THE GERONTOLOGICAL SOCIETY OF AMERICA®

Journals of Gerontology: Psychological Sciences
cite as: *J Gerontol B Psychol Sci Soc Sci*, 2020, Vol. 75, No. 3, 522–533
doi:10.1093/geronb/gby036
Advance Access publication April 13, 2018

OXFORD

Original Research Report

Uncovering Susceptibility Risk to Online Deception in Aging

Natalie C. Ebner, PhD,[1,2,3,4] Donovan M. Ellis, BS,[1] Tian Lin, PhD,[1] Harold A. Rocha, BS,[1] Huizi Yang, MS,[5] Sandeep Dommaraju, MS,[5] Adam Soliman, BS,[5] Damon L. Woodard, PhD,[4,5] Gary R. Turner, PhD,[6] R. Nathan Spreng, PhD,[7,8] and Daniela S. Oliveira, PhD[4,5]

[1]Department of Psychology, [2]Department of Aging and Geriatric Research, Institute on Aging, [3]Center for Cognitive Aging and Memory, Department of Clinical and Health Psychology, [4]Florida Institute for Cybersecurity Research, and [5]Department of Electrical and Computer Engineering, University of Florida, Gainesville. [6]Department of Psychology, York University, Toronto, ON, Canada. [7]Laboratory of Brain and Cognition, Montreal Neurological Institute, Department of Neurology and Neurosurgery, McGill University, Montreal, QC, Canada. [8]Human Neuroscience Institute, Department of Human Development, Cornell University, Ithaca, NY.

Address correspondence to: Natalie C. Ebner, PhD, Department of Psychology, University of Florida, PO Box 112250, Gainesville, FL 32611. E-mail: natalie.ebner@ufl.edu.

Received: September 28, 2017; Editorial Decision Date: March 12, 2018

Decision Editor: Bob G. Knight, PhD

Abstract

Objectives: Fraud in the aged is an emerging public health problem. An increasingly common form of deception is conducted online. However, identification of cognitive and socioemotional risk factors has not been undertaken yet. In this endeavor, this study extended previous work suggesting age effects on susceptibility to online deception.

Methods: Susceptibility was operationalized as clicking on the link in simulated spear-phishing emails that young (18–37 years), young-old (62–74 years), and middle-old (75–89 years) Internet users received, without knowing that the emails were part of the study. Participants also indicated for a set of spear-phishing emails how likely they would click on the embedded link (susceptibility awareness) and completed cognitive and socioemotional measures to determine susceptibility risk profiles.

Results: Higher susceptibility was associated with lower short-term episodic memory in middle-old users and with lower positive affect in young-old and middle-old users. Greater susceptibility awareness was associated with better verbal fluency in middle-old users and with greater positive affect in young and middle-old users.

Discussion: Short-term memory, verbal fluency, and positive affect in middle-old age may contribute to resilience against online spear-phishing attacks. These results inform mechanisms of online fraud susceptibility and real-life decision-supportive interventions toward fraud risk reduction in aging.

Keywords: Affect, Cognition, Decision making, Online, Spear phishing

Introduction

Online deception is becoming more common as individuals increasingly navigate through a digitally connected world (Anderson, 2013). Technological advances are opening up multiple avenues for online fraud. Internet users (called "users" in this article) and corporate employees have become frequent targets of online spear-phishing attacks, usually in the form of spear-phishing emails. Spear-phishing attacks attempt to lure users into visiting web pages that procure personal information or into

clicking on links to malicious downloads (Carr, 2011; Hadnagy, 2010). Spear-phishing attacks are particularly appealing because they are low-cost to attackers, do not have to occur in mass-scale to be effective, and make it complicated to attribute an attack to a particular person or group (Carr, 2011). Successful spear-phishing attacks can result in negative psychological and financial consequences for individuals. In the case where an individual's computer is leveraged for later attacks on other users and organizations, successful attacks can have devastating, wide-reaching impact on national cybersecurity. Spear phishing (the type of attack considered in this work) is different from spam (Hao, Syed, Feamster, Gray, & Krasser, 2009; Meyer & Whateley, 2004; Ramachandran, Feamster, & Vempala, 2007; Schwarz, 2004; Stone-Gross, Holz, Stringhini, & Vigna, 2011). Spear phishing is always malicious and targets one or a few individuals in a particular demographic group, for example, CEOs, older male in a particular community, etc. In contrast, spam can be malicious or benign. Spam are unsolicited and undesired email messages to advertise products, distribute malware, or attempt to lure Internet users into falling for financial scams. Spam messages are usually sent by botnets, massive networks of compromised computers, which can be rented by spammers for their campaigns. In other words, spam is sent in bulk, which makes it easier for machine learning/text matching methods to filter them out into spam folders. Once an email provider detects that a piece of message is spam (human manual analysis, user reported), it can employ automatic methods to detect that particular pattern of text in other messages. As spear phishing is not distributed in bulk form, is targeted, and can be undistinguishable from a legitimate email, phishing emails usually evade modern spam-filtering techniques.

Spear-phishing attacks and malware (malicious software) distribution via email are quite prevalent. As reported in the Symantec (2017) Internet Security Threat Report email spear phishing is one of the favorite avenues for malware distribution, with the rate of these attacks increasing. For example, in 2015, one in 220 emails sent contained malware, while in 2016 the amount increased to one in 131 emails. These statistics do not differentiate by demographic cohorts nor do they account for internet usage patterns, which would make penetration rates for malware infected emails highly variable across individuals.

Old age is the time at which retirement savings have accumulated over the course of many decades and individuals often have well-established credit. Further, older adults increasingly navigate the Internet and use networked software in their daily lives (Perrin & Duggan, 2015). Even though older adults are getting more comfortable using the Internet (Smith, 2014), many are comparatively less experienced with computers and have lower confidence in their information technology skills than young adults (Dyck & Smither, 1994; Marquié, Jourdan-Boddaert, & Huet, 2002). This, combined with reduced decision-making capacity and decreased sensitivity to deception cues in aging (Castle et al., 2012; Ruffman, Murray, Halberstadt, & Vater, 2012; but see Lichtenberg, Sugarman, Paulson, Ficker, & Rahman-Filipiak, 2016; Ross, Grossmann, & Schryer, 2014; Wood, Liu, Hanoch, & Estevez-Cores, 2016), may underlie a heightened risk for cyber fraud among older, particularly female, individuals (Oliveira et al., 2017). Importantly, adverse events from fraud in old age are associated with declines in health, including greater rates of hospitalization and long-term care admissions and higher mortality (Dong & Simon, 2013). Furthermore, older adults often occupy positions of power in organizations and politics, and thus online deception of these individuals can result in negative consequences with broad societal impact.

Notably, chronological age has been neglected in current research on social engineering attacks such as email spear phishing. We therefore recently developed the PHishing Internet Task (PHIT; Oliveira et al., 2017) to determine young and older users' susceptibility to simulated spear-phishing email attacks. This novel behavioral field experiment was conducted in participants' homes for increased ecological validity and showed a particular susceptibility to online spear-phishing attacks in older women and less awareness of online fraud susceptibility among older compared with young users. Oliveira and colleagues focused on investigating adult age differences in susceptibility to online spear phishing and on determining (general and age-differential) efficiency of weapons of influence and life domains as techniques to lure Internet users into clicking on potentially malicious links. In contrast, the present study constituted a secondary data-analytic extension of Oliveira and colleagues by exploring cognitive and socioemotional factors contributing to susceptibility risk to online deception in young and older adults, while differentiating between young-old and middle-old Internet users, as described below.

Previous epidemiological studies have identified broad demographic risk factors for fraud, including socioeconomic status, household size, and race (Peterson et al., 2014). While these factors are critical for informing broader policy and public health initiatives, they provide only marginal benefit for individual surveillance and protection efforts. Specific markers of fraud risk are needed to aid clinical and community service decision making. However, research efforts in this area are hampered by the challenge of recruiting seniors who have been victims of fraud (Spreng et al., 2017). Addressing this research gap, the present study set out to characterize risk factors associated with increased susceptibility and susceptibility awareness to online deception in aging.

Of note, the current literature has investigated deception in aging almost exclusively with regard to age-related cognitive decline (James, Boyle, & Bennett, 2014; Judges, Gallant, Yang, & Lee, 2017). Cognitive deficits have been linked to decision-making deficits and heightened deception risk in aging (Sherod et al., 2009). Fraud, however,

is, by definition, a social transaction. Thus, a link between fraud and socioemotional functioning is not surprising. Even though there are various social and affective changes documented with age (Ebner & Fischer, 2014), socioemotional contributors to decision-making processes and fraud susceptibility in aging are currently understudied (for review, see Spreng, Karlawish, & Marson, 2016).

In particular, the ability to detect negative information and untrustworthy behavior is important for identifying deception. Normal aging is associated with affective changes that dampen these socioemotional processes. There is considerable evidence that with age, attention becomes more biased toward positive relative to negative information (Reed, Chan, & Mikels, 2014). This reduced processing of negative information may lead older adults to take more risks when making decisions that involve losses (Best & Charness, 2015; Tymula, Rosenberg Belmaker, Ruderman, Glimcher, & Levy, 2013). Also, older adults showed greater self-reported trust (Li & Fung, 2013; Poulin & Haase, 2015), and higher levels of trust, in turn, were associated with a lower accurate deception detection rate in text-based online chat (Friend & Fox Hamilton, 2016).

A parallel literature suggests that positive mood may impair deception detection because of its incorporation of nonverbal cues and reliance on (possibly more shallow information processing) heuristics. Negative mood, in contrast, may enhance deception detection by increasing reliance on situation-specific, verbal cues (Forgas & East, 2008). For example, negative mood resulted in longer and greater attention to details of the communicative content of messages (Matovic, Koch, & Forgas, 2014). This line of work has, however, not yet been applied in an aging context or to online deception.

Regarding the field of cybersecurity, a current shortcoming is that it does not consider user age. In Oliveira and colleagues (2017), we demonstrated the importance of considering age in studying online fraud susceptibility. While much psychological research has focused on the impact of age-related cognitive changes on decision making, our increasing understanding of socioemotional changes with age and their impact on decision-making abilities suggests that an exclusive examination of cognitive changes may be too narrow. Thus, adopting an aging perspective, the present study set out to understand specific risk factors (cognitive, socioemotional capacity) associated with online fraud susceptibility using our newly developed PHIT, thereby going beyond the results reported in Oliveira and colleagues. In particular, the present study constituted an important first step toward uncovering susceptibility risk to online deception in aging. In line with Lichtenberg (2016), we adopted a person-centered approach and considered cognitive and socioemotional variables in our identification of risk factors for online fraud in young, young-old, and middle-old adulthood. Given the still limited knowledge on factors contributing to fraud risk, especially in the context of cybersecurity, the present study was exploratory in nature. We addressed the following two research questions: (a) Are behavioral susceptibility to online deception and awareness of online deception risk associated with cognitive and socioemotional capacities? (b) How do these associations vary with age?

Methods

Participants

Taking a differentiated approach to aging in line with considerations in gerontology (Forman, Berman, McCabe, Baim, & Wei, 1992; Zizza, Ellison, & Wernette, 2009), we captured the diversity of old age in subgroups to reflect significant late life changes, rather than aggregating across wide age ranges (Baltes & Mayer, 1999; Cicirelli, 2006). We defined young adults as ranging from 18 to 37 years, young-old adults as ranging from 62 to 74 years, and middle-old adults as ranging from 75 to 89 years. The study comprised 157 users, of which 100 were young (M = 21.7 years, SD = 4.10, 56% female, n = 8 not reported), 41 were young-old (M = 68.0 years, SD = 3.60, 49% female), and 16 were middle-old (M = 80.0 years, SD = 4.43, 31% female). We conducted the present analysis on the same sample as the one reported in Oliveira and colleagues (2017). We dropped one older man from the present sample because of missing data regarding his chronological age, thus making it impossible to categorize him into the young-old or the middle-old group. This reduced the present sample size to 157 participants as opposed to the sample size of 158 in Oliveira and colleagues.

Participants were recruited from North Central Florida through fliers and handouts disseminated throughout the community, ads in senior magazines, an established laboratory participant pool, Healthstreet (a university-affiliated community recruitment and outreach program), and through social media and online forums. We compensated young participants recruited through the University Subject Pool with course credit; all other participants received $50.

To be included in the final data analysis, participants had to complete 21 days of study sessions, check their email inbox on at least half of the days during the intervention, and respond to the final-day survey (see below for details). We applied the criterion for regular checking of their email inbox to assure that participants in fact checked their inbox several times during the study duration and thus were indeed exposed to the simulated spear-phishing emails sent by our team. Based on these criteria, 33.5% (n = 79) of the total 236 enrolled participants were excluded, with approximately equal numbers across age and gender. Supplementary Table A summarizes demographic, health, and Internet usage information of the final sample of 157 participants for the present analyses, separately for the three age groups.

Study Design, Procedures, and Measures

Before study enrollment, participants provided written informed consent. For ecological validity, we conducted the

study remotely out of the participants' homes across 21 days. University of Florida IRB approved all study procedures.

The study started with a brief phone interview to determine study eligibility. For enrollment, participants had to be between 18 and 39 years or 60 and 90 years and engaged in online activities, such as web browsing and email checking. Daily use of the Internet was not an eligibility criterion. However, the study required participants to use their Internet on a daily basis during the 3-week study period. Recent evidence supports increasing use of the Internet among older individuals. In 2014, over half of the individuals older than 65 already used the Internet, with faster adoption rates in older individuals compared to middle-aged or young adults (Perrin & Duggan, 2015). For young-old and middle-old adults, the Telephone Interview for Cognitive Status (TICS; Brandt, Spencer, & Folstein, 1988) screened for signs of cognitive impairment (cut off score < 30).

During a second phone call, we administered the Brief Test of Adult Cognition by Telephone (BTACT; Tun & Lachman, 2006). The BTACT is a 30-min test battery, sensitive to cognitive status in normal aging, comprising the following subtests: (a) total number of digits correctly produced in *backward counting* measured speed of processing; (b) highest number of digits reached in *digit backward recall* measured working memory span; (c) total number of unique correct responses in *category fluency* measured verbal fluency; (d) total number of unique correct responses in *immediate and delayed word list recall* measured short- and long-term episodic verbal memory, respectively, and (e) total number of correct items in *number series* measured inductive reasoning. We excluded the *stop and go task* from the present analyses, as standard administration requires audio recording of the responses to determine latency times, which was not implemented in our study. Table 1 presents descriptive information and age-group differences in these subtests.

At the start of each study day, participants completed the short Positive and Negative Affect Schedule (PANAS; Watson, Clark, & Tellegen, 1988), to assess their daily mood via an online link. Participants used a scale from 1 = *very slightly or not at all* to 5 = *extremely* to evaluate a list of adjectives (e.g., *excited, happy, afraid, alert*; 13 positive and 13 negative mood items). We calculated the averages of these means for positive affect items and negative affect items for each participant to indicate positive affect and negative affect, respectively (Table 1). Cronbach's alpha was .98 for positive affect and .98 for negative affect.

Participants completed the PHIT (Figure 1) by engaging in 1 hr of Internet browsing every day, which included approximately 15 min of (a) reading an informative source of their choice (e.g., news media websites); (b) reading entertainment/social network sources (e.g., entertainment websites or social media); (c) engaging in unstructured browsing; and (d) checking emails from the account they registered for the study. Unbeknownst to participants, the study team sent 21 simulated spear-phishing emails containing links, one a day, over the study period. These simulated spear-phishing emails were based on theoretical and empirical considerations pertaining to the use of specific techniques to lure Internet users into procuring personal information or into clicking on links to malicious downloads (Carr, 2011; Hadnagy, 2010; see Oliveira et al., 2017 for details). These emails were modeled after a large set of real-life emails that we had collected as part of a pilot study from an independent sample of young and older adults. We used none of the actual real-life emails in the study. The email links directed participants to harmless, static web pages created by our team. These fake web pages never asked for personal information and were all associated with fictitious people and institutions. The specific email sent and the time it was sent during the participant's browsing session were chosen randomly.

Table 1. Means (Standard Deviations) and Age-Group Differences in Cognitive and Socioemotional Measures

	Young	Young-old	Middle-old	*F* Value	*p* Value
Cognitive measures					
Backward counting[a,b,c]	49.17 (11.20)	41.00 (9.96)	32.63 (16.09)	18.02	**<.001**
Backward digit span	4.61 (1.42)	4.41 (1.50)	3.81 (1.64)	2.11	.125
Category fluency[a]	21.99 (5.39)	19.56 (4.89)	20.13 (4.72)	3.40	**.036**
Delayed word list recall[a,b]	5.91 (2.50)	4.49 (2.65)	4.25 (1.98)	6.33	**.002**
Immediate word list recall[b]	7.77 (2.06)	6.87 (2.32)	6.00 (1.55)	6.34	**.002**
Number series[a,b]	3.82 (1.18)	2.92 (1.38)	2.94 (1.65)	8.41	**<.001**
Socioemotional measures					
Positive affect[b]	2.58 (0.78)	2.84 (0.84)	3.19 (0.80)	4.68	**.011**
Negative affect[a,b]	1.51 (0.52)	1.21 (0.28)	1.13 (0.18)	10.18	**<.001**
Trust	2.63 (0.34)	2.64 (0.43)	2.55 (0.44)	0.32	.728

Notes. Of the 157 participants used in the present analyses, cognitive measures were missing for two young and two young-old users. The trust measure was missing for 10 young, 1 young-old, and 2 middle-old users. Bold indicates a significant age-group main effect at $p < .05$.

[a]Significant difference ($p < .05$) between young users and young-old users. [b]Significant difference ($p < .05$) between young users and middle-old users. [c]Significant difference ($p < .05$) between young-old users and middle-old users. Bonferroni correction for pair-wise age-group comparisons.

A browser extension installed on the participants' computers recorded all websites they visited during the study period. This recording included whether a participant clicked on a link in a simulated spear-phishing email and when the link was clicked. As shown in Table 2, the majority of participants either never clicked on a link in an email or clicked on only one email link throughout the 21-day intervention. Only a few participants clicked on more than one link. In real life, a single click on a malicious email link is sufficient to infect a user's computer with malicious software. Given this data pattern, we operationalized *susceptibility* as the clicking (vs not clicking; dichotomous variable) on the link provided in each of the spear-phishing emails, indicating that the user would have fallen for the attack had it occurred in real life.

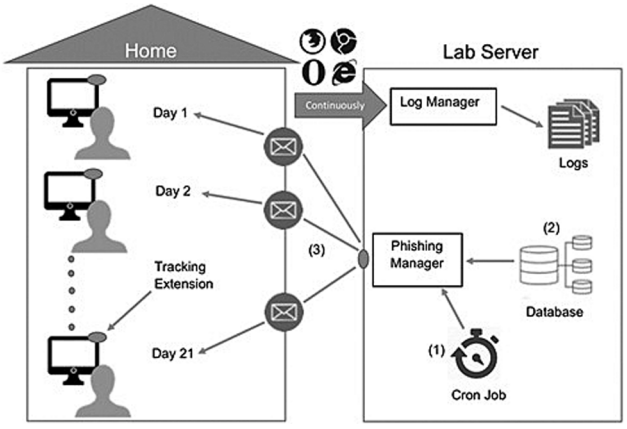

Figure 1. PHIT study framework. Special software (cron-jobs) invoked our spear-phishing manager software module daily to (1) fetch user, schedule information, and spear-phishing email from database (2) and sent spear-phishing email to user; (3) a browser extension and a full-system behavioral extractor sent all computer events generated by the user (web links visited, timestamps, and information about software executed, files opened and network connections established) over the study course to the log manager software module, which recorded this data in log files (see "continuously" in figure).

Table 2. Frequency (Percentage) of Users by Age Group Who Did Not Click on Any, Clicked on Only One, Two, or More Than Three Simulated Spear-Phishing Email Links

Number of email links clicked	Young	Young-old	Middle-old
0	56 (56.0%)	24 (58.5%)	9 (56.3%)
1	33 (33.0%)	10 (24.4%)	6 (37.5%)
2	8 (8.0%)	4 (9.8%)	1 (6.3%)
3+	3 (3.0%)	3 (7.3%)	0 (0%)

Notes. Of the 84 spear-phishing emails used across participants in this study, links in 40 spear-phishing emails were not clicked by any participant. Links in 23 spear-phishing emails were clicked by one participant, links in 8 spear-phishing emails were clicked by two participants, links in 6 spear-phishing emails were clicked by three participants, and links in 7 spear-phishing emails were clicked by at least four participants.

On the last study day, participants were provided with a complementary set of 21 spear-phishing emails that they had not seen during the study (counterbalanced across participants) and were asked to indicate how likely they would click on the link in each of these emails on a scale from 1 = *not at all* to 5 = *very much*. We used the averaged rating across the 21 emails to indicate each participant's *susceptibility awareness*, with higher scores indicating greater susceptibility awareness (i.e., higher self-reported likelihood of clicking on the link).

On that day, participants also self-reported their level of trust using the *Interpersonal Trust Measure* (ITM; Rotter, 1967). Participants also responded to Forer's Gullibility Measure (Forer, 1949) and to the Trust Inventory (Couch, Adams, & Jones, 1996). We did not analyze data from these two measures, however, given technical problems that led to significant data loss. This instrument has 25 items to assess a person's tendency to deem the statements and actions of others as truthful and reliable. The ITM comprises questions delineating between a person's predisposition to both trust and distrust others in a variety of settings and situations (e.g., "*Parents usually can be relied on to keep their promises.*"). Participants indicated their level of trusting on a scale from 1 = *strongly agree* to 5 = *strongly disagree* (Table 1). Cronbach's alpha was .80. Participants also indicated their state and trait anxiety via the State-Trait Anxiety Inventory (STAI; Spielberger, Gorsuch, Lushene, Vagg, & Jacobs, 1983) for sample descriptive purposes (Supplementary Table A).

The study closed with a debriefing about the true purpose of the experiment. Participants had the opportunity to provide feedback regarding their experiences during the study and received reimbursement.

Results

Descriptive Analysis of Susceptibility and Susceptibility Awareness

Susceptibility was dichotomous with 0 indicating that the user did not click on a link in any of the spear-phishing emails (i.e., not susceptible) and 1 indicating that the user clicked on a link in at least one of the spear-phishing emails (i.e., susceptible). Susceptibility awareness (i.e., averaged ratings across 21 emails) was continuous, with higher scores indicating greater susceptibility awareness. Table 3 shows the descriptive statistics for susceptibility and susceptibility awareness and the point-biserial correlation between these two measures in each age group. Susceptibility was not different among the three age groups [$\chi^2(2) = 0.08$, $p = .96$] while susceptibility awareness was marginally significant [$F(2, 133) = 2.51$, $p = .09$]. The two constructs susceptibility and susceptibility awareness were not significantly correlated in either of the age groups, suggesting that they constituted independent dimensions in our data.

Table 3. Descriptive Statistics and Correlations for Susceptibility and Susceptibility Awareness in Each Age Group

Age group	Susceptibility	Susceptibility awareness	*r* (*p*)
Young	44 (44.0%)	2.24 (0.86)	–.02 (.90)
Young-old	17 (41.5%)	1.89 (0.76)	–.06 (.71)
Middle-old	7 (43.8%)	1.97 (1.04)	.16 (.58)

Notes. Descriptive statistics for susceptibility reflect the frequency (percentage) of users who clicked on at least one of the simulated spear-phishing email links. Descriptive statistics for susceptibility awareness reflect the mean (standard deviation) rating of how likely (1 = *not at all* to 5 = *very much*) a user would click on a link across the 21 simulated spear-phishing emails presented to each participant during the end-of-session survey; *r* reflects the point-biserial correlation between susceptibility and susceptibility awareness.

Cognitive and Socioemotional Susceptibility Risk Factors

To explore cognitive (*Hypothesis 1a*) and socioemotional (*Hypothesis 1b*) factors contributing to susceptibility in young, young-old, and middle-old users we ran two logistic regression analyses, one for each of the functional domains. There were significant age-group differences in various cognitive and socioemotional measures (Table 1). To control for multicollinearity between these measures and age group, we removed the covariance with age for each of these measure and used the unstandardized residuals as predictors in the regression analyses. Aligning with our exploratory research approach, in a first step, we statistically considered all cognitive and socioemotional variables that we had assessed in the study.

Cognitive variables

Performance on each of the BTACT subtests (i.e., backward counting, backward digit span, category fluency, delayed word list recall, immediate word list recall, and number series), age group (1 = *young*, 2 = *young-old*, 3 = *middle-old*), and their interactions were considered as independent variables using the forward stepwise method with likelihood ratio as selection criteria to statistically determine the inclusion of factors in the final model. The final model comprised the interaction term between immediate word list recall and age group as predictors of susceptibility [Wald $\chi^2(2) = 5.72$, $p = .057$]. We conducted a follow-up logistic regression on susceptibility with performance on immediate word list recall, age group, and their interaction as independent variables to interpret this interaction. To overcome the biased estimation of standard errors because of the unbalanced sample size across our three age groups and to address the small sample size in particularly the middle-old group, we used 2,000 bootstrapped samples to estimate the confidence interval (CI) for each effect. The main effect of immediate word list recall was not significant ($B = 0.07$, CI = [–0.14, 0.29]; odds ratio = 1.07, $p = .48$). However, the effect of immediate word list recall was significantly different between young and middle-old users ($B = -1.38$, CI = [–36.43, –0.54], odds ratio = 0.25, $p = .01$), but was not significantly different between young and young-old users ($B = -0.17$, CI = [–0.67, 0.19], odds ratio = 0.90, $p = .34$). As shown in Figure 2A, middle-old users with worse immediate word list recall showed greater susceptibility. This effect was not supported in young and young-old users.

Socioemotional variables

We entered scores for positive affect, negative affect, trust, age group, and their interactions as independent variables using the same statistical procedure as for the cognitive measures. Data from 13 participants were missing for trust due to technical difficulties. The final model comprised the interaction term between positive affect and age group as predictor of susceptibility [Wald $\chi^2(2) = 5.72$, $p = .057$]. For interpretation of this interaction, we conducted a follow-up logistic regression on susceptibility with positive affect, age group, and their interaction as independent variables. We used 2,000 bootstrapped samples to estimate the CI for each effect. The main effect of positive affect was not significant ($B = 0.41$, CI = [–0.11, 1.18], odds ratio = 1.51, $p = .14$). However, the effect of positive affect on susceptibility was significantly different between young and young-old users ($B = -1.23$, CI = [–2.64, –0.34], odds ratio = 0.29, $p = .02$) and between young and middle-old users ($B = -2.34$, CI = [–75.98, –.67], odds ratio = 0.097, $p = .02$). As shown in Figure 2B, young-old and middle-old users with lower positive affect showed greater susceptibility. This effect was not supported in young users.

Cognitive and Socioemotional Factors Contributing to Susceptibility Awareness

To explore cognitive (*Hypothesis 2a*) and socioemotional (*Hypothesis 2b*) factors contributing to susceptibility awareness in young, young-old, and middle-old users we ran two linear regression analyses, one for each of the functional domains.

Cognitive variables

Performance on each of the BTACT subtasks, age group (specified by two independent/orthogonal dummy coded contrasts: young vs young-old and young vs middle-old), and their interactions constituted independent variables using the forward stepwise method to statistically determine the inclusion of factors in the final model. The final model comprised the main effect of number series [$B = -0.19$, $t(129) = -3.57$, $p = .001$, $R_p^2 = .09$], the young versus young-old contrast [$B = -0.41$, $t(129) = -2.61$, $p = .01$, $R_p^2 = .05$], and the interaction between category fluency and the young versus middle-old contrast ($B = -0.10$, $t(129) = -2.02$, $p = .045$, $R_p^2 = .03$]. Young-old compared to young users showed lower susceptibility awareness. Users

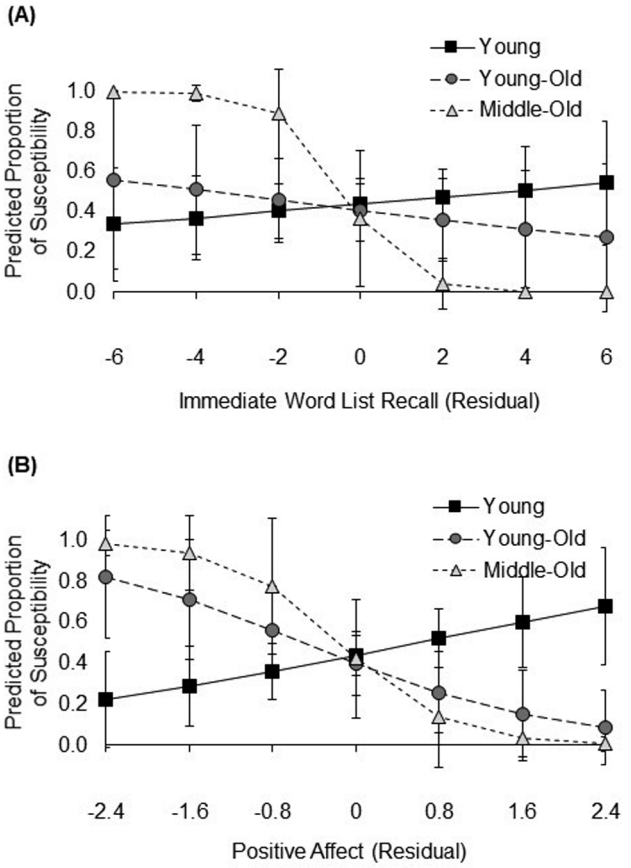

Figure 2. Predicted probability of susceptibility (dichotomous variable; 0 = *not susceptible*; 1 = *susceptible*) for (A) immediate word list recall and (B) positive affect in young (solid line), young-old (long-dashed line), and middle/old-old (dashed line) users. The *x*-axis ranged from approximately –3 to +3 *SD* for each variable. Error bars represent 95% confidence intervals.

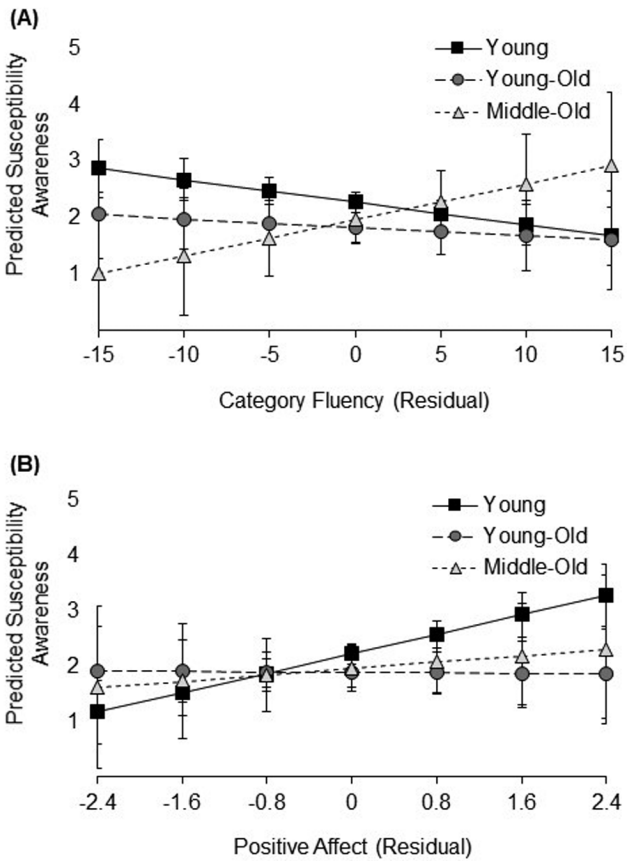

Figure 3. Predicted susceptibility awareness (continuous variable; higher scores indicate greater susceptibility awareness, that is, greater self-reported likelihood of clicking on link in spear-phishing email) for (A) category fluency and (B) positive affect in young (solid line), young-old (long-dashed line), and middle/old-old (dashed line) users. The *x*-axis ranged from approximately –3 to +3 *SD* for each variable. Error bars represent 95% confidence intervals.

with better performance on the number series test showed lower susceptibility awareness. For interpretation of the interaction, we conducted a follow-up regression on susceptibility awareness with the two age-group contrasts, category fluency, and its interactions with the two age-group contrasts as independent variables, and number series as covariate. We used 2,000 bootstrapped samples to estimate the CI for each effect. The main effect of category fluency was significant (B = –0.03, CI = [–0.05, –0.002], p = .04, R_p^2 = .03). This effect of category fluency was not different between young and young-old users (B = 0.03, CI = [–0.03, 0.08], p = .35, R_p^2 = .005). However, it was significantly different between young and middle-old users (B = 0.10, CI = [–0.04, 0.20], p = .04, R_p^2 = .04; note that the CI of this effect crossed 0). As shown in Figure 3A, young and young-old users with better category fluency showed lower susceptibility awareness, while middle-old users with better category fluency showed greater susceptibility awareness.

Socioemotional variables

We considered scores on positive affect, negative affect, trust, the two age-group contrasts, and their interactions as independent variables using the same statistical procedure as for the cognitive variables. The final model comprised the main effect of positive affect [B = 0.26, t(130) = 2.89, p = .005, R_p^2 = .06] and the interaction between positive affect and the young versus young-old contrast (B = –0.38, t(130) = –1.98, p = .050, R_p^2 = .03). For interpretation of the interaction, we conducted a follow-up regression on susceptibility awareness with the two age-group contrasts, positive affect, and its interactions with the two age-group contrasts as independent variables. We used 2,000 bootstrapped samples to estimate the CI for each effect. The effect of positive affect was significant (B = 0.28, CI = [0.10, 0.49], p = .004, R_p^2 = .08). While this effect of positive affect was not different between young and middle-old users (B = –0.30, CI = [–0.88, 0.83], p = .42, R_p^2 = .007), it was significantly different between young and young-old users (B = –0.45, CI = [–0.82, –0.09], p = .01, R_p^2 = .04). As shown in Figure 3B, young and middle-old users with greater positive affect showed greater susceptibility awareness. This effect did not hold in young-old users. Debriefing showed that 14 young, 2 young-old, and 1 middle-old adults (10.8%) were suspicious of the true study intent.

Analyses with these participants removed resulted in comparable findings.

Supplementary Material 2 presents findings from a principal component analysis for both the cognitive and the socioemotional variables. Supplementary Material 3 presents the findings when collapsing young-old and middle-old users into one group of older adults.

Discussion

Highly effective forms of fraud are conducted online. A recent study showed that current social engineering attacks in the form of spam emails adopt an age-tailored approach to deceive users (Oliveira et al., 2017). The majority of research in cybersecurity, however, ignores age. Further, research on poor decision making and age-related deficits in deception detection mostly considers age-related cognitive decline as the underlying mechanism. Socioemotional factors contributing to heightened risk susceptibility in aging are understudied. The present study advanced understanding of aging and cybersecurity by adopting an adult developmental perspective in the context of a newly developed field experiment to identify person-specific cognitive and socioemotional risk factors to online deception.

Taking a differentiated approach to aging by dissociating young-old from middle-old individuals, our study provides insight into mechanisms of online fraud susceptibility, particularly in middle-old age. Our findings suggest that greater short-term memory and verbal fluency and greater positive affect in middle-old age are associated with resilience against spear-phishing attacks. In particular, higher short-term episodic memory and higher levels of positive affect were associated with lower susceptibility in middle-old users. Furthermore, greater susceptibility awareness (i.e., greater alertness to potential risks) was associated with better verbal fluency in middle-old users and with greater positive affect in this age group, and in young users.

Our findings of effects prominent in the middle-old age cohort are in line with evidence that this age demographic constitutes a particularly vulnerable group regarding cognitive and socioemotional impairment (Singer, Verhaeghen, Ghisletta, Lindenberger, & Baltes, 2003). There are declines in positive affect in middle-old adults, and these negative affective changes appear associated with age-related situational factors such as illness, the loss of loved ones, and limited social interaction (Lichtenberg, Stickney, & Paulson, 2013), changes that may directly affect susceptibility to fraud. In contrast, young-old users showed no associations between functional levels and susceptibility to online deception. It is possible that experience (also specifically with the use of computers) in this age cohort may have counteracted some of the cognitive decline associated with susceptibility to online fraud. Declines in both fluid and crystallized capacities (Karbach & Verhaeghen, 2014) and increasing negative change in socioemotional functions in middle-old age significantly alter decision-making ability (Spreng et al., 2016), leaving low-functioning middle-old individuals vulnerable to deception.

Short-term episodic memory was associated with susceptibility to spear-phishing emails, while verbal fluency was associated with susceptibility awareness, providing evidence of cognitive functioning influencing online fraud risk. A future step will be to recruit cognitively impaired older adults, a group of individuals so far understudied in this domain of research (Lichtenberg et al., 2016), to determine their risk profiles. Unexpectedly, users with better performance on the number series test showed lower susceptibility awareness. This finding contrasts some evidence of an association between improved numeracy and lower self-reported risk for financial exploitation in community-dwelling older adults (Wood et al., 2016; see also Anderson, 2013). Discrepancies between studies (e.g., due to methodological differences like examining online vs in-person fraud, use of behavioral vs self-report measures) will have to be further explored.

None of the other cognitive processes showed significant effects. In the socioemotional domain only positive, but not negative, affect or level of trust contributed to susceptibility or susceptibility awareness. One explanation for the specificity of these results could be methodological, given the present study's small sample size, especially when stratified into three age cohorts, limiting statistical power to detect significant effects for measures that are less sensitive to age-related change. Future studies need to confirm our findings in an independent, larger sample and will have to explore alternative explanations, such as that memory and verbal fluency may be particularly relevant for detection of deception in text-based fraud. Cognitive processes like processing speed may not serve as protective factors for deception detection in general, or at least not for the specific type of cyber fraud deception prevalent in spear-phishing attacks.

The literature on deception detection suggests that affective states influence social information processing and inference of social behavior, with effects on the ability to detect deception. For example, negative mood resulted in longer and greater attention to the details of the communicative content of messages (Matovic et al., 2014). Relatedly, higher levels of anxiety decreased the truth bias (Schindler & Reinhard, 2015). This evidence from social psychology, however, is in contrast to our observation that positive affect was associated with lower susceptibility and higher susceptibility awareness, particularly in middle-old adults, and that there was no effect for negative mood. Previous studies examined young adults only. In contrast, the specific focus of our research was to shed light on susceptibility risk factors in an aging population. Our findings are in support of the idea that maintaining high positive affect in middle-old age may be part of a protective profile against online fraud in old age.

Different from previous work, we did not manipulate mood to measure its effect on deception detection. Rather, we correlated an aggregated mood score assessed via the daily survey with our real-life behavioral measure of susceptibility to online fraud. Technical unreliability with administering this survey online resulted in a significant amount of missing data. Also, our technical infrastructure recorded whether a participant visited their email inbox on a daily basis and recorded a participant's clicking on specific links, including the date for clicking on a link, but it did not record the date when a participant viewed an email and decided not to click on a link. That is why we were able to link mood with clicking on a specific email link, but we were not able to match daily mood on days participants did not to click on a link, which was the majority of the days. Thus, a day-to-day analysis of the mood–susceptibility link was not possible. Future research is warranted to determine the extent to which daily mood, also measured via fine-grained assessments of experiencing daily positive and negative events, and daily mood fluctuations predict level and fluctuations in daily susceptibility to spear phishing.

Longitudinal evidence suggests that being depressed is significantly related to fraud susceptibility (Lichtenberg et al., 2016). Also, it is possible that the level of cognitive distractibility is related to online fraud susceptibility, and may especially render older individuals more prone to falling for spear-phishing attacks. Our participants were generally healthy and we did not assess depressive mood or level of cognitive distractibility. We were, therefore, not able to determine the extent to which these variables were associated with susceptibility in our study. Further, in line with Anderson (2013), determination of the role of variables such as willingness to take risks, experience of negative life events, and other personality measures, as well as demographics like race, marital status, and financial standing on online fraud risks in aging are needed for a comprehensive examination.

We used bootstrap resampling to overcome the violation of normal distribution and violation of homogeneity of variance assumptions. This statistical approach does not allow us to overcome a possible bias in the representativeness of our sample. Especially, our young-old and middle-old individuals were likely better cognitively and physically functioning than individuals of that age in the general population, as is true in many research studies. This design feature somewhat limits the generalizability of our findings. However, our data possibly underestimate true age-group differences, given that the general population of middle-old adults is frailer than the middle-old individuals in our sample. Studying frail older adults, including early MCI and preclinical AD is an important avenue for future extension of this research (Lichtenberg, 2016).

Our study went beyond previous work in considering age and specifically contrasting young and older (young-old and middle-old) users regarding their risk factors. Despite being based on a small subgroup sample size, our data provides important first evidence suggesting that young, young-old, and middle-old users show differential susceptibility profiles. Future research will benefit from covering a continuous age sample across adulthood and even earlier life phases, like late adolescence and emerging adulthood, given that the use of the Internet is prevalent in these age groups (Perrin & Duggan, 2015). We propose to also consider age-related change in neurobiological factors such as hormonal changes (e.g., oxytocin; Ebner, Bailey, Horta, Joiner, & Chang, 2017), physiological reactivity (Denburg et al., 2007), and structural and functional change in brain regions associated with deception detection (Spreng et al., 2017). For example, Spreng and colleagues report that older adults who had been financially deceived, compared to age-matched controls who had avoided deception, showed cortical thinning in anterior insula and superior temporal gyrus/sulcus, regions implicated in affectively based decision making (Samanez-Larkin & Knutson, 2015) as well as social cognition (e.g., default network) (Andrews-Hanna, Smallwood, & Spreng, 2014). Deceived older adults also had lower functional connectivity within the salience network, and increased salience-to-default network connectivity. These findings provide crucial preliminary evidence that fraud risk may be related to altered socioemotional neurocircuitry in older adulthood. Greater functional interactions between salience and default networks suggests that exploited older adults may place greater reliance on low fidelity, and possibly misleading, social information to guide affectively based decision making, increasing susceptibility risk. It will be interesting to directly relate these brain mechanisms to older adults' susceptibility to online deception in real life.

A potential methodological limitation of the present work refers to the operationalization of susceptibility as a dichotomous variable (i.e., susceptible vs not susceptible). This measure did not reflect individual variance on the degree of susceptibility. As summarized in Table 2, only a limited number of users clicked more than one link, limiting our ability to compute a continuous measure for our analyses. While clicking once on a malicious link can already infect a user's computer (and downstream other users' computers), greater susceptibility is characterized also by more frequent clicking. Future research will need to obtain a sensitive measure of frequency of clicking, by, for example, prolonging the study period, increasing the number of simulated spear-phishing emails, and measuring browsing behavior and keystrokes on simulated malicious websites. Further, robust controls for possible alternative explanations like poorer mouse control or accidental clicking in older adults will have to be developed, even though these processes may actually underlie increased susceptibility to online fraud in real life.

As described in the text, on the last study day, participants were provided with a complementary set of 21 spear-phishing emails that they had not seen during the study (counterbalanced across participants) and were asked to

indicate how likely they would click on the link in each of these emails on a scale from 1 = *not at all* to 5 = *very much*. Participants responded to this question after completion of the 21-day intervention that measured actual behavioral susceptibility and as part of the larger debriefing procedure in which we also inquired information about how convincing and how interesting the content of the respective emails were. We did not explicitly inform participants that the emails they were presented with in the complementary set were simulated spear-phishing emails (i.e., potentially malicious emails if encountered in real life). However, it is possible that during this rating procedure triggered by the questions we asked, participants developed some ideas about the emails and did not view them entirely unbiased, as during the behavioral portion of the study. Accordingly, we interpreted high self-reported likelihood of clicking on a link when embedded in one of the simulated spear-phishing emails as reflective of high awareness that one would fall for such an attack. However, Oliveira and colleagues (2017) found no relationship between behavioral susceptibility and self-reported susceptibility awareness. Thus, future research could further explore this relationship by asking participants whether they identified specific content within an email as malicious. Our debriefing protocol kept participants blinded as to whether these could be spear-phishing emails, so we are unable to explore this distinction here. Planned studies will directly assess susceptibility awareness in relation to participant's ability to identify email content as malicious.

In conclusion, this study integrated research on age-related cognitive and socioemotional change with cybersecurity in a highly interdisciplinary fashion (see also Lichtenberg, 2016) and thus constitutes a critical first step toward a full characterization of markers associated with online fraud susceptibility in aging, including middle-old age. This work extends previous research examining decision making in aging and, more specifically, deception detection. We have introduced a significant methodological advance by conducting a behavior-based examination in a real-world context, enabling us to objectively operationalize fraud susceptibility and determine associations with risk factors. Fraud in real life happens at a low base rate. The current approach via our PHIT task constitutes an important advance in experimentally manipulating fraud and making fraud susceptibility behaviorally measurable in an ecologically valid way. Knowledge gained and methodologies developed from this research have the potential to inform future real-life decision-supportive interventions that adopt an age-targeted, individualized approach based on specific risk profiles, as opposed to a one-size-fits-all solution targeting any individual. The long-term goal is risk reduction and prevention of online fraud in older adults, and particularly those at-risk middle-old individuals with low cognitive and affective functioning, to avoid negative consequences of social engineering attacks.

Supplementary Material

Supplementary data is available at *The Journals of Gerontology, Series B: Psychological Sciences and Social Sciences* online.

Funding

This work was supported by the National Science Foundation (SES-1450624 to D. S. Oliveira and N. C. Ebner) and in part by a grant from the Elder Justice Foundation (R. N. Spreng).

Acknowledgments

The authors are grateful to research teams from the Social-Cognitive and Affective Development lab and the Florida Institute for Cybersecurity (FICS) for assistance in study implementation, data collection, and data management. D. M. Ellis and T. Lin contributed equally to this work.

Conflict of Interest

None declared.

References

Anderson, K. (2013). *Consumer Fraud in the United States, 2011. The Third FTC Survey*. Staff Report of the Bureau of Economics. Washington, DC: Federal Trade Commission.

Andrews-Hanna, J. R., Smallwood, J., & Spreng, R. N. (2014). The default network and self-generated thought: Component processes, dynamic control, and clinical relevance. *Annals of the New York Academy of Sciences*, **1316**, 29–52. doi:10.1111/nyas.12360

Baltes, P. B., & Mayer, K. U. (1999). *The Berlin aging study: Aging from 70 to 100*. P. B. Baltes & K. U. Mayer (Eds.). Cambridge: Cambridge University Press.

Best, R., & Charness, N. (2015). Age differences in the effect of framing on risky choice: A meta-analysis. *Psychology and Aging*, **30**, 688–698. doi:10.1037/a0039447

Brandt, J., Spencer, M., & Folstein, M. (1988). The telephone interview for cognitive status. *Neuropsychiatry, Neuropsychology, & Behavioral Neurology*, **1**, 111–117.

Carr, J. (2011). *Inside cyber warfare* (2nd ed.). M. Loukides (Ed.). Sebastopol: O'Reilly Media.

Castle, E., Eisenberger, N. I., Seeman, T. E., Moons, W. G., Boggero, I. A., Grinblatt, M. S., & Taylor, S. E. (2012). Neural and behavioral bases of age differences in perceptions of trust. *Proceedings of the National Academy of Sciences of United States of America*, **109**, 20848–20852. doi:10.1073/pnas.1218518109

Cicirelli, V. G. (2006). *Older adults' views on death*. New York: Springer Publishing Company.

Couch, L. L., Adams, J. M., & Jones, W. H. (1996). The assessment of trust orientation. *Journal of Personality Assessment*, **67**, 305–323. doi:10.1207/s15327752jpa6702_7

Denburg, N. L., Cole, C. A., Hernandez, M., Yamada, T. H., Tranel, D., Bechara, A., & Wallace, R. B. (2017). The orbitofrontal cortex, real-world decision making, and normal aging.

Annals of the New York Academy of Sciences, **1121**, 480–498. doi:10.1196/annals.1401.031

Dong, X., & Simon, M. A. (2013). Elder abuse as a risk factor for hospitalization in older persons. *JAMA Internal Medicine*, **173**, 911–917. doi:10.1001/jamainternmed.2013.238

Dyck, J. L., & Smither, J. A. (1994). Age differences in computer anxiety: The role of computer experience, gender and education. *Journal of Educational Computing Research*, **10**, 238–248. doi:10.2190/E79U-VCRC-EL4E-HRYV

Ebner, N. C., Bailey, P. E., Horta, M., Joiner, J. A., & Chang, S. W. C. (2017). Multidisciplinary perspective on prosociality in aging. In J. Sommerville & J. Decety (Eds.), *Frontiers in developmental science series: Social cognition development across the life span* (pp. 303–325). New York, NY, US: Routledge/Taylor & Francis Group. Retrieved from https://www.routledge.com/Social-Cognition-Development-Across-the-Life-Span/Sommerville-Decety/p/book/9781138859944

Ebner, N. C., & Fischer, H. (2014). Emotion and aging: Evidence from brain and behavior. *Frontiers in Psychology*, **5**, 996. doi:10.3389/fpsyg.2014.00996

Forer, B. R. (1949). The fallacy of personal validation: A classroom demonstration of gullibility. *Journal of Abnormal Psychology*, **44**, 118–123. doi:10.1037/h0059240

Forgas, J. P., & East, R. (2008). On being happy and gullible: Mood effects on skepticism and the detection of deception. *Journal of Experimental Social Psychology*, **44**, 1362–1367. doi:10.1016/j.jesp.2008.04.010

Forman, D. E., Berman, A. D., McCabe, C. H., Baim, D. S., & Wei, J. Y. (1992). PTCA in the elderly: The "young-old" versus the "old-old". *Journal of the American Geriatrics Society*, **40**, 19–22. doi:10.1111/j.1532-5415.1992.tb01823.x

Friend, C., & Fox Hamilton, N. (2016). Deception detection: The relationship of levels of trust and perspective taking in real-time online and offline communication environments. *Cyberpsychology, Behavior and Social Networking*, **19**, 532–537. doi:10.1089/cyber.2015.0643

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Hoboken, NJ: John Wiley & Sons.

Hao, S., Syed, N. A., Feamster, N., Gray, A. G., & Krasser, S. (2009). Detecting spammers with SNARE: Spatio-temporal network-level automatic reputation engine. In *Proceedings of the 18th Conference on USENIX Security Symposium* (pp. 101–118); August 10–14, 2009; Montreal, Canada: USENIX Association. doi:10.1145/1920261.1920287

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, **26**, 107–122. doi:10.1080/08946566.2013.821809

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, **8**, 588. doi:10.3389/fpsyg.2017.00588

Karbach, J., & Verhaeghen, P. (2014). Making working memory work: A meta-analysis of executive-control and working memory training in older adults. *Psychological Science*, **25**, 2027–2037. doi:10.1177/0956797614548725

Li, T., & Fung, H. H. (2013). Age differences in trust: An investigation across 38 countries. *The Journals of Gerontology, Series B: Psychological Sciences and Social Sciences*, **68**, 347–355. doi:10.1093/geronb/gbs072

Lichtenberg, P. A. (2016). Financial exploitation, financial capacity, and Alzheimer's disease. *The American Psychologist*, **71**, 312–320. doi:10.1037/a0040192

Lichtenberg, P. A., Stickney, L., & Paulson, D. (2013). Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist*, **36**, 132–146. doi:10.1080/07317115.2012.749323

Lichtenberg, P. A., Sugarman, M. A., Paulson, D., Ficker, L. J., & Rahman-Filipiak, A. (2016). Psychological and functional vulnerability predicts fraud cases in older adults: Results of a longitudinal study. *Clinical Gerontologist*, **39**, 48–63. doi:10.1080/07317115.2015.1101632

Marquié, J. C., Jourdan-Boddaert, L., & Huet, N. (2002). Do older adults underestimate their actual computer knowledge? *Behaviour & Information Technology*, **21**, 273–280. doi:10.1080/01449290210000020998

Matovic, D., Koch, A. S., & Forgas, J. P. (2014). Can negative mood improve language understanding? Affective influences on the ability to detect ambiguous communication. *Journal of Experimental Social Psychology*, **52**, 44–49. doi:10.1016/j.jesp.2013.12.003

Meyer, T., & Whateley, B. (2004). SpamBayes: Effective open-source, Bayesian based, email classification system. *Proceedings of the First Conference on Email and Anti-Spam (CEAS)*, **98**, 1–8.

Oliveira, D., Lin, T., Rocha, H., Ellis, D., Dommaraju, S., Yang, H., … Ebner, N. C. (2017). *An empirical analysis of weapons of influence, life domains, and demographic-targeting in modern spam—An internet user perspective*. Unpublished manuscript.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., … Ebner, N. C. (2017). Dissecting spear phishing emails: On the interplay of user age, weapons of influence, and life domains in predicting phishing susceptibility. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6412–6424) May 6–11, 2017; Denver, CO, USA: ACM Association for Computing Machinery.

Perrin, A., & Duggan, M. (2015). *Americans' internet access: 2000–2015*. Washington, DC: Pew Research Center, pp. 1–13.

Peterson, J. C., Burnes, D. P., Caccamise, P. L., Mason, A., Henderson, C. R. Jr, Wells, M. T.,…Lachs, M. S. (2014). Financial exploitation of older adults: A population-based prevalence study. *Journal of General Internal Medicine*, **29**, 1615–1623. doi:10.1007/s11606-014-2946-2

Poulin, M. J., & Haase, C. M. (2015). Growing to trust: Evidence that trust increases and sustains well-being across the life span. *Social Psychological and Personality Science*, **6**, 614–621. doi:10.1177/1948550615574301

Ramachandran, A., Feamster, N., & Vempala, S. (2007 October). Filtering spam with behavioral blacklisting. In *Proceedings of the 14th ACM conference on Computer and communications security (CCS)* (pp. 342–351); Oct 29 to Nov 2, 2007; Alexandria, VA, USA: ACM Association for Computing Machinery.

Reed, A. E., Chan, L., & Mikels, J. A. (2014). Meta-analysis of the age-related positivity effect: Age differences in preferences for positive over negative information. *Psychology and Aging*, **29**, 1–15. doi:10.1037/a0035194

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science: A Journal*

of the Association for Psychological Science, **9**, 427–442. doi:10.1177/1745691614535935

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, **35**, 651–665. doi:10.1111/j.1467-6494.1967.tb01454.x

Ruffman, T., Murray, J., Halberstadt, J., & Vater, T. (2012). Age-related differences in deception. *Psychology and Aging*, **27**, 543–549. doi:10.1037/a0023380

Samanez-Larkin, G. R., & Knutson, B. (2015). Decision making in the ageing brain: Changes in affective and motivational circuits. *Nature Reviews Neuroscience*, **16**, 278–289. doi:10.1038/nrn3917

Schindler, S., & Reinhard, M.-A. (2015). Increasing skepticism toward potential liars: Effects of existential threat on veracity judgments and the moderating role of honesty norm activation. *Frontiers in Psychology*, **6**, 1–11. doi:10.3389/fpsyg.2015.01312

Schwarz, A. (2004). *Spam Assassin: The open source solution to SPAM*. Sebastopol, CA: O'Reilly Media.

Sherod, M. G., Griffith, H. R., Copeland, J., Belue, K., Krzywanski, S., Zamrini, E. Y.,…Marson, D. C. (2009). Neurocognitive predictors of financial capacity across the dementia spectrum: Normal aging, mild cognitive impairment, and Alzheimer's disease. *Journal of the International Neuropsychological Society*, **15**, 258–267. doi:10.1017/S1355617709090365

Singer, T., Verhaeghen, P., Ghisletta, P., Lindenberger, U., & Baltes, P. B. (2003). The fate of cognition in very old age: Six-year longitudinal findings in the Berlin Aging Study (BASE). *Psychology and Aging*, **18**, 318–331. doi:10.1037/0882-7974.18.2.318

Smith, A. (2014). Older adults and technology use. Washington, DC: Pew Research Center. Retrieved January 25, 2017 from http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/

Spielberger, C. D., Gorsuch, R. L., Lushene, R., Vagg, P. R., & Jacobs, G. A. (1983). *Manual for the state-trait anxiety inventory STAI*. Palo Alto, CA: Consulting Psychologists Press.

Spreng, R. N., Cassidy, B. N., Darboh, B. S., DuPre, E., Lockrow, A. W., Setton, R., & Turner, G. R. (2017). Financial exploitation is associated with structural and functional brain differences in healthy older adults. *The Journals of Gerontology, Series A: Biological Sciences and Medical Sciences*, **72**, 1365–1368. doi:10.1093/gerona/glx051

Spreng, R. N., Karlawish, J., & Marson, D. C. (2016). Cognitive, social, and neural determinants of diminished decision-making and financial exploitation risk in aging and dementia: A review and new model. *Journal of Elder Abuse & Neglect*, **28**, 320–344. doi:10.1080/08946566.2016.1237918

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. (2011). The underground economy of spam: A Botmaster's perspective of coordinating large-scale spam campaigns. *LEET*, **11**, 4.

Symantec (2017). *Symantec internet security threat report* (Technical Report). Mountain View, CA: Symantec Corp.

Tun, P. A., & Lachman, M. E. (2006). Telephone assessment of cognitive function in adulthood: The brief test of adult cognition by telephone. *Age and Ageing*, **35**, 629–632. doi:10.1093/ageing/afl095

Tymula, A., Rosenberg Belmaker, L. A., Ruderman, L., Glimcher, P. W., & Levy, I. (2013). Like cognitive function, decision making across the life span shows profound age-related changes. *Proceedings of the National Academy of Sciences of the United States of America*, **110**, 17143–17148. doi:10.1073/pnas.1309909110

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology*, **54**, 1063–1070. Retrieved from http://psycnet.apa.org/psycinfo/1988-31508-001

Wood, S. A., Liu, P. J., Hanoch, Y., & Estevez-Cores, S. (2016). Importance of numeracy as a risk factor for elder financial exploitation in a community sample. *The Journals of Gerontology, Series B: Psychological Sciences and Social Sciences*, **71**, 978–986. doi:10.1093/geronb/gbv041

Zizza, C. A., Ellison, K. J., & Wernette, C. M. (2009). Total water intakes of community-living middle-old and oldest-old adults. *The Journals of Gerontology, Series A: Biological Sciences and Medical Sciences*, **64**, 481–486. doi:10.1093/gerona/gln045