Training Older Adults to Resist Scams with Fraud Bingo and Scam-Detection Challenges

Molly Davies
WISE & Healthy Aging
mdavies@wiseandhealthyaging.org

Daniel Marino
Amelia Nash
Kevin A. Roundy
Mahmood Sharif
Acar Tamersoy
NortonLifeLock Research Group
{Daniel.Marino, Amelia.Nash, Kevin.Roundy, Mahmood.Sharif, Acar.Tamersoy}@nortonlifelock.com

CHI'20, Workshop on Designing Interactions for the Ageing Populations - Addressing Global Challenges, April 25–30, 2020, Honolulu, HI, USA

Abstract
Older adults are disproportionately affected by scams, many of which target them specifically. In this interactive demo, we present *Fraud Bingo*, an intervention designed by WISE & Healthy Aging Center in Southern California prior to 2012, that has been played by older adults throughout the United States. We also present the Scam Defender Obstacle Course (SDOC), an interactive web application that tests a user's ability to identify scams, and subsequently explains how to recognize the scams. SDOC is patterned after existing phishing-recognition training tools for working professionals. We present the results of running a workshop with 17 senior citizens, where we performed a controlled study that used SDOC to measure the effectiveness of Fraud Bingo. We outline the difficulties several participants had with completing SDOC, which indicate that tools like SDOC should be tailored to the needs of older adults. Additionally, we discuss how to adapt Fraud Bingo and SDOC for international audiences.

Author Keywords
Scams, Fraud, Interventions, Older Adults

CCS Concepts
•**Human-centered computing** → **Human computer interaction (HCI);** User studies;

S	C	A	M
S2 Bank Examiner Scam	C12 Direct Express Text Scam	A17 Grandchild In Distress Scam	M30 Recovery Room Scam
S6 Boiler Room Fraud	C16 Free Airline Ticket Scam	A23 Limit Personal Info on the Internet	M27 Nigerian Letter Scam
S1 "Advance Fee" Loan Scam	C9 Click Bait	A20 Guard Pin Number	M32 TypoSquatting
S8 Check links/urls	C13 Do Not Call List	A18 Guard Bank Accounts	M31 Install Anti-Virus

Figure 1: A Fraud Bingo card (please zoom in for improved readability).

Scam Tips

S1. "Advance Fee" Loan Scam - for an advance fee, you will get the loan you need. But then the paperwork stall begins and the loan never comes.
S2. Bank Examiner Scam - someone posing as law enforcement or bank security calls to tell you that fraudulent activity has been detected on your account. You are asked to participate in catching the "thief" by withdrawing money and giving it to this person as "evidence"
S3. Be Wary of Online Dating Sites - An online love interest who asks for money is almost certainly a scam artist.
S4. Be Cautious of Email Attachments - Opening email attachments from from unknown senders may infect your computer
S5. Block Pre-Screened Credit Offers - www.optoutprescreen.com or (888)567-8688
S6. Boiler Room Fraud - Call center selling questionable investments
S7. Charitable Solicitations - Before you donate over the phone, look up the charitable organization's number online and call them back. Scammers will say they are from the American Cancer Institute when the real organization's name is National Cancer Society.
S8. Check links/urls - Hover the mouse over a link to a url to see where it's taking you. Destination URL should be displayed in lower left corner in most browsers
C9. Click Bait - Be careful when opening attachments or clicking links on emails that claim to relate to an emotionally charged current event, internet memes, conspiracy theories, etc.
C10. Credit Report - Review annually with all 3 credit bureaus. Freeze credit if you don't need to apply for new credit for a while.
C11. Report Scams to FTC - Federal Trade Commission (877)382-4357
C12. Direct Express Text Scam - Text message from a party claiming to be Direct Express, you are directed to call a number to provide card and pin number
C13. Do Not Call List - (888) 382-1222 or https://www.donotcall.gov/
C14. Dumpster Diving - Remember to shred documents with personal info
C15. Email Phishing - Do not follow links in emails or supply personal information
C16. Free Airline Ticket Scam - Phishing scam to obtain your personal info by claiming to be a reputable airline company & offering a free flight
A17. Grandchild In Distress Scam- Slowdown, talk to someone you trust and do not send money to anyone claiming to be your grandchild
A18. Guard Bank Accounts - Don't provide account information to anyone calling or emailing
A19. Guard Internet Passwords - Use complex password that do not contain identifying info
A20. Guard Pin Number - do not share it with anyone
A21. IRS Money Owed scam - The IRS does not send taxpayers unsolicited e-mails about their tax accounts, tax situations or personal tax issues.
A22. Jury Duty Scam - Scammer calls to say that you missed jury duty and now have a warrant out for your arrest. They ask for your social security number so they can "verify" that you were on the list.
A23. Limit Personal Info on the Internet - Only sign up for trusted websites
A24. Lottery Scam - The scammer claims you have received a prize but you need to pay taxes on the prize before you can receive your winnings.
M25. Mail Theft - Don't leave incoming or outgoing mail in your mailbox overnight or on weekends. Have the post office hold your mail if you're out of town.
M26. Use Caution When Browsing Websites - Always look for the https:// prefix. If you don't see the "s" don't enter any information on that webpage that you want to keep secure
M27. Nigerian Letter Scam - Nigerian Official asks for your help in exchange for a reward, this help is usually asking for money.
M29. Online Auction Fraud - Do not purchase underpriced items, they may be counterfeit
M28. Text Phishing - Fake alerts that your accounts have been compromised
M30. Recovery Room Scam - These "recovery rooms" get the names of people who have been defrauded in other scams and then call and claim to be Federal attorneys or agents who will recover your losses for a fee.
M31. Install Anti-Virus - protect your computer from being hacked by installing anti-virus software on your computer and mobile device.
M32. TypoSquatting - Also known as "url hijacking" where bad actors own hostnames that intentionally look like valid domain names with typos such as Goggle.com

Figure 2: Reverse side of a Fraud Bingo playing card with descriptions of all scams. Participants take these cards home with them if they so desire.

Introduction

Older adults are disproportionately affected by scams and frauds of various kinds. For example, the United States' Federal Trade Commission reported that in 2018, romance scams resulted in reported losses of $143 million, more than any other type of scam [5]. While the median loss reported per victim was $2,600, it rose to $10,000 for victims that are 70-years-old or older. Prior work has identified factors that correlate with susceptibility to scams, among which age is often cited as a key factor [7, 8, 6]. Researchers found that older adults experience declining sensitivity to untrustworthy information [1, 3] and a reduced ability to detect lies [1, 10]. Studies also highlighted age-related functional brain changes in response to untrustworthy cues [1].

The lack of intervention tools specifically designed for older adults motivated the WISE & Healthy Aging Institute to develop Fraud Bingo—an activity to educate participants about frauds while playing the popular game Bingo—which has since been recommended by federal and state governments throughout the United States for use at senior centers (e.g., [13]).

We also developed the Scam Defender Obstacle Course (SDOC), an interactive web application, in similar vein to existing training tools used to educate working professionals about phishing scams [9]. Utilizing Fraud Bingo as a scam training, we explored SDOC's suitability as an evaluation tool during a workshop that involved 17 senior citizens in Santa Monica, California. We found that tools like SDOC that are designed to evaluate and train working professionals to recognize phishing scams are less effective for many older adults. In this paper, we present Fraud Bingo, SDOC, and lessons learned from running both tools with groups of older adults.

Fraud Bingo

Fraud Bingo is an educational game, similar to Bingo. The main difference is that when the bingo caller calls out the number of a square, they also announce the name of an associated fraud or fraud-prevention tip, along with its more detailed explanation on the back of the bingo card. Fraud Bingo was developed and rolled out by WISE and Healthy Aging, who have run dozens of events in Los Angeles County for more than eight years to groups of 30 to 150 participants. Its development was motivated by a need to create an engaging educational tool that could attract large audiences, and in which people of all skill levels and cultures could participate. It builds on bingo's popularity, and prizes are given out in events help attract audiences. The game has spread by word of mouth to other parts of the United States. It has also been translated to languages other than English, including Armenian, Chinese, Korean, and Spanish. Various incarnations of the game exist, some of which cover frauds broadly, while others focus on specific frauds (e.g., investment frauds).

The majority of frauds and fraud tips that we printed on the Fraud Bingo cards were derived from the original WISE & Healthy Aging Institute's game. We adapted the game by eliminating the frauds and fraud-prevention-tips that were least relevant to computer security. Moreover, we added computer-security-related prevention tips identified in prior work [4, 8] and advice related to online romance scams, typo-squatting, and techniques that are typically used by scammers to mislead victims. Additionally, we modified Fraud Bingo from a 5×5 to a 4×4 square to focus game play on relevant tips and frauds, and to increase the likelihood that all relevant clues would be covered in 45 minutes of play.

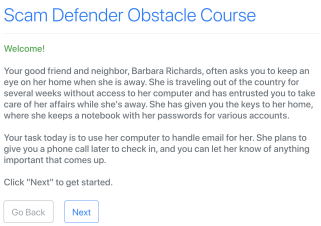

Figure 3: The SDOC instructions ask participants to perform computer tasks and respond to emails on behalf of a friend.

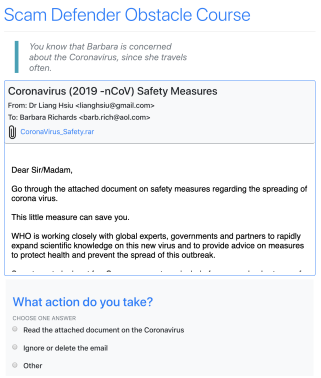

Figure 4: SDOC uses scam examples derived from real scams. This scam uses fears about the 2020 COVID-19 virus to entice users into opening a malicious attachment.

Scam Defender Obstacle Course

The Scam Defender Obstacle Course (SDOC) is an online evaluation and training tool that we developed to *1)* measure susceptibility to a set of common online fraud schemes; and *2)* educate users on scam-warning signs.

SDOC asks participants to imagine that they are handling the affairs of a good friend who is out of the country and away from her computer (Fig. 3). Participants are then shown a series of ten challenges in the form of emails and browser windows that they encounter while using their friend's computer (Fig. 4). Four challenges present legitimate correspondence with actions that should be taken—for instance, the gas company sending a notice that the payment for service was declined and the balance must be paid. The other challenges present common, real-world scams that include a range of lures to get users to click links, open attachments, or otherwise take actions that could lead recipients to be defrauded. For each of these challenges, participants are asked to indicate what actions they would take (e.g. "Ignore and delete email", or "Click on link to update billing information"). Participants are also presented free-form text boxes to explain their choices.

SDOC was designed as a dual-purpose tool, to both evaluate and educate. We aim to use it to measure the effectiveness of educational interventions, such as Fraud Bingo, in helping older adults to avoid falling for scams. However, since the participants are engaged in a hands-on exercise and being exposed to real-world fraud lures, we did not want to miss the opportunity to provide feedback and tips to help educate them. In order not to affect the results of the evaluation, we refrained from providing any feedback until all ten challenges were completed. Afterward, users were shown which challenges were legitimate and which were scams, along with an explanation of the indicators that can be used to arrive at the correct conclusion.

Lessons from our Bingo & SDOC Workshop

We ran a two-hour workshop whose intended purpose was to serve as a controlled study evaluating the effectiveness of Fraud Bingo as an intervention technique. The event was free and advertised and open to the general public. Participants were informed that they would participate in Fraud Bingo and in a computer training. Overall, 17 older adults participated in the workshop. They were divided into two groups. One group of eight participants began the workshop in a computer lab where they tried their hand at SDOC. Eight additional participants began the workshop in an adjacent room where they played Fraud Bingo. After 50 minutes, the two groups switched rooms, and participated in the opposite activity. An additional participant arrived at this time and participated only in SDOC. Eight of the 17 participants were part of a class hosted by WISE & Healthy Aging for individuals experiencing early-stage memory loss. These participants were split evenly between both groups.

Running this workshop taught us valuable lessons about how to run an improved version of our study in the future. We share those insights below.

Running Fraud Bingo

When asked, participants reported being satisfied with the experience of playing Fraud Bingo, or made no comment. We observed several reasons for which Fraud Bingo works well as an educational tool for older adults. First, the game of Bingo exists in various incarnations throughout the world and is easily learned. At least three participants had never played Bingo before our event, yet they were able to participate in our workshop without any difficulty. Second, the activity was inclusive—even participants with memory loss and other forms of cognitive decline were able to participate

Figure 5: The Fraud Bingo portion of the workshop.

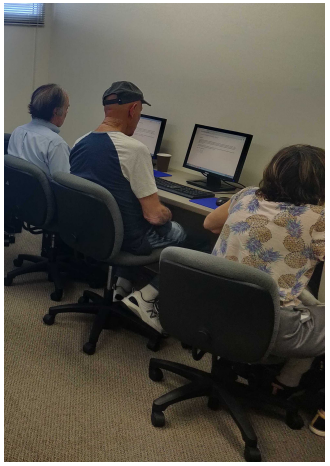

Figure 6: The SDOC portion of the workshop.

effectively. Third, via interactions throughout the workshop, participants were able to contextualize frauds for one another by relating experiences they have had. Such forms of cooperative learning have been shown to make educational activities effective [14].

Running SDOC

Our workshop represented the first occasion on which senior citizens had tried out SDOC. The course was successful in certain ways, but the workshop also taught us several lessons in how to improve upon SDOC's design.

On the positive side, participants who were able to complete the SDOC (about half), reported enjoying the activity. Furthermore, SDOC increased participants' confidence in their knowledge, as several reported that it "reinforced what they already knew." This can potentially motivate the participants to adopt secure behavior in the future [11].

At the same time, the workshop highlighted several limitations of SDOC that should be addressed to improve its applicability for educating older adults. To mention some: *1)* The emails may have been long for certain participants, some of whom had difficulties scrolling through and answering the subsequent questions (especially participants with cognitive decline); *2)* Participants were biased to mark emails as scam (potentially because the rate of scam was higher than what would be expected in practice [12]); and *3)* Free-form answers took up time (as certain participants had difficulty typing) and left too much room for interpretation. These limitations may also be relevant for other educational tools in the vein of SDOC (e.g., [9]).

Adaptations for a Global Audience

To serve the needs of international audiences, Fraud Bingo and SDOC should be adapted to local needs (e.g., certain frauds are mostly encountered in specific parts of the world [2]). Fraud Bingo has already been translated into several languages, which is a good first step, yet the clues and tips themselves are still tied to scams that prey upon older adults in the United States. Fortunately, existing bingo-card generation software makes it easy for advocates for older adults replace US-specific scams with local equivalents, while preserving tips that are universally applicable.

Similarly to Fraud Bingo, SDOC can be easily adapted to include scams that are relevant to the region and culture of the participants. In general, scams that prey upon similar fears tend to exist across many cultures, yet customization is necessary, as much of the educational value of SDOC lies in its ability to expose participants to scams that they are likely to encounter in practice. Localized patterns of computer or device usage must also be considered. For instance, in countries where older adults are more likely to use mobile devices than computers, scam-detection training should focus on mobile devices.

Conclusion

In conclusion, we found Fraud Bingo to be an effective training tool for older adults that span a wide range of cognitive abilities. While SDOC was appreciated by some older adults, it needs to be adapted to different skill levels, particularly in a workshop setting. In addition to adopting design guidelines for improved usability, we advocate that similar training tools be of flexible duration so that participants can complete as many or as few challenges as they can get to in a set amount of time and still receive feedback on their performance.

REFERENCES

[1] E. Castle, N. I. Eisenberger, T. E. Seeman, W. G. Moons, I. A. Boggero, M. S. Grinblatt, and S. E. Taylor. 2012. Neural and behavioral bases of age differences

in perceptions of trust. *Proceedings of the National Academy of Sciences* (2012).

[2] Nicolas Christin, Sally S Yanagihara, and Keisuke Kamataki. 2010. Dissecting one click frauds. In *ACM Conference on Computer and Communications Security*.

[3] N. C. Ebner, P. E. Bailey, M. Horta, J. Joiner, and S. W. C. Chang. 2015. Multidisciplinary perspective on prosociality and aging. *Frontiers in Developmental Science: Social Cognition Development Across the Life Span* (2015).

[4] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *ACM CHI Conference on Human Factors in Computing Systems*.

[5] Emma Fletcher. 2019. *Romance scams rank number one on total reported losses*. (2019). `https://tinyurl.com/FTC18Report` Online; retrieved Feb 14, 2020.

[6] Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. 2019. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction* (2019).

[7] José M. Fernandez Lévesque, Fanny Lalonde and Dennis Batchelder. 2017. Age and gender as independent risk factors for malware victimisation. In *British Computer Society Human Computer Interaction Conference*.

[8] Daniela Oliveira, Donovan Ellis, Huizi Yang, Harold Rocha, Sandeep Dommaraju, Devon Weir, Melis Muradoglu, and Natalie Ebner. 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 *ACM CHI Conference on Human Factors in Computing Systems*.

[9] proofpoint. 2018. ThreatSim Phishing Simulations: Key Features and Benefits. (2018). `https://www.proofpoint.com/us/products/phishing-simulations-knowledge-assessments/threatsim` Online; retrieved Feb 18, 2020.

[10] T. Ruffman, J. Murray, J. Halberstadt, , and T. Vater. 2012. Age-related differences in deception. *Psychology and Aging* (2012).

[11] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *ACM CHI Conference on Human Factors in Computing Systems*.

[12] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. 2017. Can unicorns help users compare crypto key fingerprints?. In *ACM CHI Conference on Human Factors in Computing Systems*.

[13] The United States Attorney's Office. 2019. U.S. Attorney's Office Presents "Fraud Bingo" Game to Help Teach Seniors How to Avoid Scams. (2019). `https://preview.tinyurl.com/SCFBingo` Online; retrieved March 18, 2020.

[14] Steven Yamarik. 2007. Does cooperative learning improve student learning outcomes? *The Journal of Economic Education* (2007).