Intergenerational Support for Deepfake Scams Targeting Older Adults

Karina LaRubbio[1], Alyssa Lanter[1], Seihyun Lee[2*], Mahima Ramesh[3*], Diana Freed[1]
1- Brown University, 2- Tenafly High School, 3- Acton-Boxborough Regional High School, *authors contributed equally

Motivation

- Older adults have lost an estimated $61.5 billion to fraud in the United States [1].
- “Grandparent scams” involve attackers impersonating trusted family members in need of urgent financial support, sometimes using AI-generated deepfakes, such as audio or visual content [2].
- Older adults often rely on family to support their online safety [3].
- Collaborative online safety is especially relevant to scams that target both older adults and the family member being impersonated.

Research Questions

RQ1: How do older adults currently perceive and protect themselves against deepfake impersonation scams?

RQ2: What opportunities exist to engage youth to support older adults against deepfake impersonation scams?

Methods

- Focus groups about AI and online safety
- 37 total participants ages 70-94, compensated $10
- Qualitative data analysis
- Approved by Brown University’s IRB

RQ1 Results: Protective Practices

Older adults described **intergenerational protective practices:** Collaborative approaches to online safety in which a younger family member, such as a grandchild, supports an older adult’s online safety. In the context of deepfake impersonation scams, participants expressed these intergenerational protective practices:

Advice to ignore unknown callers

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

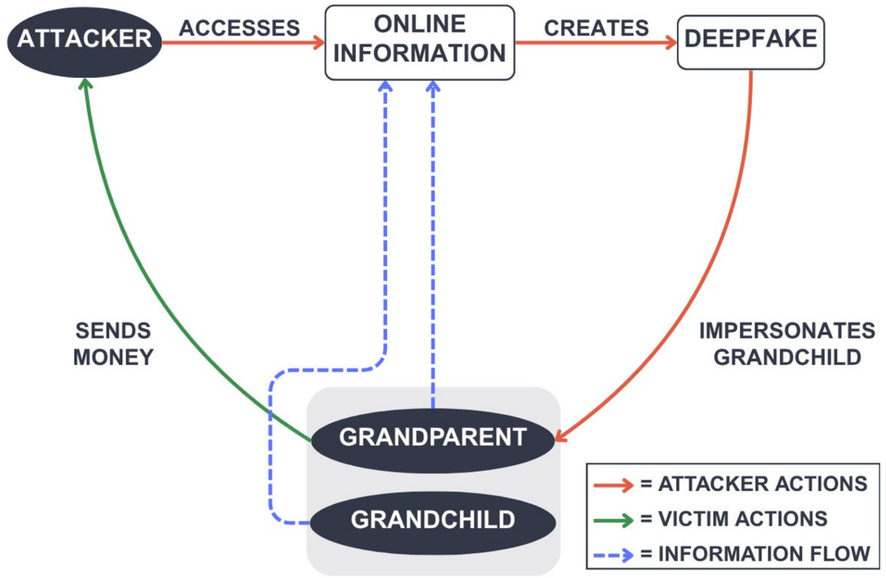
Contact for verification

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

Shared knowledge

> “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)

Dual Victimization Framework



RQ2 Results: Engaging Youth

Participants emphasized younger family members’ roles in supporting their resilience to deepfake impersonation scams. We propose proactive approaches to engage youth in their older adult family members’ online safety:

Online safety education in school

Leveraging social media

Future work should include youth to investigate their perceptions of opportunities to provide support and suggested interventions.

References
1. L.M. Khan, R.K. Slaughter, A.M. Bedoya, M. Holyoak, and A.N. Ferguson. Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission. United States Federal Trade Commission, October 2024.
2. Y. Zhai, X. Xue, Z. Guo, T. Jin, Y. Diao, and J. 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.
3. X. Tang, Y. Sun, B. Zhang, Z. Liu, R. Lc, Z. Lu, and X. Tong. "I Never Imagined Grandma Could Do So Well with Technology": Evolving Roles of Younger Family Members in Older Adults’ Technology Learning and Use. In Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2):1–29, November 2022.