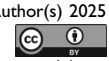
Check for updates

Special Issue: The Human Factor in Cybercrime

European Journal of Criminology

Explaining fear of cybercrime: A focus on interpersonal and property cybercrime differences

European Journal of Criminology
1–25
© The Author(s) 2025

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14773708241312820
journals.sagepub.com/home/euc

Inês Sousa Guedes
University of Porto, Portugal

José Martins
University of Porto, Portugal

Samuel Moreira
University of Porto, Portugal
University Lusíada, Portugal

Abstract

Fear of crime is a hot topic in the criminological field, yet differentiation between fears associated with various types of cybercrimes remains underexplored. This study ($N = 726$) conducted in the Portuguese context via an online survey investigates the distinct determinants of fear for two main categories of cybercrime: interpersonal (cyberbullying and cyberstalking) and property-related (online consumer fraud, identity theft, and malware discovery). The findings reveal that while offline fears strongly predict both types of cybercrime fears, the specific variables influencing them differ significantly. Property cybercrime fear is primarily driven by economic insecurity, while interpersonal cybercrime fear is less influenced by socioeconomic factors and more by the fear of offline interpersonal crimes. Additionally, the study highlights that traditional factors from Routine Activity Theory, such as capable guardianship and target suitability, play a minimal role in explaining the variance in cybercrime fears. These insights not only contribute to our understanding of the multifaceted nature of cybercrime fears but also underscore the need for tailored preventative strategies that address the unique drivers of each type of fear.

Corresponding author:
Inês Sousa Guedes, Faculdade de Direito da Universidade do Porto, Rua dos Bragas 223, 4050-123 Porto, Portugal.
Email: iguedes@direito.up.pt

Keywords
Cybercrime, fear of cybercrime, fear of interpersonal cybercrime, fear of property cybercrime, individual variables, Routine Activity Theory

Introduction

Over the last few decades, scholars have extensively examined the nature, measurement, scope, and determinants of fear of crime (Hale, 1996; Warr, 2000). However, most of this research has focused on fear of traditional crimes, such as sexual assault or burglary, without adequately addressing the impact of the internet on individuals' daily lives. Consequently, studies investigating emotional responses to online threats have been relatively limited (with a few exceptions, including Brands and Wilsem, 2021; Maher and Hayes, 2023; Roberts et al., 2013; Virtanen, 2017). In fact, with the unprecedented use of the internet and technology in general, the lack of studies analyzing the nature and determinants of fear of online crime is a significant oversight (Henson et al., 2013). Fear of online crime not only negatively affects people's well-being (e.g., Hanslmaier, 2013; Pearson and Breetzke, 2014) but also has other significant adverse consequences (e.g., Hille et al., 2015; Reisig et al., 2009). For instance, Brands and Wilsem (2021) found that online fear strongly predicted avoidance behaviors, specifically relating to online purchasing and banking, impeding an individual's perceived online freedom and opportunities. Accordingly, Hille et al. (2015) observed a negative relationship between fear of financial losses related to online identity theft and online purchase intentions. This was similarly suggested by the study conducted by Jordan et al. (2018), which identified a positive correlation between fear of identity theft and perceived risk, decreasing individuals' intentions to make online purchases.

It is plausible that fear of crime not only manifests differently in online contexts compared to traditional forms of crime but also differs among various types of cybercrimes (Yu, 2014). For instance, the fear associated with identity theft might involve concerns about long-term financial harm and the complex process of restoring one's credit and reputation. On the other hand, fears related to cyberstalking may more closely mirror those of physical stalking, involving concerns about personal safety and mental health.

The present study is, to the best of our knowledge, the first in the Portuguese context that seeks to shed light on the underlying factors contributing to distinct forms of fear related to cybercrimes, specifically, fear of interpersonal victimization (cyberstalking and cyberbullying) and fear of property victimization, including online identity theft, online consumer fraud, and encountering malicious software. It focuses not only on sociodemographic variables but also on individual dimensions (such as fear of offline crimes, economic insecurity, previous online victimizations) and contextual variables derived from the Routine Activity Theory (RAT). Besides introducing new insights into the fear of cybercrime within the Portuguese context, our findings may hold significant relevance internationally. By incorporating variables such as broader economic insecurities, this work opens paths for comparative studies that could validate these dynamics across different cultural settings. The article begins with a theoretical background section, presenting the primary concepts and explanations related to the fear of cybercrime. Subsequently, the methodology employed in this study will be explained. Finally, we

will present and discuss the study's results, drawing attention to its potential implications for the field of fear of online crime.

Fear of (online) crime

In broad terms, fear of crime is typically conceptualized as a construct characterized by three dimensions: emotional fear of crime, perceived risk of victimization, and safety-related behaviors, such as avoiding certain locations or securing one's home (Gabriel and Greve, 2003). The emotional fear of crime, in a narrower sense, refers to the emotional response evoked by actual crimes or symbols associated with them (e.g., Ferraro, 1995; Ferraro and LaGrange, 1987), characterized by a sense of danger and anxiety. Perceived risk of victimization may be related to the emotional fear of crime, but they are not interchangeable phenomena (Warr, 2000). Perceived risk of victimization stems from the recognition of certain places or situations as potentially dangerous for criminal victimization (Mesch, 2000).

These distinctions are also relevant when studying the fear of cybercrime (Brands and Van Doorn, 2022). In the present study, fear of crime is defined in its narrowed sense as the set of emotional reactions to different types of cybercrimes. Furthermore, we use the terms 'fear of victimization' and 'fear of crime' interchangeably based on the premise that fear of crime typically arises from the apprehension that one might become a victim or that a criminal act is imminent.

There has been notably less investigation on fear of crime within the realm of the internet (Randa, 2013). Nevertheless, some important insights have been emerging. In a systematic review, Brands and Van Doorn (2022) observed that in most studies women reported greater fear of cybercrime compared to men. As for age and educational levels, mixed results were found. Regarding previous victimization, in nine studies, seven showed a positive relationship, suggesting that victims report a greater fear of cybercrime.

Exploring the relationship between the fear of cybercrime and traditional or offline crime is crucial, yet only a few studies have tackled this issue. Roberts et al. (2013) discovered that fear of traditional crime strongly predicted fear of cybercrime (specifically, fear of cyber-identity theft and related fraudulent activities). Guedes et al. (2022) also identified that the most significant predictor of fear of online identity theft was a general fear of crime.

Less explored is the relevance of economic insecurities on fear of cybercrime. Recent reflections describe the fear of crime as a 'sponge' that absorbs all sorts of generalized anxieties (e.g., Britto, 2013). As Jackson (2011: 11) argues

> fear of crime may operate as a 'sponge', absorbing all sorts of anxieties about related issues of deteriorating moral fabric, from family to community to society. People may use the language of 'worry' and 'crime' to express connecting conflicts, insecurities and anxieties.

Individuals who experience economic insecurity, including uncertainty about their economic position, health, employment status, or financial stability, may be more prone to fearing crime (Britto, 2013; Garcia et al., 2017; Hirtenlehner and Farrall,

2013). These studies support the assumption that fear of crime is a manifestation of more diffuse anxieties and a function of broader insecurities.

Fear of specific (online) crimes. Researchers have been acknowledging that fear of crime should be examined in a crime-specific context, pointing out, for instance, that fear of violent or personal crime may not be like fear of property or financial crime (Ferraro, 1995; Warr, 1984). As such, it is important to distinguish between fear of different types of crimes.

Several authors have found that women report considerably higher fear of personal harm (e.g., violent and sexual crimes) compared to men, but no differences are observed in property crime (e.g., Moore and Shepherd, 2007; Schafer et al., 2006). Regarding age, studies have consistently revealed a positive relationship with fear of property crime (e.g., Lane and Fox, 2012). Furthermore, Rader et al. (2012) found that older individuals tended to exhibit higher levels of fear.

Few studies have attempted to disaggregate cybercrime types, which might be crucial to better understanding the complex nature of fear of crime. Individuals may be worried about becoming a victim of cyber-harassment without being worried about a hacking attack (Cook et al., 2023). Furthermore, factors associated with increased fear may differ across different cybercrimes. For instance, Yu (2014) found that perceived seriousness, victimization experiences, engaging in online downloading, and online shopping were predictors of fear of computer viruses. In the case of cyberbullying, online interaction and perceived risk positively influenced this dependent variable.

Other studies have provided relevant results concerning the variables that explain specific types of cybercrimes. For instance, the study by Henson et al. (2013) focused on the fear of interpersonal victimization, including online harassment, cyberstalking, and intimidation and threat of violence. The results showed that the perceived risk of victimization was a strong and positive predictor of fear of interpersonal victimization. However, no relationship between previous interpersonal victimization by a stranger and fear of interpersonal victimization was found. Gender was also a significant predictor of fear of interpersonal victimization, with women experiencing more fear than men. This result is consistent with previous studies finding that women report higher levels of fear of crimes such as cyber-harassment and cyberbullying (e.g., Pereira et al., 2016) but not of online identity theft or computer viruses (e.g., Roberts et al., 2013). Moreover, younger individuals exhibited higher levels of fear for this type of crime (Henson et al., 2013).

In turn, Brands and Wilsem (2021) investigated the predictors of fear of online financial crime, finding higher levels of this fear among females and elderly people. Moreover, lower levels of fear were observed in the higher educated. Finally, previous victimization experiences (e.g., being hacked, being infected by a computer virus) increased the levels of fear of online financial crime.

Finally, Cook et al. (2023) analyzed the predictors of fear of economic cybercrime (e.g., purchase theft fraud, malicious software) across 28 countries. The authors found that, after controlling for between-country differences, women were more likely to be fearful than men, and that age had a significant curvilinear association, showing that young and middle-aged adults were more fearful of economic cybercrime than older people. Furthermore, they found that the most economically deprived reported higher levels of fear of economic cybercrime.

RAT and fear of online crime. According to Cohen and Felson (1979), crime is a function of three core conditions: the presence of a motivated offender, the suitability of a target (a person or an object), and the absence of capable guardianship.

Since RAT was developed to explain victimization in the physical world, its application to cyberspace has been the subject of several debates (e.g., Leukfeldt and Yar, 2016; Yar, 2005). Originally formulated for crimes requiring spatial and temporal convergence, the core elements of RAT have been considered continuous when adapted to cybercrime (Park and Vieraitis, 2021). As Wilsem (2013) argues, in an online context, motivated offenders and suitable targets are more likely to 'converge' the more targets expose themselves to computer activities and the more they interact with offenders.

Concerning the relationship between exposure and fear of cybercrime, findings show mixed results. Roberts et al. (2013) and Cook et al. (2023) observed that aspects of internet usage, such as frequency and context (home vs. mobile), were predictors of fear related to online identity theft and economic cybercrime. Conversely, Henson et al. (2013) and Guedes et al. (2022) found that exposure dimensions did not explain fear of online identity theft. These results align with Virtanen's study (2017), which found that internet use was not associated with fear of cybercrime.

Concerning 'target suitability,' often measured by engagement in risky behaviors, a set of studies provide insights into how individuals' actions might elevate their fear. For instance, Lee et al. (2019) found that users who exhibited higher levels of personal information disclosure on social networking sites reported increased fear of victimization through perceived risk of victimization. Similarly, Park and Vieraitis (2021) found that having a greater number of social networking services accounts was associated with higher levels of victimization and fear. Guedes et al. (2022) observed that individuals who reported having more interactions with strangers online were less fearful of online identity theft, potentially because this is indicative of lower perceived risks of victimization. Finally, Choi et al. (2021) noted that none of the target suitability measures (engage in identity theft and download pirated software) explained fear of identity theft.

The studies that include online guardianship to address fear of cybercrime are scarce. For instance, Brands and van Wilsem (2021) found inconclusive negative correlations between the fear and the use of spam filters and wireless network security. Guedes et al. (2022) found that those who reported adopting more avoidance behaviors had higher levels of fear of online identity theft. Cook et al. (2023) observed that all the dimensions of guardianship measures were associated with higher levels of fear.

Computer skills can be considered a measure of online guardianship since they enhance an individual's ability to implement effective cybersecurity measures. Virtanen (2017) and Guedes et al. (2022) observed that individuals with higher computer skills were less fearful; perhaps increased levels of technical skills perception might increase the feelings of control over the risk of becoming a victim.

Current study

This study analyzes the determinants of fear of interpersonal cybercrime (fears of cyberbullying and cyberstalking) and of fear of property cybercrime (fears of online consumer

fraud, online identity theft, and malware discovery), and whether those determinants are different according to the type of fear of cybercrime. The selection of these cyber offenses was based on their significant social impact and prevalence, as well as previous studies that generally focus not only on victimization but also on fear of cybercrimes. Works such as those by Pereira and Matos (2016), Fissel et al. (2024), Randa (2013), and Aizenkot (2022) are some examples where those crimes are included. It is important to note that some of the offenses selected for this study have legal recognition in the Portuguese context, even if not autonomously categorized. For instance, cyberstalking is encompassed within the general statutes of stalking crimes, which are prosecutable when facilitated through digital means (Art. 154-A, Portuguese Penal Code). Accordingly, cyberbullying, while not autonomously recognized as a crime, entails behaviors that are punishable under multiple existing statutes, including threat (Art. 153), coercion (Art. 154), and others. For property cybercrimes, our selection of online consumer fraud, identity theft, and malware reflects their significant repercussions on personal and organizational assets. For instance, malware software disrupts and damages systems, leading to considerable data and financial losses, which aligns with the legal categorization of property crimes. Any malware attack results in affecting users in various ways, such as loss of data, business, and overall directly or indirectly caused financial loss (Kumar et al., 2021).

Compared to other studies, our investigation is innovative because it: (i) uses crime-specific measures instead of generalized measures of fear of crime; (ii) operationalizes the three elements of RAT (exposure to motivated offenders, target suitability, and absence of a capable guardianship) in the explanation of fear of cybercrimes.

The hypotheses of the present study are as follows:

1. Fears of interpersonal and property cybercrime are associated with sociodemographic (e.g., gender, age, education, economic insecurity) and individual variables (victimization experiences and offline fears);
2. Fears of interpersonal and property cybercrime are partially associated with the dimensions of RAT.
3. The variables that are significantly associated with fear of interpersonal cybercrime differ from those associated with fear of property cybercrime.

Material and methods

Data

Through a quantitative methodological approach, an anonymous online self-report survey was administered in 2020. Data were collected through two different and complementary ways: (i) an email presenting the purposes of the study and the link to the survey was disseminated by the University of Porto inviting students and staff to participate in this research; (ii) the online survey was disclosed on different social media platforms, including Facebook, Instagram, and LinkedIn, to reach a diverse audience beyond the students and staff of the University of Porto. The survey link was posted on these platforms with a brief description of the study, inviting participants to contribute to the

study on perceptions and victimization of cybercrimes. The participation was explicitly stated to be voluntary. Moreover, this approach was intended to engage individuals who were active online, thus likely to have relevant experiences and opinions on the subject matter.

In total, 726 individuals answered the questionnaire, of which 61.7% are students. About 70% were female, and the mean age of the sample was 27.47 years. The majority (79.20%) were living more individually (single, divorced, or separated), and the average educational level (in years) was approximately 13 (completion of secondary education). The remaining sociodemographic and individual features of the sample are presented in Table 1.

Measures

The operationalization of the dependent (fears of interpersonal and property cybercrimes) and independent (sociodemographic and individual characteristics, fear of offline crime, previous online victimizations, and RAT core elements) variables will be described next.

Dependent variable

In the current study, fear of online crime was measured using five types of cybervictimization: online identity theft, online consumer fraud, malicious software, cyberstalking, and cyberbullying. Two aggregate measures of fear were then constructed (fear of interpersonal and fear of property cybercrime). Following previous measures of fear of crime (e.g., Gray et al., 2008), participants were asked: 'On a scale from 1 (no fear) to 4 (very afraid), how afraid are you of the following situations occurring to you?'

The category *fear of interpersonal cybercrime* included both fear of cyberstalking and fear of cyberbullying (Cronbach's $\alpha = .88$). Concretely, and following Pereira and Matos (2016), to measure fear of cyberstalking participants were asked how afraid they were that 'someone, repeatedly and intentionally, imposes unwanted forms of communication, approach or pursuit on you, through the internet or other electronic device?' To operationalize cyberbullying, participants were asked how afraid they were of 'receiving hostile or aggressive messages that cause you harm or discomfort, via the internet or any other electronic device?' (Tokunaga, 2010).

Fear of property cybercrime was measured using three types of fear of cybercrime: online identity theft, online consumer fraud, and discovering malicious software (Cronbach's $\alpha = .65$). Specifically, to measure fear of online identity theft, a question based on Hille et al. (2015) was used, asking participants the level of fear that 'someone appropriates, via the internet, your personal and financial data without prior consent and knowledge and use them improperly?' In turn, fear of online consumer fraud victimization ==was measured by asking how afraid they were of 'purchasing products or services via the internet that do not reach home, are counterfeit or do not match the way they were advertised?' (European Commission, 2020). Fear of encountering malicious software was measured by asking participants whether they were afraid of 'discovering malware in your device (e.g., viruses, trojans, spyware)?' (European Commission, 2020).

Table 1. Descriptive statistics.

Variables	*N*	*M* (*SD*)	*F*	%	Min.–Max.
Dependent variables					
Fears of property cybercrimes (α = .65)	726	3.09 (.64)*	—	—	1–4
Fears of interpersonal cybercrimes (α = .88)	726	2.66 (.99)	—	—	1–4
Independent variables					
Sociodemographic and individual characteristics					
Gender (female)	723	—	511	70.70	—
Age	725	27.47 (11.78)	—	—	16–72
Education	726	—			1–18
Marital status (single/divorced/separated)	726	—	575	79.20	—
Economic insecurity (α = .86)	726	5.82 (2.52)	—	—	1–10
Fear of offline interpersonal crime (α = .83)	726	3.35 (1.29)	—	—	1–5
Fear of offline property crime (α = .90)	726	3.37 (1.14)	—	—	1–5
Previous online victimizations	726	.52 (.86)	—	—	0–5
Dimensions of the RAT					
Exposure to motivated offenders					
Hours spent on the internet	726	3.67 (.94)			1–5
Economic exposure	726	2.42 (.84)			1–4
Interactive exposure	726	1.33 (.50)			1–4
Entertainment exposure	726	3.01 (.67)			1–4
Target suitability					
Opening unknown files, links, or attachments	726	1.13 (.36)			1–4
Communicating or providing data to strangers	726	1.34 (.50)			1–4
Risky use of internet pages	726	1.26 (.43)			1–3.5
Quantity of information published	726	4.10 (2.36)			0–12
Capable guardianship					
Overall capable guardianship index	726	10.54 (2.24)			2–16
Computer knowledge	726	1.89 (.61)			1–3

Note: F = absolute frequency.

Independent variables

Sociodemographic and individual characteristics. Sociodemographic variables included gender, age, education, marital status, and perceived economic insecurity. *Gender* was measured by asking participants to select one of three options: female, male, and other. Since only three individuals answered 'other,' gender was treated as a dichotomous variable (0 = female; 1 = male). *Age* was a continuous variable measured in years. *Education levels* ranged from 1 (1 year of education) to 18 (post-PhD). Participants were also asked about their *marital status*, which was subsequently dichotomized (0 = single, encompassing individuals who were single, divorced, or separated; 1 = married or in a *de facto* union). *Economic insecurity*, adapted from Britto (2013), was assessed using a set of three items

gauging individuals' concerns about: 'the possibility of losing or not finding a job due to the current economic situation'; 'the possibility of not moving up in your career due to the current economic situation'; and 'confronting a considerable and unforeseen expense.' Participants answered on a 10-point Likert scale (1 = not worried at all, to 10 = extremely worried) and an overall index was created ($\alpha = .86$).

Concerning other individual variables, this survey included fear of offline interpersonal crime, fear of offline property crime, and previous online victimizations. To measure fear in offline contexts, individuals were asked to rate, on a scale ranging between 1 (not afraid) and 4 (very afraid), 'How much do you fear that the following events might happen to you?' The options included crimes such as being physically and sexually assaulted, getting robbed, and experiencing a home invasion. An index of *offline interpersonal fear*, comprising the fears of physical assault and sexual assault ($\alpha = 0.83$), and an index of *offline property fear*, consisting of fears related to robbery, home invasion, property vandalism, and car theft ($\alpha = 0.90$) was computed.

Previous online victimizations were measured through an aggregate measure of cybervictimization, including the above-referred cybercrimes: online identity theft, online consumer fraud, the discovery of malicious software, cyberstalking, and cyberbullying. For instance, regarding online consumer fraud, participants were asked: 'In the last 12 months, have you purchased any products or services via the internet that do not reach home, were counterfeit or did not match the way they were advertised?' Given that these cybervictimizations were assessed dichotomously (0 = non-victim; 1 = victim), we aggregated the occurrences over the past 12 months to create a cybervictimization index. Consequently, a higher score on this variable indicates a greater number of reported cybervictimizations.

RAT. The operationalization of the three core theoretical elements of RAT (online exposure to motivated offenders, target suitability, and capable guardianship) followed previous studies (e.g., Reyns, 2013).

Online *exposure to motivated offenders* was measured not only by the number of hours spent on the internet but also by the frequency of online activities undertaken by individuals. Participants were asked, 'On average, how many hours a day do you spend on the internet?' ranging between <1 hour and 10 or more hours. To measure their online activities, based on previous studies (e.g., Henson et al., 2013; Reyns, 2013), individuals were asked about their engagement, on a scale from 1 (not often) to 4 (very often), in the following routine online activities: (1) online banking or managing finances; (2) buying goods or services on the internet; (3) email or instant messaging; (4) social networking (e.g., Facebook); (5) daily social networking updates; (6) reading or writing blogs or forums; (7) actively participating in chat rooms or other forums; (8) interaction on dating websites (e.g., Tinder, Omegle); (9) downloading music, movies, games, or podcasts; (10) watching entertainment content (e.g., YouTube); and (11) work or study support. After performing a factor analysis (data not shown), three composite indexes were found: economic exposure (types 1 and 2), interactive exposure (types 7 and 8), and entertainment exposure (types 4, 9, and 10).

Target suitability was assessed through a set of two questions. First, based on previous studies (e.g., Choi, 2008; Marcum, 2010; Ngo and Paternoster, 2011; Reyns, 2013; 2015), participants were asked to rate the frequency of the following actions on a scale from 1 (not

often) to 4 (very often): (1) communicated with strangers online; (2) opened any unfamiliar attachments to emails that they received; (3) opened any file or attachment they received through their instant messengers; (4) voluntarily provided their personal data to someone unknown; (5) clicked on a pop-up message; and (6) visited risky websites. A factor analysis was performed (data not shown) and three underlying composite indices were obtained: opening unknown files, links, or attachments (types 2 and 3); communicating or providing data to strangers (types 1 and 4); and risky use of internet pages (types 5 and 6).

Target suitability was also captured by the quantity of information published on social networks and the internet in general. Therefore, the sum (0 = no, 1 = yes) of 12 types of information, including complete name, age, gender, sexual orientation, and relationship status. This scale varied between 0 (no information) and 12 (all types of information described).

Finally, *online capable guardianship* was divided into two types: physical/technological and personal. The former encompasses all varieties of security software such as antivirus, antispyware, and firewall programs. Therefore, using previous measures used by Williams (2016) and Ngo and Paternoster (2011), individuals were asked (0 = no, 1 = yes) whether they: (1) use a spam filter in the email; (2) use internet browser security software (e.g., Avast Secure Browser, Google Safe Browsing, Tor Browsing); (3) have installed and updated paid antivirus software, antispyware software, or firewall software/hardware; and (4) have installed and updated free antivirus software, antispyware software, or firewall software/hardware. Moreover, within the scope of personal guardianship, we further delineated three subcategories: protective behaviors, avoidance behaviors, and computer knowledge. Protective behaviors included in our measurement were: (5) regularly change of passwords; (6) use of strong passwords in length and characters; (7) use of two-step security verification; (8) use of biometric features (e.g., facial recognition, fingerprint); (9) exclusive use of their own computing devices; and (10) accessing only trusted websites. The types of avoidance behaviors were: (11) avoiding accessing online banking; (12) avoiding online shopping; (13) avoiding opening emails from people you do not know; (14) avoiding connecting to the internet via public Wi-Fi networks; (15) avoiding using dating/making friends websites (e.g., Tinder, Omegle); and (16) avoiding sharing personal information on social media or the internet in general.

Online capable guardianship was assessed through a sum of behaviors, with higher scores indicating a greater adoption of security-related practices.

Finally, for computer knowledge, participants were asked to assess their perception of computer skills, ranging between basic, medium, and advanced (Holt and Bossler, 2013).

Data analysis

This study examines the determinants of fears of interpersonal and property cybercrimes and whether those determinants are different according to each type. First, we present descriptive statistics. Second, we explore the determinants of both types of fear of cybercrime using linear regression analyses. For each dependent variable, three models were performed: first, a partial model composed of sociodemographic variables; second, a partial model in which other individual variables (fears of offline interpersonal and property crime and previous online victimizations) were added to the sociodemographics variables; lastly, a full model comprising the two previous sets and the RAT variables. To build the indexes related to the

RAT dimensions, we conducted exploratory factor analysis with Varimax rotation, ensuring that only items with factor loadings above 0.5 were included. Subsequently, the items that clustered significantly under each factor were computed to create a consolidated index for each dimension. IBM SPSS Statistics 28 was used in all stages to analyze the data.

Results

Descriptive statistics

Table 1 presents the descriptive statistics of the study variables. Concerning the dependent variables, we observe that the mean value of *fear of property cybercrime* ($M = 3.09$) is higher than the mean value of *fear of interpersonal cybercrime* ($M = 2.66$), suggesting that participants are more fearful of the former than of the latter type of cybercrime. This difference is statistically significant ($t = -15.797$, $p < .001$).

Regarding the independent variables, the mean ratings of *fear of offline property crime* ($M = 3.37$) and *fear of offline interpersonal crime* ($M = 3.35$), in turn, are very approximate. For *previous online victimizations*, the mean value was 0.52, meaning that there is less than one victimization experience per person on average in the sample. On the first dimension of the RAT (exposure to motivated offenders), for the variable *hours spent on the internet* the majority of participants reported that they spent daily between 6 and 9 hours (39.40%), followed by between 3 and 5 hours (29.80%), 10 or more hours (19.70%), between 1 and 2 hours (10.10%), and <1 hour (1.10%) (not displayed in Table 1). The average score of this variable, varying between 1 and 5, was 3.67. For the other variables of this dimension, respondents expressed higher mean ratings for the scale of *entertainment exposure* ($M = 3.01$) than for the scales of *economic exposure* ($M = 2.42$) and *interactive exposure* ($M = 1.33$). Note that these variables vary between 1 and 4. As for the second dimension (target suitability), the activities with higher mean values were *communicating or providing data to strangers* ($M = 1.34$) and *risky use of internet pages* ($M = 1.26$), followed by *opening unknown files, links, or attachments* ($M = 1.13$). However, these are considered low values since the maximum scale ranges from 3.5 to 4. Therefore, it appears that the sample engages in these behaviors infrequently. The mean rating for the quantity of information published on social networks and on the internet was 4.10, on a scale from 0 to 12. This suggests that the quantity of information shared by the sample is relatively low. Concerning the third dimension (capable guardianship), for the *overall capable guardianship index*, the average score was 10.54, suggesting a moderate level of capable guardianship within the sample, and for the *computer knowledge*, it was 1.89 (out of a maximum of 3).

Determinants of fear of interpersonal and property cybercrime

Linear regression analyses were run to explore which factors influence both types of fear of cybercrime. As mentioned, for each dependent variable, three models were performed: (a) a partial model composed of sociodemographic variables; (b) a partial model in which other individual variables (fears of offline interpersonal and property crime, and previous

online victimizations) were added to the sociodemographic; (c) a full model comprising the two previous sets and the RAT variables.

Linear regressions on fear of interpersonal cybercrime

Table 2 presents the results on fear of interpersonal cybercrime. The first column represents the first partial model based on demographic characteristics. The model is statistically significant and explains nearly 21% of variation in the dependent variable. *Gender* ($\beta = -.280$, $p = < .001$), and *economic insecurity* ($\beta = .252$, $p = < .001$) present the strongest relationships with fear of interpersonal cybercrime. Thus, females and individuals who feel more insecure economically have higher levels of fear of interpersonal cybercrime. *Education* ($\beta = -.163$, $p = < .001$) and *marital status* ($\beta = -.125$, $p = .006$) also explain the dependent variable. Concretely, those with lower levels of education and who are living more individually (single, divorced, or separated) are more fearful of interpersonal cybercrime. No significant effects of *age* are found.

The second partial model, in which the fears of offline interpersonal and property crime and previous online victimizations were added, explains around 37% of variation in the dependent variable. The most relevant variables explaining the fear of interpersonal cybercrime are *fear of offline interpersonal crime* ($\beta = .342$, $p = < .001$) and *fear of offline property crime* ($\beta = .209$, $p = < .001$). *Economic insecurity* ($\beta = .100$, $p = .003$), *marital status* ($\beta = -.092$, $p = .024$), and *education* ($\beta = -.087$, $p = .008$), although remaining associated with the dependent variable, lose strength. Additionally, the effect of *gender* disappears. Thus, these results suggest that the influence of those sociodemographic characteristics on fear of interpersonal cybercrime is substantially mediated by fears of offline interpersonal and property crime. No significant effects of *previous online victimizations* were found.

The full model, which also comprises the RAT variables, explains approximately 40% of variation in the fear of interpersonal cybercrime. This modest increase suggests that the RAT variables contribute minimally to explaining the variation in fear of interpersonal cybercrime. *Fear of offline interpersonal crime* ($\beta = .336$, $p = < .001$) and *fear of offline property crime* ($\beta = .205$, $p = < .001$) remain the variables with strongest associations with the dependent variable. Additionally, *opening unknown files, links, or attachments* ($\beta = .116$, $p = < .001$), *computer knowledge* ($\beta = -.104$, $p = < .001$), *risky use of internet pages* ($\beta = -.078$, $p = .017$), and *overall capable guardianship index* ($\beta = .072$, $p = .021$) explain the fear of interpersonal cybercrime. Therefore, individuals more involved in online activities, such as opening unknown files, links, or attachments, and who adopt more online measures and behaviors to protect themselves report higher levels of fear of interpersonal cybercrime. On the other hand, higher levels of computer skills and risky use of internet pages (e.g., clicking on pop-up messages) are associated with lower levels of fear of interpersonal cybercrime. Regarding the sociodemographic variables, only *economic insecurity* ($\beta = .099$, $p = .003$) maintains its statistical significance. This suggests that, although to a lesser extent, the RAT variables also have a mediating effect between sociodemographic characteristics and fear of interpersonal cybercrime.

Table 2. Linear regression models on fear of interpersonal cybercrime.

	Partial model 1			Partial model 2			Full model		
Predictors	*B*	*SE*	β	*B*	*SE*	β	*B*	*SE*	β
Sociodemographic characteristics									
Gender (female = 0)	−.606	.075	**−.280*** **	−.145	.079	−.067	−.096	.081	−.044
Age	.005	.004	.059	.006	.004	.074	.005	.004	.054
Education	−.076	.017	**−.163*** **	−.040	.015	**−.087** *	−.028	.015	−.061
Marital status (single, divorced, or separated = 0)	−.303	.110	**−.125** *	−.223	.098	**−.092** *	−.182	.099	−.075
Economic insecurity	.099	.014	**.252*** **	.039	.013	**.100** *	.039	.013	**.099** *
Individual characteristics									
Fear of offline interpersonal crime				.262	.039	**.342*** **	.258	.039	**.336*** **
Fear of offline property crime				.181	.037	**.209*** **	.178	.036	**.205*** **
Previous online victimizations				.063	.034	.055	.040	.035	.035
Dimensions of the RAT									
Exposure to motivated offenders									
Hours spent on the internet							.006	.033	.006
Economic exposure							−.047	.038	−.040
Interactive exposure							.108	.062	.055
Entertainment exposure							.028	.055	.019
Target suitability									
Opening unknown files, links, or attachments							.322	.088	**.116*** **
Communicating or providing data to strangers							−.017	.068	−.009
Risky use of internet pages							−.180	.075	**−.078** *
Quantity of information published							.016	.014	.037

(Continued)

Table 2. (Continued)

Predictors	Partial model 1			Partial model 2			Full model		
	B	*SE*	β	*B*	*SE*	β	*B*	*SE*	β
Capable guardianship									
Capable guardianship index							.032	.014	**.072***
Computer knowledge							−.169	.051	**−.104****
	Adjusted $R^2 = .209$ $p = < .001$			Adjusted $R^2 = .372$ $p = < .001$			Adjusted $R^2 = .396$ $p = < .001$		

Note: Bold values indicate those that achieved statistical significance.
*$p \leq .05$, **$p \leq .01$, ***$p \leq .001$.

Linear regressions on fear of property cybercrime

The models on fear of property cybercrime are displayed in Table 3. The first partial model, including sociodemographic variables, explains around 16% of variation in the dependent variable. *Economic insecurity* ($\beta = .329$, $p = < .001$) stands out as the variable that plays the most important role in explaining the dependent variable, followed by *gender* ($\beta = -.182$, $p = < .001$), *education* ($\beta = -.145$, $p = < .001$), and *age* ($\beta = .101$, $p = .048$). Thus, individuals who feel more insecure economically, females with lower levels of education, and older people report higher levels of fear of property cybercrime. No significant effects of *marital status* are found.

The second partial model explains approximately 28% of variation in the fear of property cybercrime. *Fear of offline property crime* ($\beta = .347$, $p = < .001$) presents the strongest association with the dependent variable. That is, the individuals who have higher levels of fear of offline property crime also express higher levels of fear of property cybercrime. Among the sociodemographic variables, only *economic insecurity* ($\beta = .212$, $p = < .001$) and *education* ($\beta = -.077$, $p = .029$) remain statistically significant. However, it is worth noting that both lose strength in this model, suggesting that fear of offline property crime has a mediating effect between sociodemographic characteristics and fear of property cybercrime. No significant effects of *fear of offline interpersonal crime* and *previous online victimizations* are found.

Lastly, the full model explains around 29% of variation in the fear of property cybercrime. Taking into consideration the previous percentage (28%), this slight change suggests that the RAT variables provide a minimal contribution to the variation in fear of property cybercrime, as also observed in the fear of interpersonal cybercrime. *Fear of offline property crime* ($\beta = .342$, $p = < .001$) and *economic insecurity* ($\beta = .205$, $p = < .001$) remained the most important variables explaining the dependent variable. Only *quantity of information published on social networks and on the internet in general* ($\beta = .099$, $p = .007$) and *opening unknown files, links, or attachments* ($\beta = .073$, $p = .034$) play a role in the fear of property cybercrime. Thus, individuals who publish more information on social networks and on the internet in general and are more involved in online activities such as opening unknown files, links, or attachments report higher levels of fear of property cybercrime. It is also observed that *age* ($\beta = .114$, $p = .029$) re-emerges as a significantly associated variable in this final model, which may be explained by moderating effects of the variables added in this model.

Discussion

The present study ($N = 726$) examined how individual and contextual variables differently influenced fears of interpersonal and property cybercrime. Concretely, we aimed to determine whether these types of fears are different, analyzing this by comparing the variables that explain each fear.

First, it is worth noting that the levels of fear of property cybercrime were higher compared to fear of interpersonal cybercrime. This finding aligns with previous research (Henson et al., 2022; Yu, 2014). Several reasons may account for these results. For

Table 3. Linear regression models on fear of property cybercrime.

Predictors	Partial model 1			Partial model 2			Full model		
	B	*SE*	β	*B*	*SE*	β	*B*	*SE*	β
Sociodemographic characteristics									
Gender (female = 0)	−.255	.050	**−.182*** **	−.086	.055	−.061	−.076	.056	−.054
Age	.005	.003	**.101***	.004	.003	.083	.006	.003	**.114***
Education	−.043	.011	**−.145*** **	−.023	.011	**−.077***	−.016	.011	−.053
Marital status (single, divorced, or separated = 0)	.011	.073	.007	.035	.068	.022	.055	.069	.035
Economic insecurity	.083	.009	**.329*** **	.054	.009	**.212*** **	.052	.009	**.205*** **
Individual characteristics									
Fear of offline interpersonal crime				.036	.027	.073	.037	.027	.075
Fear of offline property crime				.194	.025	**.347*** **	.191	.025	**.342*** **
Previous online victimizations				−.010	.024	−.013	−.023	.025	−.031
Dimensions of the RAT									
Exposure to motivated offenders									
Hours spent on the internet							−.026	.023	−.038
Economic exposure							−.034	.026	−.045
Interactive exposure							.042	.044	.033
Entertainment exposure							.066	.038	.069
Target suitability									
Opening unknown files, links, or attachments							.131	.061	**.073***
Communicating or providing data to strangers							−.056	.047	−.044
Risky use of internet pages							−.020	.052	−.014
Quantity of information published							.027	.010	**.099** **

(Continued)

Table 3. (Continued)

Predictors	Partial model 1			Partial model 2			Full model		
	B	*SE*	β	*B*	*SE*	β	*B*	*SE*	β
Capable guardianship									
Capable guardianship index							.010	.010	.036
Computer knowledge							−.041	.035	−.039
	Adjusted $R^2 = .158$			Adjusted $R^2 = .278$			Adjusted $R^2 = .292$		
	$p = < .001$			$p = < .001$			$p = < .001$		

Note: Bold values indicate those that achieved statistical significance.
*$p \leq .05$, **$p \leq .01$, ***$p \leq .001$.

instance, participants may perceive property-related cybercrimes as having a more significant impact on their personal well-being, resulting in important financial losses, and damaging one's reputation (e.g., Cross et al., 2016). This perceived risk of tangible loss significantly heightens fear levels. Another explanation might be that individuals have greater control over interactions and relationships online, making them feel more able to handle interpersonal cybercrimes (e.g., not talk with strangers online, which could lead to further harassment). In contrast, the perceived unpredictability and uncontrollability of property crimes, such as fraud or identity theft, could amplify fear as individuals feel less able to prevent these crimes.

As stated earlier, this study aims to discern whether the variables influencing fear of interpersonal and property cybercrime differ. We will start by detailing the findings related to the fear of property cybercrime, then proceed to the fear of interpersonal cybercrime. Subsequently, we will analyze and compare the factors associated with each type of fear.

In general, we found that participants who were older and reported higher economic insecurity presented higher levels of property cybercrime. Moreover, fear of offline property crime was the strongest variable playing a role in fear of property cybercrime. Regarding the core dimensions of RAT, results suggested that neither the exposure variables nor the guardianship ones were relevant to the fear of property crime. In contrast, those who engaged in riskier behaviors such as sharing more personal information online or clicking on unfamiliar links and attachments exhibited higher levels of fear. However, it is worth noting that the contribution of the RAT variables was relatively small, with an increase in explanatory power of only 1.4% in the model's variance for fear of property crime.

Regarding the fear of interpersonal cybercrime, the results showed that none of the sociodemographic variables were significant determinants, except for economic insecurity, with a lesser explanatory power compared to fear of property cybercrime. Furthermore, the most important predictors of fear of interpersonal cybercrime were fear of offline interpersonal crime and fear of offline property crime. Finally, with regards to the applicability of RAT, different patterns emerged when comparing both fears. Indeed, both variables of capable guardianship predicted fear of interpersonal cybercrime. On one hand, individuals who adopt more behaviors to secure their computers and personal information reported more fear of interpersonal cybercrime. Moreover, those who perceive themselves as having lower computer skills reported more fear as well. Concerning target suitability, as in fear of property cybercrime, opening unknown files or links predicted fear of interpersonal cybercrime positively, and, in the opposite direction, those who make risky use of internet pages were less fearful of interpersonal cybercrime.

The first noteworthy aspect to highlight is that the strongest (positive) relationship with both fears of cybercrime was the fear of offline crime. This result provides a significant direction for future research: in explaining fear of cybercrime, the overall experience of fear in general may be more pertinent than sociodemographic characteristics, prior victimization experiences, or online habits. Previously, Roberts et al. (2013) and Guedes et al. (2022) also observed that the strongest predictor of fear of online identity theft was general fear of crime. This result is also in accordance with Gabriel and Greve's

work (2003), which suggested that fear of concrete situations might be related to a more general tendency of experiencing fear. Also, Guedes et al. (2018) found that fear of crime was explained by the trait or dispositional emotion of fear in general. These findings also indicate a psychological continuity between offline and online fears. The fact that fear of interpersonal cybercrime was predicted by both fears might somehow shed light on the Shadow of Sexual Assault Hypothesis (Warr, 1984), suggesting that women's offline experiences and fears relating not only to interpersonal crime but also to property crimes can extend into the online realm, influencing their fear of interpersonal cybercrimes (Henson et al., 2022).

Contrary to previous research (e.g., Henson et al., 2013; Virtanen, 2017), our study found no significant impact of past online victimizations on fears related to cybercrime. Similarly, Jansen et al. (2017) noted a lack of significant correlation between victimization experiences and the fear of online crime. A potential explanation is that experiencing victimization may prompt individuals to adopt preventive measures, effectively reducing their anxiety about future cyber threats. However, future research should explore whether specific types of cybercrime victimization disproportionately influence corresponding fears. For example, Lee and Kim (2023) found that individuals are more likely to fear types of cybercrime that they have previously encountered.

Another relevant result is concerned with the significant role of economic insecurity in explaining both fears of cybercrimes. To the best of our knowledge, this is the first study analyzing the prediction of these generalized anxieties in the fear of cybercrimes. It is not surprising that the explanatory power of economic insecurity was higher for fear of property cybercrime. This suggests that financial concerns may be more intrinsically linked to the fear of material loss than to the fear of harmful interpersonal online interactions. Therefore, fear of cybercrime may act as a 'sponge' that absorbs all sorts of generalized anxieties, such as uncertainty in terms of economic position, employment status, or others (Britto, 2013).

An additional relevant result concerning age emerged. Concretely, older individuals reported being more fearful of property cybercrime but not of interpersonal cybercrime. Research has shown that older people usually report higher levels of fear of offline (e.g., Chon and Wilson, 2016; Lane and Fox, 2012) and online property crime (Brands and Wilsem, 2021). One hypothesis is that older age might be related to greater worries about online crimes through the low confidence these people have in their abilities to use computers or the internet. Relatedly, older individuals might perceive themselves as more vulnerable to property-related cybercrimes due to their lack of familiarity with online security measures and serious consequences anticipation.

Finally, this article also investigated the role of the RAT in explaining both fears of cybercrime. One key observation is that, given the relatively minor increase in variance when incorporating RAT's core dimensions, it can be inferred that what we do on the internet—our exposure, risky behaviors, and protective measures—only partially accounts for explaining our fears. In fact, as already pointed out before, neither the hours spent online nor the engagement in several online activities (e.g., online banking, buying things on the internet, interacting on dating websites) were relevant to explain why individuals fear interpersonal or property-related cybercrimes. This result is at odds with Cook et al. (2023), who observed that fear of economic-related crimes

was associated with exposure dimensions such as frequency of internet use. On the other hand, Henson et al. (2013), Virtanen (2017), and Guedes et al. (2022) found that none of the exposure variables were associated with fear of cybercrime. The lack of significant results regarding exposure to motivated offenders raises questions about the conceptual distinction between this variable and target suitability in the context of cybercrime. Given the nature of cyberspace, where potential offenders are ubiquitous and access to targets is often facilitated, it may be challenging to separate these concepts or accurately measure exposure to motivated offenders.

A relevant difference emerged between the two types of fear concerning the importance of capable guardianship in explaining them. Specifically, individuals who adopted more security behaviors presented higher levels of fear of interpersonal cybercrime, but not of property crime. This could be explained by the direct and personal nature of interpersonal cybercrimes, where victims often perceive a more immediate threat to their personal security or privacy. The positive relationship between the adoption of behaviors and fear of cybercrime aligns with the findings of Guedes et al. (2022) and Cook et al. (2023) who noted that individuals who engaged in more security online behaviors exhibited higher levels of fear of cybercrime. One possible explanation is that the dimensions of guardianship can be regarded as proxy measures of the behavioral dimension of fear of crime, which is typically positively correlated with fear (e.g., Liska et al., 1988). Furthermore, those with higher computer skills reported significantly lower levels of fear of interpersonal cybercrime, suggesting that they might feel more able to manage the risk of being victimized and avoid potentially malicious interactions with others, preventing future victimizations. On the contrary, since the sources of victimization of property-related offenses are more diffuse, it might be harder for individuals to believe that their computer skills are enough to avoid those attacks. This finding underscores the importance of enhancing digital literacy, particularly in mitigating fears related to property cybercrimes, where advanced skills are essential to navigate and respond to sophisticated attack tactics.

The last remark is related to the role of the target suitability, one of the core dimensions of RAT. The common predictor of fear of cybercrimes analyzed in the present study was opening unknown files, links, or attachments. Risky behaviors such as these not only increase the likelihood of cybercrime victimization (e.g., Al-Shalan, 2006; Reyns and Henson, 2015) but also heighten the fear of individuals. One plausible explanation is the mediating role of perceived risk. When respondents open those links or files, they may be aware that such actions could make them vulnerable to interpersonal threats. Additionally, they may recognize that these actions could potentially result in financial losses or damage to their digital property. Furthermore, the more individuals post personal information online, the more they fear interpersonal cybercrime, but not property cybercrime. This result is consistent with Park and Vieraitis (2021) and Lee et al. (2019), who found that those who exposed higher levels of personal information tended to be more fearful of cybervictimization.

In summary, although fear of interpersonal cybercrime and fear of property cybercrime share some relevant predictors (such as economic insecurity, offline fear, and risky behaviors), they are explained differently by particular predictors. These results reflect the importance of accounting for the complexity of fear of (online) crime and

using specific measures to achieve a better understanding of the nature of this phenomenon.

The present study has some limitations that need to be considered. Even though we achieved a high sample ($N = 726$), it is not representative of the Portuguese population. For instance, the survey respondents have a level of education significantly higher than the Portuguese population average, and females and younger individuals are overrepresented. Moreover, around 60% of the sample is composed of students, which may have different exposure or perceptions of cybercrime compared to other demographic groups. Thus, the results should be interpreted with caution, and further research should include more extensive and diversified samples.

The reliance on self-reported data to measure relevant behaviors related to target suitability or capable guardianship might introduce potential biases. In fact, such data are susceptible to social desirability, which may affect the accuracy of the reported behaviors. What people say they do online often differs from what they do online (e.g., Wilcockson, Ellis, and Shaw, 2018). The study's cross-sectional design also restricts our ability to infer causality. Longitudinal studies, which are scarce in this field (one recent exception is the study employed by Van 't Hoff-de Goede et al., 2024) would provide a deeper understanding of the evolution of cybercrime fears and the effectiveness of preventative measures over time.

Another important caveat of this study is the limited number of cybercrimes included, especially in the online interpersonal fear. In fact, only two offenses were included (cyberbullying and cyberstalking). Moreover, in the future, it would be relevant to explore fears of other online offenses such as hacking and phishing. Also, in upcoming studies, it would be beneficial to employ victimization measures that encompass longer time frames, such as experiences in the last 3–5 years or lifetime experiences. It is similarly important to acknowledge that the Cronbach's alpha of the fear of property cybercrime is relatively low (.65), perhaps being indicative of the diverse nature of these cybercrime fears. Future research could consider refining the scale items and, as mentioned above, including other online offenses. Finally, future studies should consider incorporating broader measures of generalized fear of anxiety, beyond economic insecurity, to further explore their potential influence on fear of cybercrime.

Despite the limitations, this study provides valuable insights into the literature and research on fear of cybercrime, contributing to disentangling its complex nature. The results suggest that fears of interpersonal and property cybercrimes are influenced by fundamentally different factors. Interpersonal cybercrime fears are more related to general and personal fears that translate from the physical to the digital environment, whereas property cybercrime fears are strongly tied to economic insecurity and concerns over tangible material losses, both offline and online. These differences call for targeted prevention and education strategies, alongside strengthened technological defenses and public awareness campaigns focusing on vulnerable groups and risky behaviors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Inês Sousa Guedes https://orcid.org/0000-0002-4804-9394
José Martins https://orcid.org/0009-0001-9453-1608
Samuel Moreira https://orcid.org/0000-0002-6873-492X

References

Aizenkot D (2022) The predictability of routine activity theory for cyberbullying victimization among children and youth: Risk and protective factors. *Journal of Interpersonal Violence* 37(13-14): NP11857–NP11882.

Al-Shalan A (2006) *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Mississippi State University.

Brands J and Van Doorn J (2022) The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior* 127: 107082.

Brands J and Van Wilsem J (2021) Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology* 18(2): 213–234.

Britto S (2013) 'Diffuse anxiety': The role of economic insecurity in predicting fear of crime. *Journal of Crime and Justice* 36(1): 18–34.

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

Choi J, Kruis NE and Choo KS (2021) Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice* 37(3): 406–426.

Chon DS and Wilson M (2016) Perceived risk of burglary and fear of crime: Individual-and country-level mixed modeling. *International Journal of Offender Therapy and Comparative Criminology* 60(3): 308–325.

Cohen LE and Felson M (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588–608.

Cook S, Giommoni L, Pareja NT, et al. (2023) Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. *British Journal of Criminology* 63(2): 384–406.

Cross C, Richards K and Smith RG (2016) The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice* 518: 1–14.

European Commission (2020) Special Eurobarometer 499: Europeans' attitudes towards cyber security (report). Available at: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en.

Ferraro K (1995) *Fear of Crime: Interpreting the Victimization Risk*. New York: University of New York Press.

Ferraro K and LaGrange R (1987) The measurement of fear of crime. *Sociological Inquiry* 57(1): 70–97.

Fissel ER, Reyns BW, Nobles MR, et al. (2024) Cyberstalking victims' experiences with fear versus other emotional responses to repeated online pursuit: Revisiting the fear standard among a national sample of young adults. *Crime & Delinquency* 70(4): 1116–1147

Gabriel U and Greve W (2003) The psychology of fear of crime: Conceptual and methodological perspectives. *British Journal of Criminology* 43(1): 600–614.

Garcia E, Francisco JP and Caliso RAC (2017) Reassessing fear of crime: The role of broad insecurities. RSN-PCC Working Paper No. 17-001. Available at SSRN: https://ssrn.com/abstract=2895837 or http://dx.doi.org/10.2139/ssrn.2895837.

Gray E, Jackson J and Farrall S (2008) Reassessing the fear of crime. *European Journal of Criminology* 5(3): 363–380.

Guedes I, Domingos S and Cardoso CS (2018) Fear of crime, personality and trait emotions: An empirical study. *European Journal of Criminology* 15(6): 658–679.

Guedes I, Martins M and Cardoso CS (2022) Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal* 36: 472–497.

Hale C (1996) Fear of crime: A review of the literature. *International Review of Victimology* 4(2): 79–150.

Hanslmaier M (2013) Crime, fear and subjective well-being: How victimization and street crime affect fear and life satisfaction. *European Journal of Criminology* 10(5): 515–533.

Henson B, Reyns BW and Fisher BS (2013) Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice* 29(4): 475–497.

Henson B, Reyns BW and Fisher BS (2022) Adapting and applying offline theory to online victimization: A test of the shadow of sexual assault hypothesis with fear of online victimization. *Victims & Offenders* 17(6): 795–812.

Hille P, Walsh G and Cleveland M (2015) Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing* 30: 1–19.

Hirtenlehner H and Farrall S (2013) Anxieties about modernization, concerns about community, and fear of crime: Testing two related models. *International Criminal Justice Review* 23(1): 5–24.

Holt TJ and Bossler AM (2013) Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice* 29(4): 420–436.

Jackson J (2011) Revisiting risk sensitivity in the fear of crime. *Journal of Research in Crime and Delinquency* 48(4): 513–537.

Jansen J, Kop N and Stol W (2017) Internetbankieren: Veiligheidspercepties van gebruikers. *Tijdschrift voor Veiligheid* 16(1): 36–51.

Jordan G, Leskovar R and Marič M (2018) Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija* 51(2): 146–155.

Kumar A, Choi BJ, Kuppusamy KS, et al. (2021) Malware attacks: Dimensions, impact, and defenses. *In: Advances in Nature-Inspired Cyber Security and Resilience. Cham: Springer International Publishing*, 157–179.

Lane J and Fox KA (2012) Fear of crime among gang and non-gang offenders: Comparing the effects of perpetration, victimization, and neighborhood factors. *Justice Quarterly* 29(4): 491–523.

Lee CS and Kim JH (2023) How victims perceive fear of cybercrime: Importance of informed risk. *Criminal Justice Studies* 36(3): 206–227.

Lee S, Choi K, Choi S, et al. (2019) A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence Cybercrime* 2(2): 5–22.

Leukfeldt ER and Yar M (2016) Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37(3): 1–18.

Liska AE, Sanchirico A and Reed MD (1988) Fear of crime and constrained behavior specifying and estimating a reciprocal effects model. *Social Forces* 66(3): 827–837.

Maher CA and Hayes BE (2023) Shadow of personal fear? The role of personal and altruistic fear of cyberharassment. *Crime & Delinquency* 70(9): 2532–2558.

Marcum C, Higgins G and Ricketts M (2010) Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior* 31(5): 381–410.

Mesch GS (2000) Perceptions of risk, lifestyle activities, and fear of crime. *Deviant Behavior* 21(1): 47–62.

Moore SC and Shepherd J (2007) Gender specific emotional responses to anticipated crime. *International Review of Victimology* 14(3): 337–351.

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

Park Y and Vieraitis LM (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.

Pearson AL and Breetzke GD (2014) The association between the fear of crime, and mental and physical wellbeing in New Zealand. *Social Indicators Research* 119: 281–294.

Pereira F and Matos M (2016) Cyber-stalking victimization: What predicts fear among Portuguese adolescents? *European Journal on Criminal Policy and Research* 22: 253–270.

Pereira F, Spitzberg BH and Matos M (2016) Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior* 62: 136–146.

Rader NE, Cossman JS and Porter JR (2012) Fear of crime and vulnerability: Using a national sample of Americans to examine two competing paradigms. *Journal of Criminal Justice* 40(2): 134–141.

Randa R (2013) The influence of the cyber-social environment on fear of victimization: Cyber bullying and school. *Security Journal* 26: 331–348.

Reisig MD, Pratt TC and Holtfreter K (2009) Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior* 36(4): 369–384.

Reyns BW (2013) Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency* 50(2): 216–238.

Reyns BW and Henson B (2015) 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.

Roberts LD, Indermaur D and Spiranovic C (2013) Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law* 20(3): 315–328.

Schafer JA, Huebner BM and Bynum TS (2006) Fear of crime and criminal victimization: Gender-based contrasts. *Journal of Criminal Justice* 34(3): 285–301.

Tokunaga RS (2010) Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior* 26(3): 277–287.

Van 't Hoff-de Goede MS, van de Weijer S and Leukfeldt R (2024) Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual self-protective online behavior related to future cybercrime victimization? *Journal of Crime and Justice* 47(4): 472–491.

Virtanen S (2017) Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law* 24(3): 323–338.

Warr M (1984) Fear of victimization: Why are women and the elderly more afraid? *Social Science Quarterly* 65(6): 81–702.

Warr M (2000) Fear of crime in the United States: Avenues for research and policy. *Measurement and Analysis of Crime and Justice* 4: 451–489.

Wilcockson TD, Ellis DA. and Shaw H (2018) Determining typical smartphone usage: What data do we need? *Cyberpsychology, Behavior, and Social Networking* 21(6): 395–398.

Williams ML (2016) Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology* 56(1): 21–48.

Wilsem JV (2013) Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice* 29(4): 437–453.

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

Yu S (2014) Fear of cybercrime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology* 8(1): 36–46.