IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms

Pawankumar Sharma[1], Bibhu Dash[2], Meraj Farheen Ansari[3]

Dept. of Computer and Information Systems, University of the Cumberlands, KY USA[1]

Dept. of Computer and Information Systems, University of the Cumberlands, KY USA[2]

Dept. of Computer and Information Systems, University of the Cumberlands, KY USA[3]

Abstract: Phishing has been a constant issue across the global community. The approach has primarily been related to most attackers gaining access to sensitive information about users. Lack of awareness is among the main factors that result in successful phishing attacks. There are different types of phishing attacks available. However, cybersecurity specialists have developed algorithms that have effectively prevented phishing attacks. The report below includes information on anti-phishing algorithms that can detect phishing attacks. The algorithms include different technologies and capabilities that promote safety for most individuals. The paper focuses on describing each of these concepts and how they promote cybersecurity across the globe.

Keywords: Anti-phishing, sensitive information, phishing, social engineering, cybersecurity, cyberattacks

I.INTRODUCTION

Studies have indicated an increase in the number of attacks associated with phishing. Phishing attacks have been increasing for the past decade. Lack of awareness and technical abilities to avoid the attacks has been a critical factor in the majority of the public being vulnerable to the attacks [1]. Most company breaches have also been successful due to the phishing attack technique. The impacts associated with successful breaches were among the key factors promoting the development of anti-phishing attacks. See figure.1, which illustrates the 12 months of large-scale phishing data from its security cloud to detect key developments, industries, and characteristics at risk and develop strategies. Anti-phishing attacks are systems and browsers designed to protect users from phishing attacks [2]. There has also been an increase in software systems created to protect users from phishing attacks. The anti-phishing software always includes modules and programs that can detect any types of attacks and prevent them [3].

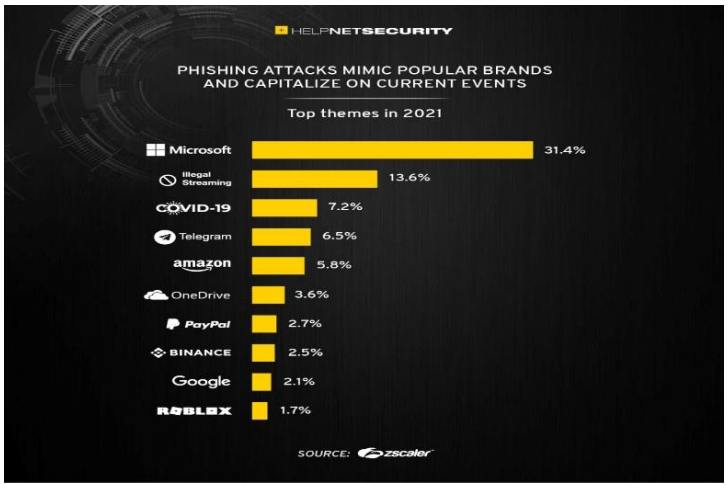

Figure 1: 12 months of global phishing data from its security cloud to identify key trends, industries and geographies at risk, and emerging tactics [5].

This software can also include a warning system that ensures users are not doped into providing sensitive information [4, 5]. Companies with effective anti-phishing technologies have even succeeded in avoiding these attacks. Users who've implemented the anti-phishing browsers have also recorded increased security from phishing attacks, suggesting the algorithms' effectiveness.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

II.BACKGROUND ON PHISHING ATTACKS

Phishing is a type of cyberattack which engages special tools and steps to obtain sensitive information from users. By definition, phishing is a social engineering attack that attackers apply to receive sensitive information from users [6]. The attacker could masquerade as a trusted entity, duping a user into offering their login information. There are different ways through which these attacks are achieved. Each of these approaches is described to be a type of phishing attack [6]. The main methods included duping clients and users include emails, instant messages, and social media.

An excellent example of a phishing attack (see figure.2) includes the user receiving an email masquerading to be from a trusted website [6]. The email could also have a link requiring users to retain their login and other sensitive information. When the user inputs their information, the action will provide the attacker with the information for them to use as they would like [6]. Users are therefore always unable to understand when a phishing attack has occurred. Not being aware of the attack results in critical consequences for the user, who could permanently lose valuable information [7]. The inclusion of an anti-phishing algorithm in detecting these attacks could therefore be described as the only solution.

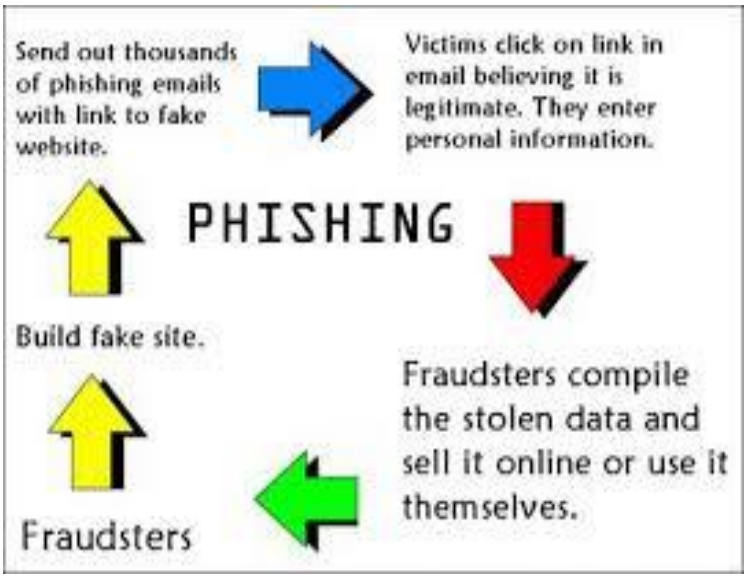

Figure 2: How does phishing work?

The two main types of phishing attacks include email and spear phishing techniques. Email phishing attacks have an attacker sending many fraudulent messages and waiting for vulnerable users to fall for the trap [7]. The doped individuals could send small user sums of money, which accumulate to be huge. The phishing emails are always well-created to look like that of an organization. Spear phishing attack, on the other hand, is continually developed to target an individual or enterprise [7]. The attacker engages this approach after finding a specific user to the target. The approach involves researching the individual and manipulating them into providing their sensitive information [8]. This type of phishing attack is mainly included when targeting an employee of a large company to acquire their login information to the company.

The need for anti-phishing algorithms is associated with the need to detect phishing attacks. The description shows that phishing attacks could take valuable time [9]. Including an algorithm to detect when the attack has commenced is significant in providing a user with the knowledge required to stop the attack [8]. The user would be educated to understand his requirements to avoid the attack [10]. Therefore, this factor shows that the anti-phishing algorithms effectively ensure safety against phishing attacks.

III.DETECTING PHISHING WITH ANTI-PHISHING TECHNIQUES

Spotting phishing emails and communication is a practical approach to securing oneself from these attacks. Spotting phishing attacks has long been described as a practical approach to being safe from such attacks [1]. Cybersecurity experts expressed the need for developing anti-phishing software by focusing on detecting these attacks. Understanding how phishing is achieved remains the first step in detecting these attacks [1]. A user should be able to understand the characteristics associated with phishing emails and messages. The social engineering techniques should remain understood, therefore being safe from the attacks.

There are significant websites that educate users to avoid phishing attacks. The websites and blogs ensure that people are educated on the proper ways to prevent most attacks [3]. One of the main methods of understanding a bogus attacker

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

would be using a public email domain. The domain "@gmail.com" is broadly used by most attackers when trying to engage in an attack against the users [2]. Emails and messages that require one to click a link should also be approached with care [2]. Most links associated with emails result in users placing their sensitive information and obtaining significant losses [11]. Detecting phishing emails requires the user to be more alert and focus on weaknesses across these emails. Detecting phishing attacks should always be a concern for the user. Some attackers are, however, always one step ahead, making their attacks impossible to detect [2]. Spear phishing attacks are always more advanced and more challenging to detect for regular users see figure.3. These attackers, therefore, make most users vulnerable despite knowing phishing attacks [4]. The anti-phishing algorithms are the leading solutions for preventing these attacks [11]. These algorithms are always more effective in detecting well-designed phishing scams than user knowledge.

Figure 3: Steps involved in spear phishing

Anti-phishing algorithms are included in any piece of software or system which protects against phishing attacks [12]. The development of these types of systems has been on the rise, especially from the significant increase in phishing attacks across the globe. Phishing is considered adequate as a result of the deceit included towards users. The deceit ensures that a victim does not become aware of the attack until it is too late. The algorithms are effective in the fact that they detect the attack while it is happening. AI and machine learning technologies have contributed to the success of anti-phishing algorithms [12]. The technologies can detect phishing since machine learning focuses on machines reasoning like humans. The learning ability ensures that the systems can learn from before and detect phishing attacks in advance. AI technology in phishing prevention has proven to be very effective. One of the key benefits of using AI in detecting phishing attacks has been its effectiveness in being fast and effective [13]. Most security defenses are recently engaging the use of AI as a result of its responsiveness. The high-end responsiveness of AI can be seen in the development of technology in recent years. The technology has accumulated great results over the past couple of years. Over the past few years, the overall capability and protection required to promote a defined type of security have increased. Therefore, the technology's growth and development show the potential associated with anti-phishing algorithms.

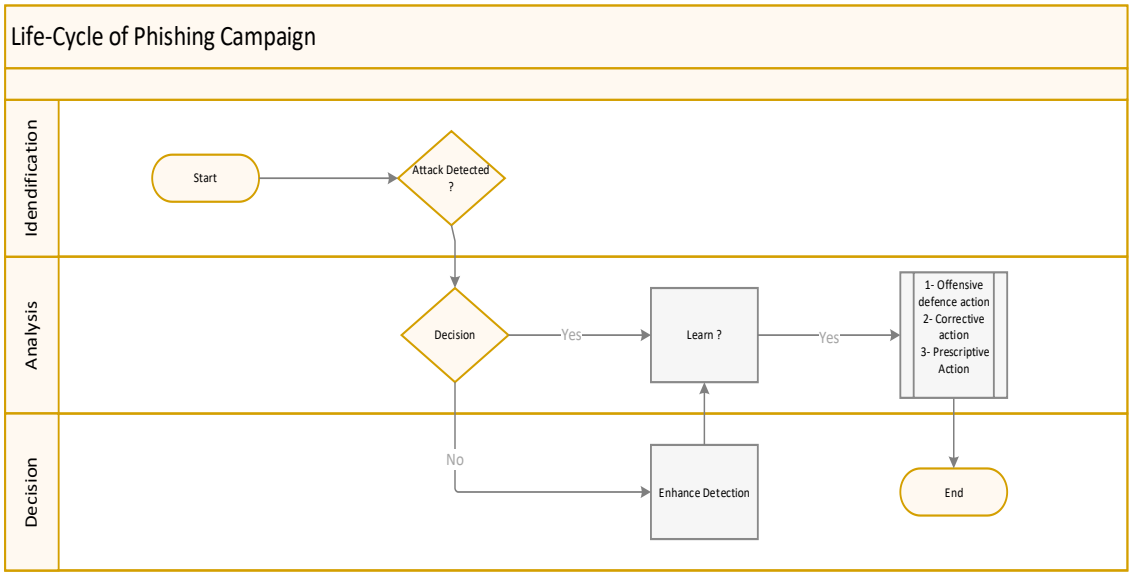

Figure 4: Lifecycle of technology-enabled phishing campaign [16]

Cybercrime has adopted AI technology to achieve its key attacks [14]. The interest in completing successful attacks has seen more creative ways of promoting cybercrime [14]. Some phishing attacks have been seen to engage social

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

engineering through AI technology. These attacks also showcase the need for AI in the anti-phishing algorithms. It ensures that systems can defend against attacks with a similar or more effective approach. This also showcases the capabilities of anti-phishing algorithms.

AI technologies such as machine learning technologies are increasingly influential in fending off such attacks [14]. The technology is increasingly effective in promoting a higher level of security (see Fig. 4) against phishing attacks. Machine learning is a technology in AI where it promotes learning by machines [14]. The technology ensures a machine can learn from previous experiences [14]. This means that machine learning can enable a machine to learn from the last phishing attacks and understand which protective measures should be included [14]. The machine would be able to engage in a practical prevention approach to similar phishing attacks in the future [14]. Anti-phishing technology, including machine learning, is effective in detecting phishing attacks.

The analysis presented, therefore, concludes with anti-phishing AI techniques being more effective in detecting phishing attacks [3]. The technologies described are showcased to influence the capabilities of anti-phishing algorithms. Machine learning ensures that similar attacks have not succeeded [3]. These attacks are avoided by detecting them before they are successful. The technologies present are, therefore, very effective in ensuring that phishing attacks can be detected and prevented [14]. Because of the effect of these anti-phishing algorithms, these techniques should be incorporated into the first line of defense against any form of phishing assault against a user or an individual.

Cybersecurity specialists have indicated vital benefits associated with using algorithms to detect any attack associated with phishing [15, 16]. Understanding phishing was the first step in preventing such attacks. Most reports have described phishing to be best resolved through detection and prevention. Including technologies that can detect such attacks effectively prevents each type of attack. The overall focus on avoiding every attack ensures no successful attacks are achieved.

Several phishing algorithms have been developed over the years. The different types of technologies developed include various rules for detecting phishing attacks. Most companies avoid phishing attacks by providing access to specific machines [15]. Providing computers with certificates has also been a practical approach to detecting phishing attacks. The company's server, therefore, understands to give access to specific machines. If a hacker has gained access to an employee's logins, trying to access the server through these logins and without a certificate becomes impossible [17]. The server may also limit login in through this login information [16]. The use of such defense and algorithms ensures a company's sensitive data. Therefore, this algorithm ensures a company remains protected from any phishing attack.

Regarding attack accuracy, there are four different states for any action detected by Intrusion Detection (IDS). A genuine positive condition occurs when an activity is identified as an attack by the IDS, and the step is indeed an assault. A true positive is a successful assault identification. A real negative condition is comparable. This occurs when the IDS classifies a behavior as acceptable, and the action is genuinely acceptable. Ignoring appropriate conduct effectively is a real negative. Neither of these conditions is hazardous since the IDS is functioning normally. A false positive condition occurs when an IDS recognizes an action as an attack even if the activity is normal behavior. A false positive is the same as a false alarm.

		Actual	
		Positive	**Negative**
Predicted	**Positive**	**True Positive** Rule matched and did attack present	**False Positive** Rule matched, but no attack present
	Negative	**False Negative** No rule matched and no attack present	**True Negative** No rule matched, but attack present

Figure 5: Chart explaining ruled-based logic of actual vs. predicted phishing outcomes

The most severe and deadly state is a false negative state. IDS classifies an action as acceptable when it is actually an attack. A false negative occurs when the IDS fails to detect an attack. This is the riskiest situation since the security expert is unaware that an assault has occurred. False positives, on the other hand, are at best inconvenient and might create serious problems. Conversely, false positives may be successfully adjudicated with the correct amount of overhead; false negatives cannot (see fig. 5).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

Another type of algorithm that ensures phishing attacks can be detected is the two-factor authentication algorithm [17]. These algorithms provide two levels of security that they must pass before accessing sensitive information. The employee could have a USB disk and their login information to access the sensitive information. These precautions and technologies ensure that attackers cannot complete their attacks (see fig. 6). When engaging in such an attack, the attacker will remain locked out of the system until they provide the second key to the second level of security present.

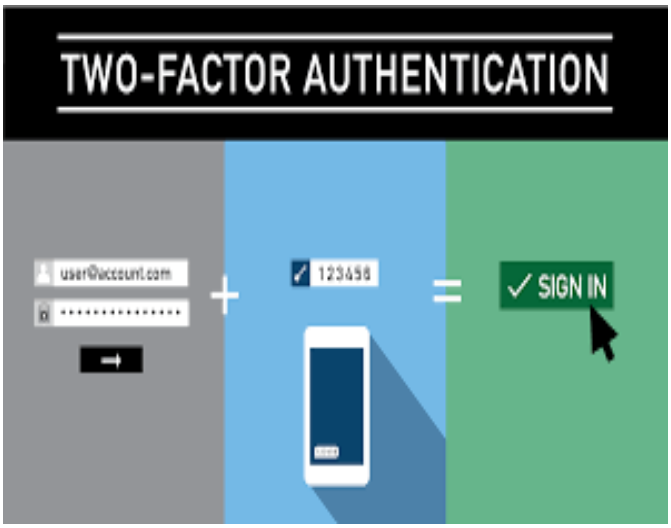

Figure 6: Two-Factor Authentication

The technologies above are some of the most adopted by different organizations today. Below fig. 7 demonstrates different types of 2FA. The technologies ensure that phishing attacks have been detected and prevented [18]. The approach has been relevant in avoiding most technologies in recent years. It has been found to have relevant results over the past few years. Adopting such measures has been found to ensure that such technologies cannot be achieved. Including such measures ensures one cannot complete the attacks by accessing users' passwords.

Figure 7: Multiple types of 2FA [17]

Companies like Google have also become increasingly concerned with detecting and preventing potential phishing attacks. Google's G-mail service has high-level anti-phishing algorithms which aid in detecting phishing attacks [4, 18]. The technologies ensure that insecure website links have been flagged for the user. Users are therefore advised not to access any website that is flagged to be dangerous [19, 20]. The company's spamming algorithm is also very effective in spamming sites that seem very dangerous. Below fig.8 indicates how Gmail ensures a spam-free inbox. Spamming email messages from suspected senders is found to be very effective in protecting users from any risks of phishing. The spammed messages get deleted after some time [2, 18]. The spamming and flagging technologies are, therefore, very effective in protecting users from phishing attacks [21]. The anti-phishing algorithms from Google and other companies

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

ensure that users have remained protected in the long run by ensuring all phishing attacks have been detected and prevented [21].

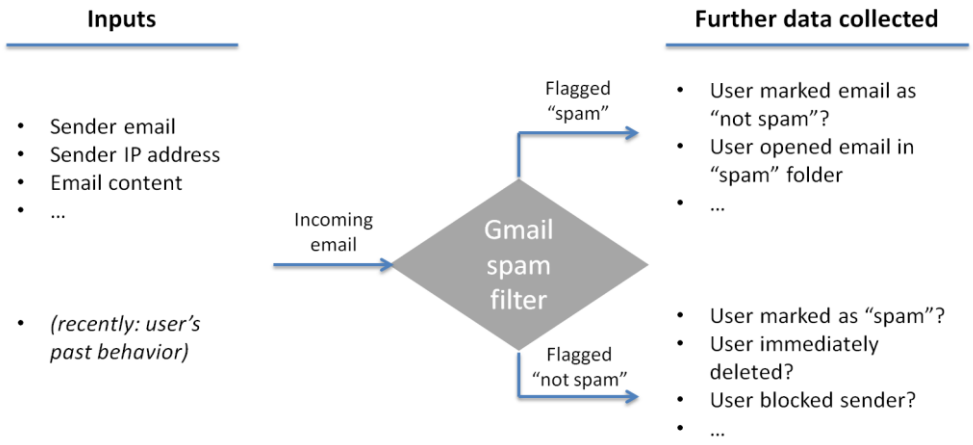

Figure 8: Gmail-ensuring a spam-free inbox with Machine Learning

Each phishing technology described above is very effective in detecting phishing attacks. The anti-phishing algorithms can protect the users by preventing these attacks [21]. Technologies that implement anti-phishing algorithms are also being developed at an increased rate in recent years [21, 22]. Developing these technologies has been found to ensure that people remain protected. The technologies should therefore continue to be created and implemented across different websites and social media pages [23, 24]. This factor will ensure that the number of phishing attacks has been reduced. Security analytics and visualization operations are now causing a revolution in security management, identity and access management, fraud prevention and governance, and risk and compliance [25]. For example, security analytics is managed through a threat data consolidation and alert management system, with hundreds of thousands of alerts and network events per second and constant real-time risk assessment with proper hazard prioritization.

IV.CONCLUSION

Anti-phishing algorithms have proven very effective in detecting phishing attacks. Technologies developed from these algorithms have proven to be effective in preventing phishing attacks and constantly changing. The prevention is associated with ensuring that the user has been notified of such attacks. The paper describes how phishing attacks have been rising for a long time. Detecting phishing attacks through anti-phishing algorithms is an effective approach to protecting most users. Companies are therefore required to focus on including similar technologies in their companies. This action will ensure that people have remained protected from similar attacks. Such activities will ensure that companies and individual users are protected from similar attacks. Adopting the anti-phishing algorithms across different sectors and technologies will also ensure that the number of phishing attacks has been reduced significantly.

ACKNOWLEDGMENT

Thanks to our University of Cumberlands' computer science professor **Dr. Azad Ali** and other faculty members for their guidance and support during the writing of this paper. Appreciate Dr. Ali's hard work in reviewing and sharing his valuable feedback for this work.

REFERENCES

[1] A. Baiomy, M. Mostafa and A. Youssif, "Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks", Indian Journal of Science and Technology, vol. 12, no. 44, pp. 01-10, 2019. Available: 10.17485/ijst/2019/v12i44/147850.

[2] V. Suganya, "A Review on Phishing Attacks and Various Anti Phishing Techniques", International Journal of Computer Applications, vol. 139, no. 1, pp. 20-23, 2016. Available: 10.5120/ijca2016909084.

[3] D. Glăvan, "Detection of phishing attacks using the anti-phishing framework," Scientific Bulletin of Naval Academy, vol., no. 1, pp. 208-212, 2020. Available: 10.21279/1454-864x-20-i1-028.

DOI: 10.17148/IJARCCE.2022.11728

[4] G. Kumar, S. Gunasekaran, .. Nivetha, P. Sangeetha and .. Shanthini, "URL PHISHING DATA ANALYSIS AND DETECTING PHISHING ATTACKS USING MACHINE LEARNING IN NLP", International Journal of Engineering Applied Sciences and Technology, vol. 3, no. 10, pp. 26-31, 2019. Available: 10.33564/ijeast.2019.v03i10.007.
[5] M. Et. al., "Detecting Phishing Attacks using NLP", Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 2, pp. 369-372, 2021. Available: 10.17762/turcomat.v12i2.816.
[6] Bhuvana, A. Bhat, T. Shetty and M. Naik, "A Study on Various Phishing Techniques and Recent Phishing Attacks", International Journal of Advanced Research in Science, Communication and Technology, pp. 142-148, 2021. Available: 10.48175/ijarsct-2094.
[7] Bhagya Bajanthri and Mr. Sayeesh, "A Study on Various Phishing Techniques and Recent Phishing Attacks", International Journal of Advanced Research in Science, Communication and Technology, pp. 296-302, 2022. Available: 10.48175/ijarsct-2870.
[8] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches", Future Internet, vol. 12, no. 10, p. 168, 2020. Available: 10.3390/fi12100168.
[9] T. Venkat Narayana Rao, Sreeja Reddy, "Investigation of Phishing Attacks and Means to Utilize Anti Phishing Techniques", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 7, no. 2, pp. 05-10, 2019. Available: 10.17762/ijritcc.v7i2.5224.
[10] V. Bhavsar, A. Kadlak and S. Sharma, "Study on Phishing Attacks", International Journal of Computer Applications, vol. 182, no. 33, pp. 27-29, 2018. Available: 10.5120/ijca2018918286.
[11] B. Wardman, "Phorecasting Phishing Attacks: A New Approach for Predicting the Appearance of Phishing Websites", International Journal of Cyber-Security and Digital Forensics, vol. 5, no. 3, pp. 142-154, 2016. Available: 10.17781/p002156.
[12] G. Sonowal, "Detecting Phishing SMS Based on Multiple Correlation Algorithms", SN Computer Science, vol. 1, no. 6, 2020. Available: 10.1007/s42979-020-00377-8.
[13] R. Gupta and P. Kumar Shukla, "Performance Analysis of Anti-Phishing Tools and Study of Classification Data Mining Algorithms for a Novel Anti-Phishing System", International Journal of Computer Network and Information Security, vol. 7, no. 12, pp. 70-77, 2015. Available: 10.5815/ijcnis.2015.12.08.
[14] N. Mudiraj, "Detecting Phishing using Machine Learning", International Journal of Trend in Scientific Research and Development, vol. -3, no. -4, pp. 488-490, 2019. Available: 10.31142/ijtsrd23755.
[15] "A Novel Customized Anti Phishing Framework for Mobile Environment", International Journal of Science and Research (IJSR), vol. 4, no. 11, pp. 134-136, 2015. Available: 10.21275/v4i11.sub158798.
[16] Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), 2091-2121.
[17] M. FIDA and A. JOVITH, "Anti-Phishing Strategy Model for Detection of Phishing Website in E-Banking", International Journal of Information Security and Cybercrime, vol. 5, no. 1, pp. 75-80, 2016. Available: 10.19107/ijisc.2016.01.07.
[18] R. Ramdas T, "Detecting Phishing Websites Based On Improved Visual Cryptography", International Journal Of Engineering And Computer Science, 2015. Available: 10.18535/ijecs/v4i8.67.
[19] H. Abusaimeh, "Detecting the Phishing Website with the Highest Accuracy", TEM Journal, pp. 947-953, 2021. Available: 10.18421/tem102-58.
[20] Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.
[21] S. Hawa Apandi, J. Sallim and R. Mohd Sidek, "Types of anti-phishing solutions for phishing attack", IOP Conference Series: Materials Science and Engineering, vol. 769, no. 1, p. 012072, 2020. Available: 10.1088/1757-899x/769/1/012072.
[22] Brad. K. How Machine Learning Helps in Fighting Phishing Attacks. (2021). Phish protection. https://www.phishprotection.com/blog/machine-learning-helps-fighting-phishing-attacks/
[23] Lifshitz, A. (2015, November 21). Gmail: ensuring a spam-free inbox with Machine Learning. Retrieved July 13, 2022, from https://digital.hbs.edu/platform-digit/submission/gmail-ensuring-a-spam-free-inbox-with-machine-learning/
[24] 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, 3(3), 61–72. https://doi.org/10.47893/IJSSAN.2022.1221
[25] Dash, B., & Ansari, M. F. (2022). Self-service analytics for data-driven decision making during COVID-19 pandemic: An organization's best defense. Academia Letters, 2.

BIOGRAPHY

Pawankumar Sharma is a Senior Product Manager for Walmart at San Bruno, California. He is currently on his Ph.D. in Information Technology at the University of the Cumberlands, Kentucky. Pawankumar Sharma has completed his

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11728

Master of Science in Management Information Systems from the University of Nebraska at Omaha in 2015. He also holds another Master of Science in Information Systems Security from the University of the Cumberlands, Kentucky and graduated in 2020. His research interests are in the areas of Cybersecurity, Artificial Intelligence, Cloud Computing, Neural Networks, Information Systems, Big Data Analytics, Intrusion Detection and Prevention.

Bibbu Dash is an Architect-Data and Analytics in a Fortune 100 financial organization at Madision, WI. He is currently a Ph.D. student in Information Technology at the University of the Cumberlands, Kentucky. Bibhu has completed his Master of Engineering in Electronics and Communication Engg., and MBA from Illinois State University, Normal, IL. Bibhu's research interests are in the areas of AI, Cloud Computing, Big Data and Blockchain technologies.

Dr. Meraj Farheen Ansari completed her Ph.D. (IT) from the Graduate School of Information Technology, University of the Cumberlands. She also completed her MBA with a Specialization in Management Information Systems from Concordia University, Milwaukee, WI, USA. Her research interests include awareness of cybersecurity, eliminating Cyber Threats, & ML. Her current research involves how to aware organizational employees of cyber security threats using AI awareness programs. Currently, she is working as a Security Analyst in Northern Trust Bank, Chicago, IL, USA.

