IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

# Navigating the Link Between Internet User Attitudes and Cybersecurity Awareness in the Era of Phishing Challenges

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

School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, USA[1]

Department of Computer Science, Colorado Technical university, Colorado Springs, CO, USA[2]

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

**Abstract:** Phishing attacks persist as a prevalent cyber threat exploiting the vulnerability of internet users, tricking them into clicking malicious attachments or links under the guise of legitimacy. This study aims to investigate the impact of users' attitudes on cybersecurity awareness, specifically focusing on phishing attacks and related social engineering tactics such as smishing, vishing, and spear-phishing. Our findings reveal that internet users with positive and proactive attitudes toward cybersecurity demonstrate heightened awareness of phishing attacks and are more adept at adopting preventive measures. Conversely, those with complacent and dismissive attitudes are more susceptible to falling victim to phishing. The study underscores the importance of tailoring cybersecurity measures to foster a security-conscious and proactive mindset among internet users, ultimately strengthening overall cybersecurity resilience in the face of evolving threats.

**Keywords:** Phishing attacks, cyber threat, internet users, attitude, cybersecurity awareness, phishing attempts, smishing, vishing, spear-phishing, and cybersecurity resilience.

## I. INTRODUCTION

As the relentless march of technological progress continues unabated, the growing dependence of internet users on digital platforms for storing personal data and accessing online services elevates their vulnerability to phishing attacks [1]. Phishing, a sinister form of social engineering orchestrated by cyber attackers, capitalizes on this dependency by deceptively acquiring individuals' or entities' data, with attackers adeptly disguising themselves as legitimate entities.

The arsenal of techniques employed by phishers includes artful strategies such as enticing users to click on malicious attachments or links, thereby initiating a cascade of consequences—ranging from malware installation and theft of sensitive information to the execution of calculated ransomware attacks.

The repercussions of phishing attacks are far-reaching and severe, casting a wide net of financial losses, unauthorized transactions, and identity theft for individuals, while businesses grapple with the jeopardized integrity of sensitive data, ransom demands, and the erosion of their hard-earned reputation [2]. Notwithstanding the strides made in technological advancements leading to the development of robust cybersecurity measures, the human factor remains an indomitable force in the realm of online security. The attitudes exhibited by internet users emerge as a pivotal force in shaping cybersecurity awareness, intricately weaving into their perception of risks and the imperative need for security.

This research endeavours to probe the intricate relationship between users' attitudes and their awareness of phishing attacks, seeking to unravel the nuanced responses to such insidious attempts. The overarching goal is to formulate effective approaches that not only decode user reactions but also mitigate the multifaceted landscape of social engineering attacks, encompassing phishing, smishing, vishing, and spear-phishing.

In response to the escalating tide of phishing emails and the profound impact of human attitudes on cybersecurity, organizations are increasingly turning to cutting-edge solutions. Machine Learning models are emerging as indispensable tools for detecting and filtering phishing emails. This proactive adoption of advanced technologies underscores a concerted effort to fortify defences against the burgeoning threat landscape, marking a strategic response to the evolving dynamics of cyber threats.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

## II. BACKGROUND

The attitude of traditional internet users towards cybersecurity was shaped by various factors like complacency, lack of security awareness, taking basic precautions, and resistance to change [3]. It is worth noting that some internet users had a complacency attitude due to assuming they were not treasured targets to attackers and their online actions were not important to gain cybercriminal's attention. Below figure 1 show increase in phishing emails from year 2020 to first quarter of 2021.

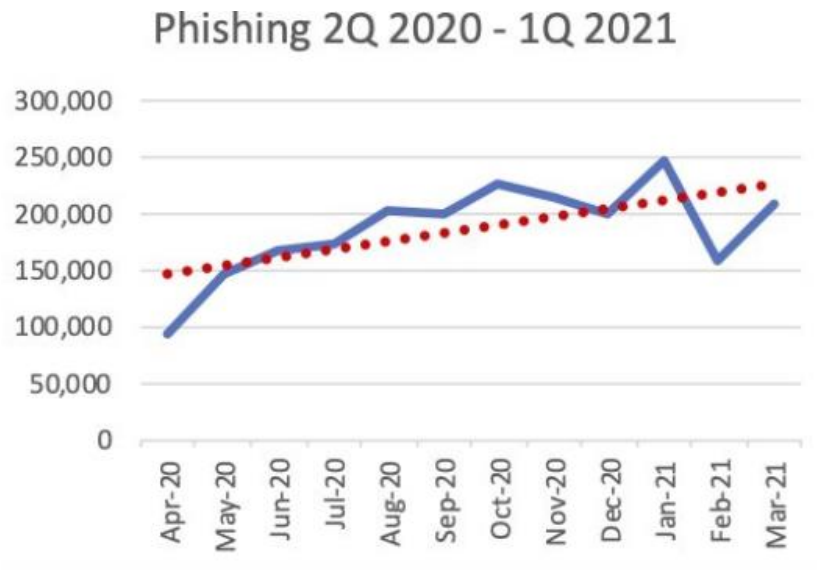


Fig 1: Phishing Attacks 2020-2021 (APWG Report)

Traditional internet users lacked awareness of cyber threats and the need of safeguarding their systems and therefore they did not know possible risks of utilizing the internet or potential outcomes of becoming phished [4]. While traditional internet users took basic security precautions like setting robust passwords, utilizing antivirus software, updating their software on regular basis, they were not aware of advanced cybersecurity measures, thus increasing their vulnerability to phishing attacks. Equally, traditional internet users were resistant to embracing new security practices and technologies because of the discomfort related to change. Internet users who had experienced identity theft, data breaches, or cyber-attacks tended to develop a cautious attitude towards cybersecurity. Personal experiences habitually served as worthy lessons that necessitated internet users to enhance their cybersecurity practices. Additionally, increased coverage of security incidents on the media, increased awareness concerning digital threats, and online educational programs influenced internet consumers to be extremely conscious about their security in the digital world.

## III. PROBLEM STATEMENT

The efficacy of cybersecurity defences remains intricately intertwined with the human element of internet users, despite the continuous evolution of technology fortifying security measures [5]. A pivotal determinant influencing the susceptibility of internet users to phishing attacks is their stance towards cybersecurity. The impact of this attitude on users' ability to detect and thwart phishing attempts is profound; a positive security attitude serves as a shield, while a dismissive one leaves them exposed and highly susceptible to potential phishing attacks.

Therefore, delving into the intricacies of internet users' attitudes becomes paramount in comprehending the dynamics of security awareness and their subsequent vulnerability to phishing endeavours. In the context of this study, attitude encompasses a spectrum of factors, including intentions, beliefs, emotions, and perceptions that shape the approach of internet users toward security practices and the ever-present landscape of cybersecurity threats [6].

The pivotal role played by the attitude of internet users becomes evident in determining whether they proactively adopt measures to shield themselves from phishing attempts or unwittingly succumb to the manipulative tactics of cybercriminals [7]. Unravelling this complex interplay between attitude and cybersecurity outcomes provides valuable insights into developing targeted and effective educational programs and awareness campaigns.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

By acknowledging the nuanced relationship between attitudes and cybersecurity, stakeholders in the realm of online security can craft interventions that go beyond the technical aspects, addressing the human dimension that often serves as the linchpin in the success or failure of cybersecurity measures [8]. Recognizing the multifaceted nature of attitude empowers the formulation of strategies that resonate with users on cognitive and emotional levels, fostering a culture of vigilance and resilience against the ever-evolving landscape of cyber threats.

In conclusion, understanding and dissecting the intricacies of internet users' attitudes towards cybersecurity is imperative for devising comprehensive and tailored approaches to enhance security awareness. Such insights not only aid in fortifying defences against phishing attacks but also lay the foundation for a proactive and resilient cybersecurity culture, ultimately contributing to a safer and more secure digital ecosystem.

## IV. SIGNIFICANCE OF THE STUDY

Understanding how users perceive cybersecurity and respond to phishing attacks is crucial for cybersecurity professionals seeking to fortify digital defences [9]. By tailoring educational efforts and launching targeted awareness campaigns, experts can empower internet users with the knowledge to recognize and thwart potential phishing attempts effectively. The consequences of falling victim to phishing are severe, ranging from the exposure of sensitive personal data to identity theft, financial loss, and compromise of online accounts [10]. This study aims to shed light on users' risky attitudes, providing a foundation for the development of educational strategies that specifically address the nuanced risks associated with phishing attacks, particularly those tied to financial and personal implications.

Beyond the surface, the research delves into the intricate psychological aspects influencing user decision-making. It unveils how cybercriminals skilfully exploit these psychological factors to execute deception successfully. Recognizing the multifaceted nature of internet user attitudes emerges as a pivotal factor in determining the success or failure of phishing attempts and attacks. Internet users who are vigilant and security-aware possess the capability to reduce the likelihood of falling prey to phishing schemes, thereby mitigating the potential for data breaches and associated losses. Furthermore, this study contributes to a more profound understanding of internet user attitudes, providing cybersecurity experts and developers with valuable insights. This deeper understanding enables the crafting of user-centric cybersecurity solutions aligned with the cognitive behaviours and patterns of internet users. The ultimate goal is to create security measures that are not only more effective but also less intrusive. Essentially, the nuanced comprehension of user attitudes cultivated through this study serves as a cornerstone for ongoing refinement and development of cybersecurity strategies tailored to the dynamic and ever-evolving landscape of the digital realm [11].

## V. LITERATURE REVIEW

The attitude of internet users predisposes them to phishing attacks as they believe to be avoiding loss. Research posits that internet users are always ready to give up their privacy attitude for the purpose of getting benefits and as a result, they behave in a manner that makes them act against their judgments, concerning their privacy, to avoid losses or costs such as their online accounts being suspended. As a result, many cybercriminals' notices users' insecurities and capitalizes on such moments by using threats of account suspension or closure to con users into supplying them with their sensitive information like banks details, passwords, or even username and ends up phishing them. Since such ensuing phishing attacks are difficult for internet users to recognize previous studies and research urges internet users to always carefully inspect URLs, be mindful of redirections, check out grammar mistakes, generic salutations, spelling errors and key in their login credentials on sites that are HTTPS protected only, use anti-virus software on their devices and make security upgrades provided by their trusted provider of their internet service.

The research asserts that internet users' risk attitude, under the pretence of ignorance, influences the making of their final decision. For instance, Users' risk attitude influences their aptitude to effectively detect phishing attacks and report them or stop them. Hence, internet users' risk attitude towards cyber deception and security issues influences their susceptibility to cybercrimes. For example, internet users depicting a high-risk attitude or gambling desire have a high possibility of clicking on phishing links, messages, or attachments sent by cybercriminals like phishers, and are likely to become victims to cyber-attacks like phishing, spear-phishing, and ransomware. Developing a good attitude on protective behaviour is important in increasing the awareness of computer users towards cyber threats because it offers behavioural advice on the way to handle phishing messages as well as mitigate their threats, particularly in crimes related to phishing attacks. Computer users can develop a positive attitude concerning protective behaviour after they recognize their susceptibility to becoming phishing victims. The positive attitude on protective behaviour, such as not sharing valuable personal information, plays an important in raising computer users' threat awareness so that they can lower or mitigate risks of phishing attacks.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

Internet users are weak towards combating phishing irrespective of enormous cybersecurity technology and training because of their curiosity. Internet users must overcome their curiosity about clicking malicious links through cybersecurity training in order to detect phishing attempts and attacks regardless of their attitudes, behaviour, and phishing IQ scores. Below Fig 2 shows the trends related to people problem related to cyber attacks.

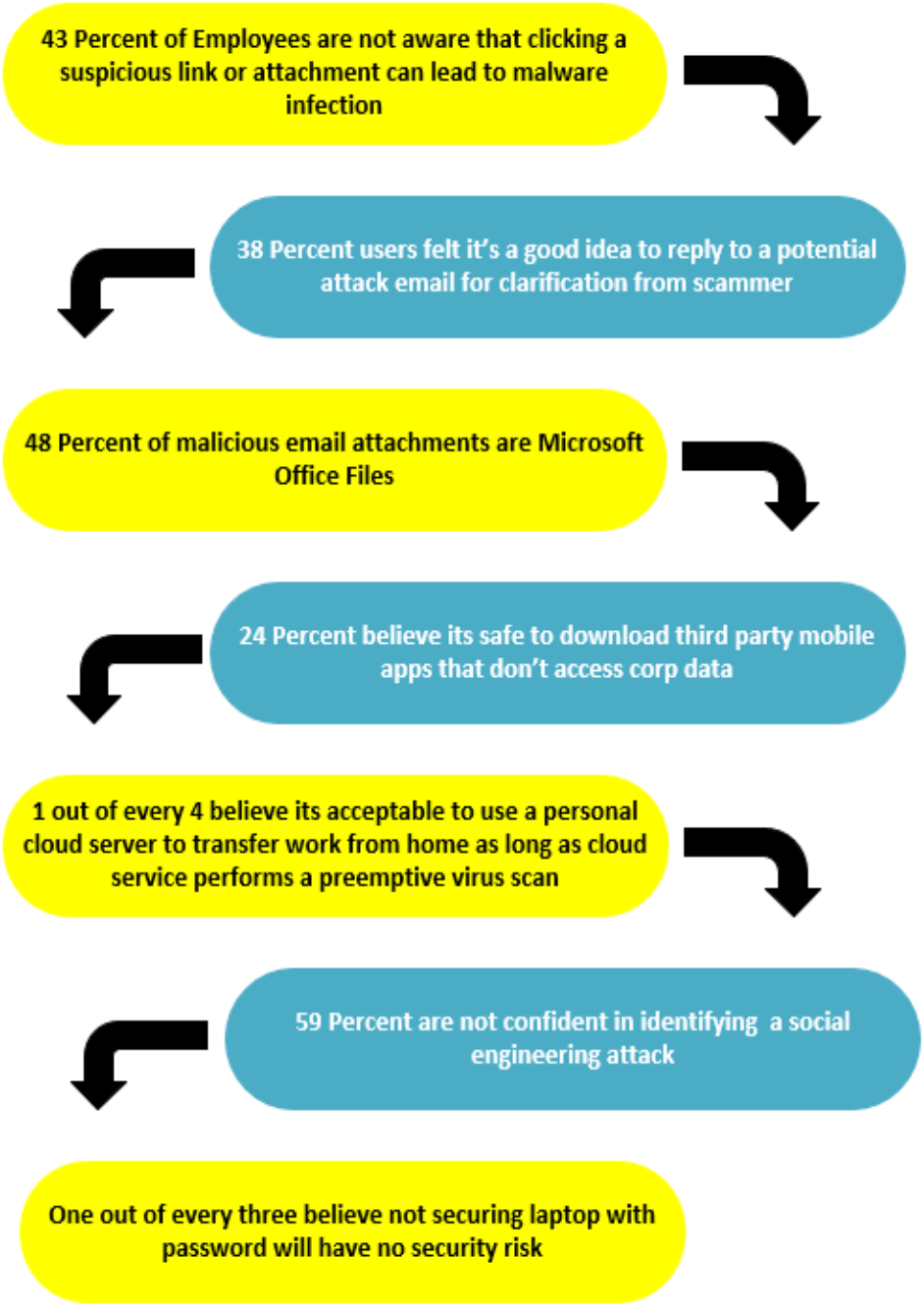


Fig 2: Cybersecurity's User Attitude Problem

Digital illiteracy makes computer users to develop an attitude of disregarding the use of digital tools that protect them from cybercrimes. Studies posits that digital illiterate computer users develop the defiance attitude towards cybersecurity due to lack of recognizing cyber threats like risks of clicking on unknown emails and suspicious links, lack of using firewall and antivirus software, phishing, and man-in-the-middle attacks. Phishing attacks trends from last 5 years stresses the urgent necessity to change computer users' attitude towards practices of secure information sharing, adherence to security best practices, and prevention of cyberattacks to ensure they are not vulnerable to cybercriminals.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

Users' attitude can be changed through engaging in cybersecurity workshops and online security training programs to enable them recognize cyberattacks and prevent falling victim of cybercriminals. Internet users to always develop an attitude of reading the terms and conditions of use of every application prior to installing it and always updating their computers with current security updates as soon as they are available.

## VI. METHODOLOGY

This quantitative study investigates the role of individuals' attitudes within the financial sector in determining their ability to identify phishing attempts [12]. Utilizing a 5-point Likert scale (ranging from strongly disagree=1 to strongly agree=5), the survey aims to gauge participants' attitudes toward phishing through 10 questions related to their behavior and perceptions. The survey questions focus on various aspects, including the perceived safety of clicking on links or opening email attachments, awareness of phishing risks, and preventive measures [13].


Fig 3: Research Methodology (Survey Based Research)

**Survey Questions:**

1. It's always safe to click on links in emails from people.
2. Nothing bad can happen if I click on a link in an email from an unknown sender.
3. It's risky to open an email attachment from an unknown sender.
4. It can be risky to download files on my work computer.
5. There is a high probability of receiving a malicious e-mail attachment.
6. The chances of receiving a malicious e-mail attachment are high.
7. Checking email link authenticity will help prevent phishing attacks.
8. Before opening an email attachment, I first check if the filename makes sense.
9. There is a good possibility that I will receive a malicious email in a phishing attack.
10. The best way for me to avoid email phishing attacks is to verify the authenticity of email links.

Participants responded to each question on a scale of 1 to 5, reflecting their level of agreement or disagreement. Higher scores indicate a more positive attitude toward security practices. The data collected from participants' responses will be analyzed to understand trends and patterns in attitudes towards phishing. The "Results" section will provide a detailed examination of the data, shedding light on the prevailing sentiments and potential areas of improvement in individuals' awareness and behavior regarding email security. The goal is to offer insights that can contribute to enhancing cybersecurity practices within the financial sector.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

## VII. RESULTS

This section summarizes the study's findings and analyses the collected data. The dataset comprises responses to a series of statements or questions, with participants indicating their level of agreement or disagreement. The responses fall into five categories: "Strongly Agree," "Somewhat Agree," "Neither Agree nor Disagree," "Somewhat Disagree," and "Strongly Disagree."

**Breaking down the frequency of each response:**

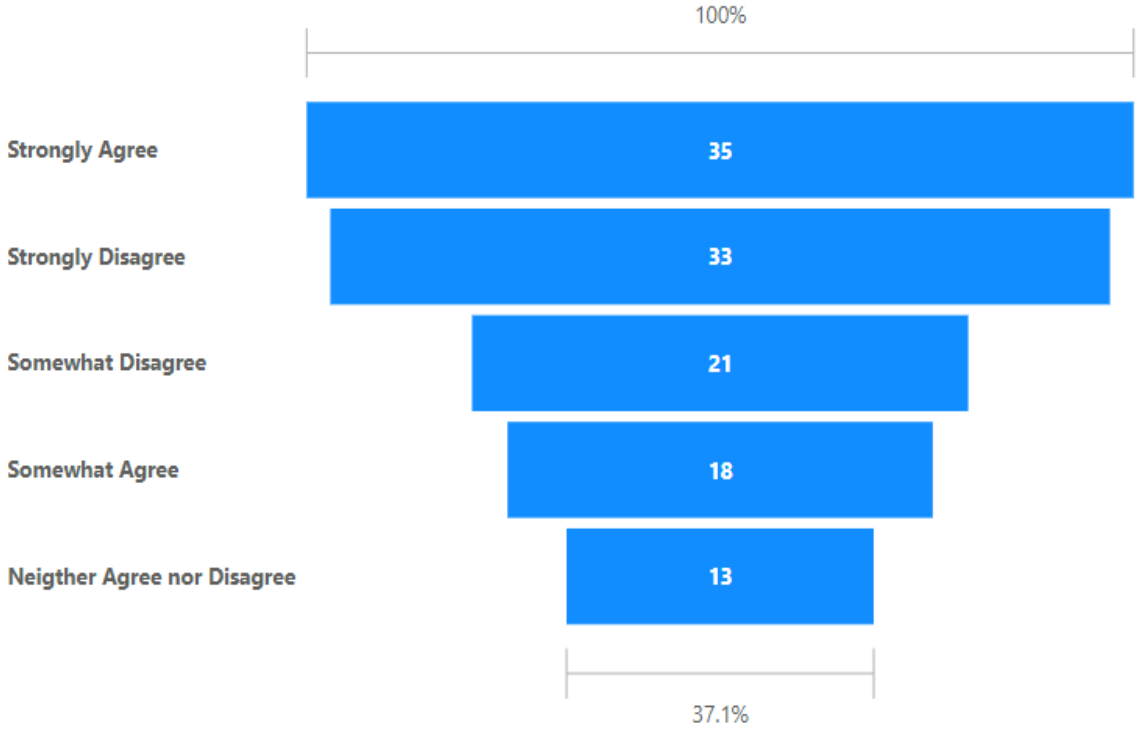


Fig 4: Category Based Responses

**Analyzing the overall sentiment based on the aggregated responses:**

Agree (combining Strongly Agree and Somewhat Agree): 53 (35 + 18)
Neutral (Neither Agree nor Disagree): 13
Disagree (combining Somewhat Disagree and Strongly Disagree): 54 (21 + 33)
In summary, the data suggests that a majority of participants either disagree or somewhat disagree with the statements, with a slight inclination towards disagreement. The neutral responses fall in the middle, and the agreement responses are comparatively less prevalent. The detailed interpretation of the data has been discussed below.

**Many People Disagree:**
More people said they either somewhat disagree or strongly disagree (54 out of 100).
This suggests that a lot of participants don't really agree with whatever was asked in the survey.

**Some are Unsure:**
A significant number (13 out of 100) didn't strongly agree or disagree; they were in the middle.
This might mean some participants weren't sure or didn't strongly feel one way or the other.

**Not a Strong Agreement:**
While some people agreed (53 out of 100), it's not as strong as the disagreement.
It seems like there's a mix of opinions, and agreement isn't the most common response.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

**We Need More Details:**
To understand better, we'd need to know the exact questions asked in the survey.
Knowing what people disagreed or agreed on could give more insight.

**Look at Different Groups:**
It might be interesting to see if different groups of people (based on age, gender, etc.) had different opinions. This could help us understand if certain factors influence how people feel.

**Think about Taking Action:**
Depending on the context, if a lot of people disagree, it might be worth looking into why and considering changes. In simple terms, it looks like people have different opinions, with more leaning towards disagreement. Understanding the specific questions and looking at different groups can help make sense of these responses. The clear disagreement responses clearly stated that individuals lack of security awareness towards phishing.

## VIII. DISCUSSION

Internet users with positive attitude towards cybersecurity are extremely likely to spot and evade phishing attempts as likened to those having less proactive attitude [14]. This is because they understand online risks and cyber threats such as phishing attacks and takes proactive defense measures of protecting their sensitive information and systems through use of security tools like web browser extensions that assist in identification and blocking of phishing attempts, anti-phishing software, updated software, spam filters, and enable as well as use two factor authentication to add a security layer to their online accounts, thus thwarting phishing attempts. Equally, internet users with dismissive attitude are more vulnerable targets of phishers because their dismissive attitude makes them develop a tendency of downplaying or ignoring possible security risks and taking the needed security precautions seriously and are overconfident of their immune to cyber risks [15]. Moreover, Internet users with proactive security attitude are very cautious and vigilant on recognizing and responding to phishing attempts and attacks. Proactive internet users are familiar with phishing methods and can recognize suspicious websites, messages, links, misspellings, sender addresses, and emails more effectively. Their proactive attitude makes them effective in taking direct actions to not only reporting, but also mitigating any phishing attempts [16]. With the results, the observed clear disagreement responses signal a potential lack of security awareness towards phishing within the surveyed population. This highlights the critical importance of targeted interventions, considering specific areas of disagreement, and tailoring educational efforts to address these gaps. Additionally, examining demographic influences can inform a more nuanced approach to enhance security practices [17]. In conclusion, the study calls for a comprehensive understanding of participant attitudes, emphasizing the need for further investigation into specific survey questions. The findings prompt a proactive approach to address security awareness challenges and encourage tailored interventions to foster a more informed and resilient community in the face of phishing threats.

## IX. CONCLUSION

In the end, the study tells us that many people don't agree on how to stay safe from online scams, especially phishing. This means lots of folks might not fully understand the risks. Some are not sure, making it clear that getting everyone on the same page about online security is tricky. To make things better, we need to look closely at the specific questions people disagreed on. This way, we can create ways to help them understand better. It's also important to think about how different groups of people might see things differently. So, tailoring online safety lessons to fit different groups is a good idea. The study suggests we should do something now to improve online safety awareness, especially about phishing. This could include special lessons, workshops, or training that speaks directly to what people are unsure about. It's all about making sure everyone has the right information and feels confident about staying safe online. In short, the study shows that online safety is still a bit confusing for many. To fix this, we should understand where people disagree, create specific ways to help them, and consider what different groups might need. Taking action now can make online safety clearer for everyone.

## ACKNOWLEDGEMENTS

We researchers would like to thank Phishing Box’s president for providing tools to conduct extensive research related to phishing emails. We want to express our sincere appreciation University of the Cumberlands, Colorado Technical University and Harrisburg 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 International Advanced Research Journal in Science, Engineering and Technology for allowing us to publish the paper.

 

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

## REFERENCES

[1]. D. J. Borkovich and R. J. Skovira, "CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO'S WORSE, EMPLOYEES OR HACKERS?," Issues in Information Systems, 20(3), p. 88, 2019.
[2]. J. L. Kröger, M. Miceli and F. Müller, "How data can be used against people: A classification of personal data misuses," SSRN 3887097, 2021.
[3]. B. Dupont, "The cyber-resilience of financial institutions: significance and applicability.," Journal of cybersecurity, 5(1), p. tyz013, 2019.
[4]. V. Karagiannopoulos, A. Kirby, S. O. M. Ms and L. Sugiura, "Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study.," Computer Law & Security Review, 43, p. 105615, 2021.
[5]. J. Wu and J. Wu, "Security risks from vulnerabilities and backdoors.," Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security, pp. 3-38, 2020.
[6]. S. L. Horgan, "Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder," 2019.
[7]. F. A. Ngufor, "Understanding the Perspectives of Information Security Managers on Insider Threat: A Phenomenology Investigation," Doctoral dissertation, 2020.
[8]. C. Lewin, D. Niederhauser, Q. Johnson, T. Saito, A. Sakamoto and R. Sherman, "Safe and responsible internet use in a connected world: Promoting cyber-wellness," Canadian Journal of Learning and Technology, 47(4), p. n4, 2021.
[9]. W. Steingartner, D. Galinec and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model.," Symmetry, 13(4), p. 597, 2021.
[10]. Z. Alkhalil, C. Hewage, L. Nawaf and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, p. 563060, 2021.
[11]. L. Wessels, "How South African universities can contribute to preparing the future workforce for the fourth industrial revolution," Doctoral dissertation, 2020.
[12]. S. Y. A. R. U. L. N. A. Z. I. A. H. Anawar, D. L. Kunasegaran, M. Z. Mas'ud and N. A. Zakaria, "Analysis of phishing susceptibility in a workplace: a big-five personality perspectives," J Eng Sci Technol, 14(5), pp. 2865-2882, 2019.
[13]. E. J. Williams and A. N. Joinson, "Developing a measure of information seeking about phishing," Journal of Cybersecurity, 6(1), p. tyaa001, 2020.
[14]. M. Martens, R. De Wolf and L. De Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general.," Computers in Human Behavior, 92, pp. 139-150, 2019.
[15]. R. Zhu, A. Srivastava and J. Sutanto, "Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective.," Information Technology & People, 33(6), pp. 1601-1626, 2020.
[16]. H. Shahbaznezhad, F. Kolini and M. Rashidirad, "Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?.," Journal of Computer Information Systems, 61(6), pp. 539-550, 2021.
[17]. Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier and F. Schaub, "Examining the adoption and abandonment of security, privacy, and identity theft protection practices," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-15, 2020.

## 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.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91224

**Dinesh Kalla** works at Microsoft as a Big Data and Azure Cloud Escalation Engineer and has eight 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 Big Data Analytics, Data Science, Machine Learning, Artificial Intelligence, IoT, and Cybersecurity. He published several papers on Big data, Artificial Intelligence, and cybersecurity threats in International Journals and conferences. He completed his Master of Science at the University of New Haven and is pursuing a professional doctorate in Computer Science with an emphasis on Big Data Analytics from Colorado Technical University.

**Fnu Samaah** currently working in U.S. bank as a Java Full Stack Developer and Team Lead. Samaah has six years of industry experience as a Java Full Stack Developer and Tech Lead. Her main areas of expertise and research interest are Python, Data Analysis, Machine Learning, Chatbots and Cybersecurity. She published several papers on Chatbots, Artificial Intelligence and cybersecurity awareness in International Journals. She completed her Master of Computer Science from Northeastern Illinois University and Master's in data science from Harrisburg University of Science and Technology.