ASSESSING VULNERABILITY TO SOCIAL SECURITY SCAMS

Research conducted by
Clifford Robb, University of Wisconsin-Madison
Stephen Wendel, Behavioral Technology

September 2021

Over the last few years, Social Security scams have become one of the most common forms of government imposter fraud. These scams cost innocent people in the United States millions of dollars a year and undercut the ability of the Social Security Administration to contact and interact with citizens about their benefits.

A Simple, Interactive Process that Teaches People to Spot SSA Fraud

This report presents research on how to help individuals discriminate between digital imposter scams and real appeals from the Social Security Administration. On a nationally representative sample of United States residents, the authors randomly assign participants to one of four training programs: from general tips about scams to a targeted experiential learning program inspired by *inoculation theory*. Inoculation theory posits that exposing people to a weakened version of a dangerous appeal can help them learn to identify and resist such appeals over time.

There is strong evidence that the inoculation process successfully and significantly increases fraud-detection without decreasing trust in real communications, and that the effects persist over time. The researchers found that the training works for both a mocked-up research environment in Qualtrics and in a real email platform called Rainloop. The researchers also found that impact of the training generalized to non-Social Security Administration fraud, including Amazon.com imposter scams. However, the inoculation training is effective only for the type of communication addressed in the training (email) and may not apply well to other areas, as such SMSes and letters, without additional training.

A Low Cost, Straightforward Training

A low cost, targeted training can reduce the chances that recipients fall victim to Social Security scams. In our study, subjects were presented with less than five minutes of targeted training around identifying Social Security imposter scams. Our findings suggest that this low-cost intervention is not only effective at improving participants' ability to recognize fake communications but does so in a what that does not diminish participants' ability to recognize real communications. It should be noted that training should be specific to the form of communications (e.g., phone, email, letter).

Implications

- This study suggests that a low-cost, four-and-a-half minute training can help individuals fight fraud messaging; such trainings (specific to fraud modality) should be examined for further refinement and potentially for broad deployment.

- The research community can use this randomized control trial approach to rigorously measure the drivers of fraud susceptibility, something that, to date, has been difficult to do with self-reported data on fraud.

The research reported herein was performed pursuant to a grant from the U.S. Social Security Administration (SSA) funded as part of the Retirement and Disability Consortium. The opinions and conclusions expressed are solely those of the author(s) and do not represent the opinions or policy of SSA or any agency of the Federal Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of the contents of this report. Reference herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply endorsement, recommendation or favoring by the United States Government or any agency thereof.