ISSN: 2996-3397

Research Article

International Journal of Criminology and Criminal Law

A Preventive and Detective Model for Phishing Attack in Small and Medium Size Businesses

Muyisa Patayo Clemence*

Mit – Network security bugema university/ Uganda

*Corresponding Author
Muyisa Patayo Clemence, Mit – Network security bugema university/ Uganda.

Submitted: 2025, Oct 16; **Accepted:** 2025, Nov 27; **Published:** 2025, Dec 03

Citation: Clemence, M. P. (2025). A Preventive and Detective Model for Phishing Attack in Small and Medium Size Businesses, *Int J Criminol Criminal Law, 3*(4), 01-08.

Abstract

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in an digital communication. Phishers take advantage of the trusting nature of humans who are considered to be the weakest point of the security triangle. Phishing attacks lead to loss of money, reputation, job etc. A lot of research has been made on this regard and many solutions have been made available but hackers still find and develop new method to trick the security measures in place. The study in this paper proposes a process model that we believe can help to reduce the impact of phishing attacks to some extend; it is composed of Business Security Objectives, Preventive Measures, Detective Measures, Awareness Measures, Responsive Measures, Knowledge Base as main components. It also outlines some best practices to follow in order to prevent phishing attacks.

Keywords: Phishing Attacks, Prevention, Detection, Diagramed Network

1. Introduction

As by September 2020, the number of internet users worldwide was of 4,929,926,187 which is huge number as compared to previous years (Stats, 2020) [1]. This represent not only individual users but also organization that are computerizing most of their services at all levels and the use of internet is sometimes a must to gain access to the information stored on these systems.

A group of people known as hackers, has given itself a mission of deceiving legitimate people who are online to gain access to the information they keep on the internet or locally but that they access remotely, using various means one of which is phishing.

Cisco (Cisco, n.d.), one of the leading companies in networks and security devices says that: “Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source.” It is also defined as a social engineering technique to fraudulently acquire sensitive information such as usernames and passwords by attempting to trick users of popular website by emailing them fake versions of the website to provide their credentials to [2].

Phishing aims to steal users’ credentials such as usernames and passwords, social security numbers, credit or debit cards information; or anything that can let the phishers(hackers) access a system or steal money from their victims.

The most utilized vector used in phishing attacks is email. But also, instant messages using social networks such as Facebook, Messenger, WhatsApp and many more can also be used as a delivery means of a phishing link. In phishing attack, based on the type of vector being used, the attacker sends a message containing a link that take the user to a site asking for his/her credentials used to access either a system, a bank account or any other facility.

In July 2017, a new type of phishing attack was discovered and was specifically targeting SME by the Internet Security Company Comodo [3]. The emails were sent out to more than 3000 businesses including the subject line “Shipping Information”. The email noted a forthcoming delivery by the United Parcel Service (UPS) and included a seemingly innocent package tracking link. Once the recipient clicked on the link, a malware was released and installed itself on the recipient ‘device.

Phishers took advantages of the COVID-19 pandemic to increase phishing attacks impact on the world; attackers were and are still impersonating as World health Organization (WHO) or Disease Control and Prevention to trick users to click on a link in order to get update on the COVID-19 statistics or other ways of prevention (2020 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends, 2020).

Because of the easiness in the phishing payload delivery to the victims, other types of attacks are conducted and encapsulated in its payload. This the case for Ransomwares that represented 35% of all attacks orchestrated in the three quarters of 2020, 26% of them were delivered using phishing emails to their victims [4].

The treat pose by phishing attack is great and affect everyone from the receptionist to the CEO of an organization, measures have been developed to fight this threat which include spam detection, other email filtering as outlined in the paper written by [5]. Machine learning too have been employed to try to make an end on using phishing attack based on classification algorithms such as Random Forest, Support Vector Machine and many more (Ike & Sathish, 2018). But unfortunately, no method has been able to fully end the treat that phishing attacks represents.

In this paper, we present a model that we believe, if followed well, can help in the prevention and detection of phishing attacks. The model has six main modules: Businesses Security Objectives, Preventive Measures, Detectives Measures, Awareness Measures, Responsive Measures and a Knowledge Base to store the security experiences of the organization utilizing the present model. The model also shows the collaboration between the organization and the security partitioners who are in charge of the development of security tools.

The paper is divided in six sections: the first one is the introduction, the second is the literature review that presents the related work on solutions that have been proposed to fight the treat pose by phishing attacks; the third one presents the methodology used; the fourth one present the model and the demonstration on diagramed networks showing how each component of the proposed model can feet in the organization network plan; section five presents some best practices and awareness measures that can help in the education of users; the last section is the conclusion.

1.1. Related Work

A. Types of Phishing attacks

- Spear phishing is a phishing email that is tailored to a specific person or organization. The hacker first looks for information about the victim so that the later won’t be able to know that an attack is taking place. This system is ranked among the top thread on internet, having 91% of assaults [6].
- Whaling targets, the high rank employees of the organization such as CEOs or managers to access highly confidential information. Whaling is difficult to detect as it doesn’t use malwares or fake website as in other type of phishing.
- Catphishing (with “ph”) is a type of phishing attack where by the hacker forget a friendly relationship with the victim in order to gain access to the system or resources that store the information’s that the hacker wants. The hacker wants to get control of the victim once he discovers something bad about her/him and he/she is obliged to give away everything the hacker demands demands [7].
- Catfishing (with “f”) it is similar to catphishing but is a different concept; it involves the hacker creating a social network profile as a fictional person in order to manipulate someone into a relationship either romantic or simple friendship. It is first online, with the hope of it to be real-life relationship, but this is not the goal of the hacker. His or her goal is to make money or gain access to some resources, to receive gifts or other benefits that they can gain from the victim.
- Clone phishing is a type of phishing attack in which a legitimate, previously delivered, email containing an attachment or a link has had its content and other information such as sender and recipient taken by the hacker to create an almost matching or cloned email. The attachment or link within the email is replaced with a malicious version and it is then resent. To appear legitimate and in order to convince the receiver to open the link or the attachment, the hacker say that the new email is the updated version of the first or original received email.
- Voice phishing also called “Vishing” is a phishing attack where by the hacker the hacker sends a message to the victim asking him/her to call a number owned by her bank or any other organization that the victim work with but in reality, the number in the message is owned by the hacker; once dialed, the hacker ask the victim to enter their credentials. Vishing uses sometimes false caller-ID to give the appearance that calls come from legitimate and trusted organizations or sources.
- SMS phishing also called “Smishing”. In this particular type, the hacker uses cell phone text messages to deliver the payload bait which will induce victims into divulging their personal information.

B. Other Phishing Solutions

Presents different methods and techniques that can be used to detect and prevent phishing with their shortcoming [5]. Among the proposed solutions that are outlined DNS-based Blacklist is mentioned; it utilized anti-spam filtering as its utility and it is based on a list of blacklisted IP addresses and domain names to allow or prevent users from being victims of phishing; its disadvantage is that it doesn’t recognize zero-day phishing. Another method mentioned in this paper is Email Authentication which is utilized mostly by Gmail, Hotmail and Yahoo; it works by authenticating the password hashing with the domain name, the shortcoming of this method is that not all users use email authentication. Spoof Guard is a plugin used mostly in IE uses a set of heuristics to detect anomalies in the webpage content. It detects phishing patterns based on HTTP. It defines a threshold value and if the result of heuristics crosses the threshold level a warning message is given to the user. It checks if the URL is similar to the whitelist one, then detect for the presence of hidden attributes in the URL; if the URL in the text attribute is different from the actual one then the site is malicious. The disadvantage of this method is that once the hacker knows the defined threshold, he can create his/her URL accordingly and the software won't be able to classify it as malicious.

Propose a model to detect phishing attacks, focusing on Cross-site Scripting (XSS) [8]. The authors say that in this particular type of attack, the application is not faulty, it is the user who is vulnerable and pose the threat because he/she is the one who validate the cause on the web application which allow the attacker to take control of the user's computer from a remote location. The model proposed in this paper is based on the Decision Tree classifier to classify the URL; which are obtained from two datasets named respectfully as user feedback database which store the URL that the user identified as malicious or legitimate; and a phish tank database which store specifically website that are identified as phishing. The shortcoming of this model is that it doesn't take into account other type of phishing attacks such malware or key loggers which install themselves on the computer when the email is opened.

Classification of phishing Email Using Random Forest Machine Learning Technique focus on the application of machine learning to identify phishing email [9]. It first introduces the concept of phishing and the problems that are associated with it. It says that most technique for discovering phishing email have not evolved with the technique's hackers used to conduct this type of attack, that why machine learning need to be used for the automation of this process. They used the Random Forest Algorithm on a dataset of rules which accomplished an accuracy score of 99.7% with a minimal percentage of false positive (about 0.06%). To be effective, with the innovative tactics used by hackers, the dataset should be kept up to date and maintained by the conceiver of this idea, which can be time consuming.

Propose a model which use Link Guard algorithm for the detection and prevention of phishing attacks based on webpage and URL-based similarity [10]. The system has a database containing legitimate URL and Webpage, the Link Guard algorithm compare the URL of the link contained in the phishing email to the one in the system database, if a match is find the link is assumed to be legitimate, the algorithm then proceed to comparing similarities in the webpage for confirmation of the legitimacy of the site, in case the webpage is different an alert is sent to the User who can avoid to give out his information. The algorithm doesn't consider key and screens loggers or malware loggers with can be triggered by the simple action of opening the email send by the hacker. Also, new websites are being created every day and each of them has a unique URL, if the database used by the link guard algorithm fell to receive update, the network will be prone to phishing attack.

2. Methodology

The research used the Design Science approach to carry out the research. The research also took a Design science approach of research; this was done because it is the approach suited for the creation and evaluation of IT artifacts, such as models which is the focus of this research, frameworks, methods; intended to solve organizational problems.

The model is the combination of the framework proposed by (Ike & Sathish, 2018) which state that to effectively fight phishing attacks, three components must be in place: Prevent phishing, Detect phishing and Stakeholder training.

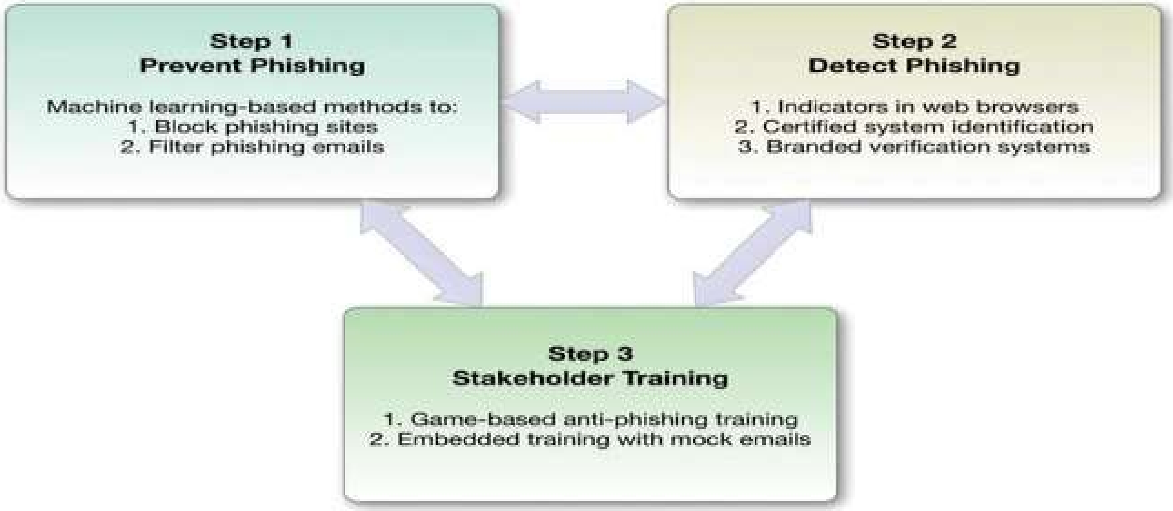
Step 1
Prevent Phishing
Machine learning-based methods to:
1. Block phishing sites
2. Filter phishing emails
Step 2
Detect Phishing
1. Indicators in web browsers
2. Certified system identification
3. Branded verification systems
Step 3
Stakeholder Training
1. Game-based anti-phishing training
2. Embedded training with mock emails

Figure 1: Preventive phishing framework (source (Ike & Sathish, 2018))

The Hybrid Phishing Detection and Loss Computation Model proposed by which state the use of three modules: Risk analysis, Loss estimation and Risk mitigation [11].

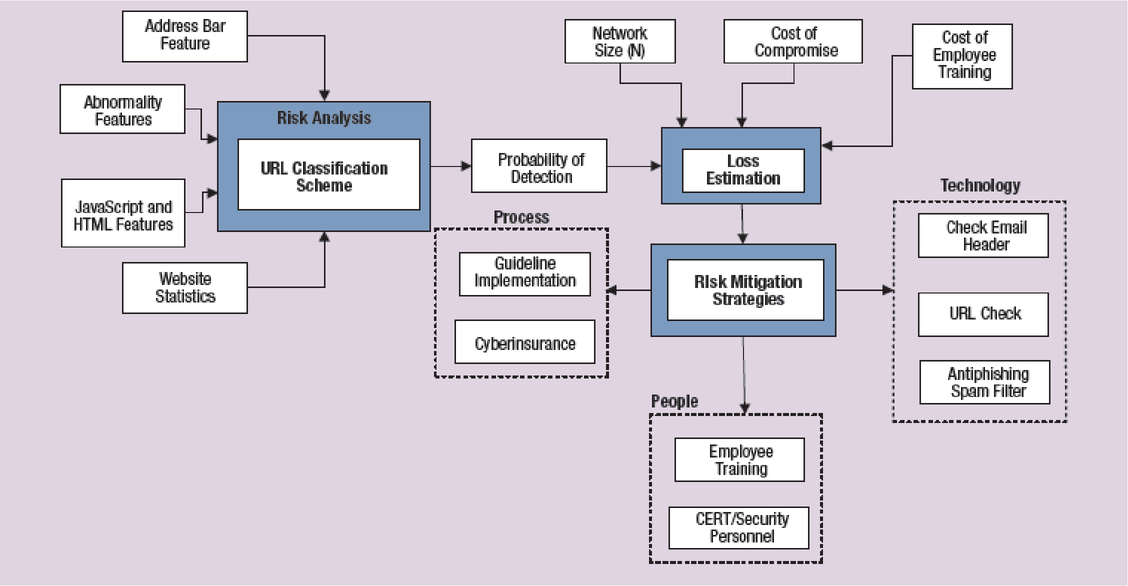

Figure 2: Hybrid Phishing Detection and Loss Computation Model (Biswas & Mukhopadhyay, 2017)

For the demonstration of the effectiveness of the model, a diagramed network was design using Microsoft Visio to show an example of a simple organization network [11].

3. Model Design and Demonstration

3.1. Model Design

The model that we came up with based on the framework and the model above is as shown

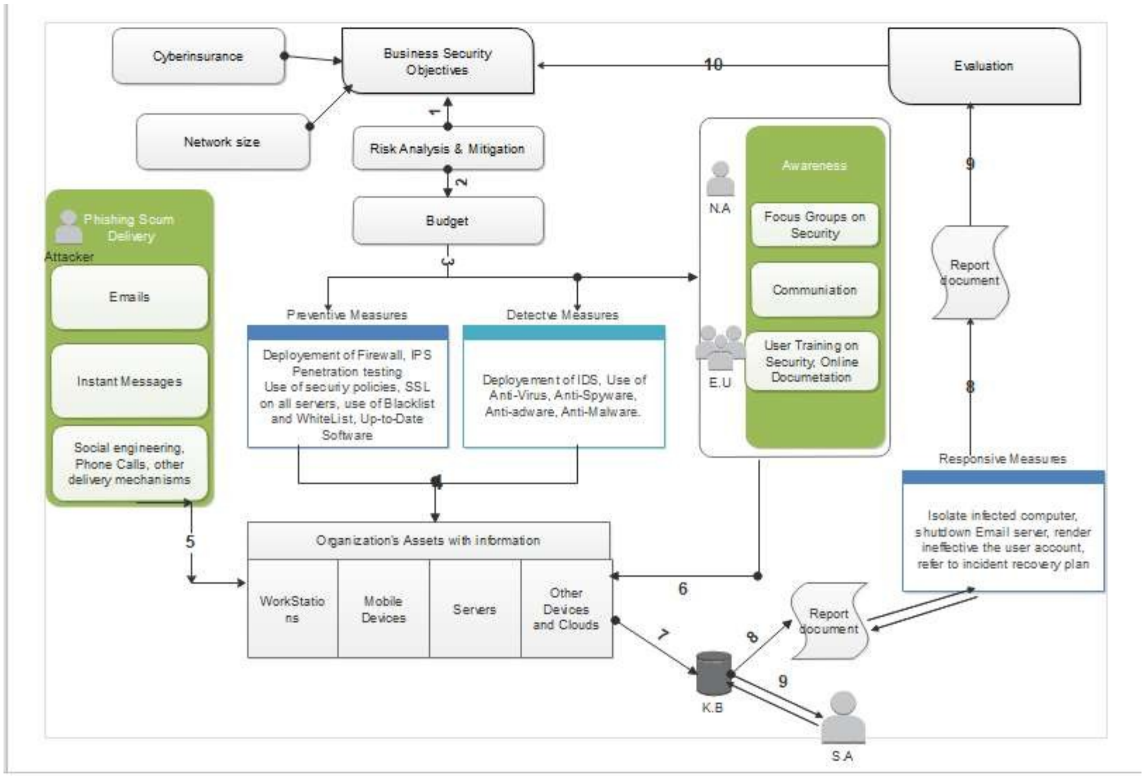
Cyberinsurance
Business Security Objectives
Evaluation
10
Network size
1
Risk Analysis & Mitigation
2
Budget
3
Phishing Scam Delivery
Attacker
Emails
Instant Messages
Social engineering, Phone Calls, other delivery mechanisms
Preventive Measures
Deployement of Firewall, IPS Penetration testing Use of secuiry policies, SSL on all servers, use of Blacklist and WhiteList, Up-to-Date Software
Detectve Measures
Deployement of IDS, Use of Anti-Virus, Anti-Spyware, Anti-adware, Anti-Malware.
N.A
E.U
Awareness
Focus Groups on Security
Communiation
User Training on Security, Online Documetation
9
Report document
8
Responsive Measures
Isolate infected computer, shutdown Email server, render ineffective the user account, refer to incident recovery plan
4
5
Organization's Assets with information
WorkStations
Mobile Devices
Servers
Other Devices and Clouds
6
7
8
9
Report document
K.B
S.A

Figure 3: Preventive and Detective model for phishing attacks (Author Made)

Base on this model, for an organization to protect itself effectively from phishing attacks, it has to follow these steps

i. The organization has to decide on its security objectives by deciding on the network size, doing risk analysis and mitigation, deciding on whether or not to supply on a cyberinsurance company.

Ï. Based on the decision take in phase one, the organization will decide on the budget to make available for security measures.

iii. Security measures are purchased and decide on; Preventive measures, Detective Measures, Awareness Measures and Responsive Measures

iv. Security measures are applied to organization devices with information to be secured

v. The hacker sends the phishing payload to the organization

vi. On reception of the phishing payload, it is filtered by preventive, detective and awareness measures

vii. If the attack is stopped by one of these measures, a report document is sent to the knowledge base

viii. In case the attack is successful, responsive measures are to be applied as soon as possible to contain and prevent much loss for the organization

ix. A report document is sent to the security partitioners, and the other is used for evaluation in the organization

x. The organization decide on other security objectives and the process start again.

- **Phishing Scum Delivery**

This shows the different means used by attackers to deliver the payload to their victims. This includes email, instant messages on social media such as Facebook, WhatsApp, LinkedIn, Instagram etc. and even SMS or phone calls when the hacker want to increase the level of confidence of the victim. Social engineering is also used to convinced the user to do want the hacker want.

- **Organization's assets with information or has access to information**

These are all the devices that have access to information kept by the organization. They include workstations, mobile devices owned by the organization or by individual employees and servers that store that information.

- **Business Security Objectives (BSO)**

These are objectives set by the organization even before any security measures are applied in the company. Each organization must have objectives so that it can budget how much it is willing to spend on the security aspect of its information. This process involves also knowing the exact size of the network, if possible, also to apply to a cyber-insurance company and most importantly to perform the risk analysis to know well the vulnerabilities so that they can know what security measures to put in place.

- **Preventives Measures (PM)**

The organization should put in place measures to prevent phishing link to reach users; if the payload doesn't reach its destination, there is 80% of chance for the user to not open it and read it which will prevent the attack from occurring. Organizations can accomplish this by deploying on their network well configured firewalls, intrusion prevention system, email filtering using whitelist for allowed addresses and blacklist for blocking addresses that are already recognized as vector for phishing, the use SSL on their critical server systems, the use of security policies, penetration testing and auditing, use of preventive algorithm that have been developed and prove themselves on the market. These measures can be extended according to the capability of the organization.

- **Detective Measures (DM)**

Organizations should also put in place detective measures to detect earlier the scum that might successes to lure the preventive measures. A detected phishing scum can reduce by 90% the chance of a phishing attack to take place. The detective measures that can be put in place are but not limited to Intrusion Detection Systems both Network-based and Host-based, anti-virus software, anti-spyware software and other anti-malware software, detective algorithm that have been developed and prove themselves on the market.

- **Awareness Measures (AM)**

The biggest weakness to security is users. Preventives and Detectives measures are effective enough only if end-users can also do their part; and the only way they can do it is if they are aware of what they are supposed to do. This is done through communication, user training, security campaign, focus group on security and many more. Network Administrators and security officers should tell the users how important security of information is and that they are responsible for it. They should train them on how to verify basic security utilities on their personal host such firewalls, HIDS and IPS and ant-malwares, so that they know if they are running before they can connect to the internet or open their email. Security campaign and focus groups on security should also be organized to refresh the awareness of users about security.

- **Responsive Measures (RM)**

In case the user is unable to detect a phishing email, and the hacker get her/ his credentials or the virus get spread on the network, responsive measures should be put in place to contain the propagation of the virus or to prevent the hacker to use the credential he/she has stolen. This can be done by defining clearly the responsibilities of individuals in the Business Continuity Plan in case such incident occurs, it can be by isolating the infected computer from others on the network, shutting down the mail server if the phishing email were numerous, and other measures. In case of stolen credential, the user should communicate with the system administrator who should change the user's credentials immediately or render ineffective the user's account.

- **Report Document**

After the responsive measures have been applied and the attack contained and resolved, the attack and all the processes and measures took to resolved it must be documented and kept in the knowledge base of the organization. A copy of the report can be sent to security practitioners who are responsible for the development of security tools.

- **Knowledge Base (KB)**

This is the database that keeps all the virus, malware or any attack that the organization is aware of and have been subject to. It is populated by the organizations'expiriences on security but also by other organization and security practitioners.

- **Evaluation**

Evaluation is done after a security attack have been resolved. It is also done periodically to make sure that the security mechanisms used by the organization are effective. If they are not effective or when new update from security practitioners have been released, the organization has to apply them.

- **Security Authority (SA)**

These are security practitioners who develop security tools. They can add data to the organization's knowledge base and the organization can also supply them with new that when are faced with a new attack.

3.2. Demonstration

For demonstration, we came up with a network diagram plan to show how each module of the model can feet on the network.

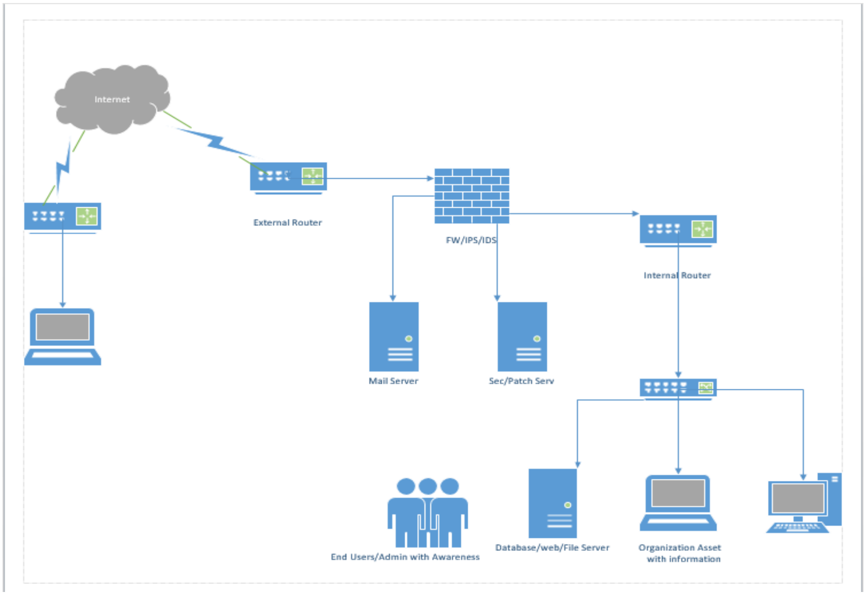

Figure 4: Network diagram supporting the preventive and detective model

The diagram presents a network with two routers: un external router which connects to the internet and to the network dedicated firewall, and the second one is connected to an internal router and to a Demilitarized Zone (DMZ) network which host servers that are not only accessed for the internal network but also from the internet. Apart from that, the IPS/IDS is installed on the firewall and the internal router; the internal network has other server that are exclusively used on the intranet for internal use. With this architecture, the chance of a successful phishing attacks is reduced to some point.

The phishing scum sent through the internet by a hacker, will first reach the first router which base on the ACL configurations might block the email and the attack won't happen; in the case that the hacker used IP Spoofing to lure the router, a dedicated firewall is there for further analysis and the attack could still not happen because blocked by the firewall; if the firewall is not successful in preventing this attack, it will first send the email to the mail server in the DMZ which will view the send and the content of the email and classify it either as legitimate or spam base on the various machine learning classification algorithm that are implemented on the server, that means, the attack could also be stopped at this point; but if again the hacker used words or addresses that the classification algorithm could not classify as spams, in its way to the internal mail sever, the phishing email still have to pass through the IPS/IDS that based on its configuration, might stop the attack, the internal router also will have to inspect the email before delivering it to the internal mail server; again, the internal SMTP server, will have to inspect more the email before deciding to whether or not it can deliver the email to the end user who is the rightful destination of the email. Once the phishing email is delivered in the end user's mail inbox, his/her HIPS/HIDS will still inspect the email before even the user opens it; if they still not able to detect the email as phishing, the last line of defense is the end user; who base on the education and training that he/she would have attended would be able to decipher that the email is phishing and won't click on the phishing link. In the end if the phishing email lures the end user also, and this one clicks on the link and provide his/her credentials to the fake site, and discover right away that she/he has been phishing, she/he can directly tell the IT department which base on the incident response plan, will take appropriate measures to stop or limit the damage that the phishing email will have caused to the company network. One of these responsive measures could be to disable the user account whose credentials would have been stolen, another one could be to isolate the infected machine in case the phishing email delivered a malware, or to shut down the email server if it was the target of the phishing email or maybe it is still delivering phishing emails to other end users and it can't be stopped. Also, another method to apply, is to use SSL on all the company web site to avoid site cloning by hackers; if the users of a web site know that their web site use SSL and the cloning site doesn't which in most cases is the case, they won't provide their credentials to that site.

After the responsive measures have been applied, the IT department should write a report to document the incident and keep it in the Knowledge Base Database, another copy of the report should be sent to security experts or authorities who are in charge of the development of security tools who can develop patches to close the holes in the security tools currently in use so that they won't be exploited again. Also, the management and the IT department should do the evaluation of the incident and see how they can revise the business security objective of the organization to reflect the new measures that they should implement to avoid being the victim of another similar attack.

4. Awareness Best Practices

Security guideline to help in the prevention of phishing attacks in organizations

1. Train your employees to recognize scams - This will help them to stop the attacks in case neither of the preventing measures such as firewall and IPS could not detect and stop the attack
2. Use two-step verification - The attacker will surely not be aware of the fact that the organization is using two-factor authentication, in case the employee has been phished, if he/she doesn't receive the PIN or code that confirm the change of his credentials, he/she will know that she/he is victim of phishing and report it to the appropriate department for corrective actions.
3. Have regular security evaluation checks -Performing security evaluation regularly helps the organization to discover the security holes but also to assess the attacks that hit the organization and see what could be done to prevent the occurrence of similar attacks
4. Continually update your software-Some phishing attack, such as malware attacks exploit vulnerabilities or install backdoors on the systems, update of software is the effective remediation against these attacks.
5. Secure the application browsers-Updated browsers are using SSL/TLS that provide a layer of security from the previous version of browsers and limit the abilities of casual hackers to impersonate the trusted web site.
6. Use different password-The use of one password is to dangerous in case a hacker gets a hand on it, he has access to all the systems accessed using the password. Some software; such as LastPass, help in the management of passwords and users can be advised to use them.
7. Hold mock drills for phishing attacks-The security team can use mock emails to test the ability of employees to recognize phishing emails. It also helps in determine the state of security software such anti-virus and firewall on end-hosts.
8. Install reliable anti-virus software-Many phishing emails carry malware, reliable anti-virus software will detect and remove all those malwares or any backdoor. Users should be taught on how to active and update them regularly
9. Never click on link in emails-Most of phishing emails contain links to fake web sites. User should be train on this issue and should avoid to click on this link. Instead, they can open another window and access the intended site from there.
10. Report phishing attacks-The organization should have a mean for reporting phishing attacks in the organization [12].

Some additional tips to avoid phishing

1. If you are not inspecting an email, you should reject it or call the person who sends the email before opening it
2. Hover to discover: when hovering over a link, it shows where it directs you. If you are not sure or recognize the destination of the link, don't click on it
3. Password in an email, an email that ask for credentials such as username, password is surely a phish.
4. Implement Email policy and have a standard email format in the organization [12,3].

5. Conclusion

The research came up with a model that can help in the prevention and detection of phishing attack as they are carried out to individuals and to organizations. It proposed the use of organizational processes, technological factor and the human factor to end the threat pose by phishing attacks and we believe that it can effectively help to reduced their impacts on organizations.

Because of the threat pose by phishing attacks, more researches should still be carried out to add on the existing knowledge solutions; hackers are still creating new way to exploit the human trust nature. And a more adequate technique for model testing should be considered to help in a better way of validation for artifact (model) before its deployment in real world.

References

1. Stats, I. W. (2020, September 30). *Usage and Population Statistics*. Retrieved from Internet World Stats.
2. Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security, 2018*(1), 15-20.
3. Pickard-Whitehead, G. (10). *Phishing Examples in 2017 that Targeted Small Business. Aug 29*.
4. Gendre, A. (2020, November 12). *Top 6 Phishing Trends of 2020.*

5. Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67*, 247-267.
6. Dakpa, T., & Augustine, P. (2017). Study of phishing attacks and preventions. *International Journal of Computer Applications, 163*(2), 5-8.
7. Shukla, A., & Gehlod, L. (2014). A survey on phishing detection and prevention technique. *International Journal Of Engineering And Computer Science ISSN: 2319, 7242, 6255-6259.*
8. Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. *Journal of Applied Mathematics, 2014*(1), 425731.
9. Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). An ideal approach for detection and prevention of phishing attacks. *Procedia Computer Science, 49*, 82-91.
10. Biswas, B., & Mukhopadhyay, A. (2017). Phishing detection and loss computation hybrid model: A machine-learning approach. *ISACA Journal, 1*, 22-29.
11. Gerber, S. (2018). 11 security strategies to protect your company from phishing attacks. (2025), 3, 23.
12. 2020 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. (2025).
13. Sneath, P. H. (1957). The application of computers to taxonomy. *Microbiology, 17*(1), 201-226.
14. *Phishing*. (2021, January 19). Retrieved from Wikipedia: