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 & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13402

IMPLICATIONS OF PHISHING SCAM ACTIVITIES IN ADULTS BETWEEN AGE 50-80 IN THE UNITED STATES OF AMERICA

Tunbosun Oyewale Oladoyinbo

University of Maryland Global Campus, 3501 University Blvd E Adelphi, MD20783

Abstract: The use of the internet across different generations has been on the rise recently. By providing unmatched connectivity, convenience, and access to other sets of information, the internet has also had severe effects, and phishing is one of them. Recent studies have also shown that the attacks on the aging population have been rampant, and they are expected to increase as cyber criminals become more complicated and ruthless in the execution of their strategy. While phishing attacks agonist multiple factors have caused older people, this study focused on the relationship between age and susceptibility to pushing attacks. A sample size of 140 participants was asked the same question, and results were calculated from a scale of 0-10. The main findings of this analysis were that only 2.1% of the variation in susceptibility can be explained by the use of the variation in age; the correlation coefficient of 0.1448 indicates a low but positive relationship between age and susceptibility to phi. The p-value of 0.6871 is more than 0.05 level of significance, which means that age is not a significant predictor of susceptibility to phishing attacks.

I. INTRODUCTION

In the contemporary digital age, internet use and consumption have become a critical part of daily life. By offering unmatched connectivity, convenience, and access to different sets of information, the global space has had to bear the benefits and hazards of increased internet use in equal measure. However, technological advancements have also created room for the emergence of cybercrimes. According to [1], the global cybercrime rate has increased by more than 60% in the last five years, while in the U.S., the numbers went up by 22% in the colander year ending 2023 [2], among the most noticeable cyber threats in the U.S. The scams have evolved from simple attacks to sophisticated and complex attacks targeting individuals and organizations. Notably, [1] and [3] report that there has been a common trend among the attacks where they have been directed to a particular group, with the cyber community pointing out that older people are more prone to the attacks.

According to [3], phishing scams are social engineering attacks in which cybercriminals attempt to convince and trick individuals into divulging sensitive personal information to sources they think are representatives of other organizations to which they owe allegiance. Common information attackers seek includes login credentials, credit card numbers, social security numbers and other personal identifiers that could be used to tell who owns or uses a specific type of data or information.

The scams are usually executed through spoofed emails, fake websites, and, in some instances, fraudulent phone calls that have been modified to appear legitimate, while, in the real sense, they are not [4]. The impacts of the phishing attacks differ from one attack to the other depending on their magnitude and the nature of the information that has been compromised. Severe levels may lead to financial losses, and indecent exposure may cause psychological and emotional disturbances to the targeted individuals. When conducted among the aged, the effects of phishing attacks are more psychological than financial [5]. The emotional toll of the aged feeling that they have fallen into the tricks of the scammers leads to unprecedented levels of embarrassment and anxiety. In other cases, the lasso led to the loss of trust in technology and other institutions that are responsible for protecting their data.

Understanding the population dynamics of the U.S. is critical in understanding and establishing solutions to the problem. According to the U.S. Census Bureau, the country's population aged between 65 years is expected to double the current one of about 52 million in 2018 to 94 million in 2060. A systematic review by [6] shows that the aged are convenient to cyber criminals because they are usually treated as having the slightest knowledge of using technologies.

Addressing the issues of phishing scams targeting the older generation is a rather broad field of specialization, and it requires experts to focus on specific areas that they can study in detail and provide solutions that are not only detailed but also evidence-based. The effect of such studies is to ensure that comprehensive and detailed information is provided to adults so they can understand the best methods to prevent further attacks.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13402

In addition, this study seeks to establish a balanced review of the governmental and non-governmental measures that can be undertaken to ensure a safe working environment for older people. Therefore, this study carries a high responsibility to guard the digital space for the aged. Through linear aggression on collected data, the study seeks to establish whether there is a correlation between age and susceptibility to phishing attacks in the U.S. Responses from the participants were measured using a Linkert scale of 0-10.

II. LITERATURE REVIEW

To understand the topic in-depth, the literature review examined the vulnerability factors and risk awareness, implications, reliant legal and regulatory framework, preventive measures, and educational initiatives.

2.1 VULNERABILITY FACTORS

2.1.1 Technological Literacy and Familiarity

[4] and [7] note that technological literacy and familiarity play a significant role in an individual's exposure to phishing attacks. According to [8], technologically literate individuals are more likely to recognize suspicious emails or websites that may be phishing attempts. Such persons can identify red flags such as spelling errors, unfamiliar sender addresses, and requests for personal information and mitigate them immediately. In addition, literacy and familiarity levels affect how individuals familiar with common phishing tactics are less likely to fall victim to these attacks. For example, [7] points out that the level of literacy and familiarity is equal to the level of understanding of the importance of never sharing sensitive information online. In addition, the level of technological literacy on the up-to-date security software and practices in place determines how an individual can risk their level of attack on a system. With a growing consensus that the level of these attacks will not go down, the higher the level of technological literacy and familiarity directly impacts how professionals and users will understand phishing attacks.

2.1.2 Cognitive Changes Among the Aged

As individuals age, they will likely experience cognitive changes that can make them more vulnerable to scams. [9] and [10] note that one of the ways in which this susceptibility to phishing scams increases is through declines in memory and attention. There is consistent evidence among psychologists to argue that older adults may have difficulty recalling essential details or focusing on complex information, making it easier for scammers to deceive them. Some of the concepts with low rotation rates are passwords and other personal identification information, which system attackers can easily manipulate three to give out information. Age also affects changes in decision-making abilities, which can also lead to increased susceptibility to scams among older people. Collectively, the literature by [7], [9] and [10] shows that as individuals age, they may become less able to evaluate risks effectively, leading them to make poor choices when faced with fraudulent schemes.

Furthermore, declines in cognitive flexibility and problem-solving skills can make it harder for older adults to recognize and avoid scams [11]. Given that contemporary hackers are highly malicious and manipulative, they have mastered the best procedural methods they can use to manipulate users; older people with cognitive challenges can easily be manipulated to give out their data, which is, in return, used to agonist them. More importantly, changes in social cognition can also contribute to increased vulnerability among the aged. Older adults may struggle with interpreting social cues and detecting deception, making them more likely to fall victim to manipulative tactics used by scammers. However, other researchers argue that what causes exposure to phishing scams is more than the mere loss of memory by aging. [12] argued that the concept of age and technological literacy is luckily disappearing in the contemporary global community, which questions the studies by [7], [9] and [10].

2.2 IMPACTS OF PHISHING

ATTACKS AMONG THE ELDERLY

2.2.1 Financial Impact

As noted by [1], over 80% of phishing attacks have significant financial impacts on older individuals who may not be as aware of the dangers of online scams. In this sense, the term “financial impact” means not only the actual loss of money but also information that can lead to the loss of finances. [8] notes that the loss of personal and sensitive information, such as bank account details and social security numbers, exposes older people to severe and continuous loss of finances,

DOI: 10.17148/IJARCCE.2024.13402

for example, by compromising the pension details of an individual, which means that the hacker can continuously access information on how they are paid and scam them. In addition, the information can be used by cybercriminals to steal money from their accounts and, in the worst case, commit identity theft, leading to financial losses that can be devastating for older individuals on fixed incomes. In addition, phishing attacks can also result in the aged falling victim to fraudulent schemes and scams, where they are tricked into sending money and making purchases under pretenses [1]. The long-term impact of such activities is the depletion of savings and retirement funds, leaving them financially vulnerable and at risk of financial ruin.

2.2.2 Trust in Online Platforms

The ageing population has high trust levels in online platforms due to their convenience and availability. As noted by [1] [3] [4] and [14], when individuals fall victim to phishing scams, they risk financial loss and compromise their data and privacy, which is a direct breach of a duty of trust that the user has bestowed on the target organization. This breach of trust can have far-reaching consequences, as users may become hesitant to engage with online platforms for fear of being targeted by scammers. Further, [9] notes that the loss of trust depends on the nature of the attack and the type of information lost. The prevalence of phishing scams can tarnish the reputation of legitimate businesses and websites, which makes it difficult for consumers to differentiate between trustworthy and malicious sources. The problem becomes more pounced among the aged, who may feel that they are being targeted due to their inability to comprehend complicated technology platforms. Therefore, the erosion of trust in online platforms due to phishing scams highlights the importance of vigilance and cybersecurity measures in today's digital age.

2.2.3 Emotional Impact

Phishing has a profound emotional impact on older individuals, who [15] note they might be affected on a larger scale than young internet users. In explaining the direct and significant effects of the attacks on older people, experts have used the theory that as people age, they develop a psychological defence which makes them hypersensitive to any new threat. The emotional toll of falling victim to a phishing scam can be devastating for older people who feel embarrassed by being tricked by scammers, leading to guilt and self-blame [16]. In addition, the loss of personal information and financial assets causes immense stress and worry for older adults with structured incomes. Notably, different studies in the field have had consistent results that show that emotional, financial, and lack of trust in the source of information are intertwined effects that should be studied concurrently.

2.3 Control Measures

2.3.1 Industry Control

The nature of controlling cybercrime is that its success is highly dependent on the ability of its different market players to come together and forge standard solutions. Some of the common measures that online platforms can take include establishing a role framework, which requires companies to undertake deliberate measures to control the loss of data in their specific areas of specialization. [17] points out that financial institutions are critical in preventing phishing scams by educating their elderly customers about the warning signs of fraudulent emails and websites. With such reports, banks can provide clear and concise information on identifying and reporting suspicious activity, creating a more cyber security-conscious ageing population. In addition, technology companies can develop more robust security measures to detect and prevent phishing attempts targeting older people. [18] points out that standard measures include implementing multi-factor authentication systems, encryption protocols, and advanced spam filters to safeguard sensitive information. Government agencies should collaborate with industry stakeholders to establish regulatory frameworks that hold perpetrators of phishing scams accountable for their actions. The enforcement of strict penalties for those who engage in fraudulent activities targeting older people helps authorities deter cybercriminals from exploiting vulnerable individuals.

2.3.2 Legislative and Regulatory Framework

Interestingly, despite being a global leader in many issues, the U.S. lacks a single and comprehensive law specifically targeting phishing attacks. However, the law enforcement agencies in the country rely on a complex web of regulations across various agencies aimed at curbing these deceptive practices. Each law has specific objectives, duties and responsibilities for different organizations that are in love with the control of cybercrimes. The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing) focuses on commercial email. It requires and calls upon businesses to ensure transparent processes of identifying the email's receiver and sender. The law also prohibits the sending or circulation of deceptive subject lines and misleading headers that can be used to mislead readers. While [19] acknowledges that the CAN-SPAM Act may not directly target phishing scams, it helps establish standards for what constitutes legitimate commercial emails.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13402

In addition, the Federal Trade Commission Act (FTC Act) gives the Federal Trade Commission (FTC) the power to prevent unfair and deceptive practices in commerce, including phasing attacks. The FTC has the FTC Act extensively to target phishing attempts and, in proven cases, issuing cease-and-desist orders and pursuing legal action against companies found to be engaging in deceptive practices [20]. Equally, the Gramm-Leach-Bliley Act (GALBA) has been used to protect the privacy of financial information by requiring financial institutions like banks to implement robust security measures to protect customer data. The measures that the institutions should take include the ability to detect and prevent phishing attacks that target financial information [21]. The Electronic Funds Transfer Act (EFTA) protects consumers who use electronic money transfer systems like debit cards and ATMs by offering them a recourse for bank clients who lose money due to unauthorized transfers. More importantly, the Children's Online Privacy Protection Act (COPA) has been used to protect the data and interests of children on Internet platforms [22]. As a result, websites directed towards children have stricter data collection and use regulations. The Cybersecurity Act of 2015 is among the comprehensive tools for compelling cybercrime in the U.S., and it establishes a framework for improving cybersecurity across the federal government. While not directly targeting phishing, it emphasizes information sharing and collaboration between government agencies to address cyber threats, including phishing campaigns.

2.4 Challenges in Mitigating Phishing Attacks on the Elderly

According to [17] and [18], the gap in digital literacy has become increasingly apparent with young generations being well-versed in navigating the complexities of the online world, the aged often find themselves struggling to keep up with the ever-evolving technology. More profoundly, the differences are evident in cyber security, where the aged may not understand the technical terms that signal a phishing attempt. Lack of awareness of terms such as spoofed email addresses, misspelled URLs, and generic greetings puts them at a higher risk of falling victim to online scams and fraud. As a result, older people must receive proper education and training on navigating the digital landscape safely. By increasing their digital literacy skills, older people can protect themselves from potential threats and make informed decisions when using technology [19].

With the ever-changing nature of cyber threats, keeping up with the complex security measures required to protect personal information and sensitive data can be overwhelming. The problem is more pounced among the elders who may not be familiar with these advanced security protocols; the constant need to stay on top of these measures can lead to what is known as "security fatigue," which is a phenomenon which occurs when individuals become tired and overwhelmed by the multitude of security requirements and end up overlooking crucial steps or relying on weaker safeguards.

Cybercriminals have also mastered the art of urgency, instilling fear among older people. [23] notes that they instill a sense of urgency or fear in their victims through deceptive emails. These emails often contain alarming messages such as imminent account suspension, urgent tax demands, and unclaimed lottery winnings, which prompt older people to act quickly without proper scrutiny. The fear and limited timeframes created by phishing attacks can lead seniors to make hasty decisions that compromise their personal information and financial security. The pressure to respond immediately can cloud judgment and prevent individuals from questioning the email's legitimacy.

2.5 Research Question

Does age affect the susceptibility to phishing scams in U.S. citizens aged 50- 10 years?
Is linear aggression an effective way of measuring the relationship between age and susceptibility to phishing scams?

III. METHODOLOGY

In addressing the research question, I created an online survey where participants were identified randomly. The 140 participants were to answer ten different questions. Purposeful sampling was used to determine the participant’s ad from a sample population of 180 14 participants were identified. Participants; answers were rated on a scale of 0-10.

IV. RESULTS

Data was analyzed through Linear Regression. The results are demonstrated in Figures 1 and 2 below. The main findings of this analysis were that only 2.1% of the variation in susceptibility can be explained by the use of the variation in age; the correlation coefficient of 0.1448 indicates a low but positive relationship between age and susceptibility to phi. The p-value of 0.6871 is more than 0.05 level of significance, which means that age is not a significant predictor of susceptibility to phishing attacks.

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 & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13402

Figure 1

Scatter plot of age and susceptibility to phishing

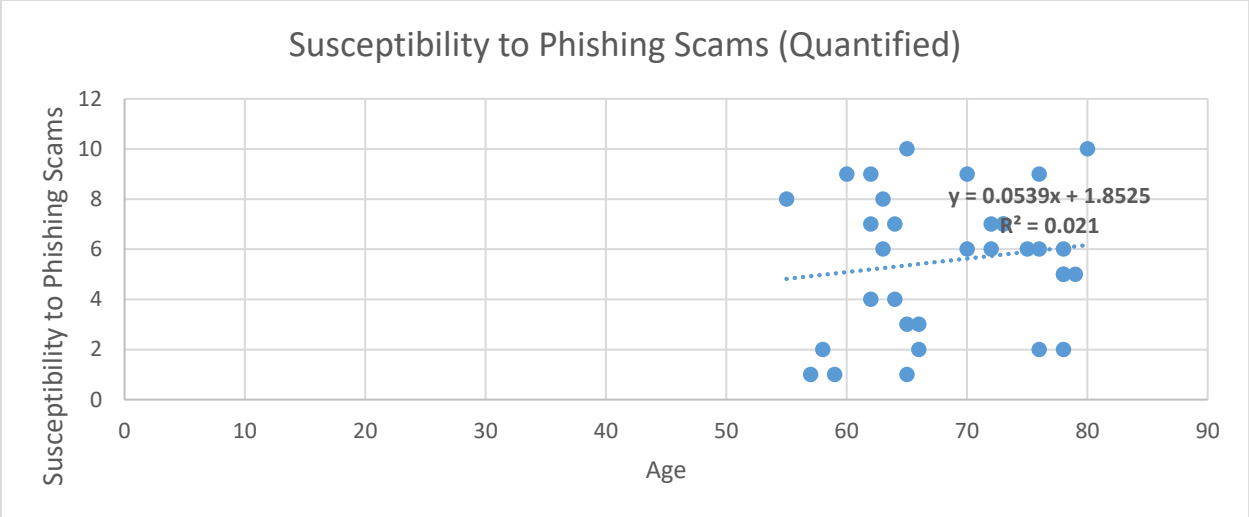

Figure 2

Regression analysis

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.144882015
R Square	0.020990798
Adjusted R Square	-0.010590144
Standard Error	2.765561417
Observations	33

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	5.083589658	5.083589658	0.664666625	0.421137111
Residual	31	237.0982285	7.648329952		
Total	32	242.1818182			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*pper 95.0%*
Intercept	1.85245788	4.555289463	0.406660849	0.687051145	-7.438116233	11.14303199	-7.438116233	11.14303
Age	0.053924288	0.066142785	0.815270891	0.421137111	-0.080974813	0.188823388	-0.080974813	0.188823

V. DISCUSSION AND CONCLUSION

Several reasons contribute to these results. According to this study, while older people are often targeted for phishing attacks due to a perceived lack of digital literacy, age alone is not the sole factor in determining susceptibility. These findings are consistent with other studies in the field. Notably, phishing tactics evolve to exploit vulnerabilities across demographics, and other factors can influence how susceptible someone is to being phished. [8] points out that there is a growing segment of the elderly population that is comfortable with technology, and they can computably use online banking and social media and shop online, making them potential targets for phishing attacks that target these activities. Therefore, in such instances, the attacks are not just limited to the age factor but also the lifestyle. In the literature review, it was also evident that cognitive decline associated with aging can indeed make seniors more susceptible. However, [17] points out that mental decline can affect people of all ages due to various medical conditions.

DOI: 10.17148/IJARCCE.2024.13402

From a broader perspective, some researchers have argued that phishing scams can exploit universal human emotions like fear, urgency, and greed beyond the lament of fear. Contemporary cyber experts also pointed to the potential use of social engineering tactics that play on trust and authority figures. Impersonating institutions like credit card companies, social security offices, and phishers can manipulate people across generations into revealing personal information without necessarily being controlled by age. Other factors that can lead to these results include digital habits, financial knowledge, and cybersecurity awareness. Regardless of age, people who spend a lot of time online are more likely to encounter phishing attempts, for they frequently click on links in emails or engage with social media posts without proper scrutiny. In addition, people who are trusting have a higher urgency response and may be more susceptible to falling for phishing tactics that exploit these traits [1] [7]. Regardless of an individual's age, their limited understanding of financial products and services can make someone more vulnerable to phishing scams that pose as legitimate financial institutions or investment opportunities.

COMPETING INTERESTS

I did not have any conflicting interest in the study.

REFERENCES

[1]. Alghamdi, M.I., 2020. A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. *International Journal of Engineering Research and Technology*, *9*, pp.731-5. 10.17577/IJERTV9IS060565

[2]. Hendrey Simon. 2024, March 7. FBI: Cybercrime cost Americans over $12.5B in 2023. SC Media. https://www.scmagazine.com/news/fbi-cybercrime-cost-americans-over-12-5b-in-2023

[3]. Singh, M.M., Frank, R. and Zainon, W.M.N.W., 2021. Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), pp.1658-1668. https://beei.org/index.php/EEI/article/view/3028

[4]. Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, p.563060. https://doi.org/10.3389/fcomp.2021.563060

[5]. DeLiema, M., Burnes, D. and Langton, L., 2021. The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, *5*(4), p.igab043. https://doi.org/10.1093/geroni/igab043

[6]. Salloum, S., Gaber, T., Vadera, S. and Shaalan, K., 2022. A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, *10*, pp.65703-65727. https://doi.org/10.1109/ACCESS.2022.3183083

[7]. Tornblad, M.K., Jones, K.S., Namin, A.S. and Choi, J., 2021, September. Characteristics that predict phishing susceptibility: a review. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 65, No. 1, pp. 938-942). Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1071181321651330

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

[9]. Sarno, D.M., Lewis, J.E., Bohil, C.J. and Neider, M.B., 2020. Which phish is on the hook? Phishing vulnerability for older versus younger adults. *Human factors*, *62*(5), pp.704-717. https://doi.org/10.1177/0018720819855570

[10]. Pehlivanoglu, D., Shoenfelt, A., Hakim, Z.M., Heemskerk, A., Zhen, J., Mosqueda, M., Wilson, R., Huentelman, M., Grilli, M.D., Turner, G.R. and Spreng, R.N., 2023. Phishing vulnerability compounded by older age, APOE4 genotype, and lower cognition. https://doi.org/10.31219/osf.io/6f2y9

[11]. Safaei, B. and Head, M., 2024. Investigating Age-Related Factors in Phishing Susceptibility: A Focus on Decision-Making Processes in HCI Context. https://aisel.aisnet.org/sighci2023/5

[12]. Grilli, M.D., McVeigh, K.S., Hakim, Z.M., Wank, A., Getz, S.J., Levin, B., Ebner, N.C. and Wilson, R.C., 2020. Is this phishing? Older age is associated with greater difficulty discriminating between safe and fraudulent emails. *PsyArXiv*. *June*, *25*. https://web.archive.org/web/*/https://files.osf.io/v1/resources/upf6c/providers/osfstorage/*

[13]. Abroshan, H., Devos, J., Poels, G. and Laermans, E., 2021, June. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. In *Adjunct proceedings of the 29th ACM conference on user modeling, adaptation and personalization* (pp. 345-350). https://doi.org/10.1145/3450614.3464472

[14]. Cross, C. and Gillett, R., 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *27*(3), pp.871-884. https://doi.org/10.1108/JFC-02-2020-0026

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13402

[15]. Ebner, N.C., Ellis, D.M., Lin, T., Rocha, H.A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D.L., Turner, G.R., Spreng, R.N. and Oliveira, D.S., 2020. Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75*(3), pp.522-533. https://doi.org/10.1093/geronb/gby036

[16]. Ebner, N.C., Pehlivanoglu, D. and Shoenfelt, A., 2023. Financial Fraud and deception in aging. *Advances in geriatric medicine and research*, *5*(3). https://doi.org/10.20900%2Fagmr20230007

[17]. Sadiq, A., Anwar, M., Butt, R.A., Masud, F., Shahzad, M.K., Naseem, S. and Younas, M., 2021. A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human behavior and emerging technologies*, *3*(5), pp.854-864. https://doi.org/10.1002/hbe2.301

[18]. Lain, D., Kostiainen, K. and Čapkun, S., 2022, May. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 842-859). IEEE. https://ieeexplore.ieee.org/abstract/document/9833766

[19]. Smith, D., 2021. Robocalls Have Been Blocked, but Business Can-Spam Emails with Little Regulation. *Wash. UL Rev.*, *99*, p.1753. https://heinonline.org/HOL/LandingPage?handle=hein.journals/walq99&div=46&id=&page=

[20]. Gupta, N., 2023. Correcting Corrective Advertising: A Tool to Address Harm Caused by Dishonest Advertisers. *Geo. LJ Online*, *112*, p.55. https://heinonline.org/HOL/LandingPage?handle=hein.journals/gljon112&div=4&id=&page=

[21]. Chopra, R. and Levine, S.A., 2021. The case for resurrecting the FTC Act's Penalty Offense Authority. *U. Pa. L. Rev.*, *170*, p.71. https://heinonline.org/HOL/LandingPage?handle=hein.journals/pnlr170&div=5&id=&page=

[22]. Anderson, H., 2024. The Guardian of the Digital Era: Assessing the Impact and Challenges of the Children's Online Privacy Protection Act. *Law and Economy*, *3*(2), pp.6-10. https://heinonline.org/HOL/LandingPage?handle=hein.journals/gslr38&div=46&id=&page=

[23]. Alwanain, M.I., 2020. Phishing awareness and elderly users in social media. *Int J Comput Sci Netw Secur*, *20*(9), pp.114-119. 10.22937/IJCSNS.2020.20.09.14