

Analysis of Risk Factors and Stimulating Reasons in the Phenomenon of Cyber Victimization

Elham Shafaiimoghadam^{a*}, Zahra Baratian^b, Saeedeh Mirzaee^c

^a Assistant Professor, Department of Social Sciences, Faculty of Humanities and Law, University of Kashan, Kashan, Iran; E.Shafaii.M@Kashanu.ac.ir

^{b, c} Graduate with a Bachelor's degree in Social Sciences, University of Kashan, Kashan, Iran; zahrabaratiyan009@gmail.com^b, saeedehm399@gmail.com^c

ABSTRACT

Due to the popularity of mobile phones and the internet, as well as the development of electronic devices and various software, numerous benefits and facilities have emerged. However, misuse of these tools can lead to serious problems such as deliberate harm to others or cyber victimization. This study utilizes the Everyday Activities Theory and questionnaire techniques to analyze the risk factors and stimulating reasons for cyber victimization among citizens of Kashan City. According to the research findings, there is a significant relationship between independent variables such as online protection, online proximity to motivated offenders, risky offline activities, online attractive targets, deviant lifestyle, and the level of cyber victimization. Among these, the correlation between online proximity to motivated offenders and cyber victimization is greater than other independent variables ($r=0.505$, $sig=0.000$). Path analysis results also indicate that the linear combination of the independent variables present in the model can explain 37% of the variance in cyber victimization.

Keywords — Cyber victimization, Everyday Activities Theory, Online Protection, Online Attractive Target, Proximity to Motivated Offenders.

1. Introduction


Significant technological advancements in communication and entertainment over the past few years have reshaped social interactions. The ability to communicate remotely at any time of day, facilitated by these devices, offers substantial benefits for forging new relationships or maintaining connections with family and friends. However, misuse of these tools can potentially lead to various dangers. One of these dangers includes using these devices to attack others, such as harassing, insulting, or intentionally causing harm to them. In this context, Cybervictimization refers to any form of aggression, harassment, or abuse individuals experience in the virtual space [1]. This phenomenon has become a serious social issue with the widespread use of the internet and communication technologies.

The term "Cybervictimization" or "cyber victimization" in this text will refer to the experience

of harassment and distress by individuals through mobile phones or the internet, primarily encompassing verbal, written, or visual harassment, deletion, and identity fraud [2].

Visual victimization includes images (usually photos or videos) taken or distributed electronically that are harmful or detrimental to the victim. Verbal-written victimization refers to receiving intrusive, threatening, or insulting calls, messages, or comments via mobile phones or the Internet. Online deletion refers to exclusion or expulsion from groups, typically on social networks or instant messaging applications. Identity forgery refers to situations where someone impersonates the victim on a mobile phone or the internet to mock or cause trouble for them [2, 3, 4].

Reviewing the literature on internet crimes and victims indicates that Cybervictimization is a relatively new concept referring to threats and unwanted aggressive acts in the digital space. This

 <http://dx.doi.org/10.22133/ijwr.2024.468435.1230>

Citation E. Shafaiimoghadam, Z. Baratian, S. Mirzaee, "Analysis of Risk Factors and Stimulating Reasons in the Phenomenon of Cyber victimization", *International Journal of Web Research*, vol.7, no.2, pp.65-74, 2024, doi: <http://dx.doi.org/10.22133/ijwr.2024.468435.1230>.

*Corresponding Author

Article History: Received: 18 January 2024; Revised: 29 February 2024; Accepted: 14 March 2024.

Copyright © 2022 University of Science and Culture. Published by University of Science and Culture. This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 International license (<https://creativecommons.org/licenses/by-nc/4.0/>). Noncommercial uses of the work are permitted, provided the original work is properly cited.

issue has garnered attention primarily from legal perspectives and its impact on individuals and societies [5, 6, 7, 8, 9, 10]. However, sufficient research from a sociological perspective, especially in Iran, has not yet been conducted in this area.

Based on international studies and cultural and social similarities, it can be assumed that the rate of cyber victims in Iran may be similar to other countries. According to a recent study by the European Union Agency for Cybersecurity (ENISA), approximately 20-30% of adolescents in certain European countries have reported experiencing cyber victimization. This study highlights the significant prevalence of cybercrime among young people in Europe and underscores the need for enhanced protective measures and awareness programs [11]. Assuming a similar situation in Iran, it can be estimated that a significant percentage of Iranian adolescents and youth have experienced cyber victimization. According to the annual report of the Cyber Police in 2020, the number of reports related to cybercrimes has increased, many of which involve Cyber victimization. In this regard, a study conducted at Mazandaran University in 2019 showed that about 50 percent of students had a moderate experience of Cyber victimization [12]. Given that cyber victimization, especially in severe cases, can harm an individual's mental and social health and contribute to the onset of depression and suicidal thoughts [13], it is important to identify the significant variables that affect the likelihood of an individual becoming a victim of cyber-attacks, to improve prevention, detection, and treatment.

The study of factors influencing the risk of cyber victimization is relatively new and there are still gaps and inconsistencies in this area. This study focuses on analyzing some social and technological factors that are still under discussion for their predictive potential in cyber victimization.

One of the factors examined in this study is the attractiveness of the target online. Online target attractiveness refers to characteristics and behaviors that can make a person attractive to cyber criminals [14]. These characteristics may include having public profiles, a large number of friends or followers, sharing personal information or sensitive posts, and so on. Research has shown that individuals with more attractive online profiles are more likely to experience Cyber victimization. In this context, research by [15] showed that displaying personal information and engaging in online activities can increase the risk of cyber victimization. Additionally, the researchers found that individuals who use public profiles more frequently and share more personal information are at a higher likelihood of experiencing cyber victimization. Additionally, [16] examined the role

of online target attractiveness in Cybervictimization and found that factors such as online popularity and a large number of followers can act as risk factors for cyber victimization. This study showed that individuals who are more popular on social networks may become targets of cyber-attacks due to envy or competition from others.

Studies have shown that online protection can play an important role in reducing the risk of cyber victimization. Individuals and adolescents who take appropriate protective measures are less likely to be exposed to cyber victimization. Online protection refers to taking security measures to protect personal information and privacy in the online space. These measures may include privacy settings on social networks, using strong passwords, avoiding sharing sensitive information, and regularly updating security software [17, 18]. In this regard, the study [19] showed that students who use appropriate privacy settings on social networks and limit their personal information are less likely to experience Cyber victimization. Furthermore, Research [20] explores how cyber security awareness and protective behaviors significantly impact the reduction of cyber victimization risk. The study demonstrates that increased awareness of security issues and the implementation of preventive measures, such as strong passwords and secure browsing practices, can notably diminish the likelihood of cyber incidents [20]. Moreover, the study [21] showed that adolescents who use online security measures such as strong passwords and regular updates of security software are less likely to be at risk of cyber victimization. [12] also confirmed the inverse relationship between online protection and cyber victimization. Researchers emphasize that educating and promoting a culture of cyber security can effectively reduce cyber victimization.

Additionally, deviant online lifestyles are emerging as a new phenomenon in modern societies. This concept involves using information technology to facilitate and support activities such as sexual trafficking, drug consumption, and sexual communication [22]. These behaviors are widely conducted through websites, mobile applications, and social networks, posing serious risks to young people, including Cybervictimization [23]. In other words, deviant or risky online activities, such as participating in provocative discussions, communicating with strangers, sharing sensitive information, or engaging in illegal activities, can directly or indirectly lead to cyber victimization. Studies [24, 25] showed that deviant online behaviors, such as downloading illegal content, participating in risky online forums, and sharing sensitive information, can increase the risk of cyber victimization. Moreover, [26] demonstrated that risky online behaviors, such as communicating with strangers and sharing personal information, can

significantly increase the risk of cyber victimization. In Iran, research [12] on deviant online lifestyles and the online proximity of offenders, as well as [27] on the etiology of women's cyber victimization on social networks, highlighted the impact of lifestyle, interactions, choices of a female user, and social pressure on her cyber victimization.

Based on the above discussions, the primary objective of this study is to analyze the risk factors and provocative reasons for the phenomenon of cyber victimization.

2. Cyber Victimization: Conceptual Framework

Due to its vastness and anonymity, the virtual space is an ideal environment for cybercrime and victimization. Cyber victimization refers to the experience of being victimized in the online and internet space. This type of victimization includes illegal and destructive actions online that harm individuals or organizations [28]. Accordingly, cyber victimization can encompass various forms of online attacks and harassment, such as sending threatening, insulting, or humiliating messages through social networks, email, or text messages [29], hacking and intrusion: unauthorized access to personal information, user accounts, and financial information [14], phishing: attempts to obtain sensitive information like passwords and credit card information through deceiving users [30], and disclosure of private information: disclosing individuals' personal information online without their consent [31].

Therefore, cyber victimization is considered a complex and multidimensional phenomenon that requires a deeper understanding of its concepts and related factors [32]. The most important perspectives related to cybercrime and its victims have been discussed in the rational choice theory, opportunity theory, vulnerability theory, and routine activities theory. Rational choice theory assumes that criminals assess the pros and cons before committing a crime. In the context of cyber victimization, cyber criminals seek low-risk, high-reward goals [33]. Opportunity theory also suggests that existing opportunities to commit a crime play a crucial role in its occurrence. Cyber opportunities such as security weaknesses and unsafe online behaviors can increase cyber victimization. Vulnerability theory examines characteristics and conditions that make individuals or systems vulnerable. According to this theory, individuals with limited awareness of cyber security or systems with security weaknesses are more vulnerable to cyber victimization [34].

Routine activities theory, proposed by [35], suggests that changes in people's daily activities and lifestyles can influence crime opportunities.

Increased external activities, urbanization, and social changes can lead to increased crime opportunities. Similarly, in the digital world, increased use of the Internet, social networks, and new technologies provide more opportunities for cybercrimes. According to these researchers, for cybercrimes to occur, there is a need for motivated criminals, suitable targets, and a lack of online protection, emphasizing environmental conditions and available opportunities for crime instead of focusing on individual characteristics of criminals. In the context of cyber victimization, cyber criminals such as hackers and internet fraudsters or others motivated by financial gain, revenge, or simply for recreation and challenge, use technical skills to achieve their online goals. Suitable targets in cyberspace can include personal or financial information, user accounts, sensitive corporate information, and other high-value data. In other words, the attractiveness of online targets can depend on factors such as information value, level of information protection, and ease of access.

In this theory, lack of online protection means insufficient security measures including not using antivirus software, weak passwords, not updating systems and software, and risky online behaviors. In this regard, consider a person who frequently uses social networks and shares personal information publicly. This behavior makes them a suitable target for cybercriminals. If this person does not use proper security measures such as strong passwords, two-factor authentication, and antivirus software, they become unprotected. As a result, this person can easily become a victim of phishing attacks or identity theft.

Based on the above theories, routine activities theory can be used as a theoretical framework to understand and explain cyber victimization behaviors in the digital age, helping to examine opportunities, targets, and criminal behaviors in cyberspace. In other words, in the context of cyber victimization, this theory explains how everyday online behaviors such as using social networks and sharing personal information can turn an individual into a suitable target for cybercriminals.

By adopting routine activities theory as a theoretical framework, cyber victimization can be seen as influenced by various factors, each of which can increase the risk of victimization in the virtual space. One of these factors is the attractiveness of online targets. Online target attractiveness includes features such as valuable personal information or financial resources that make an individual or system an attractive target for cybercriminals [36]. In other words, the attractiveness of online targets can be understood as valuable assets or easily accessible information. In the context of online harassment, information such as email addresses,

phone numbers, or photos can increase the attractiveness of a target [34]. Increasing the attractiveness of online targets leads to an increased risk of cyber victimization.

Another factor is online protection. The level of protective and security measures individuals take to protect their information and systems plays a crucial role in reducing the risk of cyber victimization. The effectiveness of protective and security measures that individuals implement to safeguard their information and systems plays a critical role in reducing the risk of cyber victimization. Recent advancements in cyber security, including the adoption of strong passwords, updated antivirus software, and robust privacy settings, have been shown to significantly mitigate the likelihood of cyber incidents. For instance, the implementation of multi-factor authentication (MFA) and regular updates to security protocols are increasingly recognized as essential practices for enhancing online security and privacy [37, 38]. Also, being exposed to the view of motivated offenders means facing cyber threats from individuals seeking specific goals of intrusion and access to sensitive information, including other influential factors in cyber victimization. Motivated offenders may be after financial gain, data theft, or even system destruction. [39], in his book "Cyber Crime: Key Issues and Debates," states that with the development of technology and the increase in the use of internet-connected devices, new opportunities for misuse by cybercriminals have emerged. The amount of online interactions and internet activities can expose individuals more to cybercriminals. Users with extensive online activities and active presence on social networks are more at risk of cyber victimization [40].

Deviant lifestyles include behaviors such as visiting untrustworthy websites, downloading illegal content, and sharing personal information. These behaviors significantly increase the risk of cyber victimization. Recent research indicates that risky online activities, including clicking on unknown links and interacting with strangers, can lead to cyber victimization and inflict serious harm on users [41, 42]. According to [39], irresponsible and insecure online behaviors can expose individuals to risks such as hacking, identity theft, and misuse of information.

Based on the above discussions, in this study, variables such as online target attractiveness, online protection, exposure to motivated offenders, deviant lifestyle, and risky offline activities are considered risky factors and motivating reasons in the phenomenon of cyber victimization.

3. Research Method

This study is a social survey based on random sampling from the population of Kashan citizens. This method was chosen to ensure sample diversity and to reduce potential biases in the data. Additionally, all participants completed the questionnaire with full awareness of the study's purpose and with assurance of the confidentiality of their personal information. The sample size was estimated at 384 individuals according to Cochran's formula. In total, 400 questionnaires were collected online from the statistical community. In this study, inspired by [34], the scale of each variable is designed in the form of a 4-option Likert spectrum (never, rarely, sometimes, and often). The results of Cronbach's alpha coefficient for all scales were above 70%, indicating high internal consistency among the scales.

It is worth noting that: The operational definitions employed in this study, focusing on online behaviors and specific indicators such as "cyber victimization," "risky online activities," and "online protection," are generally aligned with the concepts found in global data protection and privacy laws, such as the GDPR in the European Union and relevant regulations in Iran. For instance, GDPR, with its emphasis on privacy and data protection, directly relates to concepts like "online protection" and "exposure to motivated offenders." Similarly, in Iran, cybercrime laws, such as the Computer Crimes Law of 2009, cover aspects related to cyber victimization and personal data protection. The operational definitions used in the present study are aligned with these legal definitions due to their focus on these fundamental legal principles.

4. Research Findings

According to the research findings, 37.5% of respondents were male and 62.5% were female. The average age of the respondents is 27.39 ± 7.47 years. 3.3% of the respondents had primary education, 50% had diplomas and associate degrees, 36% had bachelor's degrees, and 10.8% had master's and doctoral degrees. 48% of the respondents were unemployed and 52% were employed. Additionally, 55.3% of them were single, 39.5% were married, and 5.2% were divorced.

4.1. Research Variables

The distribution of dependent and independent research variables is presented in Table 1.

The findings in Table 1 represent the indices of dispersion for the independent and dependent variables of the research. The average of cyber victimization is 99.20 (with a minimum of 15 and a maximum of 46), with a standard deviation of 77.4.

In the next section, a hypothesis test is conducted based on the presence of a dialectical relationship between the independent variables of the research and the level of cyber victimization using the Pearson correlation coefficient.

Based on the findings of the Table 2, there is a significant relationship between the independent variables of online protection, online proximity to motivational offenders, risky online activities, and attractiveness of online targets, deviant lifestyle, and the level of cyber victimization. Among these variables, the intensity of the correlation between online proximity to motivational offenders and cyber victimization is higher than that of other independent variables ($r = 0.505$, $sig = 0.000$). In other words, as individuals' online proximity to motivational offenders increases (including indicators such as allowing others to find them on social media networks, using online services (friend-finding apps) to connect with friends on social media, getting to know more about those with whom they have formed virtual friendships, and having face-to-face meetings with those they have befriended online), their level of cyber victimization also increases. The high intensity of this relationship underscores the potential importance of online proximity to motivational offenders in explaining cyber victimization.

Conversely, there is a significant inverse relationship between the level of online protection (including setting social network or blog access restrictions, using profile trackers to see who has

viewed their profile picture, equipping computers with antivirus software, not opening emails from unknown senders, using different passwords for different accounts, and ensuring the reliability of online sellers in internet purchases) and the level of cyber victimization.

Path Analysis: Path analysis is a statistical technique used to examine relationships among observed variables. This method allows researchers to build more complex models compared to traditional regression methods and analyze the direct and indirect effects of variables on each other. AMOS software is a powerful tool for conducting path analysis, enabling estimation, and evaluation of structural equation models. In this study, path analysis was performed using AMOS 23. The results of the model testing are presented in the following diagram and table.

Based on the model and Table 3, the relative chi-square index indicates a good fit of the model ($CMIN/DF = 1.494/3 < 3$). According to the path analysis results, all comparative fit indices are above 0.90 ($CFI = 0.900$, $GFI = 0.900$, $IFI > 0.900$). Additionally, the RMSEA value of 0.035 indicates an acceptable model fit. Overall, it can be expected that 37% of the variance in cyber victimization can be explained using linear combinations of the independent variables present in the model.

Furthermore, according to the results, the relationship between all variables included in the model and the level of cyber victimization is significant.

- Online Proximity to Motivational Offenders -> Cybervictimization: 0.711 (SE = 0.106, $t = 7.256$, $p < 0.001$)
- Attractiveness of Online Targets -> Cybervictimization: 0.144 (SE = 0.058, $t = 4.762$, $p = 0.014$)

Table 1. Distribution of Variables

Index	Variables	Min	Max	Range	Mean	SD
	Online Protection	19	34	15	24.27	2.89
	Online Proximity	4	14	10	7.45	2.08
	Risky Activity	5	16	11	7.25	1.81
	Online Target Attractiveness	8	25	17	14.35	3.40
	Exposure to Motivated Offenders' View	6	14	8	10.03	1.33
	Deviant Lifestyle	6	16	10	9.32	1.62
	Cyber victimization	15	46	31	20.99	4.77

Table 2. Pearson Correlation Coefficient Results for the Relationship between Independent Variables and the Level of Cyber Victimization

Cyber victimization	r	Online Protection	Online Proximity	Risky Activity	Online Target Attractiveness	Exposure to Motivated Offenders' View	Deviant Lifestyle
		Sig	-0.359 0.000	0.505 0.009	0.404 0.000	0.134 0.007	0.020 0.695

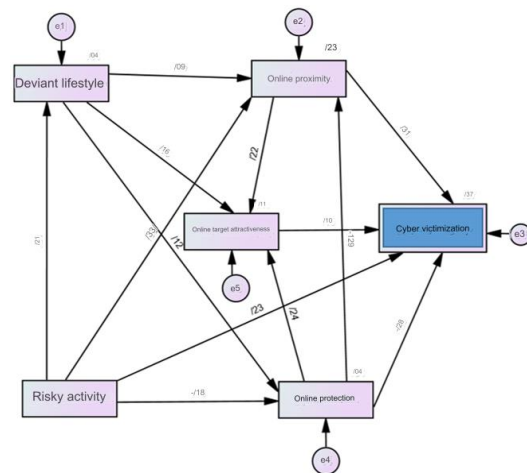


Figure 1. Path Analysis Model of Risk Factors and Motivational Triggers in Cyber Victimization

Table 3. Standard Estimate Values between Variables, Effects of Independent Variables on Cyber Victimization, and Model Fit Indices

<i>Endogenous variable</i>		<i>Exogenous variable</i>			<i>Estimate</i>	<i>S.E.</i>	<i>C.R.</i>	<i>P</i>	
Deviant lifestyle <-- Offline risky behaviors					0/188	0/044	4/272	***	
Online protection <-- Offline risky behaviors					-0/282	0/080	-3/508	***	
Online protection <-- Deviant lifestyle					0/222	0/089	2/487	0/013	
Online proximity to motivated offenders <-- Deviant lifestyle					0/114	0/058	1/968	0/049	
Online proximity to motivated offenders <-- Online protection					-0/206	0/032	-6/421	***	
Online proximity to motivated offenders <-- Offline risky behaviors					0/374	0/052	7/144	***	
Online target attractiveness <-- Deviant lifestyle					0/331	0/101	3/293	***	
Online target attractiveness <-- Online proximity to motivated offenders					0/354	0/083	4/273	***	
Online target attractiveness <-- Online protection					0/288	0/059	4/853	***	
Cybervictimization <-- Online proximity to motivated offenders					0/711	0/106	6/725	***	
Cybervictimization <-- Online target attractiveness					0/144	0/058	2/467	0/014	
Cybervictimization <-- Online protection					-0/459	0/072	-6/411	***	
Cybervictimization <-- Offline risky behaviors					0/598	0/113	5/272	***	
Total effect		Indirect effect		Direct effect		Variables			
0.002		0.002		-		Deviant Lifestyle			
-0.349		-0.070		-0.279		Online Protection			
0.333		0.022		0.310		Online proximity to motivated			
0.103		-		0.103		Online target attractiveness			
0.398		0.170		0.227		Offline risky behaviors			
PCLOSE	RMSEA	CMIN/DF	IFI	RFI	NFI	GFI	CFI	TLI	The goodness of Fit index
0.513	0.035	1.494	0.997	0.940	0.992	0.998	0.997	0.979	

- Online Protection -> Cybervictimization: -0.459 (SE = 0.072, t = -6.116, p < 0.001)
- Risky Offline Activities -> Cybervictimization: 0.598 (SE = 0.113, t = 5.275, p < 0.001)

5. Conclusion

Identifying factors that expose individuals to cyber victimization has significant implications for future prevention efforts. One strategy to reduce cyber victimization is to eliminate opportunities for its occurrence. This study has identified several factors that increase the likelihood of cyber victimization. Participation in risky activities (i.e., deviant lifestyles) emerges as a key risk factor for various forms of victimization, including cyber victimization. Aligning with previous work on cyber victimization [43, 31, 27, 12], deviant lifestyles, online interactions, and offenses (such as continuous contact with others, harassment, unwanted sexual advances, threats, hacking, illegal downloads, and sending/receiving sexual images via text messages) can serve as predictors for cyber victimization. Engagement in these activities not only signifies a deviant lifestyle but also exposes individuals to others engaged in such activities, thereby increasing their vulnerability to victimization. The findings of this study further support the hypothesis that engaging in deviant or risky lifestyles increases the likelihood of cyber victimization.

Moreover, based on the results, increased interaction and proximity to motivated offenders and risky situations online elevate the risk of victimization. In the current analysis, measures such as the number of social networks used, daily usage of these networks, online presence during nighttime hours, and the sending of online images serve as indicators for exposure to motivated offenders. All these criteria theoretically contribute to increased opportunities for victimization. For instance, someone who updates their daily information across multiple online social networks interacts with a larger population than someone who maintains and updates only one online account, thereby increasing their vulnerability. Furthermore, the ease and immediacy of sending photos via the internet make pursuit behaviors for causing harm to others in cyberspace relatively straightforward. Past research examining cyber victimization has generally reported that exposure to motivated offenders increases victimization in various forms [44, 45, 46, 47, 48]. The findings of these studies do not align entirely with the current study; indeed, despite the importance of this variable, its relationship with cyber victimization in the studied population did not confirm it. This effect may result from shortcomings in survey methodology or difficulties in implementing theoretical concepts [49].

Online protection refers to activities that individuals can undertake to protect themselves and others from the risks and harms of cyberspace. The theory of activities and daily life posits that the better and more protected the goals are, the less

likely they are to be victimized, and engaging in online protective activities reduces opportunities for cybercriminal activities. In this study, online protection was measured by criteria such as using online profile trackers to monitor those viewing their information, setting social media accounts to restricted or private access, equipping computers with antivirus software, and using different passwords for different accounts. The research results support a significant and negative relationship between this variable and the level of cyber victimization. In this regard, studies by [19, 1, 21] [12, 50] also demonstrate that employing online security measures can reduce the risk of cyber victimization. Additionally, several previous studies have examined user victimization in cyberspace and presented mixed results regarding the effects of online protection [31, 45, 51] [47, 52] have also emphasized the need for greater attention from researchers to details of online protection in activity theory and have found that the current study's findings confirm this issue.

According to the research findings, data and personal information security are among the primary actions in online protection. The use of encryption, precise management of accesses, and regular data backups are measures that can help individuals prevent cyber victimization. Additionally, awareness of online security threats and educating individuals about secure behaviors can help prevent cyber victimization. Training on detecting malicious messages and files, using encryption, and basic security operations can have a significant impact. Furthermore, the use of strong passwords and their regular management can prevent cyber victimization against attacks such as infiltration. Regular security planning and execution, including vulnerability assessment and software updates, also help individuals resist cyber-attacks and prevent victimization. On this basis, it is recommended to implement these measures and effectively benefit from online protection.

Considering the proximity element in activity theory and daily life, increasing closeness and proximity to criminals stimulate an increase in crime and victimization. Indeed, the concept of online proximity can be transferred from physical space to online networks. The results of this study indicate that online proximity to motivated offenders increases the likelihood of victimization in cyberspace. These findings are consistent with previous work, including [45] and [47, 46], which examined victimization from the perspective of activity theory and daily life.

Target attractiveness to offenders and the likelihood of choosing this target for cybercriminal activities are other influential variables in cyber victimization. The significant and positive

relationship between these two variables suggests that individuals who are more attractive to cyber offenders are likely to be more vulnerable to cyber victimization. Research by [15, 16] and [44, 45] have also reported the impact of target attractiveness on the level of cyber victimization.

Part of the empirical evidence, including [45, 53, 54, 47] correlates daily risky activities with various offline victimizations. However, it remains unclear whether such offline risky activities increase susceptibility to online victimization. To examine the effects of offline risky activities, a measurement based on the frequency of attendance at parties, nightclubs, and alcohol and drug consumption was considered. The research results showed that offline risky activities have a significant relationship with cyber victimization.

One of the most important privacy laws that has had a significant impact on online behavior and user security is the GDPR in the European Union. This regulation not only emphasizes the protection of users' personal data but also mandates companies and organizations to handle users' personal information transparently and responsibly. Research indicates that the implementation of GDPR has led to a reduction in data breaches and an increase in user trust in online platforms [55]. The regulation also empowers users to have greater control over their data, which contributes to reducing cyber victimization. For instance, a study by [56] found that increased public awareness of GDPR has led to an increase in protective behaviors among users online, which directly reduces the incidence of cyber victimization.

While the primary focus of this study is on cyber victimization, the findings provide significant implications for criminal justice approaches in the prevention and prosecution of cybercrimes. Specifically, the operational definitions and the data gathered on online behaviors, risky activities, and online protection strategies can inform the development of robust regulatory frameworks that enhance cyber security measures.

The findings can be particularly useful in informing policies and guidelines for online platforms and internet service providers (ISPs). By understanding the behavioral patterns that lead to increased vulnerability to cybercrimes, platforms can implement more effective monitoring and reporting mechanisms. For example, the data could support the creation of algorithms that detect high-risk behaviors or content, triggering preventive actions before a crime occurs. This proactive approach can significantly reduce the incidence of cybercrimes.

Additionally, the study's insights into how individuals protect their online presence can guide

legislative bodies in crafting laws that require more stringent security measures for online platforms. Such laws could mandate the use of advanced encryption, regular security audits, and transparent privacy policies that align with global standards like GDPR.

In the context of criminal prosecution, the study's findings can help legal professionals and law enforcement agencies to better understand the dynamics of cyber victimization. This understanding is crucial for developing effective strategies to prosecute offenders. For instance, the correlation between specific online behaviors and the likelihood of becoming a victim can be used as evidence in legal cases, strengthening the argument for harsher penalties for cybercriminals.

Moreover, the interdisciplinary nature of this study allows for its findings to bridge gaps between cyber security, legal studies, and public policy. This interdisciplinary approach enhances the potential for the study to inform not only legal frameworks but also the operational strategies of platforms that seek to protect their users from cyber threats. As such, the study contributes to a holistic understanding of cybercrime prevention, which is essential for developing comprehensive and effective regulatory responses.

Declarations

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

- [1] S. Hinduja and J. W. Patchin, "Bullying, Cybervictimization, and suicide," *Archives of Suicide Research*, vol. 14, no. 3, pp. 206-221, 2010, <https://doi.org/10.1080/13811118.2010.494133>.
- [2] A. Nocentini, J. Calmaestra, A. Schultze-Krumbholz, H. Scheithauer, R. Ortega, and E. Menesini, "Cybervictimization: Labels, behaviors, and definition in three European countries," *Australian Journal of Guidance & Counselling*, vol. 20, pp. 129-142, 2010, <https://doi.org/10.1375/ajgc.20.2.129>.
- [3] B. E. Palladino, A. Nocentini, and E. Menesini, "Online and offline peer-led models against bullying and Cybervictimization," *Psicothema*, vol. 24, no. 4, pp. 634-639, 2012.
- [4] D. Álvarez-García, J. C. Núñez Pérez, A. Dobarro González, and C. Rodríguez Pérez, "Risk factors associated with cybervictimization in adolescence," *International Journal of Clinical and Health Psychology*, vol. 15, no. 3, pp. 226-235, 2015. <https://doi.org/10.1016/j.ijchp.2015.03.002>.
- [5] M. Malmir and E. Zarrok, "Prevention of cyber victimization," *Crime Prevention Studies*, vol. 1389, no. 17, pp. 59-86, 2011.
- [6] M. Heydarian Dolatabadi and R. Mazaheri Kuhanestani, "A Comparative Study of the Situation of the Victims of Cyber Terrorism in the Light of Iranian Law and International Documents," *Journal of Police International Studies*, vol. 10, no. 38, pp. 115-140, 2019. <https://sid.ir/paper/388624/en>.
- [7] H. Keramati Moez and S. M. Mirkhalili, "Iran's Legislative Criminal Policy Approach and International Documents To Support Vulnerable Children on Social Media," *Journal of Police International Studies*, vol. 11, no. 41, pp. 102-125, 2020. <https://sid.ir/paper/392158/en>.
- [8] N. Sajadi and M. Madadi, "Ways of Prevention and the Role of Public Police Surveillance in Reducing Victimization of Women in Social Networks," *Journal of New Achievements in Human Studies*, vol. 4, no. 44, pp. 103-117, 2021. [in Persian] <https://www.magiran.com/p2393093>.
- [9] F. Moradi Haghighi, B. Shamloo, and A. Saibani, "The Relationship and Status of Passive Jurisdiction in Cyber Crimes with Other Types of Jurisdictions in the Iranian Legal System," *Karagah*, vol. 16, no. 60, pp. 111-132, 2022. [in Persian] <https://doi.org/10.22034/det.2022.1268260.1312>.
- [10] Z. Seydin Borojni, F. Moazen, and A. Beheshti, "Non-criminal prevention of women's victimization in cyber space," *Crime Prevention Studies*, vol. 18, no. 67, pp. 1-17, 2023, <https://doi.org/10.22034/cps.2022.1270136.1516>.
- [11] ENISA, "Youth and Cybersecurity: Trends and Statistics," European Union Agency for Cybersecurity, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/youth-and-cybersecurity-trends-and-statistics>. [Accessed: 14-Sep-2024]
- [12] A. Aliverdina and F. Ghorbanzade Siahkalroodi, "The Sociological Study of Cyberstalking Victimization among Mazandaran University Students," *Social Problems of Iran*, vol. 10, no. 1, pp. 145-169, 2019. <http://jspi.khu.ac.ir/article-1-2917-fa.html>.
- [13] R. A. Bonanno and S. Hymel, "Cybervictimization and internalizing difficulties: Above and beyond the impact of traditional forms of bullying," *Journal of Youth and Adolescence*, vol. 42, pp. 685-697, 2013. <http://dx.doi.org/10.1007/s10964-013-9937-1>.
- [14] B. W. Reynolds, B. Henson, and B. S. Fisher, "Being pursued online: Applying cyber lifestyle-routine activities theory to cyberstalking victimization," *Criminal Justice and Behavior*, vol. 38, no. 11, pp. 1149-1169, 2011. <https://doi.org/10.1177/0093854811421448>.
- [15] K. Van Royen, K. Poels, W. Daelemans, and H. Vandebosch, "Developing and evaluating a tool to prevent Cybervictimization: A participatory design approach," *Computers in Human Behavior*, vol. 69, pp. 97-107, 2017. [Online]. Available: <https://doi.org/10.1016/j.chb.2016.12.033>.
- [16] K. Thomas, C. Grier, and V. Paxson, "Consequences of connectivity: Characterizing account hijacking on social networks," in *Proceedings of the 2013 Conference on Internet Measurement Conference*, pp. 219-230, 2013. [Online]. Available: <https://dl.acm.org/doi/10.1145/2504730.2504734>.
- [17] Norton, "How to protect personal information online: A 15-step guide," 2022. <https://us.norton.com>.
- [18] Aura, "How to protect your personal information & privacy online," 2023. <https://www.aura.com>.
- [19] M. C. Martínez-Monteagudo, B. Delgado, J. M. García-Fernández, and C. Ruíz-Esteban, "Cybervictimization and social anxiety: A latent class analysis among Spanish adolescents," *International Journal of Environmental Research and Public Health*, vol. 17, no. 12, p. 4369, 2020, <https://doi.org/10.3390/ijerph17020406>.
- [20] M. Bada, M. A. Sasse, and J. R. C. Nurse, "Cybersecurity Awareness and Behavioral Interventions: A Review of Recent Findings," *Computers & Security*, vol. 112, pp. 102365, 2023. DOI: 10.1016/j.cose.2023.102365
- [21] S. Wachs and M. F. Wright, "The Moderation of Online Disinhibition and Sex on the Relationship Between Online Hate Victimization and Perpetration," *Cyberpsychology*,

- Behavior, and Social Networking*, vol. 22, no. 5, pp. 300-306, 2019, <https://doi.org/10.1089/cyber.2018.0551>.
- [22] A. Hayes, "Online deviant lifestyle as an emerging phenomenon in modern societies," in *Handbook of Online Deviant Lifestyle*, J. Allen, Ed. Springer, 2020.
- [23] B. Smith, "These behaviors are widely conducted through computer websites, mobile applications, and social networks, creating serious risks for youth and adolescents," in *Handbook of Online Deviant Lifestyle*, J. Allen, Ed. Springer, 2019.
- [24] T. J. Holt and A. M. Bossler, *Cybercrime: Causes, Correlates, and Context*, SAGE Publications, 2018.
- [25] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *Journal of Research in Crime and Delinquency*, vol. 47, no. 3, pp. 267-296, 2010, <https://doi.org/10.1177/0022427810365903>.
- [26] G. S. Mesch, "Parental mediation, online activities, and Cybervictimization," *CyberPsychology & Behavior*, vol. 12, no. 4, pp. 387-393, 2009, <https://doi.org/10.1089/cpb.2009.0068>.
- [27] M. A. Haji Deh Abadi and E. Salimi, "The Etiology of Women's Victimization in Social Networks," *Journal of Woman & Society*, vol. 9, no. 3, pp. 117-142, 2018, [20.1001.1.20088566.1397.9.35.6.4](https://doi.org/10.1001.1.20088566.1397.9.35.6.4).
- [28] T. J. Holt and A. M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*, Routledge, p. 23, 2016, <https://doi.org/10.4324/9781315775944>.
- [29] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett, "Cybervictimization: Its nature and impact in secondary school pupils," *Journal of Child Psychology and Psychiatry*, vol. 49, no. 4, pp. 376-385, 2008, <https://doi.org/10.1111/j.1469-7610.2007.01846.x>.
- [30] W. Hong and J. Y. L. Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly*, vol. 37, no. 1, pp. 275-298, 2013, <http://www.jstor.org/stable/43825946>.
- [31] A. M. Bossler and T. J. Holt, "Online activities, guardianship, and malware infection: An examination of routine activities theory," *International Journal of Cyber Criminology*, vol. 3, no. 1, pp. 400-420, 2009.
- [32] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, 2000.
- [33] D. Cornish and R. V. Clarke, "Opportunities, precipitators, and criminal decisions: A reply to Wortley's critique of situational crime prevention," In M. J. Smith and D. Cornish, Eds., *Theory for Practice in Situational Crime Prevention*, *Crime Prevention Studies*, vol. 16, pp. 111-124. Monsey, NY: Criminal Justice Press, 2003.
- [34] B. W. Reynolds, *Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective*, Ph.D. dissertation, Graduate School of the University of Cincinnati, Cincinnati, OH, 2010, http://rave.ohiolink.edu/etdc/view?acc_num=ucin1273840781.
- [35] L. E. Cohen and M. Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, vol. 44, no. 4, pp. 588-608, 1979, <https://doi.org/10.2307/2094589>.
- [36] M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *European Journal of Criminology*, vol. 2, no. 4, p. 427, 2005, <https://doi.org/10.1177/147737080556056>.
- [37] Sharma, R., Kumar, A. and Masih, S. (2014) Knowledge and Practice of Primary School Teachers about First Aid Management of Selected Minor Injuries among Children. *International Journal of Medicine and Public Health*, 4, 458. <https://doi.org/10.4103/2230-8598.144114>
- [38] C. Anderson, *The Long Tail: Why the Future of Business Is Selling Less of More*. Hyperion, 2006.
- [39] A. A. Gillespie, *Cybercrime: Key issues and debates*, 2nd ed. Routledge, 2019.
- [40] T. J. Holt and A. M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," *Deviant Behavior*, vol. 30, no. 1, p. 115, 2013, <https://doi.org/10.1080/01639620701876577>.
- [41] R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and M. R. Lattanner, "Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth," *Psychological Bulletin*, vol. 140, no. 4, pp. 1073-1137, 2014. [Online]. Available: <https://doi.org/10.1037/a0035618>.
- [42] S. Alavi and M. Rakesh, "A Review on Cybersecurity Threats and Mitigation Strategies in IoT," *Journal of Cybersecurity*, vol. 22, no. 3, pp. 112-125, 2023. [Online]. Available: <https://doi.org/10.1093/cyber/czab018>.
- [43] K. Choi, "Computer crime victimization and integrated theory: An empirical assessment," *International Journal of Cyber Criminology*, vol. 2, pp. 308-333, 2008.
- [44] B. S. Fisher, F. T. Cullen, and M. G. Turner, "Being pursued: Stalking victimization in a national study of college women," *Criminology & Public Policy*, vol. 1, pp. 257-308, 2002, <https://doi.org/10.1111/j.1745-9133.2002.tb00091.x>
- [45] B. S. Fisher, J. J. Sloan, F. T. Cullen, and C. Lu, "Crime in the ivory tower: Level and sources of student victimization," *Criminology*, vol. 36, no. 3, pp. 671-710, 1998, <https://doi.org/10.1111/j.1745-9125.1998.tb01262.x>
- [46] E. E. Mustaine and R. Tewksbury, "Sexual assault of college women: A feminist interpretation of a routine activities analysis," *Criminal Justice Review*, vol. 27, pp. 89-123, 2002, <https://doi.org/10.1177/073401680202700106>.
- [47] E. E. Mustaine and R. Tewksbury, "A routine activity theory explanation for women's stalking victimizations," *Violence Against Women*, vol. 5, pp. 43-62, 1999, <https://doi.org/10.1177/10778019922181149>.
- [48] L. E. Cohen, J. R. Kluegel, and K. C. Land, "Social inequality and predatory criminal victimization: An exposition and test of a formal theory," *American Sociological Review*, vol. 46, pp. 505-524, 1981, <https://doi.org/10.2307/2094935>.
- [49] J. R. Dunham and K. M. Monk, "Evolution or de-evolution? Assessing target attractiveness: A review of the development and measurement," Poster session presented at the annual meeting of the Academy of Criminal Justice Sciences, Boston, MA, Mar. 2009.
- [50] M. Jami Pour, M. Faraz Pour, and M. Asadi, "Investigating the Relationship between Cyber Skills and Cyber Victim Rate," *Intelligence and Criminal Research Journal*, vol. 15, no. 59, pp. 107-134, 2021, <https://doi.org/20.1001.1.17359367.1399.15.3.5.0>.
- [51] C. D. Marcum, *Adolescent Online Victimization: A Test of Routine Activities Theory*, El Paso, TX: LFB Scholarly Publishing, 2009.
- [52] D. M. Reynald, "Guardianship in action: Developing a new tool for measurement," *Crime Prevention & Community Safety*, vol. 11, pp. 1-2, 2009, <https://doi.org/10.1057/cpcs.2008.19>.
- [53] G. F. Jensen and D. Brownfield, "Gender, lifestyles, and victimization: Beyond routine activity," *Violence and Victims*, vol. 1, pp. 85-99, 1998, <https://doi.org/10.1891/0886-6708.1.2.85>.
- [54] B. Henson, P. Wilcox, B. W. Reynolds, and F. T. Cullen, "Gender, adolescent lifestyles, and violent victimization: Implications for routine activity theory," *Victims & Offenders*, vol. 5, no. 4, pp. 303-328, 2010, <https://doi.org/10.1080/15564886.2010.509651>.
- [55] T. Unal, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs," *Computer Law & Security Review*, vol. 36, no. 5, pp. 105454, Sep. 2020. [Online]. Available: <https://doi.org/10.1016/j.clsr.2020.105454>

- [56] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, "Online Behavioral Advertising: A Literature Review and Research Agenda," *Journal of Advertising*, vol. 46, no. 3, pp. 363-376, 2017. [Online]. Available: <https://doi.org/10.1080/00913367.2017.1339368>



Elham Shafaiimoghadam is an Assistant Professor in the Department of Social Sciences at the University of Kashan. She received her Bachelor's, Master's, and Ph.D. (2017) degrees in Social Sciences Research, Cultural Studies, and the Study of Social Issues in Iran, respectively, from the University of Kashan, Kashan, Iran. Her research interests include the study of social issues using quantitative techniques.



Zahra Baratian Hevdani obtained their Bachelor's degrees in Social Sciences Research from the University of Kashan, Kashan, Iran, in 2024.



Saeideh Mirzaei Khondabi obtained their Bachelor's degrees in Social Sciences Research from the University of Kashan, Kashan, Iran, in 2024.