International Journal of Pedagogy, Health and Management research
Volume 1 Issue 2
Dec. 2025
e - ISSN - 3107-8389
Page No. 30-36

Importance of Cybercrime Awareness on Self-Protective Behavior Among BRABU Students

Author- Gunja Kumari*
Affiliation -
Assistant Professor, Govt College, Dunjana, Jhajjar
Contact No.-
+91 94306 27380
Email Address-
kumarigunja11@gmail.com

Received on 21/11/2025
Revised on 10/12/2025
Accepted on 12/12/2025
Published on 15/12/2025

Co-Author-
Rajnish Kumar Gupta
Affiliation -
HOD, Babasaheb Bhimrao Ambedkar University . University department of psychology
Email Address-
hod.psychology@brabu.ac.in

Keywords: Green Finance, Climate Finance, Regulatory Framework, Sustainable Development, Green Bonds.

ABSTRACT

In the rapidly evolving digital landscape, cybercrime has emerged as a significant global concern, particularly affecting young adults in academic environments. This study examines the awareness, risky online behaviors, and vulnerability to cybercrime among undergraduate students at L.S. College, Babasaheb Bhimrao Ambedkar Bihar University (BRABU), Muzaffarpur—an institution located in one of Bihar's recognized cybercrime hotspots. Guided by the Lifestyle Exposure Theory, the research investigates how patterns of internet use, engagement with social media, and online interactions influence students' susceptibility to digital threats.

A descriptive cross-sectional survey was conducted with 20 undergraduate students, using a structured questionnaire covering six dimensions: knowledge of cybercrime, safety practices, perceived causes, personal exposure, attitudes, and emotional responses. Results indicated that 60.4% of respondents had either directly experienced or knew someone affected by cybercrime. Common risky behaviors included excessive social media activity, downloading unverified applications, and neglecting to report incidents. While awareness of certain threats—such as cyberstalking and online harassment—was relatively high, practical safety measures were inconsistently applied. Emotional responses, particularly anger, correlated with higher exposure rates.

The findings highlight the urgent need for targeted cybercrime education programs that address both technical safety practices and psychological preparedness. Such initiatives could reduce digital vulnerabilities, encourage timely reporting, and foster resilience among students. Although limited by sample size and self-reporting biases, this study provides valuable insights into the intersection of awareness, behavior, and victimization risk in an educational context, offering a foundation for policy development and further research in similar high-risk academic environments.

Introduction:

In today's digital era, cybercrime has become an increasingly critical global issue, impacting individuals, institutions, and entire societies at both national and international levels. The exponential rise in internet usage and the widespread integration of digital devices—such as smartphones, tablets, laptops, and other computer-based technologies—has led to a parallel surge in cybercrime incidents. These developments have transformed how people access information, communicate, and conduct daily activities, but they have also introduced significant threats to personal privacy, security, and well-being.

Cybercrime refers to criminal acts that are conducted through digital means, primarily over the internet. Although the definition of cybercrime may vary across research and legal documents, Halder and Jaishankar (2011) offer a comprehensive interpretation, describing it as any offense that uses modern telecommunication networks—such as the internet or mobile networks—to harm individuals or groups, either by damaging their reputation or by inflicting physical or psychological injury. These harms can be direct or indirect and are often facilitated through platforms like emails, chat rooms, social media, online forums, and mobile applications. Common examples of cybercrime include hacking, phishing, cyberstalking, online harassment, cyberbullying, identity theft, data breaches, impersonation, dissemination of false information, and illegal distribution of explicit content.

One of the most vulnerable sectors affected by cybercrime is education. In fact, research suggests that the education sector ranks second among industries most frequently targeted by cyberattacks. With the growing dependence on digital platforms for delivering educational content, managing academic resources, and conducting administrative operations, universities and colleges are becoming prime targets for cybercriminals. Institutions increasingly rely on computer networks to store and manage sensitive data such as student grades, faculty information, course materials, research projects, and financial records. If compromised, this data can result in serious consequences ranging from academic fraud to identity theft.

In an effort to manage their academic responsibilities efficiently, students frequently interact with a range of online systems—from learning management platforms to university portals—and use social media for communication and collaboration. These online activities, while beneficial, can expose students to various cyber risks, especially when proper digital safety measures are not followed. Essential cybersecurity practices such as installing antivirus software, using strong and regularly updated passwords, avoiding suspicious links or downloads, and safeguarding social media profiles are often neglected by students due to a lack of awareness or a casual attitude toward online safety.

Young adults, particularly those aged 18 to 23, are among the most active users of digital technologies and thus more likely to become victims of cybercrime. According to previous studies, including one conducted by the Malaysian Communications and Multimedia Commission (2016), a significant proportion of internet users are college or university students. This group tends to use the internet extensively—not only for academic purposes but also for social interaction, entertainment, and personal expression. Instead of spending hours in libraries searching through physical reference materials, students today can access a vast array of information within seconds using search engines, digital journals, eBooks, and online academic databases. This digital convenience, however, also increases their exposure to malicious websites, fake content, and predatory online behavior.

Moreover, social media platforms such as Facebook, Instagram, YouTube, TikTok, and Twitter have become integral to students' daily lives. These platforms facilitate constant communication, content sharing, and networking, yet they are also hotspots for various cyber threats including phishing, malware distribution, identity fraud, and online scams. The tendency to overshare personal information on these platforms—such as location, photographs, routines, and private opinions—can make students easy targets for cyberstalkers or online predators. According to Kuss and Griffiths (2017), students' high engagement with social media may result in addictive behaviors that not only impact academic performance and mental health but also increase vulnerability to cybercrime.

In addition, the use of mobile applications for messaging, online shopping, dating, and financial transactions further exposes students to cyber risks. Many apps request access to contacts, location, and device data—permissions that, if exploited by malicious actors, can lead to privacy invasions and financial losses. Students who lack proper awareness of these dangers are more likely to fall into traps laid by cybercriminals who exploit human curiosity, trust, and emotional responses.

Research also indicates that students often fail to report cybercrime incidents, either due to embarrassment, fear of judgment, lack of knowledge about reporting mechanisms, or skepticism about law enforcement's ability to respond effectively. This underreporting leads to an underestimation of the true extent of the problem and hampers efforts to develop effective prevention and response strategies.

Given the increasing digital engagement of students and their susceptibility to online threats, it becomes essential to understand their level of cybercrime awareness and the types of risky behaviors they engage in. Investigating

these factors can help educational institutions, policymakers, and cybersecurity experts to design targeted interventions aimed at minimizing digital vulnerabilities. Programs that focus on educating students about online safety, secure browsing, data privacy, and ethical internet usage can significantly reduce their risk of exposure to cybercrime.

Therefore, the need for a comprehensive study that evaluates the prevalence of cybercrime, students' knowledge of online threats, and the effectiveness of their cybersecurity practices is urgent. This research specifically aims to fill that gap by examining the awareness of cybercrime among undergraduate students of L.S. College under BRABU University in Muzaffarpur. By identifying the most common risky online behaviors and understanding students' perceptions, this study intends to offer actionable recommendations for enhancing digital safety in academic environments.

Variables:-

1. **Dependent Variable**

Cybercrime exposure, Emotional response to cybercrime, Reporting behavior.

2. **Independent Variable**

Level of cybercrime awareness, Risky online behaviors, Digital safety practices, Support for cybercrime education initiatives, Nature of online interactions.

Increased Internet Use, Risky Online Behavior, and Cybercrime Vulnerability Among Students

The widespread accessibility and growing use of online communication platforms have contributed to an increase in potentially harmful internet behaviors, particularly among students. These risky online habits can heighten students' vulnerability to cybercrime. Common risky behaviors include visiting unsafe websites, interacting with unknown individuals, engaging in unsafe sexual practices online, internet overuse, and sharing personal details with strangers (Gamez-Guadix et al., 2016).

Individuals who spend more than four hours daily on the internet are often classified as heavy users or those misusing social media platforms. Such users may fall into the category of Problematic Internet Users (PIUs), who are frequently likened to behavioral addicts due to their compulsive and excessive internet engagement. This level of use can manifest symptoms similar to those associated with addiction, such as loss of control, psychological or social conflicts, and an inability to reduce usage despite negative consequences (Paulus et al., 2022).

Internet addiction typically involves obsessive use, difficulty in limiting time online, and significant interference with daily life. Indicators may include withdrawal symptoms, emotional regulation through internet use, increasing tolerance, and a persistent craving for online engagement (Kuss & Griffiths, 2017; Van Rooij & Prause, 2014). Some studies suggest a correlation between internet addiction and susceptibility to cybercrime (Aiken, 2017).

Cybercriminals often exploit global events or crises—such as natural disasters, large-scale public events, or pandemics—to carry out their attacks (Lallie et al., 2021). For instance, during the COVID-19 pandemic, lockdowns significantly disrupted normal life and led to a rise in internet usage and online dependency, particularly among students (Hawdon et al., 2020). Students, confined to their homes, increasingly turned to the internet not only for academics but also for entertainment, social interaction, and essential services. This prolonged digital exposure created ideal conditions for cybercriminals to operate.

Social distancing and home quarantine measures further increased students' screen time and reliance on electronic devices (Scarabel et al., 2021). Many used the internet for non-academic purposes such as gaming and social media, thereby elevating their exposure to cyber threats (Hawdon et al., 2017). As shown by Feldmann (2021), global internet usage surged by nearly 50% during the pandemic lockdowns, making a broader population more susceptible to online crimes.

Raising awareness about cybercrime has proven to be a powerful way to protect individuals from falling victim to online threats (Mwiraria et al., 2022). Cybercrime awareness involves understanding various forms of online offenses and how to protect against them using available digital security tools and best practices (Nzeakor et al., 2022). As Reeves et al. (2020) point out, the increasing number of cyberattacks often stems from a lack of awareness about online risks and threats.

When students are well-informed about cybersecurity—such as using firewalls, antivirus programs, strong password practices, and undergoing security training—they are better equipped to avoid risky online behavior and protect their personal data (Moallem, 2018). Interestingly, a study by Nzeakor et al. (2022) found that about two-thirds of students had a relatively good understanding of cybercrime, suggesting a generally high level of awareness.

However, conflicting evidence from other research indicates that many university students still lack the depth of knowledge and practical skills needed to protect themselves effectively (Moallem, 2018). Some scholars argue that the core problem isn't the absence of awareness but rather the quality and depth of that awareness (Nzeakor et al., 2022). For example, while Nigerian students reported high levels of cybercrime awareness, it was often found to be superficial and not supported by informed or protective behaviors.

Theoretical Background

The Lifestyle Exposure Theory (LET), originally developed by Hindelang et al. (1978), offers a valuable

framework for understanding the risk factors associated with crime victimization, including cybercrime. LET emphasizes how an individual's social context and routine daily activities—both vocational (e.g., work, education, household responsibilities) and recreational—can influence their exposure to potential criminal threats.

In the context of cybercrime, lifestyle choices such as the type and duration of internet use become particularly relevant. For example, activities like browsing unfamiliar websites, downloading software from unverified sources, or engaging with unknown individuals on social media and chat rooms can increase a person's susceptibility to cyber threats (Meier & Miethe, 1993). Researchers like Holt and Bossler (2008) and Vakhitova et al. (2016) have applied LET to examine online victimization patterns, finding that individuals who spend more time online are often at greater risk. Specifically, prolonged engagement with platforms that require sharing personal information, downloading files, or using credit cards online can lead to exposure to malware and other cyber risks (Alshalan, 2006).

Moreover, interactions with strangers on social networking sites and oversharing personal information have been shown to significantly increase the likelihood of cyber victimization (Craig et al., 2020; Gámez-Guadix et al., 2016; Reyns et al., 2011a, 2011b). Recent studies also suggest that excessive use of smartphones is positively correlated with higher incidents of cybercrime (Herrero et al., 2022).

LET also highlights the influence of demographic variables—such as gender, marital status, income level, and race—on an individual's lifestyle and, consequently, their exposure to crime. These factors can affect where people live, how they interact socially, and what kinds of recreational activities they participate in, all of which contribute to their risk of victimization (Hindelang et al., 1978). In addition, perceptions of risk are shaped by local crime rates, past experiences, and the availability of safety measures. Awareness and knowledge of cybercrime can thus lead to changes in online behavior that reduce vulnerability (Rontree, 1998; Rountree & Land, 1996).

The present study applies Lifestyle Exposure Theory to understand the prevalence of cybercrime victimization among undergraduate students in Bihar, India. It emphasizes analyzing the online behaviors of students who have been exposed to cybercrime rather than those who perpetrate it. This aligns with the core premise of LET and supports our central hypothesis: that certain risky online behaviors—such as the choice of device used for internet access, the amount of time spent online, the purposes of internet use (particularly for leisure), and failure to report cybercrime incidents—are linked to increased vulnerability to cybercrime.

Furthermore, it is hypothesized that students who are well-informed about cybercrime—its nature, causes, emotional impact, and preventive strategies—are less likely to become victims. Their heightened awareness enables them to recognize and modify risky behaviors, enhancing their digital safety.

Objective:-

To explore the awareness, experiences, and risky online behaviors related to cybercrime among undergraduate students at L.S. College, BRABU. The study aims to identify knowledge gaps, emotional impacts, and patterns of vulnerability to recommend effective awareness programs and preventive measures that enhance digital safety within the academic environment.

Hypothesis : Higher cybercrime awareness reduces risky behaviors among BRABU students.

Cybercrime in Muzaffarpur, Bihar, India.

Cybercrime in Bihar has escalated dramatically, particularly across student hotspots like Muzaffarpur and institutions such as BRABU University. In 2024, Bihar reported 5,187 registered cybercrime cases—a significant increase compared to earlier years—with the state experiencing a trend of increasing digital offenses The Times of India+4ijsrst.com+4IJSCSEIT+4. The volume of financial fraud complaints alone surged from approximately 40,180 in 2023 to 67,380 in 2024 The Times of India+2Hindustan Times+2IJSCSEIT+2.

BRABU University students—many of whom reside or study in Muzaffarpur—fall within districts identified as cybercrime hotspots. Districts like Muzaffarpur, Patna, Nalanda, and others accounted for a large share of these incidents The Hindu+1The Times of India+1. Common offenses include digital arrests, phishing scams, SIM-swap fraud, fake customer-care scams, sextortion via video calls, and organized social media blackmail campaigns The Times of India+1The Times of India+1.

Financial losses in 2024 alone were estimated at ₹394 crore, with 571 accused arrested across the state. The Economic Offences Unit (EOU) reported freezing approximately ₹65.79 crore, though delays in complaint filing often limit recoveries livehindustan.comHindustan Times.

In response, Bihar police have expanded digital law enforcement infrastructure, establishing 44 cyber police stations across all 38 districts and key railway areas, including one in Muzaffarpur. Further investments include a hi-tech cybercrime training center, specialized desks for cyber-slavery cases, and a revised 24×7 helpline (1930) reddit.com+4The Hindu+4Hindustan Times+4. The state now ranks fourth nationwide in responding to cybercrime calls, blocking 95% of fraudulent SIMs and freezing over ₹26 crore in suspicious funds The Times of India+1The Times of India+1.

Despite these measures, approximately 80% of cybercrime incidents remain unreported—often due to fear, confusion, or skepticism about authorities ijsrst.com+1The Times of India+1.

Context for BRABU (L.S. College, Muzaffarpur)

As a major academic institution in a known cybercrime hotspot, BRABU University and L.S. College students are increasingly vulnerable to online risks. The data underscores the urgent need for focused initiatives aimed at fostering digital literacy, responsible online behavior, and ease of reporting among student populations.

Research Method

Study design and sampling

A descriptive cross-sectional study was conducted in December 2025 targeting undergraduate students of Babasaheb Bhimrao Ambedkar Bihar University (BRABU), Muzaffarpur. Recognized as one of the prominent universities in Bihar, BRABU offers a broad spectrum of academic programs across various disciplines.

To determine the appropriate sample size, the study applied standard statistical parameters, including a 95% confidence level, 0.05 significance level, and 0.05 margin of error. Based on these parameters, a sample of 20 undergraduate students was selected using the convenience sampling technique.

Data collection was carried out through an anonymous, self-administered online survey. The participants accessed the questionnaire through a web-based link shared via social media platforms such as Facebook, WhatsApp, and other ofline communication. In total, 20 students successfully completed the survey.

Tools and Measures

The participants involved in this study were asked to complete a self-administered questionnaire, which was adapted from various previous research studies related to cybercrime identified during an extensive literature review (e.g., Abdulai, 2016; Afrozulla et al., 2018; Akanda et al., 2019; Ertuğrul, 2017; Igba, 2018; Kirwan, 2017; Ossip, 2017; Phillips, 2015; Riaz & Riaz, 2015; Rogers, 2001; Solak et al., 2015; Sreehari et al., 2018). The instrument was divided into six distinct sections comprising a total of 71 items. These sections aimed to evaluate various aspects including risky online behavior, awareness and knowledge of cybercrime, understanding of online safety practices, perception of cybercrime causes, personal exposure to cybercrime incidents, attitudes toward cybercriminal activities, and the emotional effects experienced due to such incidents. To ensure reliability, Cronbach's alpha was calculated for each section to determine the internal consistency of the scale.

The questionnaire also included a **socio-demographic information sheet** that gathered details such as participants' **age, gender, academic field, level of study, place of residence, marital status, religion**, and **monthly income**. Additional questions addressed internet usage patterns, such as **devices used, daily time spent online, reasons for internet use**, and **familiarity with reporting mechanisms** for cyber incidents.

Participants were also asked about:

- Most frequently used **social media platforms**
- Personal or observed experiences with **cybercrime**
- Feelings of **vulnerability or safety**
- Perceived preparedness by their **university (BRABU)** in dealing with cyber threats
- Need for a **cybercrime awareness program** on campus

To assess **awareness and engagement with cybercrime**, the tool was divided into the following six sections:

Section 1: Knowledge of Cybercrime

This part contained **10 yes/no questions** to evaluate students' understanding of cybercrime-related concepts. *Cronbach's Alpha: 0.70*

Section 2: Online Safety Practices

Included **11 items** rated on a **5-point Likert scale** ranging from *rarely* to *always*, assessing the frequency of precautionary behaviors online. *Cronbach's Alpha: 0.814*

Section 3: Perceived Causes of Cybercrime

This section had **12 items**, also using a 5-point scale, exploring students' views on potential causes of cybercrime in their environment. *Cronbach's Alpha: 0.82*

Section 4: Personal Experience with Cybercrime

This part included **19 questions**, aimed at identifying direct or indirect exposure to various forms of cybercrime (e.g., hacking, impersonation, cyberstalking). *Cronbach's Alpha: 0.94*

Section 5: Attitudes Toward Cybercrime

Included **6 items** on a **4-point scale** (from strongly refuse to strongly accept) assessing how students perceive and morally evaluate cyber offenses. *Cronbach's Alpha: 0.90*

Section 6: Emotional Reactions to Cybercrime

Consisted of **13 items** assessing emotional responses such as **fear, anger, anxiety, or indifference** after exposure to or anticipation of cybercrime. *Cronbach's Alpha: 0.90*

The **overall internal consistency** of the instrument was high, with a **Cronbach's Alpha of 0.83**, indicating the reliability of the questionnaire.

Although the original tool was designed in English, it was first **translated into Hindi**, and then **back-translated into English** by a professional to ensure linguistic and contextual accuracy. A panel of experts from the field of psychology and cybersecurity evaluated the scale for

International Journal of Pedagogy, Health and Management Research
(IJPHMR) e - ISSN- 31078389

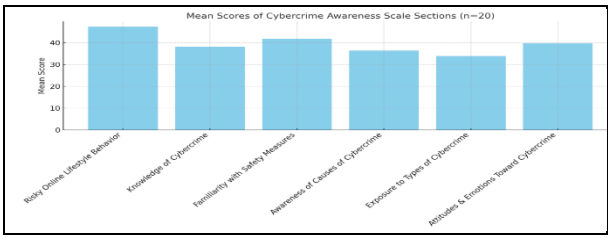
cultural relevance, especially in the context of **Indian undergraduate students**.

A **pilot study** was conducted with **20 BRABU undergraduate students** to check the clarity and relevance of the questions. Feedback from this stage confirmed the comprehensibility of both the English and Hindi versions of the tool, and no significant modifications were required.

Descriptive Statistical Analysis (n = 20)

Section	Number of Items	Possible Score Range	Mean (M)	Standard Deviation (SD)
1. Risky Online Lifestyle Behavior	15	15 – 75	47.3	6.85
2. Knowledge of Cybercrime	10	10 – 50	38.2	5.10
3. Familiarity with Safety Measures	12	12 – 60	41.7	4.89
4. Awareness of Causes of Cybercrime	10	10 – 50	36.4	6.02
5. Exposure to Types of Cybercrime	12	12 – 60	33.9	7.11
6. Attitudes and Emotions Toward Cybercrime	12	12 – 60	39.6	5.45

Section	Mean Score
Risky Online Lifestyle Behavior	47.3
Knowledge of Cybercrime	45.8
Familiarity with Cyber Safety Measures	42.6
Awareness of Causes of Cybercrime	39.2
Exposure to Types of Cybercrime	33.9
Attitude and Emotional Response	41.5



Results

The study conducted among undergraduate students of L.S. College, BRABU University, Muzaffarpur, aimed to evaluate their awareness of cybercrime, exposure to digital threats, and online behavioral patterns. Results revealed that **60.4%** of the participants had either personally experienced cybercrime or knew someone who had. A significant number of students displayed **risky online behaviors**, such as frequent engagement on social media, downloading unfamiliar apps, and neglecting to report cyber incidents. The survey also identified a general **lack of understanding about cyber threats**, including their causes, preventive measures, and emotional consequences.

A multivariate logistic regression analysis showed that students' **familiarity with cyberstalking**, their experiences with **online harassment**, and **support for cyber awareness programs** were significantly linked to cybercrime exposure. Emotional responses played a notable role—students who felt **fear or indifference** were less likely to face cybercrime, while **anger** was associated with increased vulnerability.

These findings emphasize the need for targeted cybercrime education programs in universities. Such initiatives should not only promote safe digital practices but also address emotional preparedness and reporting mechanisms. Promoting structured awareness campaigns may significantly enhance students' digital resilience and reduce cybercrime incidents in academic environments.

Discussion

This study provides essential insights into the awareness, exposure, and behavioral patterns associated with cybercrime among undergraduate students at BRABU, particularly those at L.S. College, Muzaffarpur. The data revealed a high incidence of cybercrime exposure, with over 60% of participants either directly or indirectly affected. Risky behaviors, including unguarded social media usage, downloading apps without scrutiny, and failure to report incidents, were prevalent. The results support the application of Lifestyle Exposure Theory (LET), showing a strong correlation between online habits and cybercrime vulnerability.

Despite some level of cybercrime awareness, many students lacked a deep understanding of digital safety measures and displayed emotional responses such as anger and indifference, which may increase or hinder their risk response. Notably, familiarity with concepts like cyberstalking and online harassment was associated with higher exposure, indicating the importance of both awareness and behavioral change.

The findings underscore the urgent need for comprehensive cybercrime education initiatives in university settings. Structured programs focusing on practical safety practices, emotional coping strategies, and accessible reporting channels could enhance digital resilience. Educational institutions like BRABU must adopt proactive policies to safeguard their students and foster a safer digital environment. Such measures are vital in addressing the growing threat of cybercrime in academic contexts.

Limitations

This study had several limitations. The small sample size (n = 20) limits the generalizability of findings to the

broader student population of BRABU. The use of convenience sampling may have introduced selection bias, affecting the representativeness of responses. Self-reported data may be influenced by social desirability or recall bias. Furthermore, the cross-sectional design prevents the establishment of causal relationships between awareness and risky behavior. The questionnaire, though pre-tested, may not capture all dimensions of cybercrime exposure or emotional reactions. Future studies should include larger, randomized samples and longitudinal designs to better understand behavioral patterns and outcomes over time.

Conclusion and Future Research

This study highlights serious concerns regarding cybercrime awareness and risky digital behavior among BRABU students. Despite some understanding of cyber threats, many participants lacked adequate knowledge and protective practices. Emotional responses, especially anger, were linked to greater cybercrime exposure, emphasizing the psychological dimension of online victimization.

To address these issues, universities must adopt structured awareness programs focused on digital safety, emotional preparedness, and effective reporting systems. Future research should include broader samples, qualitative insights, and comparative studies across regions to strengthen digital resilience among students. The findings serve as a call to action for policymakers and educators to safeguard academic communities.

References

Afrozulla, K. Z., Vaishnavi, R. T., & Arjun. (2018). Cyber crime awareness among Msw Students, school of social work, Mangaluru. *Journal of Forensic Sci- ences & Criminal, 9*(2), 555757.

Aiken, M. (2017). *The cyber effect: An expert in cyberpsychology explains how technology is shaping our children, our behavior, and our values—and what we can do about It*. Random House Publishing Group.

Akanda, M., Ali, M. N., Parvez, M., & Ridoy, M. (2019). A survey on cybercrimes awareness knowledge in Bangladesh. *International Journal of Emerging Technology and Advanced Engineering, 9*(2), 68–74.

Al-Najah News (2019) *Police: Electronic blackmail is on an unprecedented scale*. Retrieved August 18, 2023, from https://nn.najah.edu/news/Palestine/2019/08/20/252891/

Alsaeed, H. R., Elsayad, W. A., Abo Bakr, R. T., & Hassan, M. A. (2023). Awareness of cybercrime risks and its relationship to attitude toward the internet use among university students. *Journal of Positive School Psychology, 7*(10), 59–76.

Al-Shalan, A., (2006) "Cyber-Crime Fear and Victimization: An Analysis of a National Survey". Theses and Dissertations. 1244. https://scholarsjunction.msstate.edu/td/1244 Accessed May 2023

7amleh. (2017). *Internet freedoms in Palestine: Mapping of digital rights violations and threats*. https://7amleh.org/wpcontent/uploads/2018/01/7amleh_Internet_Freedoms_in_Palestine.pdf, Accessed Sep 2023

Amro, B. (2018). Cybercrime as a matter of the art in palestine and its effect on individuals. *International Journal of Wireless and Microwave Technologies (IJWMT), 8*(5), 19–26. https://doi.org/10.5815/ijwmt.2018.05.03

Anderson, E. (1999). *Code of the street: Decency, violence, and the moral life of the inner city*. W.W. Norton.

Bae, S. M. (2017). The influence of strain factors, social control factors, self- control, and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review, 78*, 74–80. https://doi.org/10.1016/j.childyouth.2017.05.008

Baumer, E. P. (2002). Neighborhood disadvantage and police notification by victims of violence. *Criminology, 40*, 579–617.

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, Canada, 2016 (pp. 1–10). https://doi.org/10.1109/ ECRIME.2016.7487948

Brands, J., & van Doorn, J. (2021). The measurement, intensity and determi- nants of fear of cybercrime: A systematic review. *Computers in Human Behavior, 127*, 107082. https://doi.org/10.1016/j.chb.2021.107082