Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 8, 2025

INVESTIGATION OF PHISHING ATTACK IMPACT AND PREVENTION AT A LOGICAL TECHNOLOGY COMPANY IN HYDERABAD

Fauzia Talpur[*1], Ramesh Kumar[2], Shakir Hussain Talpur[3], Hina Shafi[4], Akhtar Hussain Soomro[5], Syed Baig Ali Shah[6], Misbah Nooren[7]

[*1]*Department of Computer Science, University of Sindh Jamshoro Laar Campus*
[2,3,4,6,7]*Information Technology Centre, Sindh Agriculture University Tandojam*
[5]*Govt College University, Hyderabad*

DOI: https://doi.org/10.5281/zenodo.19399654

Keywords

Article History
Received: 28 June 2025
Accepted: 14 August 2025
Published: 28 August 2025

Corresponding Author: *
Fauzia Talpur

Abstract

Phishing has been extremely effective at infecting both people and organizations. Working and communicating online is now possible thanks to new technological developments. Phishing is currently a prevalent form of financial fraud on the internet. Attack victims are more common because of human cognition and understanding of limitations. On the other hand, despite employing various security measures, businesses may still fall prey to fraud. Emerging technologies in the modern internet era have raised security concerns regarding internet dependency. Social engineering attacks compromise security and seize control of targets when they are made against systems or networks. Scammers purposefully create links to acquire sensitive data, such as user information, login passwords, credit card numbers, and other details. Clicking on suspicious links led to the commencement of phishing and other social engineering schemes. Data loss, system information leakage, and monetary loss are the outcomes. When unaware victims click on dubious links in a true phishing email, the security of the machine or system is compromised. Phishing is a type of attack that may target consumers to gather private information about their money and personal lives. These approaches prey on users and undermine network security by taking advantage of network weaknesses, human psychological characteristics, and a lack of understanding of phishing techniques. But in addition to increasing technical awareness, contemporary phishing prevention strategies rely on a framework for detection and prevention. But when it comes to tackling technical and societal issues holistically, it is ineffectual. Therefore, effective detection and preventive techniques that combine human and technical intervention are required.

1. INTRODUCTION

Emerging technologies in the current internet era have brought up security concerns with dependence on the internet. Social engineering attacks compromise the security of networks or systems and take over the target. Scammers create links on purpose in order to collect sensitive data, such as user information, login passwords, credit card information, etc. One of the social engineering assaults that resulted from clicking on suspicious links is phishing. It might lead to data loss, financial loss, and system information disclosure(Islam et al., 2023). Because they are ignorant of phishing, victims click on malicious links contained in a real phishing email, which compromises the computer's or system's security.One of the most popular methods for sending these URLs, though, is email phishing.

Attacks take place when victims are not aware of phishing frameworks, strategies, and preventative measures. It raises the likelihood that phishing will succeed. Phishing attacks saw a noticeable increase in December 2021, with more than 300,000 reported incidents, according to the APWG's Phishing Activity Trends Report, 2022. OpSec Security, a founding member of the APWG, disclosed the attacks on several industries. However, SAAS/webmail providers (software as a service) are determined to be at the greatest risk of phishing attempts, at 23.2%, followed by the financial industry at 19.5%. as shown in figure 1 below. (Phishing Activity Trends Report, 2022)

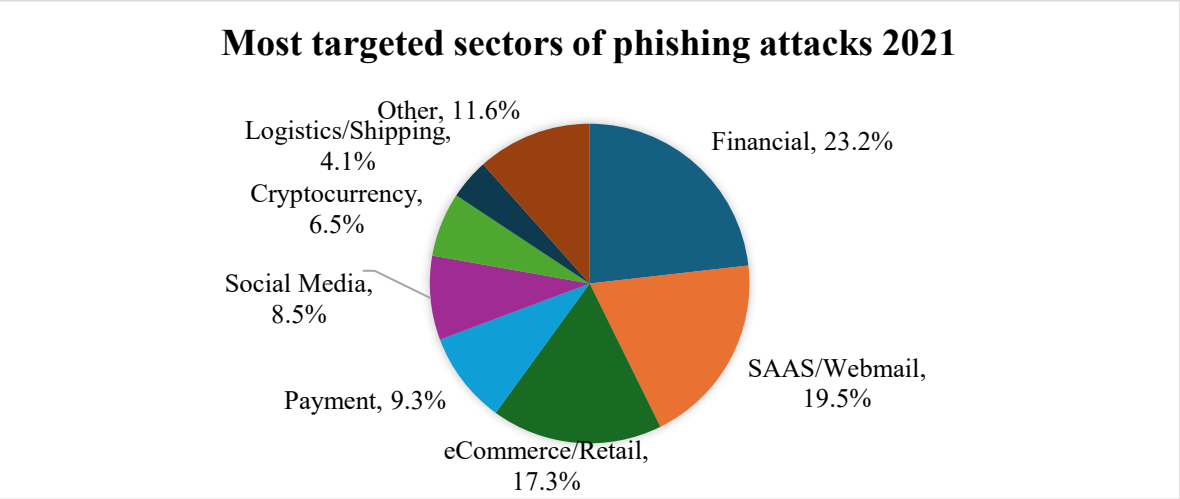

Figure 1.1: Most targeted sectors of phishing attacks 2021

In addition, different attack types in every industry have an impact on both people and organizations in terms of the cost of financial and reputational harm. Attacks utilizing social engineering are not well protected against. User vulnerability models, user-centric frameworks, and campaigns are all examples of existing preventative strategies. The inclusion of people in security sensor frameworks is the primary goal of prevention. With advice on actions or rules for secure systems, it must examine cyber security. A number of models are put forth to stop these attacks. These models are based on several social engineering attack frameworks and approaches (Ramzan, 2010).

Phishing has grown significantly in recent years with the usage of online connectivity. The most frequent methods of information theft, according to attack patterns, are requests for changes to sensible information and login credentials. These requests are sent via social media, games, SMS, emails, and a variety of other channels. The vulnerability to attacks is increased by carelessness and lack of experience with such assaults. The increasingly convincing and cunning methods used by phishing assaults to get consumers to click the link are mostly to blame for their success. The victims are misled by fake emails involving personal information such as usernames and passwords. Phishing attacks can affect anyone because they seem real and authentic. Despite the use of sophisticated anti-phishing tools, a number of factors contribute to the success of phishing attempts (IET Information Security - 2023 - Prabakaran - An Enhanced Deep Learning-based Phishing Detection Mechanism to Effectively.Pdf, n.d.). In order to better effectively stop phishing assaults in the future, this project examines the components and pre-existing models for studying phishing strategies.

Phishing is a practice that has had a lot of success infecting both people and businesses. With the development of new technologies, working and communicating are now done online. Phishing has developed into a significant form of online financial fraud. Attack victims occur more frequently as a result of human consciousness and

understanding limitations (Veeramalla et al., 2023). On the other side, even using various security measures, organizations may still fall prey to fraud. But as attackers create new phishing methods, the range of attacks and level of technological expertise rises. In order to breach security, it might use connections to the concealed virus. Due to Trojans in networks, links to download programs or update information even have the potential to compromise security systems. Email phishing, social media phishing, evil twin phishing, and many other approaches are used as phishing strategies to gather sensitive and private data. It could be risky and cause harm to a system from malicious assaults.

1.1 Problem statement

Phishing is a type of assault that has the potential to target consumers in order to collect sensitive data about their finances and personal lives. These methods prey on users and compromise network security by exploiting flaws in the network, psychological aspects of people, and a lack of knowledge about phishing techniques. However, current methods for preventing phishing rely on a framework for detection and prevention in addition to raising technical understanding. However, it is ineffective when it comes to taking a comprehensive approach to technological and human problems. Therefore, there is a need for efficient detection and prevention methods that integrate technical assistance with human intervention. The project's goal is to provide effective preventative strategies that involve human connection.

1.2 Research Objectives

The goal of research is to analyze current methods and examine the various aspects that enable phishing attacks. To safeguard both individuals and organizations against such attacks, a new effective paradigm needs to be created. In order to prevent phishing, it is critical to understand phishing trends, strategies, and attack types. Additionally, it improves knowledge and abilities in the creation of an anti-phishing strategy to increase resistance to targeted attacks.

- To identify the factors involved in the success of phishing against organizations
- To implication an efficient model for detecting and preventing phishing attacks

Understanding the elements that contribute to phishing attacks' success against enterprises is one of the goals. Develop an effective model for identifying and preventing phishing attacks by researching and analyzing current methods of defense against phishing assaults.

2. REVIEW LITERATURE

2.1 Background

Phreaking was the term used to describe phone hacking, and the "ph" in phishing stood for network hacking. Phishing is an idea that evolved from phone phreaking in which the word "fishing" was changed to "phishing." To protect passwords, computers were secured with a variety of encryptions and access controls. Since there was no phishing software available in the early 1990s, a phishing attempt in 1994 used the phishing software AOHell. In 1995, phishing software was created to circumvent computer security, giving hackers access to internet users' passwords. When ARPANET users received a spam e-mail from DEC computers, a Trojan horse was identified as the first security risk. Phrack, an electronic journal for hackers, began publication in 1985. It is a time-honored practice to trick someone into disclosing their private information. Before the usage of the internet, such actions of using such information for fraudulent purposes also existed (Jagatic et al., 2005). On the other hand, target attacks on the internet started as soon as it was created, while social engineering attacks are now expanding their frameworks and adopting cutting-edge methods under the name of phishing. Today's serious cybercrimes include financial theft, identity fraud, and many more uses of the information. The use of online services for routine tasks has increased the potential for targeted attacks, including phishing. Personal information that is targeted by criminals must be accessed for online activities like banking, shopping, etc (Islam et al., 2023). The widespread practice of spear phishing involves phishers sending emails that appear to be legitimate requests for personal and sensitive information. Many businesses have recently been

the target of email attacks that appear legitimate to organization employees(Tinubu et al., 2023).

2.2 Case Studies

APWG data (Phishing activity trends report, 2022) state that email phishing attempts are continuously rising. E-gold institutions were the first financial target of spam email in 2001. Spam mails were first used fraudulently by phishers to expand their network. Phishers regularly target many institutions, such as a focused attack on VoIP in 2006 and the theft of around 1.5 million US citizen identities in 2007. In 2008, spam messages were sent to social media platforms like Facebook. In addition, one of the biggest cyber attacks ever recorded happened in 2011 when phishers obtained the credit and debit card information of over 10 million PlayStation Network and Sony Entertainment users, causing a loss of between $1 and $2 billion. Custom phishing, according to Symantec, involves novel ways to con people for money and has a financial component. Scammers use gift cards or phishing pages as revenue sources, which causes substantial financial damage to victims. More than 25,000 phishing victims lost around 48,241,748 USD in 2018, Phishing has drawn a lot of criticism, and the targeted sectors have suffered significant financial losses. Phishing emails targeted the healthcare and educational sectors, stealing the employees' login information. Phishers had an adverse financial impact on the organizations, but they also gained access to payroll systems and stopped employees from receiving notices(IET Information Security - 2023 - Prabakaran - An Enhanced Deep Learning-based Phishing Detection Mechanism to Effectively.Pdf, n.d.). Attackers were able to deposit money into their accounts using phishing assaults and modify debit information. by phishing emails grows(*Security and Privacy - 2022 - Almousa - Phishing Website Detection How Effective Are Deep Learning-based Models and.Pdf*, n.d.). However, the attackers continue to succeed in their deception since they can easily take advantage of people rather than compromise the system. Therefore, the human component should be taken into account while detecting phishing emails.

Recent studies have focused mostly on the technical methods used in email phishing assaults. These characteristics have been exploited in email phishing tactics in the past, and by researching them, preventative techniques have been created. However, other studies suggested creative methods for spotting phishing emails. These models are created by studying the characteristics or actions of the target consumers who are vulnerable to phishing scams. Although it is insufficient to fully protect the user from email phishing assaults, studies also take into account human characteristics when recommending email phishing detection measures. Advanced feature extraction-based approaches are machine learning-based techniques. The effectiveness of these tactics is influenced by the algorithms utilized, the precision of the detection, and the accepted classification of email phishing attempts. These approaches' drawbacks include their extensive feature sets, lengthy processing times, and high memory requirements(Zhuo et al., 2022). However, very few research go into detail about how phishing strategies or targets deceive users.

Furthermore, the demographics of the targets cannot be well described by an analysis of the effectiveness of each type of medium, vector, and technical technique. The research of phishing attack motivations is restricted to factors like money gain and data loss. To stop phishing attempts, it should be expanded to include study on the viewpoint, feelings, and motivations of the perpetrator. motives might take the form of concrete outcomes like economics or more ethereal ideas like human or symbolic significance. The most recent methods for phishing detection leverage message content rather than malvertising (Pallavi et al., 2020), tab-napping, or squatting methods. Additionally, machine learning-based phishing email detection is supported by the NLP (Natural Language Processing) technique. NLP improves email text filtering and makes it simpler to detect semantic changes. As a result, models become more accurate, but they still need to be applied to larger datasets of phishing emails. The most widely used methods for detecting phishing emails are neural networks like CNN and RCNN. It is frequently employed to stop phishing

attempts. However, training takes a long time and requires expertise from professionals. When using technology to defend against an email phishing attack, human factors must be taken into account. Enhancing the solution with human variables vulnerable to phishing attempts is crucial. Technical improvement in more recent detection approaches and technologies can incorporate effective learning mechanisms.

3. MATERIALS & METHODS

This research is cover by quantitative research approach and 35 respondents fill questionnaires about Investigation of phishing attack impact and prevention at a logical technology company in Hyderabad.

3.1 Machine learning-based phishing email detection

Machine learning algorithms are effective at identifying and categorizing phishing emails. Support vector machines (SVM), decision trees, neural networks, and other machine learning methods constitute the foundation of a number of detection models. For phishing email detection, anti-phishing techniques are heavily used. To stop phishing attacks, email detection techniques involve classifying emails as suspicious and non-suspicious emails. These methods can be improved to produce greater results because they are flexible. Based on training data, machine learning is important in combating email phishing assaults. It must be trained on a large enough dataset of high quality. With careful hyper parameter adjustment, high accuracy can be attained.

3.2 Choose Email Features

Emails have a header that includes details like the subject, date, sender, and recipient. The message that includes text, attachments, links, and photos in any format is called the email's body. As a result, the header and body information must be the main focus when detecting phishing emails. However, just particular text is examined to determine whether emails are legitimate rather than the complete content. Specific elements from the phishing email content are chosen. Some keywords, sender email addresses, and hidden links are included. Additionally, the SSL certificate (Secure Socket Layer) and certificate authority of the links in the email are verified. In order to distinguish between valid and malicious emails, various carefully chosen features are collected from emails during phishing email detection(Shmalko et al., 2022).

3.3 SSL certificate is one of the key components utilized in phishing email detection

Email messages often ask the recipient to submit personal information on designated websites or supply account-related data. When data is entered or sent between a user and a server, the HTTP protocol of a legitimate source is encrypted with SSL. However, URLs in phishing emails might be provided without secure HTTPS. These emails are flagged as phishing or suspicious emails.

3.4 Credential authority

Additionally, the website link's certificate authority is examined. Links that use HTTPS may not be secure if the SSL certificate was received from an unreliable source. If the HTTPS link is not secure, it may reveal users' information to an intermediary. For instance, reliable authority include Symantec, Comodo, and GoDaddy. Therefore, it is crucial to verify that the SSL certificate is current and issued by a reputable source. If an authentic CA cannot verify the secure and reliable email source, the email is regarded as phishing.

3.5 Negative keywords

Blacklist keywords are frequently used in phishing attacks to catch people off guard. Short phrases like "click now," "update now," "valid for 24 hours," etc. are used as keywords to indicate how urgent certain tasks are. They are contained in the email's body and lead to dubious URLs. In order to sway the user, phishing emails employ a number of keywords. If the email contains one or more keywords that are on the blacklist, it is considered malicious. If not, the email is genuine.

3.6 Redirection

A user receives emails with links in them. Users

may be directed to phishing websites via these links. Before the user connects to the intended website, phishing emails first connect them inadvertently to a hostile website. These URLs lead to a covert server where private data can be stolen and the user misled. Between the user and a dangerous website, a proxy server acts. The HTTP protocol's GET request determines if a URL is trustworthy or malicious.

3.7 Covering links

Customized emails are used to send emails with hidden links, and the URL is abbreviated to highlight the relationship to the original links, such as "goo.gl." Users might not be able to locate the true hidden URL website. As a result, emails sent by phishers are examined for hidden links using cascading style sheets. JavaScript is also used in these emails to alter the URL and add personalized content or pictures. Emails with brief URLs are therefore classified as suspicious emails.

3.8 A visible IP address

Given that the website's lifespan is limited, a plain IP address can be used instead of a domain name. These links to phishing pages have only been active for a few days, and the phishers only utilize one IP address briefly. Links like "https: //50.20.215.13 /index.p hp" can be found in phishing emails. It said emails with IP addresses and pages from unverified websites are handled suspiciously.Website Traffic Website traffic is regarded as a function to monitor website visitors. Genuine websites frequently receive a certain type of visitors. Phishing emails provide links to websites with lower traffic since they are not frequently accessed. Their brief existence lowers their rating and makes them detectable as dubious websites. By locating unpopular websites in links, phishing emails can be identified.

3.9 Duration of the website

Emails are examined for connections to web pages that are available forever. Phishing websites have a brief lifespan, while legitimate websites have a long existence and can provide the necessary proof of validity. Phishing websites have been around for less than a year, and emails that contain links to them are flagged as suspicious. We consider these emails to be phishing emails.

3.10 Your email address

Next, the subject and email sender address are examined in emails. If the email's address and subject conflict, the sender might be lying. Phishing emails may have subjects like data sharing, password reset, or other irrelevant information, yet they appear to be received from a legitimate source. Phishing emails also make advantage of odd domain names that reveal the sender is malevolent. As an illustration, phishers will utilize reputable sources like Microsoft and Dropbox to demonstrate their validity while using email addresses that contain domains like dropbox.com. This anomaly makes the sender's address less trustworthy and raises suspicions about the email. Email is therefore suspect if an authentic domain name is not utilized.

3.11 The name of the attached file

Attachment files are regularly used in phishing emails to harm users' systems. Such attachment files have a workable shell script hidden in the payload. Thus, the phisher can direct the user's system to carry out specific tasks. Email phishing assaults make use of a variety of phishing technologies. It is a suspicious email if it has a ".exe" or ".dll" extension.These features are used to identify phishing emails because they are efficient at determining an email's validity. There are numerous outcomes when combining different traits.

3.12 Methods of classification

The categorization of emails is crucial for spotting phishing emails. Email classification can be done using supervised, semi-supervised, or unsupervised machine learning approaches. Such approaches have been the subject of recent study. They are simple to use and heavily rely on machine learning training data. Wide-ranging data used for training increase the model's accuracy. SVM classifiers are frequently employed for machine learning-based phishing email detection. SVM is renowned for having a higher accuracy rate than other classification techniques. SVM performs better

and addresses regression and classification problems. It can distinguish between different types of emails, including phishing scams and trustworthy ones. With hyperline h, which is provided by: SVM correctly distinguishes the email classes according on weight, bias, and the amount of features.

$$h(x) = W * \mathrm{X} + \mathrm{b} = \sum_{i=1}^{N} \propto_i y_i(x_i x) + b$$

In this equation, W (weight), b (bias), and N (number of features) of the dataset are considered with a set of training tuples xi is and class labelled yi. Each yi takes either +1 value for a phishing email or -1 value for a legitimate email where αi is Lagrange multiplier. SVM separates imbalanced data into higher-dimension space before using a linear model (Karanjai, 2022). The new email is applied to SVM classifier according to the hyper line and compares selected features to whether it matches with features of a phishing email. If features of a new email are above the hyper line, SVM classifies it in the phishing email class otherwise email is detected as a legitimate email.

3.13 Datasets

Datasets are crucial for both training models and evaluating the effectiveness of detection models. It contains pertinent information, such as emails that train the model to distinguish between legitimate emails and phishing emails. The dataset is crucial to the effectiveness and dependability of the detection model. The dataset's chosen features are used during the detection process to classify and learn about the emails. The datasets used to train the email detection model, however, may be comparable to those used to train other models, which poses a diversity problem. As a result, using various datasets is encouraged for improved performance. The dataset can make use of information from several sources, in a range of sizes and timescales, including weekly or daily data. The public can access several datasets for email phishing detection. Two datasets are used for phishing email classification. The phishing corpus dataset contains 5000 phishing emails, and the phishary corpus dataset is used to classify emails. Multiple datasets are also employed to boost the variety and effectiveness of the model, along with customized datasets of the appropriate size. The Enron dataset is a useful dataset and is available to the general public. Additionally, the following list includes publicly accessible email detection datasets. The PU dataset is a popular choice among these datasets for machine learning-based email detection methods.

Table 3.1 Publicly available datasets and their links. (Mujtaba et al., 2017)

Name of Dataset	Available Link
PU	http://www .csmining.org / index.php/ pul-and-pu123a -datasets.html
Phishing Corpus	http://www .monkey.org / *jose/wiki/doku. Php?id=PhishingCorpus
SpamBase	http:// archieve.ics.uci. edu/ml /datasets /SpamBase
Enron	http:// www. Aueb.gr/ users/ion data/ enron-spam
LingSpam	http: //www csmining.org / index.php/ ling-spam-datasets
TREC	http: / /plg .uwaterloo .ca/~gvcormac/ treccorpus07/
CCERT	http ://www .ccert.edu.cn/ spam/sa /datasets .htm

3.14 Proposed Model

Phishing Email detection and prevention using hybrid GRC and machine learning. Machine learning (ML) approaches and a hybrid approach to governance, risk, and compliance (GRC) can improve the ability to prevent and identify phishing emails. Here is a synopsis of how these two strategies might complement one another:

1. A hybrid GRC strategy

Traditional risk management techniques are combined with technology-driven solutions in a hybrid GRC strategy. It consists of the following elements:

Establish thorough policies and procedures that specify security precautions, appropriate technology use, and standards for managing sensitive information. Specific clauses addressing email security, phishing awareness, and incident response should be included in these policies.

a. Risk Evaluation: Perform routine risk evaluations to find weaknesses and threats in the organization's email infrastructure and procedures. Examine the likelihood and potential effects of phishing attempts, taking into account things like staff knowledge, technology safeguards, and prior instances.

b. Monitoring Compliance: Put in place monitoring procedures to make sure security rules and policies are followed. Review access restrictions, incident response processes, and email security controls frequently to spot flaws and implement the appropriate fixes.

d. Incident Response: Create a strategy for handling incidents that are specifically adapted to phishing assaults. Establish roles, responsibilities, and processes for quickly and successfully responding to phishing situations. Include procedures for inquiry, containment, communication, and recovery.

2. Machine Learning for Phishing Email Prevention and Detection:

By analyzing massive amounts of data and finding patterns, anomalies, and signs of phishing assaults, machine learning techniques can improve the detection and prevention of phishing emails. How ML can be used is as follows:

Email headers, body text, attachments, and embedded URLs can all be examined using machine learning techniques. A diversified dataset of well-known phishing emails, genuine emails, and spam that isn't phishing was used to train the ML model. The model can be trained to identify typical phishing traits like suspicious words, misspellings, or peculiar sender addresses.

b. Behavioral Analysis: To create baseline behavior for individuals or groups, ML might examine user behavior, such as email interaction patterns and click rates. Changes from the norm can be noted as possible phishing signs. In order to recognize new phishing patterns and attack methodologies, ML models can also learn from data collected from other organizations.

Implement machine learning (ML) models that can categorize incoming emails in real-time and give them a phishing probability score. To recognize suspicious emails, ML systems can make use of a variety of methods, including Natural Language Processing (NLP), anomaly detection, and pattern recognition.

d. Adaptive Learning: ML models are constantly able to pick up new information and adjust to changing phishing tactics. Regular modifications to the ML algorithms based on emerging trends, patterns, and indications can improve detection and lower false positive rates.

e. Feedback Loop: Create a feedback loop where user reports of occurrences or recognized phishing emails are pushed back into the machine learning system. By learning from fresh phishing attempts and user input, the model is able to constantly advance, increasing its precision and potency over time.

f. Integration with Security Systems: Connect ML-based phishing detection systems to the infrastructure already in place for email security, such as spam filters, firewalls, and endpoint security programs. ML models can supplement rule-based filtering techniques with an additional line of protection. Organizations may take advantage of technology and best practices by combining a hybrid GRC approach with ML-based phishing email prevention and detection approaches. This enables them to proactively identify and neutralize phishing risks. For a successful defense against phishing assaults, regular monitoring, ongoing development, and user knowledge are still essential.

4. RESULT

- To Implementation are efficient model for detecting & preventing phishing attacks.
- To identifying the factors involved in the success of phishing against organizations.

Table 4.1 Descriptive Statistics Implementation are efficient model for detecting & preventing phishing attacks (IEMDP)

	N	Mean	Std. Deviation
E-mail authentication protocol	35	2.25	1.03
phishing email detection	35	2.42	.94
URL analysis	35	2.51	.85
real time blacklist	35	2.57	.69
user awareness & training	35	2.51	.65
security awareness testing	35	2.62	.73
incident responses & reporting	35	2.48	.91
continuous monitoring threat intelligence	35	2.80	1.20
multi-factor authentication(MFA)	35	2.28	.82
regular software update	35	1.57	.94
Valid N (listwise)	35		

Attacks on people and businesses by phishers are getting more and more sophisticated and dangerous. It is crucial to put in place a model that is effective at detecting and preventing phishing attempts in order to counteract these attacks. This table of descriptive statistics demonstrates how such a model's various elements—advanced technology, user education, real-time monitoring, and incident response—are all included. Regular software updates indicate that there may be a lack of advanced software updates rather than other factors, as shown by value 1.57.

4.1 Advanced technological remedies:

For identifying and thwarting phishing assaults, it is essential to implement cutting-edge technological solutions. Strong email security systems with spam filters, antivirus software, and machine learning algorithms are some examples of these solutions. They can be used to scan incoming emails for suspicious patterns or known phishing signs. Additionally, anti-phishing toolbars and plugins that alert users to potentially harmful websites can be added to web browsers. Advanced tools like behavior analytics and artificial intelligence can also be used to proactively spot anomalies and phishing attempts.

1. **User Education and Awareness**: A key element of a successful phishing prevention strategy is equipping users with information and awareness. People should learn about common phishing tactics, how to spot strange emails or messages, and the significance of not clicking on untrusted links or disclosing personal information online through educational programs. Users' capacity to identify and report phishing attempts can be improved through regular training sessions and simulated phishing exercises, which lowers the risk of successful assaults.

2. **Real-Time Monitoring**: To identify and stop phishing assaults, it is crucial to continuously monitor network traffic, email systems, and user activity. With real-time monitoring, suspicious behaviors can be quickly identified, such as odd email patterns, unauthorized access attempts, or strange user behavior. To quickly identify and counteract phishing attempts, security teams can make use of intrusion detection systems, security information and event management (SIEM) solutions, and anomaly detection technologies.

3. Incident Response and Remediation: Effectively addressing phishing attacks requires a well-defined incident response plan. The strategy should specify the actions to be performed, such

as incident containment, investigation, and remediation, in the event of a suspected or verified phishing incident. In order to lessen the effects of the attack, recover compromised systems and data, and stop further attacks, incident response teams should work in tandem with IT departments, legal counsel, and law enforcement agencies, as appropriate.

4. Ongoing Development and Adaptation: Phishing assaults are continually changing, and attackers frequently use fresh methods to get over security barriers. The phishing prevention model must be continuously enhanced and modified as a result. This entails keeping up with the most recent phishing trends, examining attack patterns, and modifying security precautions as necessary. Regular vulnerability analyses and penetration tests can assist find possible system flaws and preventing them from happening.

Table 4.2 Descriptive Statistics Investigation of the Impact of Phishing Attacks(IPAI)

	N	Mean	Std. Deviation
understanding scope	35	2.20	.99
identifying attack vector	35	2.14	1.08
assessing damages	35	2.14	.73
gathering evidence	35	2.22	.84
Valid N (listwise)	35		

Phishing assaults now target both individuals and companies, and they are a pervasive and persistent threat in the digital age. In order to create practical prevention plans and mitigate the effects of these attacks, it is essential to understand their effects. According to descriptive statistics, investigating the effects of phishing attacks by looking at their financial repercussions, reputational damage, legal repercussions, psychological effects on victims, and organization or identifying attack vector is std deviation 1.08 means it some risky and difficult to control as opposed to other means value is showing equal existing impact.

4.2 Financial Consequences:
Phishing attacks can have significant financial consequences for both people and businesses. People who fall prey to phishing scams may suffer immediate financial loss as a result of fraudulent credit card use, unauthorized purchases, or bank account theft. Phishing attacks can cost businesses money because they corrupt client accounts, steal valuable information, or disrupt business operations. Additionally, firms might have to pay for incident response, inquiries, and corrective actions to fix damaged systems and stop further assaults.

4.3 Reputational Damage:
Phishing assaults have the potential to cause serious harm to both people and organizations' reputations. Victims may see the impacted entity as careless or unreliable when personal or financial information is compromised as a result of phishing. Losing customers' trust can result in less positive press, damaged brand reputation, and diminished consumer loyalty. The process of repairing a damaged reputation can be difficult and time-consuming; it calls for open communication, proactive security measures, and regular provision of dependable services.

4.4 Legal Consequences:
Phishing incidents may result in legal repercussions for both victims and corporations. Those who become victims of phishing schemes could have trouble getting their money back or regaining control over their compromised identities. They might also get into legal challenges as a result of dealing with bogus accounts or fixing credit problems. Businesses who do not sufficiently safeguard client data and lessen the effects of phishing assaults risk facing legal repercussions, regulatory penalties, and legal action. To reduce the legal dangers brought on by phishing assaults, compliance with data protection

and privacy legislation is essential.

4.5 Psychological impacts:

Victims of phishing attacks may experience serious psychological impacts. People who have fallen for phishing scams could feel humiliated, angry, or violated of their privacy. Additionally, they might experience worry, mistrust, and a reluctance to participate in online activities. Employees may feel guilty or responsible for failing to stop phishing assaults if their businesses are affected psychologically as well. Psychological consequences might jeopardize people's trust in digital platforms and jeopardize their general wellbeing.

Table 4.3 Descriptive Statistics Potential impact of phishing attacks(PIPA)

	N	Mean	Std. Deviation
data breaches	35	3.60	1.47
financial losses	35	3.82	1.33
business disruption	35	4.14	1.11
reputation damages	35	3.31	1.36
Valid N (listwise)	35		

Business interruptions are valuable The most recent number for the probable impact of phishing assaults is 4.14. Phishing assaults have become a common and constantly changing menace in today's digital environment. These harmful acts seek to lure unsuspecting people into disclosing private information, which could have serious repercussions for both people and businesses. Using descriptive statistics, we may examine the possible effects of phishing assaults and emphasize the dangers of falling for such shady tricks.

Table 4.4 Descriptive Statistics Preventive measure for phishing attacks (PMPA)

	N	Mean	Std. Deviation
Employees education	35	3.20	1.36
technical control	35	3.80	1.18
multi-factor authentication (MFA)	35	4.02	1.04
incident responses & recovery	35	3.80	1.07
continuous monitoring & threa intelligence	35	3.40	1.24
phishing simulation	35	2.85	1.14
Valid N (listwise)	35		

The most common factor for multi-factor authentication (MFA), which has a mean value of 4.02, is used to prevent phishing attempts and Phishing assaults are now a constant and highly advanced menace in the online environment. These assaults are designed to lure unwary people into disclosing sensitive information like passwords, credit card numbers, or personal information. It is essential to put preventive measures in place to shield ourselves and our companies from phishing assaults. A descriptive statistic demonstrates the preventative steps that people and organizations can take to lessen the likelihood that they will fall victim to phishing attempts.

1. Employee Training

Educating people about the traits and typical methods employed by attackers is one of the most effective protective tactics against phishing attempts. Organizations should regularly hold awareness campaigns to teach staff about the risks of phishing, how to spot dubious emails or messages, and how crucial it is to refrain from

clicking on random links or disclosing personal information online. People should also follow reputable sources for information on the newest phishing trends and techniques.

2. Strong Email Security:
Phishing attacks frequently use email as a platform. To stop these assaults, effective email security measures must be put in place. Anti-malware, antivirus, and complex spam filters can all be used to find and block questionable emails. In order to confirm the legitimacy of receiving emails, enterprises should also think about installing email authentication protocols as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).

3. Two-Factor Authentication (2FA):
Enabling two-factor authentication adds another layer of protection and reduces the likelihood that phishing attacks will be successful. Even if attackers manage to gain the login credentials through phishing, they would still be unable to access the account without the second authentication factor thanks to the requirement that users give an additional verification factor, like a special code sent to their mobile devices.

4. Regular Software Updates:
Phishing assaults can be avoided by regularly updating software and programs. Security patches that fix vulnerabilities that attackers might exploit are frequently included in updates. Organizations should develop guidelines to ensure that all software used in their infrastructure, including operating systems, web browsers, email clients, and other applications, receives frequent upgrades. Additionally, if practical, users should activate automatic updates.

5. URL Inspection and Hovering:
Individuals should hover their mouse pointer over links (without clicking) to disclose the actual URL before clicking any links they receive via emails, texts, or social media platforms. This enables visitors to check that the web address points to the correct location. It is advised to avoid clicking on a URL if it seems dubious or strange.

6. Use Strong Password Procedures:
Strong, unique passwords that are updated frequently are essential for thwarting successful phishing attempts. People should avoid using passwords that are simple to guess, use a combination of letters, numbers, and symbols, and avoid using the same password for many accounts. Complex passwords can be created and safely stored with the use of password managers.

7. Encrypted Communication:
When communicating sensitive information online, using encryption technologies like Secure Sockets degree (SSL) or Transport Layer Security (TLS) adds an additional degree of security. In order to ensure encrypted communication between the user's browser and the website's server, websites that handle sensitive data, such as financial institutions or online shopping platforms, should employ HTTPS (Hypertext Transfer Protocol Secure).

- To understand the factors involved in the success of phishing against organizations
- To study and analyze existing techniques against phishing attack

Table 4.5 Correlations

		IPAI	PIPA	IEMDP	PMPA
IPAI	Pearson Correlation	1	-.451**	.468**	.187
	Sig. (2-tailed)		.007	.005	.282
	N	35	35	35	35
PIPA	Pearson Correlation	-.451**	1	-.539**	.167
	Sig. (2-tailed)	.007		.001	.338
	N	35	35	35	35
IEMDP	Pearson Correlation	.468**	-.539**	1	.091
	Sig. (2-tailed)	.005	.001		.604
	N	35	35	35	35
PMPA	Pearson Correlation	.187	.167	.091	1
	Sig. (2-tailed)	.282	.338	.604	
	N	35	35	35	35
**. Correlation is significant at the 0.01 level (2-tailed).					

Investigation of phishing attack impact (IPAI) value (-.451**) is negative correlate with Potential impact of phishing attack (PIPA) and sig value (0.007) which is less than 0.05 means if lack of Investigation of phishing attack impact (IPAI) than also gap on Investigation of phishing attack impact (IPAI).

Potential impact of phishing attack (PIPA) value (-.539**) also negative correlate with Implementations are efficient model for detecting & preventing phishing attacks (IEMDP) and sig value 0.001 is less than 0.05 means if Potential impact of phishing attack (PIPA) is downfall than Implementations are efficient model for detecting & preventing phishing attacks (IEMDP) also in downfall.

Investigation of phishing attack impact (IPAI) value (.468**) is positive correlate with Implementations are efficient model for detecting & preventing phishing attacks (IEMDP) and sig value 0.001 is less than 0.05 means Investigation of phishing attack impact (IPAI) significantly effective and change to Implementations are efficient model for detecting & preventing phishing attacks (IEMDP).

Table 4.6 Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.977	49.421	49.421	1.977	49.421	49.421
2	1.112	27.790	77.211	1.112	27.790	77.211
3	.522	13.048	90.259			
4	.390	9.741	100.000			
Extraction Method: Principal Component Analysis.						

77% variances is showing yes there are some potential to preventing phishing attack and this factor working on phishing attack prevention and efficient model for detecting.

Table 4.7 ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	179.612	3	59.871	5.982	.002
	Residual	310.274	31	10.009		
	Total	489.886	34			
a. Dependent Variable: IEMDP						
b. Predictors: (Constant), PMPA, PIPA, IPAI						

In ANOVA is showing that sig value 0.002 mean if organization and software houses working on Potential impact of phishing attack (PIPA), Investigation of phishing attack impact (IPAI) than there are direct significant impact on Implementations are efficient model for detecting & preventing phishing attacks (IEMDP).

➢ To develop an efficient model for detecting and preventing phishing attacks

Developing an efficient model for detecting and preventing phishing attacks involves combining various techniques and approaches. Here are some steps you can follow to develop such a model:

Data Collection: Gather a comprehensive dataset of phishing emails, URLs, and associated features. Include both legitimate and phishing examples to train your model effectively

Feature Extraction: Extract relevant features from the collected data. These features can include email headers, URLs, content analysis, HTML structure, and other characteristics that distinguish phishing attacks from legitimate communication.

Machine Learning Algorithms: Apply machine learning algorithms to train your model on the extracted features. Some commonly used algorithms for phishing detection include decision trees, random forests, support vector machines (SVM), and neural networks. Experiment with different algorithms to find the most effective one for your dataset.

Feature Selection: Use feature selection techniques to identify the most relevant features for phishing detection. This step helps reduce the dimensionality of the data, improve model performance, and reduce training time.

Training and Validation: Split your dataset into training and validation sets. Use the training set to train your model and the validation set to evaluate its performance. Use appropriate evaluation metrics such as accuracy, precision, recall, and F1-score to measure the effectiveness of your model.

Ensemble Methods: Consider using ensemble methods like bagging or boosting to improve the model's performance. Ensemble methods combine multiple models to make predictions, leading to better overall accuracy and robustness.

Real-Time Analysis: Implement real-time analysis of incoming emails or URLs using your trained model. This can be done by integrating your model into an email filtering system or web browser extension. The model can flag suspicious emails or URLs for further investigation or block them directly.

Regular Updates: Phishing techniques evolve over time, so it's important to continuously update and retrain your model with new data. Monitor the performance of your model and incorporate new features or adapt the model as needed to ensure its effectiveness against emerging phishing attacks.

User Education: While the model can help detect and prevent phishing attacks, it's crucial to educate users about phishing risks, how to identify suspicious emails or websites, and best practices for online security. Combine your model with user awareness campaigns and provide educational resources to empower users in recognizing and avoiding phishing attempts.

Feedback Loop: Establish a feedback loop to collect user feedback and reports of potential false positives or false negatives. This feedback can help improve the model's performance and fine-tune its detection capabilities.

Remember that developing an efficient model for detecting and preventing phishing attacks is an ongoing process. As attackers continuously adapt their techniques, it's essential to stay vigilant, update your model, and employ multiple layers of security to mitigate the risks associated with phishing attacks.

5. DISCUSSION

Adopting a successful model for phishing attack detection and prevention necessitates a multifaceted strategy that incorporates cutting-edge technological solutions, user education, real-time monitoring, and fast incident response. Organizations can greatly improve their capacity to recognize and stop phishing assaults by utilizing the power of cutting-edge technology, educating users, monitoring network activity, and having a strong incident response strategy. The model should also be regularly analyzed and updated in order to accommodate changing phishing tactics. By putting such a concept into practice, people and businesses can lower their chance of falling prey to phishing scams and safeguard private data from fraud and illegal access.

The analysis of phishing attacks' results indicates their extensive implications, including monetary losses, reputational harm, legal repercussions, and psychological affects on people and organizations. A complete strategy that incorporates strong cybersecurity protections, employee education and awareness, proactive incident response tactics, and adherence to legal and regulatory standards is needed to prevent and mitigate the effects of phishing attacks. Individuals and organizations can better prepare themselves to defend against these threats, preserve sensitive information, and uphold trust in the digital ecosystem by recognizing the complex impact of phishing assaults.

Phishing assaults present serious threats to both individuals and companies, with possible repercussions ranging from lost money and identity theft to weakened security systems and reputational harm. These attacks have an effect on people's trust, privacy, and general well-being in addition to causing immediate financial and operational difficulties. To lessen the potential effects of phishing assaults, it is critical for individuals and organizations to exercise vigilance, educate themselves about phishing dangers, and put strong preventive measures in place. We may better safeguard ourselves and our digital environments from the negative effects of phishing attempts by taking proactive actions.

Phishing attacks continue to be a serious hazard to both people and businesses. Our defenses against phishing attempts can be strengthened by putting these preventive measures into place. Key strategies for reducing the danger of falling victim to phishing attacks include education, email security, two-factor authentication, routine software upgrades, URL inspection, strong password practices, and encrypted communication. In an increasingly linked digital environment, we can protect our private information by being alert and taking certain precautions.

Several variables can affect how successful phishing attacks against corporations are. Here are some important things to think about:

1. Social engineering: Phishing attacks frequently include social engineering strategies to persuade victims to act in the attacker's favor. The effectiveness of phishing assaults can be greatly impacted by elements including the attacker's capacity to write persuasive messages, exploit psychological weaknesses, and instill a sense of urgency.
2. Phishing emails' sophistication: How well phishing emails imitate real correspondence determines how effective they are. The success rate can be increased by elements including the email's design quality, inclusion of official logos or branding, proper grammar and spelling, and language.
3. A focused strategy: Phishing assaults can be broad-based or very specific. Targeted assaults, often known as spear phishing, involve specially written communications that are addressed to particular people or organizational divisions. The likelihood of success increases with the personalization and relevance of the phishing emails.
4. Knowledge and awareness: Employee cybersecurity awareness levels are vital in the fight against phishing scams. The success rate of phishing efforts can be greatly decreased if personnel are trained to recognize phishing emails, comprehend common attack techniques, and adopt effective security practices.
5. Technical defenses: Businesses that have strong technical safeguards in place can lessen the effects of phishing attempts. The likelihood of

successful phishing attacks can be decreased by taking precautions like spam filters, email authentication protocols (such DMARC, SPF, and DKIM), web filtering, endpoint protection, and anti-phishing solutions. These measures can detect and prevent malicious emails or websites.

6. Human vulnerability and error: Despite technical defenses, human error still contributes significantly to the effectiveness of phishing assaults. Attackers prey on human weaknesses like curiosity, fear, or trust to manipulate victims into divulging private information or carrying out unlawful deeds. One employee falling for a phishing scam is all it takes for a breach to happen.

7. Relevance and timeliness: Phishing attempts frequently take advantage of recent events, such as significant holidays, world news, or particular business trends. To boost their chances of success, attackers may create phishing emails that make use of certain current events. The email's relation to the recipient's job or other obligations within the company might also strengthen the attack's credibility.

8. Collaboration and information sharing: Businesses that actively inform their staff members and fellow professionals about phishing attempts, signs of compromise, and new dangers can fortify their group defenses. Phishing strategies can be recognized and avoided by people and organizations with timely awareness and knowledge of them.

9. The effectiveness of phishing assaults depends on a number of elements, and it might differ from one firm to another. The likelihood of successful phishing assaults can be drastically decreased by putting in place a multi-layered strategy that combines technical safeguards, personnel training, and proactive monitoring.

6. CONCLUSION & RECOMMENDATIONS

It is take the following actions to put into practice an effective approach for identifying and avoiding phishing attacks:

Implement email authentication methods like DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These procedures aid in confirming the legitimacy of receiving emails and identifying fake or spoof emails.

2. Phishing email detection: Examine email content and metadata for signs of phishing using machine learning algorithms and techniques for natural language processing. To find patterns, keywords, and other suspicious traits frequently observed in phishing assaults, train the model on a large sample of known phishing emails. The model should be able to identify probable phishing emails and flag them for more research.

3. Implement a system for URL analysis to look at the links that are included in emails or webpages. This system may perform real-time analysis, evaluate the reputation of the URLs, and check them against blacklists to look for indications of phishing, such as redirects to dubious or misleading websites.

4. Real-time blacklists: Use RBLs or reputation-based services to keep a database of well-known phishing domains, IP addresses, and email senders up to date. Incoming emails or links can be compared to these blacklists to help you spot and prevent potentially harmful sources.

5. User awareness and training: Inform staff members and users about phishing assaults, their traits, and typical attack methods. To educate people on the dangers of phishing, teach them to spot dubious emails or websites, and urge them to report possible phishing efforts, hold frequent training sessions.

6. Test employee training and understanding of security issues by conducting frequent phishing simulation exercises. In these simulations, fake phishing emails are sent to employees, and the replies are tracked. You can pinpoint regions that need more training and strengthen security measures by examining the findings.

7. Incident reaction and reporting: Set up explicit incident response protocols for dealing with reported cases of suspected phishing. Encourage staff members to immediately report any suspicious emails or events so that the proper precautions can be taken, such as quarantining or blocking malicious communications, looking into the source, and taking corrective action.

8. Continuous monitoring and threat intelligence: Set up a system to continuously monitor user

behavior, network logs, and email traffic in order to spot any suspicious or anomalous activity that could be a sign of phishing attempts. By subscribing to trustworthy security feeds and exchanging information with peers in the sector, you can keep up with the most recent threat intelligence.

9. Multi-factor authentication (MFA): Make multi-factor authentication available for sensitive data and critical systems. MFA increases security by asking users to submit additional verification in addition to their password, such as a special code texted to their mobile device.

10. Consistent software updates and patch management: Keep all programs and software up to current with the most recent security patches and fixes. Updating software on schedule is crucial for ensuring a safe environment since phishing attacks frequently take advantage of flaws in older software.

Keep in mind that no one solution can ensure complete security from phishing attempts. To build a strong defense against phishing, it's essential to adopt a combination of technical restrictions, user education, and proactive monitoring. Review and refine your strategy frequently in light of new threats and evolving attack methods.

A critical component of cybersecurity is the analysis of the effects of phishing attacks and their prevention. Let's talk about the importance of looking into phishing attacks, the potential effects they may have on businesses, and what steps may be taken to prevent them.

1. Examining the Effects of Phishing Attacks:

Conducting a comprehensive investigation is crucial following a phishing attempt for a number of reasons:

Understanding the scope of the breach is made easier by looking into phishing attacks. It entails counting the number of impacted people, compromised systems, and any potentially stolen or accessed sensitive data.

a. Determining the Attack Vector: Investigations can shed light on the precise methods and techniques employed by attackers, such as the kind of phishing email used, the social engineering strategies used, or the malicious URLs used. Organizations can improve their security measures and implement targeted countermeasures by having a better understanding of the threat vector.

c. Evaluating Damages: Organizations can evaluate the harm done in terms of monetary losses and reputational damage by looking at the effects of phishing attacks. For the purpose of informing impacted parties, according to legal duties, and putting incident response plans into effect, this information is essential.

d. Gathering Evidence: An investigation is essential for gathering data that may be required for court cases or for reporting the occurrence to law enforcement. To create a case and hold the guilty parties accountable, the attack's impact and proper documentation are essential.

2. Potential Effects of Phishing assaults: Organizations may suffer serious repercussions from phishing assaults, including:

a. Data Breach: Phishing attempts that are successful can give third parties access to sensitive data, including personal information, financial information, or intellectual property. Financial losses, legal fines, and reputational harm to a business may follow from this.

b. Financial Losses: Phishing attacks have the potential to cause financial losses through a number of different channels, including ransom demands, illegal access to financial accounts, and fraudulent transactions. Direct financial expenses for incident response, cleanup, and recovery may be incurred by organizations.

c. Business Disruption: Phishing attacks have the potential to completely corrupt systems, cause downtime, and productivity losses in businesses. Customers' trust and satisfaction may suffer as a result, having a substantial negative financial and operational impact.

d. Reputational Damage: A successful phishing assault can harm a company's reputation by undermining stakeholders' and partners' trust. The retention of customers, the viability of commercial partnerships, and market competitiveness can all be negatively impacted by a reputational loss.

3. Defense Against Phishing Attacks:

Employing proactive preventive measures will help firms reduce the risks phishing attacks pose:

a) Employee training should be conducted on a regular basis to inform staff members about phishing scams, their traits, and how to spot and report dubious emails and websites. Employee education and awareness are essential for thwarting successful phishing efforts.

b) Implement technical controls including spam filters, web filters, email authentication protocols, and endpoint protection to identify and stop phishing emails and harmful websites. Apply security updates and update software frequently to fix flaws that hackers might exploit.

c) c. Multi-Factor Authentication (MFA): To provide an additional layer of security, enable MFA for sensitive data and essential systems. Even if login credentials are stolen as a result of a phishing attack, MFA lowers the danger of illegal access.

d) d. Incident reaction and Recovery: To ensure a prompt and well-organized reaction to phishing incidents, develop and test incident response protocols. This covers protocols for containment, research, dialogue, and recovery.

a. Continuous Monitoring and Threat Intelligence: Use security monitoring technologies to find suspect network activity, irregular activity, or other signs of compromise. Utilize information-sharing platforms and trusted security feeds to stay up to date on the most recent threat intelligence.

e) Phishing Simulation and Testing: Run routine phishing simulation tests to evaluate the success of security awareness training and pinpoint areas that need improvement. These imitations assist in reinforcing

REFERENCES

Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2020). Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management. https://doi.org/10.1108/JEIM-01-2020-0036

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 1–39. https://doi.org/10.3390/fi12100168

Aljofey, A., Jiang, Q., Qu, Q., Huang, M., & Niyigena, J. P. (2020). An effective phishing detection model based on character level convolutional neural network from URL. Electronics (Switzerland), 9(9), 1–24. https://doi.org/10.3390/electronics9091514

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. IEEE Communications Surveys and Tutorials, 15(4), 2070–2090. https://doi.org/10.1109/SURV.2013.030713.00020

Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network., March, 61–72. https://doi.org/10.47893/ijssan.2022.1221

Bagui, S., Nandi, D., Bagui, S., & White, R. J. (2021). Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding. Journal of Computer Science, 17(7), 610–623. https://doi.org/10.3844/jcssp.2021.610.623

Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020, November. https://doi.org/10.1109/INMIC50486.2020.9318210

Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2022). Cloud-based email phishing attack using machine and deep learning algorithm. Complex and Intelligent Systems. https://doi.org/10.1007/s40747-022-00760-3

Cheena, M., & Rammohan, D. S. R. (2023). Detection and Prevention of Phishing Attacks in DDoS Using Collaborative Learning Algorithm. International Journal for Research in Applied Science and Engineering Technology, 11(2), 747–750. https://doi.org/10.22214/ijraset.2023.48906

Choi, K., Chung, K., & Shin, D. (2013). A Study of Prevention Model the Spread of Phishing Attack for Protection the Medical Information.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012). The influences of social networks on phishing vulnerability. Proceedings of the Annual Hawaii International Conference on System Sciences, 2366–2373. https://doi.org/10.1109/HICSS.2012.657

Crawford, M., Khoshgoftaar, T. M., Prusa, J. D., Richter, A. N., & Al Najada, H. (2015). Survey of review spam detection using machine learning techniques. Journal of Big Data, 2(1). https://doi.org/10.1186/s40537-015-0029-9

Fang, Y., Zhang, C., Huang, C., Liu, L., & Yang, Y. (2019). Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism. IEEE Access, 7, 56329–56340. https://doi.org/10.1109/ACCESS.2019.2913705

Guangjun, L., Nazir, S., Khan, H. U., & Haq, A. U. (2020). Spam Detection Approach for Secure Mobile Message Communication Using Machine Learning Algorithms. Security and Communication Networks, 2020. https://doi.org/10.1155/2020/8873639

Hota, H. S., Shrivas, A. K., & Hota, R. (2018). An Ensemble Model for Detecting Phishing Attack with Proposed Remove-Replace Feature Selection Technique. Procedia Computer Science, 132, 900–907. https://doi.org/10.1016/j.procs.2018.05.103

IET Information Security - 2023 - Prabakaran - An enhanced deep learning-based phishing detection mechanism to effectively.pdf. (n.d.).

Islam, S., Hasan, M. M., Sakib, M., & Mazumder, I. (2023). Phishing Attack Detecting System Using DNS and IP Filtering. April. https://doi.org/10.51983/ajcst-2023.12.1.3552

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). Social Phising. School of Informatics Indiana University, Bloomington, 2005, 1–10.

Jakobsson, M. (2005). Modeling and preventing phishing attacks. Lecture Notes in Computer Science, 3570, 89. https://doi.org/10.1007/11507840_9

Kalabarige, L. R., Rao, R. S., Abraham, A., & Gabralla, L. A. (2022). Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites. IEEE Access, 10(August), 79543–79552. https://doi.org/10.1109/ACCESS.2022.3194672

Kang, D., Li, X., Stoica, I., Guestrin, C., Zaharia, M., & Hashimoto, T. (2023). Exploiting Programmatic Behavior of LLMs: Dual-Use Through Standard Security Attacks. http://arxiv.org/abs/2302.05733

Karanjai, R. (2022). Targeted Phishing Campaigns using Large Scale Language Models. http://arxiv.org/abs/2301.00665

Khatun, M., Mozumder, M. A. I., Polash, M. N. H., Hasan, M. R., Ahammad, K., & Shaiham, M. S. (2022). An Approach to Detect Phishing Websites with Features Selection Method and Ensemble Learning. International Journal of Advanced Computer Science and Applications, 13(8), 768–775. https://doi.org/10.14569/IJACSA.2022.0130888

Khoei, T. T., Gasimova, A., Ahajjam, M. A., Shamaileh, K. Al, Devabhaktuni, V., & Kaabouch, N. (2022). A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs. IEEE International Conference on Electro Information Technology, 2022-May(May), 279–284. https://doi.org/10.1109/eIT53891.2022.9813826

Kumar, A., Chatterjee, J. M., & Díaz, V. G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering, 10(1), 486–493. https://doi.org/10.11591/ijece.v10i1.pp486-493

Leon, D., Phillip, L., Springer, C., Publishing, I., S, A. S. M., Leon, P. L. De, & Roedig, U. (2023). Detection of voice conversion spoofing attacks using voiced speech ' Detection of voice conversion spoofing attacks using voiced speech ', NordSec 2022 , 27th Nordic Conference on Secure IT Systems , Reykjavik , Iceland , 30 Nov-02 Dec , in H . P . Reiser and M . Kyas (eds) Secure IT Systems , Lecture Notes in Computer version of an article published in Lecture Notes in Computer Authors Original Citation Link to publisher ' s Rights Download date Item downloaded from Detection of Voice Conversion Spoofing Attacks using Voiced Speech.

Li, Y., Yang, Z., Chen, X., Yuan, H., & Liu, W. (2019). A stacking model using URL and HTML features for phishing webpage detection. Future Generation Computer Systems, 94, 27–39. https://doi.org/10.1016/j.future.2018.11.004

Los, U. M. D. E. C. D. E. (n.d.). No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析 Title.

Mbah, K. F., Lashkari, A. H., & Ghorbani, A. A. (2017). A phishing email detection approach using machine learning techniques. World Acad Sci Eng Technol Int J Comput Inf Eng, 4(1).

Moghimi, M., & Varjani, A. Y. (2016). New rule-based phishing detection method. Expert Systems with Applications, 53, 231–242. https://doi.org/10.1016/j.eswa.2016.01.028

Mujtaba, G., Shuib, L., Raj, R. G., Majeed, N., & Al-Garadi, M. A. (2017). Email Classification Research Trends: Review and Open Issues. IEEE Access, 5, 9044–9064. https://doi.org/10.1109/ACCESS.2017.2702187

Neupane, A., Satvat, K., Saxena, N., Stavrinos, D., & Bishop, H. J. (2018). Do social disorders facilitate social engineering? A case study of autism and phishing attacks. ACM International Conference Proceeding Series, 467–477. https://doi.org/10.1145/3274694.3274730

Pallavi, S., Laxmi, K. R., Ramya, N., & Raja, R. (2020). Study and analysis of modified mean shift method and kalman filter for moving object detection and tracking. In Advances in Intelligent Systems and Computing (Vol. 1090). https://doi.org/10.1007/978-981-15-1480-7_76

Pandey, M. K., Singh, M. K., Pal, S., & Tiwari, B. B. (2022). Prediction of Phishing Websites Using Stacked Ensemble Method and Hybrid Features Selection Method. SN Computer Science, 3(6), 1–11. https://doi.org/10.1007/s42979-022-01387-4

Phishing activity trends report. (2022). APWG, 4th Quarter 2021.

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. Handbook of Information and Communication Security, 433–448. https://doi.org/10.1007/978-3-642-04117-4_23

Rashid, J., Mahmood, T., Nisar, M. W., & Nazir, T. (2020). Phishing Detection Using Machine Learning Technique. Proceedings - 2020 1st International Conference of Smart Systems and Emerging Technologies, SMART-TECH 2020, 43–46. https://doi.org/10.1109/SMART-TECH49988.2020.00026

Rathee, D., Computer, S. M.-I. J. of, & 2022, U. (2022). Detection of E-mail phishing attacks–using machine learning and deep learning. International Journal of Computer Applications, 183(1), p.7., 183(47), 975–8887.

Rawal, S., Rawal, B., Shaheen, A., & Malik, S. (2017). Phishing Detection in E-mails using Machine Learning. International Journal of Applied Information Systems, 12(7), 21–24. https://doi.org/10.5120/ijais2017451713

Sarpotdar, S. S. (2022). A Novel Face-Anti Spoofing Neural Network Model For Face Recognition And Detection. ArXiv Preprint ArXiv:2205.11240.

Security and Privacy - 2022 - Almousa - Phishing website detection How effective are deep learning-based models and.pdf. (n.d.).

Shirazi, H., Muramudalige, S. R., Ray, I., Jayasumana, A. P., & Wang, H. (2023). Adversarial Autoencoder Data Synthesis for Enhancing Machine Learning-based Phishing Detection Algorithms. IEEE Transactions on Services Computing, i, 1–13. https://doi.org/10.1109/tsc.2023.3234806

Shmalko, M., Abuadbba, A., Gaire, R., Wu, T., Paik, H.-Y., & Nepal, S. (2022). Profiler: Profile-Based Model to Detect Phishing Emails. http://arxiv.org/abs/2208.08745

Shyni, C. E., Sarju, S., & Swamynathan, S. (2016). A Multi-Classifier Based Prediction Model for Phishing Emails Detection Using Topic Modelling, Named Entity Recognition and Image Processing. Circuits and Systems, 07(09), 2507–2520. https://doi.org/10.4236/cs.2016.79217

Sonowal, G. (2020). Phishing Email Detection Based on Binary Search Feature Selection. SN Computer Science, 1(4). https://doi.org/10.1007/s42979-020-00194-z

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access, 10, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Taloba, A. I., & Ismail, S. S. I. (2019). An Intelligent Hybrid Technique of Decision Tree and Genetic Algorithm for E-Mail Spam Detection. Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019, 99–104. https://doi.org/10.1109/ICICIS46948.2019.9014756

Tinubu, C. O., Falana, O. J., Oluwumi, E. O., Sodiya, A. S., & Rufai, S. A. (2023). PHISHGEM: a mobile game-based learning for phishing awareness. Journal of Cyber Security Technology, 00(00), 1–20. https://doi.org/10.1080/23742917.2023.2167276

Veeramalla, S. T., Bhattacharya, T., & Nutakki, J. (2023). Phishing Websites & Counter Measures. 1–9.

Yerli, E., Senturk, S., & Ibrahim, S. (2017). Email Phishing Detection and prevention by using data mining techniques. In 2017 International Conference on Computer Science and Engineering (UBMK), IEEE, 707–712.

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2022). SoK: Human-Centered Phishing Susceptibility. ACM Transactions on Privacy and Security, 26(3). https://doi.org/10.1145/3575797

Zuraiq, A. A., & Alkasassbeh, M. (2019). Review: Phishing Detection Approaches. 2019 2nd International Conference on New Trends in Computing Sciences, ICTCS 2019 - Proceedings. https://doi.org/10.1109/ICTCS.2019.8923069