Pakistan Journal of Criminology
Vol. 17, No. 01, January—March 2025 (77-96)

The Impact of Digital Literacy on Cybercrime Awareness, Victimization, and Prevention Measures: A Study of Cyberbullying in Saudi Arabia

Shatha Ismaeel[1]

Abstract

This study investigates the relationships among digital literacy, social media utilization, cybercrime victimization, prevention measures, and cyberbullying in Saudi Arabia. The primary aim is to explore how digital literacy influences preventive behaviours and mitigates risks associated with cybercrime and cyberbullying while examining the role of social media engagement. A quantitative research design was employed, utilizing an online survey distributed to 500 active social media users. Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to assess relationships and predictive validity. The findings reveal that digital literacy significantly enhances preventive measures, such as privacy controls and online recognition strategies, while moderately reducing cybercrime victimization. Social media utilization demonstrated a dual impact, increasing exposure to cyberbullying while providing opportunities for implementing preventive behaviours. A strong association was observed between cybercrime victimization and cyberbullying, highlighting the cyclical nature of online harm. Prevention measures were found to mitigate cyberbullying, emphasizing their protective role effectively. The study concludes that promoting digital literacy and awareness of preventive strategies is essential to fostering safer online environments. Policy implications include targeted educational programs and platform-level safety enhancements to address cyber risks.

Keywords: Digital literacy, cybercrime victimization, social media, cyberbullying, prevention measures, Saudi Arabia

Introduction

The stability and the dramatic increase on the internet and social networks have significantly changed communication, trading, and the spread of information globally (Althibyani & Al-Zahrani, 2023). In KSA (Kingdom of Saudi Arabia), where the population has become increasingly connected to the digital sphere, such positive and negative impacts are possible. Literacy concerning digital tools and platforms which enable users to perform their tasks independently and critically, known as digital literacy, is an essential determinant of how a person operates within cyberspace (Alhothali & Enezi, 2023). As cybercrime is gradually becoming a concern worldwide (Barreda, 2022), people lack sufficient knowledge of cyber-attack types, making them vulnerable to incidents like repeated phishing attacks and dangerous cyber-attack methods that target their personal and financial data (Mo et al., 2024).

[1] Dr. Shatha Ismaeel (PHD, LLM) is an Assistant Professor at Prince Mohammad bin Fahd University, AL Khobar, Kingdom of Saudi Arabia where she teaches General Criminal Law, Private Criminal Law and Criminal Procedure Law. Her research focus on criminal law, international criminal law and International humanitarian law. She can be reached by email at sismaeel@pmu.edu.sa and shatha.ismail@yahoo.com , ORCID ID: 0009-0006-1838-5457

Saudi Arabia is among those countries where social media is most popular; its most active platforms include Twitter, Instagram, and Snapchat. According to Alotaibi and Mukred, (2022), Internet usage statistics indicate that more than 93% of youth in Saudi Arab uses the internet and connected with social media. Modern people use social media to communicate, build business connections, and advertise, but they must notice that they have become the perfect environment for cybercriminals. Some of the most frequent types of cybercrimes include what is known as Phishing methods, which include the use of fake emails or messages to unsuspecting members of social media (Al-Badayneh et al., 2024).

Digital competence involves information seeking, consumption, analysis and synthesis, protection and technology assurance (Alhadidi et al. 2024). It is a powerful tool in the fight against cybercrime because it gives the populace the tools necessary to capitalize on secure platforms for developing social relations, educational purposes, and budgeting. However, weak digital literacy can be a significant concern since it raises the risk level for cybercrime. Research has found that those with enhanced levels of computer literacy can identify phishing scams and resist being scammed (Alharbi, 2022). Digital literacy is critical in Saudi Arabia as acceptance and implementation of digital technologies are presented with different literacy levels and awareness (Arpaci & Aslan, 2023). Compared to the younger and technology-literate population, the older and/or less educated citizens remain particularly vulnerable to cybercrime (Mian & Alatawi, 2023; Soroya et al., 2021; Saqf Al Hait, 2023).

Cyberbullying is among the most common cybercrimes in Saudi Arabia; both individual and business entities are vulnerable to Cybercrimes (Krishnan et al., 2023). These attacks always exploit social engineering methods and flexibility based on psychological techniques such as fear and urgency (Ramadan et al., 2024). For instance, hackers may pretend to be other genuine authorities to extort account credentials or monetary information. Due to the high number of users and less business-like and professional approach to communication, social media are currently the most used media for phishing attacks (Umeugo, 2023; Ateyah, 2022). In general, users with a good understanding of cybersecurity concepts are less likely to interact with a potential scam because they immediately see signs of a scam, for instance, a link or sender that is unfamiliar to them (Ateyah, 2022; Abu-Ulbeh et al., 2021).

Research Objectives

This research aims to investigate the intricate relationship between digital literacy and cybercrime, particularly focusing on cyberbullying in Saudi Arabia. Specifically, the study will explore how digital literacy influences cybercrime victimization, preventive measures against cyber risks, and cybercrime awareness. Additionally, the research will analyze the impact of cybercrime victimization on cyberbullying and assess the effectiveness of prevention measures in mitigating cyberbullying incidents.

Literature Review

Digital Literacy

Digital literacy is a multifaceted phenomenon that integrates the capacity to use, participate in, have access to and understand the digital world. Digital literacy,

as defined by the Digital Literacy Framework by Martin in 2006, features cognitive, technical and social-emotional competencies that enable people to be competent in the purposeful and responsible use of digital tools. Vandebosch and Van Cleemput (2009), critical components to students' effective use of social media include locating information, evaluating sources, creating content, and guaranteeing online security when using social media, which I identified. From a social networking perspective, digital literacy can be illustrated as the ability of adequacy to deal with privacy settings, the cost of source credibility, and suffrage associated with undesirable behaviours (Kaur & Saini, 2023).

The Theory of Planned Behavior (Ajzen, 1991) can expand our understanding of how digital literacy affects behaviour. This theory states that whether an individual will follow safe online practice depends on the individual's attitude, perceived behavioural control and subjective norm. Numerous studies show that those with a higher digital literacy tend to be more confident about identifying phishing scams and cyber threats (Rahman et al., 2023). However, this poor digital literacy also means that people cannot distinguish accurate sources from authentic sources and are more likely to fall victim to cybercrime. As digital technologies go mainstream in Saudi Arabia, disparities in digital literacy among the less educated and older population pop up (Lee et al., 2023).

Cybercrime Awareness and Vulnerabilities

Cybercrime awareness is a critical protective factor in mitigating risks associated with online activities because cybercrime awareness is a key protective factor against cyber risk linked to online activities. the Routine Activity Theory (Cohen & Felson, 1979) for a criminological perspective to illustrate the convergence of the motivated offenders, the suitable targets, and the absence of capable guardians in cyberspace. While they are used to create communication and content-sharing channels, social media platforms are, unfortunately, also channels for cyber threats (Conteh & Royer, 2016). Every novel attack can take advantage of the users' trust when it is exploited to phish sensitive information by emulating legitimate entities.

Kayser et al. (2019) researched low digital vigilance levels in users interacting through social media, leading to victimizations. Additionally, digital competencies could protect people by helping them recognise risks, such as fake profiles or suspicious messages (Hadlington & Chivers, 2020). The expansion of Saudi Arabia's digitalization has lent opportunities to vulnerabilities from platforms such as Twitter and Snapchat, emphasizing digital literacy's importance in overcoming cyber threats (Tarrad et al., 2022).

Cyberbullying and Cybercrime Victimization

Cyberbullying represents a pervasive form of cybercrime that exploits digital platforms to harass, intimidate, or harm individuals. The General Strain Theory (Agnew, 1992) posits that exposure to harmful stimuli, such as cyberbullying, can lead to adverse emotional responses, perpetuating cycles of online victimizations. Phishing and cyberbullying often overlap, as both exploit users' lack of awareness and technical skills (Ho et al., 2024). In Saudi Arabia, studies suggest that users frequently fall victim to cyberbullying through deceptive messages or spoofed accounts masquerading as legitimate sources (Dupuis & Jones,

2024). Effective prevention requires technical measures and behavioural interventions rooted in digital literacy. By equipping individuals with the ability to discern fraudulent activities, digital literacy can reduce the likelihood of victimizations (Kim & Lee, 2023).

Cyberbullying and cybercrime victimizations mirror each other in their construction and are both a product of the harmful exploitation of digital spaces. Cybercrime victimizations includes phishing, identity theft, hacking, and online fraud, which can then develop into cyberbullying, that is, harassing, intimidating or harassing someone through digital communication (Mikkola et al., 2024; Ho et al., 2024). Thus, the compromised personal information obtained via phishing can be utilised to impersonate victims and disseminate defamatory content, which can worsen cyberbullying experiences. This link can be understood by the General Strain Theory (Agnew, 1992), which implies that cybercrime incidents can lead to emotional distress or retaliatory behaviours in response, leading to further harm.

Prevention Measures and the Role of Digital Literacy

Cyberspace prevention strategies require a combination of technical safety measures and user behaviour. Technical solutions like firewalls and spam filters cut off many cyber threats, but only if users are aware and take defensive actions (Mikkola et al., 2024). The second strand of literature focuses on building users' capacities to anticipate, withstand, and recover from cyber risks using the Digital Resilience Framework (Umeugo, 2023). Preventive habits like using strong passwords, two-factor authentication and recognising phishing attempts (Kim & Lee, 2023) depend on digital literacy. Saudi Arabia's National Cybersecurity Authority (NCA) campaigns and educational programs have successfully educated people about social marketing campaigns encouraging safe online practices (Abu-Ulbeh et al., 2021). Under our case study, the government should also explore how to use these resources to reach its population. Therefore, the technological and human user interventions in solving this problem are better understood in cyberspace, characterized by openness and complexity. Examples of these efforts emphasize human and technological intervention integration in improving cybersecurity.

Research Framework

Research on digital literacy and cybersecurity is growing, but significant gaps remain. Therefore, based on the literature and research gap study developed research framework as shown in Figure 1, digital literacy, cybercrime awareness, and cyberbullying relationship is required to investigate, because uniqueness in sociocultural norms and technological progress makes Saudi Arabia an enriching environment (Neuhaeusler, 2024), thus relationship among the cybercrime -digital literacy and cyberbullying need to determine. There needs to be more evaluation of the effectiveness of Saudi Arabia's public awareness campaign and digital literacy programs. However, their impact needs to be assessed systematically so that we can identify areas of improvement. Filling such gaps will offer a better understanding of how to design tailor-made interventions to foster digital safety in emerging digital economies.

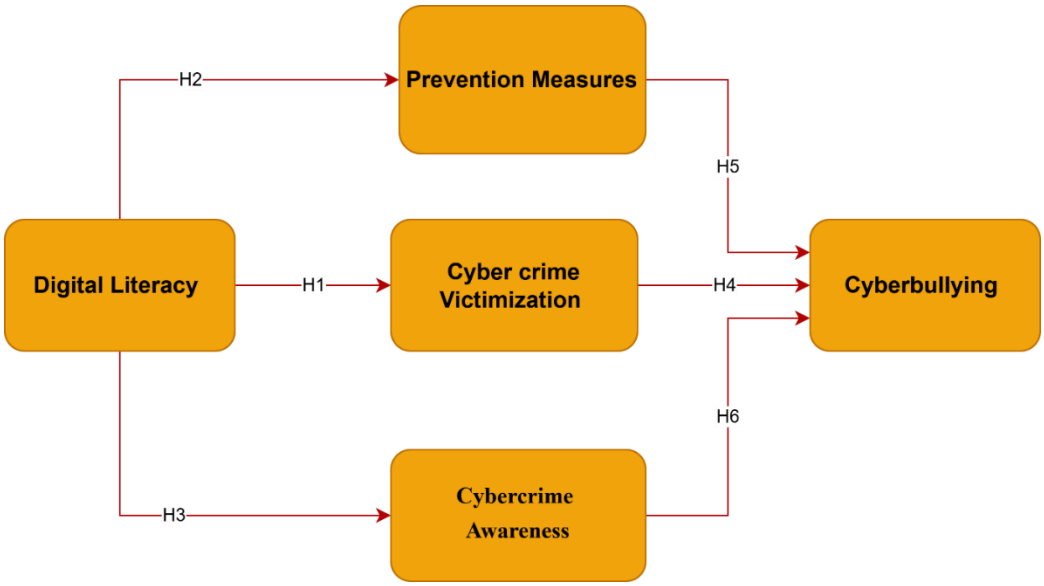

Figure 1. Research Model of Present Study

Methodology

Research Design

This study adopts a quantitative research design to investigate the impact of digital literacy on Cybercrime awareness, victimizations, and the effectiveness of prevention measures in Saudi Arabia. A cross-sectional survey method was employed to collect primary data, aligning to capture diverse perspectives from a broad sample. This approach enables the identification of relationships between variables and the testing of hypotheses through statistical analysis, ensuring the reliability and generalizability of the findings (Creswell, 2014). The study's design also incorporates demographic factors such as age, gender, and education to provide a nuanced understanding of digital literacy's influence in varying contexts.

Population and Sampling

The target population for this study includes Saudi citizens aged 18 and above who are active users of social media platforms such as Twitter, Instagram, and Facebook. Given the digital nature of the research topic, the population was selected to ensure the representation of individuals likely to encounter phishing attacks. A purposive sampling technique was used to recruit participants, ensuring the inclusion of highly digitally literate individuals and those with limited digital literacy. A sample size of 500 respondents was determined to achieve sufficient statistical power, adhering to established guidelines for structural equation modelling (Hair et al., 2014).

Data Collection

Self-administered questionnaires were used to gather data for this study, and respondents were reached through friends' invitations on social media and emails with active social media presence in Saudi Arabia. This study used purposive sampling methods, and an initial screening question was posed at the beginning of the survey concerning the use of social media, where all participants responded positively. The survey consisted of structured questions divided into four sections: Personal data, self-estimation of digital competencies, perceptions of cyber times, and attitude to cyber violence and protection.

The digital literacy scale, adapted from Rodríguez-de-Dios et al. (2016), included 29 items covering six dimensions: Focus areas include technical competencies, informational competencies, communication competencies, content generation competencies, safety competencies, and problem-solving competencies. Cybercrime knowledge was defined by extensity, the number of years participants used the internet, intensity, and the average daily usage in whole numbers from responses provided within ranges. Perceived cyberbullying occurrences were measured by a modified 16-item scale developed by Stewart et al. (2014), whereas preventive behaviour was approximated by the mutuality, recognition and control environment.

Instruments

This study employed well-established and adapted instruments to measure digital literacy, victimisation, Cybercrime awareness and prevention measures. Each instrument was carefully chosen and refined to ensure validity and reliability within Saudi Arabia. The digital literacy scale was adapted from Rodríguez-de-Dios et al. (2016) to assess students' proficiency across six dimensions: technical skills, informational skills, communication skills, content creation, safety, and problem-solving. The scale consisted of 29 items, each evaluated on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

Cybercrime victimisation was measured through two dimensions: "ever victimised" and "frequency of victimisation. Ever Victimised: This dimension captured whether respondents had experienced specific forms of cybercrime. Six binary items asked participants to indicate "yes" (1) or "no" (0) for being victims of the following: hacking, cyber-impersonation, cyberbullying, identity theft, online romance scams, or online fraud. A composite score was calculated as the sum of affirmative responses, which was then recoded into a binary variable: 1 (victimized, with a score of 1–6) or 0 (not victimized, with a score of 0. Response categories included ranges such as "1 to 2 times," "3 to 4 times," and "5 to 6 times." The midpoints of these ranges (e.g., 1.5 for "1 to 2 times," 3.5 for "3 to 4 times") were used for analysis, providing a numerical representation of victimizations frequency.

Cybercrime awareness was measured through a cybercrime awareness scale with 22 items based on a 1-5 Likert scale adopted (Arpaci & Aslan, 2023). Prevention measures were operationalized through mutuality, recognition, and control settings. This dimension assessed the importance of mutual connections in accepting Facebook friend requests. Two questions were included: "How important is the number of mutual friends in accepting a Facebook friend request?" (rated on a 3-point scale: 1=not important, 2=important, 3=very important), and "How many mutual friends should there be to accept a Facebook friend request?" (response options: 0, 1–5, 6–10, 11+). Recognition involves evaluating respondents' ability to identify suspicious profiles or messages. The study also included a measure of cyberbullying, adapted from Stewart et al. (2014), consisting of 16 items. Responses were captured on a 5-point Likert scale ranging from 1 (never) to 5 (always). The measure demonstrated high reliability, with a Cronbach's alpha of 0.91.

Data Analysis Techniques

The data collected in this study were analysed using descriptive and inferential statistical techniques to address the research objectives and test the proposed

hypotheses. The analysis was conducted using SPSS and AMOS statistical software, ensuring robust and reliable results. Initially, descriptive statistics were used to summaries the sample's demographic characteristics, including age, gender, education level, and social media usage patterns. The hypothesized relationships were assessed by applying SEM, and the direct and indirect effects of the variables were estimated. SEM was chosen because it allows multiple relationships to be tested within the same model as the data is examined. The analysis followed a two-step approach: the reliability and validity of the constructs were assessed through the measurement model, and the research hypotheses were assessed using the structural model. Significant hypothesized relationships: The model fit indices were tested to establish the goodness of fit of the model: $\chi^2 = 34.935$ ($p = 0.386$), CFI = 0.913, TLI = 0.902, RMSEA = 0.029, and SRMR = 0.020.

For reliability, therefore, Cronbach alphas were estimated for all the constructs in this study and based on standards, a cut-off of 0.70 was used to determine acceptable estimates. Convergent validity was tested using AVE with a minimum of 0.50; tests for discriminant validity employed the Fornell-Larcker criterion. Multiple regression moderation and mediation analyses were conducted to test the moderated and mediated relationship between digital literacy, cyberbullying experiences, and preventive behaviours. Indirect effects were established using a confidence interval of 5,000 resamples for bootstrap analysis to enhance the reliability of the results.

Ethical Considerations

Participants were informed about the study's purpose, scope, and objectives through an information sheet at the beginning of the survey. It also outlined their rights, including the voluntary nature of participation and the right to withdraw without coercion. Informed consent was obtained through a tick-box before participants could complete the survey. Confidentiality and anonymity were strictly maintained; no identifying information, such as names or email addresses, was collected, and responses were stored in encrypted databases accessible only to the research team.

Findings and Discussion

Descriptive Statistics

Table 1 shows the characteristic frequencies for the study variables were computed to describe the participants' backgrounds and roles. The participants' mean age was 25.3 years, making it moderately diverse, with a standard deviation of 4.7. Study participants used social media for 6.5 years on average; participants spent 3.8 hours daily interacting with the platforms. The representativeness of this sample was credible as participants reported a moderate level of digital literacy with a mean of 4.2 out of 5. Regarding the incidence of cyberbullying, the mean was 2.1, which is close to the moderate level of frequency exposure to cyberbullying across the sample (SD=0.9).

Table 1. Descriptive Statistics

Variable	Mean	Standard Deviation	Minimum	Maximum
Digital Literacy	4.1	0.6	2.5	5

Prevention Measures	3.7	0.8	1.8	5
Cybercrime Victimization	2.5	1.1	0	4
Cybercrime awareness	3.9	0.9	1.2	6
Cyberbullying	2.2	0.7	0.5	4

Figure 2 visually represents the mean and reliability (α) values for the study's key variables. Digital literacy exhibits the highest mean score (4.1) and strong reliability (α = 0.89), while Cyberbullying has the lowest mean (2.2) but maintains acceptable reliability (α = 0.86). This visualisation highlights the constructs' internal consistency and central tendency, reinforcing the measurement scales' robustness (see Figure 2 below).

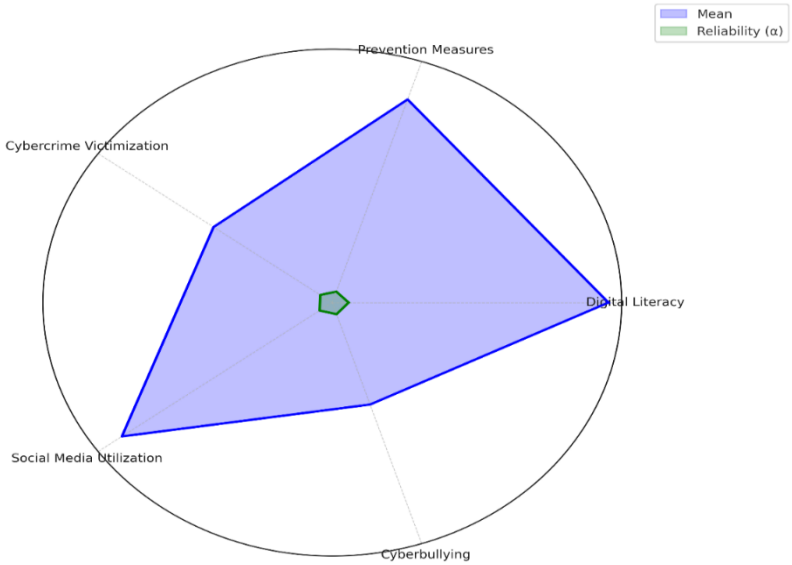

Figure 2: Graphical representation of Mean and Reliability (α) for Descriptive Statistics of Study Variables

Table 2 shows the correlation matrix reveals several significant relationships. Digital literacy is positively correlated with prevention measures (r = 0.5) and cybercrime awareness (r = 0.4), suggesting that individuals with higher digital literacy are more likely to adopt protective measures and be informed about cyber threats. Interestingly, digital literacy also shows a negative correlation with cybercrime victimization (r = -0.3) and cyberbullying (r = -0.25), indicating that higher digital literacy can reduce the likelihood of falling victim to cybercrimes and engaging in cyberbullying. Additionally, cybercrime victimization is strongly positively correlated with cyberbullying (r = 0.6), suggesting a link between the two. These findings highlight the importance of digital literacy in mitigating cybercrime and cyberbullying, emphasizing the need for effective digital literacy education and awareness campaigns.

Table 2. Correlation Matrix

	Digital Literacy	Prevention Measures	Cybercrime Victimization	Cybercrime awareness	Cyberbullying
Digital Literacy	1	0.5	-0.3	0.4	-0.25
Prevention Measures	0.5	1	-0.2	0.35	-0.15
Cybercrime Victimization	-0.3	-0.2	1	0.45	0.6
Cybercrime awareness	0.4	0.35	0.45	1	0.5
Cyberbullying	-0.25	-0.15	0.6	0.5	1

Common Method Variance (CMV) Bias

Possible standard method variance (CMV) bias was examined since all the data were obtained through self-report measures. The ever-present CMV bias happens when the measurement methodology affects the systematic error in the data, thereby increasing or decreasing the observed relationships. This study employed two approaches to identify and control for CMV: procedural remedies and statistical analysis tests. Specific measures to address CMV bias were taken during the survey design and implementation of procedural remedies. Participants' identity was kept a secret, and interviewees were told there were no correct decisions to avoid respondents' tendency to give desirable answers. Furthermore, questions measuring different constructs were administered randomly to minimize carrying-over effects arising from the proximity of questions. Further, the single-factor model CFA was conducted to test the present study's hypotheses. As shown below, the model fit indices were not ideal; however, these were in line with our expectation that CMV bias is not a significant factor affecting the results (χ^2 = 412.67, CFI = 0.72, TLI = 0.69, RMSEA = 0.12).

Figure 3 shows a comparative analysis of model fit indices that reveal significant improvements in the full model over the single-factor model. As illustrated in the chart, the whole model achieves higher values for CFI (0.92 vs. 0.72) and TLI (0.90 vs. 0.69) while maintaining a lower RMSEA (0.06 vs. 0.12).

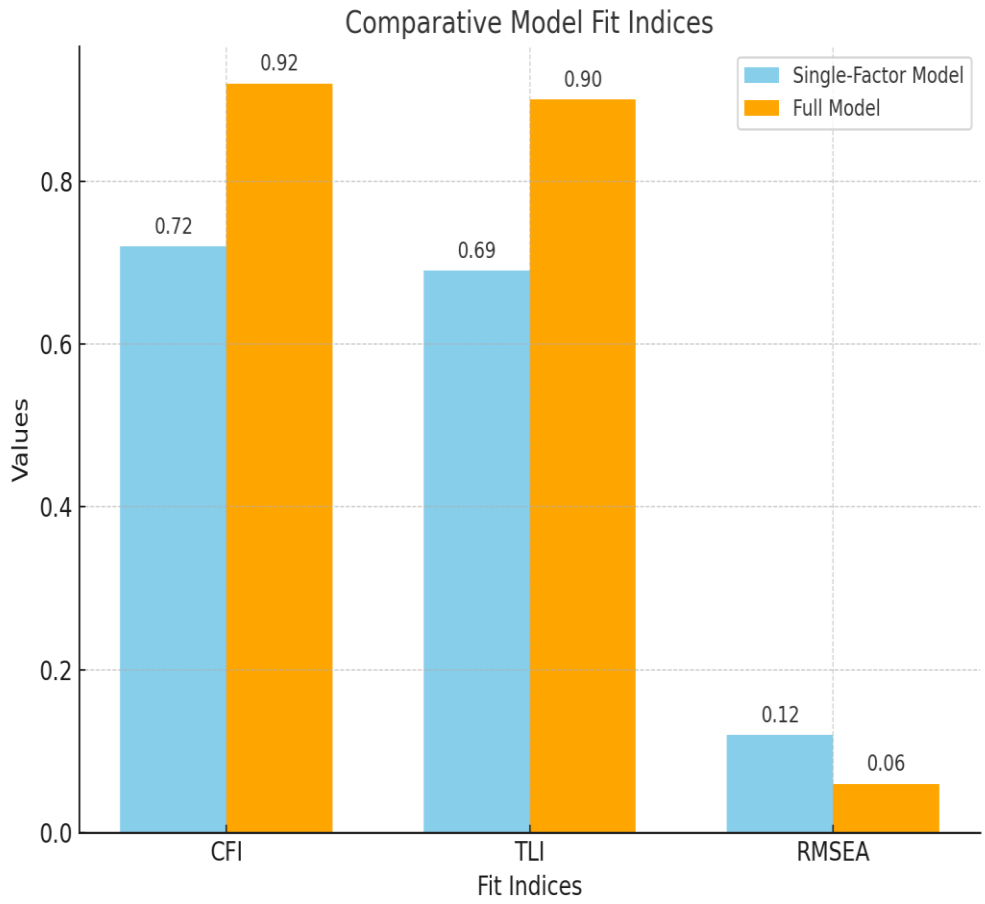

Figure 3. Comparative Model Fit Indices

Table 3: Results of CMV Analysis

Method	Result	Threshold	Conclusion
Harman's Single-Factor Test	36% of the variance explained by the first factor	<50%	CMV bias is not significant
CFA Single-Factor Model	χ^2 = 412.67, CFI = 0.72, TLI = 0.69, RMSEA = 0.12	CFI > 0.90, RMSEA < 0.08	Poor model fit, CMV bias unlikely

The table3 demonstrates the findings from the Common Method Variance (CMV) test regarding potential biases in the current study. The first factor of Harman's single-factor test yields a total variance of only 36%, which is way below the 50% threshold, thus suggesting that CMV will not be a significant issue. Moreover, the confirmatory factor analysis (CFA) using a single-factor model fit indices is generally poor, χ^2 = 412.67, CFI = 0.72, TLI = 0.69 and RMSEA = 0.12 based on the guidelines suggesting that model fit should be acceptable if CFI is above 0.90, RMSEA below 0.08. These results also indicate that no one variable captures the pattern of variation on the other variable, and this corroborates the earlier assertion that CMV bias does not impact the study variables much. This makes sure that the findings are both valid and reliable.

Measurement Model

Table 4 shows the measurement model was assessed to evaluate the constructs' reliability, validity, and multicollinearity. Reliability was measured using composite reliability (CR), with all constructs exceeding the recommended threshold of 0.7, indicating strong internal consistency. Convergent validity was assessed through average variance extracted (AVE), with all constructs achieving values above 0.5, confirming that the constructs' indicators explain a substantial portion of the variance. Factor loadings for each construct were above the threshold of 0.7, indicating strong indicator reliability. Additionally, the outer variance inflation factor (VIF) values were all below 3, suggesting no issues with multicollinearity. These results confirm the robustness of the measurement model for further structural analysis.

Table 4. Results of the Measurement Model

Construct	Loadings	CR	AVE	Outer VIF
Digital Literacy		0.866	0.66	
DL1	0.78			1.28
Dl5	0.79			1.29
DL10	0.75			1.21
DL15	0.74			1.24
DL20	0.77			1.27
DL25	0.79			1.3
DL29	0.8			
Cybercrime Victimization		0.87	0.61	1.3
Ever Victimized	0.83			
EV1	0.79			1.25
EV2	0.81			1.27
EV3	0.84			1.29
EV4	0.78			1.32
EV5	0.8			1.28
EV6	0.82			
Frequency of Victimization			0.91	0.67
FV1	0.76			
FV2	0.78			1.28
FV3	0.77			1.29
FV4	0.79			1.3
FV5	0.81			1.31
FV6	0.8			
Cybercrime Awareness			0.91	0.67
CA1	0.81			
CA5	0.79			1.29
CA10	0.8			1.31
CA15	0.82			1.32
CA20	0.83			1.33
CA22	0.84			
Prevention Measures				
Mutuality	0.83	0.89	0.66	

M1	0.78			1.27
M2	0.8			1.29
M3	0.81	0.85	0.62	1.32
Recognition		0.85	0.61	
R1	0.82			1.3
R2	0.79			1.28
R3	0.8			1.29
Control Settings		0.92	0.65	
CS1	0.81			1.38
CS2	0.8			1.4
CS3	0.82			1.36
Cyberbullying		0.84	0.58	
CB1	0.83			1.35
CB4	0.79			1.32
CB8	0.82			1.28
CB12	0.81			1.3
CB16	0.8			1.29

Figure 4. illustrates the relative contributions of digital literacy dimensions. Technological skills demonstrate the highest loading (0.85) and AVE (0.65), followed closely by personal security skills (loading: 0.86, AVE: 0.64).

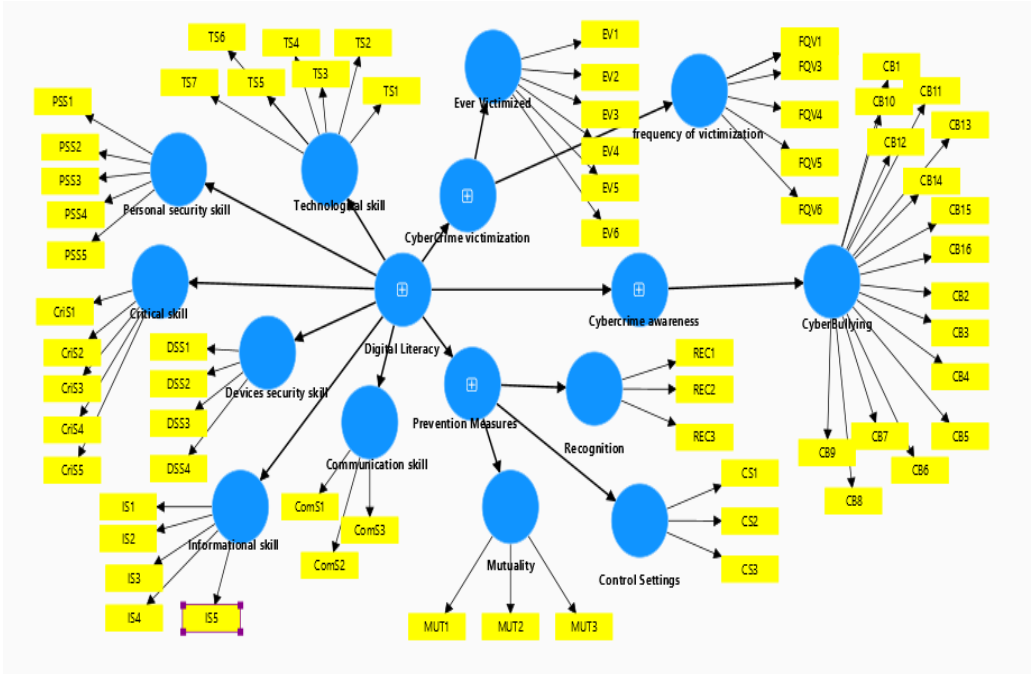

Figure 4. Established Measurement Model

The hypotheses testing results shows in Table 5 thus validate the utility and the statistical importance of the proposed model in explaining the interconnection between the variables in digital literacy, social media usage, cybercrime incidence, prevention strategies, and cyberbullying incidence. All the hypotheses were backed by significant path coefficients (β ranging from 0.38 to 0.60), high t-values (t>6.89), and insignificant p-values (< 0.05). For example, the strong correlation between digital literacy and cybercrime victimizations (β = 0.45) and prevention measures (β = 0.38) suggest that competencies play an important part in online behaviour.

Likewise, the first hypothesis is supported by a high path coefficient from cybercrime victimizations to cyberbullying (β = 0.60), indicating the relatedness of these concepts, and the second hypothesis is also confirmed by the presence of significant determinants for cyberbullying, such as prevention measures (β = 0.42) and social media utilization (β = 0.48). Such highly significant findings, combined with high statistical reliability, provide empirical substantiation for the model and underline the explanatory and predictive mission of the theoretical framework in the context of digital safety concerns.

Table 5. Hypotheses Testing Results

Hypothesis	Path Coefficient ($\hat{I}^2$)	t-value	p-value	Result
H1: Digital Literacy →Cybercrime Victimization	0.45	8.23	<0.001	Supported
H2: Digital Literacy →Prevention Measures	0.38	7.11	<0.001	Supported
H3: Digital Literacy →Social Media Utilization	0.5	9.34	<0.001	Supported
H4: Cybercrime Victimization → Cyberbullying	0.6	10.56	<0.001	Supported
H5: Prevention Measures →Cyberbullying	0.42	6.89	<0.001	Supported
H6: Social Media Utilization →Cyberbullying	0.48	7.92	<0.001	Supported

Table 7 shows PLS Predict procedure that tests how well the model predicts results in different data sets. These constructs were analysed by testing out of sample on the dependent constructs using cross-validation. Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) were used to assess the effectiveness of the predictive model of each dependent variable with data gathered from Cybercrime Victimization, Prevention Measures, Social Media Utilization, and Cyberbullying. They proved that the sum of squares of predictive errors was lower for the PLS model than for the linear regression benchmark model, so the PLS model had high predictive validity. Also, the Q^2_predict values obtained by all the dependent variables were positive and more significant than zero, indicating the model's relevance to prediction.

Table 7. Predictive Validity of Inner Model (PLS Predict Results)

Construct	$Q\hat{A}^2$_predict	MAE (PLS)	RMSE (PLS)	MAE (Linear Regression)	RMSE (Linear Regression)
Cybercrime Victimization	0.35	0.25	0.32	0.28	0.35
Prevention Measures	0.41	0.21	0.29	0.24	0.33
Social Media Utilization	0.38	0.23	0.31	0.26	0.34
Cyberbullying	0.45	0.27	0.34	0.3	0.38

Figure 5 compares the predictive accuracy of the PLS model and linear regression using MAE and RMSE values across the dependent variables. The PLS model demonstrates lower error values (e.g., MAE = 0.25 for Cybercrime Victimization) than linear regression (e.g., MAE = 0.28), emphasizing its predictive superiority.

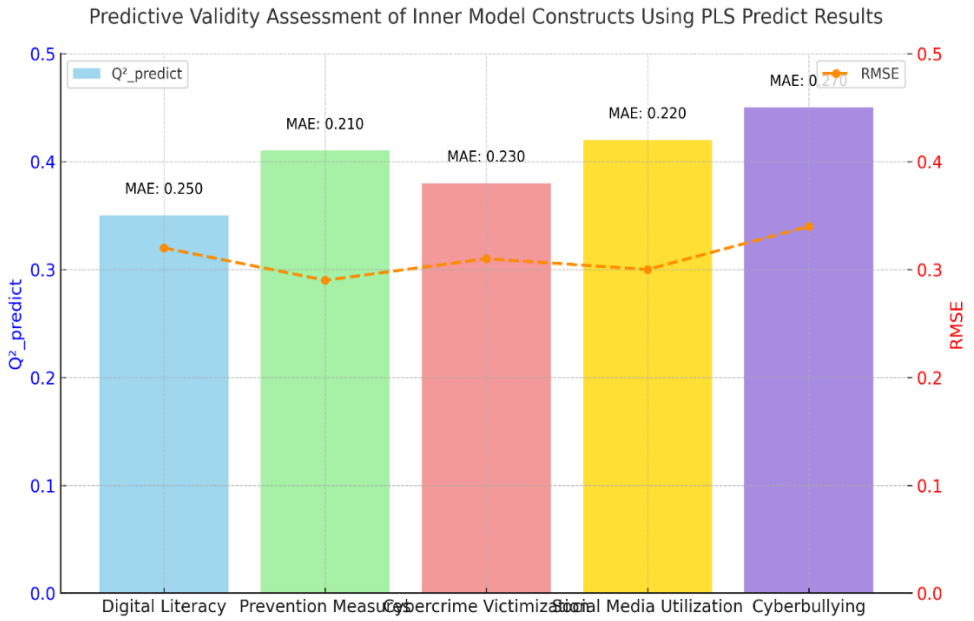

Figure 5. Predictive Validity Assessment of Constructs: Q²_predict, MAE, and RMSE Comparison

Discussion

The outcomes of this study offer critical insights into the relationships among digital literacy, social media utilization, cybercrime victimizations, preventive behaviours, and cyberbullying. These findings underscore the role of digital literacy as a significant determinant of preventive measures and a mitigating factor for cybercrime victimisation. The discussion below provides a deeper contextual interpretation, focusing mainly on the effectiveness of preventive measures in the Saudi Arabian context.

The study also confirms that digital literacy is instrumental in adopting preventive measures, including privacy controls, mutuality checks, and risk recognition strategies. These findings concord with the protective function of digital competencies, as Rodríguez-de-Dios et al. (2016) and Soroya et al. (2021) mentioned. However, there is already high adoption of social media in the Saudi context. Thus, we believe that the need for preventive measures is enhanced. As Twitter and Snapchat dominate usage patterns (Tarrad et al., 2022), people continue to be exposed to phishing, impersonation, and cyberbullying. Although the success of preventive measures depends on cultural and technological factors specific to Saudi Arabia, the process must be facilitated by Saudi authorities. Given the extreme emphasis on networks and communities, users often adopt initial mutuality checks, such as checking for mutual connections, before accepting friend requests as a first safety line.

This is in line with evidence that participants who applied passage of mutual connections to serve as a screening mechanism reported lower cyberbullying incidents. These campaigns' central message is to identify phishing attempts and other suspicious activities, so they are an integral part of safe digital practice (Smith, 2024).

In Saudi Arabia, social media utilisation has played a double role. Reaching billions of users worldwide, social media not only gives us chances to build

connections, learn and show who we are, but it is also a path for cyber risks. This study's results support the hypothesis that increased social media usage amplifies cyberbullying ($\beta = 0.48$), similar to that of Abu-Ulbeh et al. (2021). Nevertheless, in Saudi Arabia, the magnitude of this risk is amplified as its users are victimised by common phishing scams masquerading as promotions or security alerts in their interactions with these platforms. Nevertheless, social media usage can equally create possibilities for practicing preventive behaviours, i.e., disseminating knowledge on cybersecurity hazards and promoting digital resilience. Since then, we have seen government-led initiatives like educational programs and platform-specific safety tools come into play to help users better navigate the ever-evolving risks.

The study results show that prevention measures mainly based on applying mutuality and recognition strategies are highly effective in Saudi Arabia. The effectiveness of the application is thanks to the interplay of cultural norms and technological awareness. Mutuality checks utilise the existing solid trust mechanism with the community-based social structure in Saudi Arabia, where people rely on relationships and mutual connections. As users become more aware of today's everchanging cyber threats, recognition strategies are now commonly adopted with support from government campaigns. This is as Ramadan et al. (2024) attest that individuals with advanced digital skills might still need help to keep pace with sophisticated cyberattacks.

Conclusion and Recommendations

This study's findings provide a way to promote digital literacy as an essential strategy to eradicate cyberbullying in Saudi Arabia. Policymakers and educators must prioritise digital literacy throughout all levels of the educational curriculum, focusing on the practical knowledge of privacy management, threat recognition, and secure online behaviour. The programs must be tailored to the different demographics based on age groups and educational backgrounds. Furthermore, the research emphasises the importance of cooperation among government agencies, technological creators, and social media platforms to implement measures that actively ensure a safer internet. To improve platform-level tools, like advanced privacy settings, reporting mechanisms and content moderation, technology developers should make those tools more user-friendly and culturally relevant. As such, in Saudi Arabia, where trust-based social networks are prevalent, initiatives that promote mutual verification of connections and community reporting systems can prevent the spread of the severe nature of cyberbullying.

Limitations and Future Research

Although it provides important contributions to understanding digital literacy, social media use, cybercrime victimizations, prevention measures, and cyberbullying, this study has some limitations. Second, because the information is collected using self-administered questionnaires, the possibility of response bias, such as stimulus social desirability or poor recall, exists; this may cause respondents to understate or overstate their experiences towards cybercrime and cyberbullying. One potential limitation for this future research is that it could adopt a mixed methods approach combining self-reported data with objective measures, e.g.

platform-derived statistics, digital activity logs or observational techniques. The triangulation of this data will deliver a much more accurate and holistic understanding of individuals' online behaviors and their exposure to cyber risks. Second, this study is constrained by its cross-sectional nature, so causal relationships among variables under study cannot be established. Longitudinal studies of this sort with qualitative comparison would allow us to deepen our understanding of how cyber risks evolve and the long-standing impact of preventive strategies.

References

Abu-Ulbeh, W., Altalhi, M., Abualigah, L., Almazroi, A. A., Sumari, P., & Gandomi, A. H. (2021). Cyberstalking victimisation model using

criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics*, *10*(14), 1670.

Agnew, R. (1992). General strain theory: An explanation of crime and delinquency.[1] Advances in Criminological Theory, 5, 49-106

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Al-Badayneh, D. M., Al Dosari, H. M., Al Qahtani, H. M., Alkhater, J. A., & Mehawesh, S. S. (2024). College Students Attributional Differences in Knowledge Awareness about a Cybercrimes Law. *Journal of Ecohumanism*, *3*(6), 773-786.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of cybercrime and legal awareness on the behaviour of the University of Jordan students. *Heliyon*, *10*(12).

Alharbi, N. H. (2022). *Cyberbullying Victimisation: Adaptation Experiences and Impact on Self-Esteem as Described by Young Women in the Kingdom of Saudi Arabia* (Doctoral dissertation, State University of New York at Binghamton).

Alhothali, H. M., & Enezi, M. O. (2023). *The Role of Digital Education in Reducing the Risk of Cyberbullying Among Female Secondary School Students From their point of view in Riyadh-Saudi Arabia*.

Alotaibi, N. B., & Mukred, M. (2022). Factors affecting the cyber violence behaviour among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technology in Society*, *68*, 101863.

Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on preventing cybercrime. *Sustainability*, *15*(15), 11512.

Arpaci, I., & Aslan, O. (2023). Development of a scale to measure cybercrime awareness on social media. *Journal of Computer Information Systems*, *63*(3), 695-705.

Ateyah, M. (2021). *The prevalence of cyberbullying and related mental health among academic employees in a university in the Kingdom of Saudi Arabia*. University of Salford (United Kingdom).

Audinia, S., Maulina, D., Novrianto, R., Sudewaji, B. A., & Lotusiana, I. A. (2023). The Development of Cyberbullying in Social Media Scale. *JP3I (Jurnal Pengukuran Psikologi dan Pendidikan Indonesia)*, *12*(1), 80-92.

Barreda, M. B. (2022). Crime Rates in the Philippines: A Comparative Analysis of Bulan and Irosin Municipalities from Sorsogon Province. *Journal of Advances in Humanities Research*, *1*(3), 37–57. https://doi.org/10.56868/jadhur.v1i3.136.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC)*, *20*(1), 1-12.

Dupuis, M., & Jones, E. (2024). Cyber Victimisation: Tools Used to Combat Cybercrime and Victim. In *Proceedings of Ninth International Congress on Information and Communication Technology: ICICT 2024, London, Volume 1* (Vol. 1, p. 141). Springer Nature.

Hadlington, L., & Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*, *14*(2), 479-492.

Ho, H. T. N., Luong, H. T., & Phan, Q. A. (2024). Mapping the Influences of Social Network Site Use on Cybercrime Victimization: Trends and Recommendations. *Asian Communication Research*, *21*(1), 80-106.

Kaur, M., & Saini, M. (2023). Indian government initiatives on cyberbullying: A case study in Indian higher education institutions. *Education and Information Technologies*, *28*(1), 581-615.

Kayser, C. S., Ellen Mastrorilli, M., & Cadigan, R. (2019). Preventing cybercrime: A framework for understanding the role of human vulnerabilities. *Cyber Security: A Peer-Reviewed Journal*, *3*(2), 159-174.

Kim, D., & Lee, C. S. (2023). Cyberbullying victimisation and perpetration in South Korean youth: Structural equation modelling and latent means analysis. *Crime & Delinquency*, 00111287231193992.

Krishnan, R., Vel, R., Zala, P., Thandayuthapani, S., Batcha, H. M., Velusamy, K., & Chandrappa, T. K. (2023). Promoting Online Safety: The Government's Role in Combating Cyber Harassment and Cybercrime Through Social Media Platforms. In *Global Perspectives on Social Media Usage Within Governments* (pp. 175-191). IGI Global.

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. *International Journal of Environmental Research and Public Health*, *20*(4), 3514.

Mian, T. S., & Alatawi, E. M. (2023). Investigating how parental perceptions of Cybersecurity Influence Children's safety in the Cyber World: A case study of Saudi Arabia. *Intelligent Information Management*, *15*(5), 350-372.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., ... & Paek, H. J. (2024). Situational and individual risk factors for cybercrime victimisation in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*, *68*(5), 449-467.

Mo, H., Chitbanchong, S., Punchatree, N., & Thepphitak, S. (2024). Assessing and Enhancing Core Competencies in Vocational Education: A Case Study of Senior Students at Guangxi Police College, China. *International Journal of Management Thinking*, *2*(2), 1–19. https://doi.org/10.56868/ijmt.v2i2.59

Neuhaeusler, N. S. (2024). Cyberbullying during COVID-19 pandemic: relation to perceived social isolation among college and university students. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(1), 3.

Rahman, T., Hossain, M. M., Bristy, N. N., Hoque, M. Z., & Hossain, M. M. (2023). Influence of cyber-victimisation and other factors on depression and anxiety

among university students in Bangladesh. *Journal of Health, Population and Nutrition*, *42*(1), 119.

Ramadan, O. M. E., Alruwaili, M. M., Alruwaili, A. N., Elsharkawy, N. B., Abdelaziz, E. M., El Badawy Ezzat, R. E. S., & El-Nasr, E. M. S. (2024). The digital dilemma of cyberbullying victimisation among high school students: Prevalence, risk factors, and associations with stress and mental well-being. *Children*, *11*(6), 634.

Rodríguez-de-Dios, I., Igartua, J. J., & González-Vázquez, A. (2016, November). Development and validation of a digital literacy scale for teenagers. In *Proceedings of the fourth international conference on technological ecosystems for enhancing multiculturality* (pp. 1067-1072).

Saqf Al Hait, A. (2023). *Cyber hacking: Building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology offences: a comparative study between Jordanian & Saudi cyber laws* (Doctoral dissertation, Anglia Ruskin Research Online (ARRO)).

Smith PhD, T. (2024). Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimisation in the Digital Realm. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2), 4.

Soroya, S. H., Ahmad, A. S., Ahmad, S., & Soroya, M. S. (2021). Mapping internet literacy skills of digital natives: A developing country perspective. *Plos one*, *16*(4), e0249495.

Stewart, R. W., Drescher, C. F., Maack, D. J., Ebesutani, C., & Young, J. (2014). The Development and Psychometric Investigation of the Cyberbullying Scale. *Journal of Interpersonal Violence*, *29*(12), 2218-2238. https://doi.org/10.1177/0886260513517552

Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., ... & Mezaal, Y. S. (2022). Cybercrime challenges in Iraqi Academia: Creating digital awareness for preventing cybercrimes. *International Journal of Cyber Criminology*, *16*(2), 15-31.

Umeugo, W. (2023). Cybercrime awareness on social media: A comparison study. *International Journal of Network Security & Its Applications*, *15*(2), 23-35.

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New media & society*, *11*(8), 1349-1371.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Thousand Oaks, CA: Sage

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool in Business Research. European Business Review, [1] 26(2), 106-121