

# Intergenerational Support for Deepfake Scams Targeting Older Adults

Karina LaRubbio  
*Brown University*

Alyssa Lanter  
*Brown University*

Seihyun Lee  
*Tenafly High School*

Mahima Ramesh  
*Acton-Boxborough Regional High School*

Diana Freed  
*Brown University*

## Abstract

AI-enhanced scams now employ deepfake technology to produce convincing audio and visual impersonations of trusted family members, often grandchildren, in real time. These attacks fabricate urgent scenarios, such as legal or medical emergencies, to socially engineer older adults into transferring money. The realism of these AI-generated impersonations undermines traditional cues used to detect fraud, making them a powerful tool for financial exploitation. In this study, we explore older adults' perceptions of these emerging threats and their responses, with a particular focus on the role of youth, who may also be impacted by having their identities exploited, in supporting older family members' online safety. We conducted focus groups with 37 older adults (ages 65+) to examine their understanding of deepfake impersonation scams and the value of intergenerational technology support. Findings suggest that older adults frequently rely on trusted relationships to detect scams and develop protective practices. Based on this, we identify opportunities to engage youth as active partners in enhancing resilience across generations.

## 1 Introduction

In the United States, older adults lost an estimated \$61.5 billion to fraud in 2023 [8]. Advances in technology have given rise to more sophisticated scams. In the "grandparent scam," attackers impersonate trusted family members in need of urgent financial support, sometimes using AI-generated deepfakes, such as audio or visual content [15]. These scams have recently prompted media coverage [3, 13, 14] and multiple consumer alerts [1, 2], emphasizing their rising prevalence.

Deepfake impersonation scams deviate from the threat models for other scams because they create a situation of

**dual victimization**<sup>1</sup>: in a successful attack, the older adult being targeted experiences a monetary loss, and the family member being impersonated unknowingly has their likeness used to cause harm. Older adults are not inherently more vulnerable to scams than other demographics [9], though they are specifically targeted in this context. Intergenerational support strategies are especially relevant in this context, where two parties are victimized, older adults and youth. Prior work emphasizes the importance of community support such as peers in mitigating scams against older adults [7, 11], sometimes identifying younger family members as crucial sources of support [5, 10, 12].

This research aims to understand older adults' perceptions of deepfake impersonation scams, specifically focusing on the role of youth supporters, such as grandchildren. We address the research questions: 1) How do older adults currently perceive and protect themselves against deepfake impersonation scams? 2) What opportunities exist to engage youth to support older adults against deepfake impersonation scams?

Through focus groups with older adults, we offer insights into how older adults perceive and respond to deepfake impersonation scams, contributing a greater understanding of their reliance on interpersonal networks for scam detection and response. We additionally contribute a dual victimization framework for deepfake impersonation scams, centering youth as both affected parties and potential allies. Finally, we identify actionable opportunities to foster intergenerational digital resilience, including youth-driven support strategies. Motivated by participant perspectives, these approaches seek to address the evolving threat of AI-enabled scams.

## 2 Methods

We conducted six focus groups with older adults ( $n = 37$ ) aged 70 to 94 years in an independent living facility in the

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

*USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.*  
August 10–12, 2025, Seattle, WA, United States.

<sup>1</sup>We recognize there are different terms used to refer to people experiencing the negative impacts of online safety threats, such as "survivor". We use the term "victim" to align with the criminal nature of these offenses and participant preferences.

northeast United States between February and March 2025. The focus groups lasted approximately 60 minutes and ranged in size from six to ten participants. Participants received \$10 as compensation. Discussion guides included questions on perceptions of AI technology, online safety, and deepfake impersonation scams specifically. Each focus group was audio recorded with participants' consent and transcribed for qualitative analysis. This study was approved by our IRB.

### 3 Results

After discussing what deepfake impersonation scams are and how they work, our participants expressed broad familiarity with these threats. However, some were skeptical about the fidelity of deepfake voices, expressing that they "couldn't believe [they] would fall for such a thing" (P22). Others, and especially those who had experienced financial scams in the past, expressed fear about being scammed again. About distinguishing real callers from attackers, one participant stated:

*"You really can't tell... I just think I'm going to hit the wrong button at some time, and it's not going to be good. So I'm really nervous about that." (P12)*

Many expressed that their concerns were heightened by AI technology's ability to generate synthetic content, causing them to "second guess things" (P3). In response to the threats our participants perceived from possible deepfake impersonation scams, many described collaborating with younger family members to access support and build intergenerational protective practices in the following ways:

**Avoidance.** For many of our participants, their younger family members advised them to avoid real-time interactions with unknown parties altogether. One participant shared:

*"My grandson's advice that I've used constantly is: if it's that important, they'll leave a message." (P7)*

While this strategy did support their resilience against scams, our participants expressed that ignoring unknown callers completely led them to miss important information, such as time-sensitive medical notifications.

**Contact for verification.** Many participants expressed that they already relied on making direct contact with trusted family members to ensure that information they received from a suspicious source was reliable, and would continue this practice should they encounter a deepfake impersonation scam. One participant suggested:

*"I'd ask the caller, who else in our family knows about this and then ... call them myself." (P32)*

However, some expressed that this would be ineffective if they could not immediately contact their family members.

**Shared knowledge.** Many participants expressed that they had already collaborated with family members to create code

words that only family members knew, which could be used in situations of uncertainty. Others suggested asking a question that only family members would know the answer to in order to verify the caller's identity. One participant recounted their strategy for avoiding a recent impersonation scam attempt they had experienced:

*"I said, what's your name? He said, grandma, you don't know my name? I said, well I have three grandsons, so which one are you? And then he hung up. Just ask a family question that they won't know." (P27)*

Participants thought that using shared knowledge was a strong protective practice. However, this requires them to recognize that a call is suspicious, which may become increasingly challenging with advances in deepfake technology.

### 4 Discussion

The protective practices our participants suggested for deepfake impersonation scams all relied on support from younger family members to some extent. Advice from family members to avoid contact with attackers, reach out to verify information, and refer to shared knowledge was helpful because it was provided proactively, before the older adult was targeted. Returning to the dual victimization framework, youth may have an interest in protecting their likeness from use in deepfake impersonation scams that cause harm to their older family members. Motivated by participants' insights and perspectives from our youth team members, we considered opportunities to encourage youth engagement in their older adult family members' online safety:

**In-Class Online Safety Education.** Interventions targeting youth's own online safety have been integrated into educational curriculums with success [6]. Building on this, curriculums could explain how youth can support their older adult family members' online safety. Specifically, programming could introduce youth to collaborative protective practices, such as agreeing on a secret code word, prompting them to proactively engage in these conversations.

**Leveraging Social Media.** Youth are often exposed to information through social media [4]. In the context of deepfake impersonation scams, using social media to increase awareness and share guidelines on how to talk to older adult family members about scams could engage broad youth audiences.

Future work should investigate how youth perceive their role in older adult family members' online safety and respond to the suggested interventions. As previous work has surfaced, intergenerational technology support can create challenging family dynamics [10], which future work should also explore from youth perspectives. As scams become more technically sophisticated and involve older adults' family members, innovative approaches are needed to engage these stakeholders and build resilience across generations.

## References

- [1] FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions. Technical report, United States Financial Crimes Enforcement Network, November 2024.
- [2] FCC Warns Consumers of 'Grandparent Scam' Robocalls. Technical report, United States Federal Communications Commission, March 2025.
- [3] Sharyn Alfonsi. How con artists use AI, apps, social engineering to target parents, grandparents for theft. *CBS News*, August 2023.
- [4] Abdulmalik Alluhidan, Mamtaj Akter, Ashwaq Al-soubai, Jinkyung Katie Park, and Pamela Wisniewski. Teen Talk: The Good, the Bad, and the Neutral of Adolescent Social Media Use. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW2):1–35, November 2024.
- [5] Yue Deng, Changyang He, Yixin Zou, and Bo Li. "Auntie, Please Don't Fall for Those Smooth Talkers": How Chinese Younger Family Members Safeguard Seniors from Online Fraud, 2025. Version Number: 1.
- [6] Diana Freed, Natalie N. Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas, and Dan Cosley. Understanding Digital-Safety Experiences of Youth in the U.S. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, Hamburg Germany, April 2023. ACM.
- [7] Skye N Leedahl, Melanie Sereny Brasher, Erica Estus, Bethany M Breck, Cory B Dennis, and Samantha C Clark. Implementing an interdisciplinary intergenerational program using the Cyber Seniors® reverse mentoring model within higher education. *Gerontology & Geriatrics Education*, 40(1):71–89, January 2019.
- [8] Lina M. Khan, Rebecca Kelly Slaughter, Alvaro M. Bedoya, Melissa Holyoak, and Andrew N. Ferguson. Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission. Technical report, United States Federal Trade Commission, October 2024.
- [9] Benjamin Alan Morrison, James Nicholson, Lynne Coventry, and Pam Briggs. Recognising Diversity in Older Adults' Cybersecurity Needs. In *Proceedings of the 2023 ACM Conference on Information Technology for Social Good*, pages 437–445, Lisbon Portugal, September 2023. ACM.
- [10] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–24, April 2021.
- [11] James Nicholson, Lynne Coventry, and Pamela Briggs. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–11, Glasgow Scotland Uk, May 2019. ACM.
- [12] Xinru Tang, Yuling Sun, Bowen Zhang, Zimi Liu, Ray Lc, Zhicong Lu, and Xin Tong. "I Never Imagined Grandma Could Do So Well with Technology": Evolving Roles of Younger Family Members in Older Adults' Technology Learning and Use. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–29, November 2022.
- [13] Rachel Tresiman. Dozens of Canadians are charged for scamming American grandparents out of \$21 million. *NPR*, March 2025.
- [14] Nelisha Vellani and David Common. Her grandson's voice said he was under arrest. This senior was almost scammed with suspected AI voice cloning. *CBC News*, March 2025.
- [15] Yuxiang Zhai, Xiao Xue, Zekai Guo, Tongtong Jin, Yuting Diao, and Jihong Jeung. Hear Us, then Protect Us: Navigating Deepfake Scams and Safeguard Interventions with Older Adults through Participatory Design. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–19, Yokohama Japan, April 2025. ACM.