International Journal of Cyber-Security and Digital Forensics (IJCSDF) 10(1): 28-41
The Society of Digital Information and Wireless Communications (SDIWC), 2021 ISSN: 2305-0011

A Comparative Analysis between Technical and Non-Technical Phishing Defences

Joseph C. Brickley[1], Kutub Thakur[1], Abu S. Kamruzzaman[2]
[1] Professional Security Studies, New Jersey City University Jersey City, NJ United States
[2] Seidenberg School of Computer Science and Information Systems, Pace University, Pleasantville, NY United States

jbrickley@njcu.edu, kthakur@njcu.edu, ak91252p@pace.edu

ABSTRACT

Phishing attacks are a form of social engineering attacks which are designed to extract sensitive information through email and are a growing problem in today's world. The cost of falling victim to a Phishing attack could not only cause immediate financial harm, but it can cost the company at risk to tarnish its reputation and expose valuable information and data. This study compared technical and non-technical defenses that combat Phishing as a whole to determine what defense should be used. Using existing literature to compare what other scholars have found and in an un-biased way determine which defense type is better at combating Phishing as a whole. The findings pointed in the direction of non-technical defenses, as users often ignored indicators produced by technical defenses. When technical defenses blocked users from receiving Phishing attempts, the user often lacked awareness and training to properly determine a Phishing attack. In conclusion, a multi defense approach should be put in place with a focus on non-technical controls such as user training, and specifically game-based training, to complement technical defenses such as ProofPoint, Barracuda Sentinel and Anti-Phishing software.

KEYWORDS
Phishing, defense, Barracuda, Cofense, ProofPoint,

I. INTRODUCTION

As strides in technology are constantly being made and the realm of technological abilities expands, the boundaries for cyberattacks seem to become infinite. As technology itself advances, it becomes more secure as the users of that technology (people) become more susceptible to attacks. Cyber criminals are relying on people being susceptible in the aspect of cyber-security, and engaging in social engineering to target potential victims. Social engineering is explained as being "an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks" [1]. Those individuals looking to carry out cyber-attacks are utilizing a social engineering attack called Phishing to target potential victims. National Institute of Standards and Technology defines Phishing as "using deceptive computer-based means to trick individuals into disclosing sensitive information" [2]. There are various forms of Phishing attacks consisting of Whaling and Spear Phishing, which all target different groups of potential victims. Whaling targets senior level and executive leadership in organizations, while Spear Phishing is intended to target a broader group such as employees from a specific company or field. The purpose of this study will focus on Phishing as whole.

There has been a dramatic rise in the number of cyber-attacks over the last twenty years. One of the most notable increases spans from the year 2006 to 2012, where the total amount of reported cyber security incidents increased from 5,503 to 48,562, a 782 percent increase [3]. Such large increases signal that sensitive information is left at risk. With the main objective of Phishing attacks targeting the disclosure of sensitive information, this is a subject that cannot be ignored.

Falling victim to Phishing attacks not only exposes sensitive information for individuals, companies, and organizations, but it can be extremely costly. In 2015 one successful Phishing attack costed a single company 100 million dollars breaking the previous record of 62 million dollars[4]. It comes as no surprise that this particular attack and the financial loss it caused grabbed the Federal Bureau of Investigation's

(FBI) attention. The FBI released a public service announcement in 2018, where they estimated that over a five (5) year spans more than 12 billion dollars has been stolen from companies [5].
The success of a Phishing attempt will not only cost a company financially but also effects the company's reputation. It can be difficult to try to determine the exact number of successful Phishing attacks as many companies try to conceal them. If a company reports that they have fallen victim to a Phishing attack it can affect their reputation, which may negatively affect their market value. Potential customers may try to avoid using the services of a company if they have recently announced a breach of sensitive information[6]. With the threat of Phishing only continuing to increase, this study attempts to compare four technical and three non-technical defenses to Phishing attacks. The four technical defenses against Phishing that will be assessed are Anti-Phishing Toolbars, ProofPoint, artificial intelligence specifically Barracuda Sentinel, and Anti-Phishing Software. In addition to the technical defenses presented and analyzed, three non-technical defenses will be Anti-Phishing Web-Based Training, Anti-Phishing programs, and Game-Based Training. Following a comparison of both technical and non-technical defenses, the study will give recommendations for effective defenses against Phishing and for future research.

2 TECHNICAL DEFENSES

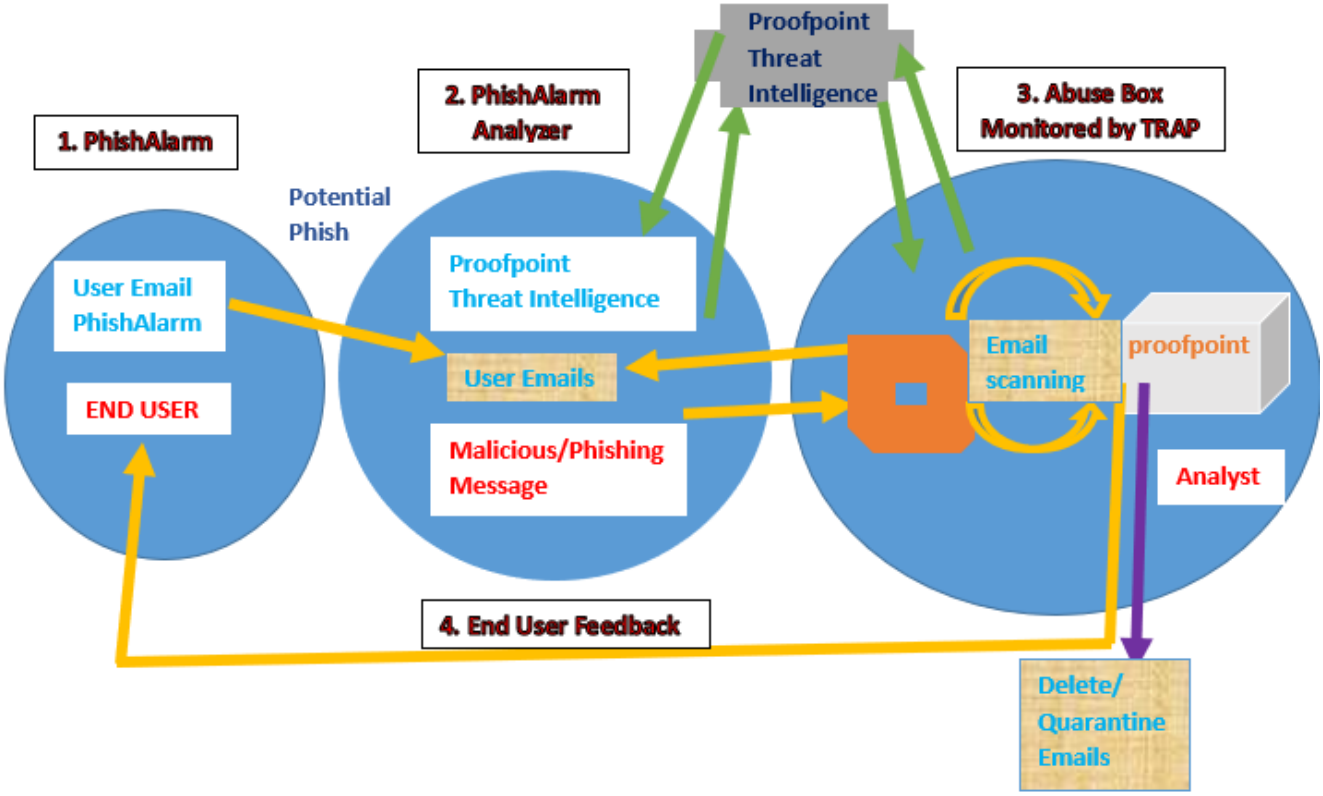
2.1 Anti-Phishing Toolbars

Anti-Phishing Toolbars are designed to identify whether a webpage is legitimate, or a Phishing webpage designed to trick the user to provide personal and sensitive information. There are multiple methods that these toolbars use to identify legitimate webpages from Phishing webpages consisting of user based, whitelisting, black listening, and heuristic based. User based is where each user judges if they believe the webpage is safe or presents a threat. Then the toolbar will present the user with whatever decision the majority of other users voted for. Each user of this type of tool bar is also presented with a score that reflects the amount of times they successfully selected the correct answer for the webpages. White listing consists of a list of websites that are verified as safe sites that are permitted access and denies users from accessing all other sites not listed. Blacklisting is the opposite, where all known Phishing websites are listed and denied access and all other websites are granted access. Lastly, there is a method called heuristic based that looks for specific behaviors to determine if a website is safe or opposes a threat.

2.2 Proofpoint

Proofpoint in [7] offers email protection for both inbound and outbound email. It is designed to help secure and control the known and unknown potential dangers that email threats present. This is done by using multilayered and machine learning techniques which determine and thwart potential email threats such as Phishing. It allows complete flexibility, allowing admins to create their own custom security rules and policies. It is offered for a variety of services such as on grounds, hybrid, and cloud installations. Proofpoint also allows users to utilize data loss protection and email encryption benefits to protect sensitive information. With benefits this vast it is no wonder Proofpoint was ranked the most implemented email security solution by the Fortune 1000.
Proofpoint according to [8] grants end users with a security assessment when their account has been created. The assessment gives them insistent feedback on each question to help reinforce correctly answered questions and educate best practices for incorrect answered questions. The training can be deployed in numerous methods consisting of game-based, video, interactive, newsletters, posters, infographics and more. It allows the Proofpoint admin to set a threshold for end users to test out of the training, based on their level of knowledge and expertise towards Phishing. Proofpoint offers preset test assessments, a library of additional questions you can assign end users, and the ability for admins to create new questions. The result of the end user assessment is gathered and displayed to show what areas the end user needs improvement. Proofpoint grants admins the ability to select five different Phishing campaigns that will send end users Phishing attacks to gauge their awareness. The five campaigns consist of data entry Phishing, attachment Phishing campaign, classic attachment Phishing campaign, drive-by Phishing campaign, and USB campaign. With the ability link Proofpoint with an active directory allows the

admin to send specific campaigns to be deployed to specific groups of end users.



Users of Proofpoint in [9] also have the ability to identify emails as a Phishing attempt with the PhishAlarm feature. Figure 1 shows a clear workflow where a user that spots a potential Phishing attempt will select the PhishAlarm button, the email will then be scored by the PhishAlarm analyzer. Following the analyzers score the email will be pulled off of every user email across the entire organization. With the end user who identified the Phishing email receiving feedback on all accounts.

2.3 Artificial Intelligence Based Phishing

Artificial intelligence (A.I.) is used to eliminate the wait time of an analyst by implementing real-time protection for emails. According to [10], Barracuda Sentinel is an example of an A.I. email protection tool used to defend against Phishing, account takeovers, and business email compromise (BEC). Barracuda Sentinel is paired with Microsoft Office 365 to form a cloud-based defense tool. Figure 2 shows an abridgment of how Barracuda Sentinel operates. By utilizing its A.I. to read internal, external, and historical emails via application programming interface, the A.I. can detect trends and patterns, which then allow the A.I. to block anomalies and Phishing attacks in real time. Barracuda Sentinel will also detect and isolate Phishing emails automatically to protect its users.

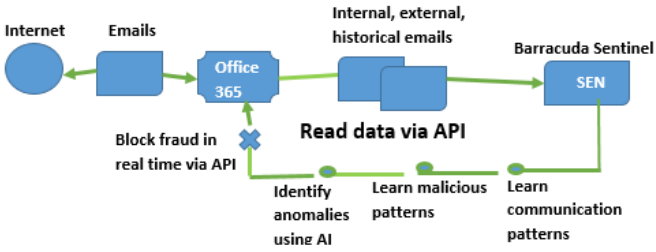


Figure 1. Demonstrates how Barracuda Sentinel functions (redrawn) [10]

2.4 Anti-Phishing Software

Anti-Phishing software has been developed to filter incoming emails, categorize it, and relocate it into the correct mailbox. The software's goal is to prevent Phishing attempts from being delivered to the potential victim. Anti-phishing software uses an out of sight out of mind approach. The software is used as a preventive control to disallow users from even receiving the potential Phishing emails in their active inbox. If the software identifies an

email as a Phishing email it will forward it into a spam inbox where the owner of the email account by default will not receive notifications of the received email.

3 TECHNICAL LITERATURE

There are many different Anti-Phishing Toolbars available on the opensource that all use their own, or a combination of methods to detect Phishing threats. The way that these toolbars are configured plays a huge role in their effectiveness in correctly identifying potential threats. In a study conducted by Cranor et al. [11] they compared ten different Anti-Phishing toolbars with their base configurations in a series of manual and automated experiments. In that study, they found that half of the tested Anti-Phishing toolbars falsely identified 15% of Phishing websites and four of the other toolbars identified less than half of the fraudulent Phishing websites, and the last toolbar could not identify any of the Phishing websites.

Not only do many Anti-Phishing Toolbars falsely identify Phishing websites, but they are far from user friendly. All ten of the Anti-Phishing Toolbars had some problems with usability [11]. If the users that are relying on these toolbars to help properly identify Phishing threats cannot seem to properly use the toolbars, then even if the toolbar could correctly identify every single threat, it would be useless. The users need to know how to simply navigate through the toolbars and to be able to comprehend what the toolbar is presenting to them. Even if users knew what configuration setting that they would like to change or set, it would be a challenge for them to navigate through the toolbars to set them.

In the supporting study by Dhamija et al. [12] the findings showed that 23 percent of the studies participants did not understand or even look at the security indicators on the toolbars, browsers, and address bars often making them ineffective. Popup warnings for insecure certificates were also found to be ignored. Which led them to make the wrong decision 40 percent of the time. Meaning that even if the Anti-Phishing toolbars correctly identified every single Phishing threat and if they didn't have usability problems, that often users would still ignore the indicators and make the incorrect decision to proceed.

The participants in Dhamija et al. [12] study were concluded to have made incorrect judgments due to their lack of knowledge of security indicators and how they functioned. Visual icons and logos deceived even the more experienced participants. With 90 percent of the study's users falling victim to a Phishing website it was determined that indicators are ineffective for a considerable number of users and that other approaches are required.

In [13], Proofpoint email protection was compared to a competitor tool named Fortimail antispam devices to determine which tool better detected malware, spam, and Phishing emails. Proofpoint and Fortimail device functions were compared which is shown in Table 1 with each device having the same functions as an anti-spam filter. The study was conducted over a three-month period of evaluation for each device's accuracy using a confusion matrix. Table 2 shows the volume and average size of the inbound and outbound emails used during the three-month study with 200 of those emails being used for the actual comparison. Both Proofpoint and Fortimail were configured to be the mail gateway for all incoming emails.

During the three-month study in [13] Proofpoint outscored Fortimail in correctly identifying true positives with 144 compared to Fortimail's 126. Fortimail scored 44 true negatives while Proofpoint scored 33. Proofpoint outscored Fortimail again in false positives with Proofpoint scoring 14 and Fortimail scoring 32. Fortimail scored zero false negatives with Proofpoint recording nine. With the findings demonstrating that Proofpoint had scored an 89% accuracy rate while Fortimail scored 84%. Concluding that Proofpoint is the more accurate product based on this comparative analysis.

When compared with a competitor, Proofpoint demonstrated that it was the more accurate product. With Proofpoint not only being more accurate, but offering a wide variety of user training options it truly is no wonder it was ranked the most implemented email security solution by the Fortune 1000[7].

A.I. based Phishing defenses such as Barracuda Sentinel have the unique ability to operate in real time. In [14] a study was conducted to determine how accurate Barracuda Sentinel was at identifying BEC and Phishing attempts. The study was conducted throughout a dataset of 4,000 attacks that were used in the real world at several organizations. Example 1,2, and 3 show the different example types of BEC attacks that were

in a sample consisting of a wire transfer, rapport, and a spoofed name with a Phishing link. The study determines the accuracy of Barracuda Sentinel by using an impersonation and content classifier algorithm on a

Table 1. Shows a comparison of the device functions. [13]

No	Function	Fortimail	Proofpoint
1	Mail Quarantine Management (search filtering, manual release)	**OK**	**OK**
2	Integration with third-party spam URL and real-time blacklists (SURBL/RBL)	**OK**	**OK**
3	Global and local sender reputation	**OK**	**OK**
4	Deep email header Inspection	**OK**	**OK**
5	Realtime email activity tracking	**OK**	**OK**
6	Logging Admin Activity	**OK**	**OK**
7	Logging Email History (Subject, Sender, Attachment)	**OK**	**OK**
8	Mail Queue Management	**OK**	**OK**
9	Behavioral/Content Analysis	**OK**	**OK**
10	Threat Prevention	**OK**	**OK**
11	Dashboard Aktivitas Email	**OK**	**OK**

Table 2. Volume and average size of the inbound and outbound emails. [13]

	Inbound	Outbound	Overall
Peak Hourly Message Volume	2000	2000	4000
Average Message Size (KB)	215	215	430

trained Barracuda Sentinel; Meaning that the dataset was introduced into an already used A.I., that had detected the trends of internal, external, and historical emails. The dataset was manually labeled in order to determine how many actual attacks there were in it.

Example 1. Wire transfer example [14]

```
From : " Jane Smith " <jsmith@acrne.com>
To : " Joe Barnes " <jbarnes@acme.com>
Subject : Vendor Payment

Hey                                    Joe,
Are you around ? I need to send a wire
transfer ASAP to a vendor.
Jane
```

Example 2. Rapport example [14]

```
From : " Jane Smith " <jsmith@acme.com>
Reply - to : " Jane Smith " <ceo.
executive@outlook.com>
To : " Joe Barnes " <jbarnes@acme.com>
Subject : At desk ?

Joe , are you available for something
urgent ?
```

Example 3. Spoofed name with Phishing Link [14]

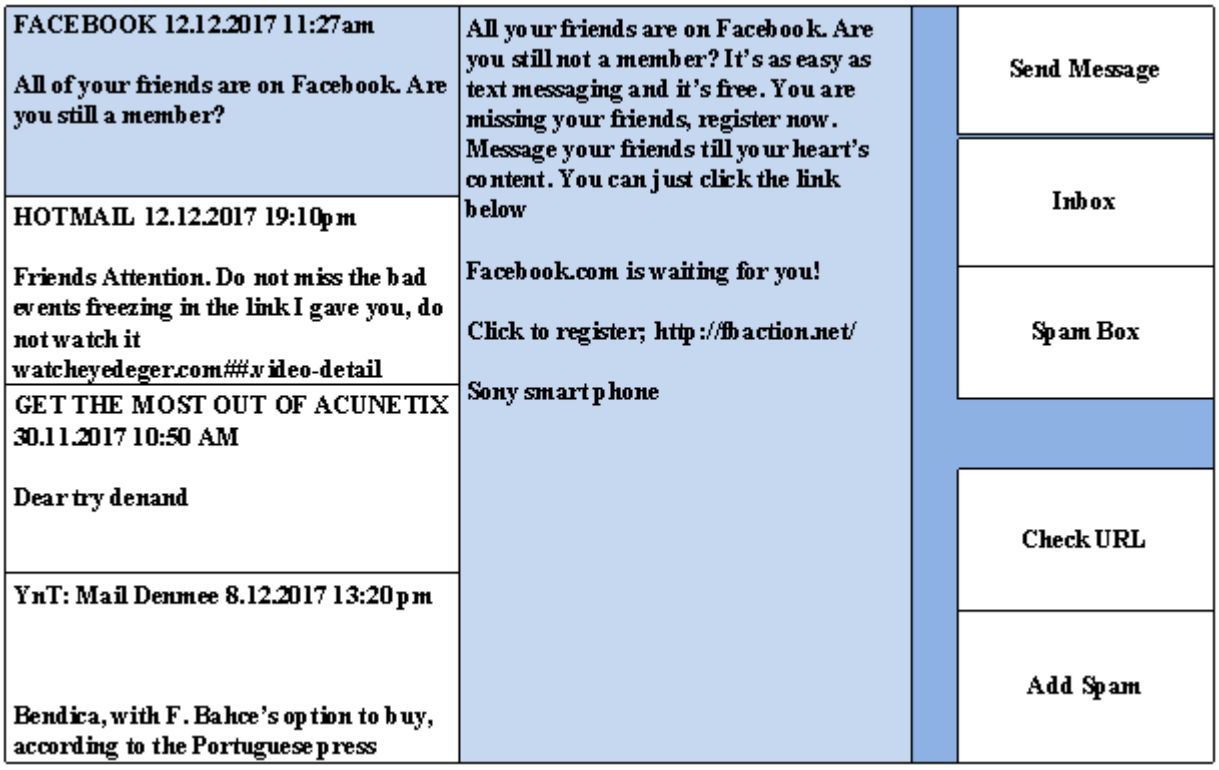
```
From : "Jane
Smith"<greyowl1234@comcast.net>
To : "Joe Barnes" <jbarnes@acme.com>

Subject : Invoice due number 381202214

I tried to reach you by phone today but I
couldn't get through. Please get back to
me with the status of the invoice below .

Invoice due number 381202214:
[http://firetruck4u.net/past-due-
invoice/]
```

The results of [14] concluded that the Barracuda Sentinel had a 98.2% efficiency rating at correctly identifying attacks from the dataset, with a one in 5.3 million false positive rate. Proving that Barracuda Sentinel is an extremely effective A.I. Phishing defense and a great technical option to combat Phishing in real time. There are many forms of Anti-Phishing software available that will help determine if incoming emails are a potential Phishing attempt. Many of the Anti-Phishing software that exists now use blacklists to determine if an email is a Phishing attempt or not. The problem is that the blacklist rarely gets updated and the individuals sending the Phishing attempts to create new methods to bypass the blacklist. Within the last few years, a study was conducted by Baykara et al. [15] where they developed software called "Anti Phishing



Phishing attacker. A study conducted by Sheng et. Al (2010) found that 28 percent of Phishing attacks aren't detected by even well-trained adults and that untrained adults would click on 52 percent of Phishing links. With 47 percent of those who clicked on the Phishing link falling victim and providing information. The findings indicated that training users can decrease the percentage of adult victims of Phishing attacks by 40 percent. The recommendations of Sheng et al. [16] study was that although user training can be extremely effective, it isn't a fix all. Comparatively speaking users can not solely rely on the blacklist alone.

Simulator" shown in figure 3 that improves on some of the weaknesses and downfalls of other existing Anti-Phishing software that use a blacklist. The Anti-Phishing Simulator uses a classification algorithm to determine if an incoming email is a Phishing attack. The algorithm will then add data that helps determine why an email is a Phishing attempt into a blacklist database to help further increase the criteria for determining future threats, thus constantly updating the blacklist database. If an email comes in with the use of overly exciting phrases that attempt to make viewers purchase something or reveal personally identifiable information the email is categorized as software has a feature called "add spam" (shown in figure 4) that allows the user to add unwanted key phrases, words and URL addresses or simply mail that the user doesn't want to receive to the blacklist a Phishing email and sent to the spam folder. The database. For users who are more technically sound the software has a feature called "URL control" that displays the HTML code so the user can determine if the links presented in the email are safe or not.

If Phishing attempts get passed the blacklist and into the users' email inbox there is no guarantee that the user will recognize that it is a Phishing attempt. They must have knowledge and be well trained in identifying potential Phishing attempts to be effective in properly identifying them. If the user isn't trained there is a very good chance they will click the link and provide information to the

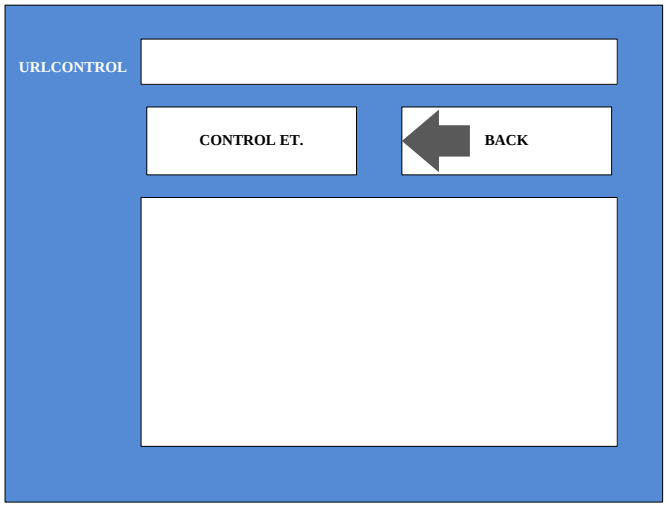


Figure 2. Shows the add spam option (redrawn). [15]

4 NON-TECHNICAL DEFENSES

4.1 Web-Based Training

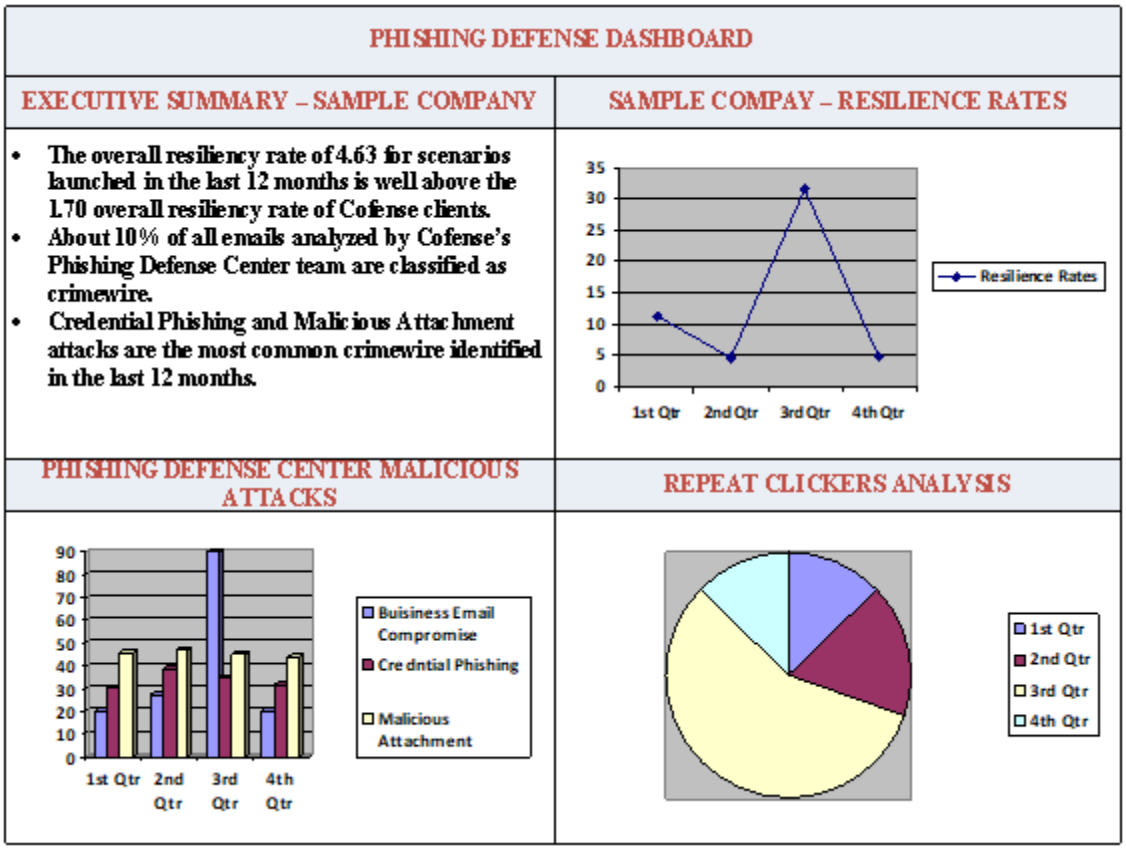
Web-based training is designed to conveniently allow its participants to view the training online via the Internet. It takes all classroom elements and makes them available to anyone in the world can view the training from anywhere. It can be extremely accessible and easy to use. Web-based training can be very cost-effective as the training can be developed once and then deployed a countless number of times; Unlike in-person training that requires an instructor to physically teach the training course every time it's presented and requires the participants to physically attend. Which can be inconvenient for many people who are not geographically or have the proper means to attend.

4.2 Anti-Phishing Program

Anti-Phishing programs are software as a service platforms (SaaS) that are customizable, aim to imitate real scenarios, and educate users. For this study we will take a look at Cofense Phishme. According to [17] Cofense Phishme trains users to identify and report Phishing emails. It offers intelligent automation by deploying educational content, attachments, landing pages and prepared Phishing scenarios throughout the year to constantly inform users, but not harass them, about relevant threats. Cofense Phishme uses machine learning to recommend scenarios to users based on relevance. The scenarios are only deployed when users are active in their inbox, increasing their involvement. The threat scenarios are pulled from an ever-growing database. The database contains Phishing scenarios that match your specific organization or industry as a whole. Cofense Phishme encourages users to actively report Phishing attempts. Overtime, the static that matters is being the report rate surpassing the click rate. Cofense Phishme offers extensive reports that track employees progress and monitor the company's performance showed in figure 5.

4.3 Anti-Phishing Game-Based Training

Anti-Phishing game-based training is designed to grab and maintain the user's attention, challenge, and educate the user. This game-based approach attempts to break the normal training methods of PowerPoint, videos, and readings. Those approaches usually find its users clicking through slides, playing videos in the background, and more times than not, bored. The game-based training approach attempts to change those modules by having active engagement always of the training and allow users to better retain knowledge.



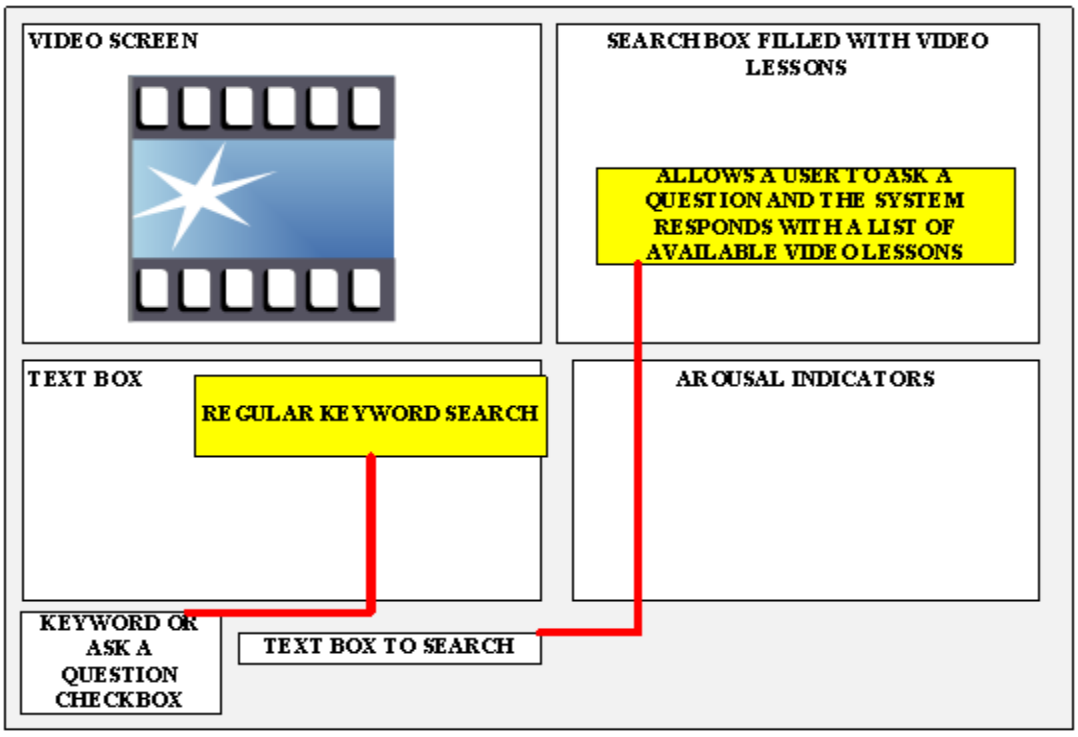
5 NON-TECHNCIAL LITERATURE

A study was conducted by Kumaraguru et al. [18] that investigated if a web-based training called PhishGuru was effective at increasing adult user resilience towards Phishing attacks. PhishGuru is web-based embedded training that focuses on educating users by sending them a comic strip that informs them of how simple it is for attackers to conduct Phishing attacks, defines Phishing, and actions that can be taken to avoid falling for potential Phishing attacks in the future. The comic strip is only sent to the user if they have fallen victim to a Phishing attack that was sent via PhishGuru. The purpose is to teach the victim in present time, the moment that he or she fell victim to the Phishing attack. The emails that are delivered via PhishGuru are meant to be used as a training opportunity and to assess the users on their ability to correctly determine a Phishing attempt.

Kumaraguru et al. [18] study had 515 participants categorized into three groups. The first group being the group that received no training, the second being those who were trained once, and the third being those that were trained twice. All 515 participants received 7 simulated Phishing emails and 3 legitimate ones over a 28-day timeline. The participants that clicked on the URL in the Phishing email, both legitimate and simulated who were in the trained one and two groups, received a PhishGuru comic strip. Those who were in the group that received zero training didn't receive any PhishGuru training upon clicking the URL.

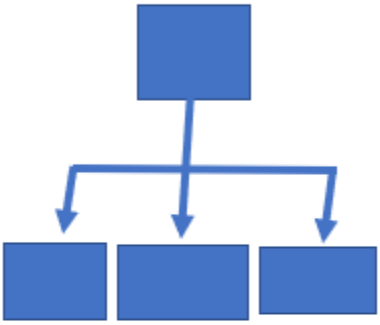
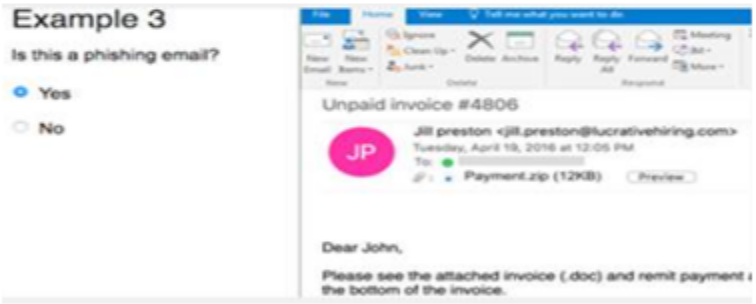
After 28 days Kumaraguru et al. [18] findings showed that users who received the PhishGuru training were less likely to click on the URL in the presented Phishing emails. The users who received the training twice outscored those who were trained once. Providing evidence that those who repeated the training improve user performance in identifying Phishing attempts thus increasing user resilience. Participants of the study who received the PhishGuru training highly recommended the training as the comic strips were a fun way to be trained. Kumaraguru et al. [18] also recommended that user technical defenses to Phishing should be complemented with non-technical defenses such as user training.

In 2008, a study was conducted that looked at the role of web-based training toward Phishing detection [19]. This consisted of a two-part study, in which each part was conducted a year apart. They were both conducted at a United States Air Force base with the first study having 119 officers



participate and the second study had 190 officers participate. There was a two-part focus of the training used for the study with one focusing on recognizing cues of deception (Phishing) and the second recognizing deception tactics. The participants of the study received two quantitative and qualitative pre and post-test with the order of questions changing for both. One of the pre and post-test was geared toward knowledge of deception detection tactics and the second focused on judgement of deception cues.

In the first study conducted by George et al. [19] participants were either assigned to a live lecture, a web-based training developed for the study called Agent99 (shown in figure 6) or received no training at all. Participants sat through three training sessions for the first study. In the second, the live lecture was removed, and participants attended one of four configurations of Agent99. One configuration was the original version of the Agent99 while the other three progressively increased user interaction with tests and quizzes. The second study conducted by George et al. [19]

	Description	Example
Section 1: Overview of Phishing	> Definition of social engineering > Anatomy of a phishing email > Demonstration of a phishing attack > Impact of phishing > How to report a phishing email	**Phishing 101** What is a Phishing Email? A phishing email is a type of social engineering designed to trick you into giving away information, or taking certain actions Attackers may ask for: > Usernames, passwords, secret questions > Social security numbers > Bank account and credit card information
Section 2: Phishing scenario	> Identification of the target > Setting the bait > Hooking the target > Mass infection > Data compromise > Consequence of a Phishing attack	**Mass Infection** John's computer is connected to the Network, therefore the malware can travel and infect other devices 
Section 3: Identifying a Phish	> Interactive examples of phishing emails	
Examination	> 10-question summary examination	

also replaced the group that received no training to receive a pre-recorded video taped lecture.

The results of the first study conducted by George et al. [19] showed that the participants who took the web-based training scored very similar in the post test deception introduction section, with the attendees of the live lecture scoring 60% and the participants from the web-based training scoring 59%. The web-based training participants scored better on the cues for deception section scoring 63% and the live lecture attendees scoring 57%. When the scores of the posttest were combined the web, based training scored 61% which outscored the live-in person lecture who scored 58.5%.

The results of the second study conducted by George et al. [19] had all participants increased their knowledge based on the post test results whether they attended the web based or the prerecorded lecture. However, the participants who took one of four configurations of the web-based training increased their pre to post test scores by an average of 15%. With the original version of Agent 99 improving post test scores by 15% and the other three more interactive versions by an average of 15% as well. Where the participants who attended the prerecorded live lecture increased their pre to post test scores by 10%.

Participants with the most interactive features scored 65% compared to the non-interactive web-based training scoring 64%. Overall, the results of George et al (2008) study showed that web-based training can be an effective way to incorporate Phishing training. The web-based training in all accounts outscored the in-person post test results when the two sections of the pre and post-test were combined. Participants of the study who used the web-based training with the most interactive features outscored the ones that used the basic version on post-test results.

The Anti-Phishing program called Cofense Phishme was deployed in [20] to better understand the click rate of a US hospital employee. The study broke the participants into two groups: offender and nonoffenders. With nonoffenders being those participants who hadn't clicked on Phishing emails and offenders being the participants who clicked on five Phishing emails. The study consisted of 5416 participants and there were 20 scenarios that were deployed between July 2015 until May 2018. 740 participants who were labeled offenders after scenario 15 received required Cofense Phishme training. The training consisted of three main sections as shown in Table 3.

The sections included an overview of phishing in section one, a Phishing scenario in section two, and section three identifying a Phish. After the three sections were completed the participants took a ten-question exam covering the material that was included in the previous three sections. The participants could retake the test as many times as needed to pass. The findings determined that 1.6% clicked on 10 Phishing emails, 65.3% clicked on two Phishing emails, and 17.9% did not click on one Phishing email. Classifying 772 participants in the offender group after all 20 scenarios concluded.

In [20] the click rate findings showed that over time they decreased with simulated Phishing scenarios being deployed. The study also showed that the group of offenders who received the mandatory training after scenario 15 did not have a significant impact on the click rate as they still remained more likely to click on a Phishing email than nonoffenders. However, the click rates in total decreased as the number of scenarios increased. Showing that real-time Phishing training deployed by Cofense Phishme when a participant clicked on a Phishing simulation decreased the click rate.

Cofense Phishme can be concluded to be an effective non-technical defense against Phishing by presenting real Phishing scenarios to users. Over time the click rate will decrease as users receive more training (when clicking on a scenario) and encountering different types of Phishing emails.

With better results leaning towards training that utilizes more user interactive features, it presents the question of whether or not game-based training developed around user interactive feature produces better results? A study conducted by Sheng et al. [21] evaluated if 15 minutes of an Anti-Phishing game, tutorial, or existing training material would better increase adult user resilience in identifying Phishing websites. In Sheng et al. [21] study the Anti-Phishing game was Anti-Phishing Phil, which was designed to educate users to identify legitimate website from Phishing websites by URLS and where to look for Phishing indicators in web browsers. Anti-Phishing Phil presents users with training messages in between each round of the game which is shown in Figure 7. The tutorial was created based off the Anti-Phishing Phil game, but was a 17-page hand out printed in color. The

existing training material was received off popular internet websites that had tutorials on Phishing. The results Sheng et al. [21] study concluded that participants who played the Anti-Phishing Phil game outscored those who used the tutorial and existing training material in determining what Phishing websites are. The Anti-Phishing Phil game also taught users about techniques to better identify Phishing websites in the future.

Anti-Phishing game-based training is nothing new and there are many different games available on-

line. One in particular is called What.Hack. The game was designed to educate users by progressively increasing the difficulty while having clearly defined objectives and goals, inform users immediately about poor decisions made, imitate actual email Phishing techniques and educate the user on Phishing defenses [22]. The game is played by having users review incoming emails to determine if they are Phishing attempts. The user will then create rules that increasingly get more specific.

A study was conducted by Wen, Lin et al. [22] to determine if What.Hack could improve on the user's ability to correctly identify Phishing emails. Wen et al. [22] compared three Anti-Phishing game-based training games consisting of Phishline, Anti-Phishing Phil, and What.Hack. The study was conducted by having participants take a quantitative pre and post-test as well as answer qualitative questions to compare what they learned and retained during the games.

The study's results demonstrated in Figure 7 show that Anti-Phishing Phil and PhishLine didn't produce any significant improvement in player correctness, where What.Hack improved player correctness by 36.7% as shown in Figure 8. Figure 9 shows engagement ratings of participants where 23% found PhishLine to be engaging or very engaging, 44% for Anti-Phishing Phil, and 95% for What.Hack. Lastly Figure 9 presents the ratings of whether participants would agree or strongly agree to recommend the training to a friend. What.Hack came in first with a 92% recommendation percentage where Anti-Phishing Phil and Phishline were tied with a 33% recommendation rating as shown in Figure 10. It is clear from this study [22] that Anti-Phishing game-based training not only results in outstanding user training, but that all Anti-Phishing games are not created equal.

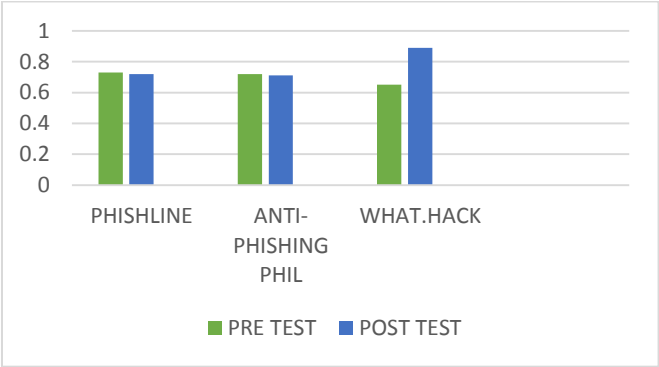


Figure 8. Correctness Percentage (redrawn). [22]

6 Multi-Defense Approach

The literature in both technical and non-technical defenses have guided and pointed in the direction of a multi-defense approach. Vayansky & Kumar [23] conducted a study where they presented a three-step approach to combat Phishing. The three-step approach consisted of, step one prevents Phishing using blacklist and filters, step two detect Phishing using indicators based in browsers and other identification tools such as Anti-Phishing toolbars, step three stakeholder training that consisted of Anti-Phishing game-based training.

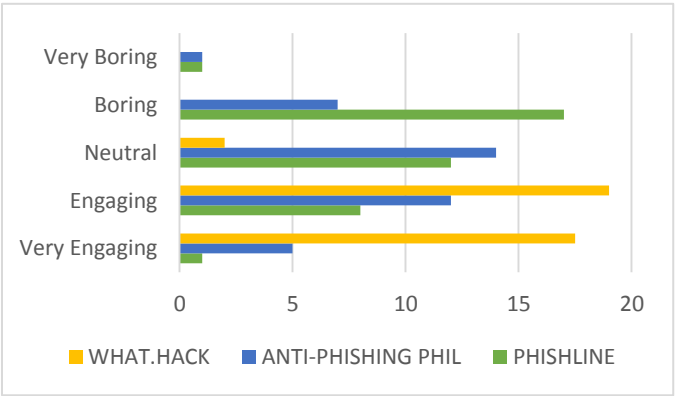


Figure 9. Engagement Ratings (redrawn). [22]

By using this approach step one will filter and limit the amount of Phishing attacks that reach the user via email, therefore decreasing the risk of a user falling victim to a Phishing attack. Step two will alert the user if a potential Phishing email does get through and persuades the user to click the link in the email leading them to a suspicious

website. Lastly, step three will teach the user in an engaging way to practice methods, properly identify, and increase awareness to prevent future attacks [23].

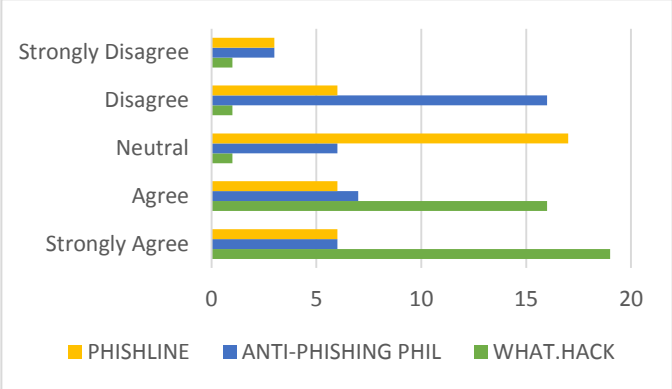


Figure 10. Recommendation Ratings (redrawn). [22]

By attacking Phishing from those three angles it will increase user resilience as a whole. In a study conducted by Chaudhry & Rittenhouse [24], it classified and presented numerous countermeasures to Phishing. The study classified Phishing countermeasures into two categories consisting of technical and employee training. The findings presented that training employees is the greatest countermeasure, but also the weakest link. Although eliminating Phishing attacks completely is difficult due to the ever-changing cyber landscape it can be containable through training. There is not one cure to stop and prevent Phishing attacks, but from having a self-growing and self-maturing training system in place you can help to contain it.

With those findings being presented it further supports Vayansky & Kumar [23] three-pronged approach as two of the three steps directly involve the user identifying the suspicious Phishing attempt and methods. Both types of defenses, technical and non-technical, have a significant role in increasing user resilience. With research pointing in the direction of non-technical being more impactful. Although non-technical has been found to be more impactful for the user, technical defenses should be fully utilized and used to compliment non-technical defenses.

7 Conclusion

Although there are many different options available to combat Phishing attacks, not all are created equal. When the four technical defenses are compared, we can conclude that the Anti-Phishing software, specifically the Anti-Phishing simulator, is the better option compared to the Anti-Phishing toolbars. Anti-Phishing toolbars can help identify Phishing websites, but not every tool bar has the same efficiency. They have poor usability and do not stop the user from accessing the potential Phishing website. The Anti-Phishing simulator has a forever-growing blacklist that increases every time a potential Phishing attempt is identified, either by the user or the software itself. Both of these technical defenses required some type of user training.

The Anti-Phishing Simulator falls short when we compare it to Proofpoint's multilayered machine learning capabilities. Proofpoint showed to be extremely accurate compared to other competitors on the market at detecting and blocking Phishing attacks. Besides being extremely accurate it offered a wide variety of phishing training to its users in case a Phishing email did slip by into the user's inbox. With the ability to tailor specific training for specific user needs Proofpoint easily hedges put the Anti-Phishing simulator.

A downfall to Proofpoint is the time between when a user identifies an email as a Phishing attack and Proofpoint's response time for an analyst to deem it a true phishing attack. To eliminate this downfall, look no farther then Barracuda Sentinel. The A.I. in Barracuda Sentinel grows with every email that comes into the mailbox. It will instantly block and remove the email without any wait time if the email is determined a true Phishing attack. Barracuda Sentinel had a much higher efficiently rating than Proofpoint based on [13],[14]. The only downside to Barracuda Sentinel is that it does not offer the vast amount of training materials and options for its users.

When we compare the Anti-Phishing web-based training with the game-based training it is clear that the game-based training specifically What.Hack can be more effective. Participants strongly recommended What.Hack and it outscored the other popular games in the study. During the web-based training the versions of Agent99 that had more user interactive features produced greater results. Game based training is specifically designed toward user interaction and changes the format of a normal quiz or test in a fun user-friendly game. With such high recommendation ratings from What.Hack it is obvious that it is the better option compared to web-based training models.

Even though What.Hack produced great user feedback and results the inability to be tailored to a specific company or industry puts it at a disadvantage. With Cofense Phishme ability to customize training, report on specific user needs, and machine learning it is a much better option then game-based learning. Cofense Phishme's ability to only be deployed when a user is active in their mailbox, provide real time educational content, and an ever-growing database of Phishing Scenarios makes it one of the best options on the market to combat Phishing.

Although any one of the defenses against Phishing, whether technical or nontechnical is a better option then no defense at all, the findings suggest that both technical and non-technical should be combined to form a multi-defense approach. Based on the results of this comparative study it can be recommended to use A.I. based Phishing defense specifically Barracuda Sentinel and deploy Cofense Phishme to adaptively train users. Barracuda Sentinel is the faster and more accurate option than Proofpoint. Even though Barracuda Sentinel does not have Proofpoint's training options if it is used together with Cofense Phishme it can be believed to produce faster, more evolved, and company specific training materials. It can be concluded that a multiple defense approach towards Phishing produces better results and recommended.

In future studies it can be recommended to compare more technical and non-technical defenses in addition to the those that were compared in this study. Using the most recent references and studies compared will help increase the accuracy of the current state of the technical and non-technical defenses.

REFERENCES

1. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-61r2
2. Souppaya, M., & Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. https://doi.org/10.6028/nist.sp.800-83r1
3. Government Accountability Office Report. (2013). Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented. Retrieved from http://www.gao.gov/assets/660/652170.pdf
4. Financial Losses. (n.d.). Infosec Resources. Retrieved July 27, 2020, from https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/financial-losses/#gref
5. Internet Crime Complaint Center (IC3) (2018) | Business E-mail Compromise The 12 Billion Dollar Scam. (n.d.). Www.Ic3.Gov. https://www.ic3.gov/media/2018/180712.aspx
6. Gowtham, R., & Krishnamurthi, I. (2014). A comprehensive and efficacious architecture for detecting phishing webpages. Computers & Security, 40, 23-37. doi:10.1016/j.cose.2013.10.004
7. Proofpoint Email Protection Detect and Block Both Known and Unknown Email Threats. (n.d.). Retrieved August 16, 2020, from https://www.proofpoint.com/sites/default/files/2020-04/pfpt-us-ds-email-protection.pdf
8. Proofpoint Security Awareness Training. (n.d.). Retrieved August 16, 2020, from https://www.proofpoint.com/sites/default/files/2020-06/pfpt-us-ds-security-awareness-training.pdf
9. Closed-Loop Email Analysis and Response Identify and Reduce Phishing Risk PRODUCTS. (n.d.). Retrieved August 16, 2020, from https://www.proofpoint.com/sites/default/files/pfpt-us-sb-closed-loop-email-analysis-and-response.pdf
10. EMAIL PROTECTION Barracuda Networks • DATASHEET • Barracuda Sentinel. (n.d.). Retrieved August 17, 2020, from https://assets.barracuda.com/assets/docs/dms/Barracuda_Sentinel_DS_US.pdf
11. Cranor, L., Egelman, S., Hong, J., Zhang, Y. (2007). Phinding Phish: An Evaluation of Anti-Phishing Toolbars..
12. 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). Association for Computing Machinery, New York, NY, USA, 581–590. DOI:https://doi.org/10.1145/1124772.1124861
13. Rahmad, F., Suryanto, Y., & Ramli, K. (2020). Performance Comparison of Anti-Spam Technology Using Confusion Matrix Classification. IOP Conference Series: Materials Science and Engineering, 879, 012076. https://doi.org/10.1088/1757-899x/879/1/012076
14. Cidon, A., Korshun, N., Schweighauser, M., Tsitkin, A., Gavish, L., & Bleier, I. (2019). High Precision Detection of Business Email Compromise High Precision Detection of Business Email Compromise. https://www.usenix.org/system/files/sec19-cidon.pdf
15. Baykara, M., Gurel, Z. (2018). Detection of phishing attacks. 1-5. 10.1109/ISDFS.2018.8355389.
16. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. 2010. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). Association for Computing Machinery, New York, NY, USA, 373–382. DOI:https://doi.org/10.1145/1753326.1753383
17. Phishing Awareness Training | Phishing Email Simulation. (2016, June 29). Cofense. https://cofense.com/product-services/phishme/
18. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L.F., Hong, J., Blair,M.A., and Pham, T. 2009. School of phish: a real-world evaluation of anti-phishing training. In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09). Association for Computing Machinery, New York, NY, USA, Article 3, 1–12. DOI:https://doi.org/10.1145/1572532.1572536
19. George, J., Biros, D., Burgoon, J., Jr, J., Crews, J., Cao, J., Marett, K., Adkins, M., Kruse, J., Lin, M. (2008). The Role of E-Training in Protecting Information Assets Against Deception Attacks.. MIS Quarterly Executive. 7.
20. Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E., Landman, A., Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system, Journal of the American Medical Informatics Association, Volume 26, Issue 6, June 2019, Pages 547–552, https://doi.org/10.1093/jamia/ocz005

21. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., and Nunge, E. 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). Association for Computing Machinery, New York, NY, USA, 88–99. DOI:https://doi.org/10.1145/1280680.1280692
22. Wen, Z.A., Lin, Z., Chen, R., and Andersen, E., 2019. What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 108, 1–12. DOI: https://doi.org/10.1145/3290605.3300338
23. Vayansky, I., Kumar, S., Phishing – challenges and solutions, Computer Fraud & Security, Volume 2018, Issue 1, 2018, Pages 15-20, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(18)30007-1. (http://www.sciencedirect.com/science/article/pii/S1361372318300071)
24. Chaudhry, J.A., Rittenhouse, R.G.,"Phishing: Classification and Countermeasures," 2015 7th International Conference on Multimedia, Computer Graphics and Broadcasting (MulGraB), Jeju, 2015, pp. 28-31, doi: 10.1109/MulGraB.2015.17