The Scams Among Us: Who Falls Prey and Why

Yaniv Hanoch1 and Stacey Wood2
1Southampton Business School, University of Southampton, and 2Department of Psychology, Scripps College

Abstract
Not a week goes by without stories about scams appearing in popular media outlets. Given the ease with which scams can be circulated, they have become one of the most common crimes globally, inflicting high emotional, financial, and psychological tolls on millions of individuals. Despite their profound and pervasive impact, researchers know relatively little about why some individuals fall victim to scams but others remain immune to the techniques utilized by scammers to lure potential victims. For example, research thus far provides mixed results about the impact of demographic characteristics (e.g., age) as well as personality variables (e.g., risk taking) on individuals’ susceptibility to scams. Even less is known about how the nature or type of scam affects an individual’s susceptibility. Gaining a deeper understanding of these issues is the key to being able to develop preventive programs and reduce the prevalence of victimization. Here, we discuss some promising directions, existing gaps in current knowledge, and the need for decision scientists to address this important problem.

Keywords
demographic variables, fraud, individual differences, risk factors, scams, susceptibility

On April 17, 2020, Google announced that it had blocked a staggering 126 million phishing scams related to COVID-19, the disease caused by the 2019 novel coronavirus, in a single week. This was the most intense and extensive phishing attack in the company’s history (Kumaran & Lugani, 2020). Millions of other COVID-19 scams were circulating the globe, including ones that asked for donations, offered COVID-19 treatments, or promised financial refunds. The extent of COVID-19 scams, however, has only served to highlight the serious problem that scams represent. Stories about scams are a weekly occurrence in the popular media, and scams have become one of the most common crimes globally. One report estimated the financial cost of fraud to the global economy at over $5 trillion per year (Gee & Button, 2019), almost 50% higher than the 2019 U.S. budget (about $3.5 trillion). Furthermore, researchers (Modic & Anderson, 2015) have argued that the psychological and emotional impact of scams is as detrimental and pervasive as the financial impact. Indeed, a survey by the European Commission (2020) showed that 79% of scam victims have suffered emotionally, whereas only 24% have suffered financially.

Scams have several features that distinguish them from most, if not all, other crimes. The perpetrators can be—and often are—located far away from their potential victims. Also, potential victims must play an active role in the process: They provide personal information, send money, keep the activity secret, and fail to report it to the authorities. In fact, without the victims’ involvement, most scams would simply fail. Thus, although there is a large scope for researchers to examine the underlying mechanisms involved in individuals’ engagement with and adherence to scammers’ requests and demands, there is a paucity of data on the topic. For example, relatively little is known about why some individuals fall victim to scams but others remain resilient, what types of preventive programs are effective, how reporting of scams to the authorities can be increased, and what types of strategies scammers use to lure potential victims and keep them engaged. There

Corresponding Author:
Yaniv Hanoch, Southampton Business School, University of Southampton
E-mail: y.hanoch@soton.ac.uk
is, at the same time, promising research that could help shed light on these key questions and pave the road for future research.

Several conceptual frameworks might be helpful in better understanding susceptibility to scams. Jones et al. (2019) have maintained that susceptibility to scams is driven by three complementary but independent factors: (a) the persuasive techniques employed by the sender, (b) the information processing of the user, and (c) individual differences. This idea resonates well with Simon’s (1990) argument that decision making is “shaped by a scissors whose blades are the structure of task environments and the computational capabilities of the actor” (p. 7). These insights suggest the need to investigate the environment in which the decision maker operates as well as the decision maker. In other words, researchers must examine a wide range of individuals’ traits and abilities—such as cognitive, demographic, emotional, motivational, and personality characteristics—as well as the characteristics of the scams—such as their use of principles of persuasion (e.g., authority). Following this framework, we divide this review into three sections. First, we summarize the demographic characteristics that are linked to victimhood; next, we review the link between individual-difference measures and susceptibility to scams; and finally, we discuss the techniques scammers employ in their attempt to bait potential victims.2

**Demographic Characteristics and Susceptibility to Scams**

The New York Times has published several stories focusing on old age and fraud (e.g., Ellin, 2019), and it is not the only outlet to advance the idea that age is one of the key demographic factors linked to fraud. Indeed, this idea has become a common stereotype. The question is whether the data support this intuition. The answer, it turns out, is complex. For example, several studies have found that older adults (65 years old and over) are not only more likely to be targeted by fraudsters (Burnes et al., 2017; Lichtenberg et al., 2016) but also more likely to become victims (James et al., 2014). Other investigations, in contrast, have found that older adults face a reduced risk of becoming a victim compared with middle-aged adults (Anderson, 2019; Office for National Statistics, 2016; Titus et al., 1995).

It is possible that young, middle-aged, and older adults respond differently to different types of scams (e.g., medical vs. financial), and there is a lack of reliable data on actual rates of victimhood (Shao et al., 2019). In fact, a growing body of evidence suggests that middle-aged adults are the age group with the highest rate of victimization (Office for National Statistics, 2016). Focusing on scams related to COVID-19, a report by the Federal Trade Commission (2021) found that adults between the ages of 30 and 39 reported the highest number of COVID-19 fraud complaints, a finding that roughly matches Anderson’s (2019) report that individuals ages 35 through 44 were most likely to report falling victim to mass-marketing solicitations (see also Titus et al., 1995). Drawing on longitudinal data from the Health and Retirement Study (of individuals 50 years old and over), DeLiema and colleagues (2020) found that age was negatively associated with being defrauded; that is, older adults were less likely to report being a victim of fraud. Two different investigations—one focusing on romance scams (Whitty, 2019b) and the other on cyber scams (Whitty, 2019a)—further illustrate the complex relationship between age and falling prey to a scam. Whereas the former found that middle-aged women were most likely to fall victim, the latter found that older age was associated with greater likelihood of victimhood. One final reason why old age has received so much attention is that older adults tend to lose larger amounts of money per incident compared with their younger counterparts. Taken together, however, current data do not provide a clear picture about the relationship between age and susceptibility to scams, and there is little insight as to why middle-aged adults are at particularly high risk of becoming fraud victims (e.g., are they targeted more often, or are they more willing to respond to scam solicitations?).

The literature on other demographic variables, such as education, gender, income, and ethnicity, is far patchier. The Office for National Statistics (2016) in the United Kingdom, for example, has reported that individuals with higher incomes report higher rates of victimhood. A survey on scams in 30 European countries (European Commission, 2020) has provided similar insights, finding that more educated individuals and individuals with higher incomes are more likely to report being a victim of fraud, and also that males are more likely than females to report being victimized. DeLiema and colleagues (2020) and Whitty (2019a, 2019b) also reported that being better educated was associated with higher rates of reporting being defrauded in investment-type scams. In contrast, studies by Wood et al. (2018) and Mueller et al. (2020) suggest that higher education is associated with a lower intention to respond to mass-marketing solicitations. Still other studies (Gavett et al., 2017; Jones et al., 2019; Lee & Geistfeld, 1999) failed to find any demographic factors that predicted susceptibility to phishing.

Finally, few studies have examined whether race serves as a contributing factor, possibly because of the low sample size of non-White participants in most studies, as well as the diverse racial makeup of different
countries. A notable exception is work by Anderson (2019), who reported that Hispanic Americans and Black Americans are more likely than White Americans to report falling victim to fraud, even after controlling for income and language. Thus, further examination of demographic variables is needed. These studies should include country-specific and cross-national comparisons, use cross-sectional and longitudinal data, and target larger sample sizes.

Why would the literature provide such a complex and diverging picture? Possible answers are that individuals with different characteristics differ in their response to the various types of scam solicitations and that scammers target different groups. Although data supporting this intuition are limited, scammers do develop “bespoke” scams, such as ones targeting Medicare beneficiaries or students. Indeed, a report by Button et al. (2009) provides some indication that which group (male vs. female, young vs. old) is more likely respond to a scam solicitation depends on the type of scam. For example, females were more likely to be victims of sweepstake scams, whereas males were more likely to be victims of foreign lottery scams; older adults were more likely to fall prey to investment scams, whereas younger adults were more often victims of work-at-home and business-opportunity scams. Statistics about scams, however, should be viewed with caution because the rate of reporting is low. In addition, scams keep changing; new ones, such COVID-19 scams, are constantly emerging.

**Individual Differences and Susceptibility to Scams**

Researchers have also been interested in the link between individual differences and susceptibility to scams, and they have employed a myriad of individual-difference measures in trying to detect what characteristics might distinguish between victims and nonvictims. Among the characteristics examined are cognitive ability, self-control, and risk taking.

A large corpus of literature has shown that declines in cognitive ability and executive functioning are associated with reduced decision-making ability. Building on this line of reasoning, a study by Ebner et al. (2018) showed that higher cognitive ability served as a protective factor against falling prey to phishing attacks, but only among adults ages 75 through 89. A better predictor of higher scam susceptibility was lower positive affect. Similarly, Mueller et al. (2020) examined the role of emotional intelligence and demonstrated that participants who scored higher on the ability dimension of emotional intelligence exhibited reduced intention to respond to mass-marketing solicitations. Moreover, older adults scored higher on emotional intelligence and exhibited reduced intention to respond to scam solicitations. Using a different set of measures, Jones and colleagues (2019) found that performance on a cognitive-reflection task (but not performance on the Stroop task or a reading span task) served as a modest predictor of susceptibility to scams. DeLiema et al. (2020), however, found no relationship between fraud victimization and cognitive ability in their data.

Two other candidate predictors are self-control (also known as time discounting or impulsivity) and risk taking, which have been employed to explain both criminal behavior and the quality of financial decision making (e.g., Ottaviani & Vandone, 2018). For instance, Anderson (2019) identified low self-control as a predictor of being a fraud victim, and Whitty’s (2019a, 2019b) examination of both cyber- and romance-scam victims revealed similar trends. A study by the AARP Foundation (2003) showed that investment-scam victims (compared with nonvictims) were more likely to buy things on the spur of the moment, and lottery-scam victims (compared with nonvictims) were less likely to plan their future purchases. In an analysis of more than 11,000 Internet users, Chen et al. (2017) showed that self-control served as a key predictor of being an Internet-scam victim. Finally, Modic and Lea (2013) developed a scale designed to evaluate susceptibility to persuasion. Data from two investigations using this scale showed that self-control was a predictor of both past and future compliance with scam solicitations.

One can think of scams as informal lotteries or gambles. Therefore, risk-taking tendencies should play a significant role in responding. Indeed, using data from a 2017 survey by the Federal Trade Commission, Anderson (2019) showed that individuals with a high tolerance for risk, compared with those with a low tolerance for risk, were almost twice as likely to report having been a fraud victim. Similarly, individuals who reported having made a risky purchase had almost double the probability of being a fraud victim, compared with those who reported having made no such purchases. However, Mueller et al. (2020) failed to show a relation between financial risk tolerance and measures evaluating scam susceptibility and susceptibility to persuasion. The studies by Anderson (2019), Mueller et al. (2020), and Modic et al. (2018) are the only ones we know of that have included a risk-taking measure. Using a different approach, Mueller et al. (2020) and Wood et al. (2018) asked participants to indicate how beneficial and how risky they perceived scam solicitations to be. Results of the two studies converged, revealing that participants’ benefit and risk perceptions were the main predictors of intentions to respond to the scam solicitations. Capitalizing on the large corpus of research
on risk taking and risk perception, future studies could examine whether, for example, the manipulation of benefits and risk could help reduce or increase intentions to respond to scam solicitations. An additional key question is why some individuals fail to see the risks involved in engaging with these scams. Belief in fake news, for example, is linked to reduced analytic thinking, delusional thinking, dogmatism, and religious fundamentalism (Bronstein, et al., 2019), but it is an open empirical question whether similar mechanisms underlie participation is certain types of scams.

The Nature of the Scam

Demographic and personality characteristics are not the only variables associated with susceptibility to scams. Indeed, the nature of the scams might also affect the likelihood of victimization. There are hundreds, if not thousands, of different types of scams, employing a myriad of techniques to lure in potential victims. Therefore, there is an equal need to examine the nature of the scams, that is, the techniques used by the scammers. Scholars of persuasion techniques would be quick to recognize that scammers often utilize at least two principles of persuasion: authority (e.g., government) and scarcity (e.g., time pressure or limited number of prizes).

A study by Fischer et al. (2013) employed two research methods to examine the content of real scams and its influence on targets’ likelihood of responding to them. Examining more than 580 different scams, the authors found that scammers often used “emotional cues, trust and authority cues, cost–benefit considerations (size of prize), behavioural commitments, and sunk–cost considerations” (p. 2063). In a second experiment, the authors created eight different types of scams (see their Table 3, p. 2069) that differed in the following delivery (or content) characteristics: delivery mode (cold vs. hot), prize amount, presence or absence of symbols of authority, and presence of absence of triggers of positive emotions. The results showed that response rates were generally similar regardless of the prize amount or the presence of symbols of authority or triggers of positive emotions. However, when the solicitation was hot rather than cold, participants’ response rate increased, but only among those who reported having been scammed before. In a more recent study, Wood et al. (2018) presented participants with mass-marketing solicitations that differed in their use of authority (Walmart vs. unknown vendor) and scarcity (a time deadline vs. no time deadline). The authors reported no differences in response rates or in participants’ perceptions of the risks and benefits of different scams. In a second study, the authors included an activation cost (such as often accompanies mass-marketing solicitations) of either $5 or $100. Participants who were asked to pay a $100 activation fee were less likely to respond to the solicitation.

These studies (see also Jones et al., 2019, for an experiment including time pressure) are among the few that have involved experimental manipulation of key scam variables. More work is clearly needed. Other researchers (e.g., Gregory & Nikiforova, 2012) have used various types of content-analysis approaches to capture the key techniques used by scammers and have demonstrated that the Nigerian scam, which has been around for a long while (Cukier et al., 2007), has changed very little over time. Employing both qualitative and quantitative methods to capture scammers’ techniques, we believe, offers the best way to develop preventive measures.

Conclusion

Scams present a multidimensional and dynamic problem. Scammers attack individuals of all backgrounds, in every corner of the world, and with novel and changing techniques and lures. Given that there are millions of scam victims every year, there is a pressing need to identify what factors render individuals more vulnerable to scam solicitations and, more important, what preventive measures can be used to alleviate this problem. Most, if not all, of the advice that exists has not been tested; nor does it seem to work—as is evident in the increased number of victims. Psychologists, as well as other behavioral scientists, have insight and training that place them perfectly to tackle this problem.

Despite the valuable knowledge gained from the studies presented here, there is plenty of room for a wide range of further work to be conducted. First, there is a growing need to develop theoretical frameworks—ones that incorporate cognitive abilities, neurological insights, and personality research—that can advance understanding of scam susceptibility. Empirical researchers, moreover, must improve the external validity of their work and conceive ways to conduct more realistic and natural field studies (e.g., Ebner et al., 2018). Furthermore, because little is known about how to reduce scam compliance, there is an urgent need to conduct research in this area that will make it possible to develop decision aids and other tools to reduce scam compliance. Although many sources on the Internet offer valuable advice (see Table 1), many people fail to follow it (e.g., use 123456 as their password). Whether nudges or other behavior-modification
techniques can improve adherence to these simple rules is, likewise, an open question. Given the complex nature of the problem, closer collaborations among researchers in different disciplines (e.g., computer scientists and psychologists) is likely to be fruitful. Finally, given the emotional effect of scams, clinical work is needed to advance understanding about the impact of fraud on victims’ psychological well-being and how to help them.

**Recommended Reading**

AARP Foundation. (2003). (See References). One of the only studies to have examined preventive measures to reduce scam compliance.

Anderson, K. B. (2019). (See References). One of the most comprehensive surveys on scamming and its links to demographic and personality characteristics.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. S. (2018). (See References). One of the few studies employing clever naturalistic and realistic experimental designs to examine response to scams.

Wood, S., Liu, P.-J., Hanoch, Y., Xi, P. M., & Klapatch, L. (2018). (See References). Reports results of experiments exploring how the content of scams affects the tendency to respond to them.

Table 1. Common Suggestions to Reduce Scam Compliance

| Recommendation                                                                 |
|-------------------------------------------------------------------------------|
| Never give your personal information over the phone                           |
| Always log on to a website directly                                           |
| Insist on time to get a third-party review                                    |
| Report scam victimization, to help other consumers                           |
| Use strong passwords                                                          |
| Keep virus software up to date                                                |
| Use consumer resources such as the Better Business Bureau to research companies|
| Consider signing up for an identity-theft protection service                  |
| Slow down and deliberate before responding to offers; resist pressure         |
| Throw out all mailed sweepstakes solicitations                                |
| Ask local contractors for their license and a permit and check websites for their history |
| Let your bank know if your financial information might have been stolen       |
| Be wary of any unsolicited pop-up message on your device; do not click on it or call the number |
| Destroy all your financial documents before putting them in the garbage or recycling them |
| Beware of advance payment                                                     |
| Never share your PINs (personal identification numbers) or passwords with anyone and choose PINs and passwords that are hard to guess |
| Get advice from someone you trust                                           |

Note: These are common suggestions offered by a range of sources, such as police departments, the U.S. Federal Bureau of Investigation, and third-sector organizations.

Declaration of Conflicting Interests

The author(s) declared that there were no conflicts of interest with respect to the authorship or the publication of this article.

ORCID iD

Yaniv Hanoch  https://orcid.org/0000-0001-9453-4588

Acknowledgments

We would like to thank Michaela Gummerum and Paurav Shukla for valuable comments on earlier drafts.

Notes

1. We use the terms *scam* and *fraud* interchangeably to denote “the deliberate intent to deceive with promises of goods, services, or other financial benefits that in fact do not exist or that were never intended to be provided” (Titus et al., 1995, p. 54).

2. Although we have drawn on diverse literature, the scope of the work cited here is somewhat limited. For example, computer scientists, whose work we have given only limited attention to, have provided important insights and (partial) solutions to the problem but have focused mainly on preventing scams from reaching consumers (but see Ebner et al., 2018).

3. We are unable to cover all the personality and individual-difference measures that have been examined thus far but have discussed the main ones that have been reported. In addition, there are many other measures—confidence, Internet knowledge, financial literacy, gullibility, numeracy, Big Five personality, and trust—that need examination.

4. In this journal, Brashier and Schacter (2020) have argued that cognitive ability can help explain older adults' higher susceptibility to fake news.
References

AARP Foundation. (2003). Off the book: Reducing participation in telemarketing fraud. https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf

Anderson, K. B. (2019). Mass-market consumer fraud in the United States: A 2017 update [Staff report]. Federal Trade Commission, Bureau of Economics. https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconumerfraud2017report.pdf

Brasher, N. M., & Schacter, D. L. (2020). Aging in an era of fake news. Current Directions in Psychological Science, 29(3), 316–323. https://doi.org/10.1177/0963721420915872

Bronstein, M. V., Pennycook, G., Bear, A., Rand, D. G., & Cannon, T. D. (2019). Belief in fake news is associated with delusionality, dogmatism, religious fundamentalism, and reduced analytic thinking. Journal of Applied Research in Memory and Cognition, 8(1), 108–117. https://doi.org/10.1016/j.jarmc.2018.09.005

Burnes, D., Henderson, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. American Journal of Public Health, 107(8), e13–e21. https://doi.org/10.2105/AJPH.2017.308621

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and victims of fraud: Literature review. National Fraud Authority. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118469/fraud-typologies.pdf

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior, 70, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, narrative and the “Nigerian letter” in electronic mail. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07) (p. 70). IEEE Computer Society. https://doi.org/10.1109/HICSS.2007.238

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Elder financial fraud among older Americans: Evidence and implications. The Journal of Gerontology B: Social Sciences, 75(4), 861–868. https://doi.org/10.1093/geronb/gby151

Ehner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. S. (2018). Uncovering susceptibility risk to online deception in aging. The Journal of Gerontology B: Psychological Sciences, 75(3), 522–533.

Ellin, A. (2019, September 12). Scammers look for vulnerability, and find it in older people. The New York Times. https://www.nytimes.com/2019/09/12/business/retirement/scams-elderly-retirement.html

European Commission. (2020). Survey on “scams and fraud experienced by consumers”: Final report. https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-final_report.pdf

Federal Trade Commission. (2021). FTC COVID-19 and stimulus reports. Retrieved April 22, 2021, from https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/FraudLosses

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. PLOS ONE, 12(2), Article e0171620. https://doi.org/10.1371/journal.pone.0171620

Gee, J., & Button, M. (2019). The financial cost of fraud 2019. http://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf

Gregory, D. W., & Nikiforova, B. (2012). A sweetheart of a deal: How people get hooked and reeled in by financial scams. The Journal of Behavioral Finance & Economics, 2(2), 96–122.

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(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

Jones, H. S., Towe, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. PLOS ONE, 14(1), Article e0209684. https://doi.org/10.1371/journal.pone.0209684

Kumaran, N., & Lugani, S. (2020, April 6). Protecting businesses against cyber threats during COVID-19 and beyond. Google Cloud. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Lee, J., & Geistfeld, L. V. (1999). Elderly consumers’ receptiveness to telemarketing fraud. Journal of Public Policy & Marketing, 18(2), 208–217. https://doi.org/10.1177/07439156990180207

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: The Journal of Aging and Mental Health, 39(1), 48–63. https://doi.org/10.1080/07317115.2015.1101632

Modic, D., & Anderson, R. (2015). It’s all over but the crying: The emotional and financial impact of Internet fraud. IEEE Security & Privacy, 13(5), 99–103. https://doi.org/10.1109/MSP.2015.107

Modic, D., Anderson, R. J., & Palomäki, J. (2018). We will comply: The development of a susceptibility-to-persuasion scale. PLOS ONE, 13(3), Article e0194119. https://doi.org/10.1371/journal.pone.0194119

Modic, D., & Lea, S. E. G. (2013). Scam compliance and the psychology of persuasion. SSRN. https://doi.org/10.2139/ssrn.2364464

Mueller, E. A., Wood, S. A., Hanoch, Y., Huang, Y., & Reed, C. (2020). Older and wiser: Age differences in susceptibility to financial fraud: The protective role of...
emotional intelligence. *Journal of Elder Abuse & Neglect, 32*(2), 152–172. https://doi.org/10.1080/08946566.2020.1736704

Office for National Statistics. (2016). *Overview of fraud statistics: Year ending Mar 2016.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

Ottaviani, C., & Vandone, D. (2018). Financial literacy, debt burden and impulsivity: A mediation analysis. *Economic Notes, 47*(2–3), 439–454. https://doi.org/10.1111/ecno.12115

Shao, K., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults’ vulnerability to fraud. *Journal of Elder Abuse & Neglect, 31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

Simon, H. A. (1990). Invariants of human behavior. *Annual Review of Psychology, 41*, 1–20. https://doi.org/10.1146/annurev.ps.41.020190.000245

Titus, R. M., Heinzelmann, F., & Boyle, J. (1995). Victimization of persons by fraud. *Crime & Delinquency, 41*(1), 54–72.

Whitty, M. T. (2019a). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Whitty, M. T. (2019b). Who can spot an online romance scam? *Journal of Financial Crime, 26*(2), 623–633. https://doi.org/10.1108/JFC-06-2018-0053

Wood, S., Liu, P.-J., Hanoch, Y., Xi, P. M., & Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied, 24*(2), 196–206. https://doi.org/10.1037/xap0000167