**Cover page**

**The scams among us: Who falls prey and why**

Corresponding author: Yaniv Hanoch

Southampton Business School

University of Southampton

Room 3021, Building 2, Highfield Campus

Southampton SO17 1BJ

England

Tel: +44 (0)23 8059 9629

E-mail: [y.hanoch@soton.ac.uk](mailto:y.hanoch@soton.ac.uk)

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

Author note: The authors declare that there are no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

No funding to declare

Word count: 3200

**Running head: The scams among us**

**Title page**

**The scams among us: Who falls prey and why**

Yaniv Hanoch1 and Stacey Wood2

1 Southampton Business School, University of Southampton

2 Department of Psychology, Scripps College

Corresponding author: Yaniv Hanoch

Southampton Business School

University of Southampton

Room 3021, Building 2, Highfield Campus

Southampton SO17 1BJ

England

Tel: +44 (0)23 8059 9629

E-mail: [y.hanoch@soton.ac.uk](mailto:y.hanoch@soton.ac.uk)

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

Author note: The authors declare that there are no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

No funding to declare

Word count: 3200

**Running head: The scams among us**

**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, we know relatively little about why some individuals fall victim to scams while others remain immune to the techniques utilized by scammers to lure potential victims. Research thus far provides, for example, 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. We know even less about how the nature or type of scam impacts 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 victims. Here, we provide some promising directions as well as point to existing gaps in our knowledge and the need for decision scientists to address this important problem.

Keywords: Demographics variables, fraud, individual differences, risk factors, scams, susceptibility

**Main text**

On April 17, 2020, Google announced that it had blocked a staggering 126 million phishing scams related to COVID-19, the 2019 novel coronavirus disease, in a single week, representing the most intense and extensive phishing attack in the company’s history (Kumaran & Lugani, 2020). Millions of other COVID-19 scams[[1]](#footnote-1) 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. One report estimated the financial cost of fraud to the global economy at over $5 trillion (Gee & Button, 2019), almost 50% higher than the 2019 U.S. budget (about $3.5 trillion). Furthermore, researchers (Modic & Anderson, 2015; Whitty & Buchanan, 2012) have argued that the psychological and emotional impact of scams is asdetrimental and pervasive as the financial impact. Indeed, a survey by the European Commission (2020) showed that 79% of scam victims have suffered emotionally while 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. Most importantly, 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, while 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. We know relatively little about, for example, why some individuals fall victim to scams while others remain resilient; what types of preventive programs are effective; how to increase reporting of scams to the authorities; and what types of strategies scammers use to lure potential victims and keep them engaged. There 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, Towse, and Race (2015) have maintied that susceptibility to scams is driven by three complementary but independent factors:: (i) persuasive techniques employed by the sender, (ii) information processing of the user, and (iii) “userX,” that is, the human–computer interaction or consumer/solicitation context. The 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). Drawing on Jones et al (2015) and Simon (1990) insights, thus, suggest the need to investigate both the environment in which the decision maker operates as well as the decision maker. In other words, we must examine a wide ranging of individuals features and abilities—such as cognitive, demographic, emotional, motivation, and personality—as well as the features and characteristics of the scams—such as, for example, their use of principles of persuasion (e.g., authority). Following this framework, we divide the present paper into three sections. First, we summarize the demographics characteristics that are linked to victimhood; next, we review the link between individual difference measures and susceptibility to scams; and finally, we discuss what techniques scammers employ in their attempt to bait potential victims.[[2]](#footnote-2)

**Demographic characteristics and susceptibility to scams**

*The* *New York Times* has published several stories that focus on old age and fraud (e.g., Ellin, 2019). *The* *New York Times* is not the only outlet to advance the idea that age is one of the key demographic factors linked to fraud, such that it 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 reported 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 to middle-aged adults (Anderson, 2019; Office for National Statistics, 2016; Titus et al., 1995).

It is possible that each age group (young, middle-aged, and older adults) responds 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 represent 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 (2020) found that adults between the ages of 30 and 39 represented the group with the highest number of COVID-19 fraud complaints, a finding that roughly matches that reported by Anderson (2019; see also Titus et al., 1995), where individuals aged 35–44 were most likely to report falling victim to mass marketing solicitations (MMSs). Drawing on longitudinal data from the Health and Retirement Study (with individuals 50 years old and over), DeLiema and colleagues (2020) found that age was negatively associated with being defrauded, such that 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 scam. While the former reported that middle-aged women were most likely to fall victim, the latter found that old age was associated with greater likelihood of victimhood. One final reason why old age has received so much attention is because older adults tend to lose higher amounts of money compared to their younger counterparts per incident. Taken together, however, current data do not provide a clear picture about the relationship between (old) age and susceptibility to scams, and there is little insight as to why middle-aged adults are at higher risk of becoming fraud victims (e.g., are they being 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, with males, more educated individuals, and individuals with higher incomes being more likely to report being a victim of fraud. 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 MMSs. Still other studies (Gavett et al., 2017; Jones et al., 2019; Lee and Geistfeld, 1999) failed to find any demographic factors that predict susceptibility to phishing. Finally, few studies have examined whether race serves as a contributing factor, possibly due to the low sample size of non-White participants in most studies as well as the diverse racial makeup in different countries. A notable exception is work by Anderson (2019), who reported that Hispanic Americans and African Americans are more likely to report falling victim to fraud, even after controlling for income and language. Thus, further examination of demographic variables is needed wherein country-specific and cross-national comparisons can be carried out with cross-sectional and longitudinal data involving wider population studies.

Why would the literature provide such a complex and diverging picture? One possibility is that individual characteristics differ in response to different scam solicitations, as well as scammers targeting different groups. While data supporting this intuition is limited, scammers do develop “bespoke” scams, such as ones targeting Medicare beneficiaries or students. Indeed, a report by the Button, Lewis, and Tapley (2009) provides some indication that different groups (male vs. female, and young vs. old) might be more likely respond to different scam solicitations. For example, females were more likely to be victims of sweepstake scams while males of foreign lottery scams; older adults were more likely to fall pray to investment scams, while younger adults were more often victims of work at home and business opportunity scams. Statistics about scams, however, are impacted by several factors, at least. First, the rate of reporting is low. And second, scams keep on changing—with new scams, such COVID-19, constantly emerging.

**Individual differences and susceptibility to scams[[3]](#footnote-3)**

In addition to demographics characteristics, researchers have been interested in the link between personality characteristics and susceptibility to scams. Researchers have employed a myriad of individual difference measures in trying to detect what factors or characteristics might distinguish between victims and nonvictims. Among the measures used are those that assess cognitive ability, impulsivity/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.[[4]](#footnote-4) Building on this line of reasoning, Ebner et al. (2018) showed that higher cognitive ability serves as a protective factor against falling prey to phishing attacks, but only among what they call middle-old adults (75–89 years old). More interesting, a better predictor of higher scam susceptibility was lower positive affect, rather than cognitive ability. Similarly, Mueller et al. (2020) examined the role of cognitive ability and emotional intelligence (EI) and demonstrated that participants who scored higher on the ability dimension of EI exhibited reduced intention to respond to MMSs. Moreover, older adults scored higher on EI and exhibited reduced intention to respond to scam solicitations. Using a different set of measures, Jones and colleagues (2019) found that the cognitive reflection task (but not performance on the Stroop task or reading span task) served as (a modest) predictor of susceptibility to scams. DeLiema et al. (2020) found, however, no relationship between fraud victimization and cognitive ability in their data.

Two other prime predictors have been self-control (also known as time discounting or impulsivity) and risk taking, which have been employed to explain both criminal behavior and poorer 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 (2003) reported investment-scam victims were more likely to buy things on the spur of the moment, and lottery-scam victim were less likely to plan their future purchases. Following an analysis of over 11,000 internet users, Chen et al. (2017) showed that self-control served as a key predictor for being an internet-scam victim. Finally, Modic and Lea (2013) developed a scale designed to evaluate susceptibility to persuasion. Data from two investigations showed that self-control was a predictor of both past and future compliance with scam solicitations.

One can think of scams as an informal lottery or a gamble. As such, risk-taking tendencies should play a significant role in responding. Indeed, using a 2017 Federal Trade Commission study, Anderson (2019) showed that individuals with a higher tolerance for risk and those who reported risky purchasing habits had almost double the probability of being a fraud victim. However, Mueller et al. (2020) failed to show a relation between financial risk tolerance and measures evaluating scam susceptibility (James et al., 2014) and susceptibility to persuasion (Modic et al., 2018). Interestingly, Anderson (2019), Mueller et al. (2020) and Modic et al., (2018) are the only studies we know of that have included a risk-taking measure in their study. 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 converge, revealing that participants’ benefit and risk perceptions were the main predictors of intentions to respond to the scam solicitation. Given 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 intention to respond to scam solicitation. An additional key question is why some individuals fail to see the risks involved in engaging with these scams. We do know that belief in fake news, for example, is linked to reduced analytical thinking, delusionality, dogmatism, and religious fundamentalism (Bronstein, et al., 2019). Whether similar mechanisms underlie partipation is certain types of scams is an open empirical question.

**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 impact 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. As such, there is an equal need to elucidate the nature of the scams, that is, the techniques used by 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 Fisher et al. (2013) employed two research methods to examine (a) the content of real scams and (b) its influence on the likelihood of responding to them. After examining over 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 identified eight different types of scams (see their Table 3, p. 2069) that differ in their delivery mode (or content): whether the scam offer appeared early or later, prize amount, symbols of authority, and triggers of positive emotions. The results show that the response rate was generally similar regardless of the prize amount, the existence of symbols of authority, or triggers of positive emotions. When the solicitation was “hot” vs. “cold”, participants’ response rate increased, but only among those who had reported being scammed before. In a more recent study, Wood et al. (2018) presented participants with MMSs that diverged in their authority (Walmart vs. unknown vendor) and scarcity (a time deadline or no time deadline). The authors reported no differences in response rates nor differences in participants’ risk and benefit perceptions of the different scams. In a second study, the authors included a small financial activation cost (which often accompanies MMSs) of either $5 or $100. This time, participants who were asked to pay a $100 activation fee were less likely to respond to the MMS. These studies (see also Jones et al., 2019, for including time pressure) are among the few that have experimentally manipulated 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—demonstrating that the Nigerian scam has not only been around for a long while (Cukier, Nesselroth, & Cody, 2007) but has changed very little. Employing both qualitative and quantitative methods to capture scammers’ techniques, we believe, offers the best way to develop preventive measures.

**Conclusion**

Scams, as the review above suggests, 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. With millions of scam victims every year, there is a pressing need to identify what factors render individuals more vulnerable to scam solicitations and, more importantly, 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, with their insight and training are perfectly placed to use their expertise to tackle this problem. Despite the valuable knowledge gained from studies presented here, there is plenty of room for a wide range of 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 better guide our understanding of scam susceptibility. Empirical research, moreover, must improve its external validity and conceive ways to conduct more realistic and natural (field) studies (e.g., Ebner 2018). We know, furthermore, little on how to reduce scam compliance. Hence, developing decision aids and tools to reduce scam compliance are urgently needed. Furthermore, while many sources in the internet offer valuable advice (see Table 1), many fail to follow them (using 123456 as their password). Whether nudges or other behavioural modification techniques can improve adherence to these simple rules is, likewise, an open question. Given the complex nature of the problem, closer collaborations between disciplines (e.g., computer scientists and psychologists) is likely to be fruitful. Finally, given the emotional effect of scams, clinical work needs to gain better understanding about the impact of fraud on victims’ psychological well-being and, importantly, on the type of method(s) that can provide help.

# Acknowledgments and endnotes

# 1. Address correspondence to Yaniv Hanoch, Southampton Business School, University of Southampton, Southampton, SO17 1BJ, England.

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

# References

AARP. (2003). *Off the hook: 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]. Bureau of Economics of the Federal Trade Commission. <https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf>

Brashier, N. M., & Schacter, D. L. (2020). Aging in an Era of Fake news. *Current Directions in Psychological Science*, 29, 316-323. <https://doi.org/10.1177/0963721420915872>

Bronstein, M., Pennycook, G., Bear, A., Rand, D. G., & Cannon, T. (2018). Belief in fake news is associated with delusionality, dogmatism, religious fundamentalism, and reduced analytic thinking. *Journal of Applied Research in Memory and Cognition*, 8, 108–117. https://doi.org/10.1016/j.jarmac.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.2017.303821>

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and victims of fraud: Literature review. *National Fraud Authority*. Retrieved from <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 behaviours. *Computers in Human Behaviour*, *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. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Hilton Waikoloa Village, Big Island.

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2017). Financial fraud among older Americans: Evidence and implications. *The Journal of Gerontology: Series B*, *75*, 861–868. 10.1093/geronb/gby151

**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). Uncovering susceptibility risk to online deception in aging. Journals of Gerontology, Psychological Sciences, 17, 522-533. [10.1145/3336141](https://doi.org/10.1145/3336141)

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.”* 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. (2020). *FTC COVID-19 and stimulus reports*. https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/FraudLosses

Fischer, P., Lea, S. E. G., & Evans, K. (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.

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. & Nikiforova, B. (2012). A sweetheart of a Deal: How people get hooked and reeled in by financial scams. *The Journal of Behavioural Finance and Economics*, *2*, 96–122.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Elder Abuse and Neglect*, *26*(2), 107–122. [10.1080/08946566.2013.821809](https://dx.doi.org/10.1080%2F08946566.2013.821809)

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLoS ONE*, 14(1), Article e0209684.

Kumaran, N., & Lugani, S. (2020). *Protecting business against cyber threats during COVID-19 and beyond*. Retrieved from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Lee, J., & Geistfeld, L. (1999). Elderly Consumers' Receptiveness to Telemarketing Fraud. *Journal of Public Policy & Marketing,* *18*(2), 208-217. Retrieved January 19, 2021, from <http://www.jstor.org/stable/30000541>

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. J., & Palomäki, J. (2018). We will make you like our research: 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 Electronic Journal*. <https://doi.org/10.2139/ssrn.2364464>

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. doi: 10.1109/MSP.2015.107

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 and 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.* Office of National Statistics. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016#which-groups-in-society-are-most-likely-to-be-victims-of-fraud>

Ottaviani, C., & Vandone, D. (2018). Financial literacy, debt burden and impulsivity: A mediation analysis. *Economic Notes*, *47*, 439–453. <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*(l), 54–72.

Whitty, M. T. (2019a). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*, 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*, 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

**Recommended reading**

AARP. (2003). *Off the hook: Reducing participation in telemarketing fraud*. <https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf>

One of the only studies to have examined preventive measures to reduce scam compliance.

Anderson, K. B. (2019). *Mass-market consumer fraud in the United States: A 2017 update* [Staff report]. Bureau of Economics of the Federal Trade Commission. <https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf>

The paper is one of the most comprehensive surveys on scam 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). Uncovering susceptibility risk to online deception in aging. Journals of Gerontology, Psychological Sciences, 17, 522-533.

The work by Ebner and colleagues is among the few to employ clever naturalistic and realistic experimental design to examine response to scams.

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>

Discuss how the manipulation of scams impact the tendency to respond to them.

Table 1

Common suggestions to reduce scam compliance.

|  |  |
| --- | --- |
| Recommendations | Source |
| **Never give your personal information over the phone** | Canadian Business Association |
| Always log on to a website directly | Met.police |
| Insist on time to get a third-party review | Met.police |
| Report scam victimization, it will help other consumers | Met.police |
| Use strong passwords | Citizens advice, UK |
| Keep virus software up to date | FBI.gov |
| Use consumer resources such as Better Business Bureau to research companies | FTC.gov |
| Consider identity theft protection service | FTC.gov |
| Slow down and deliberate before responding to offers/resist pressure. | FTC.gov |
| Throw out all mailed sweepstakes solicitations. | FTC.gov |
| Ask local contractors for license and permit and check websites for history | FTC.gov |
| Let your bank know your financial information might have been stolen | Citizen Advice, UK |
| Be wary of any unsolicited pop-up message on your device; don’t click on it and don’t call the number. | Microsoft |
| **Destroy all your financial documents before putting them in the garbage or recycling** | Canadian Business Association |
|  |  |
| **Beware of advance payment.**  **Never share your PIN number or passwords with anyone and choose PINs and passwords that are hard to guess.**  **Get advice from someone you trust.** | AARP.org  Canadian Business Association  FTC.gov |

1. We use the terms scam and fraud interchangeably. We use the terms fraud and scams 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). [↑](#footnote-ref-1)
2. While we have drawn on diverse literature, the scope of the work cited here is somewhat limited. For example, computer scientists have provided important insights and (partial) solutions to the problem. They have focused mainly, however, on preventing scams from reaching consumers (but see Ebner et al., 2018). [↑](#footnote-ref-2)
3. We are unable to cover all the personality and individual difference measures that have been used thus far. At the same time, there are many other measures—confidence, internet knowledge, financial literacy, gullibility, numeracy, the Big Five, and trust—that need further examination. [↑](#footnote-ref-3)
4. A paper in this journal has argued that cognitive ability can help explain older adults’ higher susceptibility to fake news (Brashier & Schacter, 2020). [↑](#footnote-ref-4)