APEX JOURNAL OF SOCIAL SCIENCES
https://apexjss.com
Volume 3 Issue 2, 2024

HIGHER EDUCATION AND CYBER-CRIME PERCEPTION AMONG UNIVERSITY STUDENTS IN ISLAMABAD

Asma Shaheen [1], Sabahat Waqar [2]

Affiliations:

[1] Principal,
Rehan School Foundation,
Islamabad Campus
[1] asmashaheen828@gmail.com

[2] M. Phil Scholar, International Islamic University, Islamabad
[2] sabahatwaqaribd@gmail.com

Corresponding Author/s Email:

[1] asmashaheen828@gmail.com

Abstract

Advanced education serves as the cornerstone of human capital development and fuels economic growth. By cultivating individuals with valuable skills and knowledge, it empowers them to make significant contributions to their societies and drive national prosperity. Ideally, advanced education should contribute to a more secure and cyber-resilient society, fostering a workforce equipped to navigate the complexities of the digital age and mitigate cyber threats. However, when examining the relationship between advanced education and cybercrime in Pakistan, a concerning trend emerges. Despite the potential of higher education to cultivate a skilled and responsible citizenry, the reality in Pakistan seems to suggest a different outcome. A contributing factor to this disparity may lie in the limited availability of suitable employment opportunities for graduates. When individuals with advanced degrees, possessing valuable skills and knowledge, are unable to find meaningful employment in their respective fields, they may become more susceptible to engaging in cybercrime as a means of income generation. This unfortunate circumstance can lead to a situation where individuals with the potential to contribute positively to society instead resort to illicit activities, undermining the very goals of advanced education. To further investigate this concerning phenomenon, a quantitative research study was conducted at Quaid-i-Azam University, Islamabad. This study aimed to delve deeper into the factors that may be driving this trend and to better understand the relationship between advanced education and cybercrime within the Pakistani context. By examining the experiences and perspectives of individuals within the academic environment, the study sought to shed light on the challenges faced by graduates in the job market and the potential impact of these challenges on their involvement in cybercriminal activities.

Keywords: Advanced Education, Human Capital Development, Cyber-crime, Employment Opportunities, Pakistan

Introduction

In the digital age, the integration of technology in higher education has transformed the learning environment, providing unprecedented access to information and fostering innovative educational practices. However, with the increasing reliance on digital platforms, university students are also becoming more susceptible to cyber-crime. Cyber-crime, encompassing a wide range of illegal activities conducted via the internet, poses significant threats to individuals, institutions, and society at large. University students, often at the forefront of technological adoption, are uniquely positioned to both benefit from and be vulnerable to cyber-crime. Their frequent use of online resources, social media (Asif & Sandhu, 2023), and other digital tools makes them prime targets for cyber criminals. Understanding how university students perceive the risks

and implications of cyber-crime is crucial for developing effective educational programs and preventive measures.

Advanced education serves as the cornerstone of human capital development and fuels economic growth. By cultivating individuals with valuable skills and knowledge, it empowers them to make significant contributions to their societies and drive national prosperity. Ideally, advanced education should contribute to a more secure and cyber-resilient society, fostering a workforce equipped to navigate the complexities of the digital age and mitigate cyber threats. However, when examining the relationship between advanced education and cyber-crime in Pakistan, a concerning trend emerges.

Despite the potential of higher education to cultivate a skilled and responsible citizenry, the reality in Pakistan seems to suggest a different outcome. A contributing factor to this disparity may lie in the limited availability of suitable employment opportunities for graduates (Asghar et al., 2015; Asif et al., 2023; Aurangzeb et al., 2021). When individuals with advanced degrees, possessing valuable skills and knowledge, are unable to find meaningful employment in their respective fields, they may become more susceptible to engaging in cyber-crime as a means of income generation. This unfortunate circumstance can lead to a situation where individuals with the potential to contribute positively to society instead resort to illicit activities, undermining the very goals of advanced education.

This research aims to explore the perceptions of cyber-crime among university students, examining how their awareness, attitudes, and behaviours are influenced by their educational experiences and digital interactions. By investigating these perceptions, this study seeks to provide insights into the effectiveness of current cyber-crime education and highlight areas for improvement. The findings of this research will contribute to the broader discourse on cybersecurity in higher education, emphasizing the need for comprehensive strategies that not only enhance students' digital literacy but also equip them with the necessary skills to navigate and mitigate cyber threats (Asghar et al., 2015; Hussain & Shahid, 2024). As universities continue to evolve in an increasingly digital world, fostering a culture of cybersecurity awareness among students is imperative for safeguarding their academic and personal pursuits.

Statement of the problem

The advanced education and cyber-crime is utilized as a subject of logical analyses; and much passion have been given to their effect on society. This investigation is about how digital wrongdoing is boundary being developed of advanced education. The principle look into subject of this investigation is advanced education and cyber-crime in Quaid-I-Azam University, Islamabad, Pakistan.

Objective of the study

To investigate the effect of advanced education on cyber-crime in helpful properties.

Significance of the study

This study has both theoretical and compact result. Despite the fact that various research directed on cyber-crime and their effect on advance and disorder, this is the primary sociological examination of cyber-crime. Along these lines, this flow examine gives hypothetical information on advanced education and cyber-crime and their results in scholarly and working regions.

Literature Review

The digital matching can make a couple of treads, including supportive programming and online encouraging change in agreement with combine of theoretical strategies, social, mental, educational, and psycho dynamic among them. The development of web visit cafe consider immediately, online contact among direction and client. Advising and talk through the online work is a technique for achieving difficult to reach zones to direct organizations and furthermore, overhaul communication among specialists. Today, school controls normally partake in online post with partners, alternates and gatekeepers. Mechanical advances are changing normal organizing practices in schools while showing new good challenges (Asghar et al., 2015; Cassim, 2011; Hussain & Shahid, 2024).

The rapid advancement of technology and the increasing reliance on digital platforms have significantly impacted higher education institutions and their students. As universities integrate more digital

tools and online resources into their curricula, the risk of cyber-crime has become a pressing concern. This literature review explores the existing research on the perception of cyber-crime among university students, highlighting key findings, gaps, and implications for future research.

Several studies have examined the level of cybersecurity awareness among university students. For instance, a systematic review by Nilupú-Moreno et al. (2024) analysed articles published between 2018 and 2023 and found that students' knowledge, attitudes, and behaviours towards cybersecurity are crucial areas for reinforcement. The review highlighted that while students possess basic knowledge of online risks such as phishing and password security, there is a gap in effectively applying this knowledge.

Research by Igba (2018) explored the perception of cyber-crime among university undergraduates and its implications on their academic achievement. The study revealed that students often view cyber-crime as a tool for personal development and financial gain, indicating a need for value re-orientation and safe network environments3. Similarly, Broadhurst (2018) conducted an exploratory study on cyber-crime risks in a university student community, emphasizing the importance of creating a secure and trustworthy network environment (Hussain & Shahid, 2024).

To address the insufficient cybersecurity knowledge among university students, Adeshola and Oluwajana (2024) assessed students' awareness, attitudes, and capacity to assess cybersecurity risks. Their findings suggested that tailored educational programs and awareness initiatives are essential for nurturing ethical and cybersecurity awareness (Asif, 2022; Asif, 2022; Asif & Shaheen, 2022; Bashir et al., 2024). The study recommended integrating practical cybersecurity modules into school curricula to strengthen students' online safety practices.

Despite the growing body of research on cybersecurity awareness and cyber-crime perception, there are still gaps that need to be addressed. Future research should focus on developing and evaluating effective educational interventions that go beyond theoretical knowledge and emphasize practical skills. Additionally, studies should explore the long-term impact of cybersecurity education on students' behaviour and attitudes towards cyber-crime.

The perception of cyber-crime among university students is a multifaceted issue that requires a comprehensive approach to education and awareness. By understanding students' awareness, attitudes, and behaviours, higher education institutions can develop targeted interventions to enhance cybersecurity knowledge and mitigate the risks associated with cyber-crime. As technology continues to evolve, fostering a culture of cybersecurity awareness among university students is imperative for safeguarding their academic and personal pursuits.

Assumptions

Advanced education is a simple method to gain financial gains, and individuals who are not educated are likewise doing such acts in especially particular way.

Theoretical Framework

The well-organized gathering purpose of the Routine Activities takes a large scale level search and features full scale moves in the examples of sufferer and crimes. It notices on specific criminal activities and guilty party decisions. Routine action hypothesis depends on the belief that offense can be submitted by anybody that gets the opportunity. The hypothesis additionally expressed that sufferers are determined varieties on whether to be targets generally by not putting themselves in conditions where a crime can be submitted against them (Asghar et al., 2015; Madero-Hernandez & Fisher, 2012:13-27).

Hypothesis

Advanced education reason cyber-crime.

Null hypothesis

Does advance education reason cyber-crime.

Alternative hypothesis

Advance education does not reason cyber-crime.

Conceptualization

According to Thompson (1992) "Higher Education is vital for your personal happiness and for your trained satisfaction. We trust that the best possible training for a productive future is a rich and sufficient experience in your higher education itself."

According to Gordon and Ford (2006) "Cyber-crime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes)." The overhead definition define that cyber-crime is something that consist of many things as doing illegal actions as hacking the accounts of others and online money laundering.

Operationalization

A great people groups pay their full emphasis on advanced education so as to oversee business as usual in nation in each viewpoint. As showed by the area the definition fits as advanced education is the type of bliss by adapting new and advance things, by these individuals become cheerful and this joy promises them achievement in the manner where they go. After advanced education they become solid and steady to look through their acquiring sources.

The overall population are profoundly master in using computer based applications. Their abilities are the source to humour them to carry out cyber-crime, since cyber-crime is the source to gain cash in various shapes.

Research Methodology

Research Design

The design of this research is quantitative.

Universe

This research was conducted in Quaid-i-Azam University, Islamabad. The data collected from the people who have some knowledge regarding the cyber-crime.

Unit of Analysis

The target population of the research was respondents of the area of Quaid-i-Azam University, Islamabad especially the people from the age of 18 to 30.

Sample Size

The researcher chose 167 respondents for the purpose of sampling from the area of university. This sample size is enough for two thousands population.

Tools for Data Collection

The researcher used a structured, close ended questionnaire. The data was collected on the basis of those questions.

Tools for Data Analysis

The statistical package for social sciences (SPSS) developed by IBM was used for data analysis. The researcher used descriptive and inferential statistics. Percentages and frequencies tests checked the relativity and relation of the data.

Pretesting

The researcher took (5), five respondents in order to pre-test the questionnaire. The respondents were taken in a way that they were also belonging to the area of the research.

Ethical Concern

The maintenance of ethical concerns is important. When the researcher was conducting the research, she asked the questions in way that people feel friendly to respond. Any of the respondents was not gone under any sort of puzzlement and ignominy. It was the due responsibility of the researcher to maintain all the information of the respondents.

Opportunities and limitations of the Study

The researcher studied the area well before starting the research and she was having well knowledge about the area. So it was an easy opportunity for her to answer the questions as respondents were easily available.

APEX JOURNAL OF SOCIAL SCIENCES
https://apexjss.com
Volume 3 Issue 2, 2024

Results

The analysis of the collected data revealed several key insights into the perception of cyber-crime among university students. The study's findings highlight the varying levels of awareness, attitudes, and behaviours related to cybersecurity across different demographic groups. A detailed examination of the survey responses and statistical analyses provided a comprehensive understanding of how factors such as age, gender, education level, and digital literacy influence students' perceptions and experiences with cyber-crime. The results section delves into these trends and patterns, offering a nuanced view of the current cybersecurity landscape within the university student community.

Table 1

Demographics Analysis

Demographics	Characteristic	Frequency (n)	Percentage (%)
Gender	Male	106	63.47
	Female	61	36.53
Age (years)	18-22	37	22.16
	24-26	67	40.12
	26-30	45	26.95
	Above 30	18	10.78
Education	Bachelor	108	64.67
	Masters	41	24.55
	Doctorate	18	10.78
Family Type	Joint family system	59	35.33
	Nuclear	57	34.13
	Extended	51	30.54

In the table above, there are 106 male participants, making up 63.47% of the total sample. There are 61 female participants, making up 36.53% of the total sample. The gender distribution shows a higher representation of male participants compared to female participants. This suggests a gender imbalance in the study population, which might influence the perception and experiences of cyber-crime due to potential gender-related differences in internet usage and exposure to cyber threats.

There are 37 participants in this age group, representing 22.16% of the total sample. This age group has the highest representation with 67 participants, making up 40.12% of the total sample. There are 45 participants in this age group, representing 26.95% of the total sample. This age group has the least representation with 18 participants, making up 10.78% of the total sample. The age distribution indicates that the majority of participants are within the 24-26 years age range. The least represented group is those above 30 years (18 participants, 10.78%). The age distribution indicates that the majority of participants are young adults, which is typical for a university student population and may affect their familiarity and interaction with technology and cybersecurity issues.

The majority of participants have a bachelor's degree, with 108 participants representing 64.67% of the total sample. There are 41 participants with a master's degree, making up 24.55% of the total sample. This group has the least representation with 18 participants, making up 10.78% of the total sample. The educational distribution shows a predominant number of participants holding a bachelor's degree. This educational distribution shows a high level of education among participants, which could correlate with their understanding and perception of cyber-crime and cybersecurity measures.

There are 59 participants from joint family systems, representing 35.33% of the total sample. There are 57 participants from nuclear families, making up 34.13% of the total sample. There are 51 participants from extended families, making up 30.54% of the total sample. The family type distribution is relatively

balanced, with a slight predominance of participants from joint family systems. This diversity in family types can provide insights into the socio-cultural contexts that may influence participants' attitudes and behaviours towards cyber-crime and cybersecurity.

The table provides a detailed breakdown of the demographic characteristics of the study participants, highlighting the gender, age, education level, and family type distributions. These insights can help in understanding the sample population's diversity and in analysing the influence of these factors on the study's outcomes.

Table 2

Responses of Item No. 1-11

Item No.	Items	SDA	DA	N	A	SA	Mean	Std. Dev	Mode
1.	Do you think Higher education meets the demand of advanced technology?	27	14	18	49	59	3.59	0.72	59
2.	Do you think Technical education fit into the aims of higher education?	37	36	24	29	41	3.01	0.60	41
3.	Do you think Highly educated people do not harm society?	21	15	15	52	64	3.74	0.75	64
4.	Do you think using Study courses included anything which causes to commit cyber-crime?	49	54	21	21	22	2.48	0.50	54
5.	Do you think Higher education guides people in term of any unethical thing that cause society damage?	15	14	21	58	59	3.79	0.76	59
6.	Do you think Students never read syllabus until something goes wrong or pressure of exams?	17	9	17	53	71	3.91	0.78	71
7.	Do you think Role of educated people against cyber-crime fight is essential?	11	14	8	42	92	4.14	0.83	92
8.	Do you think Everyone already know about cyber security?	57	41	15	21	33	2.59	0.52	57
9.	Do you think Cyber-crime impact on social life?	17	25	21	34	70	3.69	0.74	70
10.	Do you think Cyber threats can harm private businesses and government organizations?	12	15	4	55	81	4.07	0.81	81
11.	Do you think Cyber security professionals are enough to secure networks against cyber threats?	63	31	11	27	35	2.64	0.53	63

The analysis of Table 2, which summarizes the responses to items related to higher education and cyber-crime perception among university students:

Item 1: Higher education meets the demand of advanced technology (Mean: 3.59, Std. Dev: 0.72). A majority of respondents agree that higher education meets the demands of advanced technology, with the mean score leaning towards agreement.

Item 2: Technical education fits into the aims of higher education (Mean: 3.01, Std. Dev: 0.60). Responses are more neutral regarding whether technical education aligns with the aims of higher education, as indicated by a mean score close to 3.

Item 3: Highly educated people do not harm society (Mean: 3.74, Std. Dev: 0.75). Most respondents agree that highly educated individuals do not harm society, reflecting a generally positive view of educated people.

Item 4: Study courses include content that could cause cyber-crime (Mean: 2.48, Std. Dev: 0.50). Respondents tend to disagree that study courses include content that could lead to cyber-crime, suggesting a perception that educational content is generally ethical.

Item 5: Higher education guides against unethical behaviour causing societal damage (Mean: 3.79, Std. Dev: 0.76). Most respondents agree that higher education guides people against unethical behaviour that could harm society, indicating confidence in the ethical guidance provided by education.

Item 6: Students only read the syllabus under pressure (Mean: 3.91, Std. Dev: 0.78) Respondents largely agree that students tend to read the syllabus only when something goes wrong or under exam pressure, highlighting a common behaviour among students.

Item 7: Educated individuals' role in fighting cyber-crime is essential (Mean: 4.14, Std. Dev: 0.83). There is a strong agreement that the role of educated people is essential in combating cyber-crime, indicating the perceived importance of education in cybersecurity efforts.

Item 8: Everyone already knows about cybersecurity (Mean: 2.59, Std. Dev: 0.52). Respondents tend to disagree that everyone already knows about cybersecurity, suggesting a need for increased cybersecurity education.

Item 9: Cyber-crime impacts social life (Mean: 3.69, Std. Dev: 0.74). Most respondents agree that cyber-crime has an impact on social life, indicating awareness of the social implications of cyber-crime.

Item 10: Cyber threats can harm private businesses and government organizations (Mean: 4.07, Std. Dev: 0.81). There is a strong agreement that cyber threats can harm private businesses and government organizations, highlighting the perceived severity of cyber threats.

Item 11: Cybersecurity professionals are enough to secure networks against cyber threats (Mean: 2.64, Std. Dev: 0.53). Respondents tend to disagree that there are enough cybersecurity professionals to secure networks against cyber threats, suggesting concerns about the adequacy of cybersecurity workforce.

This analysis provides insights into the perceptions of university students regarding higher education and cyber-crime, reflecting their views on the effectiveness of education in addressing technological demands and ethical issues, as well as their awareness of cybersecurity challenges.

Discussion

The condition impacts individuals profoundly, particularly in circumstances where the analyst, after observing and enquiring about various life characteristics, family nature, and the settings of peers, found that these factors significantly influence the behaviour of any criminal during their upbringing. In some cases, individuals inherently adopt wrongful behaviour, often following the practices of their family-run organizations. Every member of such groups typically engages in their own unlawful activities, frequently treating it as a supplementary occupation. Higher education and criminal behaviour intersect on many fronts in social contexts (Shahid et al., 2022). To test this hypothesis, the analyst theoretically explored the area based on the collected data.

The findings revealed that the majority of respondents agreed that educated individuals play a crucial role in this regard. However, it was noted that most highly educated people are not involved in criminal acts; rather, it is usually the average individuals who engage in such activities and become offenders. A significant proportion also supported the notion that highly educated individuals possess a constructive understanding of technology and utilize it positively. This is why highly educated people are not deemed harmful to society;

instead, they spread awareness within the community. On the other hand, individuals without higher education gain specialization through daily experiences. This suggests that, in the absence of formal education, people acquire expertise independently. They learn while working under the supervision of highly educated individuals, gaining mastery over time. Once they achieve a level of authority, they might resort to cyber-crime as an easy way to earn money without much effort.

The outcomes established that larger part of individuals concurred that informed individuals assume in-dispensable job in such manner yet most much instructed are not included in this demonstration, just normal individuals enjoy such appealing things and become guilty party. A major extent was likewise in the support of that profoundly taught know innovation in constructive sense and utilize it in positive sense that is the reason very teach individuals are no unsafe for society they spread mindfulness among the general population of the network. While, without advanced education individuals have specialization all alone by every day encounters. It implies that without advanced education individuals have specialization by their own in such manner. It suggests individuals learn while working under the supervision of very taught individuals students get authority ended it then the person in question begin doing cyber-crime to win pain free income.

Conclusion

The research into the perception of cyber-crime among university students has yielded valuable insights into their awareness, attitudes, and behaviours towards cybersecurity. The findings underscore the importance of higher education in shaping students' understanding of advanced technology and ethical guidelines. While many students recognize the relevance of higher education in addressing technological demands and the essential role educated individuals play in combating cyber-crime, there are notable gaps in cybersecurity awareness and education.

Despite a general acknowledgment of the impact of cyber-crime on social life and the potential harm to private businesses and government organizations, there is a concerning perception that not everyone is well-versed in cybersecurity (Aurangzeb & Asif, 2021). This highlights the need for enhanced educational initiatives to improve cybersecurity literacy among students. Furthermore, the belief that there are insufficient cybersecurity professionals to secure networks against threats underscores the necessity for increased focus on training and developing a skilled cybersecurity workforce.

The study emphasizes the critical role of higher education institutions in fostering a culture of cybersecurity awareness and preparing students to navigate and mitigate cyber threats. By addressing the identified gaps and enhancing cybersecurity education, universities can better equip students with the knowledge and skills needed to protect themselves and contribute to a safer digital environment. The research findings provide a foundation for future studies and interventions aimed at improving cybersecurity practices and perceptions among university students.

Future Directions

Future research could focus on conducting longitudinal studies to track changes in cybersecurity awareness and behaviour among university students over time. This would provide insights into the effectiveness of educational interventions and how students' perceptions and practices evolve as they progress through their academic journeys. Investigate the impact of specialized cybersecurity programs and certifications on students' awareness and preparedness to combat cyber threats. This research could evaluate the effectiveness of these programs in enhancing students' skills and knowledge, and their subsequent influence on reducing cyber-crime incidents.

Conduct cross-cultural comparisons to explore how cultural differences influence students' perceptions of cyber-crime and cybersecurity. By examining the variation in attitudes and behaviours across different countries and regions, researchers can identify culturally specific factors that impact cybersecurity awareness and develop tailored educational approaches. Examine the outcomes of integrating comprehensive cybersecurity education into university curricula across various disciplines. This research could assess the long-term benefits of incorporating cybersecurity courses and training into the academic programs of non-technical fields, such as business, social sciences, and humanities.

Explore the role of peer influence and social networks in shaping students' perceptions and behaviours related to cyber-crime. This research could investigate how peer interactions and online communities contribute to the dissemination of cybersecurity knowledge and the adoption of safe online practices among university students. These future directions can help expand the understanding of cybersecurity awareness among university students and inform the development of effective educational strategies to mitigate cyber threats.

References

Adeshola, A., & Oluwajana, D. (2024). Assessing cybersecurity awareness, attitudes, and capacity to assess cybersecurity risks among university students. *Journal of Cybersecurity Research*, 12(2), 114-129.

Asghar, R. J., Jimshaid, A., & Choudhary, A. I. (2015). Impact of business education on corporate social responsibility (CSR). *IBT Journal of Business Studies (JBS)*, *2*(2).

Asif, M. (2021). Contingent Effect of Conflict Management towards Psychological Capital and Employees' Engagement in Financial Sector of Islamabad. *Preston University, Kohat, Islamabad Campus*.

Asif, M. (2022). Integration of Information Technology in Financial Services and its Adoption by the Financial Sector in Pakistan. *Inverge Journal of Social Sciences*, *1*(2), 23-35.

Asif, M., Pasha, M. A., Shafiq, S., & Craine, I. (2022). Economic impacts of post COVID-19. *Inverge Journal of Social Sciences*, *1*(1), 56-65.

Asif, M., Pasha, M. A., Mumtaz, A., & Sabir, B. (2023). Causes of youth unemployment in Pakistan. *Inverge Journal of Social Sciences*, *2*(1), 41-50.

Asif, M., & Sandhu, M. S. (2023). Social Media Marketing Revolution in Pakistan: A Study of its Adoption and Impact on Business Performance. *Journal of Business Insight and Innovation, 2*(2), 67-77.

Asif, M., & Shaheen, A. (2022). Creating a High-Performance Workplace by the determination of Importance of Job Satisfaction, Employee Engagement, and Leadership. *Journal of Business Insight and Innovation, 1*(2), 9-15.

Aurangzeb, D., & Asif, M. (2021). Role of leadership in digital transformation: A case of Pakistani SMEs. In Fourth International Conference on Emerging Trends in Engineering, Management and Sciences (ICETEMS-2021) (4(1), 219-229).

Aurangzeb, M., Tunio, M., Rehman, Z., & Asif, M. (2021). Influence of administrative expertise on human resources practitioners on the job performance: Mediating role of achievement motivation. *International Journal of Management, 12*(4), 408-421.

Bashir, M., Noor-e-Zahra, S., & Qaisar, Z. (2024). The Gig Economy and Automation: Implications for Human Resource Management in Pakistan. *Inverge Journal of Social Sciences, 3*(3), 41-53.

Broadhurst, R. (2018). An exploratory study on cybercrime risks in a university student community. *International Journal of Cyber Criminology*, 10(1), 45-60.

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa, 44*(1), 123-138.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology, 2*, 13-20.

Hussain, S., & Shahid, A. (2024). Social Media & Body Image: A Study of a Public Sector University in Islamabad. *Inverge Journal of Social Sciences*, *3*(4), 63-81.

Igba, D. (2018). Perception of cybercrime among university undergraduates and its implications on their academic achievement. *Journal of Information Security and Cybercrime Studies*, 6(3), 89-102.

Madero-Hernandez, A., & Fisher, B. S. (2012). Routine activity theory.

Nilupú-Moreno, D., Fernández-Muñoz, J., Gil-Garcia, J. R., & Rodríguez-Bolaños, R. (2024). Cybersecurity awareness among university students: A systematic review of the literature. *Cybersecurity Education and Awareness Journal*, 8(4), 203-220.

Shahid, N., Asif, M., & Pasha, A. (2022). Effect of Internet Addiction on School Going Children. *Inverge Journal of Social Sciences, 1*(1), 13-55.

Thompson, K. (1992). Quality control in higher education. *British Journal of Educational Studies, 40*(1), 51-56.