Phishing Prevention for the Elderly: How Age Impacts Efficacy of Software Phishing Prevention Methods

A Technical Report submitted to the Department of Computer Science

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

Brianna Morrison, Department of Computer Science

Phishing Prevention for the Elderly: How Age Impacts Efficacy of Software Phishing Prevention Methods

CS4991 Capstone Report, 2025

Charlotte Miller
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
wkw3mb@virginia.edu

ABSTRACT

Cybercrime in the United States impacts the elderly age group at higher rates and often through different vulnerabilities than the rest of the population. For phishing, the most common form of cybercrime, exposure and response to phishing differs across age groups, indicating methods of phishing prevention might not have equal efficacy for both the elderly demographic and younger age groups. To test this premise, I propose utilizing in a lab setting various mock versions of software phishing prevention methods and synthesizing outcomes between two age groups to find a more effective method. Using the results and feedback, a fully-developed software phishing prevention method geared towards the elderly should be developed and used for second-round testing. The results of the study are anticipated to show the efficacy of following age-specific data when developing software methods of phishing prevention. To further test the efficacy of phishing prevention, the created software should be deployed and tested in a real-world environment.

1. INTRODUCTION

Cybercrime is a rapidly increasing problem in the digital age, and a problem segregated by age in United States. The elderly population in the U.S. is substantially more vulnerable by to cybercrime than younger demographics (IC3, 2024). Although the most prevalent form of cybercrime, phishing, is an exception to this trend, the elderly show sharply different patterns when engaging with phishing. Despite these differences when it comes to interacting with phishing, there is a lack of research into age-specific phishing prevention methods, including in software methods of phishing prevention (Sarno, et al., 2020). Understanding how age affects the efficacy of anti-phishing software could be useful not only in preventing successful phishing attacks on different age groups but also is a valuable data point from which to explore the efficacy of age specific interventions in all forms of cybercrime. To determine whether tailoring anti-phishing software for an age group improves phishing outcomes for that age group, this paper proposes the development of an anti-phishing software for the elderly population.

2. RELATED WORKS

The role of age in susceptibility to phishing has been extensively researched, with varying and often contradictory results. Some research supports the stereotype of elderly people being more susceptible to phishing attacks. One study found age in addition to age-related conditions such as Alzheimer's and diminished cognition to be predictors of lessened ability to determine whether an email was safe within a lab setting (Pehlivanoglu, 2024). In addition, the elderly might lag behind when it comes to response.

A concerning study by Parti (2023) found that older adults were less likely to report or ask for help after falling victim to cybercrime. However, while the current body of research does support large differences between younger and older adults when it comes to phishing, most studies are less one-sided. Rather than one age group being more vulnerable to phishing attacks across all circumstances, current research

suggests that the older and younger adult age groups have different weaknesses when it comes to phishing.

After asking younger and older adults to classify a mix of legitimate emails and phishing attacks, a study by Sarno, et al. (2020) found no significant difference. However, when no time pressure was applied, older adults exhibited different behavior, taking more time than younger participants to classify each email, as well as being more likely to classify any given email as not safe or spam without increasing or decreasing accuracy. In this experiment, the older age group appeared more cautious than the younger participants; however, the participants' prior knowledge of phishing was not included in the study.

Another study, by Garrett, et al. (2017), pinpointed the impact of phishing education as a potential difference between the age groups when testing whether they noticed phishing attempts during a lab web-browsing activity. Having prior education on phishing had a larger impact on older adults in determining whether they found emails suspicious. The older adults with prior knowledge of phishing were the most suspicious of all groups tested. However, the older adults who did not have prior knowledge of phishing were the least suspicious of all groups tested.

In addition to evidence supporting a difference in the efficacy of phishing prevention methods such as phishing education between younger and older age groups, differences could exist in the type of attacks the age groups are most vulnerable to. When testing participants in their home over a 21-day period, a group of researchers found evidence of an age divide in falling prey to spear phishing based on the life domain the phishing attack targeted. Notably, 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, et. al. 2017).

3. PROPOSAL DESIGN

The development of this software is suggested through two rounds of feedback. The first round, meant to understand which elements of the various methods of phishing prevention are most effective for the elderly, will contain two age groups. In lieu of a fully-developed software, mock versions of software phishing prevention methods will be utilized as outlined below. Both the older and younger age groups will then be tested in navigating legitimate emails, as well as phishing attempts for each of these software phishing prevention method approaches. For simplicity, the tests and the software will be limited to the scope of only email forms of phishing. The most effective options for the elderly age group, along with collected feedback and observation will then be used to develop a complete anti-phishing software tailored to the elderly age group. This software will then be used in the second round of testing with only the elderly test group, where it will be evaluated and refined by using a mixture of feedback and the quantitative phishing results.

3.1 Phishing Prevention Tactics

For the purposes of this software, phishing prevention tactics will be split into the three categories of warning, assistance, and reporting, each of which will be implemented with multiple approaches to assess each approach's value as a potential solution.

3.2 Warning-Type Prevention

Warning-type phishing prevention will be defined as methods of phishing prevention that alert the end user to potential phishing risks. "Warning" prevention methods also include in this proposal aggressive forms of warning, such as the blocking of specific actions or materials, in addition to passive alerts. The warning methods of phishing prevention will be divided into attack detection-based warnings, or software that detects potential spam to prompt warning prevention methods, and behavior-based warnings, or software that detects potentially risky behavior independent of the potential phishing material to prompt the warning. An example of a behavior-based warning would be an alert caused by attempting

to click a link in any email, whereas an example of an attack detection-based warning would be the flagging of an email sent from a suspicious domain.

Attack detection-based and behavior-based warnings have different advantages. By producing warnings only when phishing is more likely, attack detection-based warnings are more likely to be noticed and not tuned out; whereas behavior-based warnings are present even on emails with low likelihood of phishing attacks and could become ignored over time. However, attack detection-based warnings might encourage a false sense of security in emails without a warning.

Aggressive and passive versions of phishing warnings will also be evaluated. The "aggressive" approach constitutes the blocking of specific behaviors such as directly following links or disabling images, whereas the passive version only has a pop-up warning. In total, four approaches to warning-type phishing prevention will be evaluated, as shown in Figures 1-4 below:

A) Passive Attack Detection-Based

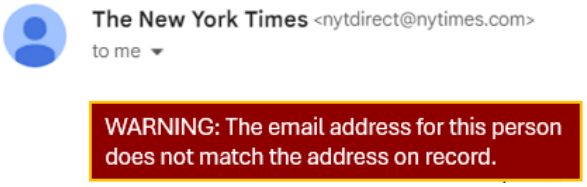

Figure 1: Example of Passive Attack Detection-Based Warning

B) Aggressive Attack Detection-Based

Figure 2: Example of Aggressive Attack Detection-Based Warning

C) Passive Behavior-Based

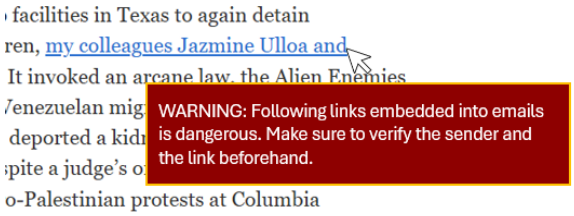

Figure 3: Example of Passive Behavior-Based Warning

D) Aggressive Behavior-Based

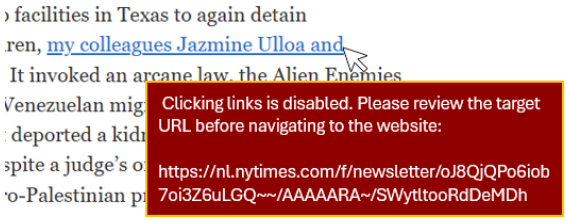

Figure 4: Example of Aggressive Behavior-Based Warning

3.3 Assistive-Type Prevention

Assistive methods of phishing prevention will be defined as the increased availability of phishing prevention resources through the software, such as the ability to ask a chat box to evaluate authenticity of an element of an email/website. Two types of assistive-type prevention will be evaluated for usage and efficacy, as shown in Figures 5-6 below:

A) AI Assistive Chat-box

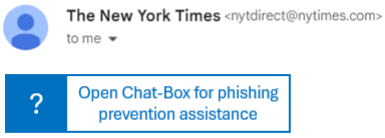

Figure 5: Example of AI Assistive Chat-Box in Software Phishing Prevention

B) Integrated Resources

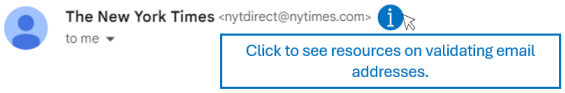

Figure 6: Example of Integrated Resources in Software Phishing Prevention

3.4 Reporting Phishing

Reporting phishing when it is encountered or after a successful phishing attack is vital to mitigating the continuation and effects of the

attack. Prior studies have shown a reluctance to report phishing among the elderly after an attack (Parti, 2023). Three different approaches to phishing report buttons will be tested to ascertain whether the design of the reporting button affects the likelihood of reporting phishing for the elderly age group, as shown in Figures 7-9 below:

A) Simple Direct

Figure 7: Image of Phishing Report Button for Simple Direct Approach

B) Indirect

Figure 8: Image of Phishing Report Button for Indirect Approach

C) Flag Icon

Figure 9: Image of Phishing Report Button for Icon Approach

4. ANTICIPATED RESULTS

Ultimately, older and younger adults have different measured reactions to phishing across all facets: phishing prevention, type of phishing attack and response. Despite this, phishing prevention methods are largely generalized and not developed to protect a specific age group. However, researchers such as Sarno et al. (2020) have seen a need for more targeted phishing prevention methods and called for the further testing of age-specialized phishing prevention.

Prior research on the different preferences in phishing prevention methods for the elderly compared to younger demographics found that elderly demographics were more willing to use support-based phishing prevention and more willing to trust the advice given by support-based phishing prevention, especially social forms such as human assistance (Pakianathan, 2024). Therefore, it can be hypothesized that more effective phishing prevention software for the elderly will more heavily incorporate assistive-type prevention methods. In addition, some prior research indicates that elderly adults are more likely to spend more time evaluating emails for phishing when there is no imposed time limit (Sarno, et al, 2020). Therefore, the time-consuming methods of phishing prevention like assistive-type methods might be better received by the older age group.

5. CONCLUSION

Phishing prevention software is vital to reducing phishing victims. Until anti-phishing technology is adjusted to address the age-based differences that impact how a potential phishing victim interacts with phishing material, a promising avenue for its development is left unexplored. Ultimately, by methodically researching and selecting effective features for the elderly age-group, the resulting anti-phishing software will provide greater protection to its targeted end-users and is certain to provide more insight into how age impacts the efficacy of software phishing prevention. The greater understanding of how phishing prevention can be optimized for age will not only improve phishing prevention posture but also provide valuable insight into preventing other forms of cyber-crime for the especially vulnerable elderly population.

6. FUTURE WORK

To reap the benefits of age-specific anti-phishing software, the experimental steps outlined above must be conducted, including the recruitment of participants. In addition, after the two rounds of testing I propose, the finalized software should be deployed and monitored in a real-world environment over a longer period of time to confirm the lab results. After verification, the software can be used both as a phishing prevention method and a model for the further development of age-specific anti-phishing or cyber-crime prevention software.

REFERENCES

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

Internet Crime Complaint Center. (2024, March 6). *2023 IC3 Annual Report*. 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. 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. Front. Psychol. 14:1118741. doi: 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. In PNAS Nexus, Volume 3, Issue 8, August 2024, page 296. https://doi.org/10.1093/pnasnexus/pgae296

Sarno, D., Lewis, J., Bohil, C., & Neider, M. (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