International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V71I11P111

Volume 71 Issue 11, 74-79, November 2023

Original Article

Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks

Sivaraju Kuraku[1], Dinesh Kalla[2], Nathan Smith[3,] Fnu Samaah[4]

[1]*School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, USA.*
[2,3]*Department of Computer Science, Colorado Technical University, Colorado Springs, CO, USA.*
[4]*Department of Computer Science, Harrisburg University of Science and Technology, Harrisburg, PA, USA.*

[1]*Corresponding Author : kalladinesh@outlook.com*

Received: 22 September 2023 Revised: 26 October 2023 Accepted: 13 November 2023 Published: 30 November 2023

Abstract *- The increased advancement of technology has increased computer users' susceptibility to cyber threats like phishing attacks, which are a type of social engineering method utilized by phishers to masquerade as legitimate entities in order to deceive computer users into disclosing sensitive information like financial data or passwords. This study determines how computer users' behavior affects their cybersecurity awareness towards phishing attacks. The study also identifies the major behavioral patterns that computer users exhibit that make them additionally susceptible to phishing attacks. These behavioral patterns include improper management of passwords, neglecting regular security and software updates, exposing sensitive information on online platforms, and clicking suspicious attachments and links. Through understanding the relationship between user behavior and cybersecurity awareness, computer users can implement proactive measures to minimize the impact and frequency of phishing attacks, thus enhancing cybersecurity resilience.*

Keywords *- Computer users, Cyber threats, Phishing attacks, sensitive information, computer users' behavior, Cybersecurity Awareness, Behavioral patterns, Cyber Attacks, Cybersecurity education, Pharming, Information technology Security and cybersecurity resilience*.

1. Introduction

Computers are indispensable tools for education, work, business, and entertainment in the current ever-evolving digital world, and their users need to be conscious of cybersecurity threats, mainly phishing attacks, in the digital landscape as they rely on technology in their daily lives. Phishing attacks, symbolized by fraudulent efforts to trick users into disclosing sensitive financial data, passwords, and information, have become dangerous yet prevalent cyber threats [1]. While security measures and technological advancements have been put in place to resolve risks associated with phishing attacks, the behavior of computer users and their awareness plays a vital role in protecting against social engineering threats like phishing attacks. Understanding the way the behavior of computer users affects their cybersecurity awareness towards phishing attacks is extremely important in developing effective strategies for combating phishing and other social engineering attacks. The way users interact with their computers and the internet, their cybersecurity knowledge, and their vulnerability to social engineering techniques influence their susceptibility to phishing [2]. The level of familiarity with online platforms and computer literacy are among the factors that impact cybersecurity awareness. Notably, users who lack enough computer skills or are less experienced with computers can have difficulties recognizing phishing attempts, thus making them extremely vulnerable to falling victim to phishers and cybercriminals [3]. Conversely, tech-savvy computer users with navigational knowledge in the digital realm better understand possible risks, thus enabling them to recognize phishing attempts more effectively.

Moreover, human psychology contributes to shaping computer users' cybersecurity behavior. Phishers often take advantage of cognitive biases, like fear and urgency, to manipulate computer users into clicking malicious attachments and links or revealing sensitive information. While computer users' vulnerability to such psychological biases differs, phishers make users behave in a hasty manner or make quick decisions that make them vulnerable to phishing attacks. This study determines how computer users' behavior affects their cybersecurity awareness towards phishing attacks. The study also focuses on identifying the major behavioral patterns that computer users exhibit that make them additionally susceptible to phishing attacks. These behavioral patterns include; improper management of passwords, neglecting regular security and software updates,

exposing sensitive information on online platforms, and clicking suspicious attachments and links. By understanding the relationship between user behavior and cybersecurity awareness, computer users can implement proactive measures to minimize the impact and frequency of phishing attacks, thus enhancing cybersecurity resilience.

2. Background

The behavior of traditional computer users was characterized by the level of cybersecurity awareness towards phishing attacks. The first behavior that unsuspecting computer users exhibited was a lack of security awareness due to being not informed about phishing attacks, suspicious URLs, inaccurate domain names, and emails soliciting sensitive information, thus making them additionally susceptible to phishers [4]. Users also clicked on malicious links embedded in messages and emails without verifying the legitimacy of their sources. These links lead computer users to fake websites made to steal their login credentials and personal data. Computer users unknowingly reveal their personal information to phishers while interacting with them on malicious websites. Traditional computer users fail to adopt two-factor authentication and enable it on their accounts, leaving them unprotected when their credentials get compromised [5]. Equally, computer users resisted security measures like using spam filters, anti-phishing tools, updating security software, Artificial Intelligence and reporting phishing tries. They termed them time-consuming and unnecessary, resulting in increased cases of phishing attacks [6]. There has been a significant increase in unique phishing sites in the last 10 years. Below Figure represents reports from APWG 2023, which shows around 345% growth in unique phishing sites.

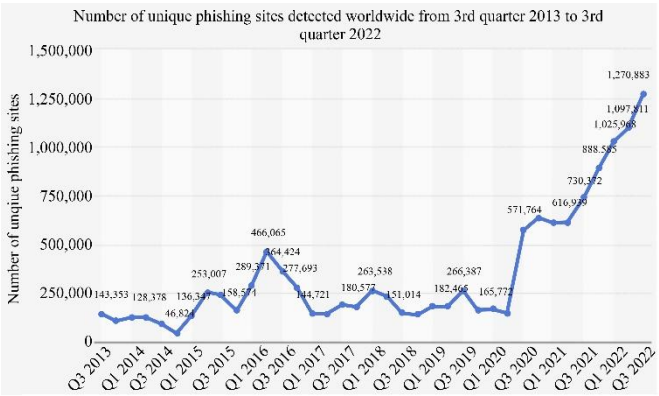

Fig. 1 Unique Phishing Sites vs Years (2023 APWG Report)

3. Problem Statement

Cybersecurity remains a key concern, particularly for computer users and organizations in this rapidly developing digital landscape, where phishing attacks remain not only a prevalent cybercrime but also a serious threat to data privacy and security. Phishing attacks exploit computer users' human vulnerabilities and utilize deceiving social engineering methods to manipulate users into executing harmful deeds or giving or exposing their sensitive information. While security experts continue progressing in cybersecurity tools and technologies, the effectiveness of such cybersecurity measures and advancements heavily rely on the computer users' behavior and cybersecurity awareness. Despite the sophistication of social engineering attacks, many computer users remain vulnerable to becoming victims of social engineering attacks, mainly phishing attacks, because of the careless behavior that they exhibit online and the lack of cybersecurity awareness of such attacks [7]. Kuraku et al. (2022) also stress that people's engagement in insecure behavior, like clicking links originating from unsecured or unverified sources, increases their susceptibility to phishing attacks. Computer users with an overly-obeying behavior are additionally receptive to numerous lures [8]. For instance, computer users who exhibit the behavior of usually obeying instructions and authorities more compared to others are likely to become the victim of business email compromise, abbreviated as BEC, seeming to originate from a legitimate institution and requesting speedy action. Hence, this study endeavors to identify the major behavioral patterns that computer users exhibit, like improper management of passwords, neglecting regular security and software updates, exposing sensitive information on online platforms, and clicking suspicious attachments and links, making them additionally susceptible to phishing attacks.

4. Significance of the Study

The study on understanding the way that computer users' behavior affects their cybersecurity awareness towards phishing attacks can help computer users to develop effective cybersecurity strategies for preventing cybercriminals from gaining access to vital sensitive information. As human weakness continues to be the weak link enabling cybercriminals to access security systems, this study can help computer users to desist from their unsecure human behavior of clicking on malicious links and sharing their personal information carelessly [9]. By identifying precise computer users' behavior that makes them more vulnerable to phishers, organizations and computer users can conduct effective risk assessments, make targeted cybersecurity training programs, and develop preventive measures to minimize the probability of phishing attacks succeeding [10]. Due to increased online spending hours, users are more prone to cyber threats and phishing attacks [11]. The study offers computer users valuable insight into improving and fine-tuning their security solutions through the use of more secure browsers with effective browser warnings, use of email filters, and other tools for detecting and preventing any kind of phishing attempt. The study's strength lies in its valuable insight on raising cybersecurity awareness, adopting an anti-phishing behavior for computer users, minimizing phishing attacks' success rate, and safeguarding computer users from detrimental aftermaths of cybercrime.

5. Literature Review

Failure or even delays in installing security software updates is a common error underlying computer users' behavior despite installing security software updates being an extremely essential [12] security action that helps secure computer systems through their experimental study on behavioral decision-making posits that risk-taking behavior explains computer user's behaviors on installing security software updates. Precisely, Rajivan et al. (2020) suggest that computer users with a tendency to take more risks delay installing software updates. Rajivan et al. (2020) further stress that knowing the exact computer users' behavior that can influence their vulnerability to phishing attacks can help to devise better technical programs focused on cybersecurity awareness to prevent social engineering attacks and other cyber-attacks. For example, risk-takers who have been found to exhibit poor security behavior can be offered more tailored cybersecurity training to help them change their cybersecurity behavior.

The study posits that an individual's capability and ability are about their behavior and not about genes, personality, or traits [13]. Therefore, unlike their personality or genetics, people can change, describe, measure, or observe their behavior. Abroshan et al. (2021) stress that computer users' capability and ability to detect phishing attacks can be increased through changing their behavior, which makes them susceptible to phishing attacks. This can be done using psychological methods like cognitive behavioral therapy, abbreviated as CBT. Abroshan et al. (2021) further state that although such behavioral therapy can take a long duration, it helps to tackle the cause of computer user's vulnerability to phishing attacks because their predisposing behavior is shaped by factors like user prior experiences on cyber-victimization, thoughts, emotions, personality, and attitude.

Computer users frequently engage in non-intentional behavior that compromises their security measures and exposes them to social engineering attacks [14]. Such non-intentional behavior includes neglecting to use strong passwords, transmitting sensitive information carelessly without encrypting it, browsing unsafe web pages, and engaging in unsafe data practices. This non-intentional behavior becomes risky for computer users and the organization at large because it exposes them to external perpetrators that can phish them and the entire organizational employees. Alzahrani et al. (2020) urge organizations to enhance their computer user's phishing resilience through embedding simulated phishing exercises in their cybersecurity awareness training to develop anti-phishing behavior among their computer users and employees.

6. Methodology

This qualitative study delves into the intricate connection between individuals' behaviors and their proficiency in recognizing phishing attempts. This study used a descriptive quantitative cross-sectional survey design to determine how an employee sample felt about phishing and security practices. Employing a 5-point Likert scale, the survey assesses participants' behaviors towards phishing through 10 questions. These questions touch upon crucial aspects such as the perceived safety of clicking on links, opening email attachments, awareness of phishing risks, and the adoption of preventive measures.

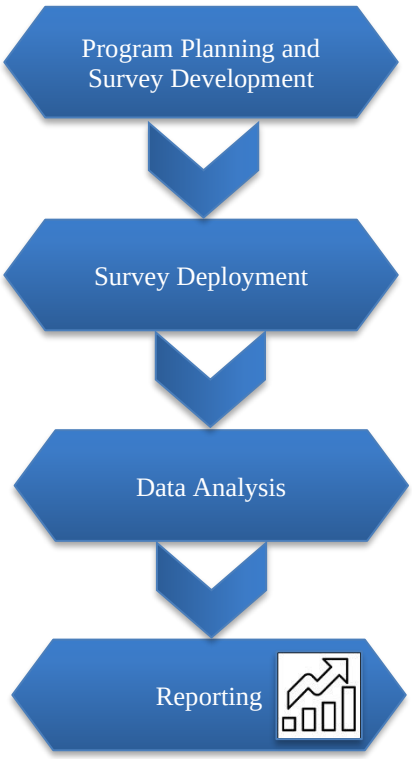

Fig. 2 Four stages of research methodology

6.1. Survey Questions

- I don't always click on links in emails just because they come from recipients I know.
- If an email from an unknown sender looks interesting, I click on a link within it.
- I intend to open emails from people that I know.
- I don't open email attachments if the sender is unknown to me.
- I download any files onto my work computer that help me get the job done.
- Before reading an email, I always check if the subject and the sender make sense.
- I am confident of recognizing a suspicious email.
- I do not open email attachments if the content of the email looks suspicious.
- I know I need to be careful before opening email attachments.
- I exercise caution when I receive an email attachment as it may contain a virus.

Participants expressed their perspectives by rating their agreement or disagreement on a scale of 1 to 5 for each question. The objective is to analyze this data comprehensively, identifying trends and behavior patterns related to phishing. In the upcoming "Results" section, we will delve into the specifics, emphasizing prevalent user sentiments and proposing enhancements in awareness and conduct concerning phishing security. The ultimate goal is to furnish insights that can contribute to the enhancement of cybersecurity practices.

7. Results

Within this section, we encapsulate the study's findings and meticulously analyze the compiled data. Participants conveyed their perspectives by responding to a series of statements or questions, utilizing a range of five categories: "Strongly Agree," "Somewhat Agree," "Neither Agree nor Disagree," "Somewhat Disagree," and "Strongly Disagree."

7.1. Clicking on Email Links

Strongly Disagree: 20%, Disagree: 40%, Neither Agree nor Disagree: 10%, Agree: 20%, Strongly Agree: 10%

7.2. Opening Email Attachments

Strongly Disagree: 15%, Disagree: 35%, Neither Agree nor Disagree: 20%, Agree: 20%, Strongly Agree: 10%.

7.3. Downloading Files on Work Computer

Strongly Disagree: 15%, Disagree: 30%, Neither Agree nor Disagree: 15%, Agree: 25%, Strongly Agree: 15%

7.4. Probability of Receiving Malicious Emails

Strongly Disagree: 5%, Disagree: 15%, Neither Agree nor Disagree: 15%, Agree: 40%, Strongly Agree: 25%

7.5. Checking Email Links Authenticity

Strongly Disagree: 5%, Disagree: 10%, Neither Agree nor Disagree: 10%, Agree: 40%, Strongly Agree: 35%

7.6. Verifying Email Attachments

Strongly Disagree: 5%, Disagree: 10%, Neither Agree nor Disagree: 15%, Agree: 45%, Strongly Agree: 25%

7.7. Phishing Attack Possibility

Strongly Disagree: 5%, Disagree: 15%, Neither Agree nor Disagree: 15%, Agree: 40%, Strongly Agree: 25%

7.8. Best Way to Avoid Phishing Attacks

Strongly Disagree: 5%, Disagree: 10%, Neither Agree nor Disagree: 10%, Agree: 45%, Strongly Agree: 30%

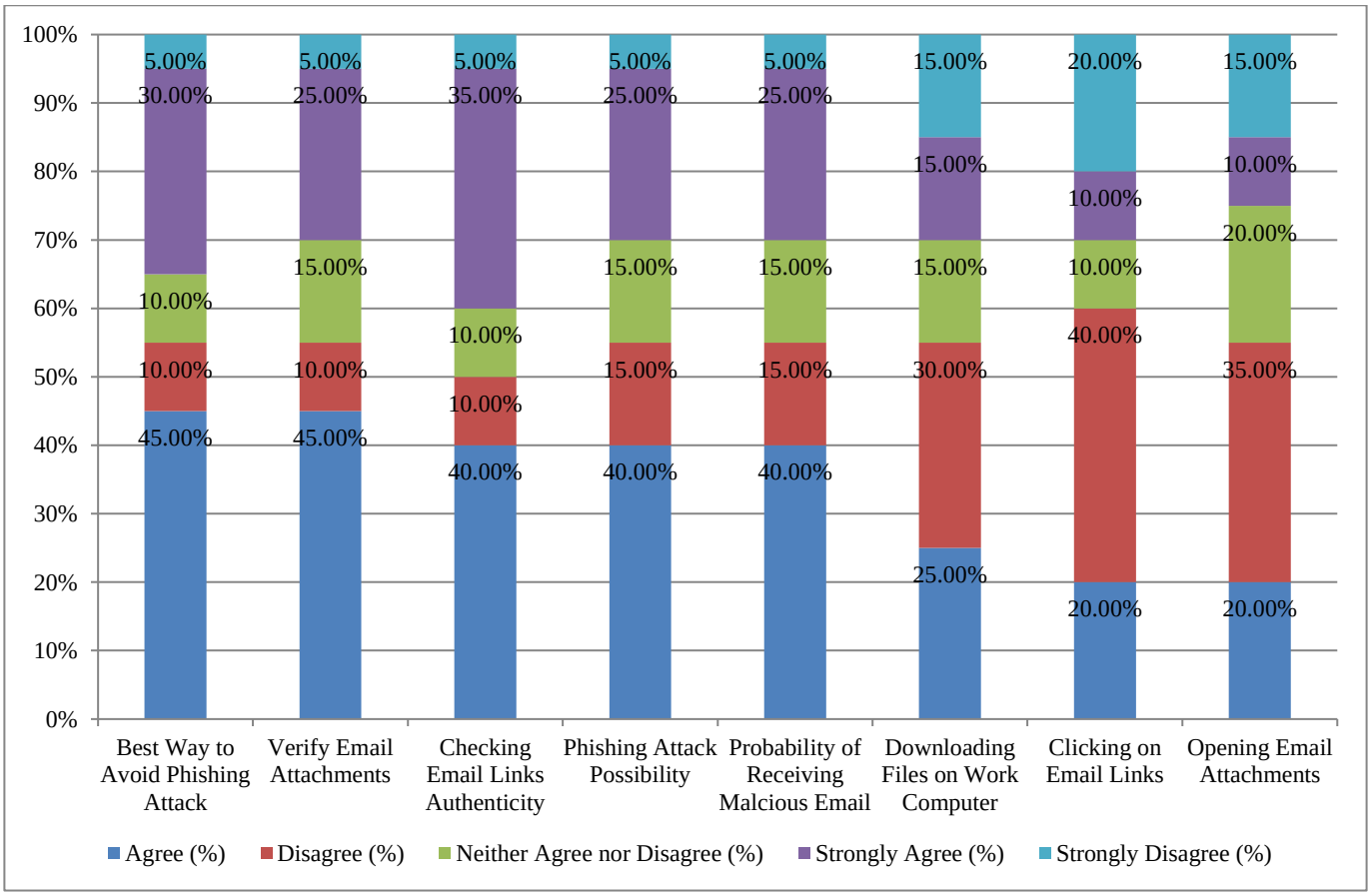

Fig. 3 Survey results based on questions

Respondents often strongly agree with questions 3, 4, 6, 7, 8, and 10. These statements likely convey positive or agreeable sentiments. Questions 2, 5, and 9 seem to have mixed responses, with a combination of "Somewhat Agree," "Neither Agree nor Disagree," and "Somewhat Disagree." Questions 1 and 10 seem to have a mix of responses, with varying degrees of disagreement. Some respondents consistently give strong agreement or strong disagreement across multiple statements. Others showed more variability in their responses.

In summary, the majority of respondents tend to be cautious about phishing, with a significant percentage recognizing the potential risks of clicking on links and opening attachments. There is a positive trend towards acknowledging the importance of verifying the authenticity of email links and attachments as a preventive measure against phishing attacks, but there is no consistency; hence, it proves that there is a lack of proper behaviors towards phishing.

8. Discussion

It is worth noting that computer user's behavior significantly influences their vulnerability to phishing attacks. Equally, computer users' degree of caution influences their aptitude to recognize phishing attempts. Fundamentally, skeptical and vigilant computer users scrutinize websites, emails, and messages before clicking or browsing on them, while complacent users overlook warning alerts and become phishing victims.

Understanding and knowing about phishing attacks affects the cybersecurity awareness of computer users. Security-cautious computer users with less risk-taking behavior are less likely to fall victim to phishers since they secure their computers and systems using spam filters and antivirus programs.

Nonetheless, computer users with risk-taking behavior neglect using security tools thus leaving themselves susceptible to phishing attempts. The data reveals a nuanced perspective on individuals' behaviors and attitudes towards email security and phishing awareness. Across various statements, respondents generally exhibit a heightened awareness of potential risks associated with email interactions. Let us delve into some key points:

8.1. Risk Perception

A substantial number of respondents express caution regarding clicking on email links, opening attachments, and downloading files on work computers. This indicates a widespread understanding of the potential risks involved in these actions.

8.2. Email Attachment Verification

The majority of participants seem to take a proactive approach by checking the authenticity of email attachments before opening them. This behavior aligns with best practices for avoiding malicious content, showcasing a sense of responsibility towards maintaining cybersecurity.

8.3. Probability Assessment

A noteworthy percentage acknowledges the realistic possibility of receiving malicious email attachments. This realistic appraisal suggests that users are not underestimating the prevalence of cyber threats and are conscious of the need for vigilance.

8.4. Phishing Attack Prevention

Respondents generally agree that verifying the authenticity of email links is an effective strategy for preventing phishing attacks. This reflects a consensus on the importance of user verification in maintaining a secure digital environment.

9. Conclusion

Computer users' behavior plays a vital role in influencing their cybersecurity awareness towards phishing attacks. The sophistication of phishing attempts and attacks necessitates increased concentration on computer user's behavior, vigilance, and cybersecurity education. As the lack of sufficient cybersecurity awareness makes computer users fall victim to phishers, their behavior leads them to tendencies like clicking malicious links, ignoring warning signs, and sharing vital sensitive information, which results in successful phishing attacks.

To raise the level of cybersecurity awareness of computer users towards phishing attacks, organizations and computer users alike should focus on adopting an anti-phishing behavior, conducting regular phishing simulations, offering cybersecurity training programs, and offering employees timely feedback on their cybersecurity behavior.

Ultimately, computer users can have a vigilant and proactive approach to cybersecurity and good online behavior through fostering a proactive cybersecurity-conscious culture of mitigating phishing threats and securing the digital environment. The data highlights a positive trend in users' awareness and cautious behavior concerning email security.

It is encouraging to observe that a significant portion of respondents approach email interactions with a discerning eye, recognizing the potential dangers of phishing attacks. The proactive measures, such as verifying attachments and links, demonstrate a willingness to take responsibility for personal cybersecurity.

However, it is crucial to acknowledge the presence of a minority who may not exhibit the same level of caution. Continued efforts in education and awareness campaigns could further enhance overall cybersecurity literacy.

This might include promoting the use of cybersecurity tools, regularly updating knowledge on emerging threats, and fostering a culture of skepticism towards unsolicited emails.

In conclusion, while the majority demonstrates commendable cybersecurity practices, there is an opportunity for ongoing education to empower users and further reduce the risk of falling victim to sophisticated cyber threats.

The data suggests a positive foundation upon which to build a more resilient and security-aware user community.

Acknowledgments

We, researchers, would like to thank Microsoft for providing big data tools to conduct extensive research related to phishing website detection. We want to express our sincere appreciation and our deepest gratitude to Colorado Technical University faculty members for providing guidance in research and writing papers. We also thank the anonymous referee, reviewers, and editors for reviewing our paper. Finally, we sincerely thank the Journal of Artificial Intelligence Tech Science Press for allowing us to publish the paper.

References

[1] Zainab Alkhalil et al., "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science*, vol. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Heather J. Parker, and Stephen V. Flowerday, "Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks," *South African Journal of Information Management*, vol. 22, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Giuseppe Desolda et al., "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Computing Surveys*, vol. 54, no. 8, pp. 1-35, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse, "Phishing Attacks and Defenses," *International Journal of Security and its Applications*, vol. 10, no. 1, pp. 247-256, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[5] Dhruv Bhanderi et al., "Impact of Two-Factor Authentication on User Convenience and Security" *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE*, pp. 617-622. 2023. [Google Scholar] [Publisher Link]

[6] Dinesh Kalla et al., "Phishing Detection Implementation Using Databricks and Artificial Intelligence," *International Journal of Computer Applications*, vol. 185, no. 11, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Kuraku Sivaraju, *Curiosity Clicks: The Need for Security Awareness*, University of the Cumberlands ProQuest Dissertations Publishing, 2022. [Google Scholar] [Publisher Link]

[8] Casey Crane, The Dirty Dozen: the 12 Most Costly Phishing Attack Examples, *The SSL Store*, 2019.[Google Scholar] [Publisher Link]

[9] D. Stafford Christina, *Weakest Link: Assessing Factors that Influence Susceptibility to Falling Victim to Phishing Attacks and Methods to Mitigate*, Utica College ProQuest Dissertations Publishing, 2020. [Google Scholar] [Publisher Link]

[10] David Maimon et al., "A Routine Activities Approach to Evidence-Based Risk Assessment: Findings from Two Simulated Phishing Attacks," *Social Science Computer Review*, vol. 41, no. 1, pp. 286-304, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Sivaraju Kuraku, and Dinesh Kalla, "Impact of Phishing on Users with Different Online Browsing Hours and Spending Habits," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 12, no. 10, pp. 34-41, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Prashanth Rajivan, Efrat Aharonov-Majar, and Cleotilde Gonzalez, "Update Now or Later? Effects of Experience, Cost, and Risk Preference on Update Decisions," *Journal of Cybersecurity*, vol. 6, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hossein Abroshan et al., "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," *IEEE Access*, vol. 9, pp. 44928-44949, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ahmed Alzahrani, "Coronavirus Social Engineering Attacks: Issues and Recommendations," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020. [CrossRef] [Google Scholar] [Publisher Link]