love, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Comput. Hum. Behav.* 38, 304–312. doi:10.1016/j.chb.2014.05.046

Arnsten, B. A., Mazure, C. M., and April, R. S. (2012). Everyday stress can shut down the brain's chief command center. *Sci. Am.* 306, 1–6. Available at: https://www.scientificamerican.com/article/this-is-your-brain-in-meltdown/ (Accessed October 15, 2019).

Bailey, J. L., Mitchell, R. B., and Jensen, B. k. (2008). "Analysis of student vulnerabilities to phishing," in 14th americas conference on information systems, AMCIS 2008, 75–84. Available at: https://aisel.aisnet.org/amcis2008/271.

Barracuda (2020). Business email compromise (BEC). Available at: https://www.barracuda.com/glossary/business-email-compromise (Accessed November 15, 2020).

Belcic, I. (2020). Rootkits defined: what they do, how they work, and how to remove them. Available at: https://www.avast.com/c-rootkit (Accessed November 7, 2020).

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., and Strobel, S. (2010). New filtering approaches for phishing email. *JCS* 18, 7–35. doi:10.3233/JCS-2010-0371

Bin, S., Qiaoyan, W., and Xiaoying, L. (2010). "A DNS based anti-phishing approach." in 2010 second international conference on networks security, wireless communications and trusted computing, Wuhan, China, April 24–25, 2010. (IEEE), 262–265. doi:10.1109/NSWCTC.2010.196

Boddy, M. (2018). Phishing 2.0: the new evolution in cybercrime. *Comput. Fraud Secur.* 2018, 8–10. doi:10.1016/S1361-3723(18)30108-8

Casciani, D. (2019). Zain Qaiser: student jailed for blackmailing porn users worldwide. Available at: https://www.bbc.co.uk/news/uk-47800378 (Accessed April 9, 2019).

Chanti, S., and Chithralekha, T. (2020). Classification of anti-phishing solutions. *SN Comput. Sci.* 1, 11. doi:10.1007/s42979-019-0011-2

Checkpoint (2020). Check point research's Q1 2020 brand phishing report. Available at: https://www.checkpoint.com/press/2020/apple-is-most-imitated-brand-for-phishing-attempts-check-point-researchs-q1-2020-brand-phishing-report/ (Accessed August 6, 2020).

cisco (2018). What is the difference: viruses, worms, Trojans, and bots? Available at: https://www.cisco.com/c/en/us/about/security-center/virus-differences.html (Accessed January 20, 2020).

CISA (2018). What is phishing. Available at: https://www.us-cert.gov/report-phishing (Accessed June 10, 2019).

Cormack, G. V., Smucker, M. D., and Clarke, C. L. A. (2011). Efficient and effective spam filtering and re-ranking for large web datasets. *Inf. Retrieval* 14, 441–465. doi:10.1007/s10791-011-9162-z

Corrata (2018). The rising threat of social media phishing attacks. Available at: https://corrata.com/the-rising-threat-of-social-media-phishing-attacks/%0D (Accessed October 29, 2019).

Crane, C. (2019). The dirty dozen: the 12 most costly phishing attack examples. Available at: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attack-examples/#:~:text=At some level%2C everyone is susceptible to phishing,outright trick you into performing a particular task (Accessed August 2, 2020).

CSI Onsite (2012). Phishing. Available at: http://csionsite.com/2012/phishing/ (Accessed May 8, 2019).

Cui, Q., Jourdan, G.-V., Bochmann, G. V., Couturier, R., and Onut, I.-V. (2017). Tracking phishing attacks over time. *Proc. 26th Int. Conf. World Wide Web - WWW '17*, Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee. 667–676. doi:10.1145/3038912.3052654

CVEdetails (2005). Vulnerability in microsoft internet explorer. Available at: https://www.cvedetails.com/cve/CVE-2005-4089/ (Accessed August 20, 2019).

Cybint Cyber Solutions (2018). 13 alarming cyber security facts and stats. Available at: https://www.cybintsolutions.com/cyber-security-facts-stats/ (Accessed July 20, 2019).

Deshmukh, M., and raddha Popat, S. (2017). Different techniques for detection of phishing attack. *Int. J. Eng. Sci. Comput.* 7, 10201–10204. Available at: http://ijesc.org/.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). "Why phishing works," in Proceedings of the SIGCHI conference on human factors in computing systems - CHI '06, Montréal Québec, Canada, (New York, NY: ACM Press), 581. doi:10.1145/1124772.1124861

Diaz, A., Sherman, A. T., and Joshi, A. (2020). Phishing in an academic community: a study of user susceptibility and behavior. *Cryptologia* 44, 53–67. doi:10.1080/01611194.2019.1623343

Dodge, R. C., Carver, C., and Ferguson, A. J. (2007). Phishing for user security awareness. *Comput. Security* 26, 73–80. doi:10.1016/j.cose.2006.10.009

eBay Toolbar and Account Guard (2009). Available at: https://download.cnet.com/eBay-Toolbar/3000-12512_4-10153544.html (Accessed August 7, 2020).

EDUCBA (2017). Hackers vs crackers: easy to understand exclusive difference. Available at: https://www.educba.com/hackers-vs-crackers/ (Accessed July 17, 2019).

Evers, J. (2006). Security expert: user education is pointless. Available at: https://www.cnet.com/news/security-expert-user-education-is-pointless/ (Accessed June 25, 2019).

F5Networks (2018). Panda malware broadens targets to cryptocurrency exchanges and social media. Available at: https://www.f5.com/labs/articles/threat-intelligence/panda-malware-broadens-targets-to-cryptocurrency-exchanges-and-social-media (Accessed April 23, 2019).

Fette, I., Sadeh, N., and Tomasic, A. (2007). "Learning to detect phishing emails," in Proceedings of the 16th international conference on world wide web - WWW '07, Banff Alberta, Canada, (New York, NY: ACM Press), 649–656. doi:10.1145/1242572.1242660

Financial Fraud Action UK (2017). Fraud the facts 2017: the definitive overview of payment industry fraud. London. Available at: https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf.

Fraud Watch International (2019). Phishing attack trends for 2019. Available at: https://fraudwatchinternational.com/phishing/phishing-attack-trends-for-2019/ (Accessed October 29, 2019).

FTC (2018). Netflix scam email. Available at: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing (Accessed May 8, 2019).

Furnell, S. (2007). An assessment of website password practices). *Comput. Secur.* 26, 445–451. doi:10.1016/j.cose.2007.09.001

Getsafeonline (2017). Caught on the net. Available at: https://www.getsafeonline.org/news/caught-on-the-net/%0D (Accessed August 1, 2020).

GOV.UK (2020). Cyber security breaches survey 2020. Available at: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020 (Accessed August 6, 2020).

Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. (2015). "Phoneypot: data-driven understanding of telephony threats," in Proceedings 2015 network and distributed system security symposium, (Reston, VA: Internet Society), 8–11. doi:10.14722/ndss.2015.23176

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3, e00346-18. doi:10.1016/j.heliyon.2017.e00346

Herley, C., and Florêncio, D. (2008). "A profitless endeavor," in New security paradigms workshop (NSPW '08), New Hampshire, United States, October 25–28, 2021, 1–12. doi:10.1145/1595676.1595686

Hewage, C. (2020). Coronavirus pandemic has unleashed a wave of cyber attacks – here's how to protect yourself. *Conversat*. Available at: https://theconversation.com/coronavirus-pandemic-has-unleashed-a-wave-of-cyber-attacks-heres-how-to-protect-yourself-135057 (Accessed November 16, 2020).

Hong, J. (2012). The state of phishing attacks. *Commun. ACM* 55, 74–81. doi:10.1145/2063176.2063197

Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. (2009). "Towards automating social engineering using social networking sites," in 2009 international conference on computational science and engineering, Vancouver, BC, August 29–31, 2009 (IEEE, 117–124. doi:10.1109/CSE.2009.205

Hutchings, A., Clayton, R., and Anderson, R. (2016). "Taking down websites to prevent crime," in 2016 APWG symposium on electronic crime research (eCrime) (IEEE), 1–10. doi:10.1109/ECRIME.2016.7487947

Iuga, C., Nurse, J. R. C., and Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Hum. Cent. Comput. Inf. Sci.* 6, 8. doi:10.1186/s13673-016-0065-2

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007). Social phishing. *Commun. ACM* 50, 94–100. doi:10.1145/1290958.1290968

Jakobsson, M., and Myers, S. (2006). *Phishing and countermeasures: understanding the increasing problems of electronic identity theft*. New Jersey: John Wiley and Sons.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., and Lim, Y. K. (2007). "What instills trust? A qualitative study of phishing," in *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, (Berlin, Heidelberg: Springer), 356–361. doi:10.1007/978-3-540-77366-5_32

Jeeva, S. C., and Rajsingh, E. B. (2016). Intelligent phishing url detection using association rule mining. *Hum. Cent. Comput. Inf. Sci.* 6, 10. doi:10.1186/s13673-016-0064-3

Johnson, A. (2016). Almost 600 accounts breached in "celebgate" nude photo hack, FBI says. Available at: http://www.cnbc.com/id/102747765 (Accessed: February 17, 2020).

Kayne, R. (2019). What are script kiddies? Wisegeek. Available at: https://www.wisegeek.com/what-are-script-kiddies.htm V V February 19, 2020).

Keck, C. (2018). FTC warns of sketchy Netflix phishing scam asking for payment details. Available at: https://gizmodo.com/ftc-warns-of-sketchy-netflix-phishing-scam-asking-for-p-1831372416 (Accessed April 23, 2019).

Keepnet LABS (2018). Statistical analysis of 126,000 phishing simulations carried out in 128 companies around the world. USA, France. Available at: www.keepnetlabs.com.

Keinan, G. (1987). Decision making under stress: scanning of alternatives under controllable and uncontrollable threats. *J. Personal. Soc. Psychol.* 52, 639–644. doi:10.1037/0022-3514.52.3.639

Khonji, M., Iraqi, Y., and Jones, A. (2013). Phishing detection: a literature survey. *IEEE Commun. Surv. Tutorials* 15, 2091–2121. doi:10.1109/SURV.2013.032213.00009

Kirda, E., and Kruegel, C. (2005). Protecting users against phishing attacks with AntiPhish. *Proc. - Int. Comput. Softw. Appl. Conf.* 1, 517–524. doi:10.1109/COMPSAC.2005.126

Krawchenko, K. (2016). The phishing email that hacked the account of John Podesta. CBSNEWS. Available at: https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ (Accessed April 13, 2019).

Ksepersky (2020). Spam and phishing in Q1 2020. Available at: https://securelist.com/spam-and-phishing-in-q1-2020/97091/ (Accessed July 27, 2020).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol.* 10, 1–31. doi:10.1145/1754393.1754396

Latto, N. (2020). What is adware and how can you prevent it? Avast. Available at: https://www.avast.com/c-adware (Accessed May 8, 2020).

Le, D., Fu, X., and Hogrefe, D. (2006). A review of mobility support paradigms for the internet. *IEEE Commun. Surv. Tutorials* 8, 38–51. doi:10.1109/COMST.2006.323441

Lehman, T. J., and Vajpayee, S. (2011). "We've looked at clouds from both sides now," in 2011 annual SRII global conference, San Jose, CA, March 20–April 2, 2011, (IEEE, 342–348. doi:10.1109/SRII.2011.46

Leyden, J. (2001). Virus toolkits are s'kiddie menace. Regist. Available at: https://www.theregister.co.uk/2001/02/21/virus_toolkits_are_skiddie_menace/%0D (Accessed June 15, 2019).

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., and Zhang, J. (2012). "Expectation and purpose," in Proceedings of the 2012 ACM conference on ubiquitous computing - UbiComp '12 (New York, New York, USA: ACM Press), 1625. doi:10.1145/2370216.2370290

Lininger, R., and Vines, D. R. (2005). *Phishing: cutting the identity theft line. Print book*. Indiana: Wiley Publishing, Inc.

Ma, J., Saul, L. K., Savage, S., and Voelker, G. M. (2009). "Identifying suspicious URLs." in Proceedings of the 26th annual international conference on machine learning - ICML '09 (New York, NY: ACM Press), 1–8. doi:10.1145/1553374.1553462

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., and Capkun, S. (2015). Personalized security indicators to detect application phishing attacks in mobile platforms. Available at: http://arxiv.org/abs/1502.06824.

Margaret, R. I. P. (2008). PBX (private branch exchange). Available at: https://searchunifiedcommunications.techtarget.com/definition/IP-PBX (Accessed June 19, 2019).

Maurer, M.-E., and Herzner, D. (2012). Using visual website similarity for phishing detection and reporting. 1625–1630. doi:10.1145/2212776.2223683

Medvet, E., Kirda, E., and Kruegel, C. (2008). "Visual-similarity-based phishing detection," in Proceedings of the 4th international conference on Security and privacy in communication netowrks - SecureComm '08 (New York, NY: ACM Press), 1. doi:10.1145/1460877.1460905

Merwe, A. v. d., Marianne, L., and Marek, D. (2005). "Characteristics and responsibilities involved in a Phishing attack, in WISICT '05: proceedings of the 4th international symposium on information and communication technologies. Trinity College Dublin, 249–254.

Microsoft (2020). Exploiting a crisis: how cybercriminals behaved during the outbreak. Available at: https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/ (Accessed August 1, 2020).

Mince-Didier, A. (2020). Hacking a computer or computer network. Available at: https://www.criminaldefenselawyer.com/resources/hacking-computer.html (Accessed August 7, 2020).

Miyamoto, D., Hazeyama, H., and Kadobayashi, Y. (2009). "An evaluation of machine learning-based methods for detection of phishing sites," *in*international conference on neural information processing ICONIP 2008: advances in neuro-information processing lecture notes in computer science. Editors M. Köppen, N. Kasabov, and G. Coghill (Berlin, Heidelberg: Springer Berlin Heidelberg), 539–546. doi:10.1007/978-3-642-02490-0_66

Mohammad, R. M., Thabtah, F., and McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. *Neural Comput. Applic* 25, 443–458. doi:10.1007/s00521-013-1490-z

Moore, T., and Clayton, R. (2007). "Examining the impact of website take-down on phishing," in Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit on - eCrime '07 (New York, NY: ACM Press), 1–13. doi:10.1145/1299015.1299016

Morgan, S. (2019). 2019 official annual cybercrime report. USA, UK, Canada. Available at: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

Nathan, G. (2020). What is phishing? + laws, charges & statute of limitations. Available at: https://www.federalcharges.com/phishing-laws-charges/ (Accessed August 7, 2020).

Okin, S. (2009). From script kiddies to organised cybercrime. Available at: https://comsecglobal.com/from-script-kiddies-to-organised-cybercrime-things-are-getting-nasty-out-there/ (Accessed August 12, 2019).

Ollmann, G. (2004). The phishing guide understanding & preventing phishing attacks abstract. USA. Available at: http://www.ngsconsulting.com.

Ong, S. (2014). Avast survey shows men more susceptible to mobile malware. Available at: https://www.mirekusoft.com/avast-survey-shows-men-more-susceptible-to-mobile-malware/ (Accessed November 5, 2020).

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S., and Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks. *ACM Trans. Intell. Syst. Technol.* 8, 1–25. doi:10.1080/00207284.1985.11491413

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud Security*, 2012, 8–11. doi:10.1016/S1361-3723(12)70007-6

Phish Labs (2019). 2019 phishing trends and intelligence report the growing social engineering threat. Available at: https://info.phishlabs.com/hubfs/2019 PTI Report/2019 Phishing Trends and Intelligence Report.pdf.

PhishMe (2016). Q1 2016 malware review. Available at: WWW.PHISHME.COM.

PhishMe (2017). Human phishing defense enterprise phishing resiliency and defense report 2017 analysis of susceptibility, resiliency and defense against simulated and real phishing attacks. Available at: https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf.

PishTank (2006). What is phishing. Available at: http://www.phishtank.com/what_is_phishing.php?view=website&annotated=true (Accessed June 19, 2019).

Pompon, A. R., Walkowski, D., and Boddy, S. (2018). *Phishing and Fraud Report attacks peak during the holidays. US*.

Proofpoint (2019a). State of the phish 2019 report. *Sport Mark. Q.* 14, 4. doi:10.1038/sj.jp.7211019

Proofpoint (2019b). What is Proofpoint. Available at: https://www.proofpoint.com/us/company/about (Accessed September 25, 2019).

Proofpoint (2020). 2020 state of the phish. Available at: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf.

Raggo, M. (2016). Anatomy of a social media attack. Available at: https://www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680 (Accessed March 14, 2019).

Ramanathan, V., and Wechsler, H. (2012). PhishGILLNET-phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training. *EURASIP J. Info. Secur.* 2012, 1–22. doi:10.1186/1687-417X-2012-1

Ramzan, Z. (2010). "Phishing attacks and countermeasures," in *Handbook of Information and communication security* (Berlin, Heidelberg: Springer Berlin Heidelberg), 433–448. doi:10.1007/978-3-642-04117-4_23

Ramzan, Z., and Wuest, C. (2007). "Phishing Attacks: analyzing trends in 2006," in Fourth conference on email and anti-Spam (Mountain View, (California, United States).

Rhett, J. (2019). Don't fall for this new Google translate phishing attack. Available at: https://www.gizmodo.co.uk/2019/02/dont-fall-for-this-new-google-translate-phishing-attack/ (Accessed April 23, 2019). doi:10.5040/9781350073272

RISKIQ (2020). Investigate | COVID-19 cybercrime weekly update. Available at: https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/%0D (Accessed August 1, 2020).

Robichaux, P., and Ganger, D. L. (2006). Gone phishing: evaluating anti-phishing tools for windows. Available at: http://www.3sharp.com/projects/antiphishing/gonephishing.pdf.

Rouse, M. (2013). Phishing defintion. Available at: https://searchsecurity.techtarget.com/definition/phishing (Accessed April 10, 2019).

Salem, O., Hossain, A., and Kamala, M. (2010). "Awareness program and AI based tool to reduce risk of phishing attacks," in 2010 10th IEEE international conference on computer and information technology (IEEE), Bradford, United Kingdom, June 29–July 1, 2010, 2001 (IEEE), 1418–1423. doi:10.1109/CIT.2010.254

Scaife, N., Carter, H., Traynor, P., and Butler, K. R. B. (2016). "Crypto lock (and drop it): stopping ransomware attacks on user data," in 2016 IEEE 36th international conference on distributed computing systems (ICDCS) (IEEE, 303–312. doi:10.1109/ICDCS.2016.46

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. (2007). "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," in Proceedings of the 3rd symposium on usable privacy and security - SOUPS '07 (New York, NY: ACM Press), 88–99. doi:10.1145/1280680.1280692

Symantic (2019). *Internet security threat report volume 24|February 2019*. USA.

Techpedia (2021). Caller ID. Available at: https://www.techopedia.com/definition/24222/caller-id (Accessed June 19, 2019).

VadeSecure (2021). Phishers favorites 2019. Available at: https://www.vadesecure.com/en/ (Accessed October 29, 2019).

Vishwanath, A. (2005). "Spear phishing: the tip of the spear used by cyber terrorists," in deconstruction machines (United States: University of Minnesota Press), 469–484. doi:10.4018/978-1-5225-0156-5.ch023

Wang, X., Zhang, R., Yang, X., Jiang, X., and Wijesekera, D. (2008). "Voice pharming attack and the trust of VoIP," in Proceedings of the 4th international conference on security and privacy in communication networks, SecureComm'08, 1–11. doi:10.1145/1460877.1460908

Wenyin, L., Huang, G., Xiaoyue, L., Min, Z., and Deng, X. (2005). "Detection of phishing webpages based on visual similarity," in 14th international world wide web conference, WWW2005, Chiba, Japan, May 10–14, 2005, 1060–1061. doi:10.1145/1062745.1062868

Whitman, M. E., and Mattord, H. J. (2012). Principles of information security. *Course Technol.* 1–617. doi:10.1016/B978-0-12-381972-7.00002-6

Williams, E. J., Hinds, J., and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *Int. J. Human-Computer Stud.* 120, 1–13. doi:10.1016/j.ijhcs.2018.06.004

wombatsecurity.com (2018). Wombat security user risk report. USA. Available at: https://info.wombatsecurity.com/hubfs/WombatProofpoint-UserRiskSurveyReport2018_US.pdf.

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci.* 59 (4), 662–674. doi:10.1002/asi.20779

Yeboah-Boateng, E. O., and Amanor, P. M. (2014). Phishing , SMiShing & vishing: an assessment of threats against mobile devices. *J. Emerg. Trends Comput. Inf. Sci.* 5 (4), 297–307.

Zhang, Y., Hong, J. I., and Cranor, L. F. (2007). "Cantina," in Proceedings of the 16th international conference on World Wide Web - WWW '07 (New York, NY: ACM Press), 639. doi:10.1145/1242572.1242659

Zissis, D., and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generat. Comput. Syst.* 28, 583–592. doi:10.1016/j.future.2010.12.006

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

GLOSSARY

AOL America Online

APWG Anti Phishing Working Group Advanced

APRANET Advanced Research Projects Agency Network.

ARP address resolution protocol.

BHO Browser Helper Object

BEC business email compromise

COVID-19 Coronavirus disease 2019

CSS cascading style sheets

DDoS distributed denial of service

DNS Domain Name System

DoS Denial of Service

FTC Federal Trade Commission

FL Fuzzy Logic

HTTPS Hypertext Transfer Protocol Secure

IE Internet Explorer

ICT Information and Communications Technology

IM Instant Message

IT Information Technology

IP Internet Protocol

MITM Man-in-the-Middle

NCA National Crime Agency

NFIB National Fraud Intelligence Bureau

PIPCU Police Intellectual Property Crime Unit

OS Operating Systems

PBX Private Branch Exchange

SMishing Text Message Phishing

SPF Sender Policy Framework

SMTP Simple Mail Transfer Protocol

SMS Short Message Service

Soshing Social Media Phishing

SQL structured query language

URL Uniform Resource Locator

UK United Kingdom

US United States

USB Universal Serial Bus

US-CERT United States Computer Emergency Readiness Team.

Vishing Voice Phishing

VNC Virtual Network Computing

VoIP Voice over Internet Protocol

XSS Cross-Site Scripting