Mitigating Social Engineering Attacks on the Elderly: Personalized Countermeasures to Enhance Cyber Situational Awareness

Jacob Vargis, Marymount University, United States
Diane Murphy, Marymount University, United States

The European Conference on Aging & Gerontology 2023
Official Conference Proceedings

Abstract
The elderly population has experienced a significant financial and psychological impact from cyber abuse, particularly during and after COVID-19. This heightened vulnerability is primarily due to the rapid shift of essential services - such as Internet banking, telemedicine, and online shopping - to digital platforms, leaving many older adults unprepared and reluctant users of these technologies. To understand this phenomenon, we conducted an inductive analysis of literature reviews across multiple technical and socio-behavioral disciplines related to cyber abuse among older adults. Our findings revealed that social engineering attacks often exploit vulnerabilities associated with socio-behavioral traits unique to this demographic. Furthermore, we utilized reflexive thematic analysis to examine and interpret victims' accounts of cybercrime incidents, identifying patterns, relationships, and the influence of situational variables on their cyber situational awareness. This research informs the development of personalized countermeasures based on *cyber phenomics* to enhance cyber situational awareness and mitigate social engineering threats for the elderly population.

Keywords: Cyber Security, Cyberethics, Cybersecurity Education, Older or Senior Cyber Users, Cyber Abuse, Software Vulnerability Discovery, Cyber Situational Awareness, Cyber Threat Countermeasures, Assistive Technologies, Intelligent Systems, Personalized Countermeasures, Phenomics, Personalized Medicine

Introduction

The growing dependence on cyberspace has left the elderly population more vulnerable to cyber threats, particularly social engineering (SE) attacks. Traditional countermeasures such as cyber threat awareness training are often inadequate for the elderly due to their lifestyle, unique socio-behavioral traits, and cognitive state.

This study applies a constructivist philosophy to understand the challenges older adults face in the digital landscape. The study explores SE attack patterns and vulnerable socio-behavioral traits by analyzing descriptive crime incident reports during the COVID-19 peak, providing a framework for personalized, information-driven countermeasures that adapt to evolving threats.

Grounded in social constructivism, this research assesses the current state of countermeasures, advocates for enhanced cyber situational awareness (cyberSA), and examines the potential of the N-of-1 approach for personalized countermeasures. By investigating the feasibility of an N-of-1 approach and leveraging discriminate data, this study offers valuable insights and a promising direction for future research in personalized cybersecurity countermeasures.

This study employed inductive reasoning and analysis of a vast array of peer-reviewed and grey literature across multiple domains and organizations related to older adults' cybersecurity, identifying emerging themes concerning cyber threats and vulnerabilities faced by this user group. A summary of the literature review is provided below.

An Aging Populace

Internet threat actors use social engineering attacks to exploit age-related vulnerabilities like emotional insecurities and difficulties adapting to fast-changing technology. **Figures 1** and **2** illustrate the projected doubling of the US population aged 60 and older by 2045, constituting over a fifth of the population.

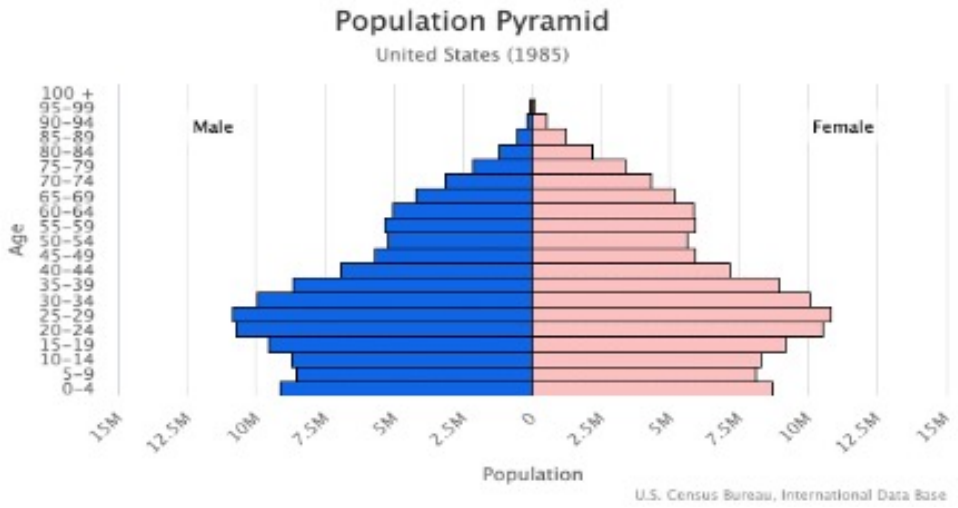

Figure 1: Population pyramid of 60+ for 1985

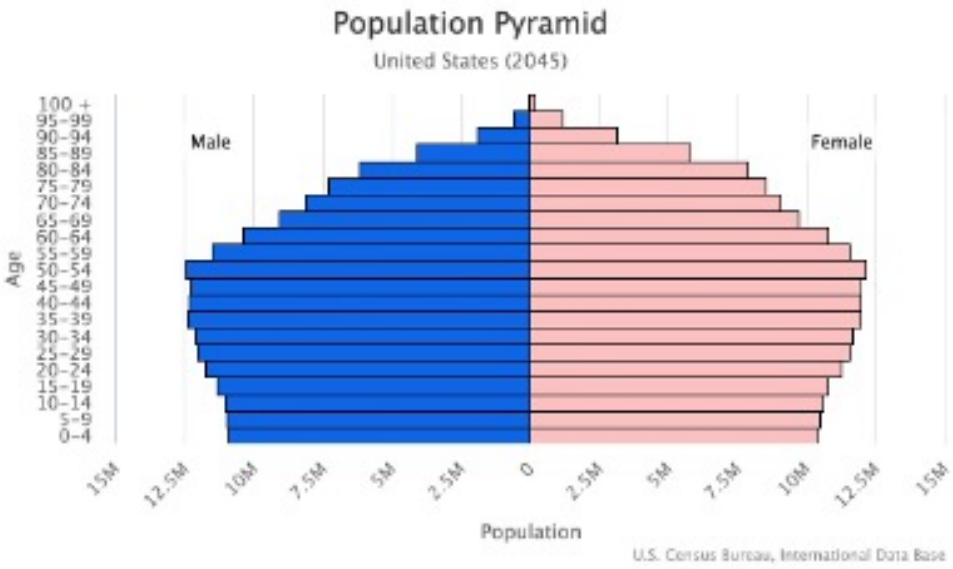

Figure 2: Population pyramid of 60+ for 2045

Social Engineering (SE) Attack Vectors

SE attack techniques aggregate and analyze large volumes of information about individuals to target them with highly personalized, adaptable, and effective attack vectors (Rößling & Müller, 2009), exploiting the inherent behavioral vulnerabilities of their victims. Attackers use advanced persistent threats such as sophisticated SE tactics that exploit social insecurities and behavior-induced vulnerabilities to dupe unsuspecting individuals into "giving" them access to social network accounts (Vargis & Schaeffer, 2022a).

Behavior-Induced Vulnerabilities

Hardin and Khan-Hudson (2005) state that aging and cognitively impaired citizens have been especially vulnerable to cyber exploits. A 2018 Federal Bureau of Investigation (FBI) report indicates that the elderly are going online in record numbers, opening social media accounts, and spending more time online (FBI, 2018), further exacerbating cyber exploits in this community.

COVID-19: Impact of the Rush to a New Computing Paradigm

The rapid shift to COVID-19-compliant operating models, prioritizing remote access to essential services, has led to hasty digitization, often compromising security and privacy (Vargis & Schaeffer, 2022b; Martinez-Alcala et al., 2021). The FBI's Internet Crime Report (FBI, 2023) highlights the exponential increase in cyberattacks targeting the elderly, with $3.1 billion in losses in 2022, doubling annually since 2019.

Current State of Countermeasures

Current countermeasures against SE attacks mainly focus on general cyber threat awareness training, which is inadequate for the elderly facing sophisticated AI-driven attacks (Puig, 2023). Assistive countermeasures are needed to combat these advanced threats. Mbaziira and Murphy (2018) highlight the limitations of existing deterrence techniques and explore AI

networks utilizing natural language processing and deception-detection discourse for detecting cybercrimes.

Understanding Cyber Situational Awareness (CyberSA)

Cybercriminals mainly use SE tactics targeting behavior-induced vulnerabilities in older adults, compromising their cyberSA. Understanding situational awareness (Endsley, 1998) is crucial for creating effective countermeasures (Gutzwiller et al., 2020). Albladi and Weir (2020) examined behavior, perceptions, and socio-emotions to identify factors predicting vulnerability to SE threats, aiming to develop targeted awareness-raising countermeasures that may vary within individuals over time due to misinformation and social manipulation.

Personalized or N-of-1 Countermeasures

SE attacks are often tailored to their intended targets' specific vulnerabilities and behaviors. Accordingly, countermeasures must be customized to everyone's unique characteristics, including socio-behavioral traits and technical artifacts. These countermeasures can enhance an individual's cyberSA of an impending SE threat by providing individualized awareness prompts to help improve an individual's understanding of imminent cybersecurity risks or threats.

Leveraging Parallels From Other Disciplines

You et al. (2022) explore "harnessing digital platforms to scale the deployment of personalized medicine." In his discussion on "the phenomics revolution," Duncan (2023) quotes Leroy Hood, "The science and technology to help us predict and prevent diseases is arriving," referring to a "new healthcare paradigm" that uses big data and predictive analytics to assess and establish a "person's state of health at any given moment as influenced by their genes and from changes in other molecules," for personalized "wellness care."

This study seeks to encourage a similar approach introducing "cyber phenome," referring to technological, procedural, and behavioral characteristics (and any other relevant situational artifacts) associated with an individual's threat ecosystem. And the study posits that "cyber phenomics," the study of these artifacts, their interplay in a threat scenario, and their decomposition, can aid in devising n-of-1 countermeasures - personalized to an individual's state of situational awareness.

Methodology

This study aimed to identify patterns and vulnerabilities in elderly individuals' SE attacks by conducting an exploratory analysis of crime incident reports from victims aged 60 and older submitted to the American Association of Retired Persons (AARP). The analysis sought to interpret themes, patterns, and relationships between situational variables and threat outcomes. Following a methodical approach, the study used literature review findings to guide deductive reasoning, analyze reports, and decompose data into situational artifacts. These artifacts were classified as thematic states and situational variables, providing a framework for exploring real-time, information-driven countermeasures.

Data Analysis

The immersive recursive thematic analysis adopted a constructivist approach, interpreting correlations between SE threats and exploitable vulnerabilities across multiple disciplines. Cyber threats were decomposed, codified, and distilled into artifacts representing thematic states, situational variables, attack tactics, and behavior-induced vulnerabilities that influence the victim's cyberSA and threat outcomes.

This grounded theory methodology sought to answer the following research questions:

1. What themes emerge from analyzing cyber incident reports?
2. Can situational artifacts associated with these themes be identified?
3. Do these artifacts facilitate exploring personalized countermeasures to SE attacks?

Data Sourcing and Collection

This study's primary data source was the AARP Fraud Watch system, comprising over 2000 cybercrime incidents reported by victims aged 60 and older within a 200-mile radius of zip code 20000 (Washington, D.C., U.S.A) between January 1, 2020, and December 31, 2021. This period was selected due to high crime rates targeting the elderly during the COVID-19 pandemic peak.

Reflexive Thematic Analysis (RTA)

This study employed reflexive thematic analysis (RTA), a flexible method for non-positivist qualitative research for an inductive data-driven methodology to transcribe explicit expressions and interpret latent information. This immersive recursive analysis produced a thematic map of situational artifacts, states, and variables influencing SE attack outcomes, aiding in developing personalized countermeasures and real-time assistive solutions.

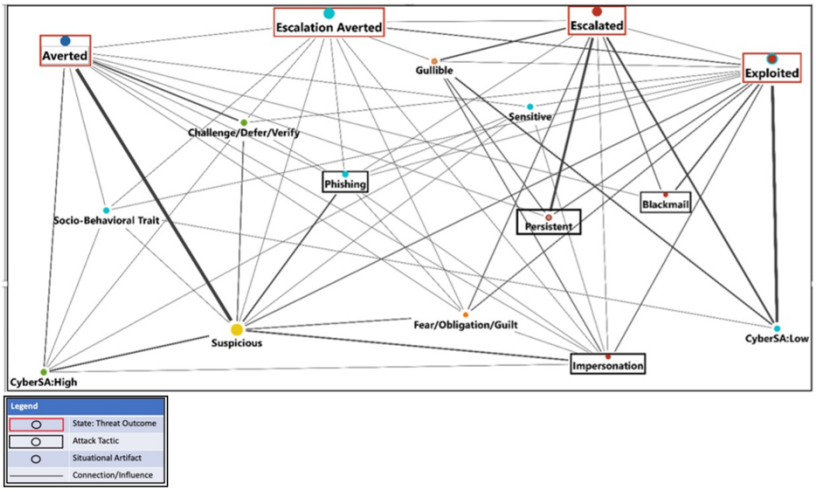

Figure 3: Revised thematic map with refined situational artifacts

Insights From the Analysis of the Research Instrument

The following is a summary of the analysis of the research instrument, decomposing each interpreted state of threat outcomes and the associated situational artifacts into tactics and situational variables that influence cyberSA.

Analysis of Patterns: Investigating patterns in situational artifacts of SE threats revealed valuable insights into tactics, strategies, and common attack patterns, vulnerabilities, and targets. Examples of insightful patterns include the timing of phishing emails, language and tone used in these emails, and target demographics and associated (sensitive and personal) information exploited in SE attacks.

Mapping of Relationships: Identifying the interconnectivity and dependencies between various factors in SE threats allowed a deeper understanding of the relationships between different situational artifacts. Examples include mapping relationships between gullibility, fear of authority, susceptibility to phishing emails, and the persistence of attackers when targeting more gullible individuals.

Analysis of Influences: Assessing the underlying factors contributing to vulnerability in SE threats helped reveal potential areas for intervention. For example, the influence of social isolation on susceptibility to impersonation scams was significant, as well as the impact of persistent attackers that exploited trust and used fear tactics.

Interplay Between the Above: The complex interplay between the *patterns analyzed, relationships mapped, and influences analyzed* led to a more comprehensive understanding of SE threats and informed the development of more effective (situational aware) countermeasures.

Table 1 is only a representative sample of tactics and socio-behavioral traits - to demonstrate the viability of the RTA process to address the research questions.

Thematic States	**Relationship to CyberSA**	**Influencers on CyberSA**	
		Tactics	**Socio-behavioral traits**
Averted	Indicates a **high level of cyberSA** and effective response to potential cyber threats.	• Phishing and email scams • Lottery and sweepstakes scams • Grandparent scams • Tech support scams • Identity theft and financial exploitation • Spear phishing, SE • Remote access scams • Fraudulent investments • Blackmail • Impersonation • Romance scams, healthcare • Medical fraud	• Fear of authority • Obligation to family members • Guilt can lead to an impulsive response • Gullibility • Delays can prevent exploitation • Sensitivity of information • Fear of authority • Verify to deter a threat • Undue trust (related to gullibility) • Assess all spurious claims
Exploited	Indicates a **potential weakness in cyberSA** and a need for improved cybersecurity measures.		
Escalated	Indicates a **need for ongoing monitoring and adaptation of cyberSA** to keep pace with evolving threats.		
Escalation Averted	Indicates **acquisition of cyberSA** that effectively responded to evolving cyber tactics, often after experiencing prior exploitation.		

Table 1: Results from the final analysis

The study's results demonstrate the complex interplay between socio-behavioral traits, SE attack tactics, and cyberSA in the elderly population. Secondary variables such as age-related cognitive decline, social isolation, trust in authority figures, and financial vulnerabilities can impact the state of cyberSA, increasing the likelihood of successful attacks.

Interpretation of the Findings

The reflexive thematic analysis enabled the researchers to deeply understand the dataset, identify meaningful themes, and uncover patterns related to cyber threats targeting older adults. This immersive method generated valuable insights for the design of practical, information-driven countermeasures.

In conclusion, this analysis effectively examined complex cyber threats, providing a nuanced understanding of situational factors, and informing targeted interventions. Future research can explore additional variables influencing older adults' susceptibility to SE attacks and test countermeasures' effectiveness, refining interventions to protect vulnerable populations. Continued qualitative research can contribute valuable insights to addressing cybercrime and its impact on older adults.

Limitations of Study

This study may be limited by the reviewed literature, emerging cyber threat themes, and the researcher's ability to extract meaningful information from the limited dataset. Incident reports were analyzed in raw form to maintain trustworthiness, with only incomplete reports filtered out. As SE attacks evolve alongside growing awareness and technology, additional literature and new threat dimensions will emerge, requiring countermeasure frameworks to adapt accordingly. Despite these limitations, the study contributes to developing situational information-driven countermeasures.

Recommendations

This feasibility study aims to create improved SE threat countermeasures using intelligent, information-driven systems inspired by AI systems trained on phenomics to devise personalized treatments in biosciences. The following recommendations aim to achieve a tailored countermeasure system based on individual situational circumstances.

Orchestrating N-of-1 Countermeasures

An N-of-1 countermeasure system must focus on personalized and dynamic security approaches, prioritizing individual needs and vulnerabilities. It requires collaboration, data-driven insights, and a multi-faceted risk mitigation approach. These systems can incorporate personalized gaming elements into threat awareness training programs to create a more engaging and realistic user experience, improving situational awareness. More elaborate systems can monitor the threat ecosystem and orchestrate a combination of strategies to mitigate threats. A notional model for monitoring and moderating cyberSA is illustrated in Figure 4.

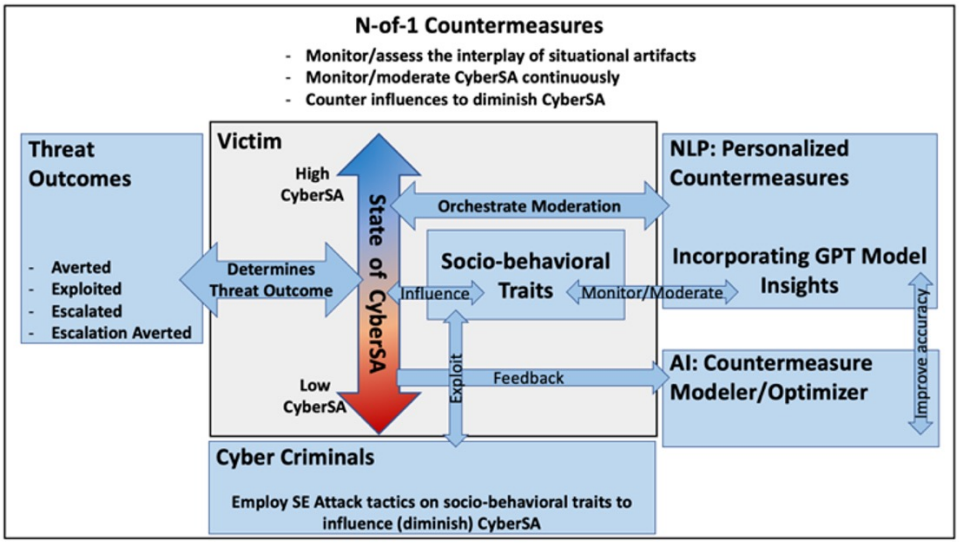

Figure 4: Orchestrating countermeasures to moderate cyberSA

Conceptual Framework for an N-of-1 Countermeasure System

A conceptual framework for an N-of-1 countermeasure system should include functional components such as data collection, data preprocessing, extraction and coding, pattern recognition and analysis, model development, and integration and deployment of application logic. The AL3RT™ framework (see Figure 5), an effort to instantiate this conceptual framework, was borne of this study, inspired by insights gleaned from the findings of the recursive thematic analysis. The *3RT* in the AL3RT framework represents the *three recursive transformers* (that are the critical workhorses for the decomposition and interplay of *patterns, relationships, and influences*) to inform the development of N-of-1 countermeasures. Recursive transformers can be trained on a large dataset of SE attacks and their associated countermeasures. Recursive transformers can learn to identify patterns and features indicative of a potential SE attack by analyzing the language and social cues used in these attacks. And based on this analysis, these transformers can generate personalized countermeasures tailored to the individual's specific vulnerabilities and risk profile. Progress on the exploration and realization of this patent-pending framework will be shared at *www.al3rt.ai*

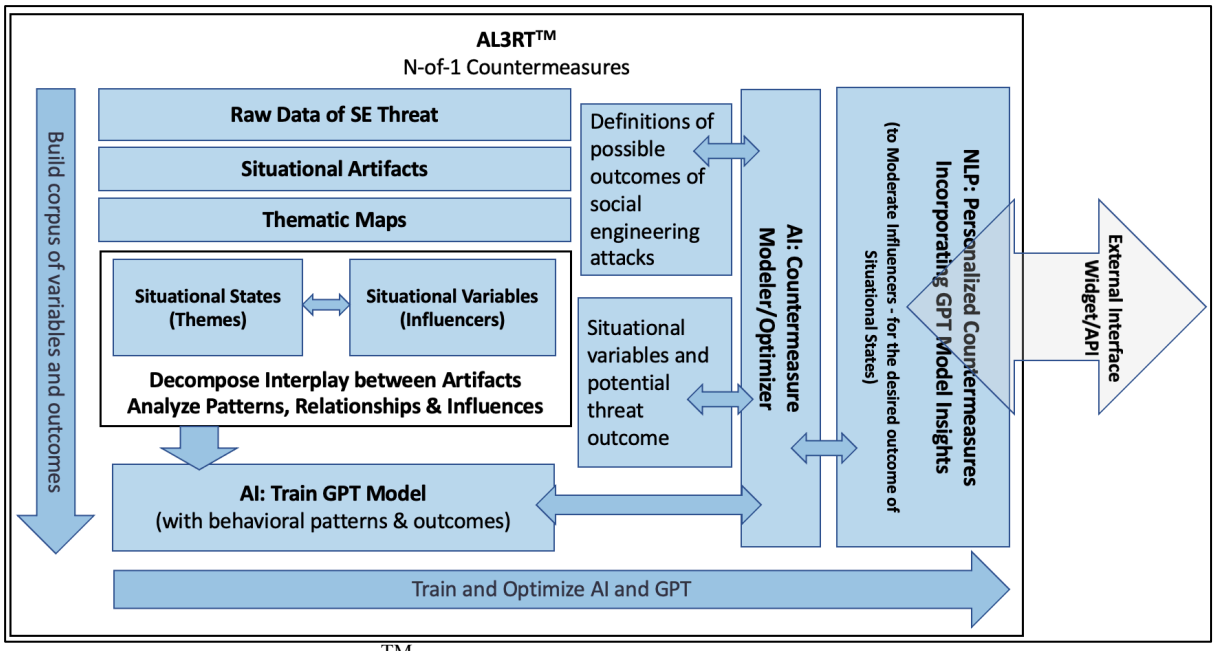

Figure 5: AL3RT™ Framework: Expanding the model from the study

Explore Cyber Phenomics as a Discipline to Enable N-of-1 Solutions

This study presents cyber phenomics as a multidisciplinary study for a data-driven approach to analyzing digital artifacts, socio-behavioral traits, and cyber interactions for insights into SE threats. An evolving corpus of cyber phenoms is essential for an AI-based, adaptive countermeasure framework. Continued research into intelligent strategies is needed to establish cyber phenomics as a discipline, enabling tailored countermeasures and fostering a resilient, inclusive digital ecosystem with user trust and confidence.

Conclusion

Older adults are increasingly vulnerable to costly, life-altering SE attacks due to age-related cognitive changes, trust in traditional communication, and continuous digital advancements. Cybercriminals will develop more sophisticated tactics as technology evolves, exploiting sensory interfaces and AI technologies. To combat this powerful threat vectors, it is essential to AI-driven “co-pilots” that monitor and enhance the cyber situational awareness of older adult cyber users with real-time alerts and guidance.

References

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, 3, 7.

Bautista-Diaz, M. L., & Agis-Juarez, R. A. (2021). The effects of COIVD-19 on the digital literacy of the elderly: Norms of digital inclusion. *Frontiers in Education*.

Duncan, D. E. (2023). The Phenomics revolution. The Science of Wellness. *Scientific American Custom Media*.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors Journal* 37(1), 32-64.

FBI. (2018). Fraud against seniors. *Federal Bureau of Investigation*.

FBI. (2023). Internet crime report 2022. *Federal Bureau of Investigations.*

Gutzwiller, R., Dykstra, J., & Payne, B. (2020). Gaps and opportunities in situational awareness for cybersecurity. *Digit. Threat.: Res. Pract. 1, 3, Article 18.*

Hardin, E., & Khan-Hudson, A. (2005). Elder abuse - "society's dilemma." *Journal of the National Medical Association*, 97, 91–94.

Martinez-Alcala, C. I., Rosales-Lagarde, A., Perez-Perez, Y. M., Lopez-Noguerola, J. S.,

Mbaziira, A. V., & Murphy, D. R. (2018). An empirical study on detecting deception and cybercrime using artificial neural networks. *Proceedings of the 2nd International Conference on Compute and Data Analysis – ICCDA.*

Puig, A. (2023). Scammers use AI to enhance their family emergency schemes. *Consumer Advice, Federal Trade Commission.*

Rößling, G., & Müller, M. (2009). Social engineering: a serious underestimated problem. *In Proceedings of the 14th annual ACM SIGCSE conference on Innovation and technology in computer science education (ITiCSE' 09). Association for Computing Machinery*, 384.

Vargis, J. M., & Schaeffer, D. M. (2022a). Cyber victimization: The subtleties of ageism. *European Conference on Aging & Gerontology (EGen2022), IAFOR*.

Vargis, J. M., & Schaeffer, D. M. (2022b). COVID-19 and digitization: Impact of escalation in cybercrimes targeting the elderly. *Chesapeake Digital Harmony Consortium 2022*.

You, K., Wang, P., & Ho, D. (2022). N-of-1 healthcare: Challenges and prospects for the future of personalized medicine. Front. Digit. Health 4:830656.

Contact email: jacob@vargis.org