Center for
Financial Security
UNIVERSITY OF WISCONSIN-MADISON

Retirement & Disability
Research Center

Enhancing Trust in the Social Security Administration and E-Government among People Targeted by Fraud

Marti DeLiema
University of Minnesota
mdeliema@umn.edu

Cliff A. Robb
University of Wisconsin
carobb@wisc.edu

Stephen Wendel
Behavioral Technology
steve@behavioraltechnology.co

Center for Financial Security

University of
Wisconsin-Madison

1300 Linden Drive
Madison, WI 53706

608-890-0229
cfs@mailplus.wisc.edu
cfs.wisc.edu

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.

Abstract

One of the insidious effects of government imposter scams is the potential erosion of trust among those who are targeted – fraud targets may learn to distrust communications and people who claim to be from the Social Security Administration (SSA) or other federal agencies. This interferes with the necessary and beneficial work of the SSA and, more broadly, of the US government. This study analyzes how individuals targeted by government imposter scams respond to communications from the SSA and how the SSA can reinforce public trust and willingness to engage. Specifically, the team developed an application to teach individuals how to identify legitimate communications from the SSA, other government bodies, and retail companies. Multiple national samples of Americans, in which some participants were prior victims of scams, were then assigned in randomized trials and tested on their ability to distinguish between real and fraudulent communications. We find nearly universal exposure to fraud attempts in the national samples, low prevalence of paying money to fraud perpetrators in response to those attempts, and a set of personal characteristics that appear to predict low trust in the SSA and other institutions. We also find evidence that interactive online training can help people both trust real communications and identify scams. The impact of the training is more pronounced for emails than for websites, and for government communications than for business communications from companies such as Amazon. A non-interactive training that provides static tips on detecting fraud provides a lesser but still significant effect.

Keywords: government imposter scam, business imposter scam, fraud detection, online shopping, randomized control trial, consumer education

JEL Classification: D91; P46

1. Introduction

Technology-facilitated imposter scams are a significant and growing form of mass marking fraud. In an imposter scam, a fraud perpetrator convinces their target to send or transfer money by pretending to be a familiar person or someone associated with a known entity, such as a government agency or a company. Imposter scams come in many forms, but the most common are government imposter scams, such as the Social Security Administration (SSA) and the Internal Revenue Services (IRS) imposter scams. There are also business imposter scams, such as tech support scams and Amazon imposters. Perpetrators typically use mass marketing tactics like Voiceover Internet Protocol (VoIP), email, text message, or phishing websites to solicit as many targets as possible at very low costs.

Although the rate of victimization following exposure to imposter scams is low (see DeLiema & Witt 2021), targeting attempts are pervasive and require consumers to stay vigilant. For example, in just a three-month period from October to December 2020, nearly half of American survey respondents reported that they received at least one bogus phone call from someone who claimed to be an SSA representative (SimplyWise 2021). In 2021, there were nearly 800,000 reports of government and business imposter scams received by federal and state agencies. Nearly a quarter of these reports involved a financial loss (victimization), with median losses of $1,000 per victim (Federal Trade Commission (FTC) 2022). Many consumers report significant psychological distress from incessant fraud solicitations, even in the absence of financial loss (Bailey et al. 2020; Figueroa 2019).

In addition to the financial and emotional costs, research indicates that fraud victimization, and even exposure to fraud, can decrease trust (Button, Lewis, & Tapley 2014; Gurun, Stoffman & Yonker 2016; Harris, Petrovits, & Yetman 2022). Diminished trust can have social and economic consequences as consumers may be more suspicious of engaging in online interactions with the government and retailers. Therefore, it is important for government agencies and businesses that are impersonated by fraud perpetrators to restore trust among those affected by scams.

The purpose of this study is to determine whether consumers who have been victimized by government or business imposter scams demonstrate lower levels of trust in digital communications (emails and websites) from government agencies (e-government) and online retailers (e-commerce) and whether an interactive online fraud training module can improve their ability to accurately discriminate between real and fraudulent communications without eliciting undue distrust.

In our results, we did not find that those who reported prior imposter fraud victimization were more distrustful of the SSA or the federal government compared to non-victims. There were no significant differences between victims and non-victims in revealed trust of online communications during the experimental assessment. There was a relationship between prior fraud and current trust in conducting online transactions, but the results are inconsistent across measures.

Our experimental findings indicate that interactive fraud detection training can help consumers discriminate between real and fraudulent online communications from both government agencies and retailers. The effect of the training is no greater for those who have experienced prior imposter fraud than those who have not. We find that training is best at helping consumers correctly discern and label fraudulent communications as fake, rather than correctly label legitimate communications as real, although there is an effect for legitimate communications as well. We also find that the training has stronger effects for email communications than for websites. That is, the interactive tutorial improved participants' ability to identify fraudulent emails more than fraudulent websites. The improvement in *fraud-detection* diminishes with time; the improvement in the *detection of legitimate messages* did not substantially decrease after a two to three week delay.

2. Background

2.1 Trust in E-government and E-commerce

Trust is critical for economic growth and a functioning democratic society (Bjørnskov 2012; Hardin 2002; Zak & Knack 2001). Unfortunately, trust and confidence in the US government and political institutions have declined substantially since the 1960s. Low trust in the government reduces support for government spending (Chanley, Rudolph, & Rahn 2000), affects political participation such as voting and political party membership (Bäck & Christensen 2016; Hoogh & Marien 2013), and undermines compliance with laws, regulations, and public health policies (Hoogh & Marien 2013; Van Dijke & Verboon 2010).

Under the backdrop of declining social and political trust, there is a deepening reliance on digital and online technologies to interact with government agencies (e-government) and engage in routine consumer purchasing activities (e-commerce). West (2004, pg. 16) defines e-government as "the delivery of government information and services online through the internet or other digital means." Examples include using government web services to file and pay taxes, apply for public benefits or licenses, register vehicles, and seek out information. For example, according to the IRS (2022), 90 percent of individual tax returns are filed electronically.

Using the internet for routine consumer activities has also grown. In 2016, still years before the COVID-19 pandemic amplified online retail, the Pew Research Center (Smith & Anderson 2016) found that 79 percent of Americans had made a purchase online, and 15 percent made online purchases on a weekly basis. Today, online retail purchases account for approximately 14 percent of all retail sales in the US (US Census Bureau 2022).

Many e-government and e-commerce activities involve the online transfer and storage of personal and financial information. Prior research has shown that trust is a critical factor in determining whether consumers will engage in these online activities (Alzahrani et al. 2017; Kim & Peterson 2017; McKnight, Choudhury, & Kacmar 2002). For example, Belanger and Carter (2008) found that trust in the internet and trust in government were positively related to intention to use e-government. Unfortunately, the pervasiveness of government and business imposter scams, combined with high-profile data breaches and other cybersecurity threats, may cause distrust and deter consumers' from engaging with government and retailers online. For example, Chakraborty et al. (2016) found that greater perceived severity of a hacking incident increased the perceived risks of online shopping and decreased online shopping intent among older adult consumers. In an Indonesian sample, Rofiq (2012) found that the more times consumers were exposed to cyber-fraud, the more resistant they were to participate in e-commerce.

2.2 The Impact of Fraud on Trust

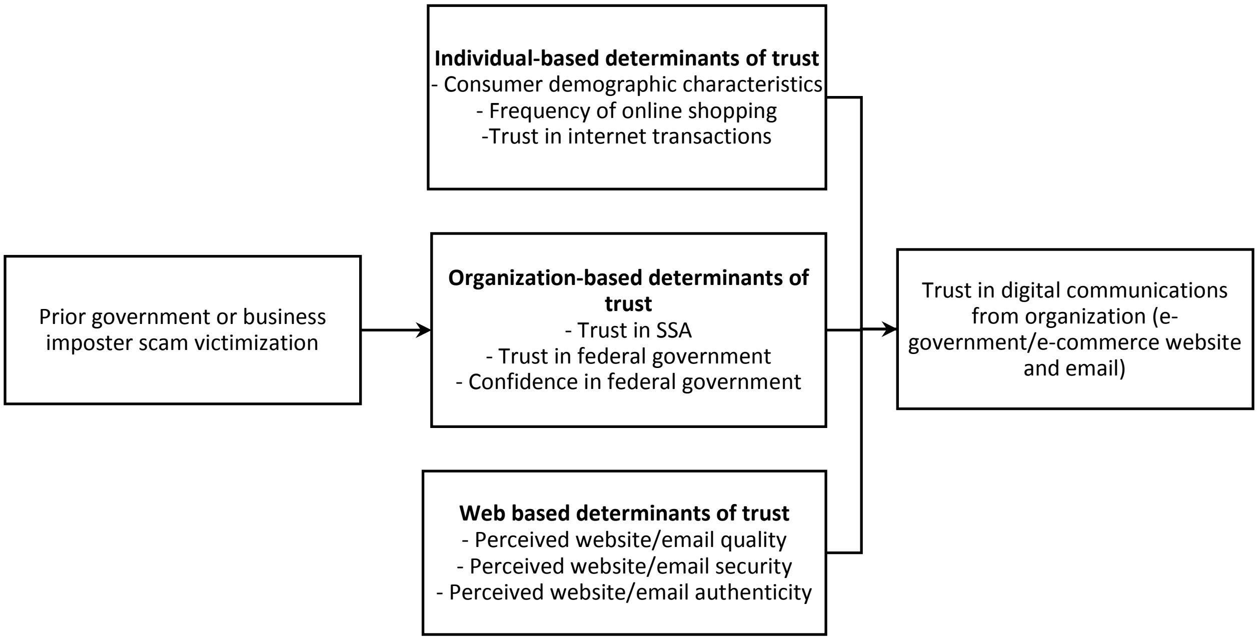
Few studies have examined the impact that fraud victimization has on citizen and consumer trust. According to Goel (2021), imposter scams can undermine the government's authority to administer laws and enforce policies. Impersonation schemes also consume law enforcement resources and redirect agency efforts toward educating the public about fraud rather than administering vital programs. In a qualitative study that examined the socioemotional aftermath of fraud, Button, Lewis, and Tapley (2014) found that many victims “were more cautious about making decisions involving finance, using their credit card and purchasing items on the internet” (pg. 51). In another study, Brenner and colleagues (2020) found that those who experienced some type of financial fraud had lower confidence in financial matters.

The consequences of diminished trust have real impacts on financial markets and consumer confidence in the legal system. Using investment advisor and branch deposit data, Gurun, Stoffman, and Yonker (2018) found that investors in communities more exposed to the Bernie Madoff Ponzi scheme subsequently withdrew more assets from registered investment advisers and increased deposits at banks, leading to lower returns. Using Gallup survey data, the authors also found that college-educated people who were more exposed to the Madoff scam reported larger declines in confidence in the criminal justice system compared to people unaffected by the fraud. Together, these findings indicate that fraud exacts a toll on trust, resulting in harmful social and economic outcomes.

2.3 Conceptual Model

We use a modified version of the framework developed by Beldad and colleagues (2012) to conceptualize the three main determinants of trust in online environments: individual, organization, and digital. In our revised model, individual-based determinants of trust include the consumer’s demographic characteristics and their frequency of internet use. Organization-based trust factors include the consumers’ trust in the company, organization, government, or government agency. Organization-based trust may be negatively affected by victimization from business and government imposter scams. Website-based trust features include perceived website quality, security, and authenticity. We posit that these factors affect consumers’ perceptions of the authenticity of government and retailer websites and emails (digital communications) and that the experience of fraud victimization may cause increased distrust.

Figure 1: Modified conceptual framework of trust in e-government/e-commerce communications adapted from Beldad et al. (2012)


Individual-based determinants of trust
- Consumer demographic characteristics
- Frequency of online shopping
-Trust in internet transactions
Prior government or business imposter scam victimization
Organization-based determinants of trust
- Trust in SSA
- Trust in federal government
- Confidence in federal government
Trust in digital communications from organization (e-government/e-commerce website and email)
Web based determinants of trust
- Perceived website/email quality
- Perceived website/email security
- Perceived website/email authenticity

2.4 Can Trust be Restored?

One potential strategy to enhance trust in e-government and e-commerce is to teach consumers how to discriminate between real and fraudulent digital communications, including emails and websites. Prior research by these authors focusing on fraudulent emails found evidence that such training is indeed possible and effective (Robb and Wendel 2022). This research employed the fact that most digital communications contain specific features that consumers can use to determine their legitimacy. For example, an email recipient can verify the true sender by inspecting the "reply-to" address located in the email header, rather than relying on the "from" email address which can be disguised. To identify phishing websites, consumers can inspect the domain in the URL to determine if it truly belongs to a government agency (.gov) or a well-known retailer (.com). Popular domains, such as Amazon.com, are difficult to fake. With careful scrutiny, most consumers can learn to spot subtle changes in the URL that scammers use to impersonate well-known entities (e.g., Amazom.com or Anazon.com). Consumers can also hover over links to preview where they direct web traffic. Sharing these cybersecurity tips in a simple online tutorial may help consumers develop more confidence in their ability to identify fraudulent websites or emails, thereby avoiding imposter scams.

In the present study, we evaluate the effectiveness of a short, interactive fraud detection training program designed to help consumers identify digital features that signal that a website or email is a phishing attempt. Based on the conceptual model outlined above, this education may help enhance the perceived security and authenticity of legitimate emails and websites. For those previously victimized by an imposter scam, gaining knowledge on digital fraud detection may help restore trust and increase willingness to engage in interactions with legitimate retailers and government agencies online, including the SSA.

3. Research Methodology

3.1 Research Questions and Hypotheses

This study sought to answer two primary research questions. First, are previous victims of government and business imposter scams less trusting of digital communications than individuals who have not experienced imposter fraud victimization? In the present study, we define fraud victimization as experiencing a financial loss after responding to a fraud solicitation. Based on our conceptual model, we hypothesize that prior imposter fraud victimization decreases trust in the Social Security Administration (the federal agency impersonated the most from 2019 to 2021), as well as reduces confidence in the federal government and trust in online transactions in general. We also hypothesize that there will be increased distrust of all government and digital business communications among former imposter scam victims relative to non-victims. Specifically, our hypotheses in this area are:

H1: Prior imposter fraud experience is associated with lower trust in the SSA, lower trust in online transactions, and lower confidence in the US government.

H2: Prior imposter fraud experience is associated with greater distrust of legitimate and fake communications

The second research question is whether an interactive online fraud detection training program can enhance trust in legitimate government and retail company communications, and whether this training has a larger effect on imposter fraud victims. The hypotheses are as follows:

H3: The interactive training will improve participants' accuracy in discerning legitimate and fake communications relative to the static training and control conditions. This effect will be consistent for those who have and have not been victimized by an imposter scam.

H4: The interactive training does not increase distrust of legitimate communications relative to the static training and control conditions.

H5: The interactive training will have a greater effect on discrimination accuracy for older participants and those who engage less frequently in online shopping relative to younger participants and participants who are more frequent online shoppers.

H6: The effect of the interactive training does not port to better fraud detection accuracy for non-digital solicitations (i.e., postal letters).

H7: The effect of the interactive training will diminish after a two-week delay.

Beyond our core research questions, we also identified data exploration opportunities that could shed light on related areas of interest to the research community. In particular, these analyses can help understand who reports fraud and how well the population of fraud reporters corresponds to the overall population. Our research questions in this area, which are not pre-registered hypotheses, are:

R1: Who is most susceptible to losing money in an imposter scam?

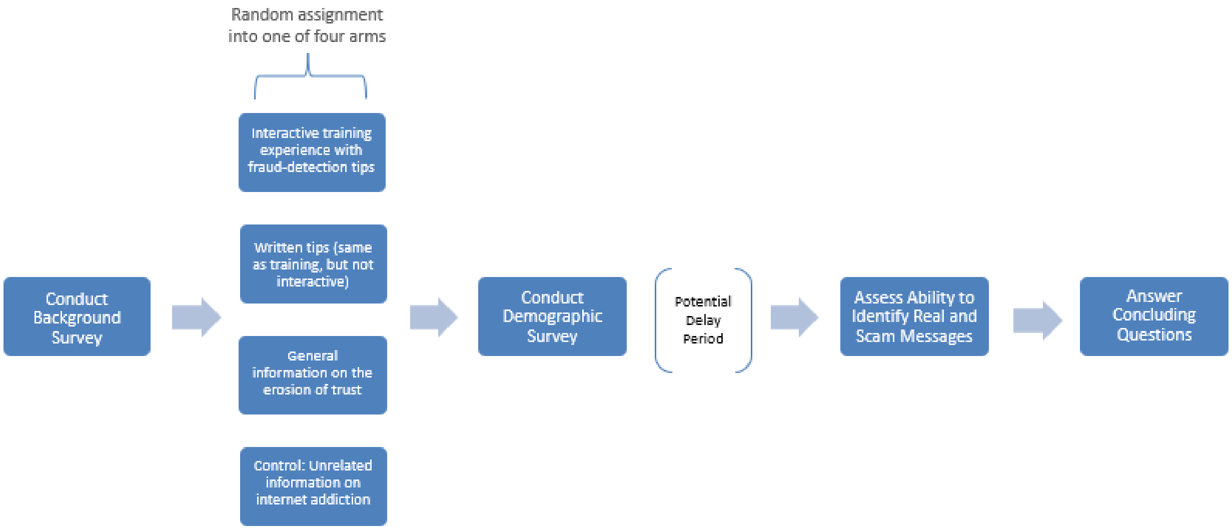
R2: Who reports fraud to public sources, such as the Better Business Bureau?

3.2 Study Design

To answer these research questions, we developed a platform in which participants first provide information in response to survey questions, are trained on the characteristics of real and fraudulent communications (or are randomly assigned to read other irrelevant information), and then are assessed in their ability to correctly label communications as real or fraudulent. Specifically, the participants went through the following five-step process (see Figure 2 for a graphical depiction of the process):

1. After providing consent to the study, participate in a Qualtrics survey with questions assessing their trust in the SSA, their trust in online transactions, confidence in the US government, and frequency of online shopping.
2. Be randomly assigned to one of four conditions:
    a. Receive an innocuous control condition (reading material about Internet addiction);
    b. Read a statement on the importance of trusting the government, based on a case study of the Ebola virus and disease prevention measures;
    c. Receive written instructions on what to look for to identify a fraudulent website or email, covering the same topics and techniques as the previous arm without the interactive experience; or
    d. Receive written instructions on what to look for to identify a fraudulent website or email, then interact with real and fraudulent simulated emails and websites with training materials in the context of these communications.
3. Complete a short demographic survey.
4. Either immediately or after a pre-specified delay of 19 days, confront a series of communications (website, email, and letter), and indicate whether they are fraudulent or real.
5. Answer a final set of questions covering prior experience with fraud and additional personal characteristics.

Figure 2: Visual depiction of the study procedures


Random assignment into one of four arms
Conduct Background Survey
Interactive training experience with fraud-detection tips
Written tips (same as training, but not interactive)
General information on the erosion of trust
Control: Unrelated information on internet addiction
Conduct Demographic Survey
Potential Delay Period
Assess Ability to Identify Real and Scam Messages
Answer Concluding Questions

The complete surveys, training materials, communications used in the assessment, and analysis code are all publicly available on our GitHub site, https://github.com/sawendel/SSATrust. The study was reviewed and approved by both the University of Wisconsin and the University of Minnesota Institutional Review Board.

3.3 Background Survey (Step 1 of the Participant Experience)

In the background survey, all participants begin with three previously developed measures: confidence in the US government, trust in online transactions, and trust in the Social Security Administration. To assess confidence in government, we used a four-item scale from the Pew Research Center, with questions such as “How much confidence do you have in the future of the United States?”. The composite score is the sum of responses, in which each question is given equal weight and scaled to be from 0 (lowest confidence) to 1 (highest confidence). For trust in online transactions, we used an eight-item scale adapted from Carter and Bélanger (2005) and McKnight, Choudhury, and Kacmar (2002), where each item asks for a 1-7 Likert agreement rating. The composite score is the mean of the eight items. Sample statements include: “Entering personal information over the internet is unsafe,” and “I would hesitate to enter personal information like my name, address, and phone number on the internet.”

For trust in the Social Security Administration, we used a ten-item scale, also adapted from Carter and Bélanger (2005) and McKnight, Choudhury, and Kacmar (2002). It similarly uses a 1-

7 Likert agreement rating, with statements such as, “The Social Security Administration is truthful in its dealings with me,” and, “In my opinion, the Social Security Administration is trustworthy.” The composite SSA trust score is the mean of the responses.

Finally, we asked participants to provide information on their frequency of online shopping using the one-item instrument from Pavlou (2003). It asks participants to complete the phrase, “I buy products online…” with an answer range from 1 (never) to 6 (a few times a week/daily).

3.4 Training Program (Step 2 of the Participant Experience)

Participants were assigned to one of the four arms described above using simple random assignment. The three control arms – unrelated information on internet addiction, trust-related information on the importance of trusting the federal government, and specific fraud-prevention tips – provided straightforward, written text. The interactive training arm was the primary focus of the experiment.

In the interactive arm, participants first received a set of written tips – identical to that of the “fraud-prevention tip” control arm – on six topics, from looking at the domain of a link to examining the “mailed by” field in an email’s headers to identifying common scammer tactics like urgency to trick recipients. Afterward, participants were directed to a custom online application where they were presented with eight example communications from government agencies or retail businesses. These were presented as mock emails, websites, and letters. Each example of communication was presented sequentially, and participants were asked to judge whether it was real or fraudulent. After responding “real” or “scam” and selecting “Next,” the online application revealed the correct answer and presented tips on what to look for within the context of the communication.

The application sought to provide a realistic setting for communications. For example, sample website communications were embedded in a mocked-up web browser, with a URL and links that could be hovered over and clicked on throughout the page. Sample email communications were embedded in a mocked-up email client, with openable email headers (closed by default, as is the case in most email clients), hoverable and clickable links, and buttons for normal functions such as reply, delete, and forward. To protect the security of the participant, all links were disabled. The user could hover over and click on the links as if they were real but were informed by a pop-up message that the links were inactive if they did indeed click on one. The application logged all relevant activity to the database, including clicking on links and opening email headers.

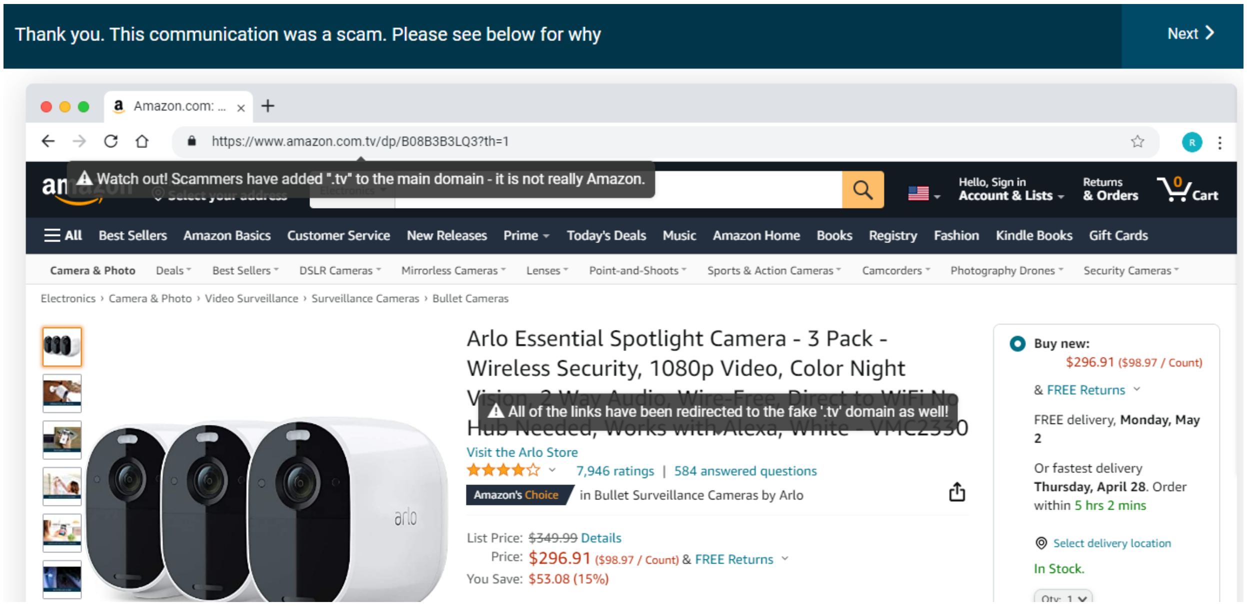
The communications were a mix of three fraudulent messages based on actual scams perpetrated in the past, and five real communications, mimicking their real sources. Four emails and four web pages were included: four came from (or impersonated) government agencies, and four came from (or impersonated) well-known businesses (Table 1).

Table 1: Content, order, and type of each mock communication used in the interactive training condition

Type	Legitimacy	Imposter Type	Short Name	Description
Email	Real	Government	Protect Yourself	Fraud awareness email from SSA
Website	Real	Business	Amazon HP	Amazon homepage
Email	Scam	Government	IRS Email_	Email from the “IRS” requesting personal information
Website	Real	Government	IRS Web_	IRS website
Website	Real	Business	AppleID	Apple ID homepage
Website	Scam	Business	Amazon Product	Home security cameras listed on “Amazon”
Email	Real	Business	McAfee Email	Email from McAfee regarding identity theft activity
Email	Scam	Government	Get Protected	Email from “SSA” about registering for social security number misuse alerts

Figure 3 provides an example of the fraud detection tips presented in the interactive training. The top line of the screen informs the participant of the correct answer (the communication presented in Figure 3 is a scam) after they made a judgment of “real” or “scam” on the previous screen. Below that, the participant sees the realistically mocked-up web browser and then the content of the (mocked-up) web page itself. In this case, the key information that the user would use to identify this page as fraudulent comes from the URL shown in the browser window and the fact that the website domain (Amazon.com.tv) is not the true Amazon.com domain – a common technique used in real scams.

Figure 3: An example used in the interactive training, showing how an Amazon page can be copied and faked by a scammer.



Thank you. This communication was a scam. Please see below for why

https://www.amazon.com.tv/dp/B08B3B3LQ3?th=1

⚠ Watch out! Scammers have added ".tv" to the main domain - it is not really Amazon.

⚠ All of the links have been redirected to the fake '.tv' domain as well!

Arlo Essential Spotlight Camera - 3 Pack - Wireless Security, 1080p Video, Color Night Vision, 2 Way Audio, Wire-Free, Direct to WiFi No Hub Needed, Works with Alexa, White - VMC2330

List Price: $349.99 Details
Price: $296.91 ($98.97 / Count) & FREE Returns
You Save: $53.08 (15%)

Buy new: $296.91 ($98.97 / Count)
& FREE Returns
FREE delivery, Monday, May 2
Or fastest delivery Thursday, April 28. Order within 5 hrs 2 mins
In Stock.

3.5 Demographic Survey (Step 3 of the Participant Experience)

Following the training (and control conditions), participants responded to a set of demographic questions, including employment status, total household income, race/ethnicity, highest level of education, age, and gender.

After the demographic survey, participants in the primary study went immediately to the assessment (Step 4). Participants in the separate “time delay” study (described in more detail below) were thanked for their time and asked to return in two weeks. The platform used to coordinate and pay participants, Prolific, experienced technical difficulties. Participants in this condition were only able to return after a minimum of sixteen days from the start of the study. They entered the assessment (Step 4) after a short reminder about the study and only after providing their continued consent.

3.6 Assessment (Step 4 of the Participant Experience)

All participants were tested on their ability to correctly distinguish fake appeals from real ones. The experience was identical to the interactive training with three notable exceptions:

1. The content of the communications was novel (not used in the interactive training condition)

2. Participants were not informed of the correct answer after they indicated whether they thought each message was real or fraudulent.
3. The communications included two mocked-up letters—one legitimate and one a scam. This was not a medium of communication that we had trained individuals on during the interactive training. Letters were included to assess the "portability" of the training to non-digital communication mediums.

Like the interactive training, a realistic, custom-designed application hosted all of the communications. Participants could hover over and click on links, open email headers, and click or interact with the mocked-up web browser and email client. The test communications also included a mix of real and fraudulent messages (all based on actual communications in real life) from both government and business sources (Table 2).

Table 2: Content, order, and type of each mock communication used in the interactive training condition

Type	Legitimacy	Imposter Type	Short Name	Description
Website	Real	Business	Walmart Product	A sample product page from Walmart.com, selling security cameras.
Email	Scam	Business	Red Cross	An email asking for donations - to a fraudulent site.
Website	Real	Government	SSA HP	The SSA's (actual) homepage
Website	Scam	Government	mySSA	A modified version of the mySSA login page.
Email	Real	Business	Amazon Mark Delivery	An email informing the recipient of a delay in the delivery of a product
Website	Scam	Business/Government	FB SSA	A Facebook page for a fake Social Security account (based on an actual scam)
Email	Scam	Government	SSA Optout	A scam-modified version of an SSA email allowing people to opt out of future SSA emails.
Email	Real	Government	Replacement Card	A (real) email from the SSA instructing recipients how to get a new SSA card.
Letter	Real	Government	Medicare Review	A notice from the SSA about an upcoming call from the Medicare office
Letter	Scam	Government	Benefits Suspension	A letter threatening the suspension of SSA benefits

3.7 Concluding Questions (Step 5 of the Participant Experience)

After completing the assessment in Step 4, participants completed a short survey on their prior exposure and responses to various types of imposter scams, their experience with cybersecurity training, and their levels of loneliness. Specifically, this survey asked participants whether they had previously been targeted by (1) Someone claiming to be from the Social Security Administration (but wasn't), (2) someone claiming to be from the IRS, (3) someone claiming to be from another government agency, (4) someone claiming to be from the company where they work, (5) someone claiming to be from another organization or group, or (6) someone selling fraudulent goods or services. Participants could check any that applied. For participants who indicated they had been targeted by any of these forms of fraud, they were then asked whether they had lost money in the scam and how much (in dollars). They were also asked, "Did you report this fraud to the Better Business Bureau, a US government agency, the police, or another group that tracks or fights fraud?"

Following the fraud exposure, victimization, and reporting questions, we asked participants two sets of questions to measure potential correlates of fraud-detection ability. First, we asked whether they had previously received cybersecurity training, and second, we administered a three-item loneliness scale from Hughes et al. (2004). Questions asked to the participant include "How often do you (1) Feel left out, (2) lack companionship, (3) isolated from others". Questions were rated on a three-point Likert scale where hardly never=1, sometimes=2, and often=3 with the composite score (3-9) as the sum of the three responses.

3.8 Participant Pool

Participants were recruited from two sources: Prolific, a commercial provider of online research participants, and the Better Business Bureau (BBB). Prolific respondents are paid to participate in online surveys and show high reliability and completion rates. Prolific provides both convenience samples and nationally representative, quota-balanced samples. It sets individual quotas according to three factors—age, sex, and ethnicity—and uses them to match the characteristics of the US

Census.[1] Research by the Prolific team[2] and others[3] find that their method leads to samples that will match the target population, but care should be taken in directly generalizing to the entire US population.

The results provided here all come from Prolific's nationally representative samples and represent the bulk of the participants. The other set of participants were recruited by email from the BBB using a listserv of North American consumers who previously reported an imposter scam to the BBB using their Scam Tracker website (https://www.bbb.org/scamtracker). These participants were thanked for their contribution but were not compensated.

The Prolific participant pool allowed us to analyze susceptibility to fraud, responsiveness to training, and prior experience with fraud on a national and generalizable sample of American residents. The BBB participant pool provided a unique look at self-reporters through the set of people who reported attempted and successful fraud, thus underlying most existing studies of fraud in the field and allowing an analysis of people with prior negative experiences.

A total of 5,891 people participated in the research across four primary studies and eleven small, iterative tests of the application code and platform. The four primary studies were as follows:

1. Primary Sample: 1,244 participants from Prolific, quota balanced on age, gender, and ethnicity to be nationally representative; they interacted with the platform between 30 July 2022 and 1 August 22. 1,191 people completed the survey and provided valid data for a 96 percent completion rate.
2. Time Delay Sample: 1,251 participants from Prolific, similarly quota balanced; they interacted with the platform between 14 August 2022 and 17 August 22 for the training and between 2 September 22 and 13 September 22 for the test. 1,213 people completed the first part of the study and provided valid data for a 97 percent completion rate. 1,017 people returned to complete the second (final) part of the study with valid data for an 81 percent completion rate.

[1] Prolific. "Representative Samples FAQ." 2021. https://researcher-help.prolific.co/hc/engb/articles/360019238413.

[2] Peer, E., Rothschild, D., Evernden, Z., et al. 2021. "Data Quality of Platforms and Panels for Online Behavioral Research." P. 1-46. https://papers.ssrn.com/sol3/papers.cfm?abstract id=3765448.

[3] Coppock, A. & McClellan, O. 2019. "Validating the demographic, political, psychological, and experimental results obtained from a new source of online survey respondents." Research & Politics, Vol. 6, Issue 1, P. 1-14. https://journals.sagepub.com/doi/pdf/10.1177/2053168018822174.

3. BBB Sample: 1,042 participants were recruited from BBB's Scam Tracker from a population of roughly 30,000 total imposter scam reporters; they interacted with the platform between 30 July 2022 and 1 August 22. 593 people completed the study and provided valid data for a 57 percent completion rate (or 2 percent of the invited population).
4. Test Sample: 1,226 participants from Prolific, also quota balanced on age, gender, and ethnicity to be nationally representative; they interacted with the platform between 9 July 2022 and 13 July 22. 1,192 people completed the survey and provided valid data for a 97 percent completion rate.

The Primary Sample, Test Sample, and BBB Sample each experienced the primary version of the study with no delay between the training and the assessment (Step 4). The Time Delay Sample had a delay period that varied based on when they responded to each round of the survey; the first round was made available to participants on 14 August, and the second round was made available on 2 September. The median delay period was 19 days. The other 1,128 participants were part of convenience samples from Prolific, who were used to test the application code. Each iteration excluded participants in its sample from prior studies.

In our initial analysis of the Test Sample, we determined that the test communications had misleading elements: it was ambiguous whether certain communications were actually fraudulent or real. We corrected these elements before conducting further studies. Thus, for the rest of the analysis, we will focus on the Primary Sample, Time Delay Sample, and the BBB Sample.

3.9 Dataset

The final dataset used in this analysis comes from two nationally representative samples (Primary Sample, with no delay between the training and assessment, and the Time Delay Sample, with a median 19-day delay), and the BBB sample of people who previously self-reported being targeted by an imposter scam (with no delay between the training and assessment). As noted above, we gathered detailed information on trust levels, demographics, and prior experience with fraud for each participant, along with their behavior during the training program and assessment.

In addition to the raw data, and composite trust scores described above, we calculated the following values:

- **Revealed trust**. Among the two control arms of the study where participants did not receive any training on identifying scams, we use the percent of real messages they correctly identified during the assessment as a revealed measure of trust. Since the arms are randomly assigned, they represent a (smaller) nationally representative sample of Americans.
- **Percent correct**. The percent of communications correctly labeled, with versions of this variable segmented by percent correct among business communications and among government or percent correct among email, website, and letters
- **Distrust**. The percent of communications labeled as fraudulent, with versions of this variable segmented as "undue distrust" (percent of communications that were real but labeled as fraudulent) and "rightful distrust" (percent of communications that were fraudulent and labeled as such).

This data is all publicly available on our GitHub site, https://github.com/sawendel/SSATrust.

4. Results

4.1 Sample Characteristics

Primary Sample

The Primary Sample was 51.6 percent female with an average age of 41 years, 15 years of education (some college), and a median income of between $60,000 and $79,999. Three-quarters of respondents identify as non-Hispanic White or Caucasian, 13 percent as non-Hispanic African American or African, 6 percent as non-Hispanic Asian American or Asian, 4 percent Hispanic, and 2 percent all other groups. Prolific balances its samples on race and does not include Hispanic Americans as a separate category (considering being Hispanic as an ethnicity, not a race). Because of this, their sample significantly under-represents Hispanic Americans (who are roughly 19 percent of the total US population).

Among the general population approximately represented by the Prolific sample, exposure to attempted fraud is widespread – 93 percent of Prolific participants reported being targeted for at least one type of imposter fraud (at any point in the past). This is likely an underestimate. Practically speaking, this limits the usefulness of modeling differences between fraud targets and non-targets since fraud exposure is nearly universal. However, only 6 percent of Prolific respondents reported having lost any money to any such fraud in the past, and only 22 percent of the Prolific respondents targeted by fraud reported the attempted fraud to the US Government, BBB, or other organization. This highlights the challenges of using fraud reports to understand the full breadth of fraud. Slightly more than one-third (36 percent) of participants reported having undergone some form of cybersecurity training in the past. Mean levels of loneliness (range = 1-3) were 1.6.

When we look at pre-training levels of trust, the sample's mean government confidence score is 0.5 (range = 0 to 1; Standard Deviation (SD)=0.2), SSA trust = 4.4 (range= 1 to 7; SD=1.3); and Internet trust = 3.6 (range =1 to 7; SD=1.0). Revealed trust (the percent of real messages labeled as real among the untrained population) is 77 percent (SD=19.6). When we look at the overall ability to correctly label messages across all arms, the mean is 69 percent (SD=15.0).[4]

BBB Sample

The BBB sample was majority female (69 percent) and older (average age 52), slightly less educated (14.6 years of education), and had lower income (median income $40,000 - $59,999) than the Prolific population. Overall, BBB respondents were less likely to correctly label communications, with 63 percent correct versus 69 percent for the national Prolific sample. BBB respondents were more likely to have been targeted by fraud, but not remarkably so; 80 percent reported being targeted by a business imposter scam (versus 75 percent for Prolific), 20 percent by an SSA imposter scam (versus 18 percent), and 45 percent (versus 51 percent) by other government imposter scams. The BBB respondents were far more likely to have reported losing money (52 percent) compared to Prolific respondents (6 percent). Note that the sample from the BBB Scam Tracker population was designed to oversample those who lack money for scams.

[4] These values are all from the primary study; the baseline trust metrics are nearly identical for the other two nationally representative balanced samples from Prolific: the initial test study, and the two-week delay study. This is to be expected since samples were selected to be representative. There were differences in the ability to correctly identify messages – which is also to be expected because the communications themselves. The time between training and assessment also varies across the samples.

Participant characteristics are not representative of the overall BBB Scam Tracker population due to the low response rate (2 percent of people invited) and the intentional targeting of people who had lost money to scams in our invitation process. Therefore, results should be treated as preliminary.

The BBB respondents were as confident in the US government (0.5 on a scale of 0 to 1) as the Prolific respondents, had slightly lower trust in the SSA (4.3 on a 1 to 7 scale), considerably lower trust in the internet (3.0 on a 1 to 7 scale), and lower revealed trust (63 percent of real messages were considered real). They were also less likely to correctly label messages overall (63 percent). These are all mean values and should not generate a narrative on their own. Subsequent analyses will tease apart the effect of differences in the demographic makeup of the two populations versus differences in fraud experience.

4.2 H1: Prior Imposter Fraud Experience is Associated with Lower Trust in the SSA, Lower Trust in Online Transactions, and Lower Confidence in the US Government

Overall, we do not find strong support for the role of prior exposure or victimization on diminished trust in the SSA. The results are inconsistent across other forms of trust and confidence in government. Table 3 presents regression results for our composite SSA trust score.

Table 3: Regression results examining the correlates of trust in the SSA; N=1144; R2=0.05[5]

	Coef.	Std. Error	T-Value	P>|t|
Intercept	4.0327	0.456	8.850	0.000
Targeted by Prior SSA Imposter Scam (Exposure)	-0.0672	0.101	-0.668	0.504
Lost Money to Fraud (Victim)	0.5341	0.674	0.792	0.428
Log(Amount of Money Loss to Fraud)	-0.1102	0.118	-0.932	0.352
Employment=Retired (ref: Employed)	-0.3274	0.158	-2.075	0.038
Employment=Under/Unemployed	-0.0408	0.090	-0.452	0.651
Log(Income)	0.0244	0.052	0.474	0.635
Years of Education	0.0356	0.020	1.791	0.074

[5] In this specification, we included both exposure to scams and loss to scams; naturally these variables are (partially) correlated and could cause multicollinearity. To check the practical significance of this issue, we conducted separate regressions for exposure and loss. The results are the same (no statistically significant effect).

Age	-0.0298	0.017	-1.772	0.077
Age Squared	0.0006	0.000	2.856	0.004
Gender (0=Male;1=Female)	-0.0846	0.078	-1.082	0.279

Both variables measuring prior fraud victimization, having lost money to fraud (SSA or otherwise), and the amount of money that people lost have no relationship with trust in the SSA. Similarly, exposure to fraud (being targeted by SSA imposters) is not related to trust in the SSA. While the results do not support H1, this is good news for public trust. The recent wave of SSA impostor scams is unlikely to have changed people's fundamental trust (or distrust) in the SSA.[6]

When looking at trust in online transactions and confidence in government, we do see relationships – but they are inconsistent. Specifically, the more money that someone lost to fraud, the less trusting they are of online transactions (coeff on logged amount lost = -0.25; SE= 0.088, p=0.005) and the less confident they are in government (coeff on logged amount lost = -.04; SE=.017; p=0.009). These results are contradicted by our analysis of revealed trust (the baseline trust in real messages shown by people who were not trained during our program). Using revealed trust as the outcome variable, we find that prior experience with business impersonation scams increases with revealed trust (coeff= 5.6, SE=1.8; p=0.002). It is possible that trusting people are more likely to be targeted by fraud (reverse causality) or are more likely to remember and report prior fraud attempts when asked in the survey. However, more research is needed to help explain these inconsistent results.

When we look more broadly at the correlates of pre-training trust measures, we find interesting relationships that warrant further analysis. Returning to Table 3, we see that after controlling for age and income, retired persons show lower trust in the SSA. From roughly age 25 onwards, trust increases with age from a low point (age 25) of 3.7/7 to 5.5/7 by age 80 (after controlling for retirement status, income, etc.). Those with higher education show greater trust, all else being equal. In other regression analyses, we see that our composite confidence in government score (coeff= 2.92; SE=0.18; p=0.000) and online shopping (coef=0.08; SE=0.04; p=0.020) are positively associated with trust in the SSA; however, our loneliness score is negatively associated with trust in the SSA (coef=-0.12; SE=0.059; p=0.046).

[6] It is possible that scam attempts depress trust in the SSA equally across the entire population – regardless of who reported being targeted and who fell victim to the scam. That is unlikely, however.

Similarly, those with higher income and education, all else being equal, tend to have more confidence in the US government. All else being equal, women have less trust and confidence in the US government. We find similar age effects, such that after roughly age 40, trust and confidence in the US government increase, all else being equal.

On the other hand, trust in internet interactions peaks at roughly age 54; however, the decline before and after is slight. We find that individuals with higher income are more trusting of interactions on the internet, controlling for other factors, but that women are slightly less trusting of internet interactions than men.

4.3 H2: Prior Imposter Fraud Experience is Associated with Greater Distrust of Legitimate and Fake Communications

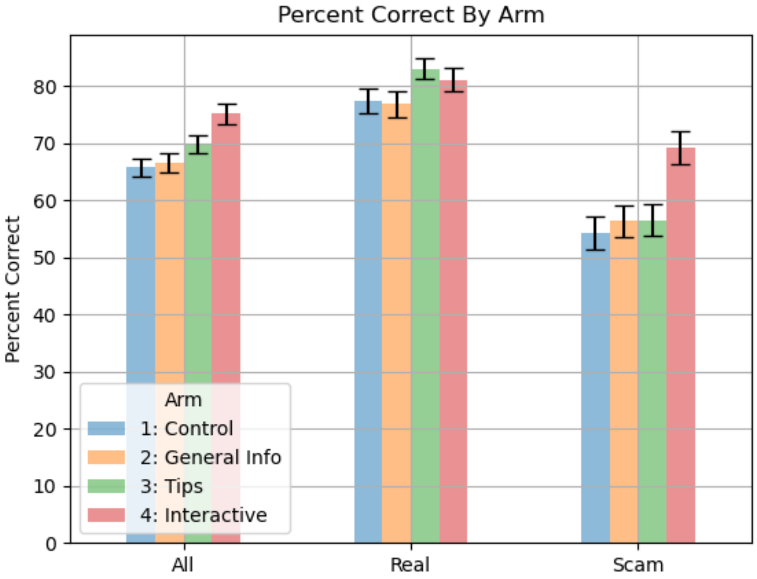
We do not find evidence that fraud victimization (losing money) or exposure (being targeted by scammers) is related to distrust across a range of metrics. There is no statistically significant relationship between each of the three dependent variables (fraud exposure, loss of money, and amount of money lost) and total distrust (total number of messages flagged as fraudulent), "rightful" distrust (total number of fraudulent messages flagged as fraudulent), and "undue" distrust (total number of true messages flagged as fraudulent). The results, while not supportive of our hypothesis, are again good news for citizen engagement with the government.

When we disaggregate fraud exposure to look specifically at business fraud, we do find a significant negative relationship (coef=-0.24; SE=0.11; p=0.026) which follows the intriguing, but inconsistent results presented previously on distrust linked to business fraud.

4.4 H3(A): The Interactive Training Will Improve Participants' Accuracy of Discerning Legitimate and Fake Communications Relative to the Static Training And Control Conditions

Participants in the interactive training show a causal increase in their fraud-detection abilities, as shown in Figure 4. They were more accurate in correctly identifying communications across all three control arms. These results are driven specifically by an increase in correctly identifying scams and less so in correctly identifying real messages. The interactive training shows a substantial 12.8 percent increase in fraud-detection abilities versus Arm 2 (fraud awareness-raising information) and 12.7 percent versus Arm 3 (non-interactive fraud detection tips). Both results are statistically significant (p=0.000; after Holm correction for multiple tests). The interactive training increases the ability to identify real messages by 4.3 percent versus Arm 2; it shows no statistically significant effect relative to Arm 3 and indeed shows a slightly lower, non-significant effect.

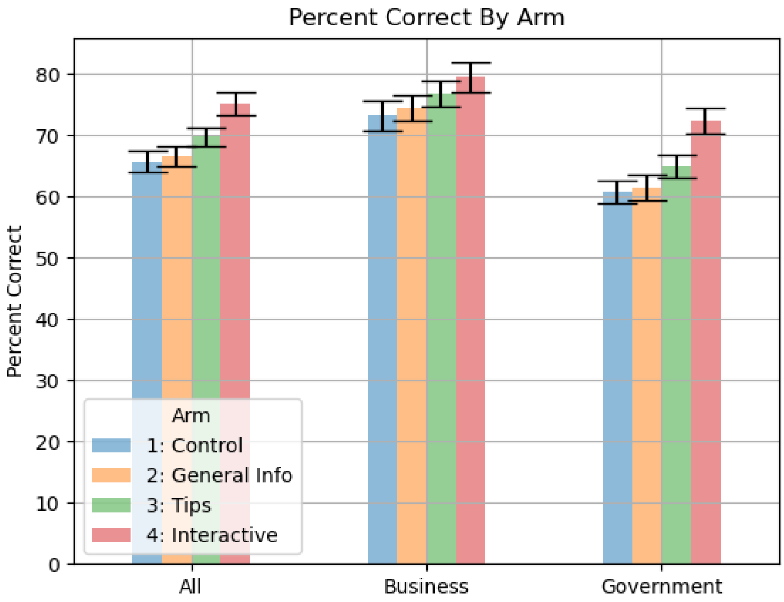
Figure 4: Differences in fraud detection accuracy for real and fake communications across four conditions



The interactive training also shows a causal improvement in fraud-detecting behavior (i.e., the actions that help people avoid scams). Interactive-training participants opened 1.1 more email headers on average (from a baseline of 1.4 and out of a total maximum of four; p=0.000); the non-interactive fraud detection tips (Arm 3) increased email open behavior by 0.53 (p=0.000). The interactive training beneficially decreased the number of links clicked in the mocked-up email and website communications (coef=-0.1; p=0.01); the non-interactive fraud detection tips had no effect on link clicks.

Importantly, we see that the experimental effect is primarily, but not exclusively, driven by teaching people to correctly identify government communications rather than business communications, as shown in Figure 5.

Figure 5: Differences in fraud detection accuracy for business and government communications across four conditions



4.5 H3(B): The Effect of the Intervention Will Be Consistent for Those Who Have and Have Not Been Victimized by an Imposter Scam

We find support for Hypothesis 3(B). When we include an interaction term to test for a differential impact of the training on participants who have been exposed to fraud, the baseline experimental effect remains, there is no differential impact by prior fraud exposure. The same results hold for exposure specifically to SSA fraud and fraud victimization (the loss of money to fraud). The effect does indeed appear to be consistent across groups.

4.6 H4: The Interactive Training Does Not Increase Distrust of Legitimate Communications Relative to the Static Training and Control Conditions

When we examine “undue distrust” – the flagging of real messages as fraudulent by the participants – we do not see any increase in distrust, which supports Hypothesis 4. On the contrary, both the interactive training and non-interactive fraud detection tips decrease “undue distrust,” as shown in Table 4.

Table 4: Effects of the training program on undue distrust

	Coef.	Std. Error	T-Value	P>|t|
Intercept (Arm 1 – Control Information)	22.5658	1.042	21.651	0.000
Arm 2: General Info on Gov’t Trust	0.3201	1.481	0.216	0.829
Arm 3: Static Fraud Detection Tips	-5.6887	1.478	-3.850	0.000
Arm 4: Interactive Training	-3.7342	1.490	-2.506	0.012

It is notable that the non-interactive tips showed a slightly larger effect than the interactive training. When we examine the time-delayed study, however, only the effect of the interactive training remains after a median wait time of 19 days (coef=-5.1; SE=1.63; p=0.002); that of the non-interactive tips fades into insignificance (p=0.822).

4.7 H5: The Interactive Training Will Have a Greater Effect on Discrimination Accuracy for Older Participants and Those Who Engage Less Frequently in Online Shopping Relative to Younger Participants and Participants Who Are More Frequent Online Shoppers

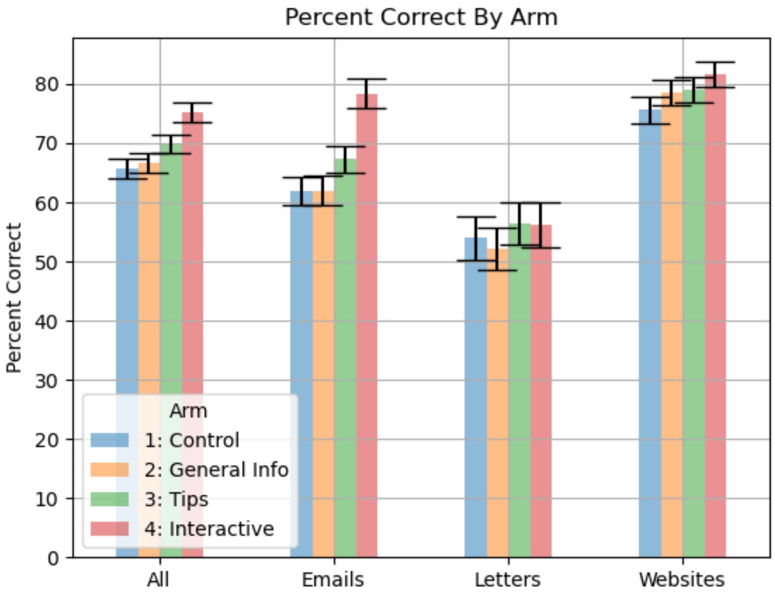
With an interaction term to test for a differential impact of the training on the total percent of correct messages by age and online shopping frequency, we find no differential impact. The impact of the interactive training is consistent. Based on these findings, we do not find support for H5.

4.8 H6: The Effect of the Interactive Training Does Not Port to Better Fraud Detection Accuracy for Non-Digital Solicitations (I.E., Postal Letters)

We used mock websites and email communications in the training program. In the assessment, we added two letters: one real and one fraudulent. As shown in Figure 6, participants who completed the interactive training were no more accurate at discriminating between real and fake letters than participants in the control arms, suggesting that the training does not help people detect that form of fraud. Letters also had the poorest accuracy overall (54 percent correct in control Arm 1).

Overall, the training is far more effective for emails than for websites: a 16.4 percent increase over Arm 2 for emails compared to a 3.0 percent increase in accuracy (relative to Arm 2) for websites. The interactive training was not significantly better than the non-interactive tips at improving accuracy for websites (change in coef=2.63; p=0.090) but was for emails (change in coef=11.1; p=0.000).

Figure 6: Fraud detection accuracy by type of communication across four conditions



4.9 H7: The Effect of the Interactive Training Will Diminish After a Two-Week Delay

In support of hypothesis 7, we find that the impact of the training on overall accuracy diminishes by half over a median delay of 19 days. As noted above, the interactive training boosted accuracy by 8.6 percent (p=0.000) in the immediate assessment and increased accuracy by 4.7 percent (p=0.001) after the delay.

We find that the decreased experimental effect is driven specifically by a decrease in scam detection: it attenuates from a 12.8 percent increase in the immediate assessment to a 4.85 percent impact (p=0.02). The effect on real-message detection is largely unchanged by time, with a boost of 4.3 percent in the immediate assessment (p=0.006) and 4.6 percent after the delay period (p=0.004). That is indeed encouraging as the training provides an effect of boosting trust in real messages that endures over moderate time periods, even if the fraud-detection abilities fade.

After the time delay, the beneficial impact of the training is concentrated in emails and in government communications. We do not see an effect for websites or for business communications as we saw for the immediate assessment as well.

In terms of the non-interactive training (Arm 3), we find that it loses all of its statistically significant effects in overall accuracy, identifying scams and real messages, emails and websites, and government and business communications. Thus, although the impact of the interactive training does decrease, the non-interactive fraud detection tips provide no enduring value in this study.

4.10 R1: Who is Most Susceptible to Losing Money in an Imposter Scam?

We can examine susceptibility in two ways: revealed susceptibility on our assessment and self-reported loss to scams via the survey. Within the Primary Sample (from Prolific), we find that, on average, women were more susceptible to scams on our assessment (coeff=4.8 percent more scams labeled as real; SE=1.4; p=0.001) and that both younger and older people were more likely than mid-life participants to be susceptible. The "best" at detecting scams were people aged 49, 7.7 percent better than participants aged 20 and 8.5 percent better than participants aged 80. We see no clear relationship between self-reported loss to scams (binary loss or amount lost) based on the survey data. The divergence between these two measures is interesting and warrants further research.

4.11 R2: Who Reports Fraud to Public Sources, Such as the Better Business Bureau?

Looking at who stated that they reported fraud to public sources, we find two relationships of interest within the Primary Sample from Prolific. First, using a logistic regression for reporting behavior, people who lose money to fraud are more likely to report it – not surprisingly.[7] In addition, reporting behavior changes with age (all else being equal) and fits a quadratic pattern: peaking at age 54. Gender, income, education, and employment status do not appear as statistically significant factors.

[7] The log of the amount loss to fraud is statistically significant (coeff=0.21; SE=0.46 p=0.000).

5. Discussion

5.1 Effects of Prior Imposter Fraud on Trust

We hypothesized that those who previously experienced an imposter scam would have lower trust in the SSA, lower trust in internet transactions, and lower confidence in the US government. We also hypothesized that compared to non-victims, prior fraud victims would demonstrate lower revealed trust in their judgments of the legitimacy of mock communications developed for the experiment. Fortunately, we did not find that those who reported imposter fraud victimization were more distrustful of the SSA or the federal government compared to non-victims, and there were no significant differences between victims and non-victims in revealed trust. We do see some relationship between trust in online transactions and prior fraud, but the results are inconsistent across measures.

Overall, these findings may suggest that any impact of imposter fraud victimization on subsequent trust is minimal or short-lived. Alternatively, imposter scam victims may have had higher levels of trust than non-victims before they experienced fraud, perhaps increasing their susceptibility, but then trust was reduced to the same levels as non-victims as a result of the scam. Such a precise effect is unlikely but cannot be ruled out. Longitudinal data are needed to determine whether there were mean differences in pre-fraud trust between the former victims and non-victims in our study samples.

In general, we find that trust is multi-faceted and that different factors may drive trust in the internet versus the SSA or the federal government. Like Tolbert and Mossberger (2006), we find that trust is mainly a function of other factors, such as age, gender, education, and income. All else being equal, women appear to have less trust in each area measured. Age is positively associated with greater trust in the SSA and confidence in the government, but age is not linearly associated with trust in the internet. We also find that people who score highly on a loneliness scale are significantly more likely to distrust the SSA. Prior research has also demonstrated a link between loneliness and lower interpersonal trust (see Rotenberg 1994), with some research indicating that low trust actually promotes loneliness through increased social disengagement (Rotenberg et al. 2010). Additional research is needed to further understand the mechanisms between lower trust in the SSA and interpersonal loneliness.

5.2 Effects of Interactive Training on Increasing Trust in Legitimate Communications

Our experimental findings indicate that interactive fraud detection training can help consumers discriminate between real and fraudulent online communications from both government agencies and retailers and that, as hypothesized, the effect of training is no greater for those who have experienced imposter fraud than those who have not. We find that training is best at helping consumers correctly discern and label fraudulent communications as fake, rather than correctly label legitimate communications as real, although there is an effect for legitimate communications as well. The fraud-detection effect diminishes with time, and the detection of legitimate messages did not substantially decrease during the period. An earlier experimental study by Sheibe and colleagues (2014) similarly found that the protective effects (of forewarning consumers about a specific fraud) decline after a four-week delay.

One possible explanation for why accuracy was higher for fraudulent communications is that the interactive tips focused primarily on the signs that indicate a solicitation is fake, such as alterations to a company's URL or disguising the sender’s email address. There were relatively few tips on the indicators that a message is legitimate. Future training programs may seek to incorporate additional tips on the indicators of authenticity; however, clever fraud perpetrators can exploit those indicators by ensuring their messages look and feel as close to the legitimate sources as possible, such as by using perfect grammar and veiling any requests for information or payment.

We find that the interactive training is mainly helpful for email fraud detection and is less beneficial for websites. The interactive training incorporated images to demonstrate actions like expanding email headers to examine the “reply to” email address, whereas the written fraud detection tips (Arm 3) only described this action with words. To detect a fraudulent website, there are no expandable headers for users to investigate, and it is possible that the written tips on inspecting the URL are sufficient. It is noteworthy that the non-interactive training, which employed the sample lessons but in a simple textual form, does provide a lesser but statistically significant benefit and requires no special platform for deployment. Unfortunately, the effect of the non-interactive training completely dissipated after the delay period; thus, timely action is needed.

Results show a stronger training effect for government communication than for business communications and that overall accuracy was higher for business communications than for government communications. One explanation is that consumers may have more existing expertise in assessing the legitimacy of emails, websites, and letters associated with businesses than they do for communications from government agencies. When inspecting business emails and websites, consumers may pay attention to other salient aspects that were not highlighted in the training, such as product reviews and whether they have an existing business relationship with the company. It is important to note that this effect may also be caused by the quality of the training materials; the "government" training materials could have been systematically more effective than the "business" training materials.

We added two mocked-up letters to the assessment part of the experiment to determine whether digital fraud detection training has an effect on non-digital forms of communication. As hypothesized, those in the interactive and written training conditions (Arms 4 and 3) were no more accurate than those control conditions at labeling the real and fake letters. In other words, the training did not port to novel, non-digital forms of communication. Importantly, participants demonstrated relatively poorer fraud detection accuracy for letters, suggesting that the SSA and other organizations should carefully consider the use of the mail when corresponding with consumers.

5.3 Limitations

This study used an experimental design embedded into an online research program to assess the impact of interactive fraud detection training on participants' ability to correctly discern real and fraudulent government and business communications. Effects may differ if the training was delivered outside of a research context, used mock emails or websites from different government agencies or companies, or if it was provided immediately after a participant experiences attempted fraud. Similarly, the relationships between imposter fraud victimization and subsequent measures of trust may diminish over time. Future studies should assess trust immediately following victimization.

Another limitation is that fraud exposure is so widespread and universal that we cannot effectively assess the impact of mere exposure on trust (93 percent reported being targeted for at least one type of fraud at any point in the past). Lastly, the response rate among consumers who reported an imposter scam to the BBB’s Scam Tracker website was low. These participants are not representative of the broader US population that is exposed to imposter scams, and from the Prolific respondents in that they are 20 percent more often female, 11 years older on average, and less skilled at detecting fraud. It is possible that those who reported fraud to Scam Tracker and who responded to our study invitation experienced relatively more severe scams compared to the Prolific respondents who indicated losing money in a prior scam.

6. Conclusion

This research project began with the concern that widespread impersonation scams would undermine the trust of citizens in their government, and especially in the Social Security Administration. Contrary to our hypotheses, that does not appear to be the case. That is welcome news. We do see some signs of distrust arising from impersonation scams in the private sector that warrant further attention, however.

Side by side with that concern was the hope that people could be trained to identify real and fraudulent communications across a variety of settings and communication mechanisms. Building on our prior research in this area (Robb & Wendel 2022), we find that, indeed, people can be trained to more accurately categorize communications. In particular, it appears to be easier to train people to identify scams than it is to train them to trust legitimate communications – though we saw an effect for both. In addition, it appears easier to train people to correctly identify emails as fraudulent than websites, and the effects of each do not necessarily port over to other communication mediums like letters.

Experimental research into fraud susceptibility and techniques to decrease that susceptibility are still quite nascent, however. This study could include only twelve sample communications in its assessment of susceptibility and the impact of the training program. These twelve are based on real communications and scams but are only one small part of the, unfortunately, growing and evolving body of techniques that scammers use to trick the public. Even if their efforts do not appear to be undermining public trust in the government, they cost Americans in terms of their time, money, and peace of mind. To say that more research is needed to counter these losses is certainly an understatement.

7. References

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. International business review, 26(1), 164-175.

Bäck, M., & Christensen, H. S. (2016). When trust matters—a multilevel analysis of the effect of generalized trust on political participation in 25 European democracies. *Journal of Civil Society*, *12*(2), 178-197.

Bailey, J., Taylor, L., Kingston, P., & Watts, G. (2020). Older adults and "scams": Evidence from the Mass Observation Archive. Journal of Adult Protection, 23(1), 57-69. https://doi.org/10.1108/ JAP-07-2020-0030

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The journal of strategic information systems*, *17*(2), 165-176.

Beldad, A., van der Geest, T., de Jong, M., & Steehouder, M. (2012). A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly*, *29*(1), 41-49.

Bjørnskov, C. (2012). How does social trust affect economic growth?. *Southern Economic Journal*, *78*(4), 1346-1368.

Brenner, L., Meyll, T., Stolper, O., & Walter, A. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology*, *76*, 102243.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. Decision Support Systems, 83, 47-56.

Chanley, V. A., Rudolph, T. J., & Rahn, W. M. (2000). The origins and consequences of public trust in government: A time series analysis. *Public opinion quarterly*, *64*(3), 239-256.

DeLiema, M, & Witt, P. (2021). Mixed methods analysis of consumer fraud reports of the Social Security Administration impostor scam. WP2021-434. https://dx.doi.org/10.7302/4195

Federal Trade Commission. (2022). Consumer Sentinel Network Data Book 2021. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021

Figueroa, C. (2019). The Pallone-Thune" TRACED Act": Expanding Consumer Protection in the Fight against Robocalls. *Loy. Consumer L. Rev.*, *32*, 318.

Goel, R. K. (2021). Masquerading the government: Drivers of government impersonation fraud. *Public Finance Review*, *49*(4), 548-572.

Gurun, U. G., Stoffman, N., & Yonker, S. E. (2018). Trust busting: The effect of fraud on investor behavior. *The Review of Financial Studies*, *31*(4), 1341-1376.

Hardin, R. 2002. Trust and Trustworthiness. New York: Russell Sage Foundation.

Harris, E., Petrovits, C., & Yetman, M. (2022). Spreading the news: Donor response to disclosures about nonprofit fraud and efforts to rebuild trust. Available at SSRN: https://ssrn.com/abstract=3021543 or http://dx.doi.org/10.2139/ssrn.3021543

Hoogh, M., & Marien, S. (2013). A comparative analysis of the relation between political trust and forms of political participation in Europe. *European Societies*, *15*(1), 131-152.

Hsu, M. H., Chuang, L. W., & Hsu, C. S. (2014). Understanding online shopping intention: the roles of four types of trust and their antecedents. *Internet research*.

Hughes, M. E., Waite, L. J., Hawkley, L. C., & Cacioppo, J. T. (2004). A short scale for measuring loneliness in large surveys: Results from two population-based studies. *Research on aging*, *26*(6), 655-672.

Internal Revenue Service (2021). Returns Filed, Taxes Collected & Refunds Issued Available at https://www.irs.gov/statistics/returns-filed-taxes-collected-and-refunds-issued#:~:text=The%20IRS%20processed%20more%20than,78%20percent%20of%20all%20filing.

Kim, Y., & Peterson, R. A. (2017). A Meta-analysis of Online Trust Relationships in E-commerce. *Journal of interactive marketing*, *38*, 44-54.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information systems research, 13(3), 334-359.

Mutz, D. C. (2009). Effects of Internet commerce on social trust. *Public Opinion Quarterly*, *73*(3), 439-461.

Robb, C.A., Wendel, S (2022). Who Can You Trust? Assessing Vulnerability to Digital Imposter Scams. Under review for publication.

Rotenberg, K. J. (1994). Loneliness and interpersonal trust. Journal of social and clinical psychology, 13(2), 152-173.

Rotenberg, K. J., Addis, N., Betts, L. R., Corrigan, A., Fox, C., Hobson, Z., ... & Boulton, M. J. (2010). The relation between trust beliefs and loneliness during early childhood, middle childhood, and adulthood. *Personality and Social Psychology Bulletin, 36*(8), 1086-1100.

Rofiq, A. (2012). Impact of cyber fraud and trust of e-commerce System on purchasing intentions: Analyzing Planned Behaviour in Indonesian Business, PhD thesis, Faculty of Business and Law of the University of Southern Queensland.

Rotenberg, K. J. (1994). Loneliness and interpersonal trust. *Journal of Social and Clinical Psychology*, *13*(2), 152-173.

Rotenberg, K. J., Addis, N., Betts, L. R., Corrigan, A., Fox, C., Hobson, Z., ... & Boulton, M. J. (2010). The relation between trust beliefs and loneliness during early childhood, middle childhood, and adulthood. *Personality and Social Psychology Bulletin*, *36*(8), 1086-1100.

SimplyWise. (2021). SimplyWise Retirement Confidence Index January 2021. https://www.simplywise.com/blog/retirement-confidence-index/.

Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and applied social psychology*, *36*(3), 272-279.

Smith, A. & Anderson, M. (2016). Online shopping and e-commerce. Pew Research Center. https://www.pewresearch.org/internet/2016/12/19/online-shopping-and-e-commerce/

Tolbert, C. J., & Mossberger, K. (2006). The effects of e -government o government. *Public Administration review*, *66*(3), 354-369.

United States Census Bureau (2022). Quarterly Retail E-Commerce Sales (2022). https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Van Dijke, M., & Verboon, P. (2010). Trust in authorities as a boundary condition to procedural fairness effects on tax compliance. *Journal of Economic Psychology*, *31*(1), 80-91.

West, D. M. (2004). E -government and the attitudes. *Public administration review*, *64*(1), 15-27.

Zak, P. J., & Knack, S. (2001). Trust and growth. *The Economic Journal*, *111*(470), 295-321.

Center for Financial Security

School of Human Ecology
University of Wisconsin-Madison

1300 Linden Drive
Madison, WI 53706

608-890-0229
cfs@mailplus.wisc.edu
cfs.wisc.edu

The Center for Financial Security's Working Papers are available at *cfs.wisc.edu/publications-papers.htm*