American Research Journal of Computer Science and Information Technology

Volume 7, Issue 1, 53-57 Pages
Research Article | Open Access
ISSN (Online)- 2572-2921
DOI : 10.21694/2572-2921.24012

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Counteracting Phishing Attacks in Corporate Environments

Avishkar Nikum
CEO, Technotronic Pvt. Ltd., India.

ABSTRACT

The article deals with the actual problem of countering phishing attacks in a corporate environment. The relevance of the topic is due to the rapid increase in the number and complexity of such attacks in the context of the digitalization of business processes, which leads to significant financial and reputational losses for business entities. The goal is to systematize modern scientific ideas in this field and develop an algorithm that allows you to protect your corporate information infrastructure from phishing threats.

The study revealed contradictions between the need to strengthen security measures and maintain the operational efficiency of business processes. In addition, the discrepancies between the pace of development of protective technologies and the evolution of social engineering methods used by intruders are very significant.

It was concluded that effective counteraction to phishing attacks requires integrating advanced technological solutions (machine learning, blockchain, quantum cryptography) with organizational measures, and carefully thought-out educational initiatives. Special attention is paid to the formation of a cybersecurity culture and the introduction of innovative authentication methods.

The article is of interest to information security specialists, IT department heads, and cybersecurity researchers. The presented results can be used in the development and improvement of protection systems against phishing attacks in the corporate sector.

KEYWORDS: *information security, corporate environment, machine learning, multifactorial protection, anti-phishing, social engineering, phishing attacks*

INTRODUCTION

In the era of digital transformations and innovations in the field of entrepreneurship, information security has become a fundamental element in the mechanism of sustainable corporate development. Among the numerous cyber threats, phishing attacks stand out due to their sophistication combined with the potential damage they can cause. Modern researchers are focused on the challenges of developing and implementing methods to counter phishing in corporate environments, with an emphasis on innovative technologies and various organizational measures.

Turning to the formulation of the research problem, it is relevant to highlight that traditional methods of phishing protection demonstrate insufficient effectiveness in countering modern multi-vector and targeted attacks, leading to significant financial and reputational losses for organizations.

The key problem lies in the absence of a holistic, adaptive approach to ensuring the security of the corporate environment from phishing threats, which would take into account both the technological aspects of protection and the human factor. Existing solutions are often fragmented and fail to keep pace with the evolution of social engineering methods employed by attackers.

METHODS AND MATERIALS

The article employs methods of comparison, analysis of modern scientific publications, synthesis, and generalization.

In the scientific literature on the detection and counteraction of phishing attacks, various approaches are utilized by authors, which can be appropriately grouped into several directions.

The first direction, represented by the studies of A.P. Abidoye and B. Kabaso [1], as well as D. Rathee and S. Mann [9], focuses on the application of hybrid and deep machine learning methods for detecting phishing attacks. A hybrid model is proposed, combining several relevant methods.

The second direction is related to the use of meta-learning. For instance, S. Asiri and co-authors [2] proposed the "Phishtransformer" method, which uses a collection of URLs and a transformer to detect phishing, representing a novel approach in this field. H. Zhu describes the nuances of online meta-learning for creating a "firewall" that prevents phishing attacks, allowing the system to adapt to new threats [10].

The third direction unites research developments aimed at reviewing existing methods and classifying them. A. Basit and colleagues conducted a comprehensive analysis of phishing detection methods based on artificial intelligence, highlighting the advantages and disadvantages of specific algorithms [3]. Similarly, S. Chanti and T. Chithralekha classified phishing attacks and provided an overview of the existing approaches to preventing them [4].

The fourth direction is related to the application of specific mathematical methods and models to analyze the dynamics of phishing attacks. For example, M. Dadkhah and co-authors applied wavelet analysis (focused on processing signals, functions that are non-stationary over time and heterogeneous in space) to study the dynamics of phishing threats, which provided additional insights regarding attacks over various time intervals [5].

The fifth direction focuses on considering the human factor in combating phishing. M. Jari emphasizes its importance from the perspective of the emotional component (user training and their reactions to attacks); the author proposed a comprehensive training program to raise awareness [6].

Finally, some scientific works are concentrated on ensuring security in specific contexts. V.K. Prasad and colleagues studied the protection of cloud systems from phishing, proposing enhanced data protection mechanisms in this environment [8]. Meanwhile, G. Mohamed and co-authors proposed a machine learning-based protective method, paying particular attention to ensuring security in corporate systems [7].

Thus, the literature on the stated topic covers a wide range of methodological approaches, each of which contributes valuable insights into the fight against cyber threats.

RESULTS AND DISCUSSION

From a retrospective standpoint, it should be noted that phishing attacks have undergone a relatively long evolutionary path—from primitive attempts to extract confidential data to complex multi-stage operations [2, 6]. Modern attackers employ methods of social engineering, automated tools, and elements of artificial intelligence to create convincing phishing messages. Below (Table 1) are the main properties of phishing attacks in the corporate environment.

Table 1. Systematization of the properties of phishing attacks in the corporate environment (compiled by the author based on [1, 3, 8, 9])

Property	Description
1. Targeted focus	Attacks are often directed at specific employees or departments, such as HR, Finance, or IT, to extract data.
2. Social engineering	Techniques of manipulation are used to compel the victim to voluntarily provide information.
3. Scalability	Attacks can target either a limited number of employees or the entire organization, such as whaling phishing, spear-phishing, or just phishing.
4. Exploitation of trust	Attackers may forge email addresses or websites that the victim perceives as reliable, such as typosquatting.
5. Temporal pressure	False urgent situations are created to push the victim into making decisions without considering the consequences.
6. Technical complexity	Modern attacks rely on sophisticated techniques for masking and bypassing security systems.
7. Financial Consequences	Successful attacks can lead to financial losses, data leaks, or the disruption of business processes.
8. Educational gaps	A lack of awareness among employees about phishing methods increases the risk of successful attacks.

In 2022, APWG logged 4.7 million phishing attacks. Since 2019, the number of phishing attacks has increased by more than 150% yearly [11] (Fig 1).

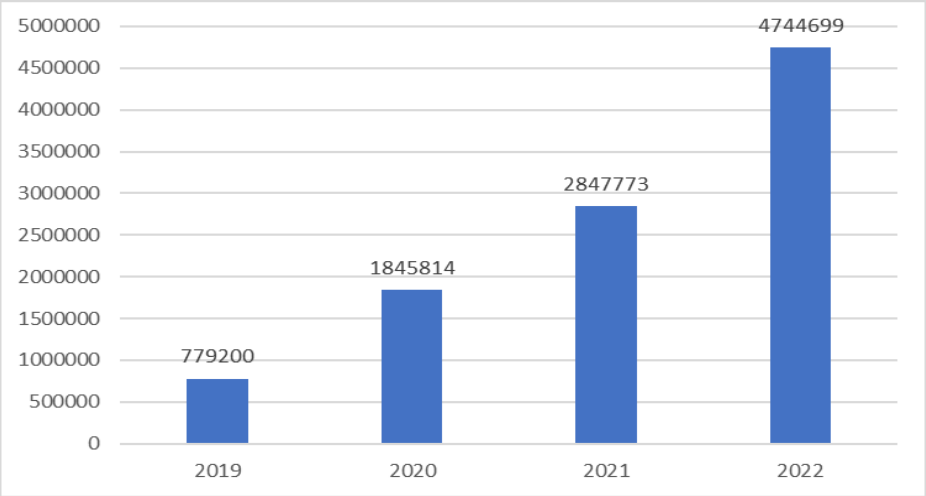

Fig. 1. Growth of phishing attacks by year [11]

Individuals working for educational institutions are most likely to open a phishing email. Healthcare and retail employees are the least likely to do so. Security organizations all have their own service and user bases. As such, when it comes to showing which sectors are targeted by phishing attacks the most, different organizations produce slightly different figures. On the whole, however, the financial sector tends to come out on top as the most attacked sector [11].

Thus, phishing attacks are becoming increasingly sophisticated and pose a significant threat to corporate organizations. Effective protection against them requires not only technical solutions but also continuous staff training. It is essential to now examine and characterize technological solutions, which include:

- machine learning systems for phishing detection;

- blockchain in authentication;

- behavioral pattern analysis.

Machine learning algorithms demonstrate high efficiency in detecting phishing attacks. Neural networks trained on large datasets can identify subtle patterns typical of phishing messages. The implementation of such systems helps to reduce the risk of successful attacks.

In turn, blockchain technology offers additional protection options. Decentralized blockchain-based authentication systems may provide a high level of security for user credentials based on the use case.

Behavioral pattern analysis systems allow the detection of anomalies that may indicate potentially suspicious or malicious activity. The use of clustering algorithms and time series analysis makes it possible to create a unique "digital fingerprint" of each employee's behavior and respond quickly to deviations.

As for organizational measures, they include the following steps and elements:

- the formation and maintenance of a cybersecurity culture;

- the development of a well-thought-out multi-factor authentication policy;

- network segmentation.

Building a culture of cybersecurity is a fundamental element in phishing protection. Regular training, phishing attack simulations, and a reward system for vigilance increase employee awareness.

The introduction of mandatory multi-factor authentication significantly complicates the task for attackers. The use of biometric data, hardware tokens, and one-time passwords creates additional layers of security. Companies that fully adopt such authentication significantly reduce the number of successful phishing attacks.

Finally, proper segmentation of the corporate network limits the potential damage from the actions discussed in this article. Dividing the network into isolated segments with strict access control makes it difficult for attackers to move within the infrastructure, even in cases of compromised individual accounts.

It is also important to focus on several innovative approaches and solutions applied in this field, particularly:

- quantum cryptography;

- neuro-interfaces for authentication [4, 7].

The development of quantum technologies offers new options in the field of phishing protection. Quantum key distribution promises to provide completely secure communication channels, making data interception theoretically impossible. Pilot projects in several technology companies demonstrate the potential of this direction.

Experimental research in the field of neuro-interfaces shows the potential for using unique brain activity patterns for user authentication. Although this technology is in its early stages, it may become a revolutionary tool in the fight against phishing.

A more detailed characterization of new developments is presented in Table 2.

Table 2. Innovative technologies used in the process of countering phishing attacks in the corporate environment (compiled by the author based on [1, 2, 5])

Technology	Advantages	Limitations
1. Artificial Intelligence (AI)	Automatically identifies suspicious patterns in emails, improving phishing detection accuracy.	May result in false positives, and requires continuous learning and data updates to enhance effectiveness.
2. Machine Learning (ML)	Capable of adapting to new threats, improving protection with each new attack.	Requires large datasets for training models and combating constantly evolving attacks.
3. User Behavior Analytics (UBA)	Detects anomalous user actions, helping to identify phishing attacks before completion.	Sometimes leads to false alerts, requiring manual verification.
4. Multi-Factor Authentication (MFA)	Protects accounts even if passwords are compromised by requiring additional authentication methods.	May reduce usability for employees, and if poorly implemented, becomes vulnerable to attacks.
5. DMARC-based Email Protection	Helps prevent domain spoofing and phishing emails, improving the reliability of corporate correspondence.	Requires precise configuration and proper implementation for maximum effectiveness.
6. Sandboxing Systems	Isolates suspicious attachments and links for safe analysis before user interaction.	May slow down message processing and miss sophisticated attacks if their obfuscation is too deep.
7. Message Metadata Analysis	Checks headers and routing data of emails to identify suspicious deviations from the norm.	Unable to detect well-masked attacks using proper headers and routing.
8. Cloud Access Security Brokers (CASB)	Ensures data protection when accessing cloud applications, preventing unauthorized access.	Difficult to integrate with existing corporate systems, and requires significant investment.

As part of this article, an algorithm is proposed that combines modern AI methods with new approaches to enhance phishing detection accuracy, reduce false positives, and improve user experience. The sequence of recommended actions is presented in Table 3.

Table 3. Implementation of the recommended algorithm for countering phishing attacks in a corporate environment (compiled by the author)

Stage	Description of actions
1. Responsible and ethical data collection	Data is collected from all corporate communication channels (email, chats, cloud services, etc.) ethically and responsibly to log all incoming messages, links, attachments, and metadata.
2. Initial filtering with machine learning (ML)	Incoming messages are analyzed based on a trained model to identify those that may pose a phishing risk. Various factors are considered at this stage: anomalies in email headers, mismatches in IP addresses, and behavioral deviations.
3. Detailed content analysis using natural language processing (NLP)	The content of messages is analyzed using natural language processing methods to detect hidden threats, even if the attack is well-masked. This involves analyzing the rhetoric of the message and searching for manipulative or stress-inducing elements (urgency, threats, etc.).
4. User behavior analytics (UBA)	The user's actions are compared with their usual behavior. If the user suddenly opens suspicious attachments, makes unusual transactions, or sends confidential data, an alert is triggered.
5. Multi-factor verification	Multi-factor verification is automatically initiated for any suspicious activity. For example, before opening a link from a questionable email, the user will be prompted to confirm their identity via SMS or using biometrics on a mobile app.
6. Dynamic sandbox with feedback	Suspicious attachments or links are placed in an isolated environment (sandbox), where they are executed or analyzed in real time. The system uses feedback: if a file or link turns out to be safe, the sandbox learns to identify similar cases faster in the future.
7. Automated reports and training	Automated reports on potential threats are generated. These are provided to the IT security department, and training notifications are generated for employees, highlighting the phishing attack signs they encounter.

The novelty of the proposed algorithm is summarized as follows:

1. Many existing solutions rely on ML for message filtering but rarely combine it with content analysis using natural language processing. The proposed algorithm uses NLP to analyze the tone and style of the message, allowing the detection of hidden signs of manipulation. Combined with UBA, this is expected to provide more accurate anomaly detection.

2. Unlike standard sandboxes that simply isolate suspicious objects, the proposed solution is based on a learning system. If the analyzed object turns out to be safe, the sandbox adjusts its models for faster processing in the future, increasing the efficiency of analysis with each iteration.

3. Multi-factor authentication traditionally requires manual input of data by the user. In the proposed algorithm, verification is automatically activated based on risk analysis, reducing the burden on users and minimizing the chances of a successful attack.

CONCLUSIONS

Countering phishing attacks in the corporate environment requires a structured approach that combines advanced technological solutions with well-thought-out organizational measures. Continuous improvement of protection methods, investment in employee education, and the implementation of innovative technologies will enable corporations to effectively combat the growing phishing threat, ensuring security and sustainable business development in the digital age.

Innovative technologies for countering phishing attacks provide numerous opportunities to enhance corporate security. However, each technology has its limitations and requires a well-planned approach for implementation. To achieve maximum protection, businesses must combine various solutions along with continuous training of their employees on emerging threats.

REFERENCES

1. Abidoye A.P. Hybrid machine learning: a tool to detect phishing attacks in communication networks / A.P. Abidoye, B. Kabaso // International Journal of Advanced Computer Science and Applications. – 2020. – Vol. 11. – No. 6. – Pp. 559-569.
2. Asiri S. Phishtransformer: a novel approach to detect phishing attacks using URL collection and transformer / S. Asiri, Ya. Xiao, T. Li // Electronics. – 2024. – Vol. 13. – No. 1. – P. 30.
3. Basit A. A comprehensive survey of AI-enabled phishing attacks detection techniques / A. Basit, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, K. Kifayat // Telecommunication Systems. – 2021. – Vol. 76. – No. 1. – Pp. 139-154.
4. Chanti S. A literature review on classification of phishing attacks / S. Chanti, T. Chithralekha // International Journal of Advanced Technology and Engineering Exploration. – 2022. – Vol. 9. – No. 89. – Pp. 446-476.
5. Dadkhah M. Methodology of wavelet analysis in research of dynamics of phishing attacks / M. Dadkhah, M.D. Jazi, V.V. Lyashenko, Z.V. Deineko, S. Shamshirband // International Journal of Advanced Intelligence Paradigms. – 2019. – Vol. 12. – No. 3-4. – Pp. 220-238.
6. Jari M. A comprehensive survey of phishing attacks and defenses: human factors, training and the role of emotions / M. Jari // International Journal of Network Security & Its Applications. – 2022. – Vol. 14. – No. 5. – Pp. 11-24.
7. Mohamed G. An effective and secure mechanism for phishing attacks using a machine learning approach / G. Mohamed, J. Visumathi, M. Mahdal, J. Anand, M. Elangovan // Processes. – 2022. – Vol. 10. – No. 7. – Pp. 1356.
8. Prasad V.K. Intensify cloud security and privacy against phishing attacks / V.K. Prasad, D. Dansana, B.K. Mishra, M. Bhavsar // ECS Transactions. – 2022. – Vol. 107. – No. 1. – Pp. 1387-1398.
9. Rathee D. Detection of e-mail phishing attacks – using machine learning and deep learning / D. Rathee, S. Mann // International Journal of Computer Applications. – 2022. – Vol. 183. – No. 47. – Pp. 1-7.
10. Zhu H. Online meta-learning firewall to prevent phishing attacks / H. Zhu // Neural Computing & Applications. – 2020. – Vol. 32. – No. 23. – Pp. 17137-17147.
11. Top Phishing Statistics for 2024: Latest Figures and Trends // URL: https://www.stationx.net/phishing-statistics/ (date of application: 10/02/2024).

Citation: Avishkar Nikum, "Counteracting Phishing Attacks in Corporate Environments", American Research Journal of Computer Science and Information Technology, Vol 7, no. 1, 2024, pp. 53-57.