Crime Prevention and Community Safety (2024) 26:373–384
https://doi.org/10.1057/s41300-024-00219-2

ORIGINAL ARTICLE

Routine activities and consumer fraud victimization: findings from a social survey in Chiba Prefecture, Japan

Ai Suzuki[1]

Accepted: 19 September 2024 / Published online: 15 October 2024

Abstract

Recently, Japan has been grappling with various forms of consumer fraud. Consumer fraud victimization causes not only monetary losses but also nonmonetary costs such as emotional stress and psychological trauma. Therefore, it is necessary to investigate the factors associated with the risk of consumer fraud victimization in order to identify vulnerable groups and implement suitable prevention measures. Consequently, this study aims to analyze the sociodemographic and routine activity factors associated with consumer fraud victimization risk in Japan. Drawing on data from a social survey of residents in Chiba Prefecture, Japan, this study employs a series of logistic regression models. This study demonstrates that while using social networking services is unrelated to respondents' likelihood of experiencing consumer fraud victimization, the frequency of contacting individuals whom respondents have only met online was statistically linked to increased consumer fraud risk. Additionally, only 10.7 to 31.9% of respondents were aware of the available support services for victims of consumer fraud and related issues. This study proposes that social networking providers could aid in preventing consumer fraud by displaying warning messages when users send messages, alerting them to possible threats.

Keywords Routine activity theory · Consumer fraud · Cyber fraud · Malicious business practices · Consumer damage

Introduction

Consumer fraud in Japan

Japan is one of the safest and most advanced nations worldwide. However, a rise in fraudulent crimes, which rob individuals of their money, has become a serious issue. With rapid advancements in information technology, which have

✉ Ai Suzuki
r430@ipc.fukushima-u.ac.jp

[1] Organization for the Promotion of Education, Fukushima University, Fukushima, Japan

drastically impacted our daily lives, the risk of cyber fraud victimization has increased in many industrialized nations, including Japan. In 2023, the police recorded 5578 cases of phishing scams, where individuals receive deceptive emails posing as well-known sources like banks, requesting individuals to provide personal information. These scams resulted in financial losses amounting to approximately eight billion JPY. The number of phishing cases has increased by 391%, with financial losses increasing by 474.6% annually (National Police Agency 2024). Additionally, the Japan Cybercrime Control Center received approximately 29,000 reports of malicious shopping sites in 2022 (Japan Cybercrime Control Center 2023). Alongside the rise in cyber fraud victimization, malicious business practices and consumer damage have also become pervasive in Japan. According to the Consumer Affairs Agency (2023), the number of consumer affairs consultations reached approximately 870,000 in 2022, marking an increase from the previous year (859,000). The category with the largest number of consumer affairs consultations was "general products," encompassing junk mail, suspicious phone calls, unrecognized packages, and fictitious bills, followed by "health and hygiene products" (e.g., cosmetic products) and "entertainment services" (e.g., adult content, dating sites/apps, internet games, and information distribution services).

Here, some examples of consumer fraud cases in Japan are described. In Sapporo, Hokkaido, a man in his 30s was defrauded out of approximately 7.4 million JPY by a phishing scam (NHK 2023). In May 2023, the man received a phishing email that claimed that deposits and withdrawals from his bank account via the Internet have been restricted. The source of the mail was the name of the man's main bank. When he clicked the "Unlock Restrictions" button on the mail, he was directed to a fake bank website that looked exactly like the real one. He entered his account number, PIN, bank branch number, and one-time password required for making deposits and withdrawals over the Internet, as instructed. Later, he received a genuine email from the bank stating that the transfer had been completed, and he realized that about 7.4 million JPY had been transferred to an unknown account without his knowledge. In Kobe, Hyogo Prefecture, a man in his 70s was defrauded out of 2.162 million JPY (NHK 2024a). The man received a friend request on Facebook around December 2023 from an account claiming to be a woman. He then contacted the woman on LINE (an app for instant communications) and was told that he had a "good investment offer." After the first transfer, he attempted to withdraw the money, but the woman said that he needed a deposit and that he needed to pay taxes, so he transferred the money one after another. A woman in her 40s living in Sapporo was defrauded of over 100 million JPY by a person she met on the Internet who offered her a false investment in crypto assets (NHK 2024b). In March 2024, she accessed an advertisement on Facebook that recommended investment and was contacted by a person claiming to be an investor and invited to a group chat on LINE. She was advised to invest in crypto assets, and in the next month, she transferred a total of about 100 million JPY to the designated account 18 times and was defrauded. The bank became suspicious of the large transfers she made and consulted the police.

Prior research on consumer fraud

In addition to actual monetary losses, consumer fraud victimization incurs nonmonetary costs that are challenging to quantify but can exceed monetary losses, such as emotional stress and psychological trauma (Lee and Soberon-Ferrer 1997; Vakhitova et al. 2022; Whitty and Buchanan 2016). For instance, in the UK, Whitty and Buchanan (2016) conducted a semi-structured interview with 20 participants who had not lost money but had been taken in by online dating romance scammers. It was found that the participants suffered different types of negative emotions, such as shame, embarrassment, depression, anger, worry, and stress, even though they did not experience money loss. Further, some participants had lost confidence, or considered attempting suicide. In the context of crime prevention, it is important to understand the factors associated with the risk of consumer fraud and identify groups that require particular protection from consumer fraud, considering the impact of consumer fraud in many ways. Vakhitova et al. (2022) conducted an online survey of adults residing in the US on the perceived victim impact of cyber abuse. Open-ended responses of cyber abuse victims about the impact of victimization on their lives from 705 participants revealed that a majority of victims (88%) reported they had experienced different types of negative impact (psychological, emotional, social, financial/education/work-related) from their victimization.

Existing research has investigated the factors associated with the risk of consumer fraud victimization. Most studies have focused on Western settings (Buil-Gil et al. 2021; Estelami and Liu 2023; Georgiadou et al. 2022; Johnson and Nikolovska 2022; Kemp et al. 2021; Lee and Geistfeld 1999; Lee et al. 2022; Murrar 2022; Reyns and Henson 2016), providing evidence on individuals that are more vulnerable to consumer fraud victimization. As with other types of crime, consumer fraud risk is disproportionally distributed across individuals, time, and space. For instance, older persons are particularly vulnerable to consumer fraud (Lee and Geistfeld 1999; Lee and Soberon-Ferrer 1997), which can be attributed to age-related cognitive decline that slows down the processing of information (John and Cole 1986). However, it has also been proven that younger people are more likely to become victims of fraud, possibly because of their increased engagement in activities related to consumer fraud risk (Lee et al. 2022; Pratt et al. 2010). Additionally, mixed results have been obtained regarding the impact of marital status on consumer vulnerability to fraud. For instance, based on a national representative sample of 957 adults in the United States, Lee and Soberon-Ferrer (1997) revealed that nonmarried (widowed, divorced, and single) individuals were more likely to experience market fraud than married individuals, possibly because family members provide psychological support that helps prevent consumer fraud victimization. Conversely, Lee et al. (2022) surveyed 477 adults in the US, revealing that full-time employment and being married were associated with higher risks of food fraud than non-full-time employment and being single. They argue that employed individuals possess greater financial resources, thereby increasing fraud risk, and that married individuals are more likely to seek healthy products that can be associated with fraud risk.

Routine activity theory, initially introduced by Cohen and Felson (1979), argues that three factors are required for a crime to occur: (1) motivated offenders; (2) suitable targets; and (3) the absence of capable guardians. When routine activities bring together potential offenders and vulnerable targets without capable guardianship, the likelihood of crime increases. Similar to offline crime, which requires contact between offenders and victims, routine activity theory is beneficial for explaining trends in and patterns of consumer fraud victimization that can occur in cyberspace. Therefore, considering routine activity factors is important in explaining consumer fraud risk.

Many previous empirical works have applied the routine activity theory to study online crimes (Johnson and Nikolovska 2022; Lee et al. 2022; Leukfeldt and Yar 2016; Mir Mohamad Tabar et al. 2021; Özaşçılar et al. 2024; Pratt et al. 2010; Reyns and Henson 2016). For instance, using nationally representative participants from the Canadian General Social Survey, Reyns and Henson (2016) analyzed the factors associated with identity theft victimization. Their analysis of binary logistic regression empirically demonstrated that the frequency of using online banking and purchasing, as measures of exposure to motivated offenders, were found to be correlates of online identity theft. Lee et al. (2022) administered an online survey of 477 adult consumers in the US to examine the patterns and predictors of food fraud victimization. It was demonstrated that the frequency of purchasing food products online and using chat apps was found to increase the likelihood of experiencing food fraud.

Vakhitova et al. (2016) argued, however, that recent studies that tested the utility of routine activity theory have provided mixed results. Specifically, they stated that the theory born in terrestrial settings may not be appropriate to discuss crime patterns in cyberspace, suggesting adopting more robust methodological designs to explain contextual effects. It is therefore important to note here that there is still a necessity to test the applicability of routine activity theory in the context of cyberspace.

The risk of consumer fraud victimization has been increasing in many industrialized nations, and Asian countries are no exception. In South Korea, for instance, cyber fraud, especially against the elderly, has been a significant problem in recent years (Button et al. 2024). Indeed, the number of those targeting the elderly has increased by 216% from 2012 to 2019 (Loveday and Jung, 2021). Although the seriousness of consumer fraud victimization has been recognized, few studies have focused on Asian settings. For instance, Lee (2021) adopted a crime script analysis to examine how customer-to-customer fraud occurs on online platforms in China. In Singapore, Lu et al. (2020) investigated the impact of different messages on posters on individuals' vulnerability to scams. Their study, involving 60 adult male participants, revealed that those who viewed emotion-normalizing posters purchased fewer items than those who viewed cognitive-focused posters. In Japan, Ochi (2001) conducted an online survey of 1500 adults to investigate factors correlated with information security behavior, revealing that information security behavior was facilitated by the social recognition of security risk, information security behavior costs, and close relationships with individuals exhibiting information security behavior. Kanayama (2017) also surveyed 13,000 men and women aged 16 and above to understand cybercrime experiences, revealing that 9.6% of respondents reported experiencing some form of cybercrime.

Understudied aspects of consumer fraud victimization patterns in Japan are associated with a high risk of such incidents. The studies conducted in Asia, as described above, have failed to explore sociodemographic and routine activity factors associated with consumer fraud victimization risk. It is unclear whether the same consumer fraud victimization patterns found in Western countries apply in the Asian context. Furthermore, little attention has been paid to consumer fraud patterns in East Asian countries, which may be partially attributed to their relatively low crime rates. Nevertheless, empirical research is necessary to understand the risk factors associated with consumer fraud victimization due to the increased number of consumer fraud cases in Japan.

Therefore, this study aims to analyze the factors associated with an increased risk of consumer fraud victimization in Japan. Despite a general decline in crime rates in Japan over the last two decades, prior research has empirically demonstrated that specific groups have experienced elevated criminal victimization risks during significant and prolonged crime reduction. While crime rates have been decreasing overall, the risk of consumer fraud victimization has been increasing in Japan. Victims of consumer fraud may often feel embarrassed to report their victimization to the police, family, or other people, fearing they may appear foolish and gullible (Lee and Geistfeld 1999). This suggests that there may be unreported or undiscovered cases of consumer fraud. Therefore, social surveys are useful for understanding individuals' experiences of consumer fraud victimization.

Methods

Data

The data used in this study was obtained from a social survey. The "Shukutoku-Yomiuri Chiba Social Survey" (SYCSS) was conducted online by Shukutoku University and the Yomiuri Shimbun, Japan's largest media conglomerate, from October 26 to November 6, 2023. The SYCSS targeted individuals aged 20 and above residing in Chiba Prefecture, Japan. Utilizing quota sampling, the SYCSS quota conditions referred to six quotas of age (20 s, 30 s, 40 s, 50 s, and 60 s), two quotas of sex (male and female), and six quotas of areas. A total of 5175 individuals participated in the SYCSS. Similar to surveys like the General Social Survey or the European Social Survey, the SYCSS encompasses a wide range of questions regarding respondents' demographics, behaviors, and attitudes. Regarding the experience of victimization, respondents were asked about their experiences of victimization across various types of crime within the past year.

Measures

Dependent variable

Consumer fraud victimization experience was measured using a binary variable (0 = no, 1 = yes). Respondents in the SYCSS were asked, "Did you experience cyber fraud, malicious business practices, and/or consumer damage last year?".

Sociodemographic characteristics

The current study employed a binary measure for sex (0 = male, 1 = female). Age was measured as a series of dummy-coded categorical variables: 20 s, 30 s, 40 s, 50 s, and 60 s (40 s was the reference category). Marital status was measured as binary (0 = single, 1 = married). Employment status was measured as a binary (0 = part-time, housewife/husband, student, unemployed, or other, 1 = full-time). Living arrangements were measured as a binary (0 = living with someone, 1 = living alone). Household income was measured as a series of dummy-coded categorical variables: less than 2 million JPY, 2 million JPY to less than 4 million JPY, 4 million JPY to less than 6 million JPY, 6 million JPY to less than 8 million JPY, 8 million JPY to less than 10 million JPY, and more than 10 million JPY (one million JPY to less than 8 million JPY was the reference category). Education was measured as a binary (0 = below a bachelor's degree, 1 = a bachelor's degree or above).

Routine activities

To determine the impact of exposure and proximity on motivated consumer fraud offenders, six routine activity measures were included: (1) using X (formerly Twitter), (2) Facebook, (3) Instagram, (4) LINE, and (5) TikTok. These measures were all coded dichotomously (0 = no, 1 = yes). Additionally, the frequency of contacting individuals solely online was measured (0 = never, 1 = rarely, 2 = occasionally, and 3 = frequently).

Analytical strategy

Only respondents who met the following criteria were included in the analyses: (1) owning a desktop computer, laptop, or tablet; (2) owning a smartphone; (3) completing all questions containing both dependent and independent variables; and (4) selecting an appropriate answer on the directed question scale (DQS) (Maniaci and Rogge 2014) inserted in the survey to filter out the respondents who put minimal effort into answering the survey (Barge and Gehlbach 2012). The analyses in this study are threefold. First, descriptive statistics of the sample are reviewed to demonstrate the prevalence of consumer fraud victimization among respondents. Second, regression analysis is conducted to determine factors correlated with consumer fraud risk. Given the binary nature of the dependent variable (consumer fraud experience), logistic regression is adopted. SPSS version 29 was employed to perform logistic regression. The variance inflation factor was used to assess the possibility of multicollinearity among the independent variables, with no signs of multicollinearity observed. Finally, respondents' knowledge of available support for consumer fraud victimization or related issues is presented.

Results

Descriptive statistics for the sample are presented in Table 1. As shown, 2.4% of respondents reported experiencing consumer fraud victimization in the past year. This victimization rate is low compared to other studies. For instance, 15.9% of participants in the survey, which represented 40.0 million U.S. adult people, reported that they had experienced the types of fraud covered by this survey at least once during the year before they were interviewed (Anderson 2019). A survey of 3478 respondents from 154 different countries showed that 1317 (38%) of respondents reported that they had been victims of online fraud in the last year (Whittaker et al. 2022). Although only a small proportion of the sample of the SYCSS reported experiencing consumer fraud victimization, considering the nature of consumer fraud, some respondents may have encountered fraud attempts or incidents. Additionally, it is possible that consumer fraud is unevenly distributed across respondents, such that a small proportion of repeatedly victimized people account for a substantial amount of all victimizations.

Table 2 presents the logistic regression models for consumer fraud victimization. Regarding sociodemographic characteristics, no variables exhibited associations with consumer fraud victimization. This suggests that individual-level

Table 1 Descriptive statistics (N = 1782)

Variable	Min	Max	Mean	S.D
Consumer fraud victimization	0	1	0.024	0.152
Sex (female)	0	1	0.400	0.491
Age	20	60	42.660	12.848
Married	0	1	0.565	0.496
Full-time employment	0	1	0.580	0.494
Single-person household	0	1	0.260	0.441
Household income	1	6	3.404	1.561
Bachelor's degree	1	2	1.440	0.496
Using X (formerly Twitter)	0	1	0.480	0.500
Using Facebook	0	1	0.230	0.423
Using Instagram	0	1	0.380	0.486
Using LINE	0	1	0.760	0.429
Using TikTok	0	1	0.120	0.328
Frequency of contacting people that respondents have only met online	0	3	0.463	0.802

Table 2 Logistic regression models for consumer fraud victimization (N = 1782)

Variables	Coefficient	SE	Exp(B)
Sex (female)	0.093	0.355	1.097
Age: 20 s	0.450	0.552	1.568
Age: 30 s	−0.307	0.560	0.735
Age: 50 s	0.216	0.450	1.241
Age: 60 s	−0.070	0.528	0.932
Married	−0.366	0.409	0.693
Full-time employment	−0.393	0.378	0.675
Single-person household	0.091	0.406	1.096
Household income: less than 2 million JPY	−0.511	0.671	0.600
Household income: 2 million JPY to less than 4 million JPY	−0.181	0.520	0.834
Household income: 4 million JPY to less than 6 million JPY	−0.056	0.498	0.945
Household income: 8 million JPY to less than 10 million JPY	−0.117	0.601	0.890
Bachelor's degree	0.485	0.335	1.624
Using X (formerly Twitter)	−0.076	0.383	0.927
Using Facebook	0.722	0.386	2.058
Using Instagram	−0.496	0.415	0.609
Using LINE	−0.068	0.407	0.934
Using TikTok	0.193	0.490	1.213
Frequency of contacting people that respondents have only met online	0.427	0.171	1.533
Constant	−4.188	0.836	0.015
-2 log-likelihood		378.503	
Model × 2		3.159	
Nagelkerke R2		0.054	

factors neither increase nor decrease the risk of consumer fraud victimization. Regarding routine activities, consumer fraud victimization was found to be statistically influenced by the frequency of contacting individuals that respondents solely met online. Specifically, those who frequently engage in such interactions are approximately 1.5 times more likely to become victims of consumer fraud. However, the use of platforms such as X (formerly Twitter), Facebook, Instagram, LINE, and TikTok showed no correlation with respondents' experiences of consumer fraud victimization.

The SYCSS requested respondents to report their awareness of available support systems, such as consultation desks or hotlines, for criminal victimization or related issues. Among the 14 types of different support queried in the survey, Fig. 1 displays respondents' knowledge of assistance for victims of consumer fraud by victims and non-victims. It is revealed that only a few victims and non-victims are familiar with any consultation support services for consumer fraud victimization, though there are some differences between victims and non-victims in the ratio of knowledge of assistance for victims of consumer fraud and which service is the most well-known.

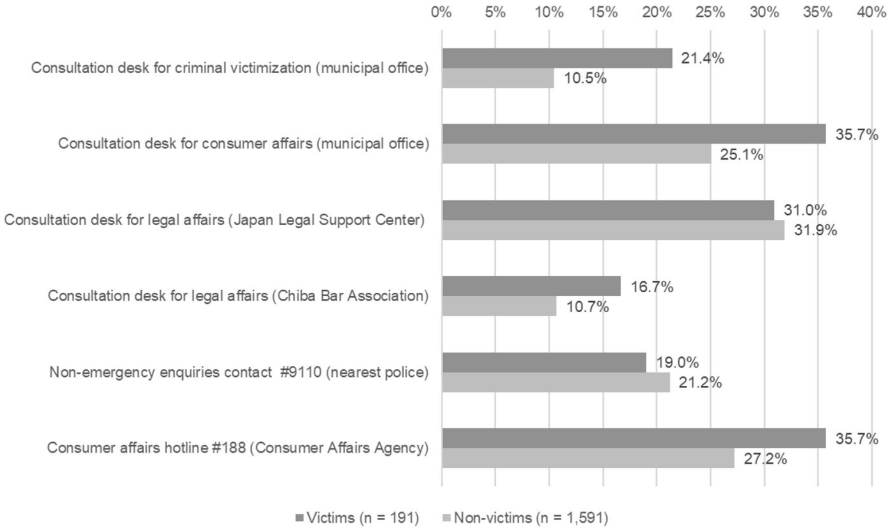

Fig. 1 Respondents' knowledge of support available for consumer fraud victimization or related issues

Discussion and conclusions

Employing data obtained from a social survey conducted in Chiba Prefecture, Japan, this study aimed to examine of the types of consumers that are more vulnerable to consumer fraud. First, it revealed that while a small minority reported being victims of consumer fraud in the past year, it is possible that some encountered fraud attempts or incidents, such as phishing emails or fake online advertisements, but managed to avoid them. Additionally, there can be high concentrations of consumer fraud victimization among those who were targeted, as previous research has revealed regarding other forms of crime (Suzuki et al. 2024).

Second, this study conducted a regression analysis of the factors associated with consumer fraud risk. The results reveal that while the use of social networking services was not associated with consumer fraud, there was a significant positive correlation between the frequency of contacting people that respondents had only met online and the risk of consumer fraud victimization. This finding aligns with previous studies conducted in other nations (Lee et al. 2022; Reyns and Henson 2016), suggesting that exposure and proximity to motivated offenders increase the likelihood of consumer fraud. This indicates that using social networking services itself does not increase the risk of consumer fraud victimization. However, how individuals use these services (e.g., contacting people that respondents have only met online) is a predictor of becoming victims of consumer fraud. Therefore, consumer fraud prevention measures should focus on those who use social networking services for networking purposes.

Third, respondents' knowledge of available support for victims of consumer fraud was examined. While several consultation desks or hotlines for consumer fraud or related problems are offered by different entitles, many respondents were unaware of these support services. Given the likelihood that some respondents may have encountered a fraud attempt or incident, these organizations should enhance their visibility among potential users.

This study has some limitations. First, it could not establish causal relationships because the data were cross-sectional. Therefore, employing panel data analysis is crucial for a better understanding of the causality of victimization and sociodemographic and routine activity variables. Second, while this study included variables representing respondents' online exposure and proximity to motivated offenders of consumer fraud, it did not consider the impact of target suitability and guardianship on the risk of consumer fraud victimization (Lee et al. 2022; Reyns and Henson 2016). Therefore, future empirical studies should investigate how target suitability and guardianship are associated with consumer fraud victimization.

Notwithstanding these limitations, this study contributes to the criminological literature by offering implications for practitioners and stakeholders. Drawing on the routine activity theory, this study revealed factors associated with a high risk of consumer fraud victimization in Japan. Given the complexity of consumer fraud crime in Japan, empirical evidence is required to develop policing strategies. The study's findings could influence public crime prevention policymaking in two ways. First, the results indicate that accelerating collaboration with different stakeholders responsible for consumer fraud victimization is necessary. This study highlights that those who had frequent contact with individuals who they had only met online showed high risks of consumer fraud victimization, emphasizing the need for interventions among these individuals. Social networking providers can make efforts to display a warning message about possible threats to users of their services. Additionally, to introduce effective crime prevention, it is recommended that future studies analyze the situations of individuals encountering fraud attempts and repeat victims of consumer fraud to better understand the prevalence of consumer fraud attempts and the factors associated with repeat victimization. Second, this study highlights the necessity of raising awareness about available support services for consumer fraud victimization or related issues. Municipal offices, the Japan Legal Support Center, the Chiba Bar Association, the police, and the Consumer Affairs Agency, which provide support for consumer fraud victimization or related issues, should explore avenues to enhance their recognition among potential users.

Declarations

Conflict of interests The author declares no competing interests.

References

Anderson, K.B. 2019. *Mass-Market Consumer Fraud: In the United States: A 2017 Update*. Washington: Bureau of Economics, Federal Trade Commission.

Barge, S., and H. Gehlbach. 2012. Using the theory of satisficing to evaluate the quality of survey data. *Research in Higher Education* 53 (2): 182–200. https://doi.org/10.1007/s11162-011-9251-2.

Buil-Gil, D., Y. Zeng, and S. Kemp. 2021. Offline crime bounces back to pre-COVID levels, cyber stays high: Interrupted time-series analysis in Northern Ireland. *Crime Science* 10 (1): 26. https://doi.org/10.1186/s40163-021-00162-9.

Button, M., V. Karagiannopolos, J. Kee, J. Suh, and J. Jung. 2024. Preventing fraud Victimisation against older adults: Towards a holistic model for protection. *International Journal of Law, Crime and Justice*. https://doi.org/10.1016/j.ijlcj.2024.100672.

Cohen, L.E., and M. Felson. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44 (4): 588–608. https://doi.org/10.2307/2094589.

Consumer Affairs Agency. 2023. White paper on consumer affairs 2023. Available at: https://www.caa.go.jp/policies/policy/consumer_research/white_paper/2023. (Accessed 15 April 2024)

Estelami, H., and K. Liu. 2023. Content analysis of American consumers' credit card fraud complaints filed with the Consumer Financial Protection Bureau. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-03-2023-0070.

Georgiadou, A., S. Mouzakitis, and D. Askounis. 2022. Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal* 35 (2): 486–505. https://doi.org/10.1057/s41284-021-00286-2.

Japan Cybercrime Control Center. 2023. Statistical information on malicious shopping sites in 2022. Available at: https://www.jc3.or.jp/threats/topics/article-485.html. (Accessed 15 April 2024)

John, D.R., and C.A. Cole. 1986. Age differences in information processing: Understanding deficits in young and elderly consumers. *Journal of Consumer Research* 13 (3): 297. https://doi.org/10.1086/209070.

Johnson, S.D., and M. Nikolovska. 2022. The effect of COVID-19 restrictions on routine activities and online crime. *Journal of Quantitative Criminology*. https://doi.org/10.1007/s10940-022-09564-7.

Kanayama, T. 2017. Results of cybercrime victimization survey. *Risk Management Studies* 1: 102–111.

Kemp, S., D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño. 2021. Empty streets, busy Internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice* 37 (4): 480–501. https://doi.org/10.1177/10439862211027986.

Lee, C.S. 2021. How online fraud victims are targeted in China: A crime script analysis of Baidu tieba C2C fraud. *Crime and Delinquency* 68 (13–14): 2529–2553. https://doi.org/10.1177/00111287211029862.

Lee, J., and L.V. Geistfeld. 1999. Elderly consumers' receptiveness to telemarketing fraud. *Journal of Public Policy and Marketing* 18 (2): 208–217. https://doi.org/10.1177/074391569901800207.

Lee, J., and H. Soberon-Ferrer. 1997. Consumer vulnerability to fraud: Influencing factors. *Journal of Consumer Affairs* 31 (1): 70–89. https://doi.org/10.1111/j.1745-6606.1997.tb00827.x.

Lee, B., R. Fenoff, and J. Spink. 2022. Routine activities theory and food fraud victimization. *Security Journal* 35 (2): 506–530. https://doi.org/10.1057/s41284-021-00287-1.

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

Loveday, B., and Jung, J. 2021. A current and future challenge to contemporary policing: the changing profile of crime and the police response. Examples of policing fraud in two police jurisdictions: England and Wales and South Korea. Policing: *A Journal of Policy and Practice* 15 (3): 1633–1650.

Lu, H.Y., S. Chan, W. Chai, S.M. Lau, and M. Khader. 2020. Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention and Community Safety* 22 (4): 313–330. https://doi.org/10.1057/s41300-020-00098-3.

Maniaci, M.R., and R.D. Rogge. 2014. Caring about carelessness: Participant inattention and its effects on research. *Journal of Research in Personality* 48: 61–83. https://doi.org/10.1016/j.jrp.2013.09.008.

Mir Mohamad Tabar, S.A., G.A. Petrossian, M. Mazlom Khorasani, and M. Noghani. 2021. Market demand, routine activity, and illegal fishing: an empirical test of routine activity theory in Iran. *Deviant Behavior* 42 (6): 762–776. https://doi.org/10.1080/01639625.2021.1927885.

Murrar, F. 2022. Fraud schemes during COVID-19: A comparison from FATF countries. *Journal of Financial Crime* 29 (2): 533–540. https://doi.org/10.1108/JFC-09-2021-0203.

National Police Agency. (2024). "Threats to cyberspace in 2023", Available at: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf. (Accessed 15 April 2024)

NHK. (2023). Major banks warn of Phishing Scam. *NHK*. https://www3.nhk.or.jp/news/html/20230909/k10014190261000.html.

NHK. (2024a). "Accepting friend requests" and "borrowing money through consumer credit": A spate of social networking scams. *NHK*. https://www.asahi.com/articles/ASS4Q3G03S4QPIHB00VM.html.

NHK. (2024b). A woman in her 40s in Sapporo suffered damage in excess of 100 million yen due to a false investment story about crypto assets. *NHK*. https://www3.nhk.or.jp/sapporo-news/20240527/7000067251.html.

Ochi, K. 2001. Factors affecting information security behavior. *Bulletin of the Faculty of Letters, Hosei University* 77: 77–104.

Özaşçılar, M., C. Çalıcı, and Z. Vakhitova. 2024. Examining cybercrime victimisation among Turkish women using routine activity theory. *Crime Prevention and Community Safety* 26 (1): 112–128. https://doi.org/10.1057/s41300-024-00201-y.

Pratt, T.C., K. Holtfreter, and M.D. Reisig. 2010. Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency* 47 (3): 267–296. https://doi.org/10.1177/0022427810365903.

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

Suzuki, A., A. Sidebottom, R. Wortley, and T. Shimada. 2024. Repeat victimisation and the crime drop: Evidence from Japan. *Crime Prevention and Community Safety* 26 (1): 1–15. https://doi.org/10.1057/s41300-023-00196-y.

Vakhitova, Z.I., D.M. Reynald, and M. Townsley. 2016. Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice* 32 (2): 169–188. https://doi.org/10.1177/1043986215621379.

Vakhitova, Z.I., C.L. Alston-Knox, E. Reeves, and R. Mawby. 2022. Explaining victim impact from cyber abuse: an exploratory mixed methods analysis. *Deviant Behavior* 43 (10): 1153–1172. https://doi.org/10.1080/01639625.2021.1921558.

Whittaker, J.M., M. Edwards, C. Cross, and M. Button. 2022. I have only checked after the event": consumer approaches to safe online shopping. *Victims & Offenders. Routledge.* https://doi.org/10.1080/15564886.2022.2130486.

Whitty, M.T., and T. Buchanan. 2016. The Online dating romance scam: the psychological impact on victims—both financial and non-financial. *Criminology and Criminal Justice* 16 (2): 176–194. https://doi.org/10.1177/1748895815603773.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.