Scam awareness found to be best defense for older adults facing fraudster phone calls

September 25 2023, by Justin Jackson

Credit: Pixabay/CC0 Public Domain

Research led by Rush Alzheimer's Disease Center, Rush University Medical Center, Chicago, has looked into the susceptibility of older adults to scammers. In a paper, "Vulnerability of Older Adults to

Government Impersonation Scams," published in *JAMA Network Open*, the researchers tested 644 older adults with an experiment designed to mimic a government impersonation scam.

Participants averaged age 85.6 and were part of the Rush Memory and Aging Project (MAP), an ongoing cohort study of common chronic conditions related to aging. As part of the experiment, they were exposed to deceptive materials through mailers, emails, and phone calls by a live agent, mimicking a government impersonation scam.

Results were classified by three engagement groups: no engagement, engagement with skepticism, and conversion (those who engaged without skepticism).

Of the 644 participants, 441 (68.5%) did not engage, 97 (15.1%) engaged but raised skepticism, and 106 (16.4%) comprised the conversion group. Of those converted, nearly three-quarters provided personal information.

The research revealed that factors like cognition, financial literacy, and awareness of fraud scams were associated with the type of engagement. Those in the skeptical engagement group had the highest cognitive scores and financial literacy, while the conversion group had the lowest scam awareness.

According to the Federal Trade Commission, phone calls are the most common and most effective method used by fraudsters for targeting older adults.

According to the nonprofit National Consumer Law Center, there are over 30 million robocalls from scammers daily in the US, resulting in ~30 billion dollars in theft each year. It is estimated that ~70% of Americans do not answer unknown numbers due to the high frequency

of robocalls.

"Do not call" lists only work with legitimate businesses, and while many telecom companies have created systems that alert consumers when a call is "Scam Likely," there are still ways that scammers can get around the designation. Spam emails also present a formidable access point, as even the best spam filters occasionally fail.

The findings highlight the need for greater public awareness of scam tactics in general and specifically for older adults.

How do these scams work?

There is an email about an overdue account, a strange purchase confirmation or the IRS asking you to contact them. It can also be an incoming robocall stating the same; press one to begin scam. The voice on the other end informs you that they are from the IRS, Microsoft, Geek Squad, or Amazon, with important information about your account. There are charges you know you do not owe, transactions that you did not make. A person receiving such a call may think they have been the victim of fraud when, in fact, the fraud has just begun.

The voice on the other end understands and believes when you say there has been a mix-up, suggesting that it could be the result of identity theft, a hacker or other third-party fraud. They might ask for personal information, account numbers or a social security number to confirm identity and ensure, for security reasons, that they are speaking with the right person.

If a computer is available, they will offer to complete a refund through a secure server, asking the potential victim to install a remote access application to "ensure a secure transaction." Of course, this is the opposite of secure as it allows the scammer full access to the computer,

but if the victim is not tech savvy or believes it is a reputable entity they are dealing with, the scammer is granted access.

From this point, the scammer can gain access to online accounts, but their job is complicated by the fact that banks flag suspicious activity. Typically, there is a fake attempt to complete a refund, in which the scammer makes it look like the victim has received too much money. A quick http screen edit via the remote access makes it look like the online bank account has been credited too much.

In order to avoid the threat of all the account funds being frozen, the scammer then directs the victim to purchase hundreds of dollars in gift cards from a local store that can be redeemed over the phone or instructions to send cash via the mail, and in some cases they will make large transfers directly out of the victim's bank account. If the bank flags it, they might send a third-party verification via text. The scammer knows this code is being sent and asks the victim to verify it by reading it to them so they can complete the fake refund and authorize the actual transfer of funds.

If it sounds like a lot of steps requiring a tremendous amount of trust, it is, and it does. Millions of robocalls and emails a day are looking for trusting conversion individuals. Bank accounts have been drained this way, life savings wiped out, and victims of these scams often have little recourse. Local police departments and prosecutors are powerless as the thieves often operate outside the country where the scam occurs.

Scam call centers in India are the epicenter of many scams targeting English-speaking countries like the US, Canada, UK and Australia. Even when evidence is collected about where the scammers are operating through a tech-savvy practice of scam baiting where anti-scammer hackers reverse the remote connection to gain access to the scammer's details, getting the local authorities abroad to take action is a challenge.

Knowing is half the battle, maybe even all of it

Amazon, Google, Microsoft, the IRS, Best Buy's Geek Squad, and credit card companies do not call consumers or transact business through email exchanges or over-the-phone gift card transactions. If a caller claims to be from any of these companies, hang up.

Other common scams include low-cost vacations, extended automotive warranties, student loan forgiveness, debt collection, police charity, and bank fraud alert texts.

A somewhat more involved one is where a fake FBI or DEA agent calls about a car full of drugs seized at the border with "your" information connected to it. Somehow, only a gift card transaction can prevent them from connecting "you" to the crime. Storywise, the drug-filled border car offers the most intrigue, but all of these scams are designed to work on that fraction of a percent of people who still have a trusting nature.

More information: Lei Yu et al, Vulnerability of Older Adults to Government Impersonation Scams, *JAMA Network Open* (2023). DOI: 10.1001/jamanetworkopen.2023.35319