Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

College Students Attributional Differences in Knowledge Awareness About a Cybercrimes Law

Diab M. Al-Badayneh[1], Hamad M. Al Dosari[2], Hamed M. Al Qahtani[3], Jassem A. Alkhater[4], Sada S. Mehawesh[5]

Abstract

The study examines attributional differences in assessing the level of knowledge awareness about Jordanian Cybercrimes Law (JCL) among college students. The study sample comprised 500 Jordanian students representing four Jordanian universities (TTU, MU, JU, & BU). Of these, 43% were males, and 57% were females. Students (19%) reported being victims of cybercrimes, and 24% were perpetrators. Reliability as estimated by the scale's Cronbach's a was 0.66, and the validity (correlation between the scale and LSC scale) was 0.157 a = 0.00 (F = 187.161, a = 0.00). More than 25% of the sample read about the JCL and observed that the law has been politicized. Moreover, three-quarters of them heard about it. More than half of the sample witnessed illegal actions on the net that required punishment. Less than 10% of the sample dealt with the JCL or participated in an online action that required punishment. ANOVA analysis of the mean gender differences in cybercrime knowledge showed females were more knowledgeable about JCL than males (F = 4.402, a =.036). Furthermore, an ANOVA analysis of the mean external attribution differences (yes vs. no) in JCL knowledge (F = 4.402, a =.036) was performed. Finally, ANOVA analysis of the mean external attribution differences in the knowledge of JCL (F = 4.402, a =.036).

Keywords: *College Students, Cybercrimes, Law, Jordanm, Attribution, Knowledge.*

Introduction

Cybercrime is a criminal activity involving computers, networks, or devices, often motivated by financial gain. It can be divide it into three categories: crimes involving the computing device, crimes using the computer as a weapon, and crimes using the computer as an accessory. Cybercriminals can be individuals or groups with little technical skill, or highly organized global criminal groups. Common types include cyberextortion, Cryptojacking, identity theft, credit card fraud, cyberespionage, software piracy, and exit scams. Common examples include distributed DoS (DDoS) attacks, malware, phishing campaigns, credential attacks, and hijacking websites. Other examples include illegal gambling, illegal items, and child pornography. Cybercrimes, also known as computer violations, computer criminality, malicious use of computers, and internet crime, are illegal, unethical, and unauthorized behavior in systems that automatically process or transmit information. They can extend beyond a room, city, country, or continent and are often referred to as computer-related crime, crimes committed via computers, high-tech crime, computer crime, and IT crime. (Ozdamli & Ercag, 2019).

Cyberspace has significantly impacted everyday life, with Jordan's internet users accounting for 88% of the population. This growth has transformed individuals' expectations and behaviors, creating opportunities and challenges for government and society. Despite taking responsible precautions and adhering to social norms, there is evidence that a deviant subculture in cyberspace pollutes the online environment through criminal activities. The number of cybercrime cases in Jordan has increased from 1039 in 2012 to 16,027 in 2022, categorized into cyber-blackmail, defamation, data theft, hacking, theft, and threat. (Maghaireh, 2023). Jordan has started to recognize cybercrimes as a social, political, legal, and health problem. Victims can

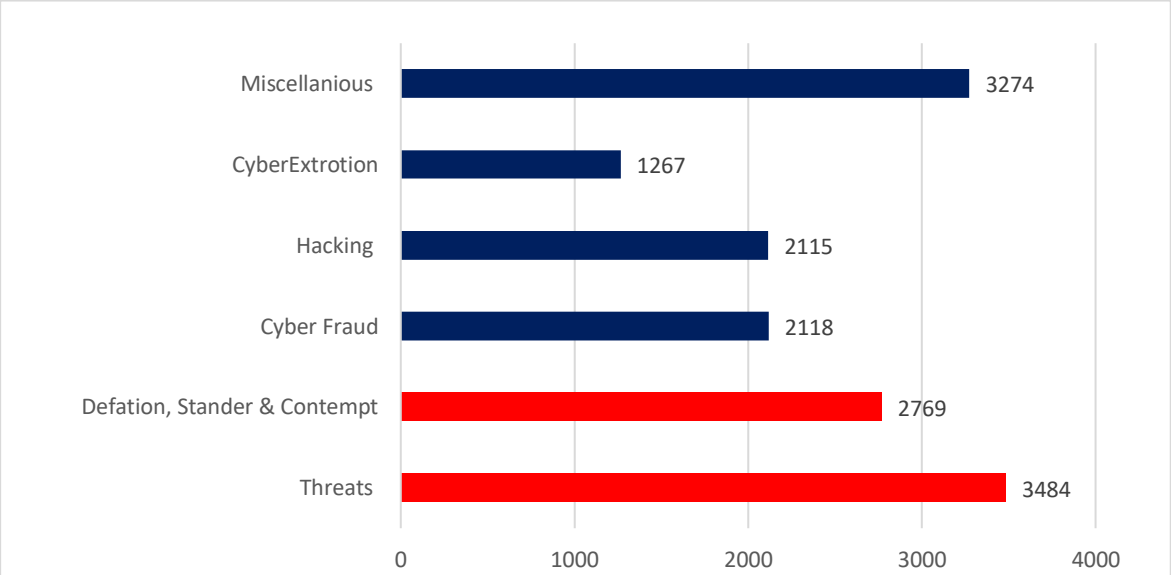
[1] Ph.D. Methodology, Criminology, and Security Studies, Department of Security Studies, Graduate College, Police Academy, MOI, Qatar & IKCRS, Amman, Jordan, Email: dbadayneh@gmail.com, ORCID 0000-0001-7416-6722.
[2] Department of Security Studies, Graduate College, Police Academy, MOI, Email: hmh458@outlook.com, 0009-0007-2125-0323
[3] Department of Security Studies, Graduate College, Police Academy, MOI, Email: hmf_5060@hotmail.com, 0000-0003-3533-6922
[4] Department of Security Studies, Graduate College, Police Academy, MOI, Email: Jassimalkhater@gmail.com, 0009-0004-8616-626X
[5] Department of Security Studies, Graduate College, Police Academy, MOI, Email: ssajm1986@gmail.com, 0009-0007-8095-9287

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

report a crime through 911 services or at a police station, and they can reach out and discuss options to end the bullying if legal action is required (Al-Nasser, 2021).

Jordan has seen a significant increase in cybercrimes, with over 1103 crimes committed until November 2011. Since 2012, the number of cybercrimes has reached 47 cases, including impersonation, e-defamation, threats, financial fraud, and email theft. In 2011, there were 427 cases of impersonation, 350 threats, 21 e-financial fraud cases, 40 email thefts, and two cases of internet server theft (Almany, 2012). Jordanian prosecutors report an average rate of cybercrime harassment, with a significant relationship between harassment and blackmail crimes. Harassment can lead to six consequences: threatening victims, family breakdown, social decay, loss of values, skepticism, and security instability. They recommend increasing awareness and criminalizing crimes. (Al-Khaza'leh & Lahiani, 2023)

Figure 1 Types of cybercrimes 2022 (UCC, 202) (Date from Alhadidi, Nweiran & Hilal, 2023).



The statistics reveal Jordan's severe cybercrime problem, necessitating further research to estimate prevalence and cause factors. This information could aid strategic plans, preventive measures, and awareness campaigns, enabling university administration and educators to create safer classroom environments.

Jordanian authorities have been modernizing cybercrime legislation since 2010, with the Cyber Crimes Act (2015) and the Cyber Crimes Act 2023 (ECA) being the most recent. However, concerns about freedom of expression have led to the controversial Cybercrimes Act 2023, which has sparked criticism from human rights organizations and activists. Jordan has implemented a variety of legislative measures to combat cybercrime, including the introduction of the Information Systems Crimes Act No. 30 in 2010 and the Cyber Crimes Act 2015 in 2015. However, concerns remain about the effectiveness and precision of these laws. The Jordanian Legislation and Opinion Bureau released a draft of proposed amendments in 2017, which drew criticism for imposing undue restrictions on freedom of expression. The Cyber Crimes Act of 2023 in Jordan has sparked controversy over its potential impact on freedom of expression. It's critical to analyze the law's relationship with individual rights as Jordan navigates cybersecurity while upholding democratic values. (Maghaireh, 2023).

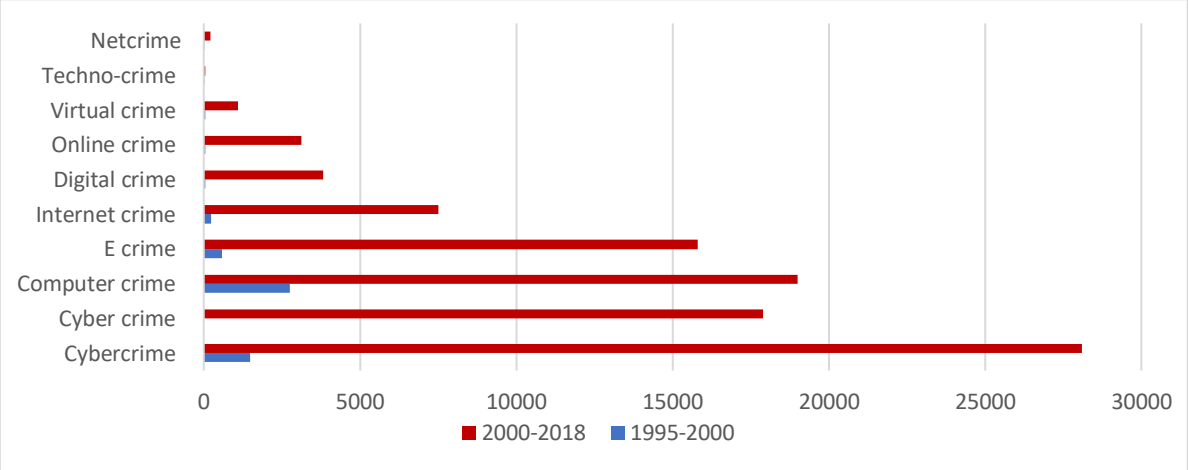
Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

Literature Review

Cybercrime: The Concept

Various terms have referred to 'Cybercrime' since its inception, with the prefix 'cyber' originating in cybernetics. As technology usage increased in the 1980s and 1990s, it became synonymous with cyberspace, cybershopping, and cybersurfing. The term "cybercrime" has been dominant since 2000, primarily used for harmful or illicit activities like cybercrime, cyberbullying, cyberterrorism, and cyberstalking. However, a systematic approach to defining and labeling cybercrime is lacking. Cybercrimes encompass a wide range of offenses and harmful behaviors, including traditional and unique crimes in the cyber landscape. No sources have provided an exhaustive list of known cybercrimes, likely due to the diverse set of behaviors and the rapidly expanding field.

The United States identified the concept of cybercrime under 12 headings, and the joint report of the EU and UN commission enumerates cybercrimes under various headings. Commonly used malware includes viruses, scams, rootkits, spam, and rabbits. Various methods, such as scavenging, eavesdropping, data diddling, trojan horse, scanning, super zapping, salami techniques, trap doors, asynchronous attacks, network worms, viruses, piggybacking, spam, logic bombs, masquerading, and credit card fraud, can commit cybercrimes, (Ozdamli & Ercag, 2019).



Note. Copyright 2020 by Routledge, from McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In The Human Factor of Cybercrime; Leukfeldt, R., Holt, T.J., Eds.; Routledge:New York, NY, USA, 2020; p. 8 (Table 1.1 and 1.2). (cited in (Phillips et al., 2022, p. 3)

Cybercrime and cybercrime concepts appeared in the literature 1476 times from 1995 to 200. The number of instances increased to 28100 and 17900, respectively. Computer crime, E crime, Internet crime, and digital crime occurred in 1995-2000 (2760, 585, 236, 50, respectively) and increased to (19000, 15800, 7500, and 3830, respectively). Figure 1 presents the cybercrime terminology in 1995–2000 and 2001–2018.

Table 2 Most Used Definitions of Cybercrimes in The Literature

Year	Organization	Definition of Cybercrime
1994	The United Nations	"The United Nations manual [23] on the prevention and control of computer-related crime (1994) uses the terms computer crime and computer-related crime interchangeably. This manual did not provide any definition" (p. 116)
2013	United Nations Office on Drugs and Crime (UNODC)	The UNODC defines cybercrime as any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. This includes offenses such as computer-related fraud, forgery, and identity theft

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

2000	The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders	1. "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them." 2. "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or is tributing information by means of a computer system or network" (p. 5)
2001	The Council of Europe Cybercrime Convention (also known as The Budapest Convention)	"action directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems, networks, and data by providing for the criminalization of such conduct" (p. 2)
2007	The Commission of European Communities	"criminal acts committed using electronic communications networks and information systems or against such networks and systems" (p. 2)
2013	Cybersecurity Strategy of the European Union	"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (p. 3)
2016	Commonwealth of Independent States Agreement	"a criminal act of which the target is computer information" (cited in Akhgar et al. (p. 298))
2005	European Union's Directive on Attacks against Information Systems (2005/222/JHA)	This directive defines cybercrime as offenses against information systems, including unauthorized access, system interference, and data interference, aiming to harmonize criminal law across the EU.
2002	Asia-Pacific Economic Cooperation (APEC)	APEC defines cybercrime as any criminal offense involving a computer system or network, including traditional crimes committed online. APEC emphasizes cooperation and capacity building to combat cybercrime.
n.d.	Interpol	Interpol defines cybercrime as any crime facilitated by or committed through the use of computer networks or hardware devices. This includes advanced cybercrime, such as cyber-attacks on computer systems, and cyber-enabled crime, such as online fraud and child exploitation.
2000	Thomas and Loader	Thomas and Loader (in 2000) define cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3),
2006	Gordon and Ford	whereas Gordon and Ford (in 2006) define cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device" (p. 14).
2021	Europol	Europol has defined cybercrime as "a growing problem for countries, such as EU Member States, in most of which Internet infrastructure is well developed and payment systems are online" p.1
2017, 2021	The European Cybercrime Center IOCTA	The European Cybercrime Center defined cybercrime as "any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)" p.3
n.d.	U.S. Department of Justice (DOJ)	The DOJ defines cybercrime as criminal offenses committed with the aid of a computer and a network, including crimes where the computer is the target (e.g., hacking), the tool (e.g., fraud), or incidental to the crime (e.g., storage of illegal data).
2015	Jordan Cybercrime Law No. 27 of 2015.	Every act criminalized by laws that would attack material and/or moral conditions is the result, directly or indirectly, of the intervention of information technology. Every act or omission using a technological means is punishable by law. All laws are in force in the Kingdom according to the text of Article 15 of the Cybercrime Law No. 27 of 2015.

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

2023	Cybercrime Law No. 17 of 2023	The Cybercrime Law criminalizes activities like unauthorized access to information networks, fake accounts, misinformation, phishing, and illegal donations. It also prohibits promoting prostitution, obtaining information on weapons, and possessing electronic data.

Jordan Definition of Cybercrimes Law

Cybercrime Law 17, 2023, defines cybercrimes as follows: The Cybercrime Law criminalizes various activities such as gaining unauthorized access to information networks, creating fake accounts, spreading misinformation, phishing schemes, collecting donations without a license, promoting competitions without a license, creating pornographic material, inciting prostitution, manufacturing weapons, and possessing electronic data without permission. It also prohibits promoting or inciting prostitution and immoral sexual behavior and obtaining information on weapons, ammunition, or explosives. The law also prohibits possessing electronic data, passwords, or access codes for committing crimes.

Related Literature Review

Cybercrime in Jordan is rising, with one million cases annually. However, authorities only officially report 5% of these offenses. The Anti-Cybercrimes Unit reports a significant increase in cybercrimes, with threats, extortion, defamation, slander, and contempt being the most prevalent. The number of cybercrimes targeting families and children has also seen a rise, with the number of reported crimes reaching 1011. Online child abuse has also seen a significant increase, with the occurrence rate reaching its peak in 2016. Despite the severity of cybercrimes targeting families and children, the statistics for 2022 indicate a relatively low incidence. Experts project global cybercrime costs to reach $6 trillion by 2021, and they anticipate an increase to $10.5 trillion by 2025. (Alhadidi, Nweiran, & Hilal, 2024).

Students at the University of Jordan differed in their understanding of cybercrime concepts, legal procedures, the unlawful acts they committed, and the unlawful acts they encountered. Results showed that males had a higher awareness of cybercrime concepts and legal procedures compared to females. Male students demonstrated a higher awareness of unlawful acts committed by their peers and the exposure to such acts . Male students may have a higher rate of cyber threat awareness due to personal experiences or knowledge gained from family members or acquaintances who have committed cybercrimes. (Alhadidi, Nweiran, & Hilal, 2024).

Research indicates that young males tend to have less self-control compared to females, leading to unlawful acts. Low self-control is a major cause of crime, characterized by impulsiveness, high risk-seeking potential, self-centeredness, and physicality. Socialization plays a significant role in committing reckless behavior, as Jordanian society allows males to engage in reckless acts forbidden for females. Men are more likely to be victims compared to women. Females' awareness of cybercrime legal procedures may be due to their fear and more cautious nature, supporting Titi's findings that women are more aware of cyber regulations than men. (Alhadidi, Nweiran, & Hilal, 2024).

A study by Alhadidi, Nweiran, & Hilal (2024) examines the level of awareness among students at the University of Jordan, revealing variations based on factors such as gender, academic level, academic achievement, and school type. The study also reveals that students often engage in illegal behaviors despite knowing the legal ramifications. The lack of efficient punitive measures does not result in a reduction in criminal activity. To address this issue, the study suggests integrating cybercrime concepts into the curriculum of select academic disciplines, as well as real-life scenarios and gamification learning techniques. Humanities students have a more relaxed attitude towards engaging in cybercrimes, which could be due to their leisure time. To address this, the study suggests incorporating cybercrime-related topics into academic syllabuses and utilizing extracurricular activities. The study also highlights the higher prevalence of male involvement in cybercriminal activities compared to females, highlighting the need for male students' conduct to be improved. Diverse forms of media across physical and digital platforms can achieve this. (Alhadidi, Nweiran, & Hilal, 2024).

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

In Jordan, Alhadidi, Nweiran, & Hilal (2023) examine the impact of cybercrime and legal awareness on young individuals' behavior. Findings showed a strong association between legal awareness and illicit cyber-acts. Factors such as gender play a significant role in discouraging individuals from engaging in such criminal activities. The study emphasizes the need for effective strategies to mitigate cybercrime involvement. (Alhadidi, Nweiran & Hilal, 2023).

Cybercrime awareness has become a significant global concern due to the increasing prevalence of such offenses. Studies have shown a lack of knowledge about effective data security measures among college students in Silicon Valley, California. In Nigeria, students have a basic understanding of cybersecurity but lack awareness about data protection measures. (Garba, Siraj, Othman, & Musa, 2020). In Saudi Arabia, a study found a correlation between knowledge of the penal system and illicit activities facilitated by modern technologies. Awareness of cybercrimes is moderate, with a significant percentage of participants not reporting incidents. (Alzuubaidi, 2023). A study by Alzubaidi found that Saudi Arabians have moderate awareness of cyber-security, with a significant portion (70.8%) not reporting incidents. This suggests a lack of trust in entities like the eGovernment portal, police, and Saudi CERT, as well as a reluctance to report cybercriminal activities. (AlZeben & AlKharabsheh, 2021).

In Saudi Arabia established the National Cyber Security Authority in 2007 to improve cybersecurity. Promoting digital literacy and responsible use of technology can create a safer online environment for all individuals, regardless of gender. Cybercrime, including hacking, identity theft, and online fraud, is particularly vulnerable to higher education students, making it crucial to investigate the role of digital citizenship in preventing cybercrime. The study found that digital citizenship significantly impacts students' awareness and prevention of cybercrime. The study found that digital law knowledge, digital manners beliefs, digital communication skills, digital rights, knowledge, and duties, digital commerce skills, digital health beliefs, digital access skills, digital security, and digital culture were the top factors. However, the study also found a negative relationship between digital citizenship and various forms of cybercrime. The findings suggest higher education institutions should integrate digital citizenship education into their curriculum. (Althibyani & Al-Zahrani, 2023).

A study by Bamatraf (2014), found that university of United Arab Emarat's students have a medium level of knowledge about cybercrimes, with only 32% having adequate knowledge. The knowledge level was significantly influenced by student major, with 21.5% of students specializing in Computer Information Technology having the highest knowledge. (Bamatraf, 2014). Bele et al (2014), discussed the strategic prevention of cybercrime, focusing on measures for children and teenagers. The study emphasizes the importance of education on illegal internet content and cybercrime. Blended learning courses are prepared to raise awareness among stakeholders, including children, teenagers, teachers, and parents. These courses use the LMS system eCampus, which is designed for use on mobile devices and PC computers, ensuring extended effects on awareness levels. (Bele, Dimc, Rozman, & Jemec, 2014).

Thakur (2018) found a strong correlation between gender and location in adolescent cyber-crime awareness. Choudhary (2020) found professional students are more aware of cybercrime than traditional course participants, but no gender difference was found. Survera & Tailor (2020) revealing significant differences in awareness across different areas and castes. Yu (2014) investigates the relationship between fear of cybercrime (online scams, cyberbullying, digital piracy, and computer viruses), victimization experience, perceived crime seriousness, and perceived risk. It finds that internet exposure predicts fear of online identity theft, but it does not include the major predictors of perceived risk, seriousness, and victimization experience. The study also found that perceived risk is a strong predictor for fear of cyberbullying but not participation in online activities. (Yu, 2014). A study developed blended learning courses for key stakeholders, including children, teenagers, teachers, and parents, using interactive educational modules and the eCampus LMS system. These courses combine face-to-face lectures with mobile and PC-based lectures, ensuring extended awareness levels. (Bele, Dimc, Rozman & Jemec, 2014). A study by Ozdamli & Ercag, (2019) reveals that most adolescents are familiar with concepts like child pornography and computer and network security, but not all cybercrimes are recognized in the media. Legal objections and obstacles hinder the definition and determination of cybercrimes. Adolescents are trying to protect themselves by not sharing account information and refraining from online shopping. Training sessions or seminars can help

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

teach unfamiliar informatics concepts, enhancing adolescents' protection. Researchers should work across the country to identify cyber-crime profiles and determine training needs, assessing adolescents' awareness and organizing relevant activities. (Ozdamli & Ercag, 2019). Goel Urmila (2015) study reveals that while there is no significant difference in cybercrime awareness based on gender, location does affect it. Spring (2018) found that male students have greater awareness and positive insight than female students.

Methodology

Sample. The study sample comprised 500 Jordanian students representing four Jordanian universities. Of these, 215 (43%) were males, and 258 (57%) were females. Students (19%) reported being victims of cybercrimes, and 24% were perpetrators.

Measurement

*Knowledge About Cybercrime Scale***.** This scale is based on the literature review. It consists of 10 items covering the levels of cybercrime knowledge. The questions are categorized into interval levels 0–5, with the most common range being 0 to 5. Reliability as estimated by the scale's Cronbach's α was 0.66, and the validity (correlation between the scale and LSC scale) was 0.157 α=0.00. (F = 187.161, α=0.00.).

Procedure and Data Collection

This quantitative study used the survey method on a sample of undergraduate students. The researchers provided informed consent to all students, requested their voluntary participation, and offered them the option to withdraw from the study at any time. The researchers also collected data by electronically sending the questionnaire to students for their completion.

Data Analysis

Data analyzed using descriptive statistical analyses and ANOVA. (using SPSS v. 21).

Findings

Knowledge about the Jordanian Cyber Law (JCL)

Table 1 and Figure 1 demonstrate that over 25% of students have read about the JCL and perceive it as politicized. Moreover, three-quarters of them heard about it. More than half of the sample witnessed illegal actions on the net that required punishment. Less than 10% of the sample dealt with the JCL or participated in an online action that required punishment.

Table 1 Students' Responses on Items of Knowledge in Cybercrimes

	Knowledge about JCL	No	Yes
1.	Have you read the Jordanian Cybercrime Law (JCL)?	73.4	26.6
2.	Have you heard about the JCL?	24.4	75.6
3.	Have you watched a discussion about the JCL?	80.4	19.6
4.	Have you watched, read, or followed the House of Representatives discussion of the JCL?	76.2	23.8
5.	Do you think the JCL is politicized against the movement and its opponents?	69.8	30.2
6.	Have you seen behaviors on the network that require punishment?	39.6	60.4
7.	Have you participated in a discussion on the network that requires punishment?	93.2	6.8
8.	Have you dealt with the JCL in a case?	93.2	6.8
9.	Have you heard of someone who was convicted of violating the JCL?	76.6	23.4
10.	Do you know someone who was convicted under the JCL?	86.6	13.4

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

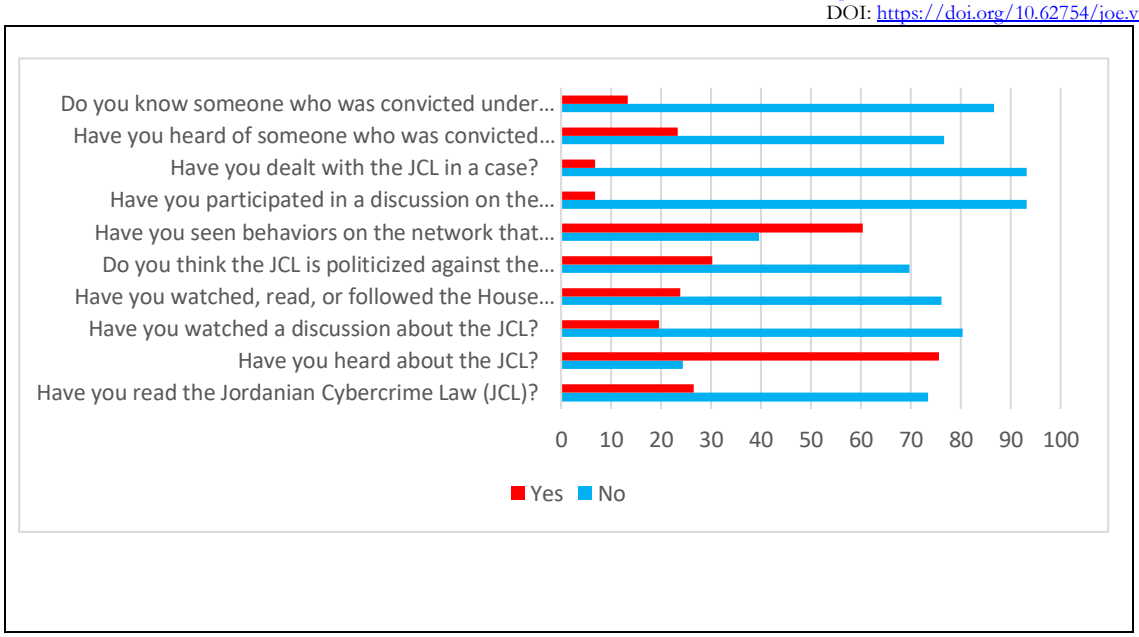


Figure 1 Students' responses on items of Knowledge in Cybercrimes

Gender Difference in the Knowledge in JCL

Tables 2 and 3 represent ANOVA analyses of the mean gender differences in cybercrime knowledge. Females were more knowledgeable about JCL than males. Table 3 shows significant differences between males and females in JCL ($F = 4.402$, $\alpha = .036$). Figure 2 shows the differences between males and females.

Table. 2 Descriptive Statistics

Groups	N	Mean	sd
Males	215	2.6	1.8
Females	285	3.0	2.0
Total	500	2.8	1.9

Table 3 ANOVA table for the Gender Difference in Knowledge in JCL

Source	Sum of Squares	df	Mean Squares	F	α
Between Groups	16.664	1	16.664	4.402	.036
Within Groups	1885.358	498	3.786		
Toala	1902.022	499			

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

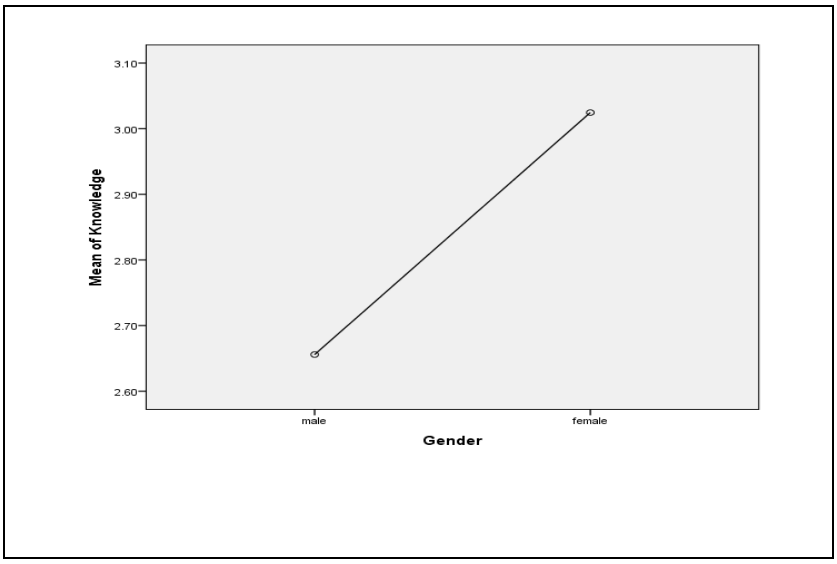


Figure 2 Gender Difference in Knowledge in CJCL

External Attribution Difference in Knowledge

Tables 4 and 5 represent ANOVA analyses of the mean external attribute differences in cybercrime knowledge. External attributers were more knowledgeable about JCL than others. Table 5 shows significant differences between groups in JCL (F = 4.402, α =.036). Figure 3 shows the differences between groups (yes=external attribution, no=no attribution).

Table. 4 Descriptive Statistics

Groups	N	Mean	sd
Disagree	330	2.7	1.9
Agree	170	3.1	1.9
Total	500	2.8	1.9

Table 5 ANOVA table for the External attributional Difference in Knowledge in Cybercrimes

Source	Sum of Squares	df	Mean Squares	F	α
Between Groups	18.679	1	18.679	4.939	.027
Within Groups	1883.343	498	3.782		
Toala	1902.022	499			

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

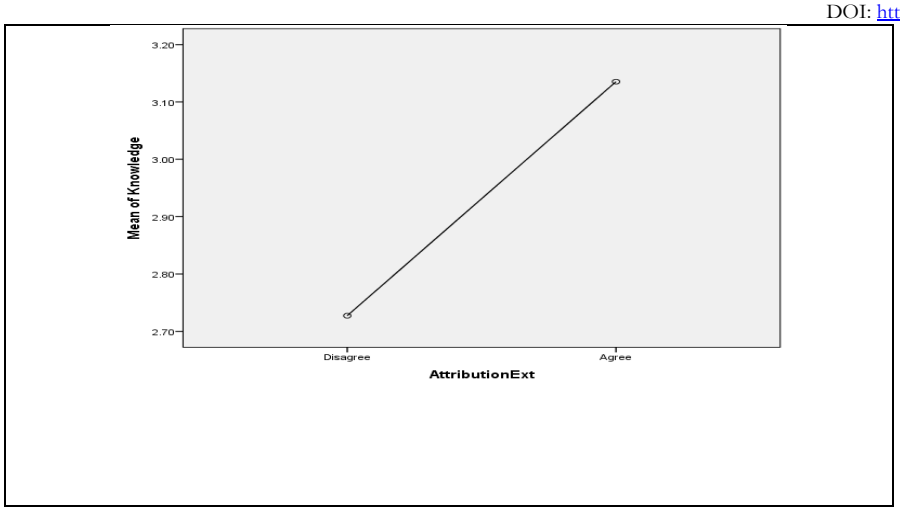


Figure 3 External Attribution Difference in Knowledge in Cybercrimes

Internal Attribution of the Difference in Knowledge

Tables 5 and 6 represent ANOVA analyses of the mean external attribute differences in cybercrime knowledge. Internal attributers were more knowledgeable about JCL than others. Table 6 shows significant differences between them in JCL (F = 4.402, α =.036). Figure 4 shows the differences between groups (yes=external attribution, no=no attribution).

Table. 5 Descriptive Statistics

Groups	N	Mean	sd
Disagree	314	2.8	1.9
Agree	186	3.1	1.8
Total	500	2.8	1.9

Table 6 ANOVA table for the Internal attributional Difference in Knowledge in Cybercrimes

Source	Sum of Squares	df	Mean Squares	F	α
Between Groups	28.724	1	28.724	7.636	.006
Within Groups	1873.298	498	3.762		
Toala	1902.022	499			

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

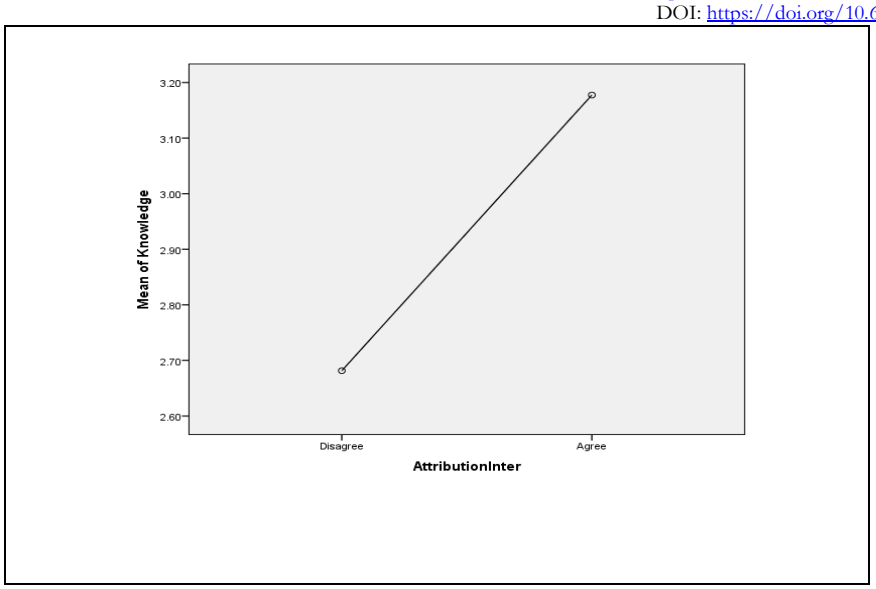


Figure 4 Internal Attribution Difference in Knowledge in Cybercrimes

Conclusion & Discussion

Cybercrime in Jordan is increasing, with an annual incidence of around one million. The most prevalent cybercrimes include threats, extortion, defamation, slander, and contempt. Online child abuse has also increased. Experts predict that cybercrime expenses will escalate to $6 trillion by 2021 and $10.5 trillion by 2025. In 2024, Jordan's legislative body enacted legislation to regulate cybercrimes (Alhadidi, Nweiran, & Hilal, 2024). The present study investigated college students' general knowledge of Jordanian Cybercrime Law. The study found that over half of the students read about the law and witnessed illegal actions online. During their daily interactions in cyberspace, students may either perpetrate or become victims of cybercrimes. On the other hand, the Jordanian cybercrime law has sparked a dialogue and debate among various segments of society and individuals about the exaggeration of the law's penalty nature, as well as the overcriminalization and politicization of the law.

The findings revealed that females possessed more knowledge about JCL than males, and there were significant differences in JCL between males and females.

Literature review revealed discrepancy in gender differences, Some research i.e., (Goel, 2015) study reveals that while there is no significant difference in cybercrime awareness based on gender, location does affect it. Others (i.e., Spring, 2018) found that male students have greater awareness and positive insight than female students. While Thakur (2018) found a strong correlation between gender and location in adolescent cyber-crime awareness. Researchers found that females possess more legal knowledge than males. This could potentially impact the disproportionate victimization and blame of females for cybercrimes, while men tend to conceal their identities more frequently. Furthermore, females use cyberspace more frequently than men, and they commit very few cybercrimes. Female cybercrime offenders face more adverse life events and barriers in predominantly masculine online communities, contributing to the lack of female involvement in cybercrime. Cyberspaces provide users with the freedom to construct gender based on their biological sex, with males choosing to be female to avoid hostility and females staying true to their real-life gender to empower themselves and change stereotypes, despite the challenges they face in online interactions. As a result, females generally face limited opportunities to receive formal training in the knowledge required to participate in technical forms of cybercrime. The second explanation pertains to the accessibility of informal knowledge. People often share informal knowledge in cyberspace. (Ismaee & Aman & Hilal, Ghofran, 2024). On the legal awareness. We found that male students had a higher awareness of cyber threats, possibly due to personal experiences or knowledge. The university's students showed varying levels of awareness of cybercrime concepts, legal procedures, and unlawful acts committed. (Alhadidi, Nweiran, & Hilal, 2024). Another study showed young men with strong computer skills may not view their

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

behavior as harmful. (Triest, 2018). Choudhary (2020) found professional students are more aware of cybercrime than traditional course participants, but no gender difference was found. Survera & Tailor (2020) revealing significant differences in awareness across different areas and castes

The study examines the differences in internal and external, of awareness on students' behavior. The ANOVA test showed that people's knowledge of JCL was significantly different when looking at internal and external attribution. According to Fritz Heider's attribution theory, people attribute behavioral outcomes to either personal traits (internal attribution) or environmental factors (external attribution). Dispositional factors are internal, while situational factors are external. Humans commonly observe the fundamental attribute error, where individuals attribute success to dispositional factors and attribute failure to situational factors. Individuals often make this error, attributing causes to themselves or to group or team behaviors. For example, sports fans may attribute a team's win to hard work and talent, while a team's loss may be due to poor refereeing (Sengupta, 2020). Research shows that young males have less self-control, leading to unlawful acts. Socialization influences reckless behavior, with Jordanian society allowing males to engage in risky activities. Women are more aware of cybercrime regulations than men.

The study suggests that university students should be educated about technology risks and cybercrime risks. It recommends integrating cybercrime concepts into academic curricula and enhancing students' understanding of legal practices. Legislation can improve prosecution facilitation and deter criminal activity. Insufficient awareness hinders prevention, but incorporating real-life scenarios and gamification can help.

References

Akdemir, N.; Sungur, B.; Ba¸saranel, B.U. (2020) . Examining the Challenges of Policing Economic Cybercrime in the UK. Güvenlik Bilimleri Derg. (Int. Secur. Congr. Spec. Issue) 2020, Özel Sayı, 113–134

Akhgar, B.; Choras, M.; Brewster, B.; Bosco, F.; Veermeersch, E.; Luda, V.; Puchalski, D.;Wells, D. (2016). Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities; Akhgar, B., Brewster, B., Eds.; Springer: Cham, Switzerland, 2016; pp. 295–321.

Al-badayneh, D. M. (2014). Cybercrimes: Definition and causes: Research paper for the Conference on New Crimes in Light of Regional and International Changes and Transformations, College of Strategic Sciences, Amman, Jordan.

Alghareeb, A., & Alameer, H., (2017). The Extent of Awareness Among the Young Age Group of the Saudi Cybercrime Penal System.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students. Heliyon. 10. e32371. 10.1016/j.heliyon.2024.e32371. https://www.researchgate.net/publication/381243039_The_Influence_of_Cybercrime_and_Legal_Awareness_on_the_Behavior_of_University_of_Jordan_Students

Al-Khaza'leh, M., S., Lahiani, H. (2023). Cybercrime and Harassment: The Impact of Blackmailing on Jordanian Society as a Case Study. Journal of Intercultural Communication, 23(3), 116-123. doi.org/10.36923/jicc.v23i3.99

Almany, N. (2012). Criminal Investigation, Declining the Rate of Cyber-crimes, Addustour newspaper, Wednesday, March 28, Issue No. 16059, Forty-sixth Year, Amman, Jordan.

AlZeben, G., AlKharabsheh, A., (2021). Cybercrimes and the awareness of its danger field study on Jordanian university youth, Journal of the Islamic University of Human Research 29 (2). http://refhub.elsevier.com/S2405-8440(24)08402-0/sref27

Al-Zoubi, M. (2023). "Crimes of Electronic Defamation, Libel, and Slander under Jordanian Cybercrimes Law", International Review of Law, Volume 12, Regular Issue 1, pp 267-284

Asia-Pacific Economic Cooperation (APEC). (2002). APEC Cybersecurity Strategy. Retrieved from [APEC](https://www.apec.org/Publications/2002/10/APEC-Cybersecurity-Strategy).

Bamatraf, S. (2014). Assessing the Level of Knowledge About Cybercrimes Among Young Adults Within the United Arab Emirates Proceedings of The National Conference On Undergraduate Research (NCUR) 2014. University of Kentucky, Lexington, KY

Basuroy T. (2022).Number of cyber-crimes reported in India 2012- 2021.Statista retrived fromhttps://www.statista.com/statistics/309435/india-cyber-crime- it-act/

Bele , J., Dimc, M., Rozman, D., & Jemec, A., (2014). Raising Awareness of Cybercrime - The Use Of Education As A Means of Prevention and Protection. 10th International Conference Mobile Learning. ISBN: 978-989-8704-02-3 © 2014 IADIS

Bele, J., Dimc, M., Rozman, D. & Jemec, A. (2014). Raising Awareness of Cybercrime - The Use of Education As A Means Of Prevention And Protection. 10th International Conference Mobile Learning. ISBN: 978-989-8704-02-3. IADIS. pp 281-284

Choudhary, D. M. (2020). Cyber Crime Awareness Among Higher Education Students From Haryana With Respect to Various Demographical Variables. PalArch's Journal of Archaeology of Egypt / Egyptology, 17(7), Article 7.

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046
Commission of the European Communities(2007). . Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a General Policy on the Fight against Cyber Crime; Commission of the European Communities: Brussels, Belgium; Volume 267.

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Retrieved from [Council of Europe](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185).

Council of Europe. Convention on Cybercrime(2001). ; European Treaty Series No. 185; Council of Europe: Budapest, Hungary; pp. 1–25. Available online: https://rm.coe.int/16800815 61 (accessed on 6 April 2022).

Thomas, D., Loader, B., Eds.; (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age; Routledge: London, UK.

European Commission(2013). . Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; European Commission: Brussels, Belgium.

European Union. (2005). Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems. Retrieved from [EUR-Lex](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005F0222).

EUROPOL, 2021.Cybercrime definition. 〈 https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime〉

Faqir, R. S. (2013). Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010International Journal of Cyber Criminology Vol 7 Issue 1 January - June 2013

Garba, A., Siraj, M., Othman, S., & Musa, M. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: a quantitative approach, Int. J. Emerg. Technol. 11 (5) (2020) 41–49.

Gargi S., Sandeep K. S., (2023). Behavioural analysis of cybercrime: Paving the way for effective policing strategies,. Journal of Economic Criminology, Volume 2,100034, ISSN 2949-7914, https://doi.org/10.1016/j.jeconc.2023.100034. https://www.sciencedirect.com/science/article/pii/S2949791423000349)

Gillespie, A. (2015). Cybercrime: Key Issues and Debates; Routledge: New York, NY, USA,

Goel(2015).Gender and locale differences in cyber crime awareness among adolescents—ProQuest. (n.d.). Retrieved November 24, 2023, from https://www.proquest.com/openview/a68a1a11f0cb4d04c1fca1ccdbc61461/1?pq-origsite=gscholar&cbl=2032134

Gordon, S.; Ford, R. (2006). On the Definition and Classification of Cybercrime. J. Comput. Virol. 2, 13–20.

Interpol. (n.d.). Cybercrime. Retrieved from [Interpol](https://www.interpol.int/en/Crimes/Cybercrime).

IOCTA(2017, 2021).Cybercrime definition by European cybercrime centre. https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf

Malby, S.; Mace, R.; Holterhof, A.; Brown, C.; Kascherus, S.; Ignatuschtschenko, E. (2013). Comprehensive Study on Cybercrime; United Nations Office on Drugs and Crime: Vienna, Austria.

National Cyber Crime Reporting Portal. (2019). Retrieved November 24, 2023, from https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1703509

Northern Cyprus. TEM Journal. Volume 8, Issue 4, Pages 1345-1350, ISSN 2217-8309, DOI: 10.18421/TEM84-35 TEM Journal – Volume 8 / Number 4 / 2019. 1345

Ozdamli F., & Ercag, E. (2019). Knowledge Levels and Attitudes Toward Cybercrimes of Adolescents in

Phillips, K., et al. (20220. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022, 2(2), 379 398; https://doi.org/10.3390/forensicsci2020028. https://www.mdpi.com/2673-6756/2/2/28

Raed S A Faqir1, Saleh Sharari2 & Salameh A. Salameh(2014). Cyber Crimes and Technical Issues under the Jordanian Information. System Crimes Law. Canadian Center of Science and Education. Journal of Politics and Law; Vol. 7, No. 2, pp 94-106

Sahu & Shukla (2024) study reveals that 69% of college students have above-average awareness of cybercrime, with urban students being more aware than rural ones, and gender has no discernible impact.

Sahu M., & Shukla, P., (2024). A Study on Cyber-Crime Awareness Among Students in Chhattisgarh. Journal of Ravishankar University (Part-A: SOCIAL-SCIENCE), 30(1), pp.54-60. DOI: https://www.jru-a.com/ShowPDF_Paper.aspx

Sengupta, S. (2020). Heider's Attribution Theory. https://managementweekly.org/heiders-attribution-theory/

Soylu, T. D. Medeni, R. Andekina, R. Rakhmetova and R. Ismailova (2021). Identifying the Cybercrime Awareness of Undergraduate and Postgraduate Students: Example of Kazakhstan," 2021 IEEE International Conference on Smart Information Systems and Technologies (SIST), Nur-Sultan, Kazakhstan. pp. 1-7, doi: 10.1109/SIST50301.2021.9465995. https://ieeexplore.ieee.org/document/9465995

Suvera, D. P., & Tailor, P. R. (2020). Cyber-crime awareness: A comparative study of male and female B.Ed. Trainees.

T. J. Holt T., (ed.), (2022). Cybercrime through an Interdisciplinary Lens (pp. 167-188). Oxon: Routledge. Gendering cybercrime Alice Hutchings and Yi Ting Chua

Thomas, D.; Loader, B. (2000). Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age; Thomas, D., Loader, B., Eds.; Routledge: London, UK, 2000.

Triest, J.V., (2018). A new target group in probation: cybercrime offenders, Retrieved from, https://www.cep-probation.org/a-new-target-group-in-probation-cybercrime-offenders/, 2018.

U.S. Department of Justice. (n.d.). Computer Crime & Intellectual Property Section (CCIPS). Available at: DOJ.

UN Congress Crimes Related to Computer Networks(2000). 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders; United Nations: Vienna, Austria, 2000. Available online: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (accessed on 6 April 2022).

Journal of Ecohumanism
2024
Volume: 3, No: 6, pp. 773 – 786
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i6.4046

United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. Retrieved from [UNODC](https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf).

United Nations(1994). United Nations Manual on the Prevention and Control of Computer-Related Crime; United Nations: New York, NY, USA, 1994.

Wall, D.S. (2001). Introduction: Cybercrime and the Internet. In Crime and the Internet; Wall, D.S., Ed.; Routledge: New York, NY, USA, pp. 1–17.

Wall, D.S.(2001). Introduction: Cybercrime and the Internet. In Crime and the Internet; Wall, D.S., Ed.; Routledge: New York, NY, USA, pp. 1–17.

.