Cybercrime and Age in the Post-Pandemic Era: What does the Adaptation of The Elderly Population to Phishing Attacks Tell Us About Cyber-Crime Prevention?

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Charlotte Miller

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

Introduction

What role does lingering effects of the pandemic play in the large drop in phishing reports among the elderly population in the post-COVID era?

As the digital world becomes more pervasive, complex, and evolved, it brings with it evolving dangers. One of these dangers is cybercrime. Cybercrime can impact the personal and financial health of its victims in addition to posing a security threat (Pehlivanoglu, 2024). While cybercrime can come in many forms, the most common form is phishing, a scam in which malicious actors craft fraudulent messages designed to illicit sensitive information or money. Hundreds of thousands of Americans each year fall prey to phishing scams. Often, its victims pay a heavy price (Internet Crime Complaint Center [IC3], 2024b).

To understand how to best prevent phishing, there is a natural resource: the past. After the pandemic, phishing reports for the elderly dropped severely, in stark contrast to the overall trend for cybercrime and diverging from the small decline in phishing reports exhibited by the general public (Internet Crime Complaint Center [IC3], 2024b). The pandemic radically impacted the life of the average American, especially with regards to technology. The increased necessity of adoption and integration of technology into daily life had an altering effect on the relationship between the elderly and technology. However, the continuous impact of the COVID-19 pandemic on the relationship between the elderly and phishing is yet unexplored.

Understanding how the phishing problem for the elderly has improved to such a large degree could provide insight into how one's relationship with technology as well as sociocultural factors impact one's vulnerability to cybercrime. This insight could be key to better preventing phishing attacks among all population groups and could lead to the creation of more effective

methods of preventing other forms of cybercrime. This paper will conduct research on the effect of a changing relationship of the elderly population with phishing in the aftermath of the pandemic.

Background

The elderly have long been stereotyped as the most vulnerable population to cyber-crime; in some ways, this stereotype has held true: Victims above the age of 60 typically constitute around 28% of all loss reported due to cybercrime in the U.S., the largest of any age group (Internet Crime Complaint Center [IC3], 2024b). However, there is a notable anomaly: Phishing reports among the elderly (60+) now represent less than 1% of total phishing reports, down from nearly 5% in the pre-pandemic era (IC3, 2024b). Phishing is the largest form of cybercrime and is defined as the practice of sending deceptive messages, frequently emails, with the appearance of legitimacy in the hopes of gaining access to private information (such as credentials) or money. Since the COVID-19 pandemic, phishing reports have dropped significantly among the elderly after reaching a peak in 2021, halving even pre-pandemic levels (IC3, 2020b). While phishing reports have also dropped among the rest of the population since 2021, they remain elevated from pre-pandemic levels (IC3, 2020a). However, total cybercrime continues to rise among both the general and elderly population. Thus, the post-pandemic reduction in phishing reports for the elderly runs contrary to the trend of the general population as well as the overall cybercrime trends for the same age group.

The elderly population has historically been technology averse, using less technology and to a lesser degree than younger demographics (Sixsmith et al. 2022). This gap of technology

usage has two opposing effects on cybercrime outcomes: On one hand, the lack of "technological literacy" and familiarity in operating technology has been postulated as an exacerbating factor for cybercrime among the elderly (Gavett et al. 2017). On the other hand, lessened usage of technology also decreases the vector of attack for cybercriminals and limits exposure to cybercrime attacks. The elderly began using technology at a much higher rate during the pandemic as a result of quarantine, following the trends of the general population. This had the side effect of increased exposure to phishing attempts. A study of older adults found that elevated technology usage during the pandemic also increased comfort with operating technology among the elderly (Sixsmith et al. 2022).

Phishing in the U.S. can be seen as a sociotechnical system containing the Internet, the general population of the U.S. vulnerable to phishing (with the elderly acting as a subset), phishing technologies, and hackers (as well as other parties such as the government, anti-phishing software and companies providing services such as email). Each of these actors have an interconnected nature and experience the effects of mutual shaping: change in one actor will create a rebounding effect in the network. The primary focus of this paper is the relationship between the elderly and phishing technologies, which is deeply intertwined with the aforementioned actors. This relationship will be examined through the context of a disruptive force on the network: The COVID-19 pandemic. The pandemic and the quarantine measures enacted during the pandemic acted as a catalyst for change, producing immediate changes to the operation of the system as well as lasting effects to the sociotechnical system that this paper will explore in depth and seek to understand.

Literature Review

While limited research has been conducted on the changes produced by the COVID-19 pandemic when it comes to phishing and the elderly, there is notable, if inconclusive, research on the role of age in susceptibility to phishing. Some research does concur with the stereotype of older adults being more susceptible to phishing: A recent study from 2024 focused on the effects of age and mental conditions related to age such as diminished cognition or Alzheimer's on determining whether or not an email was phishing found that increased age was a predicter for decreased ability to distinguish between safe and unsafe emails during lab-based testing (Pehlivanoglu, 2024). However, the majority of evidence in the current body of research indicates that while there are significant differences in how younger and older adults interact with phishing, age comes with both strengths and weaknesses.

In a study from 2017, researchers found evidence of the approach contained within a phishing attack creating an age divide in susceptibility to spear phishing, a form of phishing crafted especially to target the recipient. Over the course of a 21-day experiment where participants were tested with a series of legitimate and illegitimate emails in their daily lives, younger adults were more susceptible to emails that adopted the principle of scarcity (limited-time offers) and emails from a position of authority. Older adults were significantly more likely to click on links in emails purporting to be from people they liked or shared similarities with. Older adults were also more likely to click on links in attacks centered around “reciprocation” or repayment of a positive gesture (Oliveira, D., et. al. 2017). Another study found that having knowledge of phishing or prior education on phishing had differing impacts on younger and older age groups. While browsing the web in lab-based testing, older adults were the most likely to be suspicious of phishing attempts if they had prior knowledge or experience with phishing. However, the older adults without that knowledge background on phishing were the least likely

to notice a phishing attempt (Gavett et al. 2017). In a different study, familiarity with a computer had a negative impact on recognizing a phishing attack (Parti, 2023). The suggested benefit of increased familiarity in navigating a computer can potentially be counteracted by a resulting increase of more "casual" technological behavior leading to participation in unsafe technological behavior. Simply increasing technological familiarity is not guaranteed to result in better phishing outcomes.

Overall, the sudden drop in phishing complaints in the U.S. is not well explained by the current research on the impact of age solely on identifying phishing scams and is better explored in conjunction to other factors. In the aforementioned study by Parti, it was found that older adults were less likely to report or ask for help after falling victim to cybercrime (Parti, 2023). While this might appear to explain the relatively lower number of phishing reports from older adults relative to younger adults in the U.S., it doesn't explain the much higher number of reports compared to younger adults in other forms of cybercrime nor the recent drop in phishing reports constrained to the elderly. This research seeks to expand the current research by understanding the sociotechnical factors that have impacted the elderly population when it comes to phishing in the post-pandemic era.

Methods

This paper will perform analysis on a variety of literary sources and data. Firstly, the most recent data on cyber-crime and phishing in the United States as collected by the IC3 will be used to better understand the changes in phishing reports based on demographics. To understand the divide between age groups and relation to phishing, relevant studies will be analyzed,

including experimental studies measuring accuracy of classifying messages as phishing as well as observational studies giving insight into the difference in technological behaviors. Additionally, studies on the impact of COVID-19 on phishing technology and technological behavior, especially for older adults, will be utilized. Studies were searched for across multiple platforms including general platforms such as Virgo and Sage as well as more specific databases such as Computer and Information Systems Abstracts using keywords such as “phishing” or “cybercrime”, “elderly” or “age”, and “technology” or “technology usage”. When searching for studies occurring during or after the pandemic, keywords such as “pandemic” or “COVID-19” or similar were used. Alternatively, searches were limited to just articles published within the desired time frame. Because of the very recent nature of much of the topic, arXiv was additionally used to search for studies occurring during or after the pandemic. Sources were primarily focused on American research and data but will include foreign papers when examining global commonalities, such as the global trends in phishing as a result of the pandemic.

Results

The Adaptation of the Elderly Population during the COVID-19 Pandemic

Based on the collected studies, there is a clear consensus in the academic community that the pandemic altered the technological behaviors of the elderly during quarantine in many places across the world, namely through the increased usage, especially for technological vectors of communication, which presents a danger for phishing. A survey by Sixsmith et al. conducted in 2019 and again in 2020 found that among Canadian adults, when asked specifically about how

COVID-19 had impacted their technology use for methods of communication, vastly more adults reported increases in technology than declines across every category questioned. Potential vectors for phishing were included, including social media, which 43.6% of older adults reported using more, texting, which 39.8% of adults reported using more, as well as phone calls. The usage of phone calls was questioned in three categories: smartphone calls (29.8%), home phone calls (26.6%) and cellphone calls (18.6%). In addition, 50% of older adults reported an increase in online social activities. Very few adults reported a decline in usage in any technological form of communication, with the highest percentage being 1.8% of older adults reporting a decline in home-phone calls, even as 26.6% of adults reported an increase. Significantly, the majority of older adults, more than two thirds, also reported that they planned to continue using these technologies after the end of the pandemic. The study concluded that older adults showed a greater willingness and ability to adapt to technology than previously stereotyped. However, when examining attitude towards technology, older adults were generally less optimistic about the ability of advancing technology to help in all tested areas of aging (e.g. staying independent, prolonging life, staying active), with only one exception: A higher percentage of older adults reported that advancing technology can help with reducing social isolation. Overall, the study found that older adults were increasingly likely to rely on digital technology for connection and communication compared to before the pandemic (Sixsmith et al. 2022).

A similar study targeted at adults aged 65 and older found concurring results (Haase et al. 2021). 56% of the respondents to a cross-sectional survey conducted in January 2021 reported that they changed how they used technology to communicate during the pandemic. In addition, more than half (55.9%) of respondents reported adopting new technology during the pandemic. A staggering 91% of the respondents reported that they continued using the technology that they

had adopted during the pandemic. Older adults were also asked to describe factors that had helped them or could help them navigate using technology for socialization: one of the common themes the study found was prior knowledge of technology as a facilitator for tech use (Haase et al. 2021). Another study focused on the impact of the pandemic on elderly adults analyzed online focus group discussion among recruited participants in Seattle (Chen et al. 2021). The study narrowed its focus to older adults that met one of the conditions for frailty or pre-frailty, a community made especially vulnerable by the pandemic. Based on the discussion generated, the study concluded that technology had a large role in day-to-day life during the pandemic for the participants. Online resources, including public media, were the most common vectors for obtaining information about the pandemic. Participants were reliant on the sources of online resources as an assurance of credibility, with publicly known resources and trusted figures being more credible. The study found that elderly people used social technologies more during the pandemic, with the goal of combating social isolation (Chen et al. 2021).

The Evolution of Phishing due to the COVID-19 Pandemic

The pandemic's influence in increasing technology usage was not limited to the elderly; fraudsters also focused their attention online, resulting in large increases of cybercrime and phishing attempts. APWG, a global group dedicated to coordinating the response to cybercrime, reported a massive increase in phishing attacks in the first three quarters of 2020, quadrupling pre-pandemic numbers (APWG, 2020a). Numbers continued to rise as the pandemic went on. In 2022, phishing numbers, which had held relatively steady in the quarters immediately before the pandemic, had steadily risen to eight times the pre-pandemic levels. It was not only the volume of phishing attacks that changed during the pandemic; the strategies used to attack victims in

phishing attacks also evolved. A study examining the trends and evolution in phishing attacks in the midst of the COVID-19 pandemic analyzed the phishing attacks on 100,000 Dutch businesses and found that many phishing attacks had adapted to exploit the pandemic, including phishing attacks that were crafted to target pandemic fears such as a large campaign that centered around face masks, domains relating to the pandemic such as 'covidvirus.guru,' and the timing of attacks to profit off of increased societal fears. In general, the study found that phishing attacks were quick to change strategy to profit off of societal changes and times of crisis, not restricted to COVID-19 related crises (Hoheisel et al. 2023). In addition, the average person might not be prepared to handle the rapidly adapting phishing attack. A study from 2022 looked at the ability of participants to identify phishing when attacks contained older characteristics compared to the more advanced "new gen" of phishing attacks and found that participants were much less likely to identify phishing with newer tactics (Carroll et al. 2022). Notably, the Caroll et al. study found that participants were too reliant on outdated methods of identification such as grammar and appearance, which are vastly improved in the modern phishing attack. The study identifies several properties of website phishing attempts that have become more difficult to use as red flags, including suspicious URLs, company logos, images, and whether the transfer protocol is secure (https as opposed to http) (Carroll et al. 2022). Evidence suggests that in the pandemic era, the phishing landscape became far more dangerous than ever.

Post-Pandemic Norms

The increased danger of phishing attacks during the pandemic has not returned to pre-pandemic normal. Rather, research suggests that the modern phishing landscape is far more dangerous than the pre-pandemic era in both quantity and quality of phishing attacks. APWG

recorded more phishing attacks in each quarter of 2024 than in the entirety of 2021. This number reflects both successful and unsuccessful attempts. Numbers stabilized below the pandemic peak in 2023, remaining stable in 2024; however, post-pandemic levels are still highly elevated (roughly seven times greater) compared to pre-pandemic levels. This post-pandemic norm does not exhibit the steady increase that pervaded the pandemic but also does not show signs of returning to pre-pandemic levels (APWG, 2025). In addition, some companies have identified AI as a potential weapon for phishers. Hoxhunt, CrowdStrike, NordPass and other cybersecurity industry competitors have singled out AI as a defining element of the modern phishing landscape. The advanced elements of the phishing attacks during the pandemic in the Carroll et al. study persist and are predicted to continue to evolve, potentially through the improvement of AI (Baker, 2024). Still, while phishing attacks have advanced due to AI, so have phishing prevention methods. AI models have revolutionized identifying phishing attempts by analyzing complex patterns such as overly urgent tones and attempts at mimicking a trustworthy source (Osamor et al. 2025).

A major change in post-pandemic phishing norms is the shift of the sectors through which phishing attacks are conducted. Comparatively, SAAS (software as a service) / webmail phishing attacks and financial phishing attacks constitute a smaller portion of the targeted phishing sectors post-pandemic compared to pre-pandemic according to APWG (APWG, 2020b, 2024). SAAS / webmail attacks dropped from 33.5% of the total attacks to 23.3% of the total from the first quarter of 2020 to the last quarter of 2024. Financial institution phishing, once the second most common sector for phishing, dropped from 19.4% to 11.9%. On the other hand, social media phishing attacks more than doubled in the same time period, jumping from 8.3% to 23.3%.

Attitude changes in the elderly towards technology post-pandemic are less thoroughly researched. A recent study found age-based differences in attitude towards technology remained but were not the most significant factor: an analysis of the demographic factors that influenced the results of a survey across a wide span of ages found that, while older adults were still generally less positive about technology than their younger peers, the age of the participant was less of a significant predictor than gender for general attitudes on technology (Grissani et al. 2025).

Analysis

The evidence collected suggests that some theories for the decline in reports of phishing victimization among American older adults are unlikely. Given the high volume of post-pandemic phishing attempts compared to pre-pandemic levels, even if phishing attempts have stabilized lower than pandemic highs, it suggests the sudden decline in reports of victimization is not due to fewer phishing attempts. In addition, while a decrease in technology use after the pandemic leading to lower exposure to risk could explain some of the difference between mid-pandemic and post-pandemic reports, given the boosted technology use seen during the pandemic and the expressed enthusiasm to continue usage among most of the elderly population, lower exposure to risk compared to pre-pandemic levels is less plausible.

More plausible is the theory that the changing of targeted sectors from phishing attackers could be playing a part in fewer reports among the elderly. Despite older adults using social media more during the pandemic, social media usage is still heavily skewed towards younger adults. The increase in social media phishing attacks constitutes a shift in focus towards younger

domains. However, this shift might not be a cause of the drop but could be a result of phishers receiving less payout from attacks on more elderly domains and shifting to more vulnerable crowds. This could also result from social media, independent of user, becoming a more viable form of attack than previously, for example as a result of not needing to navigate around spam filters. Uneven improvements in phishing prevention software across sectors such as advancements in spam filters could prompt an exodus of phishers from email phishing to a more vulnerable sector like social media. It should be noted that lessened phishing attempts in other sectors do not adequately explain the drop; while certain sectors decreased by a third or a bit more in share of phishing attempts, the magnitude of the increase of number of phishing attempts was far greater in the same time period, meaning number of phishing attempts in each sector increased even as total share of phishing attempts decreased. Still, this change of preferred sector might represent an overall shift of effort and energy. In addition, phishers focused on an environment with a higher volume of younger adults may rely on campaigns that are more successful among younger adults, the most available demographic.

Because the modern phishing environment has become more dangerous on almost every front, including volume and quality of attacks, the collected data strongly indicates improvement in phishing response for the elderly. Two potential explanations include the elderly becoming more skilled at avoiding phishing attacks or advancements in anti-phishing software benefiting the elderly more. The increase in technology usage during the pandemic, combined with a shift in effort towards youth-dominated spheres, could account for an increase in skill; familiarity with technology and phishing itself was identified as an advantage in being suspicious of phishing in the Gavett et al. study, although the Parti study disagreed. In addition, as the modern phishing attack evolves, older adults might be better equipped to handle it: The Gavett et al. study found

older adults with knowledge of phishing more suspicious than younger adults with knowledge of phishing. With more advanced phishing attacks, this increased suspicion generated by greater technological awareness might be a significant advantage in avoiding attacks. However, there is not enough evidence to conclude this; more research should be conducted to examine these hypotheses.

Conclusion

Potential factors that contributed to the drop in successful phishing reports for the elderly in the U.S. post-pandemic include changing vectors of attack, greater technological familiarity and having tendencies that are better adapted to the modern phishing landscape. Factors that likely did not contribute to the drop include fewer phishing attempts, less advanced phishing attempts, or less usage of risky technology when compared to pre-pandemic levels. Since other forms of cybercrime continue to rise for older adults, the factors that provoked this improvement are isolated to phishing itself and should not be generalized to all forms of cybercrime. Despite this, further research on this topic could provide greater insight into preventing general cybercrime. Further research should be conducted examining the usage habits of the elderly and younger adults more granularly, preferably in a real-world environment.

References

APWG (2020a). *Phishing Activity Trend Reports.* 1st Quarter 2020 Technical Report, APWG (2020) https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

APWG (2020b). *Phishing Activity Trend Reports.* 3rd Quarter 2020 Technical Report, APWG (2020) https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

APWG (2022). *Trend Reports*. 1st Quarter 2022. Technical Report, APWG (2022). https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

APWG (2025). *Trend Reports*. 4th Quarter 2024. Technical Report, APWG (2024). https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

Carroll, F., Adejobi, J., & 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 COMPUT. SCI.* **3**, 170. https://doi.org/10.1007/s42979-022-01069-1

Chen A., Shaoqing, G., Cho, S., Teng, A., Chu, F., Demiris, G., & Zaslavsky, O. (2021). Reactions to COVID-19, information and technology use, and social connectedness among older adults with pre-frailty and frailty. *Geriatric Nursing*, Volume 42, Issue 1, 2021, Pages 188-195, ISSN 0197-4572. https://doi.org/10.1016/j.gerinurse.2020.08.001.

Gavett, B., Zhao, R., John, S., Bussell, C., Roberts, J., Yue, C. (2017) Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS ONE* 12(2): e0171620. https://doi.org/10.1371/journal.pone.0171620

Grassini, S., Thorp, S., Sevic, A., & Cipriani, E. (2025). Attitudes Toward Technology and Artificial Intelligence: The Role of Demographic and Personality Factors Predictors of attitudes toward technology and AI. DOI:10.31234/osf.io/7ca4t_v1

Haase, K., Cosco, T., Kervin, L., Riadi, I., & O'Connell, M. (2021). *Older Adults' Experiences With Using Technology for Socialization During the COVID-19 Pandemic: Cross-sectional Survey Study*. JMIR Aging 2021;4(2):e28010 doi: 10.2196/28010

Hoheisel, R., Capelleveen, G., Sarmah, D., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, Volume 128, 2023, 103158, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103158.

Baker, E., & Cartier, M. (2024). *Phishing trends report (updated for 2025).* The Hoxhunt Human Risk Management Platform. https://hoxhunt.com/guide/phishing-trends-report

Internet Crime Complaint Center. (2020, April 30). *2020 IC3 Annual Elder Fraud Report.* Federal Bureau of Investigation.

https://www.ic3.gov/AnnualReport/Reports/2020_IC3ElderFraudReport.pdf

Internet Crime Complaint Center. (2020, March 6). *2020 IC3 Annual Report. Federal Bureau of Investigation*. https://www.ic3.gov/AnnualReport/Reports/2020_IC3Report.pdf

Internet Crime Complaint Center. (2024, April 30). *2023 IC3 Annual Elder Fraud Report.* Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf

Internet Crime Complaint Center. (2024, March 6). *2023 IC3 Annual Repor*t. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Oliveira, D., Rocha, H., Yang, H., Ellis, D, Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017). Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6412–6424. https://doi.org/10.1145/3025453.3025831

Osamor, J., Ashawa, M., Shahrabi, A., Philip, A., & Iwendi, C. (2025). The Evolution of Phishing and Future Directions: A Review. *International Conference on Cyber Warfare and Security*. 20. 361-368. https://doi.org/10.34190/iccws.20.1.3366

Parti, K. (2023) What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. *Front. Psychol.* 14:1118741. https://doi.org/10.3389/fpsyg.2023.1118741

Pehlivanoglu, D., Shoenfelt, A., Hakim, Z., Heemskerk, A., Zhen, J., Mosqueda, M., Wilson, R., Huentelman, M., Grilli, M., Turner, G., Spreng, R., & Ebner, N. (2024). Phishing vulnerability compounded by older age, apolipoprotein E e4 genotype, and lower cognition. *PNAS Nexus*, Volume 3, Issue 8, August 2024, page 296. https://doi.org/10.1093/pnasnexus/pgae296

Sixsmith, A., Horst, B., Simeonov, D., & Mihailidis, A. (2022, June). Older people's use of digital technology during the COVID-19 pandemic. *Bulletin of science, technology & society*. https://doi.org/10.1177/02704676221094731

Suzuki, Y. E., & Monroy, S. (2022). Prevention and mitigation measures against phishing emails: a sequential schema model. *Security Journal*, 35(4), 1162–1182. https://doi.org/10.1057/s41284-021-00318-x