Технічні науки

УДК 004.89:004.932.2:004.056.5

Dashevskyi Artem
Independent Researcher
(Ukraine, Kryvyi Rih)
Дашевський Артем
незалежний дослідник
(м. Кривий Ріг, Україна)

NLP METHODS AND LINK ANALYSIS FOR PHISHING DETECTION
МЕТОДИ NLP ТА АНАЛІЗ ПОСИЛАНЬ ДЛЯ ВИЯВЛЕННЯ ФІШИНГУ

Summary. *The article focuses on the use of natural language processing (NLP) methods and link analysis for detecting phishing attacks. It highlights key NLP directions, including text analysis, sentiment detection, and entity extraction. The paper examines the life cycle of phishing attacks and techniques used, such as email spoofing, malicious websites, and social engineering. Statistical insights are provided, emphasizing the growing use of AI and chatbots in enhancing phishing tactics. The study supports the effectiveness of applying machine learning and NLP for user behavior analysis and anomaly detection.*

Keywords: *natural language processing, NLP, phishing, cybersecurity, text analysis, sentiment detection, entity extraction, link analysis, domain reputation, machine learning.*

Анотація. *У статті розглянуто використання методів обробки природної мови (NLP) та аналізу посилань для виявлення фішингових атак. Описано ключові напрями NLP, зокрема аналіз тексту, визначення емоційної забарвленості та вилучення сутностей. Розглянуто життєвий цикл фішингової атаки та способи її реалізації, включаючи підробку*

електронних листів, шкідливі сайти та соціальну інженерію. Наведено статистичні дані та підкреслено зростаючу роль штучного інтелекту й чат-ботів у вдосконаленні фішингових методів. Обґрунтовано ефективність використання методів машинного навчання та NLP для аналізу поведінки користувачів і виявлення аномалій.

Ключові слова: *обробка природної мови, NLP, фішинг, кібербезпека, аналіз тексту, емоційна забарвленість, вилучення сутностей, аналіз посилань, репутація домену, машинне навчання.*

Introduction. This article examines natural language processing (NLP) methods and link analysis as effective tools for detecting phishing attacks. Phishing is one of the most widespread forms of cybercrime, and its successful prevention requires the application of modern technologies. The paper outlines key NLP directions such as text analysis, sentiment detection, and entity extraction.

Web applications accumulate and process significant volumes of user data, which may include confidential or personal information such as names, email addresses, passwords, and credit card details. As the popularity of various electronic services, including medical and banking platforms, continues to grow, so does the volume of collected private information. This attracts the attention of malicious actors seeking access to such data.

The development of the Internet has significantly simplified many aspects of life. As of today, approximately 62.5% of the world's population actively uses the Internet, and the number of users has doubled over the past ten years. In early 2024, the global Internet audience reached 4.95 billion people. The number of social media users also increased by more than 10%, totaling 4.62 billion, which corresponds to 58.4% of the total global population.

Email remains the most vulnerable component of any organization and serves as the entry point for 91% of cyberattacks. A single malicious message can

result in significant financial losses and harm to a company. Such crimes are typically based on principles of social engineering, where attackers impersonate a trusted entity in order to gain access to personal information. Awareness of the principles behind these constantly evolving attacks and understanding the tactics employed are key factors in staying ahead of cybercriminals [1].

Problem Statement. One of the most serious threats faced by users of email and social networks is phishing attacks. Phishing is a cyberattack method in which attackers contact the victim via email or social media platforms, often posing as legitimate organizations such as banks or universities. The purpose of such actions is to prompt individuals to disclose their confidential information, including logins, passwords, and bank card details.

Victims are deceived into clicking malicious links or entering personal data, which can lead to the installation of malware or the leakage of sensitive information. Phishing attacks on large companies often involve highly technological and complex schemes used to penetrate corporate networks as part of larger-scale cyberattacks [2].

The phishing problem remains highly relevant in the context of social media. Despite significant efforts aimed at countering this threat over the years, no definitive solution has yet been found. Since phishing largely relies on social engineering methods, users must exercise particular caution online and stay informed about possible fraudulent schemes. Interestingly, studies show that individuals with a high level of education are most susceptible to phishing attacks. They are also more likely to become targets of such fraud, as they tend to maintain substantial funds in their accounts [3].

There are several technologies that can be used to carry out phishing attacks:

1. **Email spoofing (masquerading):** The attacker sends an email pretending to be a known sender, allegedly requesting confidential information.

2. **Phishing websites:** The attacker creates a webpage that visually mimics the official site of a company or service, prompting users to enter their personal data.
3. **Social networks:** Attackers utilize social media platforms to gather users' personal information, which is then used to generate fake emails or phishing websites.
4. **Malicious software:** Attackers may distribute malware through email that installs itself on the victim's computer and collects confidential data.
5. **Smishing (SMS phishing):** Attackers send text messages to mobile devices requesting users to follow a link or input personal information.

These methods highlight the diversity of approaches employed by cybercriminals to execute phishing attacks and the importance of increased vigilance on the part of users.

Let us suppose that the attack is carried out via email. In this case, the life cycle of a phishing attack can be divided into several key stages:

1. **Planning:** At the initial stage, the attacker identifies the target audience, selects vulnerabilities and attack methods, and determines on behalf of which organization the phishing messages will be sent. It is also important to figure out how to obtain the email addresses of potential victims.
2. **Preparation:** After selecting the target, attackers develop strategies for delivering messages and collecting data. Email addresses are typically used for distribution, and phishing web pages are created to collect information.
3. **Attack:** At this stage, attackers begin sending phishing messages or links to fake websites. The primary goal is to capture the user's attention and trick them into providing confidential information.
4. **Data collection:** Attackers gather the information entered by victims on phishing pages. During this stage, victims may realize they have been attacked and begin taking action to protect their data. Detection may occur either by the victims themselves or by companies that warn their clients of

potential threats. Victims may change passwords, block credit cards, contact support services, or notify law enforcement authorities.

5. **Use of the collected information:** Attackers use the acquired data to carry out unlawful activities, such as making purchases on behalf of the victim or executing other fraudulent schemes.

Conclusion. Thus, cybercriminals distribute emails with the aim of compelling victims to disclose personal information, which is subsequently used to steal their data. The email redirects the victim to a website where they are asked to update their personal credentials (logins, passwords, bank card numbers, etc.). These data are later used by attackers to commit fraudulent activities.

Let us examine the sectors that are most vulnerable to such attacks.

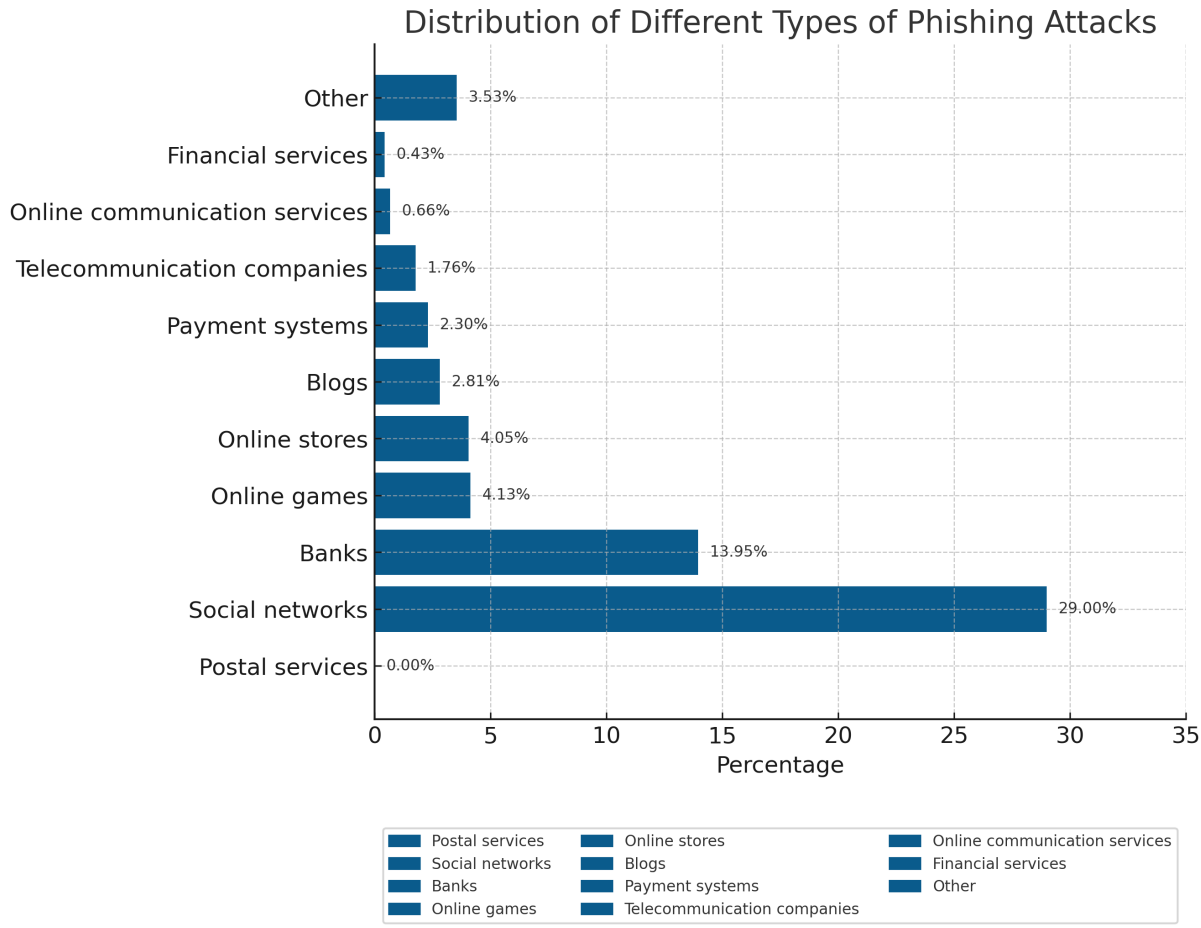

Fig. 1. Distribution of Various Types of Phishing Attacks

Results and Discussion: The number of phishing attacks continues to rise: in 2024, compared to 2023, their volume increased by 33%, and by 72% compared to 2022. These data were presented in a study conducted by experts from Positive Technologies at the Positive Hack Days cyberfestival. In cooperation with specialists from SDM Bank, they analyzed the tools and topics used by attackers [4].

Last year, the largest number of attacks targeted government institutions (15%), industrial enterprises (10%), and IT companies (9%). Hackers' actions can result in various consequences, including theft of confidential information (63%), disruption of organizational operations (28%), harm to state interests (6%), and direct financial losses (5%).

Experts note that targeted attacks are aimed at specific groups of individuals. This approach requires more time and resources from attackers but significantly increases the likelihood of success. Methods used by APT (Advanced Persistent Threat) groups are often employed in such cases. At the same time, the majority of attacks are mass phishing campaigns in which attackers send messages to large numbers of people, hoping that at least a small percentage of them will take the desired action. In these cases, attackers often disguise themselves as well-known brands.

Experts predict that the distinction between mass and targeted phishing will gradually diminish. It is also expected that artificial intelligence (AI) will become an integral part of the attackers' arsenal. Currently, hackers are using AI to generate phishing content, allowing them to make attacks more personalized.

Analysts note that chatbots significantly increase phishing adaptability by modifying language and communication tactics depending on the user's response. According to Positive Technologies, messages from "employers" accounted for 10% of all incidents in 2022–2023, and a similar trend was observed in 2024. In addition, there is a growing use of deepvoices and deepfakes.

According to information from Positive Technologies, 84% of all phishing attacks are conducted via email, far surpassing other channels such as websites (23%) and social networks and messengers (4%). Experts emphasize that effective protection of mail servers requires the implementation of comprehensive information security solutions.

The application of natural language processing (NLP) for detecting insurance fraud involves the analysis of a wide range of unstructured data, such as claims forms, insurance documents, and client correspondence. By leveraging powerful algorithms to process large volumes of information, NLP technologies assist insurance companies in identifying patterns, inconsistencies, and anomalies that may indicate potential fraud.

Natural language processing (NLP) is an advanced artificial intelligence technology that enables machines to understand, interpret, and process human language. It underpins everything from chatbots to search engines and voice assistants [5].

One of the key advantages of NLP lies in its ability to interpret and account for context, making it more effective than traditional rule-based programming methods. Furthermore, NLP can detect subtle nuances and identify implicit inconsistencies. It is also capable of analyzing the sentiment of text, which may serve as an indicator of deception in communication.

NLP enables deeper and more consistent analysis of large data volumes than a human could achieve, significantly reducing the likelihood of overlooking fraudulent activities. This leads to process automation, which in turn accelerates fraud detection and facilitates faster decisions on legitimate claims.

Machine learning (as applied to NLP) can be used to analyze user behavior and detect anomalies or suspicious activity. For example, one can study how a user interacts with a website—their clicks, data entry, and navigation patterns. Based on this data, a profile of normal behavior is constructed, and any deviations from it may signal a potential phishing attack.

Natural language processing (NLP) is a scientific field situated at the intersection of computational linguistics and machine learning technologies. With NLP, computers are trained to engage in dialogues, answer questions, translate texts into various languages, and even generate them from scratch. This technology enables the automation of routine tasks, such as classifying customer support requests by topic or language, greatly simplifying the work of support staff.

One of the key areas of NLP is speech recognition, which enables computers to convert spoken commands into text. This is essential for applications that interact with users through voice, such as smart speakers with voice assistants like Alice.

Natural language generation involves converting structured data—such as tables—into natural language text. This task is the inverse of speech recognition and allows the creation of understandable texts based on numerical or categorical information [6].

Another important task is word sense disambiguation. NLP enables computers to accurately interpret the meaning of words in context. For example, the word "замок" in Russian can refer to either a "lock" (a mechanical device) or a "castle" (a fortified building). The role of NLP is to determine which meaning is intended in a given sentence.

Sentiment analysis is another area where NLP proves its effectiveness. Algorithms can extract subjective characteristics from text, such as emotions, which is useful for marketing and public opinion research.

In addition, machine learning can be applied to analyze the content of phishing emails, web pages, and other online resources. This makes it possible to detect counterfeit logos, spelling and grammatical errors, suspicious links, and other indicators of phishing.

Successful training of machine learning models requires large datasets, including information on known phishing websites and emails. It is also essential

to capture typical user behavior so that this data can be used to train models capable of identifying phishing resources [7].

One of the key advantages of machine learning in the context of phishing detection is the ability of models to update automatically based on new data. This enables them to adapt to constantly evolving attacker techniques and effectively identify new phishing attacks.

Before applying machine learning algorithms, it is necessary to perform data preprocessing. This stage includes cleaning and normalizing the data, as well as removing outliers and irrelevant features, which is essential for improving the accuracy and efficiency of the models.

References

1. A. Mandadi, S. Boppana, V. Ravella, and R. Kavita, "Detection of phishing websites using machine learning," *2022 IEEE 7th International Conference for Convergence in Technology (I2CT)*, Mumbai, India, pp. 1–4, 2022.

2. S. Kuraku and D. Kalla, "Emotet Malware – A Banking Data Stealing Program," *IOSR Journal of Computer Engineering*, vol. 22, pp. 31–41, 2020. [Google Scholar]

3. A. Kulkarni and L. L. Brown, "Detection of phishing websites using machine learning," *International Journal of Advanced Computer Science and Applications*, vol. 10, 2019. https://doi.org/10.14569/IJACSA.2019.0100702

4. D. Kalla and A. Chandrasekaran, "Heart disease prediction using machine and deep learning," *International Journal of Data Mining & Knowledge Management Process (IJDKP)*, vol. 13, no. 3, 2023.

5. A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *Journal of King Saud University – Computer and Information Sciences*, 2023.

6. S. Das Gupta, K. T. Shahriar, H. Al-Qahtani, D. Al-Salman, and I. H. Sarker, "Hybrid feature modeling for phishing website detection using machine learning techniques," *Annals of Data Science*, 2022.

7. D. Kalla, F. Samaa, S. Kuraku, and N. Smith, "Implementing phishing detection using Databricks and artificial intelligence," *International Journal of Computer Applications*, vol. 185, no. 11, pp. 1–11, 2023.

8. P. Gupta and A. Mahajan, "Detection and prevention of phishing attacks using logistic regression," *International Journal of Creative Research Thoughts*, vol. 10, pp. 2320–2882, 2022.

9. T. A. Assegie, "K-nearest neighbors based URL identification model for phishing attack detection," *Indian Journal of Artificial Intelligence and Neural Networking*, vol. 1, no. 2, pp. 18–21, 2021.

10. D. Ahmed, K. Hussein, H. Abed, and A. Abed, "Phishing website detection model using decision tree algorithm and optimal feature selection method," *Turkish Journal of Computer and Mathematics Education*, vol. 13, no. 1, pp. 100–107, 2022.