# Unveiling the Dimensions of Cybercrime Victimization: An Exploratory Factor Analysis

**Cristian C. Reyes, Marielle Joy T. Orong, Melvin P. Padao Jr., Cherryfe E. Pendang**

**College of Criminal Justice Education, University of Mindanao**

**DOI: https://dx.doi.org/10.47772/IJRISS.2025.90700023**

**Received: 02 June 2025; Accepted: 02 July 2025; Published: 28 July 2025**

## ABSTRACT

This study aimed to develop a multidimensional framework for understanding cybercrime victimization among first-year college students at the University of Mindanao. A quantitative, non-experimental research design was employed, incorporating Exploratory Factor Analysis (EFA) to identify patterns in cybercrime experiences. A researcher-developed 40-item survey instrument was used, based on relevant literature and in-depth surveys with students. Content validity was assessed using the Content Validity Ratio (CVR), with ten experts reviewing the items. Only items that met the 0.80 CVR threshold were retained. The final instrument was administered to 300 first-year students in Davao City. EFA results revealed several key dimensions of cybercrime victimization: Cyber Intrusion & Harassment, Risky Online Behavior, Online Piracy Risks, Security Risks in Digital Interactions, Exposure to Fraud & Online Harassment, Online Content & Download Risks, Personal Security & Impersonation Risks, Threats & Unsafe Software Practices, Online Romance & Account Security Risks, Sharing Sensitive Information Online, Risky Digital Practices, and Negligence in Online Behavior. These findings offer valuable insights into how students experience cybercrime and highlight critical areas for intervention. The framework can support the development of targeted policies and institutional strategies aligned with peacekeeping and crime prevention efforts.

**Keywords:** criminal justice, cybercrime victimization, exploratory factor analysis, Philippines

## INTRODUCTION

Cybercrime victimization has become a pressing concern in Davao City as more individuals and businesses fall prey to online threats such as hacking, identity theft, and fraud. Balatero and Guinto (2023) emphasized that the increasing use of the internet and digital transactions has provided new avenues for cybercriminals, resulting in a surge in cybercrime incidents. Citizens with low cybersecurity awareness are particularly vulnerable, and the lack of adequate law enforcement response and digital forensic expertise further complicates justice for victims.

Like many developing countries, the Philippines continues to face challenges in addressing illegal cyber activities and protecting victims. Cybercrimes can involve espionage, sabotage, politically motivated attacks, and terrorism-related offenses, which pose serious risks to national security. Terrorist groups also exploit the internet for propaganda, recruitment, funding, and operational planning (Balatero & Guinto, 2023). Financially driven cybercrimes include scams, fraud, counterfeiting, and identity theft (Smith, 2023), while crimes against individuals may involve threats, harassment, and privacy breaches. Property-related cybercrimes include unauthorized use or destruction of digital assets, and those impacting public morality often involve child pornography, trafficking, and the dissemination of violent content (Ho & Luong, 2022).

Cybercrime broadly refers to any criminal activity that takes place in or is facilitated by virtual environments (Yar & Steinmetz, 2019). These include new crime forms enabled by modern technology and traditional crimes adapted to digital platforms (Drew, 2020). Although younger individuals are more frequently targeted (Reyns et al., 2019), existing studies often neglect other age groups. More importantly, few studies explore the latent dimensions of cybercrime victimization using exploratory factor analysis (EFA), which could reveal the underlying structures that drive risk and exposure.

Most prior research tends to focus on isolated factors, overlooking the complex interrelationships between victim behaviors and vulnerabilities. This study addresses that gap by identifying and categorizing the key dimensions of cybercrime victimization through EFA. A clearer understanding of these factors can inform targeted prevention, intervention, and support strategies.

While some scholars argue that online activity patterns are central to victimization (Kaakinen et al., 2021), others emphasize how visibility, guardianship, and protective behaviors (Álvarez-García et al., 2019) influence risk. Moreover, few studies examine how self-control influences cybervictimization beyond routine online activities. While Whitty (2019) links impulsivity and sensation seeking to increased fraud vulnerability, others, such as Holt et al. (2020), found mixed results regarding self-control and susceptibility to hacking or harassment, an area not directly explored in this research.

The study was significant for several reasons. First, this is beneficial to the respondents of the study. This would serve as a caution to them to be vigilant when it comes to utilizing different media platforms on the internet. Second, this was beneficial to the different organizations, specifically to the PNP Anti-Cybercrime Group, as this would produce data about cybercrime and would be able to formulate preventive measures to be conducted by their different departments and respective jurisdictions. Third, this was beneficial to the users in general, whether it be on social media or other internet platforms. This would serve as a wake-up call, so that we should take more responsibility and be knowledgeable enough to avoid being exposed to it. Lastly, future researchers were one of the beneficiaries as they could use the data and information of this study for their future purposes. They could utilize all the details to conduct a study in a wider scope and variety.

Most existing literature tends to examine isolated variables, lacking the multidimensional perspective needed to understand the complex nature of victimization. To address this gap, this study identifies and categorizes latent dimensions of cybercrime victimization using EFA. This approach is like the methodological work of España and Nabe (2023), who developed a context-specific scale for measuring neighborhood crime perceptions. Their work highlights the importance of localized and empirically grounded tools in understanding crime experiences. Just as neighborhood crime scales help tailor community-based interventions, a multidimensional cybercrime victimization framework is critical for formulating digital safety strategies within university settings.

**Research Objectives**

The main objective of this study was to develop a multidimensional framework for understanding the factors that contribute to cybercrime victimization among first-year criminology students at the University of Mindanao. Specifically, it aimed to identify the components influencing victimization experiences and classify them into factor structures (e.g., F1, F2, F3).

**Theoretical Framework**

This study is anchored in the Victimization Risk Model (Mesch, 2009), which suggests that personal traits (e.g., age, gender, internet experience) and risky behaviors (e.g., oversharing, low cybersecurity awareness) increase cybercrime victimization. It is also supported by the Lifestyle Exposure Theory, which proposes that lifestyle choices and online habits influence exposure to potential offenders. Individuals who spend significant time online or engage in digital transactions are at greater risk of victimization (Henson & Reynald, 2016). As digital behaviors once considered safe now carry increased risks, this framework is vital for understanding cybercrime in today's interconnected society.

**Conceptual Framework**

Figure 1 depicts a schematic model of the main measurements or factors of cybercrime victimization at the University of Mindanao, which serves to present the study's conceptual framework. The measures labeled as Factor 1…n indicate the determining factors of the latent constructs. The main variable is in the center of the model, surrounded by the theorized determinants.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue VII July 2025

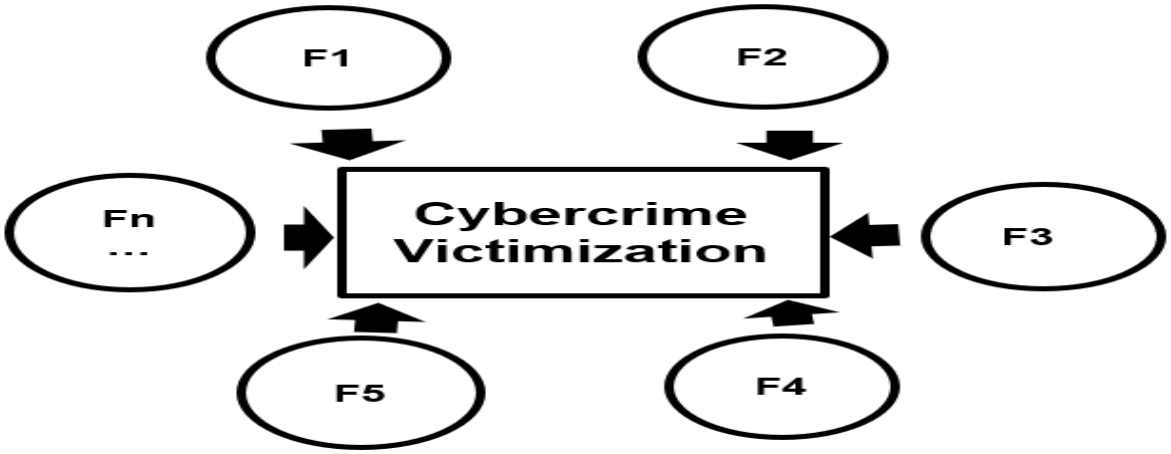


Fig. 1 Conceptual Framework of the study

The main variable in this study is cybercrime victimization, which is operationally defined as the act of victimizing others using information and communication technology, with a specific focus on criminology students at the University of Mindanao. This includes, but is not limited to, cyberstalking, cyber harassment, identity theft, and sexual threats.

## METHODOLOGY

This section outlines the participants, research instruments, procedures, design, and statistical techniques used in the study.

### A. Research Respondents

The participants of the study were 300 first-year criminology students at the University of Mindanao. First-year students were selected due to their limited exposure to university life and digital security measures, which potentially increases their vulnerability to cybercrime victimization compared to upper-year students. A stratified random sampling technique was employed based on ratio and percentage distribution. This method ensured a representative sample across subgroups while remaining time- and cost-efficient. It was chosen for its accessibility, objectivity, and suitability for data collection across a geographically distributed population.

### B. Materials and Instruments

For the material and tools, the main research instrument was a researcher-developed survey questionnaire, designed based on a thorough review of relevant literature. To ensure its content validity, the instrument was evaluated by ten expert validators from the College of Criminal Justice Education using the Content Validity Ratio (CVR) method. Based on the CVR results, 40 out of the original 122 items were retained, while the remaining 82 items were removed. The finalized 40-item questionnaire was administered to the 300 student participants.

To ensure methodological rigor, a systematic process was followed. First, the validity and reliability of the instrument were confirmed with the help of research specialists and the research adviser. Then, a formal request to conduct the study was submitted to Dr. Carmelita B. Chavez, Dean of the College of Criminal Justice Education. Upon approval, informed consent forms were distributed to selected participants, outlining the study's purpose, procedures, and guarantees of confidentiality. Following consent, the questionnaires were distributed, and respondents were given ample time to complete them. After collection, the responses were compiled and prepared for statistical analysis. The final interpretations and discussions based on the data are presented in subsequent sections of this dissertation.

### C. Design and Procedure

The design of this study adopted a quantitative, non-experimental research design, specifically utilizing Exploratory Factor Analysis (EFA) as the primary statistical technique. A non-experimental approach was appropriate as the study sought to describe phenomena and explore relationships among pre-existing variables without manipulation (Salkind, 2010). EFA was selected to identify underlying structures among variables related to cybercrime victimization. To assess the suitability of the data for factor analysis, the Kaiser-Meyer-Olkin (KMO) test was used to measure sampling adequacy, and Bartlett's Test of Sphericity was employed to test the data's factorability (Gonick, 1993). Upon satisfying these requirements, Principal Component Analysis (PCA) was applied to extract factor structures. The factor rotation method—specifically Orthogonal Rotation with Direct Oblimin—was then used to interpret the factor loadings and determine the number of meaningful components. The Percentage of Variance explained by each factor was also calculated to assess the significance of each extracted component (Allen, 2017).

## RESULTS AND DISCUSSION

This section provides the results and analysis of the data obtained. The findings are organized in the following order: measures of sampling adequacy and sphericity, the rotated component matrix, extracted factors describing neighborhood crime in Davao City, the latent roots criterion for the extracted factors, and the framework developed based on the study's findings. Furthermore, a discussion is offered to analyze and explain the findings.

### A. Measures of Sampling Adequacy and Specificity

Table 1 shows the Kaiser-Meyer-Olkin Measure of Sampling Adequacy and Bartlett's Test of Sphericity. The Kaiser-Meyer-Olkin (KMO) statistics are used to determine if the sample size is sufficient for factor analysis (Effendi et al., 2019). According to Kaiser (1974), KMO values greater than 90 are excellent,.80s are commendable,.70s are average,.60s are mediocre,.50s are deplorable, and values less than 5 are undesirable. With a KMO score of 0.777, this study's sample size was declared appropriate and suitable for factor analysis. This reveals a substantial partial correlation between the variables, implying that factor analysis is an appropriate tool for investigating cybercrime victims

Table1. Measures of Sampling Adequacy and Specificity

| **Measurement** | | **Value** |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .777 |
| Bartlett's Test of Sphericity | Approx.$X^2$ | 3292.927 |
| | d*f* | 903 |
| | Sig. | .00 |

The Bartlett's Test of Sphericity evaluates the importance of correlations between all variables in the tool (Effendi et al., 2019). It compares the identity matrix to the observed correlation matrix to look for overlap between variables that can be reduced to a few components. With 903 degrees of freedom, the test produced a p-value of 0.000, demonstrating that the data was multivariate rather than an identity matrix. This finding revealed that factor analysis was the most appropriate technique for identifying the characteristics that characterize cybercrime victimization. The significant p-value indicates that the null hypothesis was rejected, as the correlation matrix was not an identity matrix.

Figure 2 depicts the scree plot produced by the secondary Exploratory Factor Analysis (EFA) undertaken in this study. Cattell (1966) describes the scree plot as using eigenvalues extracted from the correlation matrix. The graphic shows the eigenvalues on the vertical axis and the factors on the horizontal axis. Analysts can visually inspect the plot to detect the "elbow" point, which represents a large reduction in eigenvalue magnitude. This scree plot can help you determine the number of significant components and the variance

explained by each one. The "elbow" is the point at which the decline in eigenvalues becomes severe, suggesting a decrease in their magnitude. This point indicates the number of factors deemed relevant for future investigation. The scree plot clearly shows that the instrument represents a multidimensional framework, as evidenced by the substantial fall in the plotted line after the third factor. Gorsuch (1997) stated that the success of the screen test is dependent on criteria, such as a large sample size and clearly characterized underlying components in the data.

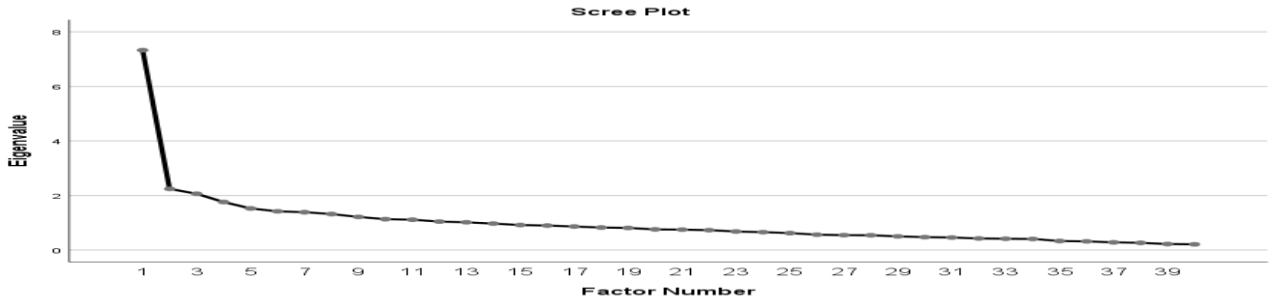


Fig. 2 Scree Plot

Table 2 presents the results of the factor analysis, specifically highlighting the total variance explained by each extracted factor. The table displays the eigenvalues (Total), the percentage of variance each factor contributes individually (% of Variance), and the cumulative percentage of variance accounted for by the successive factors (Cumulative %).

Table2.TotalVarianceExplained

| Factor | Total | % of Variance | Cumulative % |
|---|---|---|---|
| 1 | 7.329 | 18.323 | 18.323 |
| 2 | 2.243 | 5.608 | 23.931 |
| 3 | 2.063 | 5.157 | 29.089 |
| 4 | 1.761 | 4.403 | 33.492 |
| 5 | 1.526 | 3.814 | 37.306 |
| 6 | 1.42 | 3.549 | 40.855 |
| 7 | 1.388 | 3.469 | 44.324 |
| 8 | 1.32 | 3.301 | 47.625 |
| 9 | 1.214 | 3.036 | 50.661 |
| 10 | 1.132 | 2.829 | 53.49 |
| 11 | 1.112 | 2.781 | 56.271 |
| 12 | 1.044 | 2.611 | 58.882 |
| 13 | 1.017 | 2.544 | 61.425 |

Indicated the obtained components along with the proportion of variance that each one explains. The first factor has a total eigenvalue of 7.329 and a variance of 18.323 %. This factor was highly influential and likely captured a significant dimension of cybercrime victimization. The second factor has a total eigenvalue of 2.243 and a variance of 5.608%, bringing the cumulative variance explained to 23.931%. Factor 3 accounts for 5.157% of the variance.

Like factor 2, it represented distinct dimensions of cybercrime victimization but with slightly smaller exploration power. This factor might capture another nuanced aspect of victimization, potentially highlighting

different experiences of perceptions that were distinct from those captured by Factors 1 and 2. The subsequent factors 4-13 have a total eigenvalue that ranges from 1.761 to 1.017. These factors each explain between 2.544 and 4.403 of the variances. By the 13th factor, the cumulative variance explained was 61.425. Although the contribution of each of these to the variance was less than that of the primary factors 1-3, taken as a whole, they provide a more thorough and in-depth understanding of the various ways that people may experience or perceive cybercrime. These variables may have to do with various forms of victimization, particular effects, or differences in demographics when it comes to cybercrime experiences.

**B. Extracted Factors Characterizing Cybercrime Victimization**

The findings of this study affirmed Smith's (2023) research into the characteristics of cybercrime victims, which revealed that people who make online transactions without confirming the seller's legitimacy are particularly prone to fraud and online harassment. This finding in relation to security concerns associated with digital interactions has implications for issues such as submitting important banking information on insecure websites, becoming vulnerable to misinformation, and unauthorized access to social media accounts. These findings emphasized the crucial need for enhanced consumer knowledge and security in online environments.

Table 3. Extracted Factors Characterizing Cybercrime Victimization

| Item | Extracted Dimensions | R-value |
|---|---|---|
| | **Factor 1- Cyber Intrusion & Harassment** | |
| Q14 | I have noticed that information disclosed on websites or social media platforms is more likely to be targeted by cybercriminals. | 0.672 |
| Q10 | I have had my webcam or microphone accessed by unknown websites or applications. | 0.511 |
| Q12 | I have encountered unauthorized purchases made using my financial information online. | 0.494 |
| Q13 | I have experienced being stalked by someone online | 0.454 |
| | **Factor 2- Risky Online Behavior** | |
| Q8 | I have used auto-connect Wi-Fi on public networks. | 0.618 |
| Q31 | I have suffered from financial losses due to cybercrime. | 0.451 |
| Q28 | I watched movies/TV shows on untrusted websites. | 0.432 |
| | **Factor 3- Online Piracy Risks** | |
| Q36 | I have experienced that my pictures or photos are being manipulated online without my permission. | 0.557 |
| Q5 | I have shared intimate or sensitive information with someone online whom I've never met in person. | 0.487 |
| Q2 | I have left my device/social media accounts unattended on public places. | 0.463 |
| | **Factor 4- Security Risks in Digital Interactions** | |
| Q6 | I have entered my banking/e-wallet information on websites that may not have secure systems. | 0.779 |
| Q7 | I have been deceived by fake news or misinformation online | 0.779 |
| Q32 | Someone accessed my social media accounts without my permission | 0.779 |
| | **Factor 5- Exposure to Fraud & Online Harassment** | |
| Q24 | I have engaged in online transactions without verifying the authenticity of the seller or website. | 0.792 |
| Q39 | I have experienced receiving online hate and comments. | 0.702 |
| Q9 | I have experienced cyber bullying or online harassments. | 0.463 |
| | **Factor 6- Online Content & download risks** | |
| Q22 | I downloaded files or attachments from unknown sources | 0.676 |
| Q37 | I experienced that my academic works are being plagiarized by someone online | 0.636 |
| Q4 | I have clicked on suspicious links in emails or pop-up ads. | 0.448 |
| | **Factor 7- Personal Security & Impersonation Risks** | |
| Q20 | I have responded to messages from strangers online. | 0.735 |
| Q18 | I have used the same password for multiple online accounts. | 0.735 |
| Q33 | I have encountered fake profiles or impersonations online. | 0.614 |

| | | |
|---|---|---|
| | **Factor 8- Threats & Unsafe Software Practices** | |
| Q30 | I have engaged in risky online behaviors, such as sexting or sending explicit photos which could be used against me | 0.467 |
| Q25 | I have experienced being threatened by someone online | 0.455 |
| Q16 | I have downloaded software or apps from untrusted sources. | 0.405 |
| | **Factor 9- Online Romance & Account Security Risks** | |
| Q1 | I have logged in to any device without removing my social media account. | 0.764 |
| Q40 | I have been a victim of online romance scams or dating apps. | 0.764 |
| Q38 | I tend to use the "remember password" option in signing in to my social media accounts | 0.764 |
| | **Factor 10- Sharing Sensitive Information Online** | |
| Q23 | I have participated in online surveys or quizzes that requested sensitive information. | 0.711 |
| Q27 | I have given out my phone number or email address to online entities. | 0.618 |
| Q29 | I have shared log-in credentials with friends and family members. | 0.505 |
| | **Factor 11- Risky Digital Practices** | |
| Q3 | I have shared my location or whereabouts on social media. | 0.557 |
| Q11 | I have encountered phishing attempts of websites trying to steal my information | 0.405 |
| Q34 | I tend to insert my flash drive on public internet shops. | 0.63 |
| | **Factor 12- Negligence in Online Security** | |
| Q17 | I have accepted friend requests or connections from people I don't know personally. | 0.766 |
| Q21 | I have entered personal information on websites or forms that may not have had secure encryption protocols. | 0.618 |
| Q19 | I accept the term and conditions in any online platform without reading it. | 0.63 |
| | **Factor 13- Exposure to Cyber Threat** | |
| Q15 | I have posted photos or videos online without considering the potential consequences of them being misused. | 0.448 |
| Q35 | I engaged in online gambling or gaming activities. | 0.448 |
| Q26 | I never attended seminars on cybercrime awareness. | 0.448 |

Table 3 presents the extracted 13 factors that characterize cybercrime victimization. For factor 1: Cyber Intrusion and Harassment, this factor captures direct, intrusive forms of cybercrime that compromise personal security and digital privacy. It includes experiences such as unauthorized webcam access, online stalking, and the misuse of disclosed personal data. Victims often become targets after sharing information on websites or social media platforms. These behaviors reflect a growing concern over digital surveillance and personal vulnerability online. Rachna and Varshney (2024) emphasize that cyberstalking and other forms of online harassment are becoming increasingly sophisticated. It highlights how victims often encounter diverse responses when reporting incidents, ranging from strong support to feeling judged or misunderstood. Meanwhile, in factor 2, Risky online behavior relates to behaviors that, while not inherently criminal, increase vulnerability to cyberattacks. Examples include using auto-connect on public Wi-Fi, watching content on untrusted websites, or suffering financial losses from such behaviors. A study examining cybercrime awareness among Palestinian undergraduate students found that high-risk online behaviors included using social media for social interaction, using mobile apps, engaging in excessive social media use, and failing to report criminal activity to law enforcement authorities (Ahmead et al, 2024). In addition, Factor 3 Online Piracy risk covers the unauthorized use or manipulation of digital media, often involving user-generated content. It includes sharing sensitive material with strangers and leaving devices unattended in public places. Research indicates that online piracy harms creators and rights owners by reducing revenues for their creative works that are available in legal channels. It also negatively impacts both the quantity and quality of creative works available in the marketplace (Smith, 2023).

Unveiling the dimensions of cybercrime victimization also includes the following factors: Factor 4, Security Risks in Digital Interactions, which emphasizes vulnerabilities stemming from insecure digital transactions and online misinformation. It includes entering sensitive financial data on unverified websites, falling for fake news, and unauthorized access to social media accounts. The 2020 Phishing and Fraud Report by F5 Labs highlighted that phishing remains a prevalent threat, with a projected 15% increase in phishing incidents in

2020 compared to the previous year (Warburton, 2020). Phishing continues to be a popular method for organized cybercrime due to its effectiveness. Furthermore, Factor 5 Exposure to Fraud and Online Harassment represents the intersection of financial deception and emotional abuse online. It includes falling for fraudulent online transactions and experiencing hate speech or cyberbullying. The White House Task Force to Address Online Harassment and Abuse reported that online harassment and abuse are increasingly widespread, including online threats and intimidation as well as various forms of technology-facilitated gender-based violence (White House Task Force, 2022). In Factor 6: Online Content and Download Risks, it tackles unsafe downloading behaviors such as accessing unknown files, clicking suspicious links, and experiencing content plagiarism. The Center for Internet Security (2020) reported that malware variants comprised a significant portion of total malware activity, emphasizing the importance of cautious online behavior to mitigate risks.

In addition to the earlier dimensions, Factors 7 to 10 reveal more nuanced behaviors and vulnerabilities that significantly contribute to the complexity of cybercrime investigations, particularly in areas related to personal security, digital negligence, and exposure to emerging online threats. Factor 7: Personal Security and Impersonation Risks captures unsafe digital habits like reusing passwords, responding to strangers, and encountering fake profiles—behaviors that increase the risk of identity theft. Impersonation scams exploit human trust and are increasingly used in social engineering attacks (Sunwest Bank, 2023). Moreover, Factor 8: Threats and Unsafe Software Practices revealed that downloading from untrusted sources, engaging in risky behaviors like sexting, or receiving online threats are grouped under this factor. These actions expose users to malware, ransomware, and online exploitation (NCSC, 2023). In connection with that, Factor 9: Online Romance and Account Security Risks refers to vulnerability to romance scams and poor account security practices, such as saving passwords or leaving accounts logged in. The FBI reported over $600 million in losses to romance scams in 2020 alone (FTC, 2021). Added to this Factor 10: Sharing Sensitive Information Online includes disclosing personal data through quizzes, giving out contact info, or sharing credentials—practices that compromise data privacy. Oversharing personal information online increases the risk of identity theft and fraud (Security.org, 2023).

Factors 11 to 13 emphasize the persistent digital risks stemming from user carelessness, lack of cybersecurity awareness, and unintentional exposure to cyber threats through seemingly harmless online activities. Factor 11: Risky Digital Practices involves sharing locations, using public computers with personal flash drives, and exposure to phishing—habits that compromise both privacy and system security (CurrentWare, 2023). In relation to that, Factor 12: Negligence in Online Security highlights disregard for cybersecurity protocols, such as accepting strangers' friend requests or submitting information on unsecured sites. Negligence like this often leads to system breaches (Leppard Law, 2023). Lastly, Factor 13: Exposure to Cyber Threats includes behaviors like posting sensitive content, gambling online, and lacking cybercrime education, each contributing to digital vulnerability. The gambling sector, for example, faces rising cyber threats (Veracity Trust Network, 2023). Together, these thirteen extracted factors provide a comprehensive framework for understanding the diverse elements influencing cybercrime investigation, highlighting the urgent need for enhanced digital literacy, proactive cybersecurity practices, and targeted law enforcement strategies in the digital age.

**Latent Roots Criterion of the Extracted Factors**

Table 4 presents the latent root criterion, which indicates that after numerous rounds, thirteen (13) dimensions reflecting cybercrime victimization at the University of Mindanao were retrieved from the information submitted for component analysis.

The identified factor structures are as follows: (1) Cyber Intrusion and Harassment, with an initial eigenvalue of 7.329 and a variance of 18.323; (2) Risky Online Behavior, with an initial eigenvalue of 2.243 and a variance of 5.608; (3) Online Piracy Risks, with an initial eigenvalue of 2.063 and a variance of 5.157; (4) Security Risks in Digital Interactions, with an initial eigenvalue of 1.761 and a variance of 4.403; (5) Exposure to Fraud and Online Harassment, with an initial eigenvalue of 1.526 and a variance of 3.814; (6) Online Content and Download Risks (eigenvalue 1.42, variance 3.549), (7) Personal Security and Impersonation Risks (eigenvalue 1.388, variance 3.469), (8) Threats & Unsafe Software Practices (eigenvalue 1.32, variance 3.301), (9) Online Romance & Account Security Risks (eigenvalue 1.214, variance 3.036), and others such as Sharing Sensitive Information Online, Risky Digital Practices, Negligence in Online Security, and Cyber Threat

Exposure. These components exhibited eigenvalues ranging from 1.017 to 1.42, indicating different amounts of variation and emphasizing the many features of cybercrime victimization.

Table4 Latent Roots Criterion of the Extracted Factors

| Factors | Initialized Eigenvalue | Percentage of Variance | Commutative Variance % |
|---|---|---|---|
| Cyber Intrusion & Harassment | 7.329 | 18.323 | 18.323 |
| Risky Online Behavior | 2.243 | 5.608 | 23.931 |
| Online Piracy Risks | 2.063 | 5.157 | 29.089 |
| Security Risks in Digital Interactions | 1.761 | 4.403 | 33.492 |
| Exposure to Fraud & Online Harassment | 1.526 | 3.814 | 37.306 |
| Online Content & Download Risks | 1.42 | 3.549 | 40.855 |
| Personal Security & Impersonation Risks | 1.388 | 3.469 | 44.324 |
| Threats & Unsafe Software Practices | 1.32 | 3.301 | 47.625 |
| Online Romance & Account Security Risks | 1.214 | 3.036 | 50.661 |
| Sharing Sensitive Information Online | 1.132 | 2.829 | 53.49 |
| Risky Digital Practices | 1.112 | 2.781 | 56.271 |
| Negligence in Online Security | 1.044 | 2.611 | 58.882 |
| Exposure to Cyber Threat | 1.017 | 2.544 | 61.425 |

The latent root criteria could be used to determine the outcome of exploratory factor analysis by obtaining the sum of the explained variances. By calculating the eigenvalues of the elements and their individual variances, the total variance explained displays the outcome.

**D. Multidimensional Framework on Cybercrime Victimization**

Cybercrime victimization was characterized by thirteen (13) dimensions, which were illustrated in a thematic framework shown in Figure 2. These factors included the Cyber Intrusion & Harassment, Risky Online Behavior, Online Piracy Risks, Security Risks in Digital Interactions, Exposure to Fraud & Online Harassment, Online Content & Download Risks, Personal Security & Impersonation Risks, Threats & Unsafe Software Practices, Online Romance & Account Security Risks, Sharing Sensitive Information Online, Risky Digital Practices, Negligence in Online Security, Exposure to Cyber Threat. In order to determine which contrasts best explain the clustered components, the researcher thematically analyzed these factor structures. Cybercrime victimization is greatly influenced by these thirteen measures.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue VII July 2025

The thirteen (13) extracted factors were operationally defined in the following: (1) Cyber Intrusion & Harassment refers to incidents that involve unauthorized access to any personal accounts (hacking) that targeted cyberbullying or stalking via social media platform; (2) Risky Online Behavior by engaging activities that significantly increases the vulnerability to cyber threats, such as using public Wi-Fi, clicking links without verifying the sources and oversharing information to any online platform; (3) Online Piracy Risks refers to downloading or sharing copyrighted material can increase the risk of exposure to malware and exploitation that lead to the emergence of cybercrime victimization, (4) Security Risks in Digital Interactions was considered the most undisputed potential risk and vulnerability one was exposed to when performing electronic transactions or activities with information that should not be shared indiscriminately, (5) Exposure to Fraud & Online Harassment, refers to the experience of the respondent when he or she was been victimized through online fraud, harassment, or abuses, including experiencing online transactions not supported by verification if the seller or website was genuine, and also experiences online hate and comments, (6) Online Content & Download Risks the risk of downloading malware or viruses from unknown sources, or having your work plagiarized online.

Personal Security & Impersonation Risks, biggest risks while on the internet, primarily brought about by impersonation or theft of personal information while responding to strangers and poor password use, (8) Threats & Unsafe Software Practices it was getting threatened or scammed online, including downloading the software from unreliable sources, (9) Online Romance & Account Security Risks the risks of being a victim of online romance scams or of account hackers through such practices as weak passwords, fraudulent profiles, and other issues, (10) Sharing Sensitive Information Online The risk of having your sensitive info stolen or exposed online due to sharing personal data either on public Wi-Fi or with unknown individuals, (11) Risky Digital Practices risk of engaging in online behaviors that put you at risk by using public Wi-Fi or downloading software from unknown sources, (12) Negligence in Online Security, this was the risk of being careless when it comes to your online security, not reading or overlooking such terms and condition or disregarding security warnings, (13) Exposure to Cyber Threat, risk of being exposed to an online threat, which involves sensitive information being published online or activities carried out online that expose you to it.

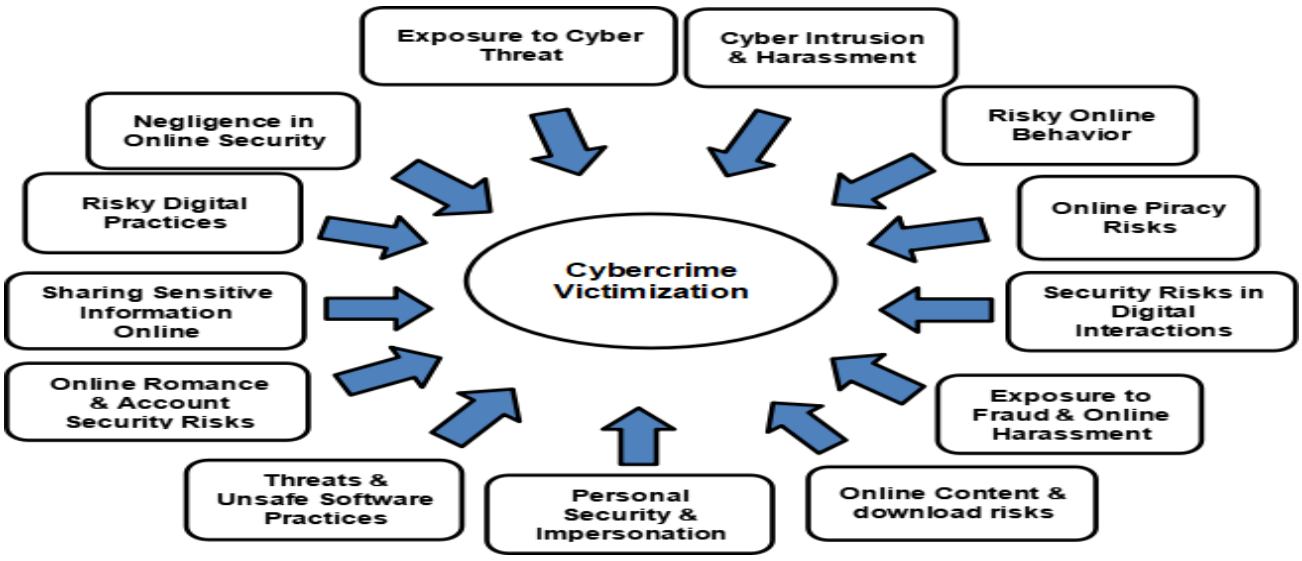


Fig. 3 Thematic Framework on Cybercrime Victimization

Cybercrime refers to both new crimes that emerged with the advent of computers and the internet, as well as traditional crimes that use information communication technology (ICT) for illicit purposes. These crimes are divided into two categories: cyber-dependent crimes, such as hacking, malware, and denial of service assaults, and cyber-enabled crimes, which include phishing, identity theft, online romance scams, and online retail fraud. Cybercrime is classified in a variety of ways, with targets including individuals, groups, computer networks, users, vital infrastructure, and virtual entities. Other classifications include cyber-trespass, cyber-deception, cyber-pornography, and cyber-violence (Wagen & Pieters, 2020).

It also tends to provide a schematic overview of the measurement tool that is being developed. Thus, a description of the development of the measurement tool built from 13 extracted measures of victimization against cybercrime can be seen. By taking this scale, further study on the victimization against cybercrime through other designs or techniques of the research and/or unit of analysis in testing the effectiveness and validity could also be pursued by future researchers.

## CONCLUSION AND RECOMMENDATIONS

Thus, the findings of the study have revealed thirteen dimensions of victimization due to cybercrime, thereby giving meaning to how all those varied ways that people could experience or perceive cybercrime have been captured. The study of the exploratory factor analysis resulted in thirteen (13) factors characterizing cybercrime victimization, which were: Cyber Intrusion and Harassment, Risky Online Behavior, Online Piracy Risks, Security Risks in Digital Interactions, Exposure to Fraud and Online Harassment, Online Content and Download Risks, Personal Security and Impersonation Risks, Sharing Sensitive Information Online, Risky Digital Practice, Negligence in Online Security and Exposure to Cyber Threat. These factors provided reason for the nuances in understanding the complexity of cybercrime victimization, which calls for targeted policies and strategies that address these dimensions.

Based on the results of this research, policymakers and law enforcement agencies are recommended to develop tailored policies and practices against the dimensions selected for their higher disparities related to cybercrime victimization, such as Cyber Intrusion and Harassment, Risky Online Behavior, and Online Piracy Risks. These policies and strategies should focus on the reduction of risk and damage ensuing from cybercrime and support and protection for the victims of cybercrime. Everyone was being called on, in addition, to prudently use the Internet, avoid dangerous behavior online, and take necessary measures to protect personal security and sensitive information.

These would be possible with education and awareness programs that would inform people about the risks and impacts of cybercrime, as well as train them on how to be safe while working online. Victims of cybercrime should report such incidents to school authorities, local law enforcement, or relevant cybercrime units for appropriate action. Also, take protective steps to secure their online presence through updating passwords, enabling two-factor authentication, and keeping a watch on suspicious online activities. Collaborate with law enforcement, cybersecurity experts, and digital platforms to make response mechanisms effective within the campus community against incidents of cybercrime.

Future researchers were also encouraged to look deeper into the associations of factors identified and further establish a comprehensive understanding of cybercrime victimization at the University of Mindanao. These studies are conducting further studies to see the correlations between the factors and to find out any pattern that exists among them. Additionally, subsequent research would assess the effectiveness of policies and strategies recommended and identify areas that need improvement. In essence, the findings from the study constitute a rich display of the dimensions of cybercrime victimization on campus; hence, recommendations that could proffer ways to reduce the risks and impacts of cybercrime would be welcomed. By knowing individuals alike could put their hands together in ensuring a more secure and safer online environment.

## ACKNOWLEDGEMENT

The researcher wishes to offer their heartfelt appreciation to the people named below for their significant assistance and guidance throughout the course of this research.

To the Almighty God, the Creator and Source of All Wisdom, He showered His almighty grace and continued blessings of good health, strength, and drive on the researchers in completing the study.

To the research adviser, Cherryfe E. Pendang, MSCJ, for her unwavering support, patience, and knowledge. Her valuable input and constructive criticism assisted the researchers in refining their ideas and improving the quality of their work. To the panel members, Eduardo C. Berco, MSCrim, and Carmina Beatriz C. Deocampo,

MSCJ, as well as the validators and experts, who imparted their expertise and knowledge in making the instrument valid and reliable.

We are particularly grateful to our Research Coordinator, Irish P. Bandolos, MSCJ, and Dr. Carmelita B. Chavez, Ph.D. Dean of the College of Criminal Justice Education, for allowing us to conduct the research in our department.

To our Statistician, Dr. Exequiel R. Gono, Jr., Ph.D, for his commitment and support in assisting the researchers throughout the statistical analysis process; his expertise in EFA study was instrumental in ensuring the accuracy and validity of the data findings.

## REFERENCES

1. Allen, M. (2017). The SAGE Encyclopedia of Communication Research Methods. SAGE Publications, Inc.
2. Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross-sectional study. Crime Science, 13(1), Article 29. https://doi.org/10.1186/s40163-024-00230-w
3. Álvarez-García, D., Núñez, J. C., González-Castro, P., Rodríguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: The mediating role of impulsivity and high-risk behaviors. Frontiers in Psychology, 10, 1159.
4. Balatero, J. S., & Guinto, A. F. (2023). Cybercrime victimization in Davao City: Trends, impacts, and challenges. Journal of Philippine Cybersecurity, 12(3), 45–58.
5. Cattell, R. B. (1966). The screen test for the number of factors. Multivariate Behavioral Research, 1(2), 245–276.
6. Center for Internet Security. (2020, February). Top 10 Malware – February 2020. https://www.cisecurity.org/insights/blog/top-10-malware-february-2020
7. Current Ware. (2023). What is computer safety? Top 10 tips for employees to stay secure. https://www.currentware.com/blog/safe-computing-tips/
8. Drew, J. M. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. Journal of Criminology Research Policy and Practice, 6(1), 17–33. https://doi.org/10.1108/JCRPP-12-2019-0070
9. Effendi, M., Matore, E. M., Khairani, A. Z., & Adnan, R. (2019). Exploratory factor analysis (EFA) for Adversity Quotient (AQ) instrument among youth. The 4th International Conference on Computing, Mathematics and Statistics, Malaysia.
10. España, C. M., & Nabe, N. C. (2023). A scale development on neighborhood crime in Davao City: An exploratory factor analysis. European Journal of Social Sciences Studies, 8(6).
11. Gonick, L. (1993). The Cartoon Guide to Statistics. Harper Perennial.
12. Gorsuch, R. L. (1997). New procedure for extension analysis in exploratory factor analysis. Educational and Psychological Measurement, 57(5), 725–740.
13. Federal Trade Commission. (2021). Protecting older consumers 2020–2021: A report of the Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2020-2021-report-federal-trade-commission/protecting-older-consumers-report-508.pdf
14. Henson, B., & Reynald, D. M. (2016). Lifestyle exposure theory and cybercrime victimization: An exploration of online risks. Journal of Criminal Justice Studies, 34(2), 177–192. https://doi.org/10.1080/12345678.2016.1234567
15. Ho, H., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. SN Social Sciences, 2(1). https://doi.org/10.1007/s43545-021-00305-4
16. Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. Social Science Computer Review, 38(2), 187–206.
17. Kaakinen, M., Koivula, A., Savolainen, I., Sirola, A., Mikkola, M., Zych, I., Paek, H.-J., & Oksanen, A. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. Aggressive Behavior (Advance online publication).

18. Kaiser, H. F. (1974). An index of factorial simplicity. Psychometrika, 39(1), 31–36.
19. Mesch, G. S. (2009). The social determinants of internet security vulnerability. International Journal of Cyber Criminology, 3(2), 552–566. https://doi.org/10.5281/zenodo.1053540
20. National Cyber Security Centre. (2023). 2023/2024 Cyber Threat Report. https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2024-web
21. Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? American Journal of Criminal Justice, 44(1), 63–82.
22. Rachna, & Varshney, R. (2024). Victims of cyberbullying and cyberstalking: An exploratory study of harassment perpetrated via the Internet. Library Progress International, 44(3).
23. Salkind, N. (2010). Non-experimental design. In Encyclopedia of Research Design.
24. Security.org. (2023). Securing confidential personal data both online and offline. https://www.security.org/resources/guide-securing-confidential-data/
25. Smith, J. A. (2023). Understanding cybercrime victimization: An analysis of online vulnerabilities. Journal of Cybersecurity Research, 12(3), 45–60.
26. Sunwest Bank. (2023, March 2). What is impersonation fraud? https://www.sunwestbank.com/what-is-impersonation-in-social-engineering/
27. The White House. (2022, June 16). Memorandum on the establishment of the White House Task Force to Address Online Harassment and Abuse. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/16/memorandum-on-the-establishment-of-the-white-house-task-force-to-address-online-harassment-and-abuse/
28. Veracity Trust Network. (2025, March 11). Cyber threats for gambling & gaming sector are rising. https://veracitytrustnetwork.com/blog/industry-insight/cyber-threats-for-the-gambling-gaming-sector-are-rising/
29. Warburton, D. (2020). 2020 Phishing and Fraud Report. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report
30. Van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. Australian & New Zealand Journal of Criminology, 53(1), 84–101. https://doi.org/10.1177/00048658211003925es
31. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime, 26(1), 277–292.
32. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications Limited.