Audible Phishing Attack Identification and Prevention Google Extension

(Technical Report)

An Analysis of the Difficulties for Elderly and Disabled People in Phishing Attack Prevention

(STS Report)

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
Alan Sameth

November 3, 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

Gerard J. Fitzgerald, Department of Engineering and Society

Briana Morrison, Department of Computer Science

Introduction

For as long as the internet has existed, cybercriminals have been looking for methods to steal personal information from unaware victims. Now that every company uses the internet and networks in order to access and manipulate essential data, it is more important than ever to be vigilant against cyber-attacks. According to Crowdstrike, a cybersecurity company based in Austin, phishing attacks are the third most common form of cyberattack (Baker, 2024). A phishing attack is a cyberattack where criminals impersonate known and trustworthy individuals, groups, or websites to steal personal data such as passwords or Social Security numbers usually sent through email, text, or phone calls. Phishing attacks are the most common cause of data breaches and lead to hundreds of millions of dollars in damages for users every year. As phishing attacks become more sophisticated, especially with the rapid adoption of artificial intelligence or AI, the elderly and disabled only become disproportionately more susceptible to cyber criminals. University of Florida researchers found that older adults were weaker at phishing detection and older individuals carrying the genotype apolipoprotein E e4 (APOE4), the gene that increases the risk of Alzheimer's disease, were even worse at preventing phishing attacks (Didem, 2023). Additionally, dyslexic individuals struggle to prevent phishing attacks (Grimes, 2023) and visually impaired people struggle to identify phishing attacks with their assistive software (Janiero, 2016). With more valuable information and money online than ever before, older adults and disabled people are at a much greater threat of phishing and stand to lose more than ever before

As the internet continues to grow and more websites are published daily, both elderly and disabled people find websites more difficult to interact with. Modules and functions become

more complex as there is no standardization in website conventions or terminology, making new sites incredibly hard to use and leading to distrust for the disabled and elderly. In addition, the assistive software used to access the internet such as text-to-speech for visually impaired people is not helpful in phishing attack prevention. From the perspective of human-computer interaction (HCI), the study of the communication and use between people and computers, my STS research intends to analyze the barriers in accessibility between vulnerable groups, websites, phishing attacks, and software to understand the shortcomings of current phishing prevention and assistive software.

The technical project is a Google extension that would actively identify and notify users of potential phishing attacks. Many websites, assistive software, and anti-phishing software are developed with healthy adults in mind and fail to take into consideration both physical and mental disabilities. Therefore, my anti-phishing software will address these barriers in usability and accessibility. The extension would contain a database of trustworthy sites and compare uniform resource locators (URLs) to whitelisted and blacklisted websites and notify the user through visual and audio cues that the link is a phishing attempt. The technical project intends to address the needs of both elderly and disabled people by focusing on accessibility.

Technical Project Proposal

Anti-phishing software is widely available throughout the internet and is incorporated with anti-virus such as Norton or McAfee. Anti-phishing tools examine various attributes to identify phishing attempts, primarily through URL structure, content, email headers, or cataloging trustworthy users and websites. When a phishing attack is identified, the software then provides a warning to the user through a visual element and blocks the site from being

accessed at the user's discretion. However, many of these tools strictly have visual notifications for users and accessibility features for visually impaired people.

In an analysis of the accessibility from an HCI perspective, many anti-phishing tools do not adequately accommodate visually impaired users. Almost every application relies on visual notifications such as color and pop-ups, which are inaccessible for visually impaired users through a screen reader. Additionally, phonetic similarities and a lack of shortcuts and guidelines make it harder for users to utilize current anti-phishing software (Sonowal, 2017). To accommodate the visually impaired, the anti-phishing prevention tool I am proposing will have accessibility-conscious features to allow visually impaired people to use it daily.

The anti-phishing software I plan to develop will primarily analyze links and email headers to identify phishing attacks. The software will have access to a local database containing data from legitimate websites such as Google and Amazon and phishing websites. The software will then compare the URLs and look for discrepancies to correlate links as either legitimate or deceptive. If the site is deemed legitimate, the user can proceed to the site as normal and a notification containing both visual and audio notifications will notify the user as safe. If a link is deemed a phishing attempt, an alert will pop up for the user, play an audio tone of the problem, and then notify the user of the specific discrepancy in the link through text-to-speech. If a legitimate website is mistakenly identified as a phishing attempt, the user can click a button to ignore the warning and continue to the site or use a keyboard shortcut. The keyboard shortcuts are essential for visually impaired people as the shortcuts assist them with interacting with the software rather than relying on a mouse. In addition to the features of the anti-phishing software, there will be a concise and clear set of guidelines for the user to teach the user how to interact

with the program. The introduction guidelines will provide all the different warnings and audio tone samples and point out areas of concern for the user to combat phishing attacks.

The technical project aims to build an anti-phishing extension with the consideration of disabled people as users. From an HCI perspective, by making accessibility a priority of the software by providing both audio cues and keyboard shortcuts, visually impaired people can use the extension to avoid phishing attacks.

Science, Technology, and Society Project Proposal

For 2023 alone, 298,878 phishing attacks were reported by the public to the Federal Bureau of Investigation (FBI) through the Internet Crime Complaint Center (IC3) for victims and lost more than $18 million to phishing attacks. It represents an overall 10% increase in cyber attacks and has led to a 22% increase in losses for 2023 (IC3, 2023). As phishing attacks continue to increase year over year and evolve with the assistance of AI, it is more important than ever to be skeptical of emails and websites. In addition, with more assets and money poured into servers and cloud computing, companies have to train and test their employees to prevent phishing attacks so that they can protect their data. However, elderly and disabled people are disproportionately armed to prevent phishing attacks and struggle in corporate phishing tests. The various physical disabilities that cause visual impairment not only make it harder for people to detect phishing attacks, but it also makes it harder to access trustworthy websites as they have to treat every website with more scrutiny, often needing to rely on other healthy individuals for confirmation. On the other hand, elderly people due to a combination of unfamiliarity with technology and cognitive impairments fall for scams more often.

Visually impaired people are disproportionately affected by phishing attacks. When interacting with the internet, visually impaired people have to use a variety of assistive tools, the most common being screen readers Job Access with Speech (JAWS) for desktops, and Voiceover for mobile/phone devices(Inan, 2016). Even though text-to-speech software functions normally for day-to-day use, they fail when identifying phishing attacks. Screen readers and image recognition software frequently issued inaccurate warnings or malfunctioned when analyzing emails for phishing attacks (Janeiro, 2024). These frequent screen reader failures made it challenging for visually impaired users to detect phishing attempts themselves (Janeiro, 2024). Due to these issues, visually impaired individuals had to often rely on a healthy second party for confirmation, a resource that would not always be available to them (Janeiro, 2024). These limitations highlight that current tools are far from optimal solutions for phishing prevention among users with disabilities.

In an examination of internet security and accessibility, the researchers found that the visually impaired with higher levels of knowledge in cybersecurity had a negative correlation with internet use, suggesting that cybersecurity concerns led to less internet use for various activities (Inan, 2016). The study implies that visually impaired individuals with concerns for their safety and security have to be conservative with their internet use, a vital resource in today's society. These concerns may lead them to turn to anti-phishing software for daily internet use to be safer. However, the current market of anti-phishing software lacks the accessibility features that would allow visually impaired people to use the tool. Every available anti-phishing software relies heavily on visual notifications such as colors, which would be completely inaccessible to the visually impaired. In addition, the lack of keyboard commands and well-written instructions makes it more challenging for the visually impaired to use these tools

(Sonowal, 2017). The systemic lack of support for the visually impaired leads them to not only be more vulnerable to phishing attacks but also to withdraw from internet use.

Unfortunately, older individuals find themselves just as susceptible to phishing attacks. Older individuals tend to be unfamiliar with technology and as a result, lack the awareness of dangerous cyberattacks that would target them (Oliveira, 2017). The awareness of older individuals along with cognitive decline directly affects their judgment and causes them to mistake legitimate for phishing emails and vice versa (Grilli, 2020). In addition, in adults without dementia, it was found that older age and declining health correlate directly with susceptibility to fraud (James, 2014), and those with the APOE4 genotype, the primary gene that increases the chances of developing Alzheimer's disease, are even more vulnerable to cybercriminals (Didem, 2023). Cognitive disabilities and decline are issues when it comes to defending against phishing attacks.

I argue that the tools and websites currently available to disabled and elderly individuals lack accessibility for them and make them more vulnerable to phishing attacks. In order to demonstrate the accessibility issues and vulnerabilities, I will examine current trends in software design and cyberattacks through an HCI and social engineering perspective. I will analyze the vectors of attack for phishing attacks, current software available, websites, and elderly and disabled people as victims and their struggles to demonstrate the lack of accessibility for marginalized victims with their tools.

Conclusion

The technical project will provide the proposal for assistive software for visually impaired people to prevent phishing attacks through the incorporation of accessible modules and

features. The STS research will provide a socio-technical analysis of marginalized groups of phishing attacks, websites, assistive software, and elderly and disabled people to identify shortcomings in current software and modern website design to discover vectors of attack and vulnerabilities. Both the STS and the technical project will provide a foundation for the creation of accessibility-focused anti-phishing and cybersecurity software in the future to protect the personal data of vulnerable elderly and disabled people

References

Adams, R., Reiss, B., Serlin, D., & Ebook Central Diversity, E., &. I. S. (2015). *Keywords for Disability Studies*. New York University Press.

Rembis, M. A., Kudlick, C. J., & Nielsen, K. E. (Eds.) (2018). *The Oxford Handbook of Disability History*. New York, NY: Oxford University Press.

James, L., Ebook Central - Academic Complete, & O'Reilly Online Learning: Academic/Public Library Edition (2006). *Phishing Exposed*. San Diego: Syngress Press [Imprint].

Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016, January 1). Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments. *Educational Technology & Society*, 19(1), 28 - 40.

Janeiro, J., Alves, S., Guerreiro, T., Alt, F., & Distler, (2024, September 1). Understanding Phishing Experiences of Screen Reader Users. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, 22(5), 63 - 72.

Sonowal, G., Kuppusamy, K. S., Kumar, A., (2017, January 7). Usability evaluation of active anti-phishing browser extensions for persons with visual impairments. *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, IEEE Secur. Privacy

BARBOSA, N. M., HAYES, J., KAUSHIK, S., & YANG WANG (2022, September 1). "Every Website Is a Puzzle!": Facilitating Access to Common Website Features for People with Visual Impairments. *ACM Transactions On Accessible Computing*, 15(3), 1 - 35.

Didem Pehlivanoglu, Shoenfelt, A., Hakim, Z. M., Heemskerk, A., Zhen, J., Mosqueda, M., Wilson, R., Huentelman, M. J., Grilli, M. D., Turner, G. R., R. Nathan Spreng, & Ebner, N. C. (2023). *Phishing Vulnerability Compounded by Older Age, APOE4 Genotype, and Lower Cognition*.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of elder abuse & neglect*, *26*(2), 107–122.

Griffiths, C. (2024, June 26). *The Latest Phishing Statistics (updated June 2024): AAG IT Support*. AAG IT Services. https://aag-it.com/the-latest-phishing-statistics/#:~:text=With%20an%20average%20of%20%24136,emails%20per%20100%20internet%20users.

Baker, K. (2024, May 13). *12 most common types of cyberattacks*. Crowdstrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

Grimes, L. G. (2023) *Susceptibility of dyslexic individuals to phishing attacks*. Auckland, New Zealand. University of Auckland

Alanazi, F., and Renaud, K. and Tal, I. (2023) Understanding the impact of dyslexia on online privacy and security. *IEEE Cyber Research Conference Ireland*.

Internet Crime Complaint Center. (2023). *Internet Crime Report*. FBI.

Grilli, M., McVeigh, K., Hakim, Z., Wank, A., Getz, S., Levin, B., Ebner, N., Wilson, R. (2020) Is This Phishing? Older Age Is Associated With Greater Difficulty Discriminating Between Safe and Malicious Emails, *The Journals of Gerontology: Series B*, Volume 76, Issue 9, November 2021, Pages 1711–1715,

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.