International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

SECURITY IN SOCIAL MEDIA: AWARNESS OF PHISHING ATTACKS TECHNIQUES AND COUNTER MEASURES

Assistant Professor Mr. Umesh T

Sindhu BR, Nihal Waseem, Rakshith R, Sainath Jadhav

Department of Computer Science and EngineeringRajiv Gandhi Institute of Technology

Bangalore-560032, Karnataka

Abstract - As time and technology progresses, the social media security is one of the basic and most important aspects to consider when browsing the internet.Nowadays all people using social media mostly, using social media is widely spread among different age groups to meet several purposes including education, entertainment, or even pursue a research. With the increase of using smartphones and social media, the cyber security threats also increased. The most widely-perpetrated form of social media attacks is phishing; it is used to gather sensitive personal and professional information such as social security numbers, credit card numbers, bank account numbers, user logins and passwords, as well as other information entered through a web site or online sources. Furthermore, many users of different age groups and mainly the old age people have been exposed to social media security violations most times due to a lack of awareness about phishing attacks and how to address with them. Our paper focuses primarily to make people of all age group aware of exposure to this type of attack while using social media networks.

***Key Words*:** Cyber security, Social media, Phishing attack

1. INTRODUCTION

Social media is the most widespread and usage platforms that allow a lot of individuals to contact with each other. The rate of using social media is amazingly and substantially growing nowadays; it has become a common phenomenon for billions of people around the world between all the age groups. Examples of social media platforms: Facebook, Twitter, LinkedIn, Instagram.

As the growth of social media usage as increased over the years as of 2024, the security-threatening issues are more intense than past to the covid pandemic arrival in social media including cyber threats, such as malicious software (malware), unsolicited e-mail (spam), monitoring software (spyware), social engineering and online identity theft (phishing).

The simplest method of acting is cheating people therefore impersonating someone's identity, to steal sensitive information. To illustrate, the operator in a security uniform can ask people the national personal and professional identity without suspicious him/her, or the operator can be disguised as an employee in a bank can ask the clients a secret information. In the world of social media, there are persons who have malicious intentions to trick users by getting their money or assets by impersonating someone's identity or facility's. Correspondingly, the online fraudulent act that trick users and to get their secrecy information is known as phishing.

A phishing is a cyber security-attack that uses the integration of social engineering and technical spoofing to conviction the online users. Social engineering is a use of propaganda by an authorities of a government and manipulative manner aims to get the users identity or confidential information; it tends to entice users into disclosing data by using the fraud emails, unreal SMS, fake websites, etc. Instead, spoofing techniques include the malicious software that plant onto computers to steal credentials directly without the owner's knowledge such as keyloggers, content injection, etc.

2. Body of Paper

Moreover, as social media continues to evolve and integrate into various aspects of daily life, ensuring the security and integrity of these platforms is paramount for maintaining trust and confidence among users. By shedding light on the sophisticated tactics employed by attackers and identifying proactive strategies to mitigate these threats, this project aims to empower individuals and organizations with the knowledge and tools needed to safeguard their online presence. At the first checkpoint, here the phishing attack entrance, we place a step wise security: Link Spoofing ,Link Manipulation and Fake profiles. For social media companies, the presence of security vulnerabilities poses significant business risks, including legal liabilities, financial penalties, and damage to brand image. Investing in security measures is a proactive approach to mitigating these risks.

Email Phishing detection For email phishing detection, the system will analyze email content to flag potential phishing attempts, identifying suspicious URLs and calculating a spam score based on factors like misspellings, urgency phrases, and offers. Users will receive clear notifications indicating whether the email is deemed phishing. SMS Phishing detection Regarding SMS phishing detection, similar processes will occur, with the system analyzing SMS content for potential threats and calculating spam scores based on similar criteria as email phishing . URL Phishing detection URL phishing detection will involve users inputting URLs for analysis, with the system checking them against a whitelist of trusted domains and analyzing for urgency or offer phrases to gauge phishing risk. Machine learning spam classification In terms of machine learning spam classification, the system will implement a Naive Bayes model trained on labeled data, capable of making predictions on new messages and computing performance metrics like precision, recall, and F1-score. Visualization of the confusion matrix will aid in understanding model performance.

The system aims for optimal performance, ensuring timely results especially in email and SMS phishing detection by efficiently analyzing message content and URLs. Machine learning model predictions are designed to handle large datasets effectively, maintaining responsiveness even with increased data volumes. Comprehensive documentation and comments accompany the codebase, facilitating future updates and maintenance tasks for developers. Compatibility across platforms and devices is ensured to maximize accessibility for users. Thorough testing is conducted on various browsers and operating systems to guarantee consistent performance across different environments.

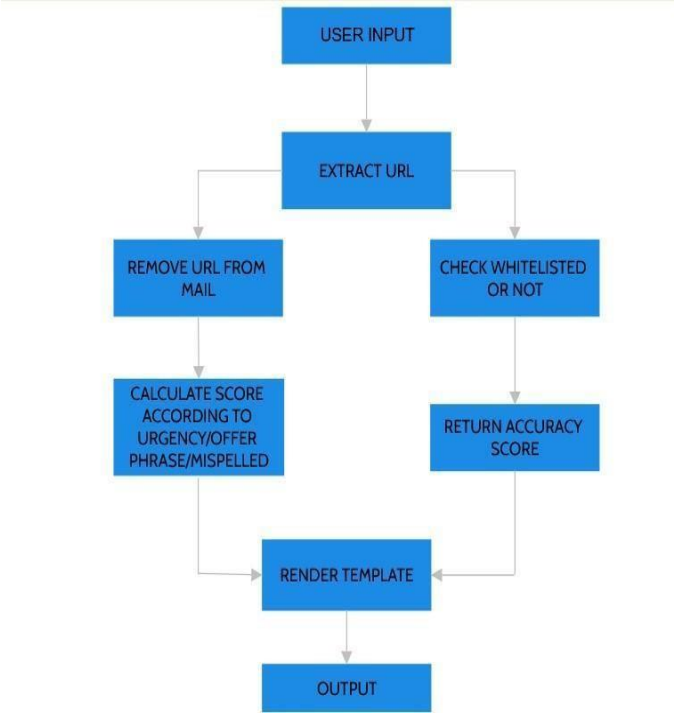

Figure -1: System Desgin

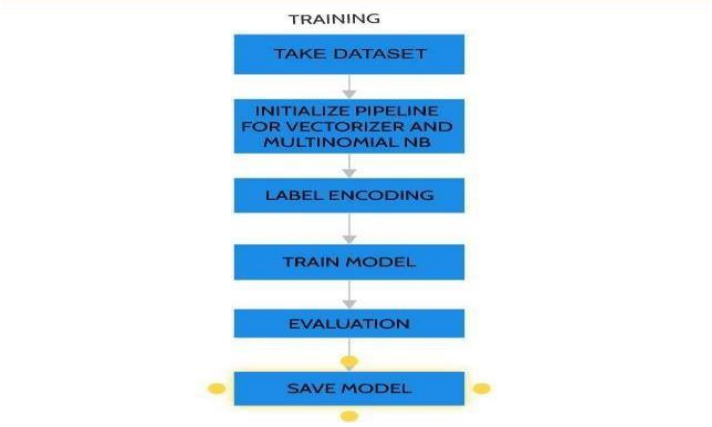

Figure-2:Email Phishing Machine Learning Training

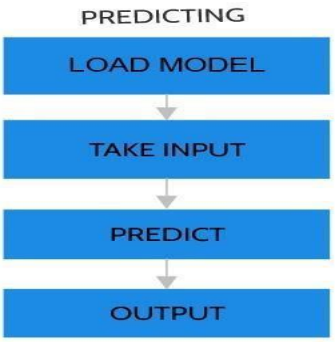

Figure-2:EmailPhishing Machine Learning Predicting

RELATED WORKS

Therefore, in this section we collected significant studies about phishing attack.highlighting methodical and comprehensive phishing approaches review.
The study authors illustrated the different types of phishing and awareness of phishing techniques. They mentioned three components of phishing techniques that are the medium of phishing, which is the fundamental means of the phishing attacks to arriving the victims, where there are three mediums of the attackers to be able to near their possibility victims: internet, voice and short messaging service. The second component is the vector to transmit the attack that is deployed by attackers the mediums for launching the phishing attacks such as fax, email and instant messaging. Moreover, the last component is the technical approaches that used over the attack. These technical approaches are: Browser vulnerabilities,Clickjacking,Cloudcomputing,Malvertising,Man-in-the-Middle (MITM), java-script obfuscation, Spear phishing, Whaling, Typo-squatting and Structured Query Language (SQL) injection.

In the one of the commonest phishing methods occurs when you click on the fake link that connects the victim with any type of phishing. They suggested a approach using an artificial neural network model to classify the Uniform Resource Locator (URL) into a non-phishing URL or a phishing URL.The neural network is a digital model of the brain that is affected by how biological neurons interpret data to solve human problems. ANN equipped to improve particle swarm optimization.The researcher use a URL dataset, which is a mixture of phishing and non-phishing URLs and tablel of some attributes. And they run the model on the number of hidden layers, the output layer, on various teaching ratios and multiple activation functions.For the evaluation of the artificial neural network with particle swarm optimization (ANN PSO) model, accuracy and RMSE parameters were selected.

In terms of accuracy with respect to the Back Propagation Neural Network(BPNN), the ANN-PSO model offers better preparation. The comparison of BPNN & NN-PSO was shown in this paper and the MSE value and accuracy were shown in Figure 2-3 for each pair of activation functions. The results showed that for training neural network models, the NN PSO method performs better than the BPNN for training neural network models.

proposed the deep learning model named THEMIS that employs improved recurrent convolutional neural network (RCNN) model with multilevel vectors and attention mechanisms in the header and the body to model the email header and the email body at both the character level and the word level to detection phishing email. The authors build the model to analyze the email structure, using Word2Vec and mine the text features from four more detailed parts: the email header, the email body, the word-level, and the char-level. This way, it captures the deep underlying semantics of the phishing emails efficiently.

The THEMIS model obtains a promising result. That the overall accuracy of THEMIS reaches that the filter can identify phishing emails with high probability and filter out legitimate emails as little as possible However, email formatscan be casily manipulated with time by the attackers, which renders traditional method inefficient.

MODULES INVOLVED

Email Phishing Detection:The Email Phishing Detection encompasses several key components aimed at identifying potential phishing attempts within email communications. Firstly, the Text Preprocessing submodule ensures that the email text is appropriately cleaned and prepared for analysis. This involves tasks such as removing HTML tags, extracting email headers, and tokenizing the text into individual words. Next, the URL Extraction component is responsible for identifying and extracting any URLs embedded within the email content, which is essential for further analysis of potentially malicious links. Lastly, the Spam Score Calculation submodule determines the likelihood of the email being a phishing attempt by calculating a spam score based on various factors such as misspelled words, urgency phrases, offer phrases, and other suspicious patterns.

Machine Learning Spam Classification:In the Machine Learning Spam Classification, textual data is preprocessed to prepare it for training the machine learning model. This involves tasks such as tokenization, vectorization, and feature extraction. The model is then trained using the Naive Bayes algorithm on labeled data to distinguish between spam and non-spam messages. Once trained, the model is used to make predictions on new messages, and performance metrics such as

precision, recall, and F1-score are calculated to evaluate its effectiveness in classifying spam.

SMS Phishing Detection:The SMS Phishing Detection operates on SMS messages, employing similar processes to analyze and detect potential phishing attempts. It also includes Text Preprocessing, URL Extraction, and Spam Score Calculation submodules to clean and preprocess the SMS content, extract URLs, and calculate a spam score based on various criteria.

URL Phishing Detection:The URL Phishing Detection focuses specifically on analyzing URLs to identify potential phishing sites. It checks the input URL against a whitelist of trusted domains and conducts Suspicious Phrase Analysis to identify suspicious phrases or characteristics commonly associated with phishing attempts, such as urgency phrases, offer phrases, or patterns indicative of malicious intent. Bank Vault Security System User Interface: The User Interface Module facilitates interaction with the system through a user-friendly web-based interface developed using Flask. It handles input and output, allowing users to input email content, SMS messages, or URLs and receive analysis results indicating the likelihood of phishing or spam. The interface provides clear and informative feedback, enhancing user understanding of the analysis results.

IMPLEMENTATION

Building Blocks are Flask: The application leverages Flask, a lightweight web framework, to construct its core structure.Flask facilitates handling user interactions, routing requests to appropriate functions, and rendering web pages.Natural Language Toolkit (nltk): This library provides tools for text processing tasks like tokenization (splitting text into words), stop word removal (eliminating common words like "the" and "a"), and spell checking. These functionalities are crucial for analyzing email content for signs of phishing.Regular Expressions: The application utilizes regular expressions for pattern matching within text. This is particularly useful for URL validation (ensuring the URL format is valid) and domain name extraction (identifying the website's address) when analyzing email content and classifying URLs.URL Parsing: The urllib.parse library is used to break down URLs into their individual components, such as scheme (http/https), hostname (domain name), and path. This breakdown allows for more granular analysis of the URL and identification of potentially suspicious elements.

Email Spam Score Calculation involves Preprocessing: The email content undergoes preprocessing steps like tokenization and stop word removal. This helps focus the analysis on relevant keywords and reduces noise from common words. Urgency/Offer Phrases: The function checks the preprocessed text for predefined lists of urgency-inducing or promotional phrases commonly used in phishing attempts. Phrases like "urgent action required" or "limited time offer" can raise suspicion. Misspelled Words: The application employs a spell checker within nltk to identify potentially misspelled words in the email content. Phishing attempts often contain grammatical errors or typos, which can be indicative of malicious intent. The is spam function assigns a score based on the number of detected urgency/offer phrases and misspelled words. This score contributes to the overall phishing score.

URL Classification involves Bank wl: Sees rite function first compares the URL against a trusted list (whitelist) of safe websites, URLs on the whitelist are deemed safe and categorized accordingly .Domain Name Checks: If the URL isn't whitelisted, the function examines the domain name for suspicious patterns. This could involve checking for keywords or patterns commonly associated with phishing attempts. Based on the whitelist check and domain name analysis, the check _url function assigns a classification label to the URL, such as "whitelisted and safe" or "Suspicious domain name".

Phishing Score and Message involves Details Generation: Along with the final phishing score, the function can provide a breakdown of the contributing factors, such as the presence of urgency/offer phrases, misspelled words, and any suspicious aspects identified in the URL analysis and alert the user for an phishing attempt. Web Application Functionality: The application offers various functionalities through its routes defined in Flask:Home Page (): This is the starting point, allowing users to select the type of phishing attempt they want to analyze (email, SMS, or URL).Email Analysis (/email_phishing): Users can paste the email content into a text box for analysis. Based on the calculated phishing score and details, the application displays a clear

message like "This Email Is Not Phishing," "Proceed with Caution," or "This Email Is Phishing."URL Classification /url_phishing): Users can enter a URL for classification. The application categorizes it as "whitelisted and safe" or provides details about suspicious aspects, including a score indicating the Likelihood of being phishing

RESULTS

The effectiveness of phishing attacks can vary depending on various factors such as the sophistication of the attack, the vigilance of the target, and the security measures in place. Here are some general observations about the security of phishing:Success Rate: Phishing attacks can be highly successful, especially if they are well-crafted and target unsuspecting individuals or organizations. Social engineering techniques used in phishing emails, texts, or phone calls can trick even cautious users into divulging sensitive information. Mitigation Measures: However, organizations and individuals have implemented various mitigation measures to combat phishing. These measures include email filtering systems that detect and block phishing emails, security awareness training for employees to recognize phishing attempts, and multi-factor authentication to protect against unauthorized access even if credentials are compromised. Evolution of Tactics: Phishing tactics continue to evolve, with attackers constantly refining their methods to bypass security measures and exploit human vulnerabilities. This includes spear phishing, which targets specific individuals or organizations with personalized messages, and smishing, which involves phishing via SMS or text messages. Collaborative Efforts: Collaboration between organizations, cybersecurity professionals, and law enforcement agencies has also played a significant role in improving the security posture against phishing. Information sharing about new phishing techniques and indicators of compromise helps to detect and mitigate attacks more effectively. User Education: User education remains a crucial aspect of phishing defense. Teaching individuals how to recognize phishing attempts, verify the authenticity of communications, and report suspicious activities can significantly reduce the success rate of phishing attacks. Overall, while phishing remains a prevalent cybersecurity threat, proactive security measures, ongoing education, and collaborative efforts can help mitigate its impact and protect individuals and organizations from falling victim to these attacks.

CONCLUSION

In conclusion, while phishing attacks continue to pose significant security risks, proactive measures can effectively mitigate their impact. By implementing a multi-faceted approach that includes technological solutions, user education, and collaborative efforts, organizations and individuals can enhance their defenses against phishing attempts.Technological solutions such as email filtering systems and multi-factor authentication play a crucial role in detecting and preventing phishing attacks before they cause harm. These systems can help identify suspicious emails, links, or attachments, reducing the likelihood of users inadvertently disclosing sensitive information.User education is equally important in strengthening security against phishing. Teaching individuals how to recognize common phishing tactics, verify the authenticity of communications, and report suspicious activities empowers them to become active participants in safeguarding their personal and organizational information.Furthermore, collaborative efforts among organizations, cybersecurity professionals, and law enforcement agencies enable the sharing of threat intelligence and best practices, enhancing the collective ability to detect and respond to phishing attacks effectively.While phishing attacks may continue to evolve in sophistication, a proactive and collaborative security approach, coupled with ongoing user education, can significantly reduce the success rate of these attacks and help protect against potential data breaches, financial losses, and reputational damage.

REFERENCES

[1] Zephoria, The Top 20 Valuable Facebook Statistic. https://zephoria.com/top-15-valuable-facebook-statistics/(30-10- 2020)

[2] Anti-Phishing Working Group (APWG) Apwg trends report q1 2020. https://apwg.org/trendsreports/(30-10-2020)

[3] R. Alotaibi, I. Al-Turaiki, and F. Alakeel. "Mitigating Email Phishing Attacks using Convolutional Neural Networks," in Proc. of 3rd International Conference on Computer Applications & Information Security (ICCAIS),2020.

[4] E.D. Frauenstein, and S. Flowerday, “Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model,” 2020.

[5] A.K. Jain, S. Parashar, P. Katare, and I. Sharma, "PhishSKaPe: A Content based Approach to Escape Phishing Attacks,” Procedia Computer Science, vol.171, pp. 1102-1109, 2020.

[6] A.A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A predictive model for phishing detection,” in Proc. Journal of King Saud University-Computer and Information Sciences, 2019.

[7] K.L. Chiew, K.S. Chek Yong, and C. Lin Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” Expert Systems with Applications, vol. 106, pp. 1 -20, 2018.

[8] S. Gupta, and A. Singhal. "Phishing URL detection by using artificial neural network with PSO,” in Proc. 2ndInternational Conference on Telecommunication and Networks (TEL-NET), 2018