Computer and Information Science; Vol. 17, No. 2; 2024
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Generative AI Increases Cybersecurity Risks for Seniors

Zahm Siyed[1]

[1] Diamond Cyber Defense, Diamond Bar, CA, United States

Correspondence: Zahm Siyed, Diamond Cyber Defense, Diamond Bar, CA, United States. Tel: 909-680-9000

Received: June 18, 2024 Accepted: July 25, 2024 Online Published: September 6, 2024

doi:10.5539/cis.v17n2p39 URL: https://doi.org/10.5539/cis.v17n2p39

Abstract

We evaluate how generative AI exacerbates the cyber risks faced by senior citizens. We assess the risk that powerful LLMs can easily be misconfigured to serve a malicious purpose, and that platforms such as HackGPT or WormGPT can facilitate low-skilled script kiddies to replicate the effectiveness of high-skilled threat actors. We surveyed 85 seniors and found that the combination of loneliness and low cyber literacy places 87% of them at high risk of being hacked. Our survey further revealed that 67% of seniors have already been exposed to potentially exploitable digital intrusions and only 22% of seniors have sufficient awareness of risks to ask techno-literate for remedial assistance. Our risk analysis suggests that existing attack vectors can be augmented with AI to create highly personalized and believable digital exploits that are extremely difficult for seniors to distinguish from legitimate interactions. Technological advances allow for the replication of familiar voices, live digital reconstruction of faces, personalized targeting, and falsification of records. Once an attack vector is identified, certain generative polymorphic capabilities allow rapid mutation and obfuscation to deliver unique payloads. Both inbound and outbound risks exist. In addition to inbound attempts by individual threat actors, seniors are vulnerable to outbound attacks through poisoned LLMs, such as Threat GPT or PoisonGPT. Generative AI can maliciously alter databases to provide incorrect information or compromised instructions to gullible seniors seeking outbound digital guidance. By analyzing the extent to which senior citizens are at risk of exploitation through new developments in AI, the paper will contribute to the development of effective strategies to safeguard this vulnerable population.

Keywords: generative AI, cybersecurity, senior citizens, digital vulnerability, social engineering

1. Introduction

1.1 New Risks with Generative AI

The rapid progression of generative AI technology is transforming numerous aspects of digital interaction. Historically, all citizens, especially seniors, have struggled with poor digital literacy, making them susceptible to cyber-attacks and digital exploitation.

Generative AI, particularly in the form of Large Language Models (LLMs) can generate text, images, voices and videos, all with increasing human-like realism. While these advancements have already delivered benefits across various sectors, they have also opened new avenues for cybercriminals. Generative AI allows low-skilled threat actors, colloquially known as “script kiddies” to deploy attacks on susceptible individuals with a lower skill threshold than previously required (Taddeo et al., 2019).

The widespread availability and actionable capacity of powerful LLMs, such as GPT-4, make them prime tools for potential misconfiguration and malicious use (Wiafe et al., 2020). Notably, these AI-driven attacks can rely on commercially available platforms to mimic the effectiveness and sophistication of highly skilled cyber attackers. For example, HackGPT, WormGPT, ThreatGPT or PoisonGPT offer frameworks for orchestrating complex cyber-attacks with lower skill requirements (Gupta et al., 2023).

Our survey involving 85 seniors revealed a combination of loneliness and insufficient cyber literacy places 87% of respondents at high risk of cyber-attacks. Further findings show that 68% of seniors have encountered potentially exploitable digital threats, while only 23% have the awareness to seek support from techno-literate family or friends.

Our risk analysis suggests that AI can augment existing attack vectors, creating highly personalized and believable digital exploits (Kumar, 2023). Such attacks are extremely difficult for seniors to distinguish from

legitimate interactions (Sasse et al., 2000). Currently, technological advances support the realistic replication of voices, live digital reconstruction of faces, personalized targeting, and the falsification of records. Inbound targeting by AI-generated intrusions is becoming increasingly sophisticated, thanks to reinforcement learning that enhances the authenticity of digital media. Generative polymorphic capabilities allow for rapid mutation and obfuscation of attacks, making them even harder to detect (Shidawa et al., 2020).

2. Benefits and Cyber Risks of Generative AI

Senior citizens have long been vulnerable to cyber risks such as phishing scams and identity theft (Velasquez, 2024). These attacks typically exploit the lack of familiarity with digital technologies and online security practices. Cybercriminals now employ advanced techniques, leveraging new AI technologies to enhance their methods (Teichmann, 2023).

While the focus of this paper is on the risks that generative AI poses, it is essential to acknowledge the potential benefits. Generative AI can enable chatbot assistants that offer immediate, personalized support, helping seniors navigate online services and manage daily tasks, especially for those with disabilities or cognitive impairments. It can support lifelong learning and offer cognitive health tools, such as adaptive learning environments and therapeutic interventions. In healthcare, it can transform service delivery through AI-driven diagnostic tools, real-time monitoring of chronic conditions, and personalized health management.

While generative AI poses cybersecurity risks, it also offers robust solutions to enhance security and detect fraud, such as machine learning algorithms that can analyze large data sets to identify patterns and anomalies indicative of fraudulent activities, protecting seniors from financial scams and identity theft. Despite these benefits, there are significant and evolving risks which we categorize into three distinctive Relative Threat Maturity levels: Low, Medium, or High, as shown in Table 1.

Table 1. Qualitative Risk Score of Generative AI Offerings

Company	Product	Output Type	Relative Threat Maturity
Open AI	ChatGPT 3	Text	Medium
	ChatGPT 4	Text	High
	ChatGPT 4o	Text, Photo	Medium
	Dall-E	Photo	Medium
	Sora	Video	Low
Google DeepMind	Gemini	Text	Medium
	AlphaCode	Code	Low
Microsoft	Copilot	Text	High
	GitHub Copilot	Code	Low
IBM	watsonx	Text, Data	Low
Anthropic	Claude	Text	High
Perplexity	Perplexity AI	Text	High
Meta	Llama 2	Text	Medium
Stability AI	Stable Diffusion 3	Video	Low
Databricks	MosaicML	Text, Data	Medium
Cohere	Generate	Text	Medium
Synthesia	Synthesia	Video	Low
Writesonic	Photosonic	Photo	Medium
	Audiosonic	Audio	Medium

3. Extrapolative Threat Ideation and Scenario Modeling

We explore capabilities of current and potential future versions of generative AI, and their potential for exploiting senior citizens. In Table 2 we present a risk analysis of ten threat scenarios.

Table 2. Cyber Risk Scenarios of Generative AI

Capability	General Benefits	Risks To Seniors	Projected Timeline
Text conversations with an LLM-enabled bot	Customer service chatbots reduce wait time for common issues and increase customer satisfaction	Automated conversational manipulation and social engineering via text	Short term. With the commercial availability of malicious GPTs, it is primed to cause harm in the short term.
Human voice is cloned, and realistic speech is generated	Informational updates are provided in a timely way especially to hearing impaired or to those preoccupied with driving or other dangerous tasks.	Synthetic voice emulation and phonetic replication	Medium term. Early attempts at voice cloning have been successful. Widespread use is possible within a half-decade in the absence of regulatory restrictions.
Videos and photos of imagined life scenarios are generated with a high degree of realism.	Creates digital entertainment and helpful real-world simulation. Valuable for offering directions, how-to manuals, self-help guides, tourist help and more.	Deepfake visual fabrication and realistic media generation	Long term. The recent launch of Sora, Dall-E, Midjourney, Stable Diffusion and others will accelerate technology adoption. Depending on resource allocation, it might take a half-decade to a decade to achieve realism.
Generate emotionally intelligent content.	Advice bots, Songs, Movies and Fiction can be created. These can enhance quality of life if generated with good intentions.	Memory jacking through enhanced interaction simulation	Medium term. There is a sufficient training data from prior human-generated successful works to make this a realistic possibility in a few years.
Generate documents and text that can be used in legal matters or documentation.	Corporations benefit by reducing the headcount needed to generate routine business and legal documents.	Financial deception and fraudulent documentation	Medium term. Seniors are particularly vulnerable to financial scams that rely on fake but realistic-looking documents.
Gather and analyze large amounts of aggregated data and create useful output.	Social profiling can be used to determine consumers and users wants and requirements in an application, creating a better user experience.	Analysis of social isolation and digital footprint profiling	Short term. Modern data aggregation systems can analyze digital profiles of online users to determine characteristic traits and exploit them.
Converse with people in specific styles of language unique to humans.	Generative text that replicates human interaction can combat loneliness in seniors and provide helpful information.	Enhanced romance scams	Medium term. Generative AI can produce human-like text responses but is not capable yet of creating completely believable romantic language.
Generate documents and synthesize information.	Document synthesizing can be used to reduce corporate load and automate documentation and authorization processes.	Medical fraud through enhanced identity fabrication	Short term. Automated generation of legal and medical documents will rapidly become more sophisticated.
Synthesize data and use human language to display urgency.	Human language manipulation can create urgency and importance in digital communications that can connect and convince people to do important tasks.	Virtual tech support exploitation using synthetic agents	Medium Term. Tech support can be generated and can potentially help but also has the potential to be maliciously altered to exploit.
Aggregate and synthesize data to advocate and promote a cause.	Digital collection of information can be converted into the synthesizing of marketing campaigns that can promote helpful causes and benefit advocates.	Manipulative misinformation campaigns via generated content	Short Term. Data collection systems can traverse social media platforms and discussion boards to create politically motivated opinions and create influential digital marketing.

3.1 Automated Social Engineering via Text

Automated texting involves the use of machine learning-powered chatbots that engage seniors in convincing conversations to gather personal information or persuade them to click on malicious links. The messages are crafted using data mining techniques, pulling information from the senior's social media profiles and online behavior (Liang & Xue, 2010). Personalization enhances the likelihood of successful deception (Sidoti & Vogels, 2023).

3.2 Synthetic Voice Emulation and Phonetic Replication

Through digital reconnaissance, threat actors can scrape voice recordings that are then processed for noise reduction, normalization, and segmentation of the audio clips to isolate the target’s voice (Mohamed Firdhous et

al., 2023). Using advanced models like WaveNet or Tacotron, the cleaned audio data is fed into the model to train it on the target's voice characteristics, including tone, pitch, and speaking style to facilitate attack scenarios. The attack begins with the perpetrator using social engineering to understand the family dynamics and identify emotional triggers. Using a spoofed caller ID to enhance credibility, the attacker places a call to the senior, fabricating a scenario such as a medical emergency or financial crisis to prompt the senior to transfer money or share sensitive information.

3.3 Deepfake Visual Fabrication and Realistic Media Generation

Deepfake technology can manipulate videos of known individuals to deliver fraudulent messages, further complicating the detection of scams. Generative Adversarial Networks (GANs), which can produce realistic images and videos that appear authentic. These deepfakes can be used in various fraudulent scenarios to deceive seniors. For instance, attackers can generate videos of trusted individuals, such as family members or friends, asking for personal information or financial help (Anderson & Perrin, 2024). The visual and auditory authenticity of these deepfakes is debatable today but will increase markedly in the decade ahead, making it extremely challenging for seniors to detect the scam. Additionally, forged documents that look legitimate, such as medical records or financial statements, can be created using similar technologies.

3.4 Memory Jacking Through Enhanced Interaction Simulation

Memory jacking involves using machine learning to recreate interactions with old friends or fabricate past events to exploit a senior's nostalgia and gain their trust and request personal details or financial assistance (Huey, 2021). Similarly, fabricating past events or shared experiences can make the senior more likely to believe the legitimacy of the interaction. Additionally, attackers can create fake contracts or agreements that appear to have been signed in the past, convincing the senior of their authenticity, and inducing financial commitments.

3.5 Financial Deception and Fraudulent Documentation

AI-generated documentation can be used to create fraudulent investment opportunities by appealing to the senior's emotions and personal circumstances (Sultan, 2019). They then generate fake investment offers that include detailed descriptions, projected returns, and testimonials. The attacker creates realistic-looking bank documents, such as account statements or transaction records, using machine learning technologies. The high level of detail and authenticity in these synthetic documents makes it difficult for seniors to recognize the fraud, leading to significant financial losses.

3.6 Analysis of Social Isolation and Digital Footprint Profiling

Advanced algorithms can analyze social media activity and other digital footprints to profile and target socially isolated seniors. The inadequate state of privacy controls on the digital life of seniors makes such profiling possible. Based on this analysis, attackers can map out the senior's social connections to identify and exploit weak points, such as distant family members or infrequent contacts. This information is used to tailor attacks that exploit specific vulnerabilities, making the scams more effective (Fenge & Lee, 2018).

3.7 Enhanced Romance Scams

Machine learning can analyze a senior's personality traits and preferences to craft highly convincing romance scams. Attackers start by mining data from the senior's social media profiles, dating sites, and other online interactions, and generate personalized messages that appeal to the senior's emotions and create a sense of connection (Kwok & Koh, 2020). The model can adapt the conversation based on the senior's responses, continuously adjusting the scam approach to maintain the senior's interest and trust. In aggregate, romance scams claimed $139 million from adults aged 60 and older in 2020, up from $84 million the year before (Munanga, 2019).

3.8 Medical Fraud Through Enhanced Identity Fabrication

Generated voices or images of medical professionals can manipulate seniors into sharing sensitive health information or making payments for fraudulent treatments. The attacker may request payments for treatments, medical equipment, or consultations, leveraging the perceived authority and trust associated with healthcare providers. The realism and adaptability of the generated voice make it difficult for the senior to recognize the scam (Ansari et al., 2022).

3.9 Virtual Tech Support Exploitation Using Synthetic Agents

Using generated voices or chatbots, the scammer contacts the senior, posing as a representative from a well-known tech company (Zeadally et al., 2020). The virtual tech support agent informs the senior of a supposed problem with

their device or software, offering to fix the issue remotely. The agent guides the senior through downloading remote access software, allowing the attacker to take control of the senior's computer. Once access is gained, the attacker can steal personal information, install malware, or demand payment for fake services.

3.10 Manipulative Misinformation Campaigns via Generated Content

Advanced algorithms can generate and disseminate fake news or misinformation specifically targeted at seniors. The attacker uses machine learning to analyze the senior's online behavior which is then exploited to create personalized fake news stories. These generated stories are disseminated through social media, email, or other digital platforms, appearing to come from credible sources. The realistic and targeted nature of machine learning-generated fake news makes it a potent tool for cybercriminals (Blackwood-Brown et al., 2019).

4. Survey Findings Show Seniors Face High Cybersecurity Risks

To understand the specific vulnerabilities of seniors, we conducted a survey involving 85 participants aged 65 and above. The seniors were accessed through community centers and retirement homes in the Greater Los Angeles area over the course of several months spanning 2023 and 2024. To conduct the survey, we approached 143 senior citizens of which 85 agreed to participate in the survey upon assurance their responses would be kept confidential. The survey was administered orally in-person and responses were recorded by this author. All senior response information has been kept anonymous to preserve safety as digital vulnerabilities were identified in surveyees. The survey aimed to assess their level of digital literacy, exposure to cyber threats and awareness of cybersecurity risks in the context of generative AI. The findings were alarming: 95% of the respondents were identified as being at high risk of cyber-attacks due to a combination of loneliness and low cyber literacy. Additionally, 78% reported having been exposed to potential digital intrusions, such as phishing attempts or unauthorized access to their accounts. While the survey provides valuable insights, it is important to note that the sample size is limited to 85 participants from the Southern California region. Consequently, the findings should not be generalized to other regions or countries without further research. Expanding the survey to include a more diverse and larger sample would enhance the robustness of the conclusions.

4.1 Awareness of AI Capabilities and Associated Risks

The survey revealed that a vast majority of seniors are unaware of the advanced capabilities of AI and the associated risks. Many respondents lack an understanding of how AI can be used in social engineering, phishing, and other attacks. The survey findings indicate in Table 3 a substantial lack of awareness of AI capabilities among seniors. Only four seniors (4%) are aware of AI's capabilities and its potential risks, while a significant majority, 81 seniors (95%), remain unaware. This lack of awareness can lead to increased vulnerability to AI-driven scams and cyber threats. The data highlights the critical need for targeted educational initiatives to enhance seniors' understanding of AI technologies and their implications for cybersecurity.

Table 3. Awareness of AI Capabilities

Condition	Count
Aware of capabilities	4
Unaware of capabilities	81

4.2 Digital Identity Management and Protection Mechanisms

The survey highlighted a troubling gap in seniors' identity management practices. A large number of respondents lack adequate protection measures, such as two-factor authentication (2FA), secure login methods, and proper privacy settings on social media. This deficiency makes them highly susceptible to identity theft. The survey findings in Fig. 1 on digital footprint awareness indicate a substantial gap in the seniors' understanding and management of their digital presence. Out of the 85 seniors surveyed, 64 (75%) are aware of the extent of their digital footprint regarding their names, while 21 (24%) remain unaware. This awareness drastically drops when considering other personal information. Only 34 seniors (40%) are aware of the digital footprint associated with their age, leaving a significant 51 (60%) unaware. Similarly, 62 seniors (72%) are aware of their contact information being part of their digital footprint, while 23 (27%) are unaware.

The awareness further diminishes concerning pictures and family information. Only 31 seniors (36%) are aware of the digital footprint of their pictures, with 54 (63%) unaware, and an alarming 8 seniors (9%) are aware of the digital footprint related to family information, leaving 77 (90%) unaware. Regarding education, 46 seniors (54.1%) are aware of its digital footprint, while 38 (45%) are not. Awareness about current address information is strikingly low, with only 13 seniors (15%) aware and 72 (84%) unaware. Furthermore, previous addresses' digital footprint awareness is also minimal, with just 9 seniors (10%) aware, while 76 (89%) are unaware.

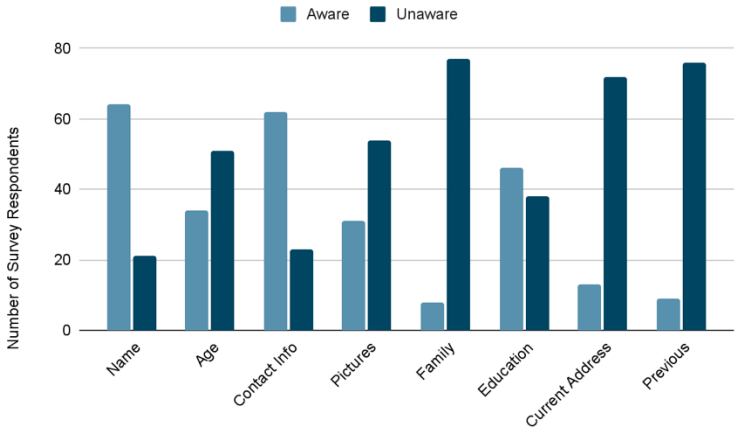

Figure 1. Digital Footprint Awareness

4.3 Recognition and Response to Phishing and Unsolicited Messages

Our survey revealed that a significant number of seniors frequently respond to unsolicited messages without verifying the sender's identity. The survey data in Table 4 shows 38 (44%) reported opening unsolicited messages, which significantly increases their risk of falling victim to phishing schemes. Furthermore, 19 seniors (22%) respond to these messages, which can lead to the disclosure of sensitive information or financial losses.

In contrast, 24 seniors (28%) ignore unsolicited messages and only 4 (4%) go further to ignore and block the sender, which is a more secure practice. This data underscores the importance of educating seniors on the risks associated with unsolicited messages and the importance of not engaging with unknown or suspicious contacts. Implementing strong spam filters and promoting awareness about phishing tactics can significantly reduce the risk of seniors being exploited through unsolicited communications.

Table 4. Response to Unsolicited Messages

Senior's action	Count
Respond to message	24
Open message	4
Ignore message	38
Ignore and block sender	19

4.4 Contact Verification and Authentication Practices

There is a critical gap in seniors' practices regarding the verification of contact information before sharing sensitive data or engaging in transactions. This failure to properly authenticate contacts can lead to impersonation scams, where attackers pose as trusted individuals or institutions to extract sensitive information or funds. The survey findings in Table 5 on how seniors verify contact information reveal both strengths and weaknesses in their security practices. Impressively, all 85 seniors (100%) verified the account names, indicating a strong initial layer of security awareness. However, this diligence diminishes significantly when it comes to verifying other details. Only 71 seniors (83%) verify account details, while 14 (16%) do not. The verification of mutual contacts is even lower, with only 12 seniors (14%) taking this step, leaving 73 (87%) potentially exposed to social engineering attacks that leverage known associates' identities. Verification through in-person contact is the least utilized method, with just 4 seniors (4%) employing this practice, compared to 81 (95%) who do not.

Table 5. Verifying Contact Information

Account details	Verifies details	No verification
Account name	85	0
Details	71	14
Mutual contacts	12	73
In-Person contact	4	81

4.5 Digital Handling of Medical Information and Associated Security Risks

Our survey data indicates that many seniors do not use secure methods for storing and sharing their digital medical information. The storage and transmission of Personally Identifiable Information (PII) in digital medical records among seniors are critical points of vulnerability. Our survey shows in Fig. 2 that 14 seniors (16%) have

no digital medical information, thus mitigating any related risks. However, 18 seniors (21%) store their medical information locally with network access, and nine seniors (10%) store it locally without network access, both practices presenting varying degrees of risk depending on the security of their local storage systems. Thirty-two seniors (37%) store their medical information in the cloud, which, while convenient, requires robust security measures to prevent unauthorized access. The majority, 38 seniors (44%), frequently transport their medical information digitally, and 25 seniors (29%) do so infrequently, both practices increasing the risk of interception and unauthorized access during transmission.

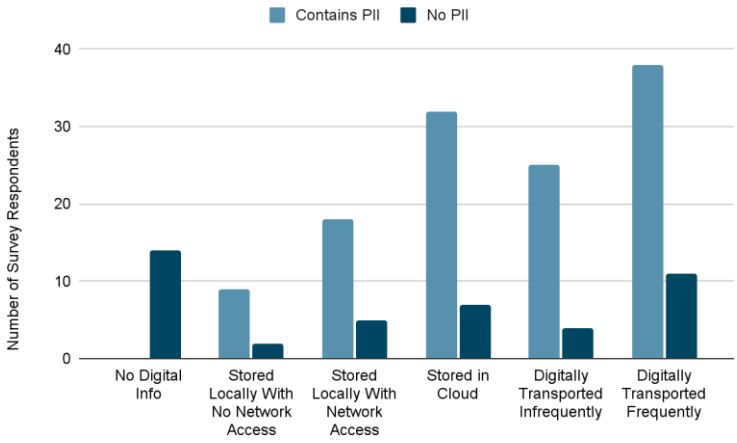

Figure 2. PII in Medical Information

4.6 Detection and Awareness of AI-Generated Chats

The survey revealed that many seniors struggle to detect AI-generated chats, leaving them vulnerable to social engineering and automated scam attempts. AI-generated chats can be highly convincing, leveraging natural language processing to mimic human conversation and extract sensitive information. The survey data shows that many seniors are not familiar with the characteristics of AI-generated text, such as repetitive patterns, lack of context awareness, and unusual phrasing.

The survey data in Fig. 3 indicates that 55 out of 85 seniors (64%) can detect AI-generated chats, which suggests a moderate level of awareness and capability to identify potentially malicious communications. However, 30 seniors (35%) cannot detect these generated chats, indicating a significant gap that could be exploited by cybercriminals using sophisticated AI-driven social engineering tactics.

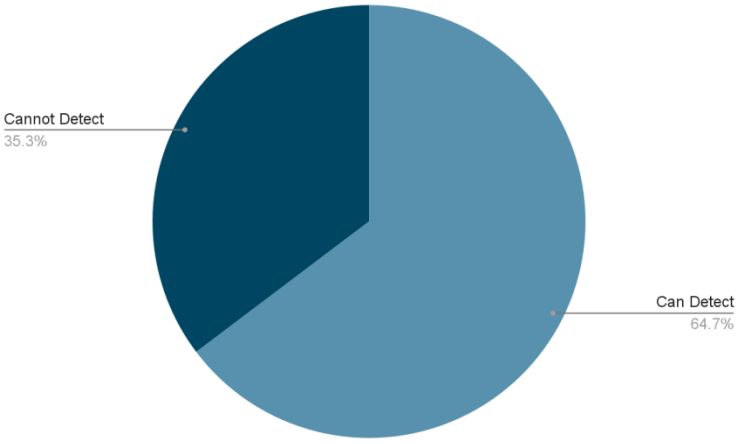

Figure 3. Generated Chat Detection

4.7 Detection and Awareness of AI-Generated Voices

Our survey data shows that a significant number of seniors struggle to detect AI-generated voices, making them susceptible to voice-based social engineering attacks. AI-generated voices can mimic family members, friends, or

trusted authorities, making fraudulent requests for sensitive information or financial help highly convincing. The ability to detect AI-generated voices is a critical skill for seniors to prevent falling victim to voice-based scams. The survey data in Fig. 4 indicates that four seniors (4%) could accurately detect AI-generated voices, highlighting a significant gap in this skill. Fifty-two seniors (61%) could identify obvious AI-generated voices, while 36 seniors (42%) detected moderately realistic AI voices. Only seven seniors (8%) were able to identify highly realistic AI-generated voices. This data suggests that most seniors are vulnerable to sophisticated AI voice scams, emphasizing the need for targeted training to improve their detection capabilities.

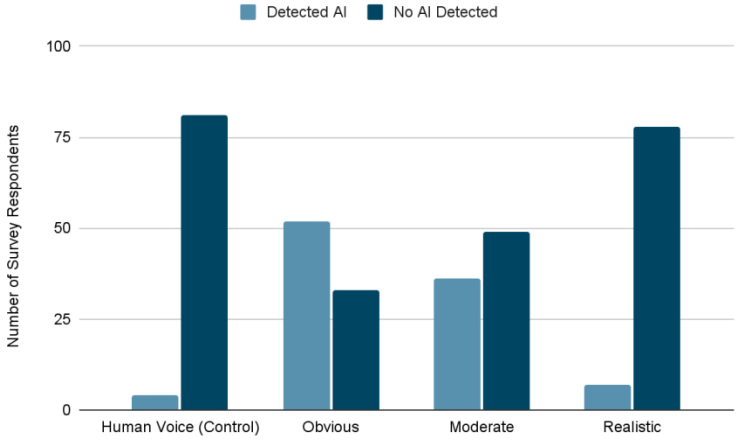

Figure 4. Generated Voice Detection

4.8 Detection and Awareness of AI-Generated Images

The survey findings indicate that many seniors are unable to distinguish between real and AI-generated images, leaving them vulnerable to image-based scams. AI-generated images can be used to create fake profiles, manipulate photographs, or fabricate documents, making fraudulent activities appear legitimate. Detecting AI-generated images is another crucial skill for preventing visual-based deception. The survey reveals in Fig. 5 that three seniors (3%) could accurately identify AI-generated images. Seventy-two seniors (84%) could detect obvious AI images, while 55 seniors (64%) could identify moderately realistic AI images. However, only 33 seniors (38%) could recognize highly realistic AI-generated images. These findings indicate a significant vulnerability to visual deception among seniors, necessitating enhanced training and awareness programs to improve their detection skills.

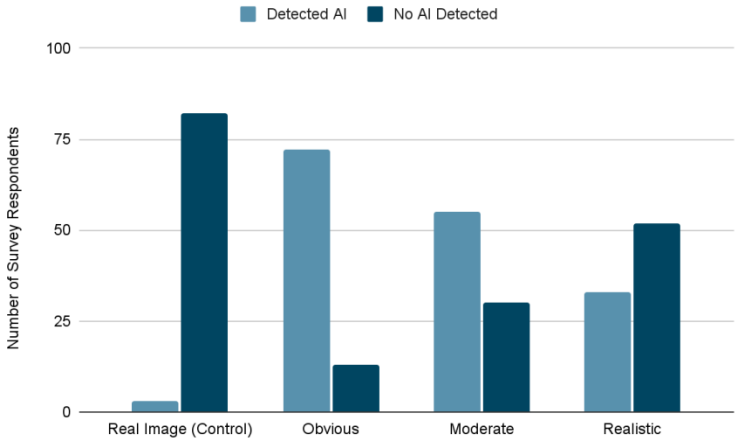

Figure 5. Generated Image Detection

4.9 Exposure to Scams in Digital Dating

The survey revealed that many seniors involved in digital dating are highly susceptible to romance scams. A significant number of respondents reported experiences with online dating platforms where they encountered requests for money, inconsistent stories, and reluctance to meet in person. Digital relationships among seniors

present unique cybersecurity challenges. Our survey indicates in Fig. 6 that 42 seniors (49%) are not engaged in any digital relationships, reducing their exposure to online relationship scams. However, 22 seniors (25%) are open to digital relationships, and 15 seniors (17%) are actively searching for them, with six seniors (7%) already in a digital relationship. These figures suggest that a significant number of seniors are potentially vulnerable to romance scams and other forms of digital exploitation.

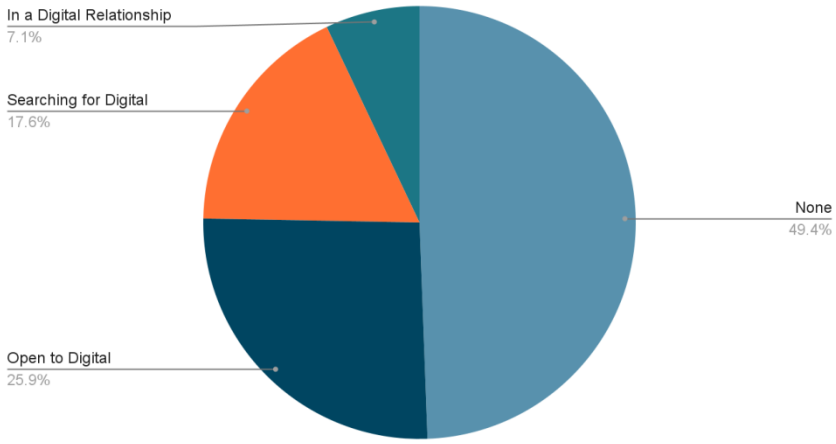

Figure 6. Digital Relationships

4.10 Intergenerational Digital Guidance and Support Networks

The survey revealed that seniors often lack access to regular guidance from younger, more tech-savvy individuals, which leaves them vulnerable to cyber threats. The survey findings in Fig. 7 on youth guidance and support reveal that many seniors lack access to assistance with digital technologies. Forty-five seniors (52%) reported having no access to youth guidance, which could significantly impact their ability to navigate and secure their digital environments. Thirteen seniors (15%) have access to such support, which can provide a valuable resource for learning and troubleshooting digital issues. Partially available guidance is reported by four seniors (4%), while seven seniors (8%) indicate that they receive no help despite having potential access to youth support. This data underscores the importance of intergenerational support systems in enhancing seniors' digital literacy and cybersecurity awareness

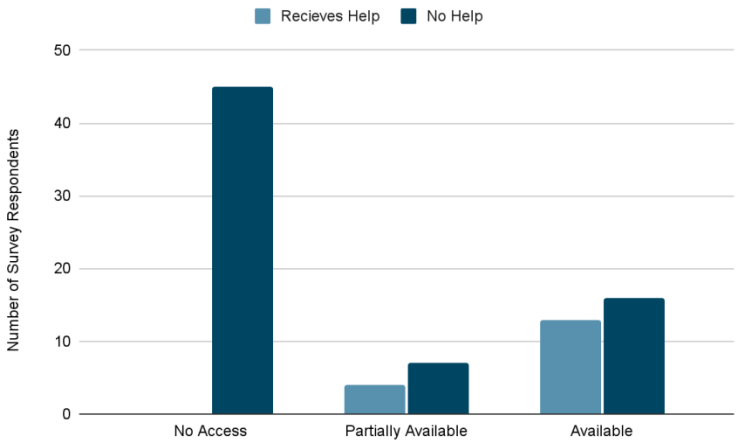

Figure 7. Youth Guidance

5. Risk Analysis

The integration of generative AI in cybersecurity presents significant challenges and risks, especially for senior citizens. These risks are multi-faceted, encompassing highly personalized phishing attacks, polymorphic and adaptive malware, and advanced social engineering tactics (Smuha, 2019). Generative AI can enhance the sophistication and effectiveness of cyber-attacks, making them more difficult to detect and counter. This section provides an in-depth analysis of these risks, exploring how AI-driven threats exploit vulnerabilities unique to

seniors and proposing advanced mitigation strategies (Nicholson et al., 2021).

5.1 Personalization and Believability of Attacks

Generative AI models enable attackers to craft highly personalized and believable phishing emails, voice calls, and deepfake videos. Attackers gather personal data through data breaches, social media scraping, and other forms of OSINT (Open Source Intelligence) to create comprehensive profiles of their targets. This level of personalization significantly increases the success rate of phishing attacks, as victims are more likely to trust and respond to messages that appear genuine. To counteract these sophisticated attacks, seniors need context-aware software tools capable of detecting anomalies in communication patterns. These tools can analyze both the content and context of messages, identifying subtle deviations from normal interactions. Such systems can utilize machine learning to adapt to new attack vectors, continuously improving their detection capabilities. To effectively deploy context-aware software tools, organizations should first conduct a comprehensive assessment of their existing IT infrastructure and identify critical points where context-aware solutions can be integrated. For instance, implementing real-time monitoring tools that adapt to user behavior and provide alerts for any deviations can significantly enhance security.

5.2 Polymorphic and Adaptive Threats

Polymorphic malware, which changes its code with each infection to evade detection, poses a significant challenge to traditional signature-based detection methods. Generative AI enhances this capability by using reinforcement learning to dynamically evolve and adapt the malware based on the defensive measures it encounters. For example, an AI-driven polymorphic malware can alter its encryption algorithms, communication protocols, and payloads in real-time to avoid detection by static and heuristic analysis tools. This adaptability makes it critical for cybersecurity defenses to also evolve continuously.

To combat these threats, AI-powered threat detection systems should be utilized. These systems can recognize patterns of polymorphic behavior rather than relying solely on static signatures. Machine learning algorithms can analyze vast amounts of data to identify subtle changes in malware behavior, enabling proactive defenses. Additionally, threat intelligence sharing among organizations can enhance collective security. By sharing information on the latest polymorphic malware trends and defense strategies, organizations can stay updated and better prepared to counter evolving threats. The deployment of AI-powered threat detection systems involves several key steps: selecting the right algorithms, training models on diverse datasets to improve accuracy, and continuously updating the models with new threat intelligence. Additionally, integrating these systems with existing security information and event management (SIEM) platforms can provide a comprehensive defense mechanism.

5.3 Advanced Social Engineering Tactics

The integration of AI in social engineering tactics has revolutionized the threat landscape. Attackers can now employ sophisticated AI models to conduct deepfake video and audio attacks, impersonating trusted individuals with high accuracy. These AI-generated deepfakes can be used to manipulate victims into divulging sensitive information or performing actions that compromise security. For example, an attacker could create a deepfake video of a company executive instructing an employee to transfer funds to a fraudulent account.

Mitigation strategies for these advanced social engineering attacks include implementing multi-factor authentication (MFA) and zero-trust principles within organizations. MFA ensures that even if an attacker successfully deceives a victim into providing credentials, additional authentication layers are required to gain access. Zero-trust principles enforce strict access controls and continuous verification, reducing the risk of unauthorized access.

The advanced deception techniques used in these attacks, such deepfake videos, can instill profound fear and anxiety, as victims grapple with feelings of insecurity and betrayal. The financial and personal repercussions often lead to stress and depression, exacerbating pre-existing mental health issues or creating new ones. Victims may withdraw from interactions due to embarrassment or fear of further attacks. The lose of trust in others, including family and institutions, further compounds the emotional distress experienced.

6. Conclusion

Our survey revealed a stark reality: a combination of loneliness and low cyber literacy places a large majority of seniors at high risk of cyber-attacks. As demonstrated, tools like HackGPT and WormGPT have lowered the barrier to entry for low-skilled threat actors.

To mitigate these risks, it is essential to implement comprehensive educational programs that enhance digital

literacy among seniors (Holgersson et al., 2021). These programs should focus on teaching seniors how to recognize and respond to phishing attempts, secure their personal information, and use cybersecurity tools effectively. Intergenerational training programs, where younger family members or volunteers teach seniors about digital security, can bridge the knowledge gap and foster a safer digital environment. Tailored cybersecurity tools designed for ease of use and minimal user intervention are also crucial. These tools should include features such as real-time monitoring for suspicious activity, simplified interfaces, and automated alerts for potential threats.

Policymakers have a significant role to play in protecting seniors from AI-enabled cyber threats (Crossler et al., 2013). Regulations should mandate robust security measures for services frequently used by seniors (Kaur et al., 2023). Enhanced penalties for cybercrimes targeting seniors can act as a deterrent, making it less appealing for cybercriminals to target this vulnerable population.

Community-based programs are equally important. Establishing support hotlines staffed by cybersecurity experts can provide immediate assistance and advice to seniors facing potential threats. Peer support networks, where seniors can share experiences and tips, can foster a sense of community and collective security. Public awareness campaigns can educate the broader community about the risks of cyber threats and the importance of cybersecurity practices, thereby contributing to a safer digital environment for everyone.

Future research should focus on developing advanced detection and prevention tools that can adapt to the evolving threat landscape (Jayabalaji et al., 2022). Additionally, further studies are needed to understand the psychological impacts of attacks on seniors, informing the development of comprehensive support systems that address not only the technical but also the human aspects of cybersecurity.

By enhancing digital literacy, developing tailored cybersecurity tools, and implementing comprehensive policy frameworks, we can protect senior citizens from the evolving landscape of AI-enabled cyber threats. This paper has laid the groundwork for these efforts, underscoring the critical importance of safeguarding our most vulnerable population in the age of generative AI.

Acknowledgments

We thank the senior citizens who participated in our survey process for their valuable time in answering the many questions that shed light on the issues involved in general cybersecurity risks and their familiarity, or lack thereof, with novel artificial intelligence technologies. We also thank them for introducing us to their social network to expand the study to additional participants.

Authors' contributions

This paper has a single author, Zahm Siyed, who was responsible for study design, data collection, drafting the manuscript, and revising. He has read and approved the final manuscript.

Funding

The authors received no specific funding for this study.

Competing interests

The author declares that they have no conflicts of interest to report regarding the present study.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

References

Anderson, M., & Perrin, A. (2024). *Technology use among seniors.* Pew Research Center.

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. *International Journal of Advanced Research in Computer and Communication Engineering, 11*(9). https://doi.org/10.17148/IJARCCE.2022.11912

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2019). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems, 61*(3), 195-206. https://doi.org/10.1080/08874417.2019.1579076

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Fenge, L. A., & Lee, S. (2018). Understanding the risks of financial scams as part of elder abuse prevention. *British Journal of Social Work, 48*(4), 906-923. https://doi.org/10.1093/bjsw/bcy037

Gupta, M. et al. (2023). From ChatGPT to ThreatGPT: *Impact of generative AI in cybersecurity and privacy. IEEE Access.* https://doi.org/10.1109/ACCESS.2023.3300381

Holgersson, J., Kävrestad, J., & Nohlberg, M. (2021). *Cybersecurity and digital exclusion of seniors: What do they fear?* In Proceedings of the Human Aspects of Information Security and Assurance, 12–21. https://doi.org/10.1007/978-3-030-81111-2_2

Huey, L. (2021). *What do we know about senior citizens as cybervictims? A rapid evidence synthesis.* Sociology Publications, Western University. https://doi.org/10.21428/cb6ab371.e6b80803

Jayabalaji, K., Harini, R., & Vengadesh, S. (2022). Artificial intelligence in the field of cybersecurity. *International Journal for Research in Applied Science and Engineering Technology, 10*(10), 1243-1246. https://doi.org/10.22214/ijraset.2022.47155

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kumar, N. (2023). Artificial intelligence and cybersecurity: A comprehensive review of recent developments. *International Journal of Innovative Science and Research Technology, 8.*

Kwok, A. O. J., & Koh, S. G. M. (2020). Deepfake: A social construction of technology perspective. *Current Issues in Tourism, 24*(13), 1798-1802. https://doi.org/10.1080/13683500.2020.1738357

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7). https://doi.org/10.17705/1jais.00232

Mohamed Firdhous, M. F., Elbreiki, W., Abdullahi, I., Sudantha, B. H., & Budiarto, R. (2023). *WormGPT: A large language model chatbot for criminals.* In Proceedings of the 24th International Arab Conference on Information Technology. https://doi.org/10.1109/ACIT58888.2023.10453752

Munanga, A. (2019). Cybercrime: A new and growing problem for older adults. *Journal of Gerontological Nursing, 45*(2), 3-5. https://doi.org/10.3928/00989134-20190111-01

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). *Training and embedding cybersecurity guardians in older communities.* Proceedings of the Association for Computing Machinery, Article 86, 1–15. https://doi.org/10.1145/3411764.3445078

Sasse, M. A., Brostoff, S., & Weirich, D. (2000). Transforming the 'weakest link' — A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131. https://doi.org/10.1023/A:1011902718709

Shidawa, A. B., Job, G. K., & Aaron, A. (2020). Survey on the applications of artificial intelligence in cybersecurity. *International Journal of Scientific & Technology Research, 9*(10).

Sidoti, O., & Vogels, E. A. (2023). *What Americans know about AI, cybersecurity and big tech*. Pew Research Center.

Smuha, N. (2019). From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. *Law, Innovation and Technology, 13*(1). https://doi.org/10.2139/ssrn.3501410

Sultan, A. (2019). *Improving cybersecurity awareness in underserved populations.* Center for Long-Term Cybersecurity, University of California, Berkeley.

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1*(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

Teichmann, F. (2023). Ransomware attacks in the context of generative artificial intelligence – An experimental study. *International Cybersecurity Law Review, 4*, 399-414. https://doi.org/10.1365/s43439-023-00094-x

Velasquez, E. (2024). *Annual data breach report*. Identity Theft Resource Center.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. *IEEE Access, 8*, 146598-146612. https://doi.org/10.1109/ACCESS.2020.3013145

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access, 8*, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045