International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 3 Article 3

11-1-2022

"Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization

scam, fraud, online, age group, older, self-control, lifestyle-routine activities, employment, reporting

Parti (2022). *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(3), 20-40.

"Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization

Katalin Parti*, Ph.D., Virginia Tech, U.S.A.

Keywords: Scam, Fraud, Online, Age Group, Older, Self-Control, Lifestyle-Routine Activities, Employment, Reporting

Abstract:
In an attempt to understand how differently fraud works depending on a victim's age, we have examined the effects of situational (lifestyle-routine activities), self-control, and sociodemographic variables on scam victimization across age groups. The analysis was carried out on a national sample of 2,558 Americans, representative by age, sex, and race, and includes additional factors such as their education, living arrangement, employment, and propensity for reporting a crime or asking for help. The results substantiate research findings of the contribution of self-control and LRAT in predicting victimization in general but could not identify major situational and individual differences between older and younger Americans' scam victimization. However, employment can function as a protective factor for older individuals in some online fraud scenarios. Furthermore, older adults show significantly more reluctance in asking for help or reporting than do younger ones. Future research must address these differences. The author also suggests developing specific variables for measuring how lifestyle-routine activity theory works in scam victimization.

Introduction

Although online fraud/scams target everyone independent of age, scams disproportionately affect people over 60. According to the FBI's Elder Fraud Report 2020, approximately 28% of total fraud losses were sustained by victims over the age of 60 and resulted in approximately $1 billion in losses to older persons (IC3, 2020). This represents an increase of approximately $300 million in losses reported in 2020 versus 2019 (IC3, 2020). In addition, older people are more digitally connected than ever. With their daily routines migrating to online platforms, older individuals are becoming increasingly vulnerable to online fraud. In a meta-analysis, Burnes et al. (2017) found that scams affect approximately one in every 18 cognitively intact, community-dwelling older adults each year.

In this study, we define online fraud/scam as when a stranger intentionally deceives a victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other—physical, mental, or emotional—expectations that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain (adapted from Beals et al., 2015b; and Titus et al., 1995). Financial fraud differs from financial exploitation/abuse, which is committed by caregivers or other trusted individuals (Hall et al., 2016).

Recent research has argued in favor of an integrated model combining the general theory of crime (Gottfredson & Hirschi, 1990) and routine activities theory (Cohen & Felson, 1979) to examine victimiza-

*Corresponding author
Katalin Parti*, Ph.D., Department of Sociology, Virginia Tech, McBryde Hall, 225 Stanger St, Blacksburg, Virginia 24061, U.S.A.
Email: kparti@vt.edu

tion (Holtfreter et al., 2008; Ngo & Paternoster, 2011; Piquero et al., 2005; Pratt et al., 2014; Schreck, 1999; Schreck et al., 2006; Schreck et al., 2002; Stewart et al., 2004). This model posits that individuals with low self-control make impulsive decisions that increase exposure to motivated offenders, decrease the utility of guardians, and increase their vulnerability to victimization. Both real world (e.g., Holtfreter et al., 2008; Piquero et al., 2005; Schreck et al., 2006; Schreck et al., 2002) and cybercrime victimization (Mikkola et al., 2021; Bossler & Holt, 2010; Holt et al., 2016; Ngo & Paternoster, 2011) are explained by the above framework. However, the results are mixed, and research suggests that the list of situational and individual factors of online victimization must be refined and extended (Ngo & Paternoster, 2011), the effects of combined theories on victimization must be tested (Mikkola et al., 2021), and the risk factors of victimization of singular cyber offenses must be examined instead of under the collapsed category of "cybercrime" (Ngo & Paternoster, 2011).

The current research intends to fulfil the above expectations. It examines the effects of situational (i.e., those situations attributable to the lifestyle routine activities theory), self-control, and sociodemographic variables of victimization on specific online cyber offenses (online fraud/scams). In addition, we compare the effects of the above measures in younger and older age groups, in an attempt to find out whether and how situational and individual level factors work differently by age. After describing theoretical considerations and age-based individual and situational factors, we turn to the current research. We close the article with implications and recommendations for future research.

Literature Review

Lifestyle routine activities (LRAT) theory

Lifestyle-exposure theory (Hindelang et al., 1978) suggests that individuals' daily activities contribute to victimization. The theory became part of routine activities theory (RAT) in which Cohen and Felson (1979) suggest that an individual's daily activities contribute to their victimization. Cohen and Felson (1979) posit that an individual's social roles and social class influence their lifestyle, including risky activities, as a result of their individual rational choices. They suggest that a crime will likely occur if a suitable target, a motivated offender, and the absence of a capable guardian spatio-temporarily converge. RAT has been tested on victimization of predatory and property crimes (Cohen & Felson, 1979; Felson, 1986; Kennedy & Forde, 1990; Massey et al., 1989; Miethe et al., 1987; Roncek & Maier, 1991; Sherman et al., 1989), computer-crime (Kowalski, 2002; Moitra, 2005; Choi, 2008) and internet-crime victimization (for a summary, see Leukfeldt & Yar, 2016). Although RAT was originally developed to explain property crime victimization, researchers argue (Newman & Clarke, 2003) that cyberspace provides ideal opportunities to commit crimes, as people are digitally connected with multiple devices, working, studying, networking, and playing online.

Lifestyle-based exposure and suitable targets

Yar (2005) suggests utilizing activities indicating online presence, such as social media use, and email use as a lifestyle component of RAT. Following this suggestion, studies (e.g., Choi, 2008; Holt et al., 2016) utilized hours spent online and social media activity as lifestyle-based exposure measures. Online lifestyle variables—online vocational and leisure activities, online risky leisure activities, and online risky vocational activities—have been used to measure the suitable target component (Choi, 2008). In his integrated cyber-LRAT, Choi (2008) concludes that the level of online lifestyle activities contributes to the potential for computer crime victimization.

In scams, secondary or repeat victimization occurs by default. Titus and Gover (2001) describe situations where victims who had already been "hooked" (that is, targeted and/or victimized) were regularly recontacted by scammers, sometimes with the same technique, other times in different scam scenarios. Whittaker and Button (2020) describe similar situations where COVID-19 related issues (increased isolation, psychological and fiscal losses) and demands (ordering pets as companions online) weaken the targets' abilities to recognize early signs of scams, thus, follow-up victimization occurs. Providing money to scammers often results in victims ending up on a special list of once successfully scammed victims (the "sucker list", see Balleisen, 2018). Scammers buy, sell, and trade lists of consumers who have fallen for a phone, mail, or email scam (Mayer, 2014). Providing money increases the risk of repeat victimization, making victims suitable targets. In these situations, contacting a trusted individual or reporting the scam to a designated agency can be a source of outside control and thus provide protection from repeat victimization.

Capable guardians

Following Choi (2008), subsequent studies have measured the digital-capable guardianship of technical guardians such as antivirus software and firewalls. However, studies produced mixed results: in some cases, security software failed to function as capable guardians (Leukfeldt & Yar, 2016) or even increased the risk of cybervictimization (Bossler & Holt, 2010; Ngo & Paternoster, 2011; Reyns, 2015). Ngo and Paternoster (2011) recommend operationalizing technical guardians as lifestyle measures instead of capable guardians, since security software can provide a false sense of protection to individuals who will in turn engage in online activities that disclose them as suitable targets for victimization. Studies also apply self-reported computer skills as a protective factor against cybercrime (Hawdon et al., 2020; Bossler & Holt, 2009; Ngo & Paternoster, 2011; Leukfeldt & Yar, 2016) since people with high levels of technical knowledge are more able to anticipate attacks and therefore have a lower risk of becoming a victim.

Self-control and online fraud victimization

According to the general theory of crime (Gottfredson & Hirschi, 1990), the main individual factor in causing crime and deviance is low self-control. Self-control is defined as the ability of the individual to exercise personal restraint in the face of tempting, immediate, and easy gratification both in the short and long term (Hirschi, 2004). While the general theory of crime was developed to explain criminal offending, it was later used to explain victimization as well (Piquero et al., 2005; Schreck, 1999; Schreck et al., 2006). Cybercrime victimization is explained with low self-control in several studies. Ngo and Paternoster (2011) applied the general theory of crime and the LRAT framework to assess the effects of individual and situational factors on cybercrime victimization. This study corroborated the effect of low self-control on person-based cybercrime (Bossler & Holt, 2010). In contrast, it did not find significant association between low self-control and cybercrime where computers were the target (Ngo & Paternoster, 2011). The authors recommended that future studies look at the effects of situational and individual variables on specific cybercrime victimization types, since the collapse of offenses into one general cybercrime category might be masking notable differences (Ngo & Paternoster, 2011).

Older people's vulnerability in a theoretical context

Although the overall crime victimization of older adults is lower than that of the younger ones (Holtfreter et al., 2014; Carcach et al., 2001; Graycar & James, 2001), out of the crime that older people experience,

fraud is the largest category (Temple, 2007; Smith & Budd, 2009). Gamble et al. (2014) associate financial fraud victimization of older Americans to decreasing cognition, overconfidence in one's financial knowledge, and a greater willingness to take financial risks relative to non-victims. Holtfreter et al. (2014) conducted telephone interviews on consumer fraud on a subject pool over the age of 60. Fraud victimization was relatively low, with approximately 14% past-year prevalence. Being male, shopping/purchasing remotely, having low self-control (impulsivity), a higher level of education, and past telemarketing purchases increased fraud *targeting* (attempt to defraud the individual); remote shopping/purchasing, low self-control, being older, and of minority status increased (actual) fraud *victimization*.

Reporting of fraud is low-level in general, but it is even lower amongst older adults (Beals et al., 2015a). First, older adults can downplay their cognitive deficits in order to maintain financial independence (Deevy & Beals, 2013). Many victims never report their fraud victimization, and even hide it from family members and caretakers for fear of being blamed (Cross, 2016). Thus, potential social guardians (i.e., relatives, family members) are not able to step in before a greater amount of financial loss manifests. However, underreporting not only distorts data on fraud victimization (Burnes et al., 2017), and limits our understanding of older people's fraud victimization, but also hinders the development of prevention programs and policies focusing on age-appropriate needs (DeLiema, 2018).

Few studies have tested RAT on older people's cyber fraud victimization. Hutchings and Heyes (2009) concluded that computer use predicted receiving a phishing email. In another study, Reisig and Holtfreter (2013) found that older adults who engage in remote purchasing activities such as making purchases over the phone, by mail, or online face a greater risk of being targeted by fraud. Pratt et al. (2010) examined the influence of routine online activities on Internet fraud targeting. Both time spent online and online purchasing activities significantly increased the odds of Internet fraud targeting.

Although situational factors had been examined, just a few studies have indicated the significance of sociodemographic information in impacting or determining the online fraud victimization of older adults. Adapting RAT to older individuals' financial fraud victimization, DeLiema (2018) suggests that aging individuals are the most vulnerable to fraud during cognitive and physical decline that are not fully recognized by social-capable guardians such as family members or medical professionals (DeLiema, 2018: 708). In a study of telemarketing fraud (AARP, 1996), victims were more likely to live alone than most in their age group in general, and less likely to seek advice on financial matters than non-victims. Therefore, social isolation is a risk factor in financial fraud (Fenge & Lee, 2018).

Contrastingly, the proxy of caring relatives can provide external control. For example, DeLiema (2018) found that fraud perpetrators took advantage of older adults when they had no trusted relatives or friends to safeguard their assets. DeLiema (2018) suggests expanding RAT by including trustworthy family members and friends, to study the effect of the presence of capable guardians in online fraud victimization of older adults. Aside of living alone, Kennedy et al. (2021) highlights additional risk factors such as having a full-time job, suggesting that employment and the absence of family members or relatives as social-capable guardians increase the stakes of experiencing financial loss.

In Whitty's (2019) research, victims of cyber fraud were more likely to be older, score high on impulsivity and addictive measures, and engage in more frequent routine activities that place them at high risk of becoming scammed. Educated people were more likely to be scammed. One explanation is that educated

people use the internet differently than the uneducated—that is, they have a more robust online presence and frequent more online spaces. Another possible explanation derives from the work of Lea et al. (2009) who suggest that overconfidence in the ability to recognize scams places people at a greater risk of becoming scammed. Educated people might have a false sense of security and make less effort to search for cues of manipulation. Whitty (2019) also found that online guardianship behaviors such as seeking advice on fraud information sites (Federal Bureau of Investigation, Federal Trade Commission) did not protect people from being victimized.

Overall, previous research highlights the need for further studying of the connection between lifestyle routine activities theory, low self-control, and online victimization, especially in older generations. In addition, it recommends extending the range of individual and situational level factors and examining specific kinds of cyber victimizations instead of using the collapsed category. Following up the above findings and recommendations, we formulated our research question: By applying LRAT and the general theory of crime, what are the differences (risk and protective factors), if any, between the situational and individual characteristics of younger and older victims when it comes to online fraud/scam victimization?

Methods

Sample

A national sample of US citizens 18 and older, representative by age, sex, and race was collected using Dynata (formerly SSI) research panel in October 2020. Utilizing random digit dialing, banner ads, and other permission-based techniques to recruit participants to create databases, Dynata provides online sampling and data collection for researchers. Dynata provides a small fee or reward to users who qualify for and participate in a survey. Of the 2,672 individuals who started the survey, 2,558 participants remained in the final sample. Individuals who failed to complete or sped through the survey were excluded. Victims 55 years of age and older comprised 32% (n=826) of the total sample, while those between 18 and 54 years of age made up 67.7% (n=1,732). While being victimized was 48.8% (n=1,249) in the full sample, 55+ individuals were slightly less likely (40.4%; n=334) to experience online fraud. Detailed demographics can be found in Table 1.

Analytical plan

The aim of the study was to map the patterns of online victimization among younger and older generations with the methods of logistic regression. The sample was divided into two distinct groups according to age; the younger age group included those between the age of 18 and 54, the older age group included those 55 years of age and above. Studies vary about determining the age of "older adults" when it comes to victimization. Some employed 50 (Lichtenberg et al., 2013, 2016), 55 (Pak & Shadel, 2011; Federal Trade Commission, 2003), 60 (Reisig & Holtfreter, 2013; Holtfreter et al., 2014), and 65 (Burnes et al., 2017; DeLiema, 2018; Fenge & Lee, 2018; Harrell, 2015; Anderson, 2004, 2007, 2013; Harrell & Langton, 2013; Holtfreter et al., 2006; AARP, 1999; Titus et al., 1995) years of age. We applied the age of 55 as a dividend between "younger" and "older" adults since people over 55 have not yet had computers and the internet as part of their everyday lives while growing up (Parker & Davey, 2014; Molnar, 1997). Thus, they had to attain digital literacy later in life, and consequently, they might have more difficulties detecting online scams. However, this generation, known as baby boomers, is worth about $9 trillion in the United States alone and climbing (AARP, 2019), which makes them a perfect target of online fraud.

Table 1. Demographics and other characteristics of the sample

	Whole sample N=2,558 (100.0%)	**Younger Victims (18-54) N=1,732 (67.7%)**	**Older victims (55+) N=826 (32.3%)**
Count measures			
Sex			
Male	1,224 (48.5)	770 (62.9)	454 (37.1)
Female	1,300 (51.5)	932 (71.7)	368 (28.1)
Race			
White	1,896 (74.1)	1,176 (62.0)	720 (38.0)
Nonwhite	662 (25.9)	556 (84.0)	106 (16.0)
Education			
Less than high school	67 (2.62)	54 (80.6)	13 (19.4)
High school	604 (23.65)	458 (75.8)	146 (24.2)
Some college or college degree	1,361 (53.29)	865 (63.6)	496 (36.4)
Masters, professional or higher	522 (20.44)	352 (67.4)	170 (32.6)
Living arrangement			
Living alone or as a single parent	698 (27.4)	453 (64.9)	245 (35.1)
Living w/partner no child in home	787 (30.8)	365 (46.4)	422 (53.6)
Living w/partner, child in home	667 (26.1)	585 (87.7)	82 (12.3)
Living w/ parents or other family type	378 (14.8)	306 (81.0)	72 (19.0)
Other (e.g., care facility)	22 (0.9)	18 (81.8)	4 (18.2)
Employment			
Paid job	1,563 (61.1)	1,300 (83.2)	1,300 263 (16.8)
Unemployed or retired	995 (38.9)	432 (43.3)	563 (56.6)
Continuous measures			
Age	**N / Mean / SD / Min-max** N=2,558 / Mean=44.75 / SD=17.31 / Min-Max=18-98	**N / Mean / SD / Min-max** N=1,732 / Mean=34.63 / SD=10.07 / Min-Max=18-54	**N / Mean / SD / Min-max** N=826 / Mean=65.97 / SD=7.05 / Min-Max=55-98

The analysis was performed using the SPSS 26 software package in two steps: first, we examined the effects of low self-control on and control variables of victimization by age group. In the second step, we examined victimization on LRAT and the control variables.

Dependent variables. Victimization was measured using six variables typical of online scams targeting older individuals. We adopted the scams scenarios used in this research from the FBI's "elder fraud" list (FBI, n.d., see also IC3 2020), including private info scam, IT support scam, grandparent scam, company impersonation scam, advance fee fraud, and romance scam. Questions had to be answered in a binary way (yes/no). Question details are displayed in Table 2. As a follow up question, the survey asked whether the individual suffered any other harmful consequences, such as losing money or experiencing distress. Only those who said "yes" were included as "victims." We ran the logistic regressions on these variables separately and broke them down into the two age groups.

Table 2. Scam scenarios (Dependent variables)

Survey question	Short name
"In the past 12 months, did you get a phone call or email directing you to go to your computer and send them private information about yourself and/or your family members, and/or send them money?"	Private info scam
"Some scammers call people pretending they are from an IT company, asking to allow remote access to the computer, and once they are given access, they lock the owner out. Then they ask for credit card details to repair the owner's computer. In the past 12 months, did you get into such situation?"	IT support scam
"Some scammers call people pretending they are their grandchildren/friends, asking for money to solve some unexpected financial problem. In the past 12 months, did you get a call from such a scammer?"	Grandparent scam
"In the past 12 months, did you receive an email from a seemingly legitimate company, bank, or institution asking you to 'update' or 'verify' your personal information via email?"	Company impersonation scam
"In the past 12 months, did you receive a call or email asking you to send money to someone so that, after everyone pays a certain amount, you would get back a greater amount of money?"	Advance fee fraud
"In the past 12 months, were you asked by someone you met on an online dating or social media platform to send them money or other donations, or to pay for their expenses?"	Romance scam

Independent variables. To examine the self-control variable, participants had to answer the following five statements with "true", "a bit true," or "not true": *1. I often get very angry and lose my temper; 2. I do dangerous things for fun; 3. I do exciting things, even if they are dangerous; 4. I'm a risk-taker; 5. I often act before I think about what I'm doing* (adapted from Vázsonyi et al., 2012). The Self-Control (SC) variable was constructed by summing up the "not true" (1) answers. The more statements participants considered "not true," the higher self-control value they got (Cronbach's alpha = 0.830).

Within LRAT, we measured three variable groups: Exposure to motivated offenders, target suitability, and capable guardianship. The exposure to motivated offenders was determined by the hours spent online, and if a participant used at least five different online services. The *hours spent online* variable measured the participants' time spent online, in hours, with the following items: *Playing online video games; Reading news or other articles online; Browsing social media like Facebook, Instagram, Twitter, etc.; On a computer, while working at a job; Shopping online; Other online activities.* The items were converted to one single variable, coding 0 for those who did not spend time with any mentioned online activity, and 3 who indicated

many hours spent online. We created an index variable from the six items ranging from 0 to 18 where the participant indicated 3 to all 6 items. The index variable named *online services* (OS) measure the frequency of social media use. Five variables were included in this category: social media, instant messenger, online games, dating services, and email services. If the respondent used one or more types of these online services they were coded with a yes (1), if they did not use any type of online services, they were coded with a no (0).

The target suitability dichotomous variable contained one question: *Did you provide money for the scammers?*, yes (1) or no (0). Finally, capable guardianship was measured by their self-reported level of computer knowledge, their usage of computer software, the application of nontechnical guardians, and whether or not they had contacted someone for help/reported. Participants had to judge their own computer knowledge on a five-grade ordinal Likert scale where the lowest level was *"I am uncomfortable using a computer"* and the highest level was *"I am comfortable manipulating or writing computer programming"*. The computer software technical guardian measure was dichotomously coded: the answer was either yes (1) if the participant used antivirus software and/or firewall, or no (0) if not. The nontechnical guardian variable incorporated non-software-based safeguards that users can apply beyond simple security software (Hawdon et al., 2020; Rader & Wash, 2015), such as covering web cameras, using identity theft protection monitoring, and freezing credit cards preemptively. The variable was scaled between 0 and 3, ranging from respondents who did not use any of these (0) to those who utilized all 3 of the nontechnical guardians. The last capable guardian, a willingness to ask for help or to report, referred to if they had contacted federal reporting agencies, IT assistance, civic organizations, retirement facility administrators, or other persons/agencies. This variable was dichotomized into yes (1) (contacted for help/reported anywhere) and no (0).

Control variables. We controlled self-control and LRAT for the same demographic variables: sex (male 1, female 0); race (white 1, nonwhite 0); education (less than a high school diploma 1, high school 2, college or some college 3, master's degree or higher 4); employment (paid job 1, in school, unemployed or retired 0); and living arrangement (living alone or single parent 1, living with a partner with no children in home 2, living with a partner with children in home 3, living with parents or other family types 4, and care facility, communal setting or other 5).

Results

In the first model (Table 3), a low level of self-control was a predictor of getting victimized by online scams in general, independent of age group, except for the grandparent scam. The grandparent scam is an exception as it only showed a significant relationship with low self-control in younger individuals. The predictor effect of low self-control was stronger in the older age group, except for grandparent (ORyv: .604, p<.001; ORov: .595, N.S.) and romance scam (ORyv: .592, p<.001; ORov: .494, p<.001). The controlling effect of gender was significant at the young age group in all online scams but was not significant in older individuals: the effect of gender was positive, with young males having significantly more risk of online victimization than older individuals in all online scams. For the education control variable, master's or higher degree showed a significant positive relationship with online victimization in young individuals. However, education came out as irrelevant in predicting victimization amongst older people in all online scams. The strongest effect of high-level education in younger individuals was observed at private information scams (ORyv: 3.135, p<.01), company impersonation scams (ORyv: 3.284, p<.01), and romance scams (ORyv: 4.448, p<.01). Highly

educated individuals between 18 and 54 years of age are more endangered by any type of scams than individuals 55 years of age and above, but especially in the latter three types of scams. The type of living arrangement did not show any significant relationship with online victimization, independent of age group: older people living alone are not more at risk of online victimization than younger ones.

In the second model, we looked at the effects of LRAT variables in the scam categories, together with the same controls. LRAT variables were classified into three groups: Exposure to motivated offenders; Target suitability; and Capable guardianship. The predictive effects of the LRAT variables and control measures are displayed in two separate tables: Table 4 displays the results of the logistic regression of the six forms of online fraud on LRAT measures and controls in younger victims, whereas Table 5 displays the same measures and controls in older victims.

Contrary to previous research findings, time spent online was not predictive of online victimization. Among the exposure to motivated offender variables, the impact of online games was only significant for younger participants' victimization in the IT support scam. This indicates that younger individuals who often play online games are more likely to fall victim to IT support scams than older individuals. The use of dating services was also a predictor of younger people's susceptibility to the grandparent scam and romance scam. Younger visitors of dating websites are therefore more likely to fall victim to grandparent and romance scams than older individuals. None of the variables was a predictor of victimization in the older age group regarding the exposure to motivated offenders' variable group.

Target suitability was measured by whether the target provided money to the offender. According to research (Balleisen, 2018; Mayer, 2014), providing money to scammers generates a cascade of victimization: those who paid an offender once would have a better chance of being victimized again. Target suitability variables showed a stronger association with online victimization than any other variable in the exposure of motivated offenders' group; therefore, our hypothesis has been supported. However, the company impersonation scam in both victim groups, and the private information scam in the older victims' group—where providing money to the offenders didn't indicate further victimization—reflect a more sophisticated picture. It seems that older people can protect their private data better than younger ones, since, contrary to younger people, their age did not show a statistically significant relationship with falling victim to the private information scam victimization.

Capable guardianship, the third variable group of LRAT, only showed a significant relationship with age group amongst younger individuals for the grandparent scam. The impact is negative, hence, young people with low level computer skills were more likely to be victimized by grandparent scams. Computer skills level was not an indicator of any cyber fraud victimization in older individuals. However, having defensive computer software (technical guardians) installed proved to be a protective factor for older individuals in romance scams. Older respondents not having antivirus software installed or a firewall were more prone to victimization of romance scams.

Having a nontechnical guardian (webcam covers, identity theft monitoring, and freezing credit cards) showed a more diverse and somewhat confusing picture: a nontechnical guardian was a significant predictor for both age groups in IT support scams. However, it was a predictor for younger individuals in the case of grandparent, company impersonation, advance fee fraud, and romance scam. This result indicates that nontechnical means of protection not only did not provide protection, but that those younger people who utilized such guardians were more likely to be victimized for a variety of scams.

Table 3. Logistic regression of six forms of online scams on low self-control and control variables (YVn=1,695; OVn=821; ∑n=2,516)

	Private info scams		**IT support scams**		**Grandparent scams**		**Company im-personation**		**Advance fee frauds**		**Romance scams**	
	YV	**OV**	**YV**	**OV**	**YV**	**OV**	**YV**	**OV**	**YV**	**OV**	**YV**	**OV**
Low self-control	-.445*** (.641)	-.260*** (.771)	-.437*** (.646)	-.327*** (.721)	-.503*** (.604)	-.519 (.595)	-.298*** (.742)	-.160** (.852)	-.484*** (.616)	-.357*** (.700)	-.524*** (.592)	-.705*** (.494)
Male	.350** (1.419)	.255 (1.291)	.563*** (1.756)	.240 (1.271)	.685*** (1.984)	-.403 (.668)	.275* (1.317)	.144 (1.155)	.459** (1.583)	.317 (1.373)	.715*** (2.043)	.693 (1.999)
White	.065 (1.067)	.015 (1.015)	.004 (1.004)	.304 (1.355)	.027 (1.027)	.466 (1.593)	.126 (1.134)	.508 (1.662)	.137 (1.147)	-.208 (.812)	-.002 (998)	.853 (2.346)
High school	.148 (1.160)	.089 (1.093)	-0.138 (.871)	.580 (1.785)	-.064 (.938)	.388 (1,474)	.158 (1.171)	.480 (1.617)	-.183 (.833)	-.191 (.826)	.214 (1.239)	-1.180 (.307)
College	.480 (1.616)	.326 (1.385)	.029 (1.030)	.289 (1.335)	.022 (1.022)	-.577 (.531)	.652 (1.919)	.624 (1.866)	.199 (1.220)	-.270 (.763)	.511 (1.667)	-.526 (.591)
Master's or higher degree	-1.142** (3.135)	.992 (2.698)	.866* (2.377)	.840 (2.315)	1.046* (2.847)	.002 (1.002)	1.198** (3.284)	.832 (2,298)	.933* (2.541)	.420 (1.521)	1.492** (4.448)	.166 (1.180)
Employed	.201 (1.223)	.140 (1.150)	.251 (1.285)	-.154 (.858)	.176 (1.193)	.529 (1.696)	-.031 (.969)	.106 (1.112)	-.032 (.969)	.483 (1.621)	.153 (1.165)	.821* (2.274)
Living alone or single parent	.793 (2.210)	-.563 (.570)	1.875 (6.518)	-.200 (.819)	19.914 (4.453)	-.876 (.417)	.427 (1.533)	.503 (1.654)	1.536 (4.648)	-.708 (.493)	19.914 (4.573)	.528 (1.696)
Living w/ partner no child home	.969 (2.635)	.106 (1.112)	1.987 (7.292)	-.034 (.967)	20.259 (6.287)	-.445 (.617)	.642 (1.901)	.660 (1.935)	1.879 (6.550)	-.379 (.685)	20.116 (5.446)	-.420 (.657)
Living w/ partner child home	1.173 (3.233)	.123 (1.131)	2.024 (7.566)	.027 (1.027)	20.164 (5.718)	.206 (1.229)	.834 (2.203)	.865 (2.375)	2.059 (7.835)	.050 (1.051)	20.252 (6.243)	.678 (1.969)
Living w/ parents or other family type	-.164 (.849)	.463 (1.589)	1.175 (3.237)	-.222 (.801)	18.910 (1.632)	-.959 (.383)	-.012 (.988)	.016 (1.017)	.835 (2.305)	-.036 (.965)	18.997 (1.779)	.723 (2.061)
Constant	-1.534* (.216)	-1.499 (.223)	-2,514* (.081)	-1.497 (.224)	-20.947 (.000)	-.732 (.481)	-1.309 (.270)	-2.156 (.116)	-2.428* (.088)	-.946 (.388)	-21.292 (5.664)	-2.233 (.107)
Model Chi-Square	376,126 ***	47.333 ***	360.144 ***	37.313 ***	425.433 ***	60.690 ***	239.048 ***	25.590 **	376.723 ***	49.917 ***	448.310 ***	85.078 ***
df	11	11	11	11	11	11	11	11	11	11	11	11
p	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
Pseudo-R-Square	.280	.101	.276	.083	.338	.194	.181	.044	.297	.137	.352	.315

Note: Entries are unstandardized coefficients; Odds ratios are in parentheses; YV=Younger Victims, OV=Older Victims. *p<.05; **p<.01; ***p<.001

Among the capable guardian variables, contacting for help was a significant predictor of IT support scam victimization in younger people: those younger individuals who reported the crime or asked for help were more likely to fall victim to IT support scams than those who did not report them. Both age groups were more likely to fall victim to grandparent, advance fee, and romance scams if they reported it or asked for help. However, the predictor effect of asking for help/reporting was higher in the older age group: those older victims who asked for help or reported the scam were prone to victimization in grandparent, advance fee, and romance scams.

Among the control variables, the effect of gender remained significant in most scams. Young men were more likely to be victimized by IT support, grandparent, and romance scams according to the model, with romance scam showing a significant association with gender in the case of both younger and older men. Race was also significant in this second model, with younger white individuals being more likely victimized by private information, IT support, and advance fee scams. The effect of education was not significant in the model, but, for IT support scams, the effect of employment was. Older employed respondents were less likely to fall victim to this specific scam category. For a detailed associations of variables see Tables 4 and 5.

Table 4. Logistic regression of six forms of online fraud on LRAT measures and control variables in Younger Victims (YVn=754)

	Private info scams	**IT support scams**	**Grandparent scams**	**Company impersonation**	**Advance fee frauds**	**Romance scams**
Exposure to motivated offenders						
Hours spent online	.011(1.011)	-0.18(.982)	-.042(.959)	-.029(.971)	-.002(.998)	-.013(.987)
OS: Social media	.244(1.276)	-21.729(0)	-.586(.557)	-20.585(0)	-.396(.673)	-.447(.640)
OS: IM	.003(1.004)	-.273(.761)	-.356(.701)	-.177(.838)	.193(1.149)	-.024(.977)
OS: Online games	-.266(.766)	.445*(1.560)	-.258(.772)	.175(1.192)	-.257(.774)	-.259(.772)
OS: Dating services	.150(1.161)	.252(1.287)	1.097**(2.995)	.203(1.225)	.201(1.223)	1.184**(3.268)
OS: Email	-.018(.982)	-.128(.880)	-.320(.726)	.131(1.140)	.173(1.188)	.018(1.018)
Target suitability						
Provided money to scammers: Yes	1.029*** (2.798)	1.037*** (2.820)	1.446*** (4.247)	-.336 (.715)	1.170*** (3.223)	1.802*** (6.064)
Capable guardianship						
Computer knowledge	-.196(.822)	-.255(.775)	-.976**(.377)	-.128(.880)	-.335(.716)	-.120(.887)
Computer software	.136(1.145)	-.138(.87)	.205(1.227)	.293(1.340)	.156(1.169)	.152(.1.164)
Nontechnical guardian	.110 (1.116)	.268** (1.307)	.334** (1.396)	.334*** (1.397)	.367*** (1.443)	.379*** (1.461)
Contacting for help: Yes	.367 (1.444)	.660** (1.935)	.953** (2.593)	.351 (1.421)	.586* (1.796)	.615* (1.851)

Control variables						
Male	.267(1.306)	.365*(1.441)	.512*(1.669)	-.038(.963)	.115(1.122)	.719***(2.053)
White	.509**(1.664)	.422*(1.524)	.418(1.518)	.295(1.343)	.419*(1.521)	.339(1.404)
High school	-.455(.634)	-.012(.988)	.264(1.302)	-.995(.370)	-.321(.725)	.934(2.545)
College	-.435(.647)	-.245(.783)	-.017(.983)	-.721(.486)	-.159(.853)	.738(2.092)
Master's or higher	-.120(.887)	.145(1.155)	.278(1.320)	-.169(.845)	.096(1.101)	1.113(3.044)
Employed	.335(1.397)	.418(1.519)	.117(1.124)	-.238(.788)	-.423(.655)	.170(1.185)
Living alone or single parent	.285(1.330)	20.262(6.304)	19.250(2.291)	-20.718(0)	-.508(.602)	20.028(4.990)
Living with partner no child in home	.362(1.437)	20.087(5.292)	19.740(3.742)	-.20.624(0)	-.162(.851)	19.947(4.602)
Living with partner child in home	.481(1.618)	19.975(4.773)	19.526(3.021)	-20.592(0)	-.061(.940)	20.008(4.889)
Living with parents or other family type	-.415(.660)	19.833(4.107)	18.845(1.529)	-21.068(0)	-.664(.515)	1.419(2.714)
Constant	-1.435(.238)	.062(1.064)	-20.778(0)	42.084(1.891)	-.943(.389)	23.442(0)
Model Chi-Square	152.367***	199.735***	320.099***	64.503***	194.440***	316.988***
df	21	21	21	21	21	21
P	.000	.000	.000	.000	.000	.000
Pseudo-R-Square	.248	.311	.470	.115	.303	.458

Note: Entries are unstandardized coefficients; Odds ratios are in parentheses; YV=Younger Victims, OV=Older Victims. *p<.05; **p<.01; ***p<.001

Table 5. Logistic regression of six forms of online fraud on LRAT measures and control variables in Older Victims (OVn=306)

	Private info scams	**IT support scams**	**Grandparent scams**	**Company impersonation**	**Advance fee frauds**	**Romance scams**
Exposure to motivated offenders						
Hours spent online	.039(1.040)	.041(1.042)	-.162(.850)	.022(1.022)	.058(1.060)	0.54(1.056)
OS: Social media	.229(1.258)	.144(1.155)	-.275(.760)	-.307(.736)	1.386(3.998)	-.163(.850)
OS: IM	0.26(1.026	-.682(.506)	.046(1.048)	-.361(.941)	-.210(.811)	.262(1.300)
OS: Online games	.176(1.192)	.022(1.022)	1.152(3.165)	.894 (2.445)	.220(1.246)	.150(1.162)
OS: Dating services	-.164(.849)	-0.31(.969)	-19.249(0)	-2.019(.133)	-.580(.560)	1.372(3.943)

Table 5. Logistic regression of six forms of online fraud on LRAT measures and control variables in Older Victims (OVn=306)

OS: Email	.043(1.044)	.128(1.136)	-.551(.576)	.036(2.446)	.061(1.063)	-.945(.389)
Target suitability						
Provided money to scammers: Yes	.505 (1.656)	1.597* (4.939)	2.658*** (14.266)	.894 (2.446)	1.315* (3.724)	3.279*** (26.558)
Capable guardianship						
Computer knowledge	-.824(.439)	-.848(.428)	-.384(.681)	-.469(.625)	-.447(.640)	-.836(.434)
Computer software	.194(1.214)	.001(1.001)	-.280(.756)	.296(1.345)	-.292(,747)	-1.436*(.238)
Nontechnical guardian	.271 (1.312)	.366* (1.442)	-.011 (.989)	-.119 (.888)	.322 (1.379)	.289 (1.335)
Contacting for help: Yes	.452 (1.572)	.478 (1.613)	.985* (2.677)	.065 (1.068)	.690* (1.994)	1.168* (3.217)
Control variables						
Male	.319(1.375)	.410(1.506)	-.437(.646)	.133(1.143)	.365(1.440)	1.310*(3.706)
White	-.113(.893)	.548(1.729)	.479(1.615)	.228(1.256)	.063(1.065)	2.356(10.548)
High school	20.466(7.579)	21.007(1.328)	20.694(9.713)	-20.177(0)	20.156(5.669)	18.525(1.110)
College	20.936(1.237)	20.789(1.068)	19.556(3.113)	-20.270(0)	19.860(4.217)	19.545(3.079)
Master's or higher	21.561(2.312)	21.74(1.420)	19.004(1.792)	-20.145(0)	20.285(6450)	19.558(3.213)
Employed	-.078(.925)	-.764*(.466)	.322(1.381)	.249(1.283)	.097(1.101)	.116(1.123)
Living alone or single parent	-20.532(0)	-19.817(0)	21.087(0)	-19.744(0)	-20.225(0)	-18.006(0)
Living w/ partner no children in home	-19.876(0)	-19.767(0)	20.444(0)	-19.508(0)	-20.067(0)	-18.845(0)
Living w/ partner children in home	-19.632(0)	-19.734(0)	19.855(0)	-19.388(0)	-19.440(0)	-18.455(0)
Living w/ parents or other family type	-18.798(0)	-19.387(0)	21.148(0)	-20.172(0)	-19.745(0)	-18.034(0)
Constant	-2.197(.111)	-2.782(.062)	.138(1.148)	40.754(5.001)	-3.569(.028)	-5.373(.005)
Model Chi-Square	49.195***	49.376***	71.482***	17.565	53.586***	96.325***
df	21	21	21	21	21	21
p	.000	.000	.000	.000	.000	.000
Pseudo-R-Square	.205	.211	.371	.079	.253	.531

Note: Entries are unstandardized coefficients; odds ratios are in parentheses. OS=Online Services.
*p<.05; **p<.01; ***p<.001

Discussion

Our data corroborates the findings of previous research that established a connection between low self-control and cybercrime victimization (Bossler & Holt, 2010; Ngo & Paternoster, 2011; Reyns, 2015). With the exception of grandparent scams, low self-control showed significant risk of victimization for all online scamming, with stronger associations amongst older people. This is unsurprising since when a loved one calls and asks for money, it is not low self-control but rather affections, care, and anxiety that make the target pay the scammer. Research shows that online fraud can involve manipulation techniques that play into emotions. Because of these intense emotions, targets are less capable of making rational judgements about requests or demands (Chantler & Broadhurst, 2008).

We have examined LRAT applying all three theory tenets: exposure to motivated offenders, target suitability, and capable guardianship. Among the exposure to motivated offender variables, using dating services and playing online games made younger victims vulnerable. However, none of the variables indicated older people's victimization. Thus, other variables not included in this analysis should be responsible for older people's victimization of online scams. Most surprisingly, excessive time spent online and high engagement in various online activities (e.g., social media, instant messenger, and email services) did not predict online victimization.

In contrast, providing money to scammers was associated with online victimization in both younger and older adults. Except for company impersonation scams, paying money to scammers puts people at greater risk of future victimization regardless of age. However, there were differences in strengths of association: older people were more strongly at risk of grandparent scams and romance scams. This result indicates that paying money to scammers makes older people more at risk of these particular scams. In other words, it does not matter how strongly older people are advised not to pay, grandparent and romance scams are very subtle forms of manipulations that can easily occur multiple times to one person. The fact that the association of paying the scammers and victimization was stronger for older individuals suggests that older generations need substantially more awareness in early recognition and assistance to build resistance against these scams.

With former research having similar results regarding cybercrime (Leukfeldt & Yar, 2016; Bossler & Holt, 2010; Ngo & Paternoster; Reyns, 2015), it is unsurprising that installing antivirus software or a firewall did not prevent online scam victimization in the current research either. Online scammers apply social engineering techniques to extract money or private information from targets, and computer savviness does not help in recognizing that kind of deception. Computer knowledge was only significant in younger people's grandparent scam victimization, indicating that for younger people, attaining basic computer knowledge was necessary to be able to recognize this type of scam. Scammers can apply multiple contact methods (via phone, text messaging, and email), and emails can contain tell-tale signs of deception which require at least some basic computer skills to recognize. In the meantime, the sample contained a relatively well-educated older subsample, who did not have as much problem identifying scams as their younger counterparts did.

Applying nontechnical guardians, such as covering webcams, identity theft monitoring, and freezing credit cards did not seem to mitigate the risk of victimization either. On the contrary, younger individuals who applied these nontechnical guardians were more prone to victimization, while it was not a protective factor for older individuals. According to one possible explanation, those younger individuals who applied these guardians did so because of prior victimization. However, due to the increased susceptibility which

comes from having been scammed before, they helped little to prevent follow-up victimization. To explain these anomalies, it is recommended to investigate what types of technical and nontechnical guardians can help prevent online fraud committed using highly manipulative social engineering methods.

Contacting for help had negative effects on victimization, similar to the application of technical and nontechnical guardians. Those who reported or asked for help, were at a higher risk of victimization for most online scams (IT support, grandparent, advance fee fraud, and romance scams for younger individuals, and grandparent scam, advance fee, and romance scams for older individuals). This suggests that reporting or asking for help does not necessarily help prevent scam victimization. Outside sources, such as communities, employers, family and friend networks need specific awareness-raising education tailored to a range of scam types. Prevention programs should ideally provide information about the latest scam scenarios to not only older people, but also to the network of individuals around them that can help guard against scamming. These concerns make sense particularly when we look at the results indicating that education, employment, and living arrangement did not have any influence on scam victimization either.

According to the analysis, having masters or higher professional degrees was not a protective factor, but rather predictor of online fraud victimization. Previous research posits that highly educated people are more likely to fall victim to online fraud and lose more than lower educated people (Gamble et al., 2014). This is a possible indication that, having higher salaries, highly educated people have more money to risk in general. However, this result might as well be connected to their level of self-confidence: people who are confident in handling large amounts of money, will eventually lose more because they risk more (Gamble et al., 2014). Nevertheless, this explanation is only feasible in younger respondents in the current research. The above finding also suggests that education is not a panacea against online scams, and instead, awareness raising campaigns can and should be the way to prevent online manipulations.

Although employment did not make any difference when it was examined in relation to low self-control, it did show a significant negative relationship with IT support scam victimization in older adults when LRAT differences were measured by age group. This indicates that the employer's secure network can prov ide protection against only this type of scam and only for older people. Perhaps older employees are more concerned about maintaining the integrity of their employers' computer network than younger ones (since IT support scams could easily lead to blocking an employer's network, contrary to the other scams that endanger private assets instead of employer network and data). Another possible explanation is that employee trainings are designed in such a way that is more appropriate for older employees than younger ones. Thus, employers' fraud awareness trainings—which employees must pass from time to time in order to be able to continue the job—need age-appropriate developments.

Living in a childless relationship might mean safer financial conditions, but the lack of grown-up children or other relatives in close proximity (i.e., social-capable guardians) might result in more victimization (Kennedy et al., 2021; DeLiema, 2018). Others find that living with family makes people less cautious in spending money online (Kadoya et al., 2021). Our results add to the mixed findings about the role of living arrangements in scam victimization, since, in connection to low self-control and LRAT measures, living alone did not predict older (or younger) people's scam victimization.

Conclusions and limitations

We examined the effects of situational (LRAT), self-control, and sociodemographic variables on scam

victimization to find out whether scams work differently by age group. Victimization was relatively high (48%) in the full sample. While it would be unusual to any official crime statistics, surveys in fact provide a more robust picture of crime victimization (Biderman & Reiss, 1967). Therefore, in the case of highly manipulative online scams that are vastly underreported (Beals et al., 2015a), it is quite realistic that survey respondents are more likely to admit victimization, hence, survey victimization rate will be higher compared to official crime statistics.

The analyses proved that scams affect individuals, independent of age. Moreover, similar factors are determinant and responsible for scam victimization in young and old ages. However, there are some subtle differences that make older individuals more vulnerable to scams than younger ones.

The most compelling research finding was that low self-control is a predictor of most scam victimization, however it is a stronger one in older adults. LRAT measures did not show a statistically significant predictor effect of scams overall, regardless of age group, although some specific measures did. For example, visiting dating websites, applying nontechnical guardians (webcam covers, identity theft monitoring, freezing credit cards), masters' degree and higher education made younger people more vulnerable to some scams. Perhaps younger individuals are more confident and less careful about sending money to unverified sources. For older individuals, low self-control and not reporting or asking for help were stronger predictors of scam victimization. However, low self-control did not influence emotion-based scam victimization such as grandparent and romance scams in older age groups. A possible explanation is that in these scenarios, the emotional pressure to send money to a loved one is much higher than in other scams.

Asking for help and reporting scams were strong predictors of victimization, however it is not possible to know when exactly the victims reached out to a helping source (i.e., whether after the first or after multiple occurrences of scam victimization). Nevertheless, those who reported or asked for help anywhere were more likely to experience scams, and this effect was stronger in older people's grandparent and romance scam victimization. Whether scam reporting and asking for help raises scam awareness and, in doing so, prevents subsequent victimization, must be studied in the future. In light of previous research (Cross, 2020) suggesting that adequate help can reduce repeat victimization, it is highly recommended to investigate how reporting/helping can reduce repeated scam victimization.

The findings according to which most LRAT measures were not indicative of scam victimization can be rooted in underlying factors. *First*, most scams in this survey targeted people via the phone (in three scenarios the initial connection was established via a phone call, in one scenario via phone call or email, and two mentioned email or online connections). This suggests the target went to the computer after the bait was set via the phone, when the necessary trust between the scammer and target was established. In such situations, computer knowledge (i.e., how to surf the net, or fix computer problems and write programs), anti-virus software or webcam covers do not provide protection. Consequently, we suggest that scam victimization must be measured utilizing variables developed specifically to sophisticated and highly manipulative scams that play with emotions and put enormous psychological pressure on the targets. A range of specific capable guardians must be developed in the future to adequately measure scam victimization.

Second, those variables usually applied in measuring suitable targets in cybercrime must be adjusted to measure the suitable target component specific to scamming. Providing money showed a strong relationship with victimization. However, the survey was not suited to investigate subsequent victimizations. Similarly

we could not measure follow-up victimizations in light of asking for help or reporting. Therefore, the author suggests developing a more appropriate measurement of motivated offenders and including variables investigating the effect of reporting. In addition, we have seen that everyday online activity (social media presence, email use, etc.) did not elevate the risk of scam victimization, regardless of age (except for visiting dating websites, which was predictive of younger people's romance scam victimization). Perhaps level of trust and factors such as mental health and cognitive decline also have to do with scam victimization; future research must investigate their effects as well.

Third, the effect of sociodemographic variables on scam victimization must be further investigated. Education can cause overconfidence in being able to identify scammers and might result in sending money to unverified callers or recklessly answering phishing emails. It remains yet to determine how exactly education could provide protection, including through scam awareness. According to the data, employment provided protection to older people, but only against IT support scams. Therefore, research must investigate what risk factors are connected to having a job, and what kind of protection an employer's secure computer network can provide against scams. It must also be examined how employee trainings should be improved to provide adequate scam preparation for employees, in order to establish age appropriate and needs-based trainings.

References

AARP (1996). Telemarketing fraud and older Americans: An AARP survey. *Washington, DC: American Asociation of Retired Persons*. Retrieved December 29, 2021, from, https://www.ojp.gov/ncjrs/virtual-library/abstracts/telemarketing-fraud-and-older-americans-aarp-survey

AARP (1999). Consumer behavior, experiences and attitudes: A comparison by age groups. *Washington DC: American Association of Retired Persons*. Retrieved December 29, 2021, from, http://assets.aarp.org/rgcenter/consume/d16907_behavior.pdf.

Anderson, K.B. (2004). Consumer fraud in the United States: An FTC survey. *Staff Report of the Bureaus of Economics and Consumer Protection. Federal Trade Commission*. Retrieved December 29, 2021, from, https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf.

Anderson, K.B. (2007). Consumer fraud in the United States: The second FTC Survey. *Staff Reportof the Bureaus of Economics and Consumer Protection. Federal Trade Commission*. Retrieved December 29, 2021, from, https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-second-federal-trade-commission-survey-staff-report-federal-trade/fraud.pdf.

Anderson, K.B. (2013). Consumer fraud in the United States, 2011: The third FTC survey. *Staff Report of the Bureaus of Economics and Consumer Protection. Federal Trade Commission*. Retrieved December 29, 2021, from, https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf.

Balleisen, E.J. (2018). The "sucker list" and the evolution of American business fraud. *Social Research, S5* (4), 699-727.

Beals, M.E., Carr, D.C., Mottola, G.R., Deevy, M.J., & Carstensen, L.L. (2015a). How does survey context impact self-reported fraud victimization? *The Gerontologist, 57*(2), 329-340

Beals, M.E., DeLiema, M., & Deevy, M. (2015b). Framework for a taxonomy of fraud. Stanford Center on Longevity and FINRA Investor Education Foundation. Retrieved December 29, 2021, from, http://longevity3.stanford.edu/framework-for-a-taxonomy-of-fraud/.

Biderman, A.D. & Reiss JR, A.J. (1967). On exploring the "dark figure" of crime. *The Annals of the American Academy of Political and Social Science, 374*(1), 1-15.

Bossler, A.M. & Holt, T.J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bossler, A., Holt, T. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227-236.

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-e22.

Carcach, C., Graycar, A. & Muscat, G. (2001). The victimisation of older Australians. *Trends and Issues in Crime and Criminal Justice, 212*, 1-6. Canberra: Australian Institute of Criminology. Retrieved December 29, 2021, from, https://www.aic.gov.au/publications/tandi/tandi212.

Chantler, A. & Broadhurst, R. (2008). Social engineering and crime prevention in cyberspace. Brisbane, QLD, Australia: Queensland University of Technology. Technical report. Retrieved from: https://eprints.qut.edu.au/7526/ [Accessed January 4, 2022]

Choi, K-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-560.

Cross, C. (2016). "They're very lonely": Understanding the fraud victimisation of seniors. *International Jounal for Crime Justice and Social Democracy, 5*, 4, 60–75.

Cross, C. (2020). Responding to individual fraud: Perspectives of the fraud justice network. In E. R. Leukfeldt & T. J. Holt (Eds.) The Human Factor of Cybercrime (pp. 359-388) New York: Routledge Studies in Crime and Society

Deevy, M. & Beals, M. (2013). The scope of the problem: An overview of fraud prevalence measurement. *Stanford University Financial Fraud Research Center*. Retrieved December 30, 2021, from, http://longevity3.stanford.edu/the-scopeof-the-problem-an-overview-of-fraud-prevalencemeasurement

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist, 58*(4), 706–718.

FBI (n.d.) Elder fraud. Federal Bureau of Investigation. *FBI.gov*. Retrieved December 30, 2021, from, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud

Federal Trade Commission (2003). Identity theft survey report. *Federal Trade Commission*. Retrieved December 30, 2021, from, https://www.ftc.gov/sites/default/files/documents/reports/federaltrade-commission-identity-theft-program/synovatereport.pdf

Felson, M. (1986). Routine activities, social controls, rational decisions and criminal outcomes. *In D. Cornish & R. Clarke (Eds.), The reasoning criminal* (pp. 302-327). New York: Springer.

Fenge, L-A. & Lee, S. (2018). Understanding the risks of financial scams as part of elder abuse prevention. *British Journal of Social Work, 48*, 4, 906–923.

Gamble, K.J., Boyle, P., Yu, L., & Bennett, D. (2014). The causes and consequences of financial fraud among older Americans. *Center for Retirement Research at Boston College.* Retrieved January 4, 2022, from, https://crr.bc.edu/wp-content/uploads/2014/11/wp_2014-13.pdf

Gottfredson, M.R. & Hirschi, T. (1990). The General Theory of Crime. Stanford, *CA: Stanford University Pess.*

Graycar, A. & James, M. (2001). Older people and consumer law. Paper presented at 4th National Outlook Symposium on Crime in Australia: New Crimes or New Responses, Canberra 21-22 June 2001. Australian Institute of Criminology. Retrieved December 30, 2021, from, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.580.6967&rep=rep1&type=pdf

Hall, J.E., Karch, D.L., & Crosby, A.E. (2016). Elder abuse surveillance: Uniform definitions and recommended core data elements for use in elder abuse surveillance, *Version 1.0, Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention*. Retrieved December 30, 2021, from, https://www.cdc.gov/violenceprevention/pdf/ea_book_revised_2016.pdf

Harrell, E. (2015). Victims of identity theft, 2014. Revised 13 November 2017. *US Department of Justice, Bureau of Justice Statistics.* Retrieved December 30, 2021, from, https://bjs.ojp.gov/content/pub/pdf/vit14.pdf

Harrell, E. & Langton, L. (2013). Victims of identity theft, 2012. *US Department of Justice, Bureau of Justice Statistics*. Retrieved December 30, 2021, from, http://www.bjs.gov/content/pub/pdf/vit12.pdf

Hawdon, J., Parti, K., & Dearden, T. (2020). Cybercrime in America amid COVID. The initial results of a natural experiment. *American Journal of Criminal Justice, 45*, 5460562.

Hindelang, M. J., Gottfredson, M. R., Garofalo, J. (1978). Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization. Cambridge, MA: *Ballinger Publishing Co*.

Hirschi, T. (2004). Self-control and crime. *In R.F. Baumeister & K.D. Vohs (Eds.), Handbook of Self-Regulation: Research, Theory, and Applications* (pp. 537-552). New York: Guilford Press.

Holt, T.J., Bossler, A.M., Malinski, R., & May, D.C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32*(2), 108-128.

Holtfreter, K., Reisig, M.D., & Blomberg, T.G. (2006). Consumer fraud victimization in Florida: An empirical study. *St Thomas Law Review, 18*(3), 761–789.

Holtfreter, K., Reisig, M.D., & Pratt, T. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189-220.

Holtfreter, K., Reisig, M.D., Mears, D.P., & Wolfe, S.E. (2014). Financial exploitation of the elderly in a consumer context. Research report. *Center for Victim Research*. Retrieved December 30, 2021, from, https://ncvc.dspacedirect.org/bitstream/id/2044/Financial%20Exploitation%20of%20the%20Elderly_IR_508.pdf

Hutchings, A. & Heyes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'net'?, *Current Issues in Criminal Justice, 20*(3), 433-451.

IC3 (2020) Elder fraud report. *Federal Bureau of Investigation, Internet Crime Complaint Center*. Retrieved December 30, 2021, from, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

Kadoya, Y., Khan, M.S.R., Narumoto, J.N., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, https://doi.org/10.3389/fpsyg.2021.649565

Kennedy, L.W. & Forde, D.R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology, 28*(1), 137-151.

Kennedy, J.P., Rorie, M., & Benson, M.L. (2021). COVID-19 frauds: An exploratory study of victimization during a global crisis. *Criminology & Public Policy, Epub ahead of print.* https://doi.org/10.1111/1745-9133.12554

Kowalski, M. (2002). Cyber-crime: Issues, data sources, and feasibility of collecting police-reported statistics. *Ottawa: Statistics Canada*

Lea, S.E.G., Fischer, P., & Evans, K. M. (2009). The psychology of scams: Provoking and committing errors of judgement, report for the office of fair trading. Retrieved December 30, 2021, from, from https://ore.exeter.ac.uk/repository/handle/10871/20958

Leukfeldt, E. R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Lichtenberg, P.A., Stickney, L., & Paulson, D. (2013). Is psychological vulnerability related to the experience of fraud in older adults?, *Clinical Gerontologist, 36*(2), 132–146. https://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*(1), 48–63. https://doi:10.1080/07317115.2015.1101632

Massey, J., Krohn, M., & Bonati, L. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency, 26*(4), 378-400.

Mayer, C. (2014). The scam of all scams: Sucker lists. *Forbes*. Feb 18, 2014. Retrieved January 4, 2022, from, https://www.forbes.com/sites/nextavenue/2014/02/18/the-scam-of-all-scams-sucker-lists/?sh=39ce90f64393

Miethe, T., Stafford, M., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/ lifestyle theories. *American Sociological Review, 52*, 2, 184-194.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B.L., Savolainen, I., Sirola, A., Zych, I., & Paek, H-J. (2021). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*, Epub ahead of print, https://doi.org/org/10.1177/0306624X20981041

Moitra, S.D. (2005). Developing policies for cyber crime. *European Journal of Crime, Criminal Law and Criminal Justice, 13*(3), 435-464.

Newman, G.R. & Clarke, R.V.G. (2003). Superhighway Robbery: Preventing E-commerce Crime. United Kingdom: *Willan*.

Ngo, F.T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individuals and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Pak, K. & Shadel, D. (2011). AARP Foundation national fraud victim study. Washington, DC: *AARP*. Retrieved December 30, 2021, from, https://assets.aarp.org/rgcenter/general/fraud-victims-11.pdf

Parker, K. R., Davey, B. (2014). Computers in schools in the USA: A social history. In A. Tatnall & B. Davey (eds.) History of computers in education. *IFIP AICT, 424*, (pp. 203–211) Springer.

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-control, violent offending and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology, 21*(1), 55-71.

Pratt, T. C., Holtfreter, K., & Reisig, M. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Pratt, T.C., Turanovic, J., Fox, K., Wright, K. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*(1), 87-116.

Rader, E. & Wash, R. (2015). Identifying patterns in informal sources of security information, Journal of C*ybersecurity, 1*(1), 121–144.

Reisig, M. D. & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime, 20*(3), 324–337.

Reyns, B.W. (2015). A routine activity perspective on online victimisation: Results of the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396-411.

Roncek, D. W. & Maier, P. A. (1991). Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of hot spots. *Criminology, 29*(4), 725-753.

Schreck, C. J. (1999). Criminal victimization and self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*(3), 633-654.

Schreck, C.J., Stewart, E.A., & Fisher, B.S. (2006). Self-control, victimization, and the influence on risky lifestyle: A longitudinal analysis using panel data. *Journal of Quantitative Criminology, 22*(4), 319-340.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly, 19*(1), 159-180.

Sherman, L.W., Gartin, P.R., & Buerger, M.E. (1989). Hot spots of predatory crime: routine activities and the criminology of place. *Criminology, 27*(2), 27-55.

Sharma, O., & White, D. (2021). Men lose more than twice as much money to scammers than women, new research reveals. *Phoenix Group*. September 15, 2021. Retrieved, January 4, 2022, from, https://www.thephoenixgroup.com/newsroom/news/men-lose-more-twice-much-money-scammers-women-new-research-reveals

Smith, R. G. & Budd, C. (2009). Consumer fraud in Australia: Costs, rates and awareness of the risks. *Trends and Issues in Crime and Criminal Justice, 38*(2), 1-6.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*(1), 159-181.

Temple, J. (2007). Older people and credit card fraud. *Trends and Issues in Crime and Criminal Justice, 34 (*3), 1-6.

Titus, R. M. & Gover, A.R. (2001). Personal fraud: The victims and the scams. In Repeat Victimization, Crime Prevention Studies (12th ed.) (pp. 133-152). *Criminal Justice Press*

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

Vázsonyi, A.T., Machackova, H., Sevcikova, A., Smahel, D., & Cerna, A. (2012). Cyberbullying in context: Direct and indirect effects by low self-control across 25 European countries. *European Journal of Developmental Criminology, 9*(2), 210-227.

Whitty, M.T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292.

Whittaker, J. M. & Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian and New Zealand Journal of Criminology, 53*(4), 497-514.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.