# A Review of the Current Phishing Problems in a Real-World Environment and Innovative Solutions Through Developing Algorithms to Incorporate the Human Behavioral Factors into Dynamic or Adaptive Training Tool

John Bako
University of Colorado, Colorado Springs
Colorado Springs, CO
jbako@uccs.edu

***Abstract*— This paper deals with the theme of a phishing scam and human psychology, and techniques used to promote online fraud on the internet and how users usually behave under certain circumstances. Likewise, proposals are presented to combat the attacks.**

**Social engineering is still one of the highest-ranking forms of attack in the computer, information and cyber security realm. This involves phishing, spear phishing, baiting, tailgating among others. Although multiple defense guidance and techniques have been proposed and implemented, it is usually easier said than done when for instance, the first human instinct upon receiving an email is to open and read it or better yet, employees accessing their physical work spaces upon badging in at the local HID badge reader and not thinking of looking back to check the next person following him or her for valid identification or ensuring that he or she also badges in successfully to grant access to the facility. The issue here can be more psychological than logical, physical, or a combination of both.**

**This paper reviews the approach most companies use to educate their employees and delve into recommendations to better prepare the so-called weakest link of information security to be aware of cyber criminals. The research aimed to gather data from various parties of the world, to try to understand whether a specific range of age would behave in a particular manner and to try to eliminate a probable bias using only North American individuals when responding to our questionnaire. The collected data shows that most people that did our survey understand to a certain degree that they need to be aware of phishing (or even spear phishing) not only at work but home and educating family and friends about this threat.**

**Moreover, it shows that a right amount of people still put the responsibility of securing the company's network entirely on the Information Technology or Information Security department, whereas the researchers noted a tendency nowadays where companies try to use other methods to educate their employees. The landscape for a bad actor to act is enormous. Users need to be more alert, and companies need to delve into other forms of awareness to protect their assets. Our intention with this paper is to tackle this issue under different light and recommending, in our view, what will need to be done for now.**

**Finally, we are going to look at how we can defend social engineering attacks with the focus on how to develop algorithms to incorporate the human behavioral factors into dynamic training tools.**

**Keywords: Review, phishing, email, spear, attack, social, engineering, psychology, cognitive, cyber, security, survey, data, continent, intentional, criminal.**

## I. Introduction

Phishing is a technique to obtain sensitive information such as user-name and password, bank account information and social account information by convincing the users to visit a fraudulent website to disclose their confidential information. These (spear) phishing attacks get steadily more sophisticated as cyber criminals use social engineering tricks that combine psychological and technical deceptions to make malicious emails as trustworthy as possible. Phishing attacks have brought considerable consequences to users and organizations. To fight against Phishing attacks, organizations rely on various defense layers and the user behavior (Social Engineering).

Phishing attacks continue to be a challenging security problem for all companies. The low cost to execute and high rate of return due to natural human behaviors mean that even with the constant incremental improvements in anti-phishing technologies, a fundamental change in approach is needed. Our focus is to evaluate the current problems in a real-world environment and come up with innovative solutions that blend new technologies and a deep understanding of human psychology in order change the paradigm and reduce risk due to phishing.

The methods used in this research are very security focused, which include research scope and time-line, phishing problems on different platforms (e.g., mobile, tablet), survey, data analysis and software utilization, design/coding methods, mathematics and statistical analysis.

To tackle the problems in this research, some significant questions have been asked; why do human behavior continue to be a substantial flaw to anti-phishing technologies? What could be the best fundamental change approach? What are the main current problems in a real-world environment that influence human behavior and affect the current plan? How can we blend new technologies and use a deep understanding of human psychology to change the paradigm and reduce risk due to phishing? Several assumptions that were made are that companies have policies, standards, procedures, processes, tools, and personnel to handle phishing incidences, including giving a periodic security awareness training.

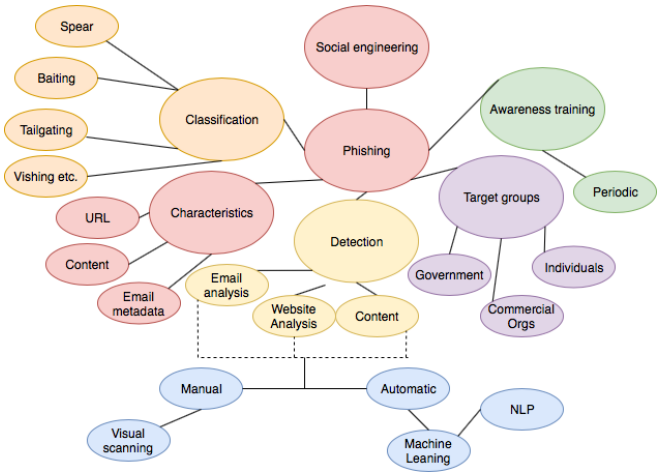


Fig. 1. Social engineering: Phishing topic map

## II. Related Work

### A. Understanding of Human Psychology

There are policies, standards, and procedures in every organization that employees are expected to follow to prevent clicking on phishing attack embedded links in emails. Even individuals in the comfort of their homes who do not have any formal documentation to govern or guide them in respect of this issue, still get enticed to click on embedded links in their email. The recommended defense against phishing attacks is to educate a user how not to fall for them. Such campaigns are not the most effective solutions, and software systems have been created to identify phishing email. By large, these systems are crisp [1]. This paper re-compares the fuzziness surrounding the abilities of human subjects and of a software system to differentiate a phishing email from a legitimate one. Without using experiments, the paper has the premise that people do it intuitively while computers follow algorithms. The authors suggest that if a human does it consistently, then there is an implicit pattern and an algorithm underlying their decisions with at least a substantial probability. There is the belief that if a computer algorithm is based on machine learning, then it is Bayesian, which clears the fuzziness and proves that the difference between humans and computers may be less than initially thought.

Humans have always overseen blacklisting and whitelisting in computing, and automation technologies have aided this effort. Other than that, IT departments of various institutions try to train users on phishing through educating them with tips in periodic memos such as mismatched URLs, messed-up domain names, impersonal/general forms of address, requests for private information, and bad English/language [1]. In response to these memos, attackers have come up with very polished ways to create phishing emails to avoid and bypass these giveaways.

There is also human manipulation where this literature ties phishing emails to usual tricks of including plausible but false reasoning, scare tactics and threats, all trying to get the recipient to act rashly in the attacker's interest. Based on a report released in 2014 by the Federal Bureau of Investigations Internet Crime Complaint Center [6], the total number of internet-related complaints reported was 269,422, with 123, 684 of those cases said losses of $800, 492, 073 [6][3]. Proofpoint [7] reported that 76% of Information Technology (IT) security personnel and operations staff had been victims of malware, with 95% of those threats derived from phishing emails. The critical result of this is that even IT professionals are vulnerable to phishing attacks whether by accident or intent. From a percentage perspective, out of every 100 malicious emails received by a person, about 60% of the time, users click on the links [2].

The common conclusion here is that it doesn't matter how much you know about the topic of phishing; whether being an IT professional or not, there is still a high probability that one would click on six malicious links out of every ten received. Insufficient knowledge, visual tricks, and inadequate attention are three cognitive dimensions that have been identified by Dhamija, Tygar, and Hearst [8], which are being used by attackers to execute successful phishing attacks [3]. There is also the feature-integration theory of attention research by Treisman and Gelade, which is the first cognitive science literature study that talks about the five primary components of this theory. These are visual search, texture segregation, illusory conjunctions, identity and location, and interference from unattended stimuli [9].

- Visual Search – this is described as a perceptual task that demands attention, commonly requires active scanning for a feature or target surrounded by other features known as distractors.
- Texture Segregation – this is to divide visual stimuli by distinguishing between spatial discontinuities among groups.
- Illusory Conjunctions - this is the impact of incorrectly combining features when multiple unattended objects are presented.
- Identity and Location – this is the understanding that identifying an object and knowing its position are two different operators, and that location must precede identification.
- Interference from Unattended Stimuli – this is when a stimulus that is not being attended to only registers at the feature level. The degree of distraction that it has on attended tasks depends on the features it is composed of and should not be affected by any conjunctions from where the features occurred.

### B. Conclusions are drawn from these five components

Two hypotheses were drawn from these five components, which are:

- The detection of additional text will be the easiest discrepancy to identify because it can be done via a parallel search process.
- The detection of crafted text, manipulation combinations, and obfuscated manipulations will be more challenging to identify because these require a serial search.

Conclusions from the five components suggest that some textual manipulations and complex visual tricks are harder to identify than others [3].

Another research by Simons and Chabris from a cognitive science standpoint was about sustained inattentional blindness for dynamic events [10]. Individuals can fail to pay attention to unexpected stimuli even though they appear viewable and in plain text. This is called Inat-intentional blindness. The results of the study showed that also when individuals are engaged in a primary task of monitoring, people still fail to catch or recognize unexpected events even when they appear so obvious. The most critical factor in this study shows that also when objects pass through an area of attentional focus, they still have a low probability of getting detected.

Both results from Treisman and Gelade [9], and Simons and Chabris [10] support our study because Treisman and Gelade suggest that manipulating texts by phishing attackers make it harder to identify their attacks, and Simons and Chabris indicate that even when you are actively monitoring events, it is tough to catch all unexpected events even when they seem so obvious.

Results from the studies conducted by Bethel, Jarosz, and Berman [3], proved that users have difficulties in detecting legitimate URLs from illegitimate ones. This is backed by the premise that when user's primary task is to check emails, then less attention is given to fraudulent or phishing emails, hence, making it very hard to be in that mindset to detect these kinds of emails. Although support to these hypotheses did not conclude that fancy visual tricks are most challenging to identify as opposed to simple text manipulations, this study still proved with its results, that additional text URLs posed the most difficulty in detecting, followed by obfuscation, crafted text, and lastly, manipulation.

### *C. Human-Computer Interaction and Social Engineering*

Anti-phishing solutions address both the technological and human aspects of the phishing attack chain. The focus of technical solutions is on preventing phishing emails from being delivered, using cryptography to preserve email authenticity, honeypots to spot spammer actions, and mitigation strategies to neuter attachments. Phishing strategies often subvert the human factor by exploiting unsuspecting users via visual deception, and by taking advantage of a bounded attention span [13].

Human-Computer Interaction (HCI) solutions focus on bridging the gap between the machine and the user. This should make detection, identification, and reaction to malicious email easier, helping to reduce the number of (spear) phishing victims. Rising interconnectedness leads to computer users having to make more security decisions. Thus, the importance of User Interfaces (UIs) of security software has grown. Solutions focused on user warnings, training, and learning about the opening of email is being developed.

In another study, there was a survey on understanding how to prevent end-users from falling for email (spear) phishing attacks. Based on the research, authors designed and proposed a novice method that combines interaction methods of reporting, blocking, warning, and embedded education to harness the intelligence of expert and novice users in a corporate environment in detecting email (spear) phishing attacks.

- User Reporting - Such warnings are usually ignored by users because they are seen as a hassle, aren't understood, take away control, and have false positives.
- Blocking - When a recipient opens a suspicious email, the User Interface (UI) shows a warning message and prevents the functionalities of the email client, i.e., the active warning enabled. Only after actively assessing the email and by clicking either 'Yes, this is a phishing email' or 'No, I trust this email' i.e., the component method will then unblock the user, and the user can proceed.
- Warning - The warning must interrupt users' primary task, and the user has to actively react to the alert before proceeding to prevent users to ignore warnings. The sign should be distinctive from other less severe warnings.
- Embedded Education/Training - Users can be made aware of phishing through anti-phishing education and training. Training must be embedded within an email client to assist users in their regular work processes where they are dealing with real threats; the training messages have to be simple, short and of a minimal duration (30-120 seconds) to maintain the user's attention. The training has to be disruptive and repeated several times to embed and engrave the procedure in user's minds.

This study provided with insights to fine-tune the webmail UI in future studies.

In another research, Social Engineering as a type of phishing where a potential victim is sent a message that impersonates a legitimate source or organization. The study presents the results of two large-scale real-life phishing attacks conducted on more than 10,000 community members of a university that includes students, alumni, faculty, and staff. Previous work suggests that users' demographics are useful indicators in identifying the most vulnerable users to phishing attacks.

Results to this illustrate that user demographics alone cannot predict user's susceptibility to phishing attacks. From this research, it was found that warning users about phishing risks alone are not enough to prevent more users from responding to the phishing attack. Even though subjects were warned not to return to phishing emails, many disregarded the warning.

Looking at the different researches carried out, it can be concluded that human behavior plays a significant role in phishing and spear phishing attacks. Education, training, awareness is critical in helping the user protect themselves, as well as the organization, they may be working. Coming up with more visible features to the system to increase user awareness whenever there are a suspicious email and training to help them know how to deal with the situation each time they come across suspicious is significant.

### D. Human-Computer Interaction and Machine Learning

The gap in these studies shows that aiding these cognitive behaviors with a user interface that not only warn and train users to report phishing emails but instead, enforces strict examination of such emails and forces users to go through IT Security before opening to read them. This will serve as a reminder and assist for when it is harder to identify manipulated texts and when it is hard to catch unexpected events even when one is actively monitoring tasks and activities. Moreover, this will apply to everybody across an organization regardless of position since there would be no exceptions. Machine learning techniques will aid the activation of a UI to show which emails are suspicious and would need to go through that scrutiny.

## III. Methods

This section presents an overview of the process used to collect data for this research. It provides the ages, professions, geolocations (continents) of each participant and their overall knowledge on the topic of phishing as well as how they go about their daily lives tackling phishing attacks. We then go further to analyze the similarities in the responses with regards to gender, profession, geolocation, level of education, and the time of the day when participants are more active and productive. The participants were informed about the purpose of the survey and how the responses would be used. A sample of the questionnaire is displayed in the data gathering section.

### A. Participants

The participants were spread over six out of the seven continents in the world, which comprised of people from Africa, Asia, Australia, Europe, North America, and South America. Participants were chosen from all over the world to reduce bias and from limiting the research to just a geographic area. There was a total of 60 participants (N = 60) with ages ranging from 16 to 50 years and above. With the age groups, half; which is 50%, were between the ages of 20 – 29. This was not surprising as this is the most active age group who hold an entry to mid-level cyber/information security roles. There were 53.3% of males and 45% females. This shows that there is still a significant number of men in the IT field than women, but the difference is not by a considerable percentage. A 1.7% of the participants preferred not to disclose their gender. The second largest was the ages from 30 – 39, which constituted to 35% of total responses. Participants between the ages of 40 – 49 made up 8.3%, and the ages from 16 – 19 made up only 1.7%. The last 5% are 50 years and above.

Participants hold several positions in accounting, advertising, brand strategy, digital marketing, hardware engineering, homemaking, IT sales management, infrastructure development, business analysis, information security analysis and consulting, project management, quality and reliability engineering, healthcare (nursing and occupational therapy), private ministry administration, real estate, software engineering, UX designing, and students. This is to show that there is a wide variety of professionals involved and not necessarily participants from just the IT industry.

There was 53.3% of participants from North America, 18.3% from Asia, 15% from South America, 6.7% from Africa, 5% from Europe, and 1.7% from Australia. The North America numbers were not surprising as it was the origin of the survey, but the rest of the other continents do represent the rest of the world. Again, this reduces the focus on just North America and takes away the bias of looking only one continent for responses.

Regarding education level, 50% of the participants held bachelor's degrees, 41.7% held master's degrees, 6.7% held associates, and 1.7% held high school diplomas. There were none with PhDs. This still makes a right mix of people with all kinds of education background.

This method of data gathering made use of Google survey, which breaks down responses into regular visualized reports based on percentages in various forms such as pie charts, histograms, line graphs. This makes it easy for analysis to be made and some conclusions to be drawn as the Google software automatically visually represents the data for more straightforward interpretation. Every data collected for research purposes must be converted into visual formats to enhance the analysis process, and this software is free and does an excellent job at that. Names of participants were not collected to ensure anonymity and the protection of participant's privacy. Mode of sharing this survey was through social media and friends of friends. Overall, there is enough randomness as participants were not handpicked.

### B. Data gathering techniques – Survey

#### 1) Used Google Forms:

- Are you Male or Female?
- What is your age?
- What is your profession?
- What is your highest level of education?
- What do you do when receiving an e-mail from an unknown source but having content that you like?
  - Open and read the e-mail
  - Pay attention to if it is not phishing but open it anyway
  - Delete the e-mail
  - Send it over to IT security to be analyzed before opening it
- Are you aware of phishing and the impact it could have on you or your company?
- Do you care about getting attacked by phishing emails? Why (explain)?
- Have you fallen victim to phishing attacks in the past? How did it happen? (Explain)?
- Do you have a way to distinguish between phishing and non-phishing emails? If yes, how?
- Do you think about phishing each time you attempt to open and read an email?
- Are you selective about the type of links you click in your email?

- Do users click on phishing emails because the subject talks about a topic of interest, e.g., finance, sports, coupons, free stuff, etc.?
- How often do you get security awareness training?
- Are you willing to lecture your family and closest friends about the dangers that phishing in general encompasses?
- Do you often click on e-mails that coincide with major world events? (Such as Olympics, World Cup, etc.)
- Do you pay attention before clicking on a shortened link?
- Do you use the companies' computer to charge your phone?
- When clicking on a link, do you trust the platform? (If yes, which platform? Such as Facebook, Twitter, etc.)
- Do you trust the person sending an e-mail or sharing a link with you?
- What do you do when spotting a phishing e-mail?
  - Delete the e-mail
  - Open just to read it knowing your company has the tools that can protect the network
  - Open and send it over to IT security to be analyzed
  - Send it over to IT security to be analyzed before opening it

## IV. Results, Findings, Interpretation, and Discussion

Analysis of the results of the survey has a lot of interpretations. Regardless of where a participant is located, 48.3% stated that they always delete any email they receive but do not know the source, even if the subject talks about something they like.

This is the usual terms should signify much awareness in the world right now because even the second highest number of 30% do claim that they pay attention and carefully verify that the email is not a phishing attack but do open to read it anyway but it leaves only a difference of 18.3% of people who delete these emails with the slightest suspicion, so, users are still not using due diligence and due care in handling phishing email matters.

On top of this, 6.6% open and read the email regardless of what they think. The situation only gets worse as only 8.3% send it over to IT security to be analyzed. This also means that even a higher percentage of IT professionals still easily fall victims to phishing email attacks.

With 81.7% saying yes to the fact that they are aware of phishing emails and its impact to them and or their organization's assets, one would still wonder why humans would not follow the right procedures in handling emails daily. 13.3% are unsure of the impact of phishing on them or their company, and 5% do not know anything about what phishing can do at all. This means that although organizations may be training their employees and students, only a few cares.

Why do most people don't care then if they know still aware of the risk? Interestingly, about 86.67% answered that they care about getting attacked by phishing emails and 13.33% don't care about it. About 80% also said that they don't believe that they have fallen victims to phishing before. 5% don't know, and the last 15% confirmed that they had dropped victims. The questions are, have they been victims before without having any idea about it or how are they a 100% sure that they haven't been victims now or in the past? 25% think they can identify a phishing email.

The most important question for this research; "Do you think about phishing each time you attempt to open and read an email?", Got a winning percentage of responses; 35% said yes, 33.3% said maybe, and 31.7% said no. 88.3% of these same people say that they are selective about the type of links they click on in their emails and 85% do the same with shortened links. Only 30% would click on a link because it talks about an area of interest such as sports, free coupons, finance. 40% reported that they do not receive any security awareness training and even the other 60% that do, mostly receive it annually. The good part is that 71.7% participants said they are ready to educate family and friends on phishing. Only 55% are not using their company's devices to charge their smart devices. A good 45% are doing otherwise. 76.7% take time to verify the source of an email and 66.7% delete the emails right away when they cannot verify the source. Out of that, only 21.7% would send it to IT security to be analyzed before opening. When participants were asked about what time they are most awake and attentive to their work, only 15% said "all the time."

In a similar effort in the paper "A comparative analysis and awareness survey of phishing detection tools", an awareness survey was conducted among fifty M.tech Computer Science Technology, and Cyber Security pursuing students at Central University of Punjab. The survey revealed that approximately 61 percent respondents were completely unaware about phishing detection tools [17].

In another survey, phishing is described as typically carried out by Email spoofing or instant messaging and targets the user who has no knowledge about social engineering attacks, and internet security, like persons who do not take care of privacy of their accounts details such as Facebook, Gmail, credit banks accounts and other financial accounts [18]. But we think this is not entirely accurate after going through several surveys and carrying out one by ourselves to prove this fact that phishing doesn't always and only target persons who do not take care of privacy of their accounts details as mentioned above in this paragraph. It has been proven in several surveys and ours that social engineering, phishing specifically, can target even Information Technology professionals, including even those in security.

## V. Recommendations and Applications

Our results indicate that most people do not think about phishing whenever they are opening to read an email. This is like the findings in previous studies that states that computer users either do not care about or are still likely to miss visible indicators of phishing emails that they may be opening to read even if their primary task is monitoring or "checking

emails." This is what is referred to as the inattentional blindness. There is usually no time allocated for monitoring or "checking emails" as a primary task, so individuals get on their computer and dive straight into the motives that took them on the computer. This also means that it doesn't matter what age, profession, gender, or even geolocation of a person, this premise applies to all. Considering how the time differs for everybody regarding when he or she is mostly awake during the day or night, it means that people are more prone to fall victims to phishing attacks during certainties of the day.

After reviewing the results, we recommend that a more advanced method of human-computer interaction should be used to prompt users about a suspicious email. Although participants agreed that human plus computer effort is the best to detect phishing, they still do not think about phishing whenever they are checking an email unless this problem of cognitive inattentional blindness is solved. We believe that making the process of checking emails with suspicious attachments or embedded links a little-sophisticated user interface process will be initiated for the user to follow to answer a set of questions before he or she will be able to download an attachment or click to open a link.

### *A. Process*

- Have you verified the source?
- If there's an attachment, are you expecting such document, or have you call to confirm with the sender if he or she truly sent that?
- If you are having second thoughts, use the forward button on the interface to send it over to IT Security to scan email for you and only open upon IT Security has confirmed.

This is like the recommendation drawn by the survey on UI [13], which combines warning, user reporting, awareness training/education, and "Blocking - When a recipient opens a suspicious email, the User Interface (UI) shows a warning message and blocks the functionalities of the email client, i.e., the active warning enabled. Only after actively assessing the email and by clicking either 'Yes, this is a phishing email' or 'No, I trust this email' i.e., the component method will then unblock the user, and the user can proceed". Except that our recommendation would be a little more enforced as it would force users to involve IT Security in almost every suspicious email activity before the user can either read or proceed to open any attachments or embedded links. Our interactive UI method will be a maximum of three short questions as shown above, which will take away user frustration and annoyance at having to go through a full education and answering a lot of questions each time an email with an embedded link or attachment is received.

To facilitate this process even further, we recommend using a machine learning algorithm to develop a software which will be helping humans in making such critical decisions. Not every email containing an attachment or embedded link will go through such a process. These machine learning algorithms will gather data on user behavior and the probability that an email should be forwarded to IT Security for examination. A combination of these heuristics will make the system's decision to pull up a supporting UI and force the user to send the email to IT Security for investigation a definite and justifiable one. This will increase the urgency on both the user and IT Security parts to deal with the email immediately so that it doesn't slow down business operations.

For instance, with such an interface that puts such restriction on any suspicious email with an attachment or embedded link, users will only be able to access emails if and only if IT Security have screened it properly. Not, a question of urgency may be asked here, but with regards to security matters, we believe that no potential malicious email is too urgent to be read.

The phishing problem has been an everlasting one that most believe cannot be solved with technology since it has a single point of failure, which is typically human error and mostly psychological. "The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks"[16]. If we think about the ways attackers go about setting up baits for human victims to eat and get compromised, we can see a pattern and some key items that we need to be looking for to start solving the phishing problem technically (logically).

Previous approaches to solve this problem used machine learning algorithms and features to perform classification of phishing emails and non-phishing emails. Some of these features are HTML formatted emails (hyperlinks are active and clickable only in formatted emails), IP-based URL, age of domain name, number of domains, number of sub-domains, presence of JavaScript, presence of Form tag, number of redirection links, URL-based image source, mismatching domains (From & Body), and keywords such as update, confirm, user, customer, client, login, username, password, social security number etc. [14][15].

In our proposal, we are going to use a solution that also uses a machine learning approach with features for classification purposes. The main difference between our solution and most other solutions is the fact that our solution uses a cloud-native Security Information and Event Management (SIEM); Azure Sentinel in conjunction with a virtual machine sandbox to perform classification based on real-time analysis of emails containing embedded links. Most importantly, we will use results from our analysis for incorporation into dynamic training for human beings.

### *B. Concept Explanation*

A user has a workstation and the workstation has an option to either host a local virtual machine on the local machine or in the cloud. Either option will work fine. Users who don't have confidence in hosting virtual machine on the local machine can always opt for the cloud virtual machine option. The virtual machine is our sandbox environment.

The virtual machine is set to unify with the local machine. In other words, the local machine can directly execute or

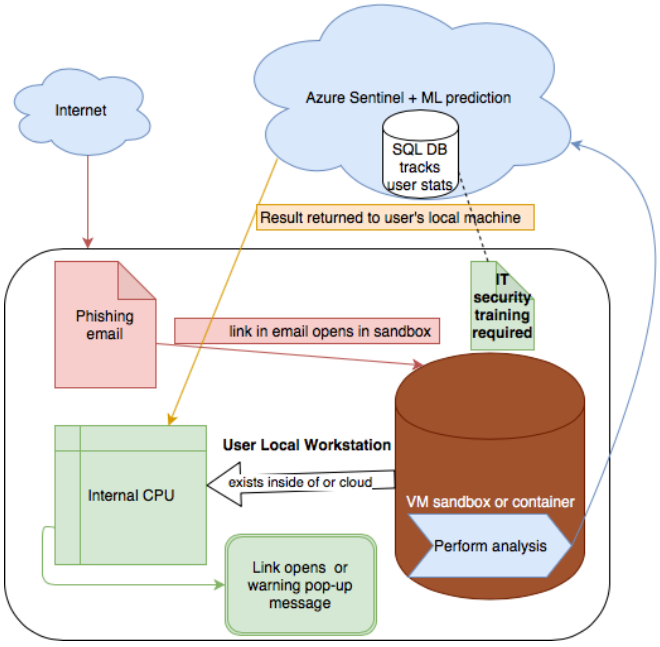


Fig. 2. Concept diagram for dynamic or adaptive training tooling for phishing. Options available for on-premise or cloud virtual machines and storage

perform specific functions on the virtual machine. In our instance, the execution of web browsers to open websites or links is extremely vital.

A user receives an email in his/her inbox. The moment an embedded link is detected in the email, due to psychological factors, there is always a high probability that a user will click on the link intentionally or unintentionally so if the user clicks on the link, it automatically executes but in this case, through the virtual machine.

A Wireshark pcap file is created and the html source code is opened and analyzed by our machine learning algorithm for classification purposes to predict if it is phishing or not. The machine learning algorithm uses real-time Azure Sentinel (SIEM) log data such as activity and history records of the domain name or source IP in conjunction with the well known phishing website indicators as features for testing and training of our model. The result is sent back to the local machine and a message pops up on the local machine to alert the user of a suspicious activity if the machine learning model's prediction is true. The user is able to see the link open in his/her local default browser.

We haven't yet found a favorable machine learning algorithm to solve this problem. In a research paper, a survey of research works conducted on classification techniques by various researchers for phishing URL detection showed that the experiments were performed using 4,500 URLs and several classification algorithms. The observed results showed that tree-based classifiers provide maximum accuracy [19]. We are yet to test this ourselves going forward in any future work in this survey.

Our intent is to have a couple seconds to an almost instantaneous decision from our model from a user clicking on the link to opening of the link on the virtual machine for analysis to making a decision and either opening the link for the user on the host machine or showing a pop-up message to the user as "Malicious/suspicious link activity!!! Your email has been forwarded to IT security for the record". A monthly analysis or report is sent for users to review, with main content highlighting users risk and or exposure to phishing.

Scoring is performed based on users statistics on clicking on email embedded links plus how many red or yellow or green indicating malicious links, suspicious links, and benign links. This monthly statistical report will initiate mandatory security training as part of user or employee periodic or as needed security training and refresher courses.

The implementation of this solution will be on mainly Windows and or Linux operating systems (OS) and will be written in Python using Azure Machine Learning platform.

## VI. Conclusion

The purpose of this research was to assess social engineering and find out ways that we can use in developing algorithms to incorporate the human behavioral factors into dynamic training tool. Regardless of the outcome of the experiments that are going to be carried out, we will still learn some useful information, which could lead us to continue to find better ways to safeguard ourselves and organizations from falling victims to phishing emails by using tools that we already have at our disposal and also develop algorithms using machine learning to incorporate the human behavioral/psychological factors into dynamic training tools.

## VII. Future Work

We intend to expand on this research to put this proposal into full implementation and use to study its effectiveness. An implementation section will be added to this paper with the steps and action taken to ensure that it works and described in full detail. This will ensure that the audience of this paper be able to try to implement this on their own if they wish to, without necessarily having to use our final solution and product from this research. Additional sources will be examined and cited to support this research.

We will also work on providing a proposal for a solution that will best address the impersonation (physical and non-techincal) aspect of social engineering and then follow up with an implementation of this solution to bring to full testing and use.

While collecting phishing data through the survey, at least two people contacted us out curiosity when we were sharing the survey link with them via text messaging, wondering if the source phone had not been hacked. So, in future research, we will be looking into phishing via other than common mediums such as text messaging. This will give the opportunity to investigate how some people are very conscious even about links they receive through texts messages on mobile platforms. It may or not matter much to some people whether

they are using their work computers or home computers. They still will look out for phishing attacks regardless. We will also explore man-in-the-middle phishing email attacks to find out if it will be possible to intercept and compromise a good email into a malicious one from the moment the original sender clicks, or taps "send" till when it delivers into the original receiver's inbox. From our survey, it is proven that users do not have the discipline to use UI warnings, reports, or awareness training effectively. But when blocking or forcing users to take action through UI before they can move on to the next work, things are taken quite seriously.

With a combination of the user's own efforts and technology (machine learning), we believe that there will be some effectiveness, which will not get on user's nerves but will make them see the importance of clicking and opening email attachments and embedded links equally crucial as ensuring that you have good locks in place whenever you leave your house or apartment.

## VIII. References


[1] Lauren M. Stuart, Gilchan Park, Julia M. Talor, Victor Raskin, "On identifying phishing emails: Uncertainty in the machine and human judgment," IEEE, pp. 1-8, 2014.

[2] Taimur Bakhshi, "Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors," IEEE, ICET, pp. 1-6, 2017.

[3] Ed Pearson, Cindy L. Bethel, Andrew F. Jarosz, Mitchell E. Berman, "To click or not to click is the question": Fraudulent URL identification accuracy in a community sample, IEEE, pp. 659-664, 2017.

[4] Ana Ferreira and Gabriele Lenzini, "An analysis of social engineering principles in effective phishing," IEEE, pp. 9-16, 2015.

[5] Paul A. Watters, "Why do users trust the wrong messages? A behavioral model of phishing" IEEE, pp. 1-7, 2009.

[6] F. B. O.I. Internet, "Internet Crime Complaint Center (IC3) — Annual Reports", Crime Complaint Center (IC3), [online] Available: https://www.ic3.gov/media/annualreports.aspx.

[7] "The Human Factor: How attacks exploit people as the weakest link in security," Proofpoint, [online] Available: https://whitepapers.theregister.co.uk/paper/view/3768/how-attacks-exploit-people-as-the-weakest-link-in-security.

[8] R. Dhamija, J. D. Tygar, M. Hearst, "Why Phishing Works," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Ser. CHI '06, pp. 581-590, 2006.

[9] A. M. Treisman, G. Gelade, "A feature-integration theory of attention," Cognitive Psychology, vol. 12, no. 1, pp. 97-136, Jan. 1980.

[10] D. J. Simons, C. F. Chabris, "Gorillas in our midst: sustained inattentional blindness for dynamic events," Perception, vol. 28, no. 9, pp. 1059-1074, 1999.

[11] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni and F. Jansen, "A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence," 2015 European Intelligence and Security Informatics Conference, Manchester, pp. 113-120, 2015.

[12] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani and A. Darwish, "Phishing in a university community: Two large-scale phishing experiments," 2012 International Conference on Innovations in Information Technology (IIT), Abu Dhabi, pp. 249-254, 2012.

[13] E. D. Frauenstein and R. von Solms, "Combatting phishing: A holistic human approach," 2014 Information Security for South Africa, Johannesburg, pp. 1-10.bv, 2014.

[14] Basnet, Ram Mukkamala, Srinivas Sung, Andrew. Detection of Phishing Attacks: A Machine Learning Approach. 10.1007/978-3-540-77465-5_19, 2008.

[15] Mohammad, Rami. Phishing Websites Features. 10.13140/RG.2.1.2595.6000, 2015.

[16] Mahmoud Khonji, Khalifa University, Youssef Iraqi, Andrew Jones. "Phishing Detection: A Literature Survey". IEEE Communications Surveys Tutorials, Volume: 15 , Issue: 4 , Fourth Quarter 2013.

[17] Himani Sharma, Er. Meenakshi, Sandeep Kaur Bhatia. "A comparative analysis and awareness survey of phishing detection tools", 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), 2017.

[18] Surbhi Gupta, Uttar Pradesh, Abhishek Singhal, Akanksha Kapoor. "A literature survey on social engineering attacks: Phishing attack", International Conference on Computing, Communication and Automation (ICCCA), 2016.

[19] Pradeepthi K V, Kannan A. "Performance study of classification techniques for phishing URL detection", Sixth International Conference on Advanced Computing (ICoAC), 2014.