Older Americans are given the wrong idea about online safety – here's how to help them help themselves

Nora McDonald Published: March 22, 2022 8.15am EDT

Recently, the U.S. Social Security Administration sent out an email to subscribers of its official blog explaining how to access social security statements online. Most people know to be suspicious of seemingly official emails with links to websites asking for credentials.

But for older adults who are wary of the prevalence of scams targeting their demographic, such an email can be particularly alarming since they have been told that the SSA never sends emails. From our research designing cybersecurity safeguards for older adults, we believe there is legitimate cause for alarm.

This population has been schooled in a tactical approach to online safety grounded in fear and mistrust – even of themselves – and focused on specific threats rather than developing strategies that enable them to be online safely. Elders have been taught this approach by organizations they tend to trust, including nonprofits that teach older adults how to use technology.

These organizations promote a view of older adults as highly vulnerable while also encouraging them to take gratuitous risks in defending themselves. As information technology researchers, we believe it doesn't need to be this way.

Older adults and online safety

Older adults may be at heightened risk of cybersecurity breaches and fraudulent behavior because they lack experience with internet technology and represent a financially attractive target. Older adults may also be more susceptible because they struggle with their confidence in using technology even as they recognize its benefits.

We have been developing technology tools that help aging Americans maintain their own online safety no matter what challenges they may face, including cognitive decline. To do so, we needed to understand what and how the people we study are learning about cybersecurity threats and what strategies they are being taught to reduce their vulnerabilities.

We have found that older adults attempt to draw on personal experience to develop strategies to reduce privacy violations and security threats. For the most part, they are successful at detecting threats by being on the lookout for activities they did not initiate — for example, an account they do not have. However, outside experts have an inordinate amount of influence on those with less perceived ability or experience with technology.

What 'experts' are telling older Americans

Unfortunately, the guidance that older adults are getting from those who presumably have authority on the matter is less than ideal.

Perhaps the loudest of those voices is the AARP, a U.S. advocacy group that has been carrying out a mission to "empower" individuals as they age for over six decades. In that time, it has established a commanding print and online presence. Its magazine reached over 38 million mailboxes in 2017, and it is an effective advocacy group.

What we found was that the AARP communiqués on cybersecurity use storytelling to create cartoonish folktales of internet deception. A regularly

featured diet of sensational titles like "Grandparent Gotchas," "Sweepstakes Swindles" and "Devilish Diagnoses" depict current and emerging threats.

Much of the cybersecurity advice given to elders fosters the cartoonish misconception that flesh-and-blood scam artists lurk in their midst. 5m3photos/Moment via Getty Images

These scenarios appeal to readers the way crime shows have historically appealed to TV audiences: by using narrative devices to alarm and thrill. Ultimately they also delude viewers by leaving them with the misconception that they can use what they've learned in those stories to defend themselves against criminal threats.

Folktales and foibles

One job of folktales is to spell out the hazards that a culture wants its members to learn in childhood. But by presenting cyber-risk as a set of ever-evolving stories that focuses on particular risks, the AARP shifts attention

away from basic principles to anecdotes. This requires its members to compare their online experiences with specific stories.

Readers are implicitly encouraged to assess the plausibility of particular scenarios with questions like, Is it possible that I have any unpaid back taxes? And, Do I actually have an extended warranty? It requires people to catalogue each of these stories and then work out for themselves each time whether an unsolicited message is a real threat based on its content, rather than the person's circumstances.

No, it's not personal

Through this inventory of stories and characters, we also found that the AARP was personalizing what is, at root, a set of structural threats, impersonal by nature. The stories often characterize scammers as people in the reader's very midst who use local news to manipulate older adults.

Real threats are not "sweepstake swindlers" or "Facebook unfriendlies," with a live scam artist sensitive to the needs and foibles of each intended victim. There is rarely a human relationship between the cyber-scammer and the victim — no con artists behind the notorious "grandparents scam." The AARP bulletins and advisories imply that there is — or, at least, implicitly foster that old-fashioned view of a direct relationship between swindler and victim.

Don't engage

Perhaps even more worrisome, AARP advisories appear to encourage investigation into scenarios, when engagement of any sort puts people at risk.

In one post alerting people to "8 Military-Themed Imposter Scams," they discuss "prices too good to be true," when the very concept of buying a car

on Craigslist, or an "active-duty service member" urgently selling a car, should be a red flag discouraging any form of engagement.

Internet users of any age, but especially more vulnerable populations, should be urged to withdraw from threats, not be cast as sleuths in their own suspense stories.

Protecting older adults in the age of surveillance capitalism

In order to reduce everyone's risk while online, we believe it's important to provide a set of well-curated principles rather than presenting people with a set of stories to learn. Everyone exposed to threats online, but especially those most at risk, needs a checklist of cautions and strong rules against engagement whenever there is doubt.

In short, the best strategy is to simply ignore unsolicited outreach altogether, particularly from organizations you don't do business with. People need to be reminded that their own context, behaviors and relationships are all that matter.

[*Get the best of The Conversation, every weekend*. Sign up for our weekly newsletter.]

Because, in the end, it's not just about tools, it's about worldview. Ultimately, for everyone to make effective, consistent use of security tools, people need a theory of the online world that educates them about the rudiments of surveillance capitalism.

We believe people should be taught to see their online selves as reconstructions made out of data, as unreal as bots. This is admittedly a difficult idea because people have a hard time imagining themselves as

separate from the data they generate, and recognizing that their online lives are affected by algorithms that analyze and act on that data.

But it is an important concept — and one that we see older adults embracing in our research when they tell us that while they are frustrated with receiving spam, they are learning to ignore the communications that reflect “selves” they don’t identify with.