Fear and perceived risk of cyber fraud victimization among Chinese University students

Jia Qu[1] · Kai Lin[2] · Yuning Wu[3] · Ivan Y. Sun[4]

Abstract

Cyber fraud has surfaced as a serious social problem in China, resulting in billions of Chinese yuan worth of financial losses in recent years. The high prevalence and large quantity financial losses from cyber fraud have sparked widespread public concerns about online safety. Based on survey data from over 1000 university students in China, this study explores the prevalence of fear and perceived risk of cyber fraud and its correlates among university students. The results showed that although only 10% of the respondents believed they would likely experience cyber fraud victimization in the next 12 months, approximately 50% reported feeling fearful of cyber fraud in the past 3 months. The logistic regression results show that both fear and perceived risk are influenced by different domains of risk factors, with higher self-control and deviant online behaviors explaining greater odds of fear. In contrast, the perceived risk of crime is linked to vicarious victimization experiences, perceived crime seriousness, and satisfaction with the police. Implications for future research and policy are discussed.

Keywords Fear of crime · Risk of victimization · Cyber fraud · China · Self-control · University students

With the advances in information and communication technology (ICT), the Internet has become an inseparable part of human life, with the number of Internet users exceeding 5 billion worldwide (TNW, 2022). While the virtual world provides many conveniences to Internet users, it also exposes them to offenders who access the Internet for criminal opportunities. Indeed, it is reported that cybercrime has grown exponentially in the past decades (Sjouwerman, 2019), with cyber fraud frequently covered by the media as the fastest-growing cybercrime. Cyber fraud refers to fraudulent activities where the Internet or other ICTs are abused to illegally extract financial gains and/or personal information from ICT service providers or their customers (Button & Cross, 2017, pp. 6–13).

Cyber fraud is prevalent in many developed countries, such as the United States (IC3, 2024), the United Kingdom (The National Fraud Intelligence Bureau, 2022), and Australia (AIC, 2023). According to the FBI's Internet Crime Report 2023 (IC3, 2024), the US lost at least 12.5 billion US dollars to various cybercrimes, the vast majority of which were frauds and scams. In a nationally representative study published in 2023, around 7.8% of the Australians surveyed reported being victims of cyber fraud and scams in the past year (AIC, 2023). Likewise, developing countries experienced a spike in cyber fraud in recent years. In China, for example, the country recorded 927,000 cases of cyber fraud, resulting in a loss of 35.37 billion Chinese yuan (roughly 5.44 billion US dollars) in 2020 (Wang, 2021). A nationally representative survey study in China revealed that nearly half of those surveyed encountered cyber fraud attempts in 2018, and 28% suffered financial losses from them (Xu et al., 2020).

Drawing upon survey data from 1065 university students in Guizhou, China, this study assesses the prevalence and correlates of university students' fear of cyber fraud in China. This study extends the current literature on fear of crime in three ways. First, the prevalence and serious societal consequences associated with cyber fraud have inspired a growing number of studies on the phenomenon (e.g., Chen, 2021; Lee, 2021; Lin et al., 2023; Xu, 2022; Xu & Xu, 2021). Nonetheless, this body of literature mainly focuses on the trends, patterns, new techniques, and potential risk factors related to cyber fraud and victimization (e.g., Lin et al., 2023; Pratt et al., 2010). Public perceptions of cyber fraud remain under-researched. Given the wide occurrence and severity of cyber fraud victimization in the general population, studying the fear of cyber fraud will assist in the development of more effective policies and practices to enhance public alert and defensiveness against this type of crime, as well as encourage help-seeking.

The limited existing studies on perceptions of cyber fraud (Choi et al., 2021; Virtanen, 2017; Yu, 2014) drew primarily on samples from developed nations (e.g., the United States and Europe), with little attention to developing countries despite the rapidly growing number of Internet users and cybercrime victims in these societies. This study focuses on China, which has witnessed a rapid increase in cyber fraud since 2017 and has passed a few legislations to deal with cyber fraud (van Wyk, 2022). The high prevalence and large sums of financial losses from cyber fraud have also seriously affected the public's sense of security and satisfaction in China (Sohu, 2021). Studying Chinese perceptions of and experiences with cyber fraud extends the existing literature to non-Western, developing countries.

Literature review

Cyber fraud in China

With advances in modern communication technologies (e.g., smartphones, social media, and video chatting) and mobile payment technology, cyber fraud emerged as the most common type of technology-based fraud due to its low costs and high returns (Sjouwerman, 2019); it has been running rampant around the world in the past two decades (TNW, 2022). As a country with a rapidly developing cyberspace

and home to the world's largest population of Internet users, China has not been immune to cyber fraud. In some provinces of China, cyber fraud accounts for more than 50% of all criminal cases (Liu, 2022). Almost a million (927,000) cases of cyber fraud were reported in 2020, amounting to roughly 5.44 billion US dollars in financial losses (Wang, 2021). Cross-border cyber fraud operations have become increasingly common, with many organized criminal groups recruiting vulnerable young Chinese adults and trafficking them to Myanmar and Cambodia to join their fraud enterprise targeting victims in China (CAICT, 2020; Qu & Cheng, 2024; Wang & Yang, 2023). In 2023, the Chinese authority cleared 437,000 cyber fraud cases and apprehended a large number of transnational cyber fraud offenders through international collaboration in law enforcement. Since August 2023, the incidence of cyber fraud has continuously declined, indicating the effectiveness of this large-scale international operation (China News Network, 2024). However, cyber fraud remains prevalent in China and faces many existing and emerging challenges (China Academy of Information and Communication Technology, 2023).

Unlike the US, where victims were chiefly adults 40 and older (IC3, 2024), victims of cyber fraud in China are primarily from the youthful population, with over 60% of those recently defrauded born after 1990 (CAICT, 2020). This is similar to cyber fraud in the United Kingdom, where those aged 20 to 39 were the primary target for victimization (The National Fraud Intelligence Bureau, 2022). The majority of young victims of cyber fraud in China may reflect the rapid shifting of the pattern of routine activities driven mainly by young Internet users. The younger population uses the Internet more frequently (e.g., chatting, online shopping, and watching short videos). However, they often lack vigilance when monitoring and disclosing personal information, both online and offline (Higgins et al., 2008), increasing the risk of being exposed to potential offenders on the Internet. The offenders have developed strategies that cater to the needs of the young victim, such as brush-targeting females who are eager for part-time jobs and phishing via erotic video chats targeting men who are desperate for a romantic or sexual partner (Xu, 2022).

Cyber fraud caused financial losses and psychological trauma (such as despair and depression) to not only the victims but also impaired public trust in the government's capability to protect public safety. As some victims were afraid of being blamed and shamed for their victimization experience (e.g., deemed as gullible, negligent, or even greedy), they were reluctant to report the crime to the police (Li et al., 2016; Wang, 2020). As a result, the genuine number of cyber fraud cases is likely much higher than that from official reports.

Research has also uncovered the offending patterns and criminal organizational processes of cyber fraud in China (e.g., Chen, 2021; Jian et al., 2017; Xu, 2022; Xu & Xu, 2021). Fraudsters typically rely on "scam scripts" to commit fraud, and they often update their scam scripts to match ongoing "hot topics" in public discourses to enhance their credibility and attract the victims' attention (Tang & Zhao, 2022; Xie & Chen, 2022). Besides scam scripts, specialized "conversation skills" are also deployed. For instance, based on content analysis of 20 fraudulent conversations intercepted by law enforcement, Chen (2021, p. 1065) found that fraudsters often used "such conversational skills in a threatening tone as repetition, interruption, higher pitch, louder speech and so on to trigger victims' psychological panic."

Fraudsters are also well-organized, working together to play different roles in the schemes to win the victims' trust (Li & Gong, 2018). After gaining trust, the fraudsters tend to threaten or coax the victims to transfer money to a fraudulent account.

Recent studies have investigated cyber fraud victimization among Chinese populations. Using self-reported scams posted on Baidu Tieba, equivalent to Craigslist, Lee (2021) found that fraud victims are normally young, active social media users and more suitable targets of cybercrime. Other studies showed that loneliness and credulity are associated with higher vulnerability to fraud among the elderly population (Shao et al., 2019; Wen et al., 2022; Xing et al., 2020). Wang et al. (2021) researched organized criminal groups' usage of the online peer-to-peer lending market to extort money from university students. The authors' interviews with university students and critical informants revealed that students are suitable targets of cyber loan-sharking due to the lack of parental supervision and financial knowledge about private loans. Student victims expressed their concerns about debt collectors' physical violence against their family members and harassment against themselves by sending text messages and threatening to distribute compromising information, such as their indecent photos. Most recently, using the data collected from 1037 university students in China, Lin et al. (2023) found that some routine online activities could predict the risk of being targeted for cyber fraud. In contrast, target suitability, such as risky/deviant online behaviors and low self-control, can predict completed victimization.

Despite these relevant studies, public perceptions of cyber fraud in China, including fear of cyber fraud, remain largely under-explored. Fear of crime, including fear of cyber fraud, bears real-life significance. First, at the societal level, excessive public fear of crime may erode public trust in the government and criminal justice institutions (Lin, 2022), which is critical to social stability. Therefore, gauging the level of public fear may help indicate the appropriate public spending on cyber fraud prevention and intervention and, if necessary, help craft policymaking and public messaging campaigns to manage fear. At the individual level, fear is a double-edged sword. On the one hand, fear may translate into alertness and defensiveness against crime, as well as help-seeking behaviors, both of which are critical to cybercrime prevention and harm reduction. On the other hand, persisting fear is correlated with anxiety and poor mental health outcomes (Beckers et al., 2023; Pearson & Breetzke, 2014). Therefore, there is a genuine need to understand the fear of cyber fraud to galvanize the public and the government's willingness to combat cyber fraud while managing the adverse effects of fear.

Fear of Crime and theoretical perspectives explaining fear of Crime

Research on fear of crime originated in the United States in the mid-1960s (Doran & Burgess, 2012; Farrall et al., 2000), subsequently evolving into an important research domain in criminology, garnering significant scholarly attention globally, notably from the United Kingdom (e.g., Brunton-Smith et al., 2014; Hale, 1996), Australia (e.g., Borooah & Carcach, 1997), China (Wu et al., 2019; Zhang et al., 2009), and various other nations. Despite the extensive body of literature in this

field, significant debate persists regarding the conceptualization and measurement of fear of crime. One widely endorsed definition characterizes fear of crime as "negative emotional reactions generated by crime or symbols associated with crime" (Ferraro & Grange, 1987, p. 73). This definition focuses on the *emotional* response to the possibility of victimization (Ferraro, 1995; Ferraro & Grange, 1987; Rountree & Land, 1996). While some studies (Skogan, 1999) found that crime fear and the cognitive perception of the risk of victimization are related, others (Mesch, 2000) found them to be distinct concepts. The former is focused on the emotional reaction, and the latter is more on the rational calculation of risk. Three theoretical perspectives have been developed in the existing literature to explain fear of crime. These are vulnerability to victimization, community disorder, and institutional confidence (Lin, 2022; Wu & Wareham, 2017).

Vulnerability to victimization

Researchers have long argued that the physical risks of victimization, which seem intuitive in explaining the fear of victimization, may not be in and of itself a robust predictor of fear, as young males who are at the greatest risk of criminal victimization were found to exhibit the least degrees of fear (Goodey, 1994; Stanko & Hobdell, 1993; Walklate, 1994). Recent research on delinquent youth has unveiled more complicated mechanisms between actual risks, perceptions of risks, and the fear of victimization. While proximity and exposure to motivated offenders, such as being associated with delinquent peers, greatly increased one's actual and perceived risk of being victimized, Gialopsos (2011) found that it did not predict a higher level of fear of victimization. Melde and Esbensen (2009) even reported a greater decrease in school-based fear of victimization among youth who became involved in a more delinquent lifestyle than more prosocial youth, although the greater perceived risk of victimization did predict a higher level of fear.

Related to, but distinct from, the risk of victimization is an individual's vulnerability to victimization, which refers to the inability to defend oneself from the risks and the severity of the consequence (e.g., death or severe injury) (Killias, 1990). Research has consistently shown that women, individuals with low socioeconomic status, individuals with disabilities, and the elderly exhibit higher levels of fear of crime due to their vulnerability to criminal victimization (Clemente & Kleiman, 1977; Hale, 1996; Killias & Clerici, 2000; Skogan & Michael, 1981).

Self-control Vulnerability also includes psychological vulnerability, such as low self-control. Low self-control is characterized by impulsivity, preference for simple tasks, risk-taking, preference for physical activities, self-centeredness, and volatile temper (Gottfredson & Hirschi, 1990). In addition to explaining criminal behavior, low self-control has been found to explain psychological vulnerability to victimization and fear of crime. Considerable studies revealed that as a personal trait, low self-control was associated with elevated risks of victimization (Holtfreter et al., 2008; Qu et al., 2021; Schreck, 1999; Schreck et al., 2002, 2006; Stewart et al., 2004), yet its impact on fear and perceived risk of crime is mixed. For example, utilizing survey data from 573 adult Internet users in Florida, Reisig et al. (2009) found

that financial impulsivity, conceptualized as a component of low self-control, had a significant positive effect on the perceived risk of crime, with impulsive respondents judging higher levels of risk. Meanwhile, Higgins and coauthors' (Higgins et al., 2008) study found that individuals with high self-control were more fearful of crime.

Deviant lifestyle Lifestyle exposure theory assumes that individuals who are exposed to high-risk "time, places, and people" are more vulnerable to potential offenders and are thus at a higher risk level of victimization (Hindelang et al., 1978). According to this theory, engagement in deviant behaviors places individuals in risky situations and increases their likelihood of being victimized (Nofziger, 2009; Turanovic et al., 2015), which, in turn, may raise their fear of crime. Empirical evidence, nonetheless, remains mixed. Melde et al.' (2016) study of gang members showed that while gang membership predicted an increased risk of victimization and greater perceived risk, it corresponded to lower levels of emotional fear of crime. Based on data from the 2008 Korean Crime Victimization Survey, Choi et al. (2021) showed that online deviance (i.e., illegal downloading of pirated software) had no significant effect on fear of identity theft.

Social ties Social ties, as an important indicator of individuals' social vulnerability, were found to increase the probability that individuals used informal means to control disruptive social activity, reducing their odds of victimization and fear of crime (Gibson et al., 2002). Similarly, conceptualizing these social ties as a type of social integration, Gibson et al. (2002) analyzed survey data collected in three US cities and found that social integration had an indirect negative effect on fear of crime through the increased perception of the collective efficacy in the neighborhood. Zhang et al. (2009) conceptualized social ties in the Chinese context as *guanxi*, a distinctive source of social capital and social resilience in China. Based on survey data collected from Tianjin, China, Zhang and colleagues found that social ties were a significant negative predictor of fear of crime, with those who had extensive neighborhood *guanxi* significantly less likely to exhibit fear of crime than their counterparts with fewer *guanxi*.

Vicarious victimization experience Another aspect of the vulnerability thesis considers the impact of prior victimization on fear. Research has repeatedly shown that prior experiences of victimization or witnessing victimization (i.e., vicarious victimization) predict elevated levels of fear (Lee et al., 2020; Nalla et al., 2011). Other than directly witnessing violence, vicarious victimization can also occur through learning about victimization experiences from other people and the consumption of crime related news media (Kohm et al., 2012), both of which may reinforce individuals' sense of vulnerability to crime and give rise to the expectation that victimization is likely and beyond individual control (Romer et al., 2003). For example, based on survey data of 2300 Philadelphia residents, Romer et al. (2003) revealed that viewing local television news increased their fear of crime. Williams and Dickinson (1993) found that those who read newspapers covering more vivid crime incidents had higher levels of fear. Wu and associates (Wu et al., 2019), based on a sample

from Shanghai, China, demonstrated that the type of media mattered in shaping people's fear of crime, with those consuming newspapers and radio reports of news having lower levels of fear of crime and those consuming TV and Internet news reporting higher levels of fear.

Community disorder

Another theoretical perspective that informs scholarship on fear of crime is grounded in neighborhood crime and disorder conditions. It is argued that neighborhoods with higher levels of crime and disorder, both actual and perceived, generate greater residents' fear of crime (Zhao et al., 2015). Findings from Lai et al.' (2016) study revealed that perception of the seriousness of crime conditions in the community, operationalized as the subjective assessment of the number of crime problems in the neighborhood, was the most robust and strongest predictor of fear. Wyant (2008) found that those who perceived more crime in the neighborhood were more fearful of crime. Similarly, Smith and Hill (1991) analyzed a large sample of 3109 cases and demonstrated that the perceived seriousness of crime conditions in their neighborhoods was positively correlated with fear of crime. In addition to traditional contact crime, research has also shown a connection between disorder in cyberspace and fear of cybercrime. For instance, Yu (2014) found that the perceived seriousness of crime conditions was positively linked to fear of online scams and computer viruses.

Institutional confidence

Crime is a social problem and combating crime and maintaining public safety fall mainly on the shoulders of the police. Therefore, the police are expected to play a critical role in the management of crime fear among citizens (Li et al., 2022; Lin, 2022). Previous studies have explored the effects of attitudes toward the police on fear of crime across different countries, but the results are mixed. A few studies showed that satisfaction with police performance, fairness, and integrity has a significant negative association with fear of crime (Lai et al., 2016; Li et al., 2022; Scheider et al., 2003). However, other research failed to find any connection between satisfaction with the police and fear of crime (e.g., Adu-Mireku, 2002; Scheider et al., 2003).

The current study

Despite existing research investigating fear of crime in cyberspace (e.g., Brunton-Smith, 2017; Choi et al., 2021; Higgins et al., 2008; Roberts et al., 2013; Virtanen, 2017; Van Wilsem, 2013; Yu, 2014), none of these studies examined the fear of cyber fraud in mainland China, a country with prevalent cyber fraud victimization and large amounts of financial losses due to cyber fraud. In addition to its prevalence and severity, cyber fraud is a prominent issue in China because even though traditional contact crimes like theft, robbery, and assault show a decreasing trend, new

types of crimes, represented by cyber fraud, continue to occur at high rates (China Economic Net, 2020). In particular, the current study explores the fear of cyber fraud among the youthful population in China. This is an important demographic group, given its disproportionately high rate of cyber fraud victimization (CAICT, 2020). In addition to fear, the current study also examines the perceived risk of cyber fraud. While some studies (Skogan, 1999) found that crime fear and the cognitive perception of the risk of victimization are related, others (Mesch, 2000) found them to be distinct concepts. Empirical research on both traditional crimes and cybercrime has not consistently documented the patterns of the factors that influence fear as opposed to perceived risk (Gialopsos, 2011; Melde & Esbensen, 2009), prompting further inquiry.

Based on the above literature review, the current study tests the following hypotheses based on a sample of 1065 university students from China:

H_1: Individuals who are physically (e.g., women), socially (e.g., low socioeconomic status), or psychologically (e.g., low self-control and vicarious victimization) vulnerable are more likely to report fear of cyber fraud.

H_2: Individuals who consider cyber fraud to be more serious in the community are more likely to report fear of cyber fraud.

H_3: Individuals who report less satisfaction with the police are more likely to report fear of cyber fraud.

H_4: Perceived risk of cyber fraud is predicted by the same factors as fear of cyber fraud.

Methodology

Data

Survey data used in this study were collected from university students at two universities in Guizhou Province of China in December 2021. This survey went through a strict review process and was approved by Guizhou University of Finance and Economics. Guizhou is located in southwest China, covering an area of 176,167 km^2 with a population of 34.7 million. As one of the less economically developed provinces, Guizhou has made significant progress in its digital economy in recent years (China Daily, 2022). Nevertheless, Guizhou has not been safe from cyber fraud predation. For instance, in December 2015, the treasurer of the Duyun City Construction Bureau of Economic Development Zone was victimized by cyber fraud, resulting in losses of 117 million Chinese yuan (roughly 18 million US dollars). This case represents the highest amount of financial loss in a single fraud in modern Chinese history (Wang, 2020).

We used a purposive and convenience sampling strategy to target the university student population while being mindful of attaining diversity in our sample from two universities. The first university is a comprehensive university jointly built by China's Ministry of Education and the Guizhou government, recruiting students nationwide and enrolling over 34,000 undergraduate students and over 13,000 graduate students. The second university is a regional higher institution with 16,000

undergraduate students and 2800 graduate students, mostly from within Guizhou Province.

Drawing on the existing literature (e.g., Abdulai, 2020; Hsu & Wei, 2017; Wei et al., 2019), we developed a survey questionnaire for this study. Before officially administering the survey, we conducted a pilot test by administering the survey online to 159 undergraduate students at the second university. Based on the answers and feedback from the respondents, we revised the survey questions to make them easier to comprehend. To administer the survey, we chose 7 undergraduate classes at the first university and 12 undergraduate and graduate classes at the second university. These classes were selected mainly because the researchers had personal connections with the instructors of these classes, who agreed to recruit potential participants from students in their classes. During the survey distribution time, the researchers visited the classrooms, explained the purpose of this survey, informed the students of the voluntary and anonymous nature of their participation, and invited all students to participate. While the students filled out the survey, the instructors were asked by the researchers to leave the classroom.

A total of 1128 students completed this survey, while 5 students refused to participate. Ten surveys contained invalid responses (massive missing data) and were discarded, rendering a sample size of 1113 and an effective response rate of 98.7%, consistent with the high return rate of delinquency and victimization studies based on the sample of students in China (Qu, Wu, & Chen, 2021). After selecting the relevant variables and removing missing cases of these variables, the final sample for analysis stood at 1065. As is presented in Table 1, the average age of this sample was 20.92 (SD = 1.94). About two-thirds (66.7%) of this sample were male. An

Table 1 Descriptive Statistics of All Variables ($N = 1065$)

Variables	Mean	SD	Min	Max
Dependent variables				
Fear of cyber fraud victimization	.50	.50	0	1
Perceived risk of cyber fraud	.10	.30	0	1
Vulnerability to victimization				
Low self-control	8.90	2.90	4	20
Illegally downloading music or movies	2.48	1.22	1	5
Downloading "cracked" software	2.07	1.07	1	5
Downloading and using Wi-Fi cracking apps	2.12	1.17	1	5
Social ties	7.61	1.71	2	10
Vicarious victimization experiences	10.37	2.40	3	15
Male	0.33	0.47	0	1
Age	20.92	1.94	17	40
Perceived family economic status	1.95	.73	1	4
Community disorder				
Perceived seriousness of cyber fraud	3.83	1.02	1	5
Institutional confidence				
Satisfaction with police	10.67	2.93	3	15

overwhelming majority (86.3%) of this sample were undergraduate students and 13.7% were graduate students. 23.8% of the respondents were freshmen (1st year) and sophomores (2nd year), 62.5% were juniors (3rd year) and seniors (4th year), and 13.7% were graduate students. About a fourth (23.3%) of this sample majored in Science, Engineering, or Medicine, 76.6% majored in Liberal Arts (Philosophy, Law, Literature, History, Sociology), and only .1% majored in the Arts (Music, Sports, Art).

Measures

Dependent variables

The first dependent variable, fear of cyber fraud, was measured by one survey item. The respondents were asked, "How worried are you about being a victim of cyber fraud?". In order to obtain more accurate self-reports, the period for this question was designated as the past 3 months (Jackson, 2011). This measure has been used in previous fear-of-crime research (Abdulai, 2020; Roberts et al., 2013). Response categories ranged from "very worried" to "not at all worried". The distribution of responses was as follows: very worried (19.9%, $n=220$), somewhat worried (30.2%, $n=333$), neutral (9.6%, $n=106$), not very worried (27.0%, $n=298$), not at all worried (13.2%, $n=146$). The preliminary analysis results showed that the assumption of the parallel lines for ordered logistic regression was violated. As a result, we chose to dichotomize the variable and perform binary logistic regressions instead. Therefore, we created a dummy variable with 1 representing the categories of "very worried" and "somewhat worried" and 0 representing the remaining categories.

The second dependent variable, perceived risk of cyber fraud, was measured by asking the respondents to estimate the likelihood of their being a victim of cyber fraud in the next 12 months. Previous research has commonly used a 12-month timeframe to measure victimization experiences and risk perceptions of victimization (e.g., Reyns, 2013), and we have referenced this established approach. The response categories featured a 5-point Likert scale, ranging from 1 (very likely) to 5 (very unlikely). The distribution of responses was as follows: very likely (2.4%, $n=27$), somewhat likely (7.6%, $n=84$), neutral (39.6%, $n=437$), somewhat unlikely (30.5%, $n=337$), very unlikely (19.8%, $n=219$). The preliminary analysis showed that the assumption of the parallel lines for ordered logistic regression was violated; thus, we also dichotomized this variable with 1 represented "very likely" and "somewhat likely," and 0 represented otherwise.

Independent variables

Vulnerability to victimization The vulnerability to victimization includes several variables. Self-control was measured using four items derived from Tangney et al.' (2004) Brief Self-Control Scale. The respondents were asked the extent to which they agreed to the following statements: (1) "Sometimes I will take a risk just for the fun of it", (2) "Excitement and adventure are more important to me than security",

(3) "I often act on the spur of the moment without stopping to think", (4) "I often do whatever brings me pleasure here and now, even at the cost of some distant goal". Response categories ranged from "strongly disagree" (=1) to "strongly agree" (=5). Exploratory factor analysis showed that the four items loaded on a common factor exhibited acceptable inter-item reliability (Cronbach's alpha=0.68). We summed the responses to these questions to create a measure of low self-control, with high scores representing low self-control.

The measure of online deviance consists of three items asking the respondents how often they engaged in the following activities in the past 3 months, including illegally downloading music or movies, downloading "cracked" software, and downloading and using Wi-Fi cracking apps. Response categories varied from "never" (=1) to "all the time" (=5). The previous online delinquency and victimization research used a similar measurement (Paek & Nalla, 2015).

Social ties were measured by asking the respondents how much they agreed that they: "often meet or talk with family or friends" and "often chat and hang out with classmates/ friends". These two items were measured on a scale of 1 (= strongly disagree) to 5 (=strongly agree). We combined these items into an additive scale, with higher scores representing stronger social ties. These items exhibited acceptable interitem reliability (Cronbach's alpha=0.66).

To measure vicarious victimization experience, respondents were asked to answer how often they had heard about cyber fraud cases from the following sources: TV/ newspaper, social media, and classmates/friends and family. Response categories varied from "never" (=1) to "always" (=5). Exploratory factor analysis showed that the three items loaded onto a common factor and exhibited acceptable inter-item reliability (Cronbach's alpha=0.66). A composite measure was created by summing the three items.

Three sociodemographic variables, often used as indicators of physical and social vulnerability, were included in the multivariate analyses. Respondents' age was measured in years at the time of this survey. Gender was measured as a binary variable, with 1 being male and 0 being female. The response options for perceived family economic status include 1=not so great, 2=getting by, 3=about average, and 4=above average.

Community disorder The perceived seriousness of cyber fraud was measured by asking the respondents, "In your view, over the past three years, cyber fraud has…" The response categories included "substantially decreased" (=1), "somewhat decreased" (=2), "remained unchanged" (=3), "somewhat increased" (=4), and "substantially increased" (=5).

Institutional confidence Satisfaction with police effectiveness was an index of three items asking the respondents how satisfied they were with the police in preventing cyber fraud, solving cyber fraud cases, and recovering the financial losses of the victim. Response categories ranged from "very dissatisfied" (=1) to "very satisfied" (=5). Exploratory factor analysis showed that three items were loaded on a factor and had excellent inter-item reliability (Cronbach's alpha=0.90). We summed up

these 3 items to create an additive scale with a higher score representing a higher level of satisfaction with the police.

Analytic strategy

All statistical analyses were conducted using SPSS 27.0. First, descriptive statistics were performed and presented. Second, given that the two dependent variables (i.e., fear of cyber fraud and perceived risk of cyber fraud) are dichotomous after transformation, binary logistic regression analyses were selected as the multivariate analytic strategy for this study. The first regression model was performed to identify the correlates of fear of cyber fraud. The second regression model was run to explore the factors influencing an individual's perceived risk of cyber fraud.

Results

As displayed in Table 1, 50% of the respondents reported they felt fearful of being a victim of cyber fraud during the past 3 months, whereas 10% of the respondents expressed that they were likely to experience cyber fraud victimization in the next 12 months.

Table 2 presents the results from logistic regressions. The Omnibus Tests of Model Coefficients showed that Model 1 exhibited excellent model fit (Model Chi-Squared = 46.13, $p < .000$). Three variables predicted fear of cyber fraud victimization, including high self-control, downloading and using Wi-Fi cracking apps, and being male. Lower levels of self-control were associated with a lower likelihood of reporting fear of cyber fraud (OR = .95). Downloading and using Wi-Fi cracking software was connected to higher odds of fear of cyber fraud (OR = 1.22). Lastly, compared with male respondents, female respondents were more likely to report a greater fear of cyber fraud (OR = .59).

Moving on to Model 2, which also showed excellent model fit (Model Chi-Squared = 48.81, $p < .000$), four variables were found to be significantly linked to the perceived risk of cyber fraud victimization. Specifically, individuals exposed to more cyber fraud representations in the media or through the experience of family/friends reported a higher perceived risk of cyber fraud victimization (OR = 1.11). Compared with female respondents, male respondents were more likely to report being at risk of cyber fraud victimization (OR = 1.99). The perceived seriousness of the cyber fraud variable was significantly predictive of greater perceived risks of cyber fraud victimization (OR = 1.41). Finally, respondents who were satisfied with police effectiveness (OR = .90) were less likely to perceive a greater risk of cyber fraud victimization.

Discussion

Drawing upon survey data from Chinese university students, this study explores the prevalence and correlates of fear and perceived risk of cyber fraud. Despite its exploratory nature, the findings derived from this study have made several

Table 2 Binary Logistic Regression on Fear of Cyber Fraud Victimization and Perceived Risk of Cyber Fraud ($N = 1065$)

Variables	Fear of cyber fraud victimization		Perceived risk of cyber fraud	
	OR	SE	OR	SE
Vulnerability to victimization				
Low self-control	.95*	.02	1.03	.04
Illegally downloading music or movies	.95	.06	.93	.09
Downloading "cracked" software	.93	.07	1.22	.11
Downloading and using Wi-Fi cracking apps	1.22***	.06	1.07	.09
Social ties	.93	.04	1.01	.06
Vicarious victimization experiences	1.05	.03	1.11*	.04
Male	.59***	.14	1.99**	.22
Age	1.00	.03	.95	.06
Family economic status	.94	.09	.75	.15
Community disorder				
Perceived seriousness of cyber fraud	1.04	.06	1.41**	.12
Institutional confidence				
Satisfaction with police	.99	.02	.90**	.04
Model Chi-Squared	46.13***		48.81***	
Nagelkerke R^2	.06		.09	

*$p < .05$; **$p < .01$; ***$p < .001$

contributions to a better understanding of the fear and perceived risk of cyber fraud, especially in the Chinese context. First of all, the current study found that a high proportion of the Chinese university students surveyed, about half of them, reported fear of cyber fraud over the last three months. However, they perceived a low risk of future victimization, with only 10% of the respondents envisioning the possibility of being defrauded in the next 12 months. It is plausible that the pervasive occurrence and significant financial repercussions of cyber fraud have instigated apprehension among Chinese university students, yet other factors may have explained their perceived invulnerability to victimization, justifying the multivariate analyses that followed.

In the multivariate analyses, the fear of cyber fraud was linked to high self-control and downloading and using Wi-Fi cracking apps, whereas the perceived risk of it was related to vicarious victimization experience, perceived seriousness of cyber fraud in the community, and satisfaction with the police. Although gender is a significant predictor for both fear and perceived risk, the directions of the correlations are different, with males showing less fear but a higher perceived risk than their female counterparts. These findings warrant further unpacking.

Consistent with our hypothesis (H_1), we found that some physical, social, and psychological vulnerabilities to victimization (i.e., high self-control, risky online behaviors, and being female) were associated with higher odds of expressing fear of cyber fraud. First, while the positive correlation between high self-control and crime

fear is supported by some studies (e.g., Guedes et al., 2023; Higgins et al., 2008), it stands in contradiction with findings from others (e.g., Reisig et al., 2009; Williams, 2010). In the context of the current study, it is possible that individuals with high self-control tend to exhibit heightened vigilance and caution while navigating the digital realm. This heightened awareness and prudence may translate into greater anxiety and fear. This fear, along with other cognitive processes, may, in turn lead to more defensive behaviors against actual victimization and thus reduce the odds of actual victimization. Further research is necessary to disentangle the relationship between self-control, crime fear, defensive behaviors, and the odds of actual cyber victimization.

Second, this study found that students who were involved in online deviance (in the form of downloading and using Wi-Fi-cracking apps) felt more fearful about cyber fraud. Previous studies on gang members (Melde et al., 2016) and elementary and secondary school students (Gialopsos, 2011; Melde & Esbensen, 2009) in the US demonstrated that those in close proximity to crime via delinquent peer association did not exhibit a greater fear of crime and some of them experienced a lower level of fear. Despite the importance of delinquent peers in shaping fear of crime, our data do not contain information on whether online deviance was conducted in a group or individual setting, preventing us from testing the linkage between deviant peers and fear of crime. More studies should be devoted to further analyzing this possible relationship.

There was not sufficient evidence, however, to accept (cyber) community disorder (H_2) and institutional confidence (H_3) as predictors of cyber fraud fear. On the other hand, community disorder and institutional confidence, alongside vicarious victimization, were found to significantly predict the perceived risk of fraud. This discovery supports the rejection of H_4 and resonates with findings from previous research advocating for the distinct evaluation of fear and perceived risk of crime, along with the independent examination of their associated factors (Ferraro, 1995; Hinkle, 2015; Li et al., 2022). It seems that the emotional expressions of fear, worry, and concern about victimization in cyberspace are more closely linked to individual-level vulnerabilities. In contrast, the more cognitive and calculative understanding of risk is more significantly influenced by community and institutional factors.

Finally, in line with findings from previous studies (e.g., Goodey, 1994; Li et al., 2022; Stanko & Hobdell, 1993; Walklate, 1994), gender is a significant predictor of fear of and perceived risk of cyber fraud. Compared with female respondents, male students were less likely to report fear of cyber fraud, even though they were more likely to report being at risk of cyber fraud victimization. The discrepancy between risk assessment and fear may have much to do with an internalized masculinity ideology (Lane & Fox, 2012; Li et al., 2022). At a high risk of being victimized, males often report a lower level of fear of crime under the influence of norms of hegemonic masculinity that discourage the expression of emotions, including fear (Li et al., 2022).

Admittedly, this study has several limitations. First, although the sample size was large enough to serve the purpose of this study, they were drawn from only two universities in Guizhou province, making the findings ungeneralizable to the entire

Chinese population or the university student population in China. Future research should consider utilizing samples from more universities in different regions to study the phenomenon of cyber fraud. Second, with a cross-sectional design, this study was not meant for rigorous causal inference. Therefore, caution should be taken when interpreting the results of the study. As such, future research should utilize a longitudinal research design to better ensure the internal validity of the relationships examined here. Third, although this study drew upon three groups of variables to explore the correlates of fear and perceived risk, there may be other important variables that we did not include, such as prior personal victimization experience with cyber fraud and routine online/telecommunication activities. Future studies should explore these variables as potential explanatory factors.

A couple of policy implications deserve discussion. Given the high levels of fear against low levels of perceived risks documented, the government and the university should promote public and student education on cyber security and take measures to reduce young people's risky online activities, such as illegal downloading and using Wi-Fi cracking apps. For instance, the significant effect of media on producing fear points to the utility of promoting public awareness of cyber fraud. Although public institutions and community organizations should be careful not to use an overly inflated fear tactic, more media promotion of cyber fraud may still be effective in galvanizing individuals into being more vigilant and defensive against this type of crime. Of course, excessive fear can exacerbate anxieties and contribute to other mental health issues and should, therefore, be well-controlled in awareness-raising media campaigns.

Conclusion

Although fear of crime has been an extensively researched topic in recent decades, the literature has been predominantly focused on fear of "street crimes." Fear of cybercrime is a relatively underexamined topic, and even more so is fear of cyber fraud specifically. Based on survey data from China, this study explores the prevalence of fear and perceived risk of cyber fraud and its correlates among Chinese university students. It shows that fear and perceived risk are influenced by different domains of risk factors. Specifically, higher self-control, online deviant lifestyle, and gender explain a greater level of fear, while vicarious victimization experiences, perceived crime seriousness, satisfaction with the police, and gender account for the perceived risk of crime. These findings point to the utility of promoting public awareness of cyber fraud and reducing public online deviant activities.

Data availability It is not possible to share research data publicly as research participants did not consent to data being shared with those outside the research group.

Declarations

Ethical approval This study underwent a research ethics review process and was approved by Guizhou University of Finance and Economics.

Informed consent Research participants were informed of the purpose and design of the study and consent was acquired from the research participants.

Competing interests N/A

References

Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology, 14*(1), 157–174.

Adu-Mireku, S. (2002). Fear of crime among residents of three communities in Accra, Ghana. *International Journal of Comparative Sociology, 43*(2), 153–168.

Australian Government, Australian Institute of Criminology (AIC). (2023). Cybercrime in Australian 2023. Retrieved on April 3, 2024, from https://www.aic.gov.au/sites/default/files/2023-06/sr43_cybercrime_in_australia_2023.pdf

Beckers, T., Hermans, D., Lange, I., Craske, M. G., Vervliet, B., & Duits, P. (2023). Understanding clinical fear and anxiety through the lens of human fear conditioning. *Nature Reviews Psychology, 2*, 233–245.

Borooah, V. K., & Carcach, C. A. (1997). Crime and fear: Evidence from Australia. *The British Journal of Criminology, 37*(4), 635–657.

Brunton-Smith, I. (2017). Fear 2.0: Worry about cybercrime in England and Wales. In M. Lee & G. Mythen (Eds.), *The Routledge international handbook on fear of Crime* (pp. 93–105). Routledge.

Brunton-Smith, I., Jackson, J., & Sutherland, A. (2014). Bridging structure and perception: On the neighbourhood ecology of beliefs and worries about violent crime. *British Journal of Criminology, 54*(4), 503–526.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims* (1st ed.). Routledge https://doi-org.ezproxy.lib.uts.edu.au/10.4324/9781315679877

Chen, J. (2021). "You are in trouble!": A discursive psychological analysis of threatening language in Chinese cellphone fraud interactions. *International Journal of Semiotics Law, 34*, 1065–1092.

China Academy of Information and Communications Technology (CAICT). (2020). *Research report on cyber fraud intervention in evolving contexts*. Retrieved on March 25, 2022, from http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201218393889946295.pdf

China Academy of Information and Communications Technology (CAICT). (2023). *White paper on preventing and governing cyber fraud in the Information and Communication Industry (2023)*. Retrieved on April 3, 2024, from http://www.twwtn.com/afinance/202311/53264.html

China Economic Net. (2020). *Ministry of Public Security has achieved interim results in cracking down on and governing cyber fraud*. Retrieved on April 3, 2024, from https://www.sohu.com/a/410231617_120702

China News Network. (2024). *Ministry of Public Security: 437,000 telecom and online fraud cases cracked in 2023*. Retrieved on April 3, 2024, from https://m.gmw.cn/2024-01/09/content_1303625437.htm

Choi, J., Kruis, N. E., & Choo, K. S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice, 37*(3), 1–21.

Clemente, F., & Kleiman, M. B. (1977). Fear of crime in the United States: A multivariate analysis. *Social Forces, 56*(2), 519–531.

China Daily, 2022. *Guizhou moving up economic rankings*. Retrieved on March 25, 2022, from https://www.chinadaily.com.cn/a/202203/01/WS621d7c6ba310cdd39bc897a4.html

Doran, B. J., & Burgess, M. B. (2012). *Putting fear of crime on the map*. Springer.

Farrall, S., Bannister, J., Ditton, J., & Gilchrist, E. (2000). Social psychology and the fear of crime. *British Journal of Criminology, 40*(3), 399–413.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. SUNY Press.

Ferraro, K. F., & Grange, R. L. (1987). The measurement of fear of crime. *Sociological Inquiry, 57*(1), 70–97.

Gialopsos, B. A. M. S. (2011). *For whom the school bell tolls: Explaining students' fear of crime and perceptions of risk*. Theses and Dissertations https://www.proquest.com/docview/1010273093

Gibson, C. L., Zhao, J., Lovrich, N. P., & Gaffney, M. J. (2002). Social integration, individual perceptions of collective efficacy, and fear of crime in three cities. *Justice Quarterly, 19*(3), 537–564.

Goodey, J. (1994). Fear of crime: What can children tell us? *International Review of Victimology, 3*(3), 195–210.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Guedes, I. S., Santos, M., Santos, G., Gomes, C., & Neves, A. (2023). Does fear of crime moderate the relationship between low self-control and victimization? An empirical study. *European Journal on Criminal Policy and Research.*, 1–20. https://doi.org/10.1007/s10610-023-09538-w[4

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

Higgins, G. E., Ricketts, M. L., & Vegh, D. T. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice, 33*(2), 223–233.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Hinkle, J. C. (2015). Emotional fear of crime vs. perceived safety and risk: Implications for measuring "fear" and testing the broken windows thesis. *American Journal of Criminal Justice, 40*(1), 147–168.

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

Hsu, Y. C., & Wei, R. (2017). Examining predictors and mediators of vulnerability to telecommunications fraud among senior citizens in Taiwan. In *14th ITS Asia-Pacific regional conference, Kyoto 2017: Mapping ICT into transformation for the next information society*. Telecommunications Society (ITS).

Internet Crime Complaint Center (IC3). (2024). Internet crime reeport 2023. In *Federal Bureau of Investigation* Retrieved on 2 April 2024, from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Jackson, J. (2011). Revisiting risk sensitivity in the fear of Crime. *Journal of Research in Crime and Delinquency, 48*(4), 513–537. https://doi.org/10.1177/0022427810395146

Jian, J., Liu, X. X., & Chen, S. Q. (2017). Research on the operation mode of online transaction fraud. *Journal of People's Public Security University of China (Social Science Edition), 06*, 27–35.

Killias, M. (1990). Vulnerability: Towards a better understanding of a key variable in the genesis of fear of crime. *Violence and Victims, 5*(2), 97–108.

Killias, M., & Clerici, C. (2000). Different measures of vulnerability in their relation to different dimensions of fear of crime. *British Journal of Criminology, 40*(3), 437–450.

Kohm, S. A., Waid-Lindberg, C. A., Weinrath, M., Shelley, T. O., & Dobbs, R. R. (2012). The impact of media on fear of crime among university students: A cross-national comparison. *Canadian Journal of Criminology and Criminal Justice, 54*(1), 67–100.

Lai, Y.-L., Ren, L., & Greenleaf, R. (2016). Residence-based fear of crime: A routine activities approach. *International Journal of Offender Therapy and Comparative Criminology, 61*(9), 1011–1037.

Lane, J., & Fox, K. A. (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, C. (2021). Online fraud victimization in China: A case study of Baidu Tieba. *Victims & Offenders, 16*, 343–362.

Lee, H. D., Reyns, B. W., Kim, D., & Maher, C. (2020). Fear of crime out west: Determinants of fear of property and violent crime in five states. *International Journal of Offender Therapy and Comparative Criminology, 64*(12), 1299–1316.

Li, J., Yolanda, M. Y., Wong, G., & Ngan, R. (2016). Understanding and preventing financial fraud against older citizens in Chinese society: Results of a focus group study. *International Journal of Offender Therapy and Comparative Criminology, 60*(13), 1509–1531.

Li, L. F., & Gong, Y. (2018). Features of cyber-frauds and countermeasures for prevention and control: An analysis of nationwide cyber-fraud cases from 2014 to 2016. *Jingyue Journal, 1*, 78–90.

Li, J. C., Wong, G. T., Manning, M., & Yeung, D. Y. (2022). Financial fraud against older people in Hong Kong: Assessing and predicting the fear and perceived risk of victimization. *International Journal of Environmental Research and Public Health, 19*(3), 1233.

Lin, K. (2022). A cross-national multilevel analysis of fear of crime: Exploring the roles of institutional confidence and institutional performance. *Crime & Delinquency, 69*(12), 2437–2459.

Lin, K., Wu, Y. N., Sun, I. Y., & Qu, J. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice*, 17488958221146144. https://doi.org/10.1177/17488958221146144

Liu, P. L. (2022). Research on the practice of investigating and combating the Crime of telecom Network fraud. *Journal of Liaoning Police College, 04*, 12–16.

Melde, C., Berg, M. T., & Esbensen, F. A. (2016). Fear, social interactions, and violence mitigation. *Justice Quarterly, 33*(3), 481–509.

Melde, C., & Esbensen, F. A. (2009). The victim-offender overlap and fear of in-school victimization: A longitudinal examination of risk assessment models. *Crime & Delinquency, 55*(4), 499–525.

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

Nalla, M. K., Johnson, J. D., & Hayes-Smith, R. (2011). Prior victimization, region, and neighborhood effects on fear of crime in Mumbai, India. *Asian Journal of Criminology, 6*, 141–159.

Nofziger, S. (2009). Deviant lifestyles and violent victimization at school. *Journal of Interpersonal Violence, 24*(9), 1494–1517.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice, 43*(4), 626–642.

Pearson, A. L., & Breetzke, G. D. (2014). The association between the fear of crime, and mental and physical wellbeing in New Zealand. *Social Indicators Research, 119*(1), 281–294.

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.

Qu, J., & Cheng, H. (2024). *Policing telecommunication and cyber fraud: Perceptions and experiences of law enforcement officers in China* (pp. 1–23). Crime, Law and Social Change. https://doi.org/10.1007/s10611-024-10143-z

Qu, J., Wu, Y., & Chen, X. (2021). Self-control, risky lifestyles, and victimization among Chinese adolescents. *International Journal of Offender Therapy and Comparative Criminology*, 0306624X2110274. https://doi.org/10.1177/0306624x211027487

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization. *Criminal Justice and Behavior, 36*(4), 369–384.

Reyns, B. W. (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.

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

Romer, D., Jamieson, K. H., & Aday, S. (2003). Television news and the cultivation of fear of crime. *Journal of Communication, 53*(1), 88–104.

Rountree, P. W., & Land, K. C. (1996). Perceived risk versus fear of crime: Empirical evidence of conceptually distinct reactions in survey data. *Social Forces, 74*(4), 1353–1376.

Scheider, M. C., Rowell, T., & Bezdikian, V. (2003). The impact of citizen perceptions of community policing on fear of crime: Findings from twelve cities. *Police Quarterly, 6*(4), 363–386.

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

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

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

Shao, J., Du, W., Lin, T., Li, X., Li, J., & Lei, H. (2019). Credulity rather than general trust may increase vulnerability to fraud in older adults: A moderated mediation model. *Journal of Elder Abuse & Neglect, 31*, 146–162.

Sjouwerman, S. (2019). Seven reasons for cybercrime's meteoric growth. Forbes. Retrieved on March 25, 2022, from https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cyber crimes-meteoric-growth/?sh=2260a58e5fa2

Skogan, W. G. (1999). Measuring what matters. In *Proceedings from the policing research institute meetings* (pp. 37–88). Department of Justice.

Skogan, W. G., & Michael, G. M. (1981). *Coping with crime: Individual and neighborhood reactions*. Sage.

Smith, L., & Hill, G. (1991). Perceptions of crime seriousness and fear of crime. *Sociological Focus, 24*, 315–327.

Sohu. (2021). Coordinated governance and overcoming difficulties to resolutely curb the high incidence of new types of telecom and internet fraud crimes. Retrieved on April 3, 2024, from https://www.sohu.com/a/458129944_727157

Stanko, E. A., & Hobdell, K. (1993). Assault on men: Masculinity and male victimization. *The British Journal of Criminology, 33*(3), 400–415.

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

Tang, H., & Zhao, M. (2022). Quantitative characteristics and governance path of cyber fraud in China from the perspective of big data. *Journal of Guangxi Police College, 35*(2), 80–90.

Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of Personality, 72*(2), 271–324.

The National Fraud Intelligence Bureau (NFIB). (2022). *NFIB Fraud and Cyber Crime Dashboard - 13 months of data*. Retrieved on 10/1/2022 from https://colp.maps.arcgis.com/apps/dashboards/03341 50e430449cf8ac917e347897d46

TNW. (2022). *More than 5 billion people now use the internet: 63 percent of all the people on Earth are now online*. Retrieved on March 25, 2022, from https://thenextweb.com/news/more-than-5-billion-people-now-use-the-internet.

Turanovic, J. J., Reisig, M. D., & Pratt, T. C. (2015). Risky lifestyles, low self-control, and violent victimization across gendered pathways to crime. *Journal of Quantitative Criminology, 31*, 183–206.

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

van Wyk, B. (2022). China's cyber crime problem is growing. SupChina. Retrieved on March 5, 2023, from https://supchina.com/2022/08/23/chinas-cyber-crime-problem-is-growing/

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

Walklate, S. (1994). Can there be a progressive victimology? *International Review of Victimology, 3*(1–2), 1–15.

Wang, J. (2020). Investigation on the effectiveness of judicial control of cyber fraud. *Chinese Criminal Science, 01*, 160–176.

Wang L. (2021). Legislating against fraud: A "battle" against cyber fraud. *CCTV*. Retrieved on January 23, 2022, from https://news.cctv.com/2021/10/27/ARTINkh8kaKvZap9Igz5tSR8211027.shtml#:~:%20text=央视网消息

Wang, P., Su, M., & Wang, J. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in **China**. *British Journal of Criminology, 61*, 303–324.

Wang, Z. L., & Yang, X. F. (2023). Research on the trends and countermeasures of telecom fraud in the context of the Internet: Taking 400 criminal judgments as an example. *Journal of Liaoning Administrators' College of Police and Justice, 2023*(5), 43–49.

Wei, R., Liu, X., & Liu, X. (2019). Examining the perceptual and behavioral effects of mobile internet fraud: A social network approach. *Telematics and Informatics, 41*, 103–113.

Wen, J., Yang, H., Zhang, Q., & Shao, J. (2022). Understanding the mechanisms underlying the effects of loneliness on vulnerability to fraud among older adults. *Journal of Elder Abuse & Neglect, 34*, 1–19.

Williams, C. (2010). *Victimization among individuals with low self-control: Effects on fear versus perceived risk of crime*. Master's Theses. University of South Florida.

Williams, R., & Dickinson, J. (1993). Fear of crime: Read all about it? The relationship between newspaper crime reporting and fear of crime. *British Journal of Criminology, 33*(1), 33–56.

Wu, Y., Li, F., Triplett, R. A., & Sun, I. Y. (2019). Media consumption and fear of crime in a large Chinese city. *Social Science Quarterly, 100*(6), 2337–2350.

Wu, Y., & Wareham, J. (2017). Perceived risk of crime: A tale of two immigrant groups in metro Detroit. *Journal of Ethnicity In Criminal Justice, 15*(2), 117–137.

Wyant, B. R. (2008). Multilevel impacts of perceived incivilities and perceptions of crime risk on fear of crime. *Journal of Research in Crime and Delinquency, 45*(1), 39–64.

Xie, B., & Chen, J. X. (2022). Research on the investigation of "romantic scams" from the perspective of investigation game theory. *Journal of People's Public Security University of China (Social Sciences Edition), 05*, 41–52.

Xing, T., Sun, F., Wang, K., Zhao, J., Wu, M., & Wu, J. (2020). Vulnerability to fraud among Chinese older adults: Do personality traits and loneliness matter? *Journal of Elder Abuse & Neglect, 32*, 46–49.

Xu L.C., Gao N., Ma Y.Y. (2020). *Credit constraints and fraud victimization: Evidence from a representative Chinese household survey*. Retrieved on March 25, 2022, from https://blogs.worldbank.org/en/allaboutfinance/credit-constraints-and-fraud-victimization-evidence-representative-chinese

Xu, Y. (2022). *Research on offenders' decision-making of new Cyberfraud Crime*. Unpublished dissertation, East China University of Political Science and Law.

Xu, Y., & Xu, T. (2021). Research on the characteristics and countermeasures of cross-border telecom-network fraud. *Issues on Juvenile Crime and Delinquency, 4*, 88–103.

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

Zhang, L., Messner, S. F., Liu, J., & Zhuo, Y. A. (2009). Guanxi and fear of crime in contemporary urban China. *The British Journal of Criminology, 49*(4), 472–490.

Zhao, J. S., Lawton, B., & Longmire, D. (2015). An examination of the micro-level crime-fear of crime link. *Crime & Delinquency, 61*(1), 19–44.

Authors and Affiliations

Jia Qu[1] · **Kai Lin[2]** · **Yuning Wu[3]** · **Ivan Y. Sun[4]**

✉ Kai Lin
  kai.lin@uts.edu.au

  Jia Qu
  201801070@mail.gufe.edu.cn

  Yuning Wu
  yuningwu@wayne.edu

  Ivan Y. Sun
  isun@udel.edu

[1] College of Public Administration, Guizhou University of Finance and Economics, Guiyang, China

[2] School of International Studies and Education, University of Technology Sydney, Ultimo, Australia

[3] Department of Criminology and Criminal Justice, Wayne State University, Detroit, Michigan, USA

[4] Department of Sociology and Criminal Justice, University of Delaware, Newark, DE 19716, USA