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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121005

# Impact of phishing on users with different online browsing hours and spending habits

**Dr. Sivaraju Kuraku[1], Dinesh Kalla[2], Fnu Samaah[3]**

University of the Cumberlands, Williamsburg, KY 40769, USA[1]

Colorado Technical University, Colorado Springs, CO 80907, USA[2]

Harrisburg University of Science and Technology, Harrisburg, PA 17101, USA[3]

**Abstract**: Due of an upward trend in browsing habits and time spent online, the number of phishing attacks on online users has spiked. Phishers use fake websites, phone calls, emails, and text messages in phishing attacks to deceive people into passing up their personal information or sensitive data, downloading malware, or making themselves or the organization they work for vulnerable to cybercrime. This paper looks at how a person's online spending habits and the amount of time they spend browsing the internet affect their awareness of phishing. By looking at the relationship between the amounts of time they spend on the web, their online browsing habits, and how they are aware of phishing attacks, the research also intends to raise cybersecurity awareness and reduce the risks of phishing attacks. The research findings demonstrate that individuals with longer online spending hours tend to have a higher susceptibility to phishing attacks, often falling victim to deceptive tactics employed by phishers. Conversely, those who exhibit more responsible online spending habits and depict security-conscious behaviours are better equipped to detect and thwart phishing attempts effectively. By shedding light on this relationship between online spending habits and security awareness, this study contributes to the collective efforts to enhance online safety and reduce the incidence of successful phishing attacks. The results presented in this paper offer valuable insights for individuals, organizations, and cybersecurity professionals seeking to bolster defences against phishing threats.

**Keywords:** Phishing Attacks; Security awareness; Online spending hours; Browsing habits; Phishers

## I. INTRODUCTION

Phishing is a sort of social engineering method that attackers use to get sensitive information, like personal data, passwords, usernames, and credit card numbers, by pretending to be trustworthy people or companies on websites or in emails. They lure consumers into clicking on their malicious links by making themselves look like legitimate online services, social networking platforms, or banks [1]. Security awareness in the online environment plays a crucial role in a person's understanding of possible threats on phishing attempts. Equally, Security awareness enables individuals who spend their time online to recognize phishing attempts, like personal information requests, grammatical errors, or suspicious links and email addresses, and avoid such phishing scams [2]. As the online environment contains a variety of personal information, including private communications, passwords, and financial information, security awareness enlightens online users on safeguarding their information and any consequences of unauthorized disclosure.

Since phishing attacks aims on stealing people's personal information with an objective of perpetrating identity theft, security awareness educates online users to not only protect their personal information but also safeguard their financial assets [3]. As well, security awareness warns online users from clicking on malicious links and downloading suspicious emails and files, thus preventing malware infections. The amount of time that people spend online significantly influence their security awareness on phishing [4]. This is because the duration of browsing and online spending hours plays a crucial role in enabling an individual identify phishing attempts and understand their potential threats [5]. However, online users are more exposed to phishing attempts and attacks the more they spend time engaging with numerous online platforms.

The landscape of cybersecurity is continually evolving, with phishing attacks remaining a persistent and dynamic threat in the digital realm. Over the years, phishers have adapted and become more sophisticated in their techniques, making it increasingly challenging for individuals to identify and protect themselves from these threats [6]. With the rise of social engineering tactics, where attackers manipulate human psychology, emotions, and trust, phishing has grown into a multifaceted menace that targets not only personal data but also exploits organizational vulnerabilities. The evolution in phishing tactics includes spear-phishing, where attackers craft highly personalized and convincing messages, and vishing, a form of phishing carried out through voice calls, further blurring the lines between legitimate communication and malicious intent [7]. Understanding the nuances of this evolving landscape is crucial for comprehending the complex

  

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal ⁜ Vol. 12, Issue 10, October 2023
DOI: 10.17148/IJARCCE.2023.121005

interplay between online habits, awareness, and susceptibility to phishing attacks [8]. As technology advances, and phishing becomes increasingly sophisticated, it is imperative to explore the factors that influence individuals' vulnerability to these threats, which is a central focus of this study [9].

The significance of contextualizing an individual's online spending habits within the broader context of cybersecurity awareness cannot be overstated. People's online behavior is hugely influenced by a multitude of factors, which incorporate their personal interests, professional requirements, and most essentially, social connections. As users traverse various online platforms and engage in diverse activities, their exposure to potential phishing attacks differs and increases as they stay online for longer. For instance, a person who spends extended hours on social media may encounter phishing attempts embedded in fake friend requests or enticing social content, whereas the one immersed in online shopping may face threats through counterfeit e-commerce sites or bogus promotional emails [10]. Consequently, examining online spending hours is not solely about quantifying time but understanding the unique digital environments and risk factors associated with different online activities [11]. This nuanced perspective is vital for tailoring effective cybersecurity education and countermeasures to suit various user profiles and activities, ultimately reducing the impact of phishing attacks in an increasingly interconnected world.

## II. BACKGROUND ON PHISHING

Phishing, traditionally referred to as brand spoofing or carding, was coined in 1996 after hackers utilized an algorithm, made randomized credit cards, and stole the passwords of users at America Online [12]. Afterwards, phishers utilized emails or instant messages to reach their targeted users by masquerading as America Online employees and convincing them to disclose their passwords [12]. After successfully stealing customers sensitive information by tricking them into updating their accounts, they began targeting larger fiscal institutions. Although the growth of internet usage has led to increased online presence as it has modernized people's ways of accessing information, communicating, interacting, and shopping, it has also exposed online users to phishing attacks, which are executable through malicious websites, links, emails, and online platforms.

The study posits those online habits influence people's vulnerability to phishing, particularly the habitual use of Facebook leading to increased vulnerability to social media related phishing attacks [13]. Users with increased online spending, mainly those that are extremely active on social platforms are additionally vulnerable to social engineering attacks compared to those who partake on social platforms less often. Furthermore, study conducted states that a people's online habits determine how they process inaccurate social engineering techniques on platforms like social media sites [13]. Therefore, poor online spending habits increase people's vulnerability to phishing attacks because they open links and reply messages without paying attention or engaging enough cognitive resource to their behaviour of spending time online. Banking credential stealing with Malware's like Emotet observed and noticed on users with online browsing and banking [14]. A study determined that people who habitually utilize Facebook are highly likely to be deceived by phishers who use phoney profiles and are highly prove to disclose sensitive information requested by attackers [15]. Hence, online spending habits influence user's vulnerability to fall victim of phishers on social media through causing them trail ritualized or blind patterns of using social media that involve less cognitive engagement during use of the platform.

The use of social platforms like Facebook with less cognitive engagement increases the likelihood that user's inconsiderately click malevolent links in messages and unknowingly accepts friend requests originating from fake profiles without contemplating on the possible consequences of their actions [13]. Behaviours like scrolling posts, liking and sharing posts, and clicking links regularly lead to users not paying enough attention to misleading information on social platforms. A supplementary study by Albladi & Weir, (2020) explains that Facebook spending hours results in increased susceptibility to phishing attacks because that habit negatively influences the risk perception and trust of users.

The dependency and usage of the internet increased exponentially during Covid-19 pandemic's period as people's necessity to do online activities like online shopping, remote working, and e-learning increased. This increased online spending resulted in increased susceptibility to cyber security attacks like denial-of-service, identity theft, ransomware, malware, and phishing. Phishing attacks are predominant among social media users because they are lured into accepting friend requests from phishers using fake profiles and subsequently clicking on their malicious links and as a result losing their passwords, credential information, and worst cases, losing control of their social media accounts.

A study conducted during the Covid-19 period on phishing by indicates that the ethical risk-taking, anxiety and stress levels caused by reassurance-seeking and compulsive checking could influence the success of phishing attacks on social platform users during Covid-19 [16]. Precisely, study posits that users with stress because of the fear of coming into contact with potentially contaminated surfaces or objects opened or clicked Covid-19 phishing attachments and links respectively while users exhibiting reassurance checking and compulsive checking related stress are vulnerable to Covid-

DOI: 10.17148/IJARCCE.2023.121005

19 phishing scams [17]. Stress plays a crucial role in users falling victims of phishers because users with reassurance seeking and compulsive checking related stress became victims of phishing attacks through clicking on Covid phishing attachments and links while finding additional information on Covid-19, such as the current status of Covid-19 infected people and Covid-19 vaccination [17].

Additionally, study posits that the level of education of users engaging in social media platforms determine the success of phishing attacks executed through common phishing tries during Covid-19, with the more educated users having high willingness to click on phishing links and respond to phishing emails [17]. While a study done prior covid-19 showed that individuals with lower level of education are more likely to fall victim to phishing attacks, considering the study's partakers were university students, the research showed that more educated social media users are at higher risk of falling victim of phishers during the pandemic [18]. However, the research suggests that further studies should be conducted on the positive association of education level with becoming a victim of phishing attacks. Due to significant increase in phishing attacks ChatGPT are used to spot patterns related to anomalies and potential cyber threats [19]

The choice of the information processing method to be utilized by people who spend hours browsing on the internet depends on the person's perception of sufficiency of available information [20]. Hence, individuals either use heuristic processing, which involves utilizing less cognitive resources in order to make decisions and judgements, or systematic processing that entails carefully assessing information to make decisions and judgements. Technology affordances expose social media users to information overloads that encourages them to process the easily available information heuristically to make effortless and quick judgements [20]. Consequently, this significantly increases user's vulnerability to phishing attempts and attacks because they overlook cues that may indicate malicious messages when processing information heuristically. Users experiencing information overloads regularly trust phishing attachments and messages due to heuristics information processing relying on judging information's credibility based on seeming or phony cues.

## III. PROBLEM STATEMENT

Online spending habits or activities like commenting, liking photos, posts, posting videos, and sending photos can seem rewarding for individuals and therefore encourage further social media platforms usage. This gratification results in the repetitive, frequent, and increased online spending that together with user's inability to regulate and control these online activities, leads to users getting unconscious habits during their engagement on online platforms. The increase in people's necessity to spend time in online platforms, like social media and e-commerce, engaging and browsing online exposes them to numerous security risks like phishing attacks. Notably, the habitual utilization of social medial make users highly vulnerable to phishing attacks since they do not carefully process links and messages with caution. Users and people who frequently engage in online platforms tend to be additionally vulnerable to phishing attempts and attacks and this correlation to factors such as high online interaction, potential contentment to security measures, and high exposure to social engineering attacks. This study aims on exploring how online spending and browsing hours determine and shape an individual's security awareness about phishing. Understanding the relationship between online spending habits and browsing hours and online user's security awareness will be crucial in defending against phishing attacks.

## IV. SIGNIFICANCE OF STUDY

This study is important for various reasons. The first one is because phishing is a major online threat that involves tricking people in revealing their sensitive information and therefore, understanding how user's browsing hours and online spending habits influence their security awareness can help in mitigating risks related to phishing attacks. Secondly, the study can help online users assess their involvement and subsequent exposure to the internet and social platforms through their online spending behaviour. Thirdly, the study will enlighten online users that their browsing hours show the time they spend online and hence likelihood of coming across phishing attempts. This will enable users identify susceptible periods when they can be more vulnerable to phishing attempts, such as when they have information overload and when tired. The study is also important because it can help to tailor cybersecurity awareness programs.

Fundamentally, this study's findings can inform advancement of targeted phishing awareness programs. By understanding precise behaviour and complacency that cause them to fall victim of phishers while spending time online, users can be equipped to identify and effectively respond to phishing attacks [21]. Additionally, this study can help users increase their security awareness on phishing attacks through identifying correlations and patterns amid security awareness, browsing hours and online spending, to enhance security strategies and measures to mitigate risks related to phishing. Due to phishing attacks resulting in negative consequences like identity theft and financial loss for individuals, the study can help users exercise safe browsing, thus enabling them to safeguard themselves and their financial, as well as personal information while conducting their activities online. The phishing attacks study is more important due to increase in attacks on social media users because they are enticing into accepting unknown friend requests from fake profiles [22].

  

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121005

## V. METHODOLOGY

This quantitative study methodology examined how online browsing hours and spending habits affect security awareness of phishing identification patterns. Participants were anonymously surveyed using Qualtrics online service. This study targeted US workers between the ages of 18 and 34. The survey questionnaire was distributed via the professional network LinkedIn. Additionally, the following two demographic questions were added to PhishingBox's quiz: 1). How old are you? 2). How many hours per day do you spend online with 3 options such as 1-4 Hours, 5-8 Hours, and More than 9 Hours? The president of PhishingBox additionally granted authorization for this study to use an online phishing IQ test at https://www.phishingbox.com/phishing-iq-test. The survey included an online quiz that participants could use to test how well they could spot phishing. The ten screenshots of emails that were either phishing efforts or real messages from big companies were shown to the people who took the test. After looking at each screenshot, participants had to say whether the email was "legitimate" or "phishing." After answering a question, the quiz would show in a different color whether the answer was right (Green Color) or wrong (Red Color). After answering all 10 questions, participants received their scores. In the "Results" part, the data collection will be looked at and explained in detail.

## VI. RESULTS

This section summarizes the study's findings and analyses the collected data. The purpose of this section is to examine how the participant's online activity and spending habits shaped their vulnerability to phishing attacks. 83 participants accurate survey responses have been collected. 17 participants reported that they spend between one and four hours every day using the internet. The results of recognizing phishing patterns showed that out of seventeen participants, only one earned a perfect 100 on identifying phishing. The average phishing recognition score among them is 57.5, which is significantly lower when compared to the score for recognizing attacks utilizing phishing through the use of email communication.

Table 1: 1- 4 Hours Online – Phishing Score

| Stats | Value |
|---|---|
| Mean | 57.5 |
| Standard Error | 3.92640633 |
| Median | 60 |
| Mode | 40 |
| Standard deviation | 15.7056253 |

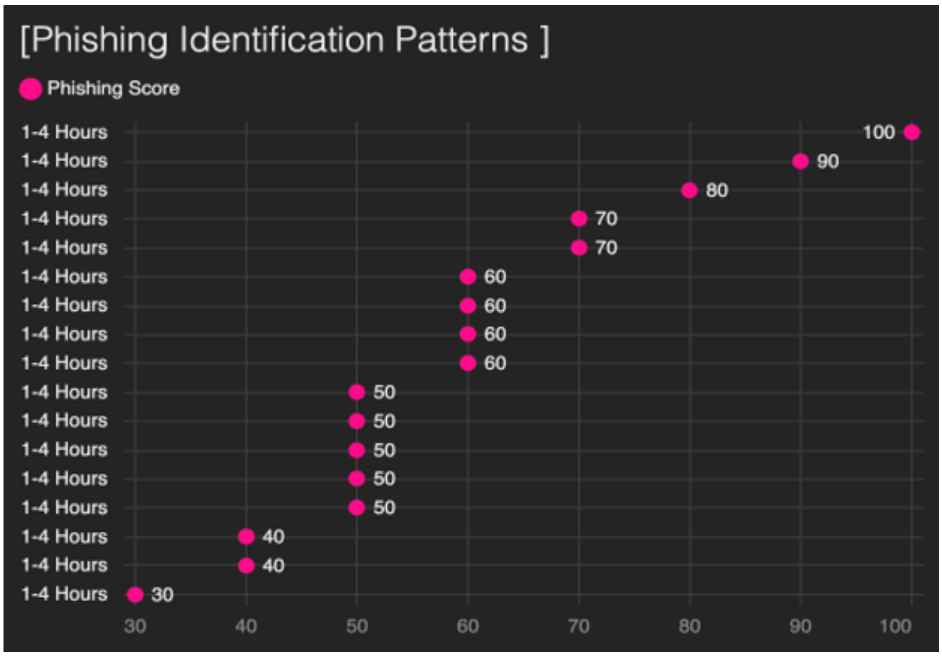


Figure 1: Dot Plot: 1-4 Hours Online vs Phishing Score

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121005

29 participants said that they spend 5-8 hours online per day. Phishing pattern results revealed that no one scored 100. The mean phishing identification score among them is 58.92, which is considerably less than identifying phishing attacks through email communication.

Table 2: 5-8 Hours Online – Phishing Score

| Stats | Value |
|---|---|
| Mean | 58.92857143 |
| Standard Error | 3.100575374 |
| Median | 60 |
| Mode | 60 |
| Standard deviation | 16.40670272 |

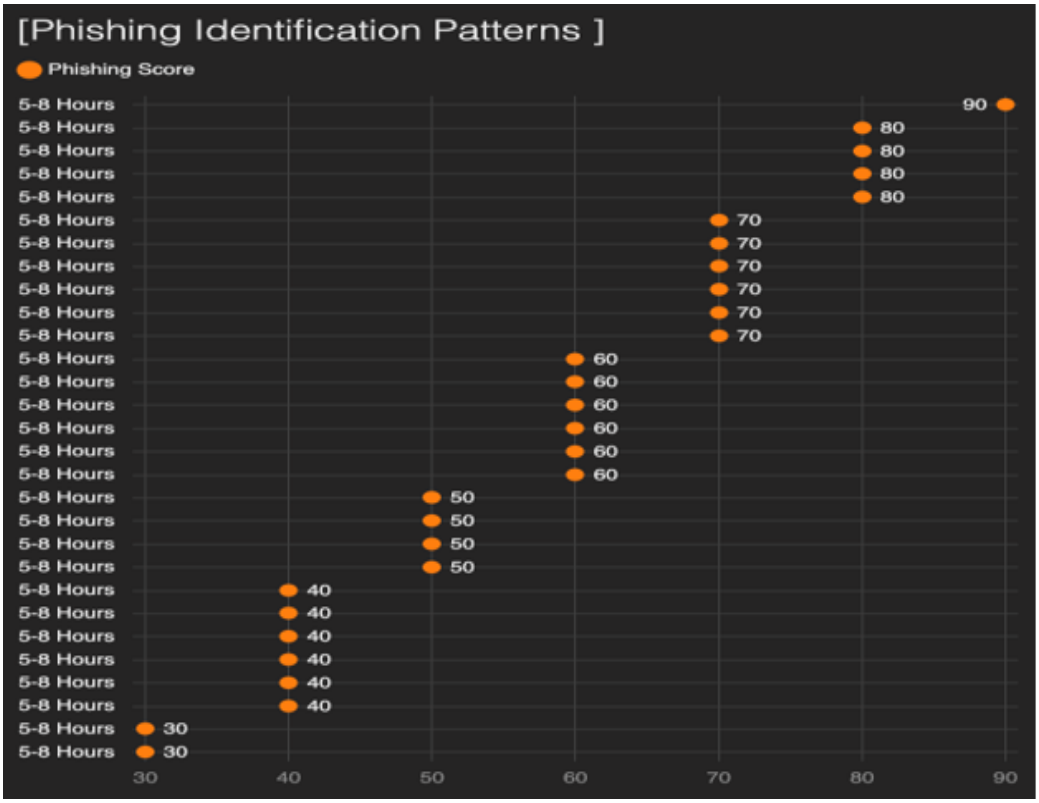


Figure 2: Dot Plot: 5-8 Hours Online vs Phishing Score

37 of the participants reported that they spend more than nine hours each day using the internet. The results of the phishing method revealed that no one earned a perfect 100. The average phishing identification score among them is 61.94, which is a level that is significantly lower than that required to identify a phishing attack through the use of email communication.

Table 3: More than 9 Hours Online – Phishing Score

| Stats | Value |
|---|---|
| Mean | 61.944444 |
| Standard Error | 2.545442377 |
| Median | 60 |
| Mode | 60 |
| Standard deviation | 15.27265426 |

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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121005

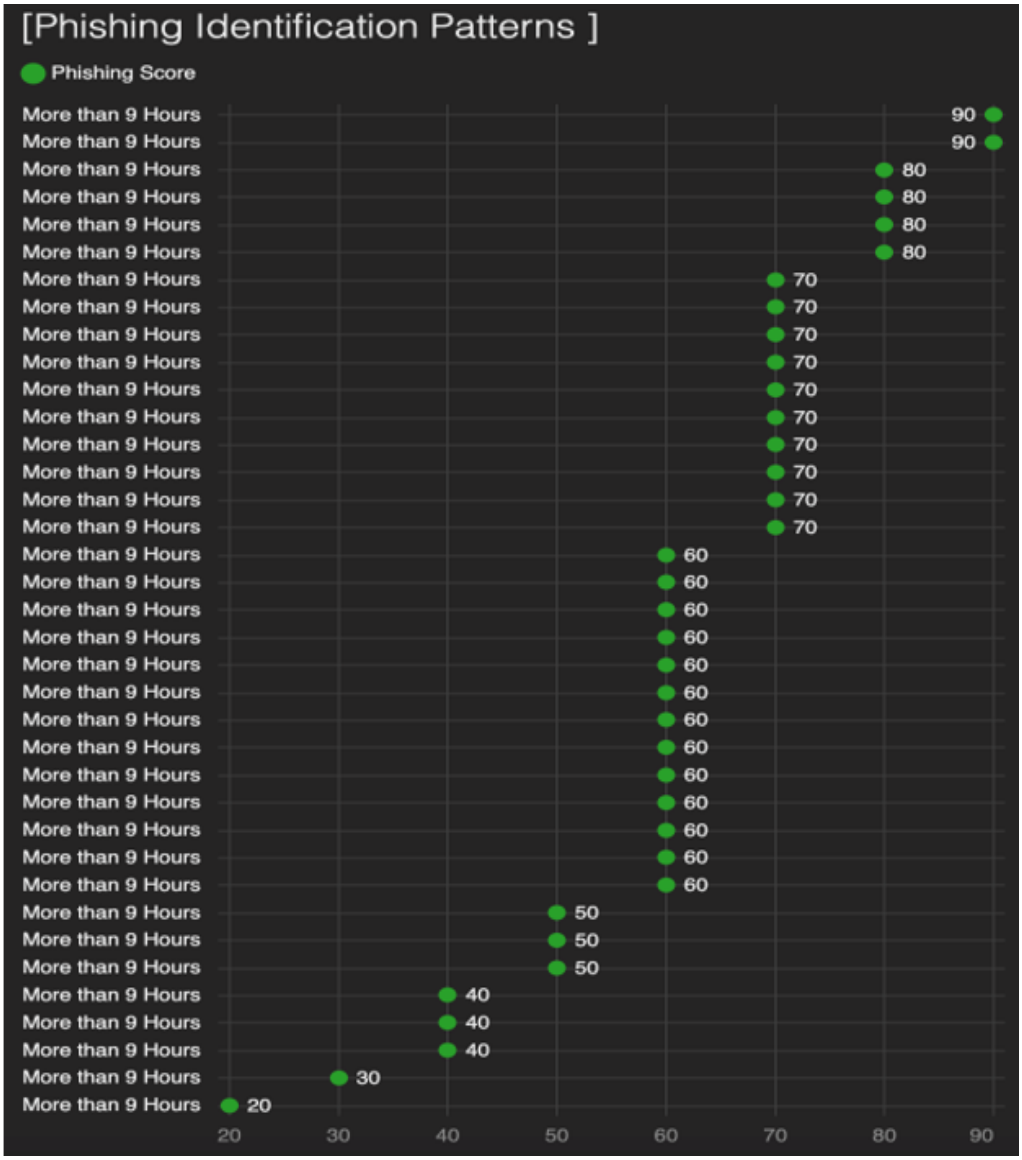


Figure 3: Dot Plot: More than 9 Hours Online vs Phishing Score

The overall responses of the respondents helped in determining how the online browsing hours and spending habits of users influence their security awareness of phishing identification patterns.

## VII. DISCUSSION

Although users spend more time browsing the internet and engaging in online activities like email communication, the exposure enlightens them on phishing attack channels like fake websites, social media messages, and emails, enabling them to protect their personal and financial assets and become more resilient to such attacks. Equally, frequent online users who spend a considerable amount of time interacting with and browsing on different online platforms and websites are likely to familiarize themselves with phishing tactics like fraudulent URLs, attachments, email spoofing, and deceptively designed websites, which can enable them to develop an intensified sense of consciousness regarding phishing attempts, thus understanding warning signs and phisher's flaws linked to phishing attacks. As people develop poor online spending habits as they process inaccurate information on platforms, thus increasing their vulnerability to phishing attacks as they open links and reply to messages without paying attention or engaging enough cognitive resources to their behavior of spending time online, they need to hone their security education and security awareness through training programs, articles, and resources, utilizing tools and features that cybersecurity experts offer on online platforms, such as warning banners and spam filters to identify potential phishing emails.

DOI: 10.17148/IJARCCE.2023.121005

## VIII. CONCLUSION

Results revealed that online browsing and spending hours online considerably influence users' security awareness of phishing. Moreover, the mean phishing identification score among participants is considerably lower, making it very inefficient to identify phishing email attacks through email communication, regardless of the number of hours they spent online. Hence, it is very important to do more research on online browsing spending habits, and provide solid security awareness. Notably, prolonged exposure to the internet, online activities, and platforms increases a user's probability of coming across phishing attempts, resulting in increased familiarity with the characteristics of phishing attacks. Nevertheless, it is important for online users to enthusiastically seek cybersecurity awareness, stay informed of evolving phishing tactics, and adopt security best and not clicking unknown links or opening unknown attachments, to effectively mitigate risks related to phishing attacks.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## REFERENCES

[1]. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, *9*, 44928-44949. https://doi.org/10.1109/access.2021.3066383.

[2]. Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or not phishing? A survey on the detection of phishing websites. *IEEE Access*, *11*, 18499-18519. https://doi.org/10.1109/access.2023.3247135

[3]. Berens, B. M., Dimitrova, K., Mossano, M., & Volkamer, M. (2022). Phishing awareness and education – When to best remind? *Proceedings 2022 Symposium on Usable Security*. https://doi.org/10.14722/usec.2022.23075

[4]. Kumar, M., Darshan, S. S., & Yarlagadda, V. (2023). Introduction to the Cyber-Security Landscape. In Malware Analysis and Intrusion Detection in Cyber-Physical Systems (pp. 1-21). IGI Global.

[5]. Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 101862. https://doi.org/10.1016/j.cose.2020.101862

[6]. Georgescu, T. M. (2021). A Study on how the Pandemic Changed the Cybersecurity Landscape. Informatica Economica, 25(1).

[7]. Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. SN Computer Science, 3(2), 170.

[8]. Ramakrishnan, U. P., & Tandon, J. K. (2018). The evolving landscape of cyber threats. Vidwat, 11(1), 31-35.

[9]. Kalla, D., Samaah, F., Kuraku, S., & Smith, N. (2023). Phishing detection implementation using Databricks and Artificial Intelligence. *International Journal of Computer Applications*, *185*(11), 1–11. https://doi.org/10.5120/ijca2023922764

[10]. Nkongolo, M. (2023). Navigating the complex nexus: cybersecurity in political landscapes. arXiv preprint arXiv:2308.08005.

[11]. Bharadiya, J. (2023). Machine Learning in Cybersecurity: Techniques and Challenges. European Journal of Technology, 7(2), 1-14.

[12]. Cui, Q., Jourdan, G., Bochmann, G. V., Couturier, R., & Onut, I. (2017). Tracking phishing attacks over time. *Proceedings of the 26th International Conference on World Wide Web*. https://doi.org/10.1145/3038912.3052654

[13]. Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *SA Journal of Information Management*, *22*(1). https://doi.org/10.4102/sajim.v22i1.1176

[14]. Kuraku, S.; Kalla, D. Emotet Malware–A Banking Credentials Stealer. Iosr J. Comput. Eng. 2020, 22, 31–41.

[15]. Vishwanath, A. (2014). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, *20*(1), 83-98. https://doi.org/10.1111/jcc4.12100

[16]. Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00047-5

[17]. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, *9*, 121916-121929. https://doi.org/10.1109/access.2021.3109091.

[18]. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1753326.1753383

  

DOI: 10.17148/IJARCCE.2023.121005

[19]. Kalla, D., & Smith, N. (2023). Study and Analysis of Chat GPT and its Impact on Different Fields of Study. International Journal of Innovative Science and Research Technology, 8(3). 827-833.

[20]. Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146-1166. https://doi.org/10.1177/0093650215627483

[21]. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, *54*(8), 1-35. https://doi.org/10.1145/3469886

[22]. Eian, I. C., Yong, L. K., Li, M., Qi, Y. H., & Z, F. (2020). Cyber-attacks in the era of COVID-19 and possible solution domains. https://doi.org/10.20944/preprints202009.0630.v1

## BIOGRAPHY

**Sivaraju Kuraku** is free-lancing with iStreetLabs LLC as a principal security consultant. With approximately 8 years of practical experience in incident handling, SOC operations, endpoint security & defense, malware research analysis & remediation, malware playbooks, threat hunting, Kubernetes container security, and vulnerability management, he is a Cyber Security SME and Leader with a strong academic background and business acumen. He also has the honor of having led MDR services and coached teams to manage numerous project assignments with excellent individual and team effort while working for leading cyber security product startups, CrowdStrike and Uptycs.

**Dinesh Kalla** is currently working at Microsoft as Big Data and Azure Cloud Escalation Engineer and has 8 years of industry experience as a .Net Developer, BI Developer, Data Engineer and Azure Cloud Engineer. His main areas of expertise and research interest are in Big Data Analytics, Data Science, Machine Learning, Artificial Intelligence, IOT and Cybersecurity. He published several papers related to Big data, Artificial Intelligence and cybersecurity threats in international Journals and conferences. He completed his Masters in University of New Haven and is currently pursuing his Doctoral Degree in Computer Science specialized in BigData from Colorado Technical University.

  