Victimization in online gaming-related trade scams

A study among young Danes

Kristiansen, Søren Ginnerup; Jensen, Aksel Vassard

Published in:
Nordic Journal of Criminology

DOI (link to publication from Publisher):
10.18261/njc.24.2.6

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Nordic Journal of Criminology

Scandinavian University Press

RESEARCH PUBLICATION

Volume 24, nr. 2-2023, pp. 1–17
ISSN online: 2578-9821
DOI: https://doi.org/10.18261/njc.24.2.6

Victimization in online gaming-related trade scams: A study among young Danes

Søren Kristiansen
Associate Dean and professor, Department of Sociology and Social Work, Aalborg University
prodekan-ssh-forsk@aau.dk

Aksel Vassard Jensen
Research Assistant, Department of Sociology and Social Work, Aalborg University
akvaje@socsci.aau.dk

Abstract
This study examines the prevalence and predictors of trade scams related to online video games, which is an emergent field of cyber-victimization. Using self-report data from a representative Danish survey among Danish children and adolescents (n = 1,026) conducted in 2022, we estimate that 36% of participants who are engaged in trading virtual items or game accounts have experienced a trade scam. The study applied lifestyle routine activities theory to explain risk of trade scam victimization, and logistic regressions were used to determine routine activities associated with such risk. Analyses show that game characteristics, use of trading sites, and engagement in risky online activities are associated with elevated risks of experiencing gaming related trade scams.

Keywords
trade scams, video games, victimization, lifestyle routine activities theory, children, youth

While possibilities for interaction have increased dramatically by online gaming and communication platforms, the internet has also laid the ground for various forms of cybercrime and cybervictimization (Almadhoor, 2021; Lee, 2022; Stevens et al., 2021). As pointed out by Holt (2023), there has been an increase in economically motivated cybercrimes over the last decade which has not been recorded in official statistics One such form of cybercrime may be cyber scams related to trades with items related to online computer gaming. In recent years, and particularly during the COVID-19 pandemic and social restrictions, there have been reports of trade scams among gamers (Cook, 2016; Lane, 2018; Kaspersky, 2023) with evidence of scammers generating more than 2,000 euros a week (Winkie, 2022). Despite the apparently significant scope of this type of online victimization, at present no game statistics or surveys among gamers have established reliable measures, based on representative samples, of the prevalence of this phenomenon. Following from this, robust information regarding the profile of the victims of this emerging type of cybercrime is very limited.

Background

Taken as a whole, online gaming (broadly defined as video games played through the internet) is a highly popular global entertainment activity with an estimated 6.2 billion players in 2023 (Liao, 2020), and an estimated revenue of 32.9 billion USD for the global online gaming market in 2027 (Statista, 2022). Many computer games involve options to earn, win or buy virtual items (sometimes referred to as 'skins') that may improve the player's performance or can be used to customize or enhance an avatar or a weapon in a particular game. In some games, such virtual items can be bought for game-specific currencies, and in others for real-life currency. Therefore, selling of virtual items has developed into a significant revenue model for online game providers (Hamari & Lehdonvirta, 2010; Järvinen, 2018; Thorhauge & Nielsen, 2021). As virtual items represent a certain symbolic and/or monetary value (Chen et al., 2005), these items are often traded among online gamers. While most virtual items are traded for relatively small amounts, some virtual items represent very high values and are traded for thousands of dollars (Ku et al., 2007). Trades of virtual items, or of entire player accounts, among players takes place on game distribution platforms such as Steam, various game-external trading platforms such as eBay, in player-to-player communication, or by using integrated inter-player trading features (such the trade functions in Runescape or Roblox). Trades are also arranged by way of a trusted third person who holds the items until payment and items are delivered.

Scams encompass a perpetrator that offers a victim an apparently bullet-proof opportunity to make a profit by way of manipulation (MacKenzie, 2022). Trade scams, then, may be defined as an "act of acquiring items or any other possession from another player through misinformation, confusion, or fraud" (Blizzard Entertainment, 2022). As such, scams should be counted as acts of theft (Strikwerda, 2012) corresponding to cyber-deception/theft in Wall's (2001) well-established cybercrime typology. Gaming related trade scams come in different forms. First, scams can take place within inter-player trade functions (see En & Lan, 2011). Second, they can be performed as social engineering whereby individuals are manipulated by a perpetrator to perform actions (such as sending an item) or disclosing confidential information (Meyer, 2011). As a subtype of social engineering, there are confidence scams by which a perpetrator manipulates a victim, such as a user of the gaming platform Steam or Roblox, to provide access to his or her player account acquiring items of value, demand a ransom to release it, or otherwise take advantage of having accessed the account (Winkie, 2022).

While the gaming community encompasses a wide range of groups, young people may be particularly vulnerable to cyber scams as they tend to be frequent users of online communities while also being relatively socially inexperienced in terms of risk assessment (Oksanen & Keipi, 2013; Holt & Bossler, 2009). Data from the UK (Communications Consumer Panel, 2020) suggests that younger age groups tend to be more susceptible to being scammed than older groups, and that young people account for most cyber scams experienced in the UK. Although there is a considerable volume of research examining the prevalence and different forms of cybervictimization among young people, the literature on online gaming trade scams is limited. As online gaming is a rapidly developing industry with millions of young daily users worldwide, and as youth gaming behaviors may be associated with online fraud victimization (Gainsbury et al., 2019), there is a need to examine the prevalence of gaming related scams and their correlates.

Literature review

While research on scams in trades of gaming-related items is scarce, some studies have examined negative online consequences and related risk factors. In a survey of 1,777 adult Australian internet users, Gainsbury et al. (2019) found that experience of online victimization was associated with engagement with online pornography sites, gaming sites, and multiple discussion forums, and expenditure on pornography, dating and gaming sites. Of particular interest, this study found a positive relationship between time spent on gaming and diverse gaming involvement on the one hand and risk of being a victim of targeted scams on the other. Additionally, time spent on gaming was found to be positively correlated with elevated risk of experience fraud, hacking, and identity theft. In terms of demographics, a study by Chang et al. (2016) found that adolescents living in rural areas had elevated risks of having their virtual items stolen compared to their urban counterparts. Similarly, age (younger age groups) and gender (male) were positively correlated with risk of online theft experience. In a related study, based on a convenience sample of 984 online gamers, Patterson et al. (2013) found that 23% of the participants had been victims of virtual property theft. Sixteen percent of these victims reported the theft to have taken place in trades of virtual items.

Another branch of related research has examined criminal records to typologize online gaming crimes and the persons involved. In a content analysis of 2,179 Taiwanese criminal cases of online gaming crimes registered between 2002 and 2004, Ku et al. (2007) identified four subtypes of crimes: theft, fraud, conversion, and receipt of stolen property, with theft and fraud constituting the majority of the online gaming crimes. While there was no examination of victim characteristics, the study found that offenders were primarily male, relatively young (the majority within the age range of 15-25 years), students, workers, unemployed, and typically with no criminal record. A more recent study examined the roles that cybercriminals may adopt in the value chains of the online criminal market (Cai et al., 2018). This study identified four specific types of value chains: real asset theft, network virtual asset theft, internet resources and service abuse, and hacking techniques. Of the total number of cases, network virtual asset theft was the least frequent crime, representing 15.63% of the cases. In terms of victim behavior characteristics, a study by Kim et al. (2017), based on log information from online game servers, found that victims of account theft had higher activity in trading virtual items compared to other users, and that their accounts were used by the perpetrator to create or sell virtual items.

Research using qualitative data and case-study design has provided evidence of various aspects related to the construction and experience of virtual item theft as a form of online victimization. Based on an ethnographic study in an online role-playing game, Downing (2010) examined how a group of players constituting a so-called "guild of thieves" who steal goods from other players construct virtual victimization in relation to virtual property and theft. He found that, although objectively victims of theft lose valuable items, the construction of victimization is based on a validation from the gaming community and that victims of theft experience it as a much more "real" victimization than other harmful actions in the online gaming world. Craft (2007) conduced a moral analysis of theft and other immoral behavior in the virtual world of EVE Online and concluded that luring virtual items from players is experienced as breaches of trust, since members of these worlds have not provided their informed consent to the nature of an environment in which such actions are acceptable.

While there is extensive research literature on cybercrime, only a few studies have examined scams in trades with virtual gaming items. Thus, there are important gaps in the research literature, one significant and conspicuous one being the prevalence and correlates of victims of such fraud among young gamers. In other words, there is little knowledge regarding the prevalence of these types of cyber scams or of the risk profiles of the victims. While research on correlates of victimization of online gaming-related trading scams is scarce, there is evidence of positive associations between online victimization and personal computer skills (Bergmann et al., 2018), internet routines (Pratt et al., 2010), and risky and deviant internet activities (Reyns et al., 2011).

Theoretical approach

This study applies lifestyle-routine activity theory (LRAT) to examine risks of victimization in trades with virtual items from computer games. In criminological literature (Ngo & Paternoster, 2011; Reyns et al., 2011; Vakhitova et al., 2019), it is common to understand LRAT as an integration of lifestyle exposure theory (Hindelang et al., 1978) and routine activities theory (Cohen & Felson, 1979) suggested by Miethe and Meier (1990). Whereas lifestyle exposure theory emphasizes risky lifestyles (exposure to times, places, and people of elevated risk) in explaining victimization, routine activities theory states that victimization occurs in situations involving motivated offenders, suitable targets, and the absence of capable guardians without attributing the convergency directly to the victim's risky activities (Pratt & Turanovic, 2016). Combining these two theories, LRAT assumes that victimization is determined by the co-presence of four distinct factors: exposure to risky situations, proximity to motivated offenders, target attractiveness, and the absence of capable guardians (Vakhitova et al., 2016). In other words, LRAT suggests that there is an elevated risk of victimization when a motivated offender and an attractive target come into contact in a situation where there is no capable guardian to prevent the crime (Ngo & Paternoster, 2011).

LRAT was developed before the Internet era, and therefore assumed that offenders and victims come into contact in physical time and space. However, recently, various studies (Bossler & Holt, 2009; Choi, 2008; Reyns & Hensson, 2016; Williams, 2016) have employed LRAT to examine various types of cybercrime and cybervictimization. Taken as a whole, studies applying LRAT to online crime have provided inconsistent support for the theory in accounting for risk of online victimization (Ngo & Paternoster, 2011). Examining this, some authors have argued that significant differences between terrestrial and virtual worlds limit LRAT's appropriateness in studies in online contexts in general (Yar, 2005), while others have pointed to different measurements (Reyns et al., 2011) and the inclusion of different types of cybercrime victimization in the same study (Vakhitova et al., 2016) as possible explanations. While studies of cybercrimes applying LRAT have shown mixed results as regards the predictive power of capable guardians, other research has shown more consistent results with regard to the applicability of routine activities (Williams, 2016). Regarding target attractiveness, previous studies of cybervictimization using LRAT have suggested that opening links and posting personal information are associated with online victimization (Ngo & Paternoster, 2011; Reyns, 2015). In terms of exposure to risk, some studies have found that engagement in deviant or risky online activities (Bossler & Holt, 2009), time spent online (Milani et al., 2022), and on specific activities increase the risk of exposure to online offenders and of victimization (Näsi et al., 2021; Ngo & Paternoster, 2011), albeit with some research finding only limited predictive value of such measures (Bossler et al., 2012). Target attractiveness was originally measured as the material attractiveness or desirability of a person and has been measured by social media behavior and participation in online discussions with some predictive value

(Vakhitova et al., 2019). As for technical or social guardianship, the existing literature has also provided mixed results, albeit with studies finding a technologically capable guardian to have some protective value (Choi, 2008; Leukfeldt & Yar, 2016).

In sum, LRAT proposes that the likelihood of becoming a crime victim increases for individuals who are exposed to risk, in proximity to potential offenders, constitute an attractive target in the absence of capable guardians (Vakhitova et al., 2019). Further, the mixed results in applying LRAT to cybercrime victimization have spurred discussions regarding the usefulness of this framework in accounting for online phenomena with a particular focus on whether victims, offenders and guardians can be viewed as being co-present in time and place in online environments (see Reyns et al., 2011; Yar, 2005). Addressing this debate, Vakhitova et al. (2016) have emphasized the significance of addressing challenges such as how to operationalize exposure to online risk, an attractive online target, or capable guardians in a cyberspace context when using LRAT to account for cybercrime victimization. In this study, we use online-adapted LRAT-measures that have been found to have some association with cybervictimization to examine the correlates of scam victimization in trading virtual gaming items.

Study aims

This study investigated how victimization in online gaming-related trade scams was associated with online routines, online literacy, and risky online behaviors. The study addressed the following research questions: (1) What is the prevalence of victimization of scams in trades with virtual gaming items and game accounts among young people? (2) How do young people's online routine activities correlate with victimization in trades with virtual gaming items and game accounts?

Methods

Sample

The study is based on a survey among a representative sample of Danish children and young people. A sample of 7,500 individuals (6,727 children aged 9-17 years and 773 young people aged 18 years) was randomly drawn from the Danish Civil Registration System. Digital invitation letters were sent to participants' digital mailbox service. For participants under the age of 18, digital invitation letters were sent to both parents if possible. Participants aged 18 received the invitation letter in their own personal digital mailbox. The invitation letter explained the purpose of the study, data protection measures, anonymity measures, opportunity to provide consent, and information regarding incentives (60 cinema tickets were randomly distributed among completed surveys) and contained a link to a web questionnaire. Informed consent was thus provided by the parents of participants under 18, whereas participants over 18 provided informed consent on their own behalf. The survey was carried out in the fourth quarter of 2022 with two reminders administered via the Danish digital mailbox service.

Sample characteristics

From the total sample of 7,500, the net sample included data from 1,186 participants, including partially completed questionnaires with at least one answer in the theme section (response rate: 15.8%). In the final sample (n = 1,026), partially completed questionaries were excluded (response rate: 13.7%). Missing values or inaccurate age information were corrected using information from participants' social security number. In terms of representativeness, the sample included an insignificant higher proportion of males compared to the general population (see Table 1). The distribution of age groups, on the other hand, showed multiple significant proportions in relation to the total population. The current study used

data from participants reporting engagement with online video games in the past 12 months (n = 887), which constituted 86.45% of the net sample. Among this subsample, 487 participants reported having engaged in trades with virtual items and game accounts.

Table 1. Gender and age distribution for sample and total population

Variables	Sample	Population	Z test for difference
Gender			
Male	0.521 (535)	0.512 (341,704)	p = 0.281
Female	0.479 (491)	0.482 (325,478)	p = 0.425
Age			
9–11	0.288 (296)	0.282 (188,080)	p = 0.319
12–14	0.338 (347)	0.306 (204,157)	p = 0.012
15–16	0.198 (203)	0.206 (137,250)	p = 0.268
17–18	0.167 (171)	0.206 (137,695)	p = 0.001

Source: Statistics Denmark, FOLK1A, 2nd quarter 2022.

Note: Age of participants was set to the age at date of data extraction (June 27, 2022).

Survey instrument

The survey instrument was divided into five main parts: (1) demographic information (age, gender, leisure activities, income), (2) gaming behavior, (3) virtual item and account trading, (4) experience of trade scams, and (5) general online behavior and digital literacy. The questionnaire was piloted on a group of children and young people recruited via the author's professional network and in a Danish lower secondary school. The pilot testing resulted in minor changes to the questionnaire, which included a total of 37 items.

Measures

Demographic profile

Demographic variables on gender and age were included to examine scam experiences across demographic groups. Age and gender were also used as control variables in logistic regression analysis.

Target attractiveness

According to Reyns et al. (2011) and Guerra & Ingram (2022), an attractive online target may be conceived as an individual holding items of social or monetary value. In the context of gaming related trade scams, an attractive online target may therefore be an individual holding virtual items or game accounts of value. A person's digital inventory on the Steam platform, for example, will display the possession of valuable items, just as a history of item or account trading will be visible to other users and therefore to potential offenders. In estimating the value of a suitable target, participants were asked if they had bought a virtual item (response categories: no/yes), traded a virtual item (response categories: no/yes), or traded gaming accounts (response categories: no/yes) in the last 12 months.

Online exposure to risk

Originally, LRAT assumed that time spent away from home increases the risk of victimization, which is not applicable in studies of online behavior. Instead, online exposure to risk may be conceptualized as time spent online, presence in online communities, and use of social media (Leukfeldt, 2014; Leukfeldt & Yar, 2016; Vakhitova et al., 2019). Following

this, participants were asked how often they play video games (not at all, once a month, once a week, daily, or several times a day) and how much time they spent playing video games last week (response categories: 1 = 0–10 hours, 2 = 11–20 hours, 3 = 21–30 hours, and 4 = 31 or more hours). Participants were also asked to estimate the volume of their online activity (response categories: 1 = not online on weekdays, 2 = 0–1 hours, 3 = 2–3 hours, 4 = 4–5 hours, and 5 = 6 or more hours) and how many hours they spend on a weekend day (response categories: 1 = not online on weekends, 2 = 0–1 hours, 3 = 2–3 hours, 4 = 4–5 hours, and 5 = 6 or more hours). Finally, participants were asked to report their online activities and social media use. Items were based on a scale measuring online activities provided by Smahel et al. (2020) and consisted of the following activities: Writing to friends or family, doing schoolwork, being on social media, listening to music, watching shows or streams, buying things online, following news, following others' lives, learning new things, doing hobbies, and passing time. Also, items involved a scale for use of social media, including Facebook, TikTok, Instagram, Snapchat, Twitter, Discord, Twitch, YouTube, Reddit, and others.

Guardianship

As online scams involve personal contacts and personal communication, the questionnaire did not include items on technical guardians such as firewall or anti-virus programs, which will have no protective effect against trade scams. Following Vakhitova et al. (2019) and Vakhitova et al. (2016), guardianship was operationalized as the personal support from parents, peers, and online communities. As for parent guardianship, only items on active parental mediation defined as the use of various prevention strategies, such as setting rules of use, to manage children's online involvement (Nikken & Jansz, 2006; Kalmus et al., 2022) were included. This choice was guided by current research suggesting a positive effect of active mediation on online risk (Kalmus et al., 2022; Livingstone et al., 2017). Participants were asked to indicate the frequency of their discussions with parents about (1) risks in video games, (2) positive aspects of video games, (3) activities in video games, (4) the games they play, (5) what they do online, (6) how often they are online without parental supervision, (7) how often parents provide advice on safe online behavior, and (8) how often they talk with their parents in situations with a specific concern (response categories: 1 = rarely or never, 2 = sometimes, 3 = all the time). As gaming communities may be considered places to share information and guidance on how to avoid potential scammers, an item on membership of gaming communities was included (response categories: 0 = no, 1 = yes). As levels of digital literacy may influence the risk of cybercrime victimization (Chang et al. 2016; Chen, et al., 2017), the questionnaire included a set of 10 items on digital literacy. Participants were asked if they (1) know how to save a photo, (2) know how to change private settings, (3) know how to see if things online were true, (4) know how to choose the best search words, (5) know what to share online, (6) know how to delete friends from contact list, (7) feel safe commenting and writing online, (8) know how to install video games, (9) know how to keep track of money spent in video games, and (10) know how to buy virtual items in games (response categories: 0 = no, 1 = yes).

Online proximity

Contrary to other forms of cybercrime, such as data theft and hacking, which do not imply the online co-presence of offender and victim, trading virtual items relies on some sort of co-presence in an online context. Online proximity may thus be conceptualized as the accessibility of a motivated offender to defraud a potential victim in direct contact within

the context of different games. Therefore, online proximity was operationalized into items measuring different spaces within an online context in which a motivated offender and an attractive target are likely to meet (Vakhitova et al., 2019; Reyns et al., 2011). Participants were asked open-ended questions to report the three most frequent games in which they have traded virtual items or accounts. Participants were also asked to report memberships of online trading groups, whether they accept friendship requests from people they do not know, and whether they participate in online activities such as buying loot boxes and skin betting (0 = no, 1 = yes).

Data analysis

Logistic regressions were used to identify routine activities correlated with risk of trade scam victimization among participants who reported having played online video games, traded virtual items, or gaming accounts in the past 12 months (n = 487). Due to the complexity of the theoretical framework, regression analysis may be affected by multicollinearity and overfitting due to the considerable number of predictors and controls (Grätz, 2022; Marttila et al., 2021; Silver et al., 2022). Therefore, this study employed LASSO regression (Least Absolute Shrinkage and Selection Operator) as a penalized regression to reduce the number of covariates. LASSO regression penalizes estimates by setting them to exactly zero or shrinking others towards zero to minimize the sum of squared residuals and keeping only relevant covariates for analysis (Huntington-Klein, 2021). The shrinkage of some estimates can be described as a favorable bias as it reduces variance in predicting regression outcomes. Using cross validation on training data, LASSO predicts the best lambda value for penalizing the regression model into a more parsimonious and interpretable regression. As LASSO regressions do not compute standard errors or confidence intervals but the most important features for predicting an outcome, it is difficult to interpret the relevant factors as a significant correlation on the outcome variable (Tibshirani 1996). Presented values therefore relate to a regular logistic regression in which estimates set to exactly zero by LASSO are excluded from the analysis. All LRAT measures were included in the LASSO regression, and the penalized model identified 12 variables relating to predicting scam victimization. Of the 12 relevant variables, six pertained to online proximity, two to online visibility, two to guardianship, and two to demographics. These variables were included in a regular logistic regression. To reduce age bias, weighted data (post-stratification weights) were used for the regression analysis. A VIF test revealed no concerns regarding multicollinearity. The logistic regression was tested for robustness by changing measures of time spent on gaming and age as ordinal, categorical, and interval measures. Robustness checks did not significantly change coefficients and significance levels of the covariates.

For the digital literacy and active parental mediation measures, factor analysis was used to explore the possibilities of multiple factors. Digital literacy showed no reliability in this regard. From active parental mediation measures, active gaming mediation and safety advice were extracted. First, a KMO test was performed to explore the possibility of a factor analysis. Second, a test of correlation was performed. The active parental mediation items showed an acceptable value for the KMO correlation value (0.83). The correlation matrix showed an overall acceptable correlation between variables. Following Mehmetoglu and Mittner (2022:365), parallel analysis was used to determine numbers of variables. As the unrotated factor loading showed acceptable loadings for only one factor, an oblimin rotation was performed extracting the two beforementioned factors. The item measuring frequency of discussions with parents about online activity affected both factors and was not included in any of the factors. Active gaming mediation and safety advice showed Cronbach

alpha values at acceptable levels (α = 0.74 and α = 0.65 respectively). Data management and analyses were conducted using R version 4.2.0.

Results

In terms of prevalence of trade scam victimization, our data showed that 35.8% of participants who engage in either trades with virtual items or game accounts had experienced a trade scam within the past 12 months.

Table 2. Trade scam experience and demographic characteristics

Variables	Trade scam experience (%/n)
Gender	
Male	34.62%
Female	38.33%
χ^2	F = 0.6553, p = 0.4184
Age	
9–11	40.18%
12–14	35.42%
15–16	23.39%
17–18	40.39%
χ^2	F = 2.3309, p = 0.0729

Note: Weighted numbers.

Our analysis showed no significant difference regarding the risk of experiencing trade scams across the two genders nor across age groups (see Table 2). However, when controlling for the most relevant online activities, females had a 1.8-times higher risk of experiencing scams when trading in video games. Also, there was a significant decline in the odds of experiencing trade scams by 0.2 times for the age group of 15–16-year-olds compared to 9–11-year-olds (see Table 3).

Table 3. Logistic regression analysis of routine activities and experience of trade scam victimization

Variable	Experienced scam				
	B	SE	P	OR	95% CI for OR
Weekly gaming hours (ref = 0–10 hours)					
11–20 hours	0.281	0.256	0.273	1.324	0.801 2.190
21–30 hours	0.022	0.348	0.949	1.023	0.516 2.025
31+ hours	0.689	0.545	0.207	1.991	0.682 5.810
Hours spent online on weekdays (ref = 0–1 hours)					
2–3 hours	–0.730**	0.340	0.032	0.482	0.247 0.939
4–5 hours	–0.518	0.387	0.181	0.595	0.278 1.274
6+ hours	–0.164	0.416	0.694	0.849	0.375 1.922
Active mediation	0.078	0.061	0.206	1.081	0.958 1.219
Social media scale	0.057	0.049	0.253	1.058	0.960 1.166
Skinbetting	0.634	0.555	0.254	1.885	0.633 5.610
Friend request	0.378*	0.226	0.096	1.459	0.935 2.275

(*Continued*)

Table 3. (*Continued*)

Variable	Experienced scam				
	B	SE	P	OR	95% CI for OR
Trading group	0.684**	0.337	0.043	1.982	1.022 3.844
Trading games	0.741***	0.176	<0.001	2.098	1.484 2.966
Gender (= Female)	0.613**	0.255	0.016	1.846	1.119 3.044
Age groups (ref = 9–11 years)					
12–14 years	–0.419	0.260	0.108	0.658	0.394 1.097
15–16 years	–1.408***	0.404	<0.001	0.245	0.111 0.541
17–18 years	–0.412	0.418	0.324	0.662	0.291 1.505
Constant	–2.676***	0.743	<0.001	0.069	0.016 0.296
Observations	481				

Note: Weighted numbers. *p<0.1; **p<0.05; ***p<0.01.

Furthermore, our analysis showed that being online 2–3 hours on a weekly basis compared to 0–1 hours did reduce the odds of experiencing trading scams with a factor of 0.5. Trading for virtual items in online video games increased the odds of experiencing trade scams by 1.9 times for each additional game. Also, being a member of a trading group appeared to increase the odds of experiencing trade scams with a factor of 2.0. Finally, accepting friend requests from strangers increased the odds of trade scam victimization with the factor of 1.5 with a marginal significance (p = 0.096).

Discussion

To the best of our knowledge, this is the first representative study to estimate the prevalence of trade scam victimization among young gamers. As no other representative data from other countries are available for comparison, the relative prevalence rate is difficult to assess. Only one survey, conducted in the UK, has estimated a range of fraud risks presented to young and adult gamers, but without focusing on trade scams. This study found that 20% of gamers have experienced a gaming related crime or knew someone who had (Lloyds Bank, 2022). While not exactly comparable in terms of sample, subject and measures, this study found a higher prevalence as our data showed that more than one-third of young people engaging in trading virtual items or gaming accounts have experienced a trade scam, which is level of some concern.

In terms of correlates of trade scam victimization, the online adapted LRAT model applied in this study provided some notable results. Regarding demographics, females were found to have a higher risk of experiencing trade scam victimization than males. This stands in contrast to Chang et al. (2016), who found that being male was associated with elevated risk of stolen virtual properties in online games. This observed difference may be related to different sampling designs and measures of online routine activities across studies. Previous research has found younger age groups to be more at-risk of cybercrime victimization compared to older ones (Chang et al., 2016; Oksanen & Keipi, 2013; Holt & Bossler, 2009). Our data partly support this pattern, as the youngest age group showed a higher risk of victimization compared to 15-16-year-olds, while not to the 17-18-year-olds. One explanation might be that youngest age groups tend to trade very frequently as part of their gaming routines, and that older age groups may constitute attractive targets as they are more likely to hold items of higher monetary value.

Online visibility was not associated with elevated risk of experiencing trade scams. This result seems to contrast with the general assumption of LRAT and other studies indicating that time spent online increases the risk of online victimization (Milani et al., 2021; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Vakhitova et al., 2019). However, trade scams often take place when being engaged in gaming (and not being active and visible on other online platforms) which may account for this observed difference. Also, the difference may be related to the types of online victimization addressed in the beforementioned studies. While risk of online victimization in the form of online bullying or cyberstalking may be associated with online visibility, victimization related to gaming trade scams may be related to online visibility in other ways. Clearly, future research on gaming-related trade scams would benefit from examining time spent in online spaces relevant for item trading.

Online proximity to potential offenders, such as being a member of trading groups and trading in numerous video games, were associated with high risk of experiencing trade scams. A trading group is a game-external forum for trading virtual items and a potentially risky environment, as they are open to all and not secured by game providers' technical protection inside the games. Obviously, our data do not allow conclusions regarding specific activities in trading groups, and the groups may differ in terms of communication forms and regarding the types of virtual items. Therefore, research examining the practices and dynamics of online trade groups is pivotal for establishing a more comprehensive understanding of online gaming-related trade scams. In our data, the strongest predictor of experiencing a trade scam was the number of games in which trade has been made. On average, an additional game almost doubled the risk of experiencing a trade scam. This corresponds to recent research suggesting a positive association between high frequency participation in online communities and cybercrime victimization (Oksanen & Keipi, 2013). Lastly, accepting friend requests from strangers was associated with elevated risk of experiencing trade scams. This corresponds with the general observation in the research literature suggesting that such behavior may bring motivated offenders into proximity to potential victims (Reyns et al., 2011).

Guardianship in terms of active parental mediation did not appear to be significantly correlated with scam victimization, which may reflect our operationalization of this LRAT component. In this study, we did not measure situational guardianship such as other people being co-present and capable of assisting the potential victim, and it is plausible that the presence of guardians in trade situations may impact the risk of experiencing trade scams. Similarly, we found no positive correlation between parental mediation and reduced risk of trade scam victimization. This may be explained by the potential indirect effect that parental mediating may have on the experience of trade scams. It is likely that parental mediation may have a direct effect on reducing online behaviors while having no direct effect on the experience of gaming-related trade scams. Future studies are needed to examine such mediating associations. Online gaming groups were not found to be relevant in predicting trade scams for the LASSO regression model. A plausible interpretation may be that gaming communities constitute places of risk and motivated scammers as well as a place for friends to share experiences and guidance. This potential double-characteristic of online communities in relation to cybercrime victimization should be examined in more detail in future studies.

This study involves some limitations that should be taken into consideration when interpreting the results. First, the overall response rate was relatively low, which may have resulted in some level of selective non-response bias, which again may be a result of the

chosen method of data collection. Specifically, individuals who tend to avoid online threats may have been less likely to complete the survey, while individuals who are more susceptible to online victimization could have been more likely to respond. We are not able to determine the exact level of this potential bias, but the high prevalence of online scam victimization identified in this study indicates some level of response bias in our data which again may influence generalizability negatively. Second, this study used logistic regression which did not account for potentially confounding and mediating relationships between LRAT variables and thus limited examination of direct effects (Silver et al., 2022). For example, it was assumed that an individual constitutes an attractive target when buying and trading virtual items without considering other variables that may impact the effect of these variables. A third limitation concerns data granularity. Our data regarding engagement in online communities might not capture the complexities of such environments as places of risk as well as of protection and guidance. Distinct items on gaming communities with friends as well as with strangers would have enabled a more detailed analysis of this component and is therefore recommended for future studies. Also, our data on guardianship have not captured the types of guardianship that relate to personal competences or capacities that are needed to protect a potential victim gaming in solitude. Clearly, the influence of such person-centered guardianship would be beneficial in future studies in this field. Finally, as we conducted a self-report cross-sectional study using measures covering the last 12 months, we are not able to specify a direction of causality for example as to whether the identified correlates affected the victimization or whether victimization caused a change in online behaviors.

Implications for policy and interventions

The evidence provided by this study may inform the development of policies and interventions to prevent and reduce online gaming scam victimization. First, online proximity appeared to have the strongest correlates with risk of trade scam victimization. Specifically, we found evidence of trading in multiple online video games and membership of trading groups increasing the risk of victimization. These findings point to measures directed at game providers encouraging them to address the issue of trading scams and to engage game users in the evaluation of already existing measures and in the innovation of new and safe trading schemes or trusted third-party trading arrangements (Chen et al., 2005). Additional measures may concern three types of controllers suggested by Vakhitova et al. (2016) asserting three distinct types of influence on potential scam victimization provided by so-called handlers, place managers and guardians. Handlers are people (such as friends or family members) who exercise some sort of control over offenders. While it may be difficult for handlers to regulate teenagers' or young adults' access to online activities, it may be suggested that school or Esport communities make efforts to discourage scamming in trading virtual items. Place managers are agents in control of the place in which scams are taking place. Future interventions may target game providers and social media platforms to better monitor and sanction scams in virtual item trade. Guardians are individuals protecting the victim by deterring a potential offender, intervening in an emerging victimization. Future actions may include gamers or users of trade communities to intervene by addressing the offender and victim directly or by reporting an observed scam to the social platform officials or game administrators. Finally, game providers or social media platforms could be incentivized to engage in scam trade prevention by public campaigns appealing to these actors in taking responsible actions in terms of initiating measures to prevent and sanction trade scams.

Conclusion and directions for future research

This study has taken a first step towards building a profile of virtual item trade scam victims considering individual level and context-related factors. As such, this study addresses current calls to examine different types of scams to enable typologies of cyberscam victims (Whitty, 2020). We found that more than one third (35.8%) of young Danish children and adolescents who engage in online trades of virtual items and accounts have experienced victimization. Obviously, future studies, in other countries and jurisdictions, are needed to evaluate the prevalence identified in this study and to develop standardized measures to estimate the prevalence. In line with previous studies of cybercrime (Oksanen & Keipi, 2013; Reyns et al., 2011; Vakhitova et al., 2019), our data showed that proximity to motivated offenders, measured as trading in multiple online video games, being a member of trading groups, and accepting friend requests from strangers, increase the risk of experiencing cybercrime victimization. Among the selected variables, none appeared to serve as protective factors.

In sum, our findings provide evidence that adolescent gaming behavior, and specifically trading virtual items or game accounts, serves as a new field for fraudulent activity in the form of trade scams. Further, while LRAT has proven useful in examining gaming-related trade scams, our study also indicated needs to re-design measures. Specifically, we call for future studies to develop context-specific measures of online activities and self-guardianship, such as self-control or online risk awareness as factors potentially impacting risk of trade scam victimization. Finally, to advance in-depth understanding of the factors affecting the risk of experiencing gaming-related trade scams, future studies should employ statistical methods to effectively address mediating or confounding relationships between variables.

Funding

This work was supported by Offerfonden [Danish Victims Fund].

References

Almadhoor, L. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 2972–2981.

Bergmann, M. C., Dreißgacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727

Blizzard Entertainment (2022). Trade scams. Available at: https://us.battle.net/support/en/article/2563 [accessed January 9, 2023].

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500–523. https://doi.org/10.1177/0044118X11407525

Cai, T., Du, L., Xin, Y., & Chang, L. Y. C. (2018). Characteristics of cybercrimes: evidence from Chinese judgment documents. *Police Practice and Research*, *19*(6), 582–595. https://doi.org/10.1080/15614263.2018.1507895

Chang, F.-C., Miao, N.-F., Chiu, C.-H., Chen, P.-H., Lee, C.-H., Chiang, J.-T., & Chuang, H.-Y. (2016). Urban-rural differences in parental internet mediation and adolescents' Internet risks in Taiwan, *Health, Risk & Society*, *18*, 188–204. https://10.1080/13698575.2016.1190002

Chen, Y.-C., Hwang, J.-J., Song, R., Yee, G., & Korba, L. (2005). Online gaming cheating and security issue. *International Conference on Information Technology: Coding and Computing*, Vol. II. https://doi.org/10.1109/ITCC.2005.215

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

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), 588–608. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, *46*(5), 505–524. https://doi.org/10.2307/2094935

Communications Consumer Panel (2020). Scammed! Exploited and afraid – What more can be done to protect communications consumers from the harm caused by scams? Available at: https://www.communicationsconsumerpanel.org.uk/downloads/ccpscammeddecember2020.pdf [Accessed November 25, 2022].

Cook, M. (2016). *2016: The year the video game industry (finally) realized its cybersecurity problem*. Available at: https://www.linkedin.com/pulse/2016-year-video-game-industry-finally-realized-its-problem-cook?trk=pulse-article_more-articles_related-content-card [Accessed January 9, 2023].

Craft, J. A. (2007). Sin in cyber-eden: Understanding the metaphysics and morals of virtual worlds. *Ethics and Information Technology*, *9*, 205–217. https://doi.org./10.1007/s10676-007-9144-4

Downing, S. (2010). Online gaming and the social construction of virtual victimization. *Eludamos: Journal for Computer Game Culture*, *4*(2), 287–301. http://doi.org./10.7557/23.6049

En, L. Q. & Lan, S. S. (2011). Balancing safety and danger in gaming for better user engagement. *8th International Conference on Information, Communications & Signal Processing, Singapore*, 1–5. https://doi.org/10.1109/ICICS.2011.6173543

Finkelhor, D., & Asdigian, N. L. (1996). Risk factors for youth victimization: Beyond a lifestyles/routine activities theory approach. *Violence and Victims*, *11*(1), 3–19. https://doi.org/10.1891/0886-6708.11.1.3

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky internet use: Associating negative online experience with specific online behaviours. *New Media & Society*, *21*(6), 1232–1252.

Grätz, M. (2022). When less conditioning provides better estimates: Overcontrol and endogenous selection biases in research on intergenerational mobility. *Quality & Quantity*, *56*, 3769–3793. https://doi.org/10.1007/s11135-021-01310-8

Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behavior*, *43*(1), 44–60. https://doi.org.10.1080/01639625.2020.1774707

Hamari, J., & Lehdonvirta, V. (2010). Game design as marketing: How game mechanics create demand for virtual goods. *International Journal of Business Science & Applied Management*, *5*(1), 14–29. https://hdl.handle.net/10419/190610

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, *19*(2), 195–208. https://doi.org/10.1177/1524838016650189

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.

Holt, T. J. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*. https://doi.org/10.1016/j.chb.2022.107493

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30, 1–25. https://doi.org/10.1080/01639620701876577

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Huntington-Klein, N. (2021). *The effect: An introduction to research design and causality*. Boca Raton: Chapman & Hall/CRC.

Järvinen, T. (2018). Examining cosmetic virtual item purchase in World of Warcraft: A theory of consumption values perspective. MSc Thesis, Alto University. Available at: http://urn.fi/URN:NBN:fi:aalto-201811195824 [Accessed January 12, 2023].

Kalmus, V., Sukk, M., & Soo, K. (2022). Towards more active parenting: Trends in parental mediation of children's internet use in European countries. *Children & Society*, *36*(5), 1026–1042. https://doi.org/10.1111/chso.12553

Kaspersky (2023). *Online gaming scams during pandemic. How to stay safe*. Available at: https://www.kaspersky.com/resource-center/threats/coronavirus-gaming-scams [Accessed January 9, 2023].

Kim, H., Yang, S., & Kim, H. K. (2017). Crime scene re-investigation: a postmortem analysis of game account stealers' behaviors. *NetGames '17: Proceedings of the 15th Annual Workshop on Network and Systems Support for Games*, 1–6.

Kristiansen, S., & Severin, M. C. (2020). Loot box engagement and problem gambling among adolescent gamers: Findings from a national survey. *Addictive Behavior*, *103*, 1–6. https://doi.org/10.1016/j.addbeh.2019.106254

Ku, Y., & Gupta, S. (2008). Online gaming perpetrators model. In: Yang, C. C. et al., *Intelligence and security informatics*. ISI Lecture Notes in Computer Science, Vol. 5075. Springer: Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69304-8_44

Ku, Y., Chen, Y.-C., Wu, K.-C., & Chiu, C. (2007). An empirical analysis of online gaming crime characteristics from 2002 to 2004. In: Yang et al. (Ed.), *Intelligence and security informatics*. PAISI 2007. Lecture Notes in Computer Science, Vol. 4430. Springer: Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-71549-8_3

Lane, A. (2018*). In the world of online gaming: Who is protecting whom from a scam artist's journey into obtaining one's information*. MSc Thesis, Utica College, New York. Available at: https://www.proquest.com/c45dd218-806e-472a-b0de-652a0f595e03 [Accessed January 9, 2023].

Lee, C. S. (2022). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13–14), 2529–2553. https://doi.org/10.1177/00111287211029862

Leukfeldt, E. R. (2014). Phishing for suitable targets in The Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. http://dx.doi.org/10.1080/01639625.2015.1012409

Liao, G.-Y., Pham, T. T. L., Cheng, T. C. E., & Teng, C.-I. (2020). How online gamers' participation fosters their team commitment: Perspective of social identity theory. *International Journal of Information Management*, *52*. https://doi.org/10.1016/j.ijinfomgt.2020.102095

Livingstone, S., Ólafsson, K., Hesper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risk for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, *67*, 82–105. https://doi.org/10.1111/jcom.12277

Lloyds Bank (2022). Fraud's no game. A Lloyds Bank report on how gamers can protect themselves from financial fraud. Available at: https://www.lloydsbankinggroup.com/assets/pdfs/who-we-are/our-purpose/fraud/lloyds-bank-game-fraud-report.pdf [Accessed February 3, 2023].

MacKenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*, *62*, 1537–1552. https://doi.org/10.1093/bjc/azab118

Meyer, T. L. (2011). *A study on trading scams in massively multiplayer online role-playing games and risk mitigation techniques*. MSc Thesis. Iowa State University.

Mehmetoglu, M., & Mittner, M. (2022). *Applied Statistics using R*. Sage Publications: London.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice and criminal victimization rates: A theory of a theoretical model. *Journal of Research in Crime & Delinquency*, *27*, 243–266. https://doi.org/10.1177/0022427890027003003

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, *43*(2), 228–240. https://doi.org/10.1080/01639625.2020.1806453

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime victimisation and polyvictimisation in Finland—Prevalence and risk factors. *European Journal on Criminal Policy and Research*, 29, 283–201.

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

Nikken, P., & J. Jansz (2006). Parental mediation of children's videogame playing: a comparison of the reports by parents and children. *Learning, Media & Technology*, *31*(2), 181–202. https://doi.org/10.1080/17439880600756803

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*, *8*(4), 298–309. https://doi.org./10.1080/17450128.2012.752119

Park, Y., & Vieraitis, L. M. (2021). Level of engagement with social networking services and fear of online victimization: The role of online victimization experiences. *International Journal of Cybersecurity Intelligence & Cybercrime*, *4*(2), 38–52. https://www.doi.org/10.52306/04020421TERZ5728

Patterson, N., Hobbs, M., & Palmer, D. (2013). A direct insight into victims of cybercrime: A survey study which investigates victims of virtual property theft and their views on security. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. https://doi.org/10.1109/TrustCom.2013.74

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (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. https://doi.org/10.1177/0022427810365903

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335–354. https://doi.org./10.1080/15564886.2015.1057351

Reyns, B. W., Henson, B., and Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119–1139. https://doi.org/10.1177/0306624X15572861

Shaheen, S., & Hoff, D. L. (2007). Cyber bullying: Clarifying legal boundaries for school supervision in cyberspace. *International Journal of Cyber Criminology*, 1(1). https://doi.org/10.5281/zenodo.18279

Silver, I. A., Lonergan, H., & Nedelec, J. I. (2022). On the selection of variables in criminology: Adjusting for the descendants of unobserved confounders. *Journal of Criminal Justice*, *81*, 1–10. https://doi.org/10.1016/j.jcrimjus.2022.101924

Smahel, D., Machckova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU kids online 2002: Survey results from 19 countries. EU Kids Online: The London School of Economics and Political Science. https://doi.org/10.21953/lse.47fdeqj01ofo

Song, R., Korba, L., Yee, G., & Chen, Y.-C. (2005). Protection of virtual property in online gaming. Proceedings of the 11th International Conference on Distributed Multimedia Systems. Available at: https://nrc-publications.canada.ca/eng/view/accepted/?id = dcb27b8c-47d9-41b2-8950-cc6a7fb5d47b [Accessed January 12, 2023].

Statista (2022). Online gaming – statistics & facts. Available at: https://www.statista.com/topics/1551/online-gaming/#topicHeader__wrapper [Accessed 28 November 2022].

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6), 367–376. http://doi.org/10.1089/cyber.2020.0253

Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics and Information Technology*, *14*, 89–97. https://doi.org/10.1007/s10676-011-9285-3

Thorhauge, A. M., & Nielsen, R. K. L. (2021). Epic, Steam, and the role of skin-betting in game (platform) economies. *Journal of Consumer Culture*, *21*(1), 52–67. https://doi.org/10.1177/1469540521993929

Tibshirani, R. (1996). Regression shrinkage and selection via the LASSO. *Journal of the Royal Statistical Society. Series B (Methodological)*, *58*(1). 267–288.

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior*, 101, 225–237. https://doi.org/10.1016/j.chb.2019.07.012

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*. 32(2). https://doi.org/10.1177/1043986215621379

Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall (Ed.), Crime and the internet (pp. 1–17). New York: Routledge.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, *26*(3), 399–409. https://doi.org/10.1007/s10610-020-09458-z

Winkie, L. (2022). Inside Roblox's criminal underworld, where kids are scamming kids. Available at: https://nordic.ign.com/roblox/62752/news/inside-robloxs-criminal-underworld-where-kids-are-scamming-kids [Accessed January 11, 2023].

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *The British Journal of Criminology*, *56* (1) 21–48. https://doi.org/10.1093/bjc/azv011

Yar, M. (2005). The novelty of cybercrime. *European Journal of Criminology*, 2, 407–427. https://doi.org/10.1177/147737080556056