Pak. j. life soc. Sci. (2025), 23(1): 4014-4020 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.00318

RESEARCH ARTICLE

The Sociology of Cybercrime: Causes and Prevention

Rahaf Salem Darabseh[1*], Ahed J Alkhatib[2]

[1] Faculty of Literature and Language, Strathclyde University, UK,
[2] Department of Legal Medicine, Toxicology and Forensic Medicine, Jordan University of Science & Technology, Jordan
[2] International Mariinskaya Academy, Department of Medicine and Critical Care, Department of Philosophy, Academician Secretary of Department of Sociology.
[2] Cypress International Institute University, Texas, USA

ARTICLE INFO

Received: Nov 22, 2024

Accepted: Jan 26, 2025

Keywords

Criminal Psychology in Cybercrime
Cyberattacks
Cybercrime
Cybersecurity
Sociology

***Corresponding Author:**

rahaf.s.darabseh@gmail.com

ABSTRACT

Cybercrime is best defined as any crime that is committed over the internet. Cybercrime has been an issue ever since the birth of the internet, dating back to as early as the 1980s. Technology currently plays a big part in people's lives, especially in this era of technology evolution, which has led to the ability of criminals to abuse technology for personal gain. The capability for someone to get questions or concerns answered immediately can make people feeling entirely comfortable on the internet when quite the opposite should be the case. Because of this, it is easier for cybercriminals to trick people into giving them credit card information, or other personal information that can be used for identity theft. One in ten people that are online are victims of cybercrime; the seriousness of cybercrime varies; some are minor crimes. Ninety percent of the 1.5 million cyberattacks that happened around the world in the 2013-2014 period were indicated to be coming from China. Legitimate websites can be hacked to enable the attacker to install malware onto the computer of a visitor of these websites. Malware can also be found on websites that contain illegal downloads such as music, movies, and software. Unfortunately, hackers have found a way to lock computers and files and then demand to be paid a fee to unlock these. There is an opportunity for people with a criminal psychology background to investigate these cases and potentially identify the cybercriminals. There are various ways a person can protect their computer from new malware by using more advanced firewalls or making some simple adjustments in their daily computer usage. However, this can be difficult when a person's computer operating system becomes outdated and is no longer supported by the vendor.

1. INTRODUCTION

1.1. Introduction to the sociology of cybercrime

As technology continues to evolve with society and become more interconnected with it, certain drawbacks of this technology have been exposed (1-3). Crime on all fronts has been taken to a new, virtually invisible place on the Internet (4). Blanketed under the name cybercrime, this new form of crime is emerging as a major threatening issue on the global community (5). Cybercrime consists of a variety of criminal activities carried out using computers or the Internet (6-7). The ability of cybercrime to transcend boundaries and affect large numbers of individuals quickly has made it a popular venture for criminals (8). There are a number of steps users can take to prevent themselves from being victims of cybercrime, but as said earlier, it is quite a different animal than traditional crime and not everything can be caught (9-11).

Sociology is the study of human relationships and institutions (2). It examines the way society is organized and how people interact within that society (3). Technology has changed the way America, as well as the rest of the Earth, is composed (12). It has allowed an ever boisterous world to remain connected through computers (13). This connection offers many benefits, with the cost of being afforded to the criminal abyss that is the Interweb (14). Cybercrime is really not a technological issue; rather it is a societal issue as well (9). When examining all sides of the good old salt and silicon debate, one would typically look at ways to prevent oneself from being a victim (15). However, for a crime to exist, there must be a criminal to perform the crime (13). It stands to reason that the focus should also be on those that partake in the cybercrime (14). In order to get rid of, or at least decrease the amount of cybercrime, it is important to understand the people behind it (12). With this being said, cybercrime is essentially a social phenomenon, as most crimes are (15).

1.2. Key concepts and theoretical frameworks

The sociology of cybercrime is a rapidly expanding field that examines the social aspects of offending and victimization in cyberspace (16). This article delves into the causes of cyber offenses from a sociological perspective and presents strategies for their prevention (17). Key concepts and theoretical frameworks of relevance to the sociology of cybercrime are introduced (18). Several significant sociological traditions used to explain online behaviors that individuals or groups commit against the law or legal norms are illustrated (19). It is important to clarify the definitions of key terms to facilitate readability (20). Cybercrime, or computer crime and cybercriminal behavior, involves a broad field of illegal activities that utilize computer networks and digital devices to unlawfully acquire and distribute data, interferes with computer operations, executes fraud, and more (21-24).

The sociological study of cybercrime has closely followed developments in technology (14). Theoretical frameworks are applied to interpret and describe the motivations behind cyber offenses (25). Central ideas with regard to cybercrime based on sociological perspectives are postulated, linking theory to practice (26). Methods are delineated for how sociological analysis can help to prevent and counteract cybercriminal behavior (27). Interdisciplinarity in the sociology of cybercrime and its importance is underscored (28). Molecular criminology is detailed, focusing on the research branches pertinent to the sociology of cybercrime (29). The interdisciplinary cooperation of computer crime research is discussed, underscoring the importance of a robust theoretical ground (30). From this perspective, effective anti-cybercrime strategies are derived, with both policing priorities and the ways in which potential offenders can be addressed being examined (25). The recommendations are aimed at policymakers, law enforcement, criminal justice agencies, and e-safety organizations working to prevent and counteract cyber-related offenses (31).

1.3. Social causes of cybercrime

Cybercrime, although rather a nascent phenomenon in most European countries, is in a number of respects neither a new, nor a specific crime (32). Against this background, six aspects of the discursive construction of cybercrime are pointed out, that pose problems for ‘serious’ criminology, reduce policy options within the criminal justice system, as well as distort the wider societal understanding of a rapidly escalating form of delinquent behavior (33-35). These myths and misleading assumptions about the nature of cybercrime are illustrated by data drawn from a research examining cybercrime offending and victimization in Slovenia (36). It is argued that both public in everyday consciousness about the cybercrime are embedded in paths that are quite congruent with the ‘production of knowledge’. If ‘reality’ is routinely constructed through crime statistics and other crime records, the less developed is a criminalistic (knowledge) infrastructure, the fewer facts are available that could serve as a basis for relevant policy formation and effective interventions (37-42). However, this does not preclude that particular forms of cyber delinquency are not only ‘criminally loaded’ in a more conventional, legal sense, but that some people’s everyday life is substantially affected by the negative consequences of this particular form of victimization (43-47).

1.3.1. Structural explanation of cybercrime

Many respectably aspects of criminal activities, deviation and delinquency can more successfully be understood through the social structures, on one side, and social learning, on the other. Society is not limited to an aggregate of individuals, but consists of stratification and classes with different opportunities and constraints (38). Many of the behaviors that are generally regarded as crime or deviant are no more than reactions to the society that is being observed, rather than pathological in themselves (48). Such behavior is held to be quite normal under particular circumstances or in particular environments, and should not be considered as deviant or criminal (49). In relation to these understandings of criminality it is thought that the cyber society, i.e. the Internet and the online social networks, holds important keys in explaining a form of criminality that has, thus far, failed to be understood and represented in (sub-)culture bound theories of crime and deviance (50). Therefore, delinquency of power, ethic business practices and warfare, the new technology and international corporatism, the preventative state and penal expansion, forms of social learning and moral panic, and the experiences of peer (cyber) bullying are examples of debates, awareness and phenomena revealing that the mainstream discipline may need to revise its concepts, act in a more coordinal stance with other sciences and examine the newly emerging social, political and cultural circumstances characterizing late modernity (51-54).

1.4. Prevention strategies and interventions

Cybercrime is a socially embedded phenomenon with multiple and interacting causes and consequences (55). Drawing on key criminological and sociological theories, this article provides an overview of the current state of knowledge about the social causes of cybercrime (56). The discussion is organized in four sections, the first which details the scope, impact, and definition of cybercrime; the second section examines why people commit cybercrimes; the third, what the consequences of cybersecurity breaches are to individuals, organizations, and broader political economies (57). Finally, drawing on these insights, the article concludes by examining suitable prevention strategies and interventions that can be deployed by individuals, organizations, and governments (58-60).

People commit cybercrime for a range of reasons, including financial gain, anger, retaliation, and thrill seeking (61). The costs of cybercrime are also extensive covering emotional, financial, and broader social ramifications (62). This has led a number of countries to consider introducing strict legislation, such as mandatory breach notification laws, to improve organizational compliance (63). Technology solutions are also playing an increasingly significant role, including encryption, tokenization, multi-factor authentication, firewalls, and intrusion detection and prevention systems (64). Yet, the effectiveness of these systems is often offset by "the human factor" and a lack of awareness about how cybersecurity threats work and permeate within organizations (65). Furthermore, cybercrime requires different stakeholders working together to create a robust defense, suggesting a multimodal prevention and intervention approach will be the most effective move forward (65).

Many prevention programs and initiatives exist aimed at cybersecurity awareness and education; these have emerged from organizations like (66). The effectiveness of such prevention programs and initiatives often takes on a twofold approach, changing broader organisational and cultural practices while fostering responsible online behavior (67). Recommendations for cyberbullying prevention and intervention are provided from the perspective of key Western Canadian stakeholders, including among students, parents, teachers, school counsellors, and healthcare professionals (68-75).

1.5. Conclusion

As the essays illustrate, a sociological perspective is fundamental to a comprehensive understanding of cybercrime (76). The sociological imagination commands that the structure of society and the wider socio-cultural landscape be systematically accounted for in any discussion of the challenges of cybercrime and strategies for its containment (77). Cybercrime is not a static phenomenon; it is thoroughly embroiled in the rapidly changing social environment provided by contemporary information society (78). More than just a backdrop, society is integrally related to the commission of cybercrime and the responses to it (79). This is manifest in the particular social causes of cyber offenses, the ways particular societies either facilitate or thwart cybercrime, the demands and

possibilities posed by global societal developments, and in the complex and often unintended consequences of interventions that are themselves socially situated (80). A variety of social factors – economic, legislative, criminological, and technological – have facilitated and presented challenges to the control of cybercrime (81). A comprehensive understanding of cybercrime must take into account these factors and engage with them at a societal level in order to develop viable means of reducing cyber offenses (31). A sociological lens is crucial to a full appreciation of the nature and prevalence of cybercrime, and it provides the most robust means to combat cybercrime and protect those most at risk of cyber victimization (55).

REFERENCES

McDaniel B. An In-Depth Look into Cybercrime. 2018. [PDF]

Goni O, Ali MH, Showrov MM, Shameem MA. The basic concept of cyber crime. Journal of Technology Innovations and Energy. 2022;1(2):16-24. ijemt.com

Goni O. Cyber crime and its classification. Int. J. of Electronics Engineering and Applications. 2022. researchgate.net

Koto I. Cyber crime according to the ITE law. International Journal Reglement & Society (IJRS). 2021 Jul 28;2(2):103-10. bundamediagrup.co.id

Yadav H, Gautam S, Rana A, Bhardwaj J, Tyagi N. Various types of cybercrime and its affected area. InEmerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3 2021 (pp. 305-315). Springer Singapore. [HTML]

Deora RS, Chudasama D. Brief study of cybercrime on an internet. Journal of communication engineering & Systems. 2021 Jun;11(1):1-6. researchgate.net

Chinedu PU, Nwankwo W, Masajuwa FU, Imoisi S. Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education Online. 2021 Jul 1;11(7). researchgate.net

Pawar SC, Mente RS, Chendage BD. Cyber crime, cyber space and effects of cyber crime. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021 Jan;7(1):210-4. researchgate.net

Matveev V, Eduardivna NO, Stefanova N, Khrypko S, Ishchuk A, Ishchuk O, Bondar T. Cybercrime in the Economic Space: Psychological Motivation and Semantic-Terminological Specifics. International Journal of Computer Science & Network Security. 2021;21(11):135-42. koreascience.kr

Sviatun OV, Goncharuk OV, Roman C, Kuzmenko O, Kozych IV. Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics. 2021 Apr;18:751-62. academia.edu

Ibrahim S, Nnamani D, Okosun O. Types of Cybercrime and Approaches to Detection. IOSR Journal of Computer Engineering. 2021;23(5):24-6. researchgate.net

Arpaci I, Aslan O. Development of a scale to measure cybercrime-awareness on social media. Journal of Computer Information Systems. 2023. academia.edu

Sarfi M, Darvishii M, Zohouri M. Why People May View Online Crimes as Less Criminal: Exploring the Perception of Cybercrime. International e-journal of criminal sciences. 2023 Dec 20(18). ehu.eus

Babanina V, Tkachenko I, Matiushenko O, Krutevych M. Cybercrime: History of formation, current state and ways of counteraction. Amazonia Investiga. 2021 Apr 12;10(38):113-22. amazoniainvestiga.info

Maluleke W. Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. International Journal of Social Science Research and Review. 2023 Jun 8;6(6):223-43. ijssrr.com

Abdulai MA. The Paradox of Cybercrime Risk and Internet Use in Canada: A Socio-Criminological Perspective. 2022. usask.ca

Mikkola M, Oksanen A, Kaakinen M, Miller BL, Savolainen I, Sirola A, Zych I, Paek HJ. Situational and individual risk factors for cybercrime victimization in a cross-national context. International Journal of Offender Therapy and Comparative Criminology. 2024 Apr;68(5):449-67. tuni.fi

Ho HTN, Luong HT. Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. SN Social Sciences. 2022. springer.com

Borwell J, Jansen J, Stol W. Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. Journal of Digital Social Research. 2021. jdsr.se

Momeni F. The impact of social, cultural, and individual factors on cybercrime. Educational Administration: Theory and Practice. 2024. kuey.net

Smith S. Assessing the Weight of Social Capital Theory in Digital Victimization Patterns Via the Oxford Internet Surveys. InThe Routledge International Handbook of Online Deviance 2025 (pp. 132-148). Routledge. [HTML]

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

Borwell J, Jansen J, Stol W. Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. International Review of Victimology. 2024 Oct 8:02697580241282782. [HTML]

Borwell J, Jansen J, Stol W. The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. Social Science Computer Review. 2022 Aug;40(4):933-54. cybersciencecenter.nl

Di Nicola A. Towards digital organized crime and digital sociology of organized crime. 2022. ncbi.nlm.nih.gov

Lusthaus J. Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. Annual Review of Law and Social Science. 2024. annualreviews.org

Hall T, Sanders B, Bah M, King O et al. Economic geographies of the illegal: the multiscalar production of cybercrime. Trends in Organized Crime. 2021. academia.edu

Chen S, Hao M, Ding F, Jiang D, Dong J, Zhang S, Guo Q, Gao C. Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications. 2023 Feb 23;10(1):1-0. nature.com

Neufeld D. Computer crime motives: Do we have it right?. Sociology Compass. 2023. wiley.com

Pallangyo HJ. Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. Tanzania Journal of Engineering and Technology. 2022. ajol.info

Gupta YK. Exploring crime from a sociological perspective. International Journal of Dynamic Educational Research Society. 2024;5(2):47-56. ijders.com

Završník A. Cybercrime - Definitional Challenges and Criminological Particularities. 2009. [PDF]

Kastner P, Mégret F. International legal dimensions of cybercrime. InResearch Handbook on International Law and Cyberspace 2021 Dec 14 (pp. 253-270). Edward Elgar Publishing. [HTML]

Fahey E. Developing EU cybercrime and cybersecurity: On legal challenges of EU institutionalisation of cyber law-making 1. The Routledge Handbook of European Integrations. 2022. city.ac.uk

Roškot M, Wanasika I, Kreckova Kroupova Z. Cybercrime in Europe: surprising results of an expensive lapse. Journal of Business Strategy. 2021 Mar 18;42(2):91-8. academia.edu

Phillips K, Davidson JC, Farr RR, Burkhardt C, Caneppele S, Aiken MP. Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic sciences. 2022 Apr 16;2(2):379-98. mdpi.com

Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies. 2021 Feb 19;23(sup1):S47-59. asiermoneva.com

Wall DS. Cybercrime: The transformation of crime in the information age. 2024. researchgate.net

Buçaj E, Idrizaj K. The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews. 2025. malque.pub

Bjelajac Z, Filipovic AM. Media and Criminal Behavior-Between Social Responsibility and Destruction. Law Theory & Prac.. 2023. pravni-fakultet.edu.rs

Ismail AS, Haniff MA, Md MN. Inside the Mind of Cybercriminals: Investigating the Influence of Socioeconomic Factors on the Ethical Decision-Making of Cybercriminals. InProceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023 2023 (p. 34). researchgate.net

Yan F. Research on the Status Quo and Prevention of Juvenile Delinquency from the Perspective of Internet. International Journal of Frontiers in Sociology. 2023. francis-press.com

Kala EM. Influence of Online Platforms on Criminal Behavior. International Journal of Research Studies in Computer Science and Engineering (IJRSCSE). 2024;10(1):25-37. academia.edu

Željko B, Aleksandar FM. MEDIA AND CRIMINAL BEHAVIOR–BETWEEN SOCIAL RESPONSIBILITY AND DESTRUCTION. 2023. researchgate.net

Ezeji CL. Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. International Journal of Business Ecosystem & Strategy (2687-2293). 2024 Dec 1;6(4):271-84. bussecon.com

Okeke CV, Obi-Nwosu H, Onuoha OC. Parental Styles and Moral Disengagement as Predictors of Attitude towards Cybercrime among Undergraduates. ZIK JOURNAL OF MULTIDISCIPLINARY RESEARCH. 2024 Dec 1;7(1). aphriapub.com

Yuzikova N. CRIMINOLOGY RESEARCH OF THE INFLUENCE OF INTERNET CONTENT ON INTERPERSONAL COMMUNICATION AND BEHAVIOR OF MINORS. Baltic Journal of Legal and Social Sciences. 2022. baltijapublishing.lv

Asli MR. Digital trends of criminology and criminal justice of the 21st century. Journal of Digital Technologies and Law. 2023. cyberleninka.ru

Horgan S, Collier B, Jones R, Shepherd L. Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. Journal of Criminal Psychology. 2021 Aug 3;11(3):222-39. worktribe.com

Maulana YI, Fajar I. Analysis of cyber diplomacy and its challenges for the digital era community. IAIC Transactions on Sustainable Digital Innovation (ITSDI). 2023 Mar 25;4(2):169-77. aptikom-journal.id

Sharma V, Manocha T, Garg S, Sharma S, Garg A, Sharma R. Growth of Cyber-crimes in Society 4.0. In2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM) 2023 Feb 22 (pp. 1-6). IEEE. researchgate.net

Basheer R, Alkhatib B. Threats from the dark: a review over dark web investigation research for cyber threat intelligence. Journal of Computer Networks and Communications. 2021;2021(1):1302999. wiley.com

AllahRakha N. Transformation of Crimes (Cybercrimes) in Digital Age. International Journal of Law and Policy. 2024. irshadjournals.com

Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security. 2021 Jun 1;105:102248. nih.gov

Sarkar G, Shukla SK. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology. 2023. sciencedirect.com

Nzeakor OF, Ede AA, Nwoke CN. UNDERSTANDING INDIVIDUAL VICTIMS'CONTRIBUTION IN THE INCIDENCE OF CYBERCRIME VICTIMIZATION ATTACKS IN ABIA STATE, NIGERIA. FUOYE JOURNAL OF CRIMINOLOGY AND SECURITY STUDIES. 2024 Jun 17;3(1). fuoye.edu.ng

Rahaman KH, Hasam MA. A Social Review on Nature & Reason of Cyber-Crime and the Laws Regarding Prevention in Bangladesh. International Journal of Research and Innovation in Social Science. 2021;5(07):171-8. researchgate.net

Olofinbiyi SA. Exploring youth awareness of cybercrime and factors engendering its proliferation in Nigeria. African Renaissance. 2021. [HTML]

Ojolo TL, Singh SB. The transnational dimension of organised crime: an investigation into the operational structure of cybercrime in Nigeria. EUREKA: Social and Humanities. 2023. eu-jr.eu

Graham A. Cybercrime: Traditional Problems and Modern Solutions. 2023. wgtn.ac.nz

Smith T. A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime. 2021. osf.io

Aftab RM, Ijaz M, Rehman F, Ashfaq A, Sharif H, Riaz N, Hussain S, Arslan M, Maqsood H. A Systematic Review on the Motivations of Cyber-Criminals and Their Attacking Policies. In2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) 2022 Dec 14 (pp. 1-6). IEEE. [HTML]

Guidetti O, Mather S. Malicious Minds: Psychological Profiling of Ransomware Attackers and Policing Challenges. Ransomware Evolution. 2024. [HTML]

Peled-Laskov R. When personal rational decision-making fails: examining the psychological limits of criminal punishment as a successful deterrent for white-collar offenders. The Journal of Forensic Psychiatry & Psychology. 2024. [HTML]

Singh S. The Cybercrime Spectrum: Understanding Digital Threats and Security. 2024. [HTML]

P. Hendry B, Michelle Hellsten L, J. McIntyre L, R. R. Smith B. Recommendations for cyberbullying prevention and intervention: A Western Canadian perspective from key stakeholders. 2023. ncbi.nlm.nih.gov

Shillair R, Esteve-González P, Dutton WH, Creese S, Nagyfejeo E, von Solms B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security. 2022 Aug 1;119:102756. ox.ac.uk

AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KK. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022 Aug 1;119:102754. researchgate.net

Chaudhary S, Gkioulos V, Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity. 2022. oup.com

Triplett WJ. Addressing cybersecurity challenges in education. International Journal of STEM Education for Sustainability. 2023 Jan 1;3(1):47-67. gmpionline.com

Corallo A, Lazoi M, Lezzi M, Luperto A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry. 2022. [HTML]

Dash B, Ansari MF. An effective cybersecurity awareness training model: first defense of an organizational security strategy. 2022. academia.edu

Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems. 2022 Jan 2;62(1):82-97. researchgate.net

Sabillon R. The cybersecurity awareness training model (CATRAM). InResearch Anthology on Advancements in Cybersecurity Education 2022 (pp. 501-520). IGI global. [HTML]

Hu S, Hsu C, Zhou Z. Security education, training, and awareness programs: Literature review. Journal of Computer Information Systems. 2022. [HTML]

Rehman TU. Theoretical context of cybercrime. InHandbook of Research on Applied Social Psychology in Multiculturalism 2021 (pp. 174-191). IGI Global. [HTML]

Lazarus S, Button M, Kapend R. Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. The Howard Journal of Crime and Justice. 2022 Sep;61(3):381-98. wiley.com

Gordon F, McGovern A, Thompson C, Wood MA. Beyond cybercrime: New perspectives on crime, harm and digital technologies. International Journal for Crime, Justice and Social Democracy. 2022 Mar 1;11(1):i-viii. informit.org

Balabantaray SR, Mishra M, Pani U. A SOCIOLOGICAL STUDY OF CYBERCRIMES AGAINST WOMEN IN INDIA: DECIPHERING THE CAUSES AND EVALUATING THE IMPACT ON THE VICTIMS. International Journal of Asia-Pacific Studies. 2023 Jan 1;19(1). researchgate.net

Lavorgna A, Holt T. Researching Cybercrimes. 2021. [HTML]

Di Nicola A. Towards digital organized crime and digital sociology of organized crime. Trends in organized crime. 2022. springer.com