THE EFFECT OF AGE ON THE EFFICACY OF PHISHING PREVENTION METHODS

THE ROLE OF POST-PANDEMIC TECHNOLOGICAL VIEWS ON REDUCED PHISHING REPORTS AMONG THE ELDERLY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Charlotte Miller

November 8, 2024

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.

ADVISORS

Kent Wayland, Department of Engineering and Society

Briana Morrison, Department of Computer Science

Introduction

Phishing, a type of cyber-crime involving fraudulent messages, often emails, designed to scam victims into sending money or to gain access to sensitive information or resources, is one of the new dangers brought by the digital age (Gavett et al., 2017; Pehlivanoglu, 2024). Hundreds of thousands of Americans each year fall prey to phishing scams and can pay a hefty financial price for it (Internet Crime Complaint Center [IC3], 2024b). However, in the past couple years, the number of victims of phishing recorded by the Internet Crime Complaint Center, or the IC3, the FBI's hub for handling cyber-crime, has shown a downward trend after peaking in 2021, even as the total amount of cyber-crime continues to rise (IC3, 2024b). In 2023, complaints of phishing were down 13% compared to the previous year. However, this number was not consistent among the age groups reported by the IC3. Nowhere is the decline of successful phishing attack reports more apparent than in the elderly population: Since 2021, phishing reports have dropped 66% among those older than 60 (IC3, 2024a). Phishing attacks are the most common form of cyber-crime among the total population, yet for the over 60 population, phishing has slipped into only the eight most common type of cyber-crime complaint reported. This age group, which still reports the highest number of cyber-crime complaints among the age groups used by the IC3, has been long stereotyped as the most vulnerable to phishing attacks (Sarno et al., 2020). Understanding how and why the elderly population seem to be falling for fewer and fewer phishing attacks could be key to preventing and addressing phishing attacks as well as creating better methods of preventing other forms of cyber-crime, both in the elderly population and for the general population. This paper will conduct research on how old age impacts interaction with phishing scams in relation to detecting phishing, both by exploring the effect of a changing attitude of the elderly population towards technology in the aftermath of the pandemic and by conducting research on different methods of phishing prevention and their efficacy among different age demographics.

Technical Report

How does age affect the efficacy and optimization of different phishing prevention methods?

It is clear from current studies and recorded phishing numbers that different age groups currently exhibit different behaviors when it comes to phishing (Sarno et al., 2020). The oldest age group reported by the IC3, which includes people aged 60 and older, once were primary victims of phishing, reflecting their increased susceptibility to cyber-crime overall (IC3, 2024a). However, in recent years a change in the reported demographics of phishing victims has occurred, as phishing rates decrease for the elderly at a far sharper rate than the general population (IC3, 2024a, 2024b). One proposed reason is an increased rate of efficacy among elderly populations when it comes to methods of preventing phishing (Sarno et al., 2020). This report will seek to answer the question of how age impacts the efficacy of phishing prevention methods.

Methods of phishing prevention are continuously developed and refined by interested stakeholders such as companies marketing software that could be a vector for phishing, such as email software creators that make features designed to flag potential phishing scams, or companies trying to prevent their employees from falling victim to a scam. Phishing prevention methods can take on a large variety of forms including training and awareness campaigns, as well as software restricting potentially dangerous behaviors, or software designed to flag potential threats (Naqvi et al., 2023). Not all members of the population have equal exposure to phishing prevention methods, creating a potential difference across age groups (Suzuki & Monroy, 2022). For example, age groups that are more likely to be employed are also more likely to receive phishing training from their company . Younger students and employees of a company might receive technology owned by their school or company with restrictive software installed to prevent potentially compromising activity. However, when exploring the impact of phishing prevention methods, efficacy is potentially equally important to deployment. There is a dearth of literature that considers how methods of phishing prevention might vary in effectiveness for different population groups such as age, even as the prevailing literature suggests different behaviors among different age groups when it comes to phishing (Sarno et al., 2020). Understanding the reaction of different age groups to varying methods of phishing prevention methods and their resultant efficacy will lead to better understanding of why trends in phishing have differed among age groups in recent years, which could help in finding the best methods for reducing phishing numbers across the population.

For this report, three simple software methods of email phishing prevention will be simulated, tested and refined among different age groups with simulations of phishing attacks. The three methods were chosen to represent different strategies in vulnerability mitigation: warning, represented in this experiment by the utilization of software that detects and "flags" indications of spam, lockdown, represented by software that disallows certain risky behaviors, such as clicking on links embedded within an email, and awareness, which will be represented by a software that requires the completion of training and provides access to resources within the inbox providing guidance on how to verify an email (Naqvi et al, 2023). Subjects will be given a baseline test in which they are tasked with individually classifying emails and messages as real or phishing, while also indicating whether they are "interested" or not in the content of the email or message. After the baseline test, one of the methods of phishing prevention will be introduced in the form of a rudimentary simulation of how each method would work incorporated into the test email environment, and the subjects, consisting of a group of adults age 60+ and a younger age group, will be asked to repeat the test. During the tests, the accuracy of their responses will be measured in addition to their behavior during the test (e.g. the time it takes to evaluate each potential scam). The "interest" metric will be used to determine the extent that real-world outcomes are dependent on preferences and not robust internet safety skills. After initial results, the subjects will be interviewed on how their method of phishing prevention affected their thought processes and decisions. The interviews and results among each age group will be used to refine the method of phishing prevention. The newly refined methods will then be tested by

new subjects in the same manner to see how the adjustments affected the results. At the conclusion of the experiment, the results will be used to develop a sample software "solution" using a blend of one or more of the phishing prevention methods tested, with the aim of maximizing phishing prevention for the elderly age group. This experiment is designed to illuminate both the differences in how different age groups vary in their responses to phishing simulations while addressing how methods of phishing prevention can be best tailored to an age group's vulnerabilities.

STS Research Problem

What role does changing attitudes towards technology play in the large drop in phishing reports among the elderly population in the post-COVID era?

Background

The COVID-19 pandemic spurred a large change in the daily use of technology among all age groups, with use increasing due to quarantine (Sixsmith et al., 2022; Parti et al. 2023). Like other age groups, the elderly population also increased their use of technology, especially for the purposes of connection, shopping, or entertainment (Sixsmith et al. 2022). The majority of older adults also claimed they planned to continue these technology usages after the pandemic (Sixsmith et al., 2022). With increasing use and reliance on technology, an increase in cyber-crime might be expected (Pehlivanoglu et al., 2024). While cyber-crime continues to rise among both the general population and the elderly population, phishing reports for the elderly peaked in 2021 and have sharply declined by 66% since, showing much better improvement than the general population (IC3, 2024a). Many potential factors could be affecting this improvement gap, such as changing technological usage. One potential reason is altered attitudes towards technology among swathes of the elderly. Older adults' view of technology and the Internet is colored by the large changes in available technology since their youth, which creates a relative unfamiliarity and potential resistance to technology (Garrett et al. 2017). Their increased exposure and usage as a result of the pandemic potentially acted as a catalyst for different outlooks on technology. Understanding why the post-pandemic phishing outcomes have differed in the elderly as opposed to other age groups is essential to understand how phishing can best be prevented, especially for populations considered more vulnerable, like the elderly.

Methodology & Literature Review

Despite the common stereotype of elderly people being the most susceptible to phishing attacks, the research and data conducted on the topic has contradictory and uncertain results. Two studies did find a correlation between being older and being more likely to fall for fraudulent emails. A study by Oliveira, D., et. al. (2017) found susceptibility differences between younger and older adults are pronounced yet mostly in what they interact with rather than accuracy in perceiving phishing. In a study by Parti, K. (2023), it was found that higher ages correlated with a higher likelihood of not reporting fraud that occurred. This is a potential explanation of the

discrepancy between the relatively low number of complaints registered in phishing among the elderly compared to the general population in recent year. However, this fails to explain the sudden drop in phishing complaints. In the same study, familiarity with a computer had a negative impact on perceiving phishing, which could offer insight into how age is affecting phishing susceptibility. More research should be conducted on whether this was because of desensitization to the threat of phishing or because of a false sense of confidence in perceiving phishing. Some research suggests that knowing more about phishing is more effective in protecting older adults than younger adults and therefore training might be more effective (Sarno et al., 2020). Overall, the trends and reports in phishing complaints in the U.S. are not well explained by the current research on the impact of age solely on the impact of identifying phishing scams. This research seeks to expand the current research by understanding the cultural elements that have impacted the elderly population as it comes to phishing scams and the role that changing attitudes have played.

To gain a better understanding of the difference in vulnerabilities among different age groups, this report will utilize the aforementioned studies of the impact of age on phishing as well as supplementary studies on cyberfraud and age. In addition, to answer the "change" aspect of the question posed by this paper, research will be examined on post-pandemic changes in attitude towards technology among the elderly, the effect attitude towards technology has on technological behavior, and the recent evolution of phishing tactics and trends. Each of these areas will be analyzed to provide context to the post-pandemic phishing report trends in conjunction with the most recent data on cyber-crime and phishing in the United States as collected by the IC3. The mutual shaping of the technological behaviors centered around phishing and the prevalent phishing methods and tactics will be used as a concept to better understand the cause of a changing cyber-crime landscape, with the additional catalysts for change of the pandemic and technological evolution. Finally, further evidence-based research as discussed in the technical project will be conducted to determine the impact of phishing prevention methods on the age discrepancy.

Conclusion

The STS portion of this report seeks to assess the connection between the attitudes towards technology of the elderly post-pandemic and the drop in phishing reports by the elderly in the same timeframe. The Technical portion of this report will seek to gauge how software methods of phishing prevention can be best tailored to different age groups for maximum efficacy. Ultimately, this report seeks to explore aspects of the relationship between age and phishing, with the ultimate goal of understanding how the impacts of age on phishing vulnerability can be used for the better prevention of phishing.

References

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., 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

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 Report*. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., Porras, J. (2023) Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security, Volume 132, 2023,103387.* https://doi.org/10.1016/j.cose.2023.103387.

Oliveira, D., Rocha, H., Yang, H., Ellis, D, Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin T., & Ebner, N. C. (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. In *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

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. C., Huentelman, M., Grilli, M. D., Turner, G., Spreng, R. N., Ebner, N. C. (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

Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2020). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human Factors, 62(5),* 704-717. https://doi.org/10.1177/0018720819855570

Sixsmith, A., Horst, B. R., 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. A. 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