International Journal of Advanced Technology in Engineering and Science
Vol. No. 12, Issue No. 05, May 2024
www.ijates.com
ijates
ISSN 2348 - 7550

A Review on Phishing Attacks and Prevention Techniques

Sujay Kumar Adoor, **Vinith Kalikar,** **Chandan Kumar M,** **Suraj,**

Sujayadur551@gmail.com vinithkalikar6@gmail.com chandankumarm10404@gmail.com the.suraj00@gmail.com

Dr. Pushparani M.K

drpushparani@aiet.org

Abstract:

The growth of online services and internet users in the digital age has led to a change in the way transactions are carried out, with sensitive financial data now moving over the web. A rise in phishing assaults has been caused by this development, too, as it has also made it easier for hackers, bad actors, and intruders to take advantage of weaknesses. Taking on the many facets of phishing attempts, this review study integrates knowledge from several academic publications.

We examine online security in detail, emphasizing the difficulties brought on by the enduring menace of phishing. By means of a review of several research publications, we clarify the different kinds and approaches used in phishing assaults, from traditional to innovative and cutting-edge strategies. We also investigate the technological and economic aspects driving the spread.

KEYWORDS: Internet based security, phishing, detection, system architecture

1. INTRODUCTION:

In an era dominated by the omnipresence of the internet, where connectivity transcends geographical boundaries and transactions occur at the speed of technological innovation, the phenomenon of phishing emerges as a persistent threat to the digital ecosystem. Phishing, a form of cybercrime rooted in deception and manipulation, targets unsuspecting individuals [4] with the aim of extracting sensitive information such as passwords, credit card details, and personal credentials.

The origins of phishing can be traced back to the early days of internet usage, with its first documented instances dating back to the mid-1990s when attackers exploited the trust of America Online (AOL) users to illicitly obtain account credentials. Since then, phishing has evolved into a sophisticated [2] and pervasive threat, leveraging a combination of social engineering tactics and technological subterfuge to exploit human vulnerabilities for financial gain.

The prevalence of phishing attacks underscores the critical need for a comprehensive understanding of its methodologies and countermeasures. As such, this review paper embarks on a journey to dissect the anatomy of phishing, examining its historical evolution, typologies, and impact on individuals and organizations alike [3]. Drawing upon insights from seminal research studies and industry reports, we delve into the intricacies of phishing techniques, ranging from classical email-based scams to modern spear phishing campaigns [4][5].

Moreover, this paper delves into the arsenal of anti-phishing strategies employed to combat this pervasive threat, including technical safeguards, user education initiatives, and legislative measures [7]. By critically evaluating the efficacy of existing countermeasures and identifying emerging trends in phishing tactics, this review aims to equip stakeholders with the knowledge and tools necessary to mitigate the risks posed by phishing attacks in an increasingly interconnected digital landscape.

2. VARIOUS TYPES OF PHISHING:

1. Impersonation Phishing: This involves pretending to be someone else or a legitimate entity to deceive victims. Impersonation tactics often include creating fake websites that closely resemble legitimate ones [5].

2. Forwarding Phishing: Phishers exploit trust in well-known entities like Amazon, eBay, or PayPal by sending fraudulent emails that mimic the appearance of these companies' communications. Victims are directed to fake websites where their credentials are harvested.

3. Clone Phishing: Attackers clone websites that victims usually visit, creating fake login pages to steal credentials. The cloned websites closely mimic legitimate ones to deceive users.

4. Spear Phishing: This targeted form of phishing involves tailoring fraudulent emails to specific individuals or groups, often using personal information obtained through social media or other sources.

5. Phone Phishing (Vishing): Phishers use voice communication, often over VoIP technology, to impersonate legitimate entities and trick victims into divulging sensitive information [8].

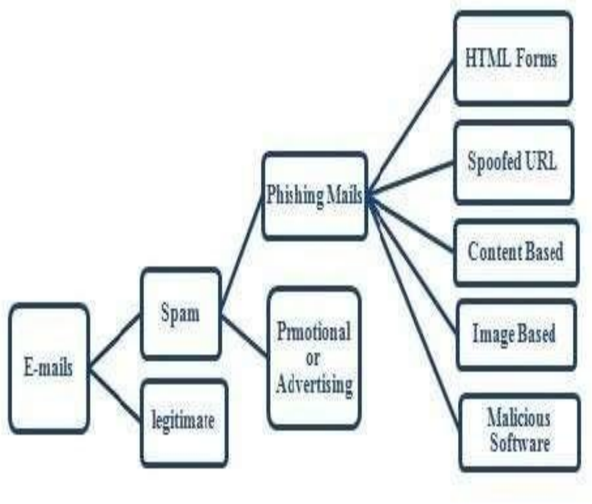
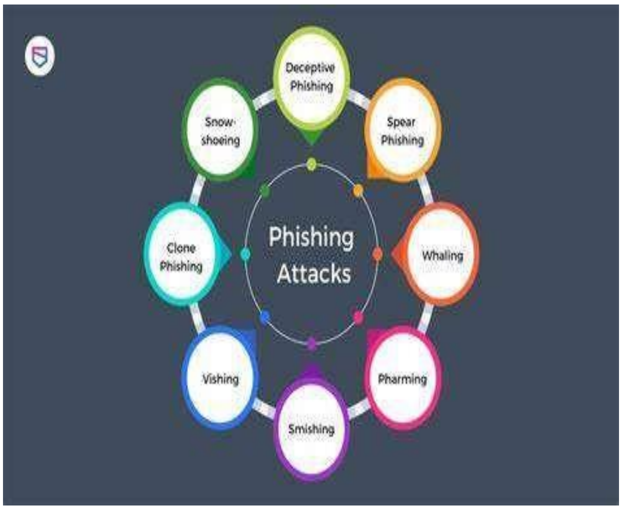


Fig 2: Classification of E-mails

6. SMS Phishing (Smishing): Phishers send fraudulent text messages pretending to be from trusted sources, such as banks [3], to trick recipients into disclosing users details or clicking on malicious links.

7. DNS-Based Phishing (Pharming): Attackers manipulate the Domain Name System (DNS) to redirect website traffic to bogus sites, where victims may unknowingly provide sensitive information.

8. Email Spoofing: They send the emails which are related to our sources, often using tactics like address spoofing to deceive recipients into believing the messages are authentic [9][12].



3. PHISHING STAGES:

There are various types of methods of phishers to follows for the phishing activities:

1) Impersonation: Well all this to be pretend someone else. The method is simple to execute for all the people with some tools [12]. In case they does the websites which looks similar to real ones to make the people to trust on that.

with false information in an attempt to deceive and dupe genuine user.

4. PHISHING MECHANISMS:

Phishing emails are a common cybercrime technique where hostile actors try to fool recipients into divulging private information like bank account information, login passwords, or personal information malevolent user replaces some original content. This phishing method uses social engineering strategies to trick people into doing things that will help the attacker [11].

a. Planning and Action

- In order to properly design their phishing efforts, attackers gather information about the target population.
- To make their phishing emails more unique, they might compile data from social media accounts, publicly accessible sources, or earlier data breaches.

b. Email Spoofing:

- In order to provide the impression that their messages are authentic, attackers use spoof email accounts.[15]
- They might trick users into believing the email is real by using tricks like display name spoofing or domain spoofing.

c. Crafting the Phishing Email

- Phishing emails are expertly crafted by attackers with alluring subject lines and convincing content to persuade recipients to act [10].
- Typical strategies include scaring messages to instill dread or a sense of urgency, promises or prizes, and urgent calls to action.

d. Incorporating Malicious links or Attachments:

- Phishing emails frequently include attachments with malicious code intended to infect the recipient's device or links to fake websites [4][17].
- Attackers might hide the real location of the infected link by using URL shortening services or URL obfuscation techniques.

e. Email Distribution:

- Phishing emails are disseminated by attackers using a variety of techniques, such as automated bots, targeted spear phishing assaults, and bulk email campaigns.
- To avoid being discovered, they might send a lot of phishing emails using compromised email addresses or botnets.

f. Social Engineering Tactics:

- Phishing emails use social engineering techniques to influence the feelings and choices of their target audience.
- Creating a sense of urgency, arousing fear or interest, posing as reliable people, or taking advantage of psychological triggers to get desired reactions are examples of common tactics[16].

g. Response and payload Execution:

- Recipients unintentionally start the attacker's payload when they interact with the phishing email by opening attachments or clicking on malicious links.

- The payload could be programs that steal credentials, malware downloads, or redirects to phishing websites that gather private data.

5. PHISHING TECHNIQUES:

The initial thing is to identify emails that seem and feel suspicious. whether via mail. so simple to create an exact replica of a bank's, Amazon's, or other website these days, it can be difficult to identify a phishing attack on the first try. Instead, we should look for context, such as asking for users' personal information via an HTML form or offering enormous jackpots, and look for generic characteristics [18].

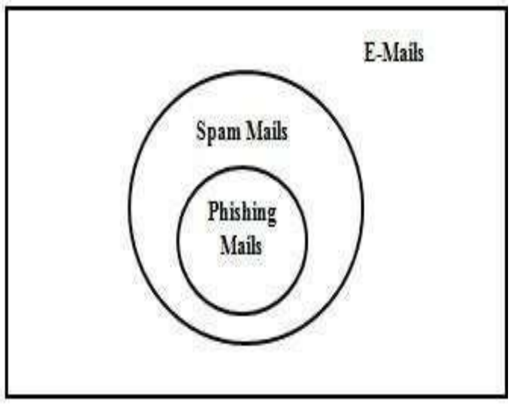


Fig 1: Relationship between Spam Mails & Phishing Mails

When a phishing attempt is discovered, numerous preventative measures are taken, yet every time a new fraud scheme emerges, the previous safeguards fall short. The following are a few well- known technical preventive measures that are used:

i. Anti-Phishing Plug-in (Browser Extension): This method expands the functionality of the browser. These days, browsers save user data and issue alerts when they discover an issue.

ii. Toolbars: In this method, email filters handle the contextual information classification that toolbars are unable to perform. It does nothing more than provide a truth rating for the website that the user ignores despite the warning [22].

iii. Phi stank: the location of all the data pertaining to links and the spammer's name who has previously committed phishing crimes. This technique's main drawback is that information gets erased from the tank as it grows older, and if spammers use the same link again later, it becomes new to the phi stank[6].

iv. Spam filters: this method is considerably more successful than any other that we have found in our investigation because it looks at both the URL and the email's context.

v. Machine Learning Algorithms: This solutions work on already present or existed data from internet sources analyze them and provide results.

vi. Domain Reputation Analysis: In this method, the reputation of the domain the email is coming from is examined [7]. It evaluates whether the email is likely to be a part of a phishing campaign by looking at things like the age of the domain, allegations of misuse in the past, and inclusion on blacklists.

vii. URL Analysis and Link Scanning: This technique looks at URLs that are inserted into emails to see if they are legitimate. Methods like link scanning, which involves comparing URLs to databases of rogue websites or recognized blacklists, can be used to detect phishing links and stop users from visiting them [20].

viii. Sender Authentication methods: Sender authentication methods, such as SPF, DKIM, and DMARC, can be used to identify spoof or forged email addresses that are frequently used in phishing attempts and to confirm the legitimacy of the sender's domain.

ix. Behavioral Analysis: These methods keep an eye on how users interact with email systems in order to spot odd trends that might point to phishing activities. This entails examining email forwarding patterns, click-through rates, and reaction times to spot anomalies in typical user behaviour [17].

x. Real-Time Threat Intelligence Feeds: Including real-time threat intelligence feeds in email security solutions gives users access to the most recent data on dangerous domains, known phishing efforts, and signs of penetration [16]. This makes it possible for businesses to stop phishing emails in their tracks before they get in consumers' inboxes.

As we know, the techniques which involve in prevention of phishing attack. We adapt two social ways ot such scams. One by educating users and alert them about such threat. The second way is punish phishing attackers legally [7].like this there are many other threat intelligence feeds which are present over ways such as adapt many things for the appropriate level of detection and tools which are required and high level of security should be provided for all the system with well updates which will provide the information needed for the users to make it secure and well organized levels of information which makes the device secure and well protected from all the threats and attackers which make your system secure in all ways.

6. PREVENTION SOLUTIONS:

Phishing solutions	Functionality	Limitations
Anti-phishing plug-in	It is an extension added on our browser which has certain functionality.	It protects the user from getting spoofed from emails.
Anti- phishing tool bars	Generate the warning against the attacks.	Its not so accurate and active which basically ignored.
Spam filters	These classify before mail research to inbox. Classify the mails on the basis of previous data filters.	This one works on the basis of rule based and machine learning.
Prevention against Malware software	Some e-mails have some unique code by clicking on those emails which are malicious software get downloaded.	Some new antivirus software to protect the system from attacks.

7. AVOIDANCE OF ATTACKS FROM PHISHING:

It focus on avoiding phishing attacks before falling victim to them. We can prevent situations where users fall victim to such crimes by thoroughly studying phishing. The various kinds are listed as follows:

1. User Education and Awareness Programs: These can dramatically lower the probability of successful attacks by teaching users about the risks associated with phishing and regularly educate them on how to spot phishing attempts [19]. This involves educating users to be wary of unsolicited demands for personal or financial information, to carefully examine email sender addresses, and to proofread their writing for spelling and grammar mistakes.

2. Putting Authentication and Email Filtering Into Practice: Phishing emails can be identified and stopped from reaching users' inboxes by implementing email filtering systems like DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) [8]. These methods highlight questionable emails and confirm the legitimacy of email senders.

3. Use of Multi-Factor Authentication (MFA): By forcing users to submit many forms of verification before being able to access their accounts, MFA offers an extra degree of protection. Attackers are less likely to access accounts without the additional authentication elements, even if they manage to gain login credentials through phishing.

4. Frequent Software Updates and Patch Management: Updating operating systems and software is essential to fixing security holes that could be used by phishing scammers. Applying security updates and patches on a regular basis improves system security overall and helps guard against known vulnerabilities [1].

5. Anti-Phishing Tools and Technologies: Using anti-phishing tools and technologies, like email security gateways, web browser extensions, and endpoint protection programs, can assist in quickly identifying and stopping phishing efforts. To recognize and stop phishing attempts, these systems frequently make use of threat intelligence and machine learning algorithms.

6. Encouraging Vigilance when Clicking Links and Downloading Attachments: Users can avoid falling victim to phishing scams by being advised not to download attachments or click on links from unknown or suspicious sources. They can also be advised to hover over links to confirm their destinations before clicking.

7. Creating Incident Response Plans: By creating and testing incident response plans on a regular basis, organizations can make sure they are ready to react quickly and efficiently in the event that a phishing assault is successful [15]. This covers procedures for documenting occurrences, looking into security breaches, and putting corrective actions in place to lessen the effects of the assault.

8. Constant Monitoring and Sharing of Threat Intelligence: Establishing strong monitoring systems to identify anomalous activity and disseminating threat intelligence to pertinent parties can assist organizations in staying abreast of new phishing techniques and patterns, enabling them to modify their defenses appropriately.

9. Phishing Simulation Exercises: By simulating phishing attacks, businesses can evaluate the success of their current security awareness training initiatives and pinpoint areas in need of development. These exercises offer important insights on user behavior and vulnerability to phishing attempts by simulating real-world phishing scenarios [4][8].

10. Collaboration and Information Sharing: Promoting cooperation between businesses, trade associations, and cybersecurity experts makes it easier to exchange threat intelligence, best practices, and lessons discovered in the fight against phishing scams. Stakeholders can bolster their defenses against phishing threats by banding together [6][9].

8. FUTURE DIRECTIONS:

AI and Machine Learning Solutions:

- Examine how machine learning (ML) and artificial intelligence (AI) can be combined to improve phishing detection and prevention skills.
- Examine whether phishing patterns may be detected by analyzing email content using natural language processing (NLP) methods.
- Investigate the possibilities of AI-driven behavioral analytics to find unusual user activity that may point to phishing attempts.

Multi-Factor Authentication(MFA) Evolution:

- Examine advancements in multi-factor authentication (MFA) technologies to strengthen authentication processes and mitigate the risk of credential theft [8].
- Explore innovative MFA methods beyond traditional approaches, such as biometric authentication, behavioral biometrics, or contextual authentication.

User Education and Awareness Campaigns:

- Stress the value of continual user education and awareness initiatives to enable people to identify and thwart phishing attacks.
- Examine successful phishing awareness training delivery methods, including as gamification, interactive multimedia tools, and simulated phishing exercises.

Collaborative Defense Strategies:

- Advocate for collaborative defense strategies that involve information sharing and cooperation among organizations, cybersecurity professionals, and law enforcement agencies [3].
- Explore the role of threat intelligence sharing platforms and collaborative initiatives in facilitating early detection and response to phishing threats.

Blockchain Technology Integration:

- Explore the potential of blockchain technology to enhance security and trust in email communication by enabling cryptographic verification of sender identity and email integrity.
- Investigate blockchain-based solutions for building decentralized reputation systems to identify and mitigate phishing attacks.

9. CHALLENGES:

1. Evolving Phishing Technique:

- Address the issue of attackers using ever- evolving phishing techniques and strategies to get around established security safeguards.
- Examine the necessity of flexible and dynamic cybersecurity tactics that can successfully identify and counter new phishing attacks [7].

2. Human Factor Vulnerabilities:

- Recognize the inherent weaknesses brought about by the human element in cybersecurity, such as your vulnerability to cognitive biases and social engineering techniques.
- In order to effectively counteract phishing attempts, address the difficulty of striking a balance between technical solutions and human-centric approaches.

3. Privacy and Data Protection Concerns:

- Talk about how phishing attempts affect data security and privacy [2], especially when it comes to the unapproved release of private information.
- Examine the necessity of strong privacy- protecting policies and legal frameworks to protect people's personal information in the event of a phishing attack.

4. Globalization of Cyber Threats:

- Acknowledge the worldwide reach of phishing attacks and the difficulties presented by cross-border cybercrime activities.
- Talk about the significance of global cooperation and coordination in thwarting phishing attempts and bolstering cybersecurity resilience [8].

5. Resource Constraints and Budget Limitations:

- Draw attention to the financial and resource difficulties that organizations— especially small and medium-sized businesses (SMEs)—face when putting comprehensive phishing prevention measures into place.
- Examine affordable cybersecurity tactics and solutions designed to meet the demands of resource-constrained enterprises.

10. CONCLUSION:

In conclusion, the ever-present and constantly- evolving threat posed by phishing attacks continues to have a significant impact on the cybersecurity landscape. It is clear from our in-depth analysis of phishing mechanisms, detection and prevention techniques, effects, and future prospects that phishing is still a significant problem that calls for cooperation and creativity.

Phishing attacks employ sophisticated technology and social engineering techniques to take advantage of gaps in human behavior and technology to trick users and compromise private data. A proactive and multifaceted defense strategy is required because to the agility and persistence of attackers, even with developments in cybersecurity technologies and awareness campaigns.

Robust technology solutions, continuous user education and awareness campaigns, cooperative information-sharing frameworks, and regulatory measures are all necessary for an effective defense against phishing. Future phishing defense capabilities could be improved by embracing cutting-edge technology like multi-factor authentication, blockchain, and artificial intelligence.

Significant obstacles still exist, though, such as resource constraints, privacy issues, and vulnerabilities related to human factors, all of which highlight the necessity of ongoing innovation and adaptation. To tackle these obstacles, a comprehensive strategy combining technology development with human-centered planning, legal structures, and global collaboration is needed.

It is critical that we cultivate a culture of cybersecurity resilience, teamwork, and alertness as we negotiate the complexity of the digital environment. We can lessen the effects of phishing attempts, safeguard digital assets, and maintain the integrity of the online ecosystem by cooperating across industries and disciplines.

11. REFERENCES:

[1].Theodore S. Rappaport, Wireless Communications: Principals and Practice, 2nd ed., Pearson Education (Singapore) Pte. Ltd., India, 2002.

[2].C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: turbo code*, Inter. Conf Commun., pp.1064-1070.1993.

[3]. D.C. MacKay, *Near Shannon limit performance of low density parity check Codes*, Electronics Letters, Vol. 32, pp. 1645-1646, Aug. 1966.

[4].C.E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., Vol. 27, pp. 379-423 (Part one), pp. 623-656 (Part two), Oct.

[5].Upena Dalal, *Wireless Communication*, Oxford UniversityPress, India, 2009.

[6]. Branka Vucetic and Jinhong Yuan, Space-Time Coding, John Wiley & Sons, 2003.

[7].Kai-Ting Shr, Hong-Du Chen, and Yuan-Hao Huang, *A Low-Complexity Viterbi Decoder For Space-Time Trellis Codes*, IEEE Transactions on Circuits and Systems-I, Vol. 57, No. 4, pp. 873-885, April 2010.

[8].N.Kumaratharan, S.Jayapriya and P.Dananjayan, *STTC*

[9].Pierre Viland, Gheorghe Zaharia and Jean-Francois Helard, *Improved Balanced 2n-PSK STTCs for Any Number of Transmit Antennas from a New and General Design Method*, IEEE Conference on Vehicular Technology, pp. 1-5, 2009.

[10]. Kabir Ashraf, *Different STTC over Rayleigh Fading Channels*, IEEE Conference, Dec. 2009.

[11].Pierre Viland, Gheorghe Zaharia and Jean-FrancoisHelard, *Coset Partitioning for the 4- PSK Space-Time Trellis Codes*, IEEE Conference on "Signals, Circuits and Systems, 2009.

[12].Thi Minh Hien Ngo, Gheorghe Zaharia, Stephane Bougeard and Jean Francois Helar*d 4-PSK Balanced STTC with two transmit antennas*, IEEE Conference, 2007.

[13].Murat Uysal, and Costas N. Georghiades, *On the Error Performance Analysis of Space-Time Trellis Codes*, IEEE Transactions on Wireless Communications, Vol. 3, No. 4, pp. 1118-1123, July 2004.

[14].J.N.Pillai and S.H.Mneney, *Adaptively Weighted Space- Time Trellis Codes*, So uthern African Telecommunication Networks and Application Conference, Sep. 2004.

[15].Helmut Bolcskei and Arogyaswami J. Paulraj, *Performance of space-time codes in the presence of spatial fading Correlation*, IEEE Conference, Vol. 1, pp. 687-693, 2000.

[16].Murat Uysal and Costas N. Georghiades, Error Performance Analysis of Space-Time Codes over Rayleigh Fading Channels, Journal of Communications and Networks, Vol. 2, No. 4, pp. 351-356, Dec. 2000.

[17].M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Perform Analysis*, John Wiley & Sons, 2000.

[18].T. S. Rappaport, *Wireless Communications: Principlesand Practice*, Prentice Hall, 1996.

[19].A. F. Naguib and R. Calderbank, *Space-time coding and signal processing for high data rate wireless communications*, IEEE Signal Processing Magazine, Vol.17, No. 3, pp. 76-92, Mar. 2000.

[20].Jakobsson, Markus, and Jacob Ratkiewicz. "Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Query Features." Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security. 2006.

[21].Kumar, Suruchi, and Sandeep K. Sood. "A Review on Phishing Attacks and Various Anti-Phishing Techniques." Procedia Computer Science 85 (2016): 652-659.

[22]. Ranganathan, Chitra, et al. "Email Phishing: A Review." International Journal of Computer Applications 65.6 (2013): 19-24. (Of phisng mechanism).

[23].P. Liu and T. S. Moh, "Content Based Spam E-mail Filtering", International Conference on Collaboration Technologies and Systems (CTS), pp. 218-224, 2016, 2016.

[24].J. V. Chandra, N. Challa and S. K. Pasupuleti, "A practical approach to E-mail spam filters to protect data from advanced persistent threat", International Conference on Circuit Power and Computing Technologies (ICCPCT) Nagercoil, pp. 1-5, 2016, 2016.

[25].Abdelhamid, N., Thabtah, F., Abdel-jaber, H. (2017). Phishing detection: A recent intelligentmachine learning comparison based on models content and features. In 2017 IEEE international conference on intelligence and security informatics (ISI) (pp. 72–77). IEEE.

[26]. Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. In Developments and advances in defense and security (pp. 51–64). Springer.

[27]. Chan, C.H., King, I.: Using Biased Support Vector Machine to Improve Retrieval Result in Image Retrieval with Self-organizing Map. In: Proceedings of International Conference on Neural Information Processing, pp. 714–719. Springer, Heidelberg (2004).

[28]. S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions", Proceedings of the 28th international conference on Human factors in computing systems ser. CHI'10. New York NY USA:ACM, pp. 373-382, 2010.

[29]. W. D. Yu, S. Nargundkar and N. Tiruthani, "A phishing vulnerability analysis of web based systems", Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC 2008). Marrakech Morocco: IEEE, pp. 326-331, July 2008.

[30]. Androutsopoulos, J. Koutsias, K.V. Chandrinos and C.D. Spyropoulos, "An Experimental Comparison of Naive Bayesian and Keyword-Based Anti-Spam Filtering with Encrypted Personal E-mail Message", Proc. SIGIR 2000, 2000.