The Impact of Cyber Crimes on User Victimization: Assessing Cyber Risks

Nasif Raza Jaffri

NFC Institute of Engineering and Fertilizer Research, Faisalabad

Correspondence:
Nasif Raza Jaffri: nasif@iefr.edu.pk

Article Link: https://www.brainetwork.org/index.php/jcai/article/view/13

DOI: https://doi.org/10.69591/jcai.1.1.5

Citation: Jaffri, N. R. (2023). The impact of cybercrimes on user victimization: Assessing cyber risks. *Journal of Computing and Artificial Intelligence, 1*(1), 83–98.

Conflict of Interest: Authors declared no Conflict of Interest

Acknowledgment: No administrative and technical support was taken for this research

Article History

Submitted: Mar 11, 2023
Last Revised: Apr 12, 2023
Accepted: May 28, 2023

Volume 1, Issue 1, 2023

Funding
No

An official Publication of
Beyond Research Advancement & Innovation Network, Islamabad, Pakistan

The Impact of Cyber Crimes on User Victimization: Assessing Cyber Risks

Nasif Raza Jaffri*

NFC Institute of Engineering and Fertilizer Research, Faisalabad, Pakistan

Abstract

Data protection, information security and system security are often referred to as cyber security. So, if you do some security research in general, you're likely to see these words very often: information security, data security, system security, cyber security, there are so many different names and terms that relate to a very deep technical point of almost the same thing. But at a very high level, there are really no variations, it's really one of the same stuffs that you're all focusing on the same thing so that digital data is protected by cyber security. We are going to discuss different methodologies for network safety which will explain your personality and access managers. A vital device in information security is personality and access to the board. It shows the periods in which such data consents are permitted to different customers and in what settings. This encryption of information means that confidential data cannot be accessed by selected customers on selected occasions. The risk of infiltration and digital assaults is significantly reduced by personality and access to executives. Cyber security's primary aim is to prosecute offenders or protect data. Criminal investigations are discussed to obtain evidence of illegal conduct. In this situation, this is important for identifying the devices, computers, cell phones, etc. used in illegal activity and deciding if the suspect used these devices in the crime. In the result we have made a pilot study against worldwide cyber-attacks with their types has been consolidated in a range and then a solution has been suggested accordingly.

Keywords: risk infiltration, Nintendo, console, cyber, digital assaults.

Introduction

Various networking networks and extensive portable gaming systems have useful features such as internet access, social communication, and interaction between email and chat. The Nintendo 3DS console was first released in Japan on 26 February 2011. "Nintendo 3DS XL", "New

* Corresponding Author: nasif@iefr.edu.pk

Nintendo 3DS XL", "Nintendo 2DS" and "New Nintendo 2DS XL" were released more than six years after the console was launched.

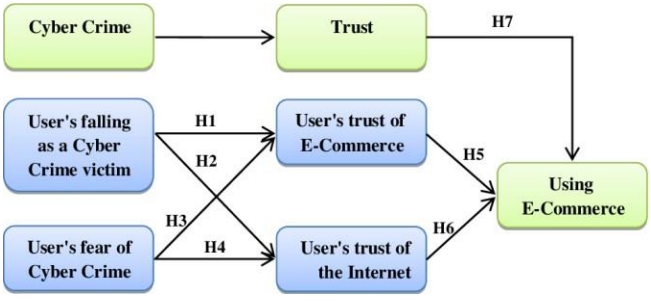
The most active handheld in the world, the 3DS, was sold for 73.53 million units [1] as was the DSi's predecessor, already involved in illegal activity (Ashcroft, 2013). It is aimed at a younger/family-oriented audience; the ESRB has 2587 Early Childhood/Everyone rated DS/DSi/3DS games but Maturity (17″) on 29 January 2019 and ranked just 38″ above [2]. It is fair to suppose that adolescents are more certainly interested in a 3DS scenario.

It also takes special attention from the digital forensic community to improve existing processes of data extraction and analysis to at least support the United States Daubert standard. Interest in hacking and modification over the lifespan of the console has grown in line with the rise in 3DS popularity. An online vulnerability called 'boot9strap' was released on [4]. This vulnerability allows arbitrary code to be run before a console boot into the system menu, along with an attack dubbed 'ntrboot.' This makes it possible to recover the memory of the NAND without booting a console that allows for forensic sound methodology.

The Nintendo 3DS uses a non-volatile NAND chip to store computer hardware information and user settings. When the console is turned on, the bootloader loads the firmware from the NAND [5]. The NAND 3DS console is protected with a special console key that prevents inspection/cyber-attacks by NAND without obtaining the decryption key.

Figure 1

Explanation of Cyber attracts



Although JTAG proves to be a feasible way to locate the NAND, to render the image readable, hardware and other methods of achieving the decryption key are needed. 3dbrew (2015a) provides a helpful information source for folder names.

Literature Review

Cybersecurity states that the rules and guidelines used to protect the device, data, and database from a malevolent attack are created. The basic functionality includes safeguarding the device with data from different cyber threats and cybercrimes. It is also an exercise in defending devices, services, and networks from different kinds of web attacks. Such crimes can, however, result in data damage, data theft, or disruption to modern and digital life [6].

Cases of Cyber Threats

Cybersecurity states that the rules and guidelines used to protect the device, data, and database from a malevolent attack are created. The basic functionality includes safeguarding the device with data from different cyber threats and cybercrimes. It is also an exercise in defending devices, services, and networks from different kinds of web attacks. Such crimes can, however, result in data damage, data theft, or disruption to modern and digital life [6]. Closer to household, we have observed that Clare centered Loyalty build firm grieve a safety rupture late previous year, that uncovered details of credit cards of clients, the bulletins feature emphasized method that police interrupted a felonious criminals' virus network that they made through to snip over a hundred million dollars [7].

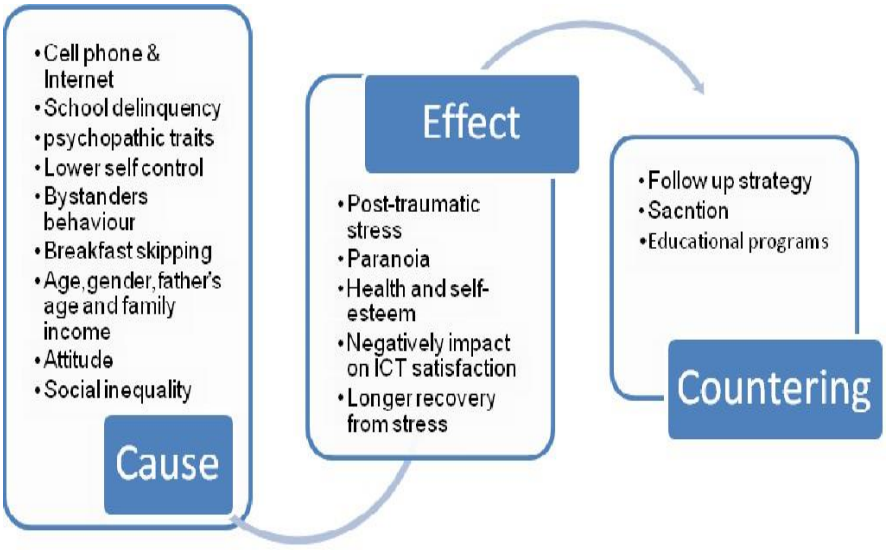
Cyber-crimes are now becoming a large entities and thieves are beholding to snip information that is fiscal details, personal entails, and information from the credit cards or some other important information may be government secrets that they can trade and sell, such delinquents are charming more complex and unpredictable where they use new techniques every day for attacking companies', individuals and even the government computer networks [8].

Among the common armaments in their collection is the virus from the computers. Mostly they used emails to pass the virus, but now they can even use flash disc or the USB device to pass the virus to a computer. The viruses

from the computer can get into the network by a USB gadget; prompt contacting from the social media podiums, file relocation, and folder allotment programs, going into an infested website, or by local operators linking straight to the venture network using an infected computer. When a virus catches a computer, it may randomly feast to other computers in a lot of means [9].

Figure 2

Cause Effects and Counting



Effects of Cybersecurity Threats

Too much security can flop and thus reveal information that is important and sensitive to individuals or even businesses, thus endangering their privacy, and it can trigger a fracturing of the economy that comes from a lot of money laundering from criminals and selling government secrets to dangerous hands. Cybercrimes, however, will impede the progress and promising future of technology if not well looked at [10]. It may also lead to trauma in people who have often been targeted by these technical know-how offenders where their private information has been leaked and also if

their credit cards have been hacked and all their money withdrawn, causing individuals a lot of tension [11].

Improperly configured firewalls may prevent users from performing certain Internet actions until the firewall is properly configured. This makes the software more sluggish than before. There are some of the positive steps that can be used to avoid cyber-attacks because of the rise in cyber threats and which has shown that it can impede many things, starting from people, communities and the government, and such measures are costlier and very few can afford to make it a cybersecurity disadvantage [12].

Cyber threats can also influence the great dangers of war between nations, where some nations can use their brilliant cyber experts to develop some deadly viruses, such as coronaviruses, to target other nations. In the future, cyber-attacks will be used as a new means of targeting nations; if not well controlled, there will be a lot of dangers in the future.

Solutions to Cybersecurity Threats

If the frequent allocation means that a device that has been compromised by a virus will blow out, it is possible to use different solutions to curb cyber threats. Fixing Anti-Virus software is advisable. Certify the installation of trustworthy antivirus software on the whole device. This should include all servers, computers and laptops. If employees are able to use homegrown PCs for business use or to access the network locally, these machines must have antivirus software enabled [13].

Always ensure that the antivirus programed is modified. Brand new PC viruses are unconfined on a daily basis, and by ensuring that the antivirus is up to date, it is vital for companies to be safe against these viruses. Companies should look at methods, if conceivable, whereby machines that do not have the new antivirus software installed are not allowed to connect to the network [14].

For PC viruses, all the traffic from the emails, incoming and outgoing emails must be sifted. This restriction should ideally be on the network limit to prevent emails from PCs viruses with confident folder attachments often castoff by viruses from PCs to blowout themselves, such as .COM and. The inflow into the network must also be prevented by SCR directories.

Train those who use emails to be careful of apprehensive messages. Confirm that any user has information that is definitely not subject to an attachment or to connect to an email link that they do not anticipate. Even, if the email is from a known source, care should be taken when opening supplements or clicking on links in emails. Felons use the trust put in a contact you know by email to coax you to click on a connection or attachment [15].

Review of copies on the Internet. This test must be conducted from one dominant situation on the network to ensure that all files are correctly scanned, certifying that the entire directories downloaded from the internet are ideally used for PC viruses before being used. Do not run Obscure Source systems. For your software requirements, it is essential that you use a reliable source. This is to ensure that it is possible to remove all the installed software and that its origins can be established to be genuine [16].

Confine end-user access to structures under which their workplaces should not be granted administrative honors to end-users where conceivable. Only from the point of view of the user who is logging into the device will most processor viruses work. That is, they just have the same permission as the program's operating user [17].

Therefore, the real and potential issues that can pull technology and technologies down if not well managed are cyber threats. They are malicious activities that seek data destruction, can also refer to the prospect of a successful cyber-attack aimed at obtaining unauthorized entry, stealing the capacity of IT, and certain intellectual possessions or even sensitive data. 2020, however, is coming with an entirely new level of cyber security terrorization that organizations need to be aware of stealing the capacity of IT, and certain intellectual possessions or even sensitive data. 2020, however, is coming with an entirely new level of cyber security terrorization that organizations need to be aware [18].

In reality, a threat horizon study shows that in the coming years, under the following refrains, organizations will experience cyber threats; disruption, over-independence on critical connectivity will increase the risk of premeditated internet outages that threaten business maneuvers. Cybercriminals use ransomware to seize items on the internet. Distortion,

bots' dissemination of manufacturing, and programmed sources can trigger confidence compromise in the information's reliability [19].

Deterioration: faster developments in cool technology and competing demands posed by sprouting national security can adversely affect the capacity of an organization to monitor data. Data breaches, service rejection, computer viruses, and other attack vectors are therefore the worst and most common cyber threats in the world we live in today.

Research Methodology

Strength Data Security and Access Management

Information security controls on main vulnerability snapshots. Character and board access often help to reduce the possibility of human error, the best explanation for data penetration. This course will introduce you to the key personalities of the models and resources of the executives, to further improve the digital flexibility of your association. In this network safety instructional class, you will be familiar with key personality and access the board idea to find key character and access the executive's ideas. It is the first of two courses addressing board access. You will learn: what character and admission mean and why the executive ideas of 'ID' and 'validation' are important to the concept of 'authorization' the part of cybercrime management hierarchical information security steps [20].

I. IDS and IPs

A system that scans incoming digital traffic is an intrusion detection system. Intrusion protection is simply a device that plays a crucial role in avoiding intrusion. During any inquiry, IP numbers are used. Cyber security

identifies an IP address, and then the specifics of any remote machine or device can be identified.

II. Internet Protocol Address

Every machine has an IP address of its own. It's just a number with the aid of a system or machine that we can quickly locate and investigate. If I want to download a file from the internet, the machine and the internet are linked to each other by underground or wireless or water cables, so my computer should have an address so that other computers on the internet can identify my computer and locate it in internet terms. The address of a camper is called IP. We can find information about remote machines with the aid of this. In the remote machine access process, it plays a vital role. In most cases, the knowledge anyone can obtain based on your IP address is minimal. You can find the neighborhoods, the zip code (or one nearby) and the area code that is associated with the area. They'll see what internet service you are using and whether there is an IP address for any blacklists [21].

III. Firewall in system

It is important to configure and test regularly updated and for security threats. We often see remote management services displayed on the public network in login research, rather than properly secured systems that allow only 'trusted' LAN or VPN access [22].

IV. Segregation of Network

For all network exit points and entry points, it is important to verify that the partition is working well. Server-customer separation should be monitored by businesses. Goal reduction where needed, before jumping into the target and finally breaching the POS network, hackers started to compromise a third-party provider network.

V. Enumeration-Strong Passwords

During our Internal Penetration Test, we've identified file sharing without proper permissions and username enumeration due to poorly configured Windows services as some outcomes. Organizations need to enforce strong password policies for all users while adhering to password complexity guidelines.

Internet-facing applications are increasingly vulnerable to attacks, posing significant risks to businesses. Common threats include SQL Injection, Cross-Site Scripting, and Parameter Tampering attacks. Tests should include rigorous examination of application code, thorough installation testing, and meticulous validation of user-controlled inputs.

It's crucial to monitor and restrict admin rights for both customers and network service accounts. Granting excessive privileges can lead to unauthorized access to admin authentication tokens and domain control data, increasing the risk of network compromise.

Regular patch management is essential to mitigate risks associated with third-party software vulnerabilities and network compromises. Conducting frequent tests, including risk scanning, can help identify vulnerabilities and weaknesses in network paths, ensuring better security measures are in place.

Cyber forensics plays a critical role in investigating criminal offenses, but challenges arise in determining the scope of incidents and implementing preventive measures, depending on their scale and complexity.

With respect to the first question, the role of forensics is evident. Information gathered at the scene is closely examined in order to explain the' who, what, where, and why' of the incident. Cyber forensic experts make detailed reports of the incident to solve all questions and use the gathered data to prevent such attacks from occurring in the future [23].

VI. PSCAP

It is an effective tool for file analysis and monitoring of your network traffic. There are many reasons why networks are being monitored using PCAP. Bandwidth usage management, identification of strong DHCP servers, malware detection, DNS setup, and transparency are some of the most common features. On analyzing overall security issues at social media, corporate sector as well in the banking sector we have found the issues resulted as below that need to be sorted out on priority [24].

VII.1-Phishing Attacks:

Attackers create counterfeit web pages resembling legitimate ones, prompting users to input their credentials. Users unwittingly fall into the trap when they enter their login details. Kaspersky Lab data from 2014 indicated that approximately 22 percent of phishing attacks involved fake social network profiles mimicking Facebook users. Phishing poses a significant threat in Russia and Europe, with a surge of 18 percent to 36.3 million attacks in Q3 2015 compared to the same period the previous year, as reported by Kaspersky Lab. For instance, a Moldovan individual orchestrated a phishing scheme resulting in a $3.5 million loss for a drilling company in western Pennsylvania. In a case study involving a school district, scammers nearly succeeded in swindling nearly a million dollars. One instance involved an email containing malware disguised as a zip file attachment, which compromised the recipient's device [24].

Identity Federation Challenges

The virus spreads through Facebook's chat feature, sending an attachment accompanied by the message "lol" to users. Clicking on the link initiates the download of malware onto the user's computer, leading to infection. Subsequently, the virus propagates through the network, gaining access to the user's details. It may seem easy, but it may not be possible for the consumer to know how and to what extent it is possible to share their personal information with third-party applications [25].

Malwares

Malware refers to programs installed on users' computers without their knowledge or consent, spreading quickly and corrupting systems. The AV-Test Institute reports that 390,000 malicious programs are registered daily (AV-TEST, 2016). Malicious software includes viruses, worms, and Trojan horses, all originating from security vulnerabilities in software. Attackers can access users' personal information by monitoring device actions, exploit computers, or launch mass attacks without user awareness, potentially stealing identities or crashing systems. Additionally, hackers may install adware, causing endless pop-up ads on users' screens. such as

1. ***'LOL' Virus***

This virus is spread through Facebook's chat function. It sends an attachment to users with the message "lol." When the user clicks on the link, the malware is downloaded to their computer, infecting it. The virus then spreads through the network, accessing the user's details [26].

2. Zeus:

This is a Trojan which spreads by clicking on the link. And all the files on the user's device are scanned when a user clicks on the link and significant information is stolen. The capacity of this Trojan is to rob the bank credentials of the recipient.

Click Jacking Attacks:

It is often referred to as Attacks of UI Redress. Where the Trojan asks the user to click on the web pages for a malicious link, and a malware is planted by the computer. It is prevalent with the word jacking on Facebook, which is when the user is caught by the attackers when a page, picture or video is liked by a user. To carry out a malicious attack or make a page famous, this kind of attack is carried out [27].

Conclusion

In this era of digital revolution and globalization, cybercriminals are constantly seeking new ways to exploit and harm organizations and institutions. They devise inventive methods to deceive and disrupt, posing a serious threat to companies, citizens, emerging technologies, and even government operations. It's crucial for companies to be aware not only of the increasing number of vulnerabilities but also of the cybersecurity threats that loom ahead. It's important to recognize the measures taken by these organizations, as outlined in this document, to address various types of attacks. This proactive approach is vital for businesses as they strive to reduce the likelihood and impact of cyber threats.

References

[1] “Pripas, M. (2014). Phishing attack detection and removal. The international journey of information security and cybercrime, 59-64.

[2] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*. oup usa, 2014. https://books.google.com/books?hl=en&lr=&id=f_lyDwAAQBAJ&oi=fnd&pg=PP1&dq=2.%09Singer,+Peter+W.,+and+Allan+Frie

dman.+Cybersecurity:+What+everyone+needs+to+know.+Our+USA,+2014%3B+27-33&ots=Dol1RFACll&sig=ajZ112iJksU6R8IkSq-NkmDmHyc

[3] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology innovation management review*, vol. 4, no. 10, 2014. Available: https://www.timreview.ca/article/835

[4] S. Peng, "Cybersecurity threats and the WTO national security exceptions," *Journal of International Economic Law*, vol. 18, no. 2, pp. 449–478, 2015.

[5] M. Lněnička, J. Čapek, J. Komárková, R. Máchová, and I. Čermáková, "A solution to combat cybersecurity threats involving big data analytics in the Hadoop ecosystem," in *Proceedings of the 30th International Business Information Management Association Conference*, International Business Information Management Association-IBIMA, 2017. Available: https://dk.upce.cz/handle/10195/69945

[6] "Latest in phishing 2016". Available: https://info.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2016.

[7] "Malware statistics. Available: https://www.av-test.org/en/statistics/malware/ - Google Search."

[8] C. S. Lee and Y. Wang, "Typology of cybercrime victimization in Europe: A multilevel latent class analysis," *Crime & Delinquency*, vol. 70, no. 4, pp. 1196–1223, 2024.

[9] I. Bernik, K. Prislan, and A. Mihelič, "Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia," *Sustainability*, vol. 14, no. 21, p. 14487, 2022.

[10] R. Mokhtar and A. Rohaizat, "Cybercrimes and Cyber Security Trends in the New Normal," in *The New Normal and Its Impact on Society: Perspectives from ASEAN and the European Union*, Springer, 2024, pp. 41–60.. Available: https://link.springer.com/chapter/10.1007/978-981-97-0527-6_4

[11] K. Lin, Y. Wu, I. Y. Sun, and J. Qu, "Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory," *Criminology & Criminal Justice*, p. 17488958221146144, 2023.

[12] H. T. N. Ho, H. T. Luong, and Q. A. Phan, "Mapping the Influences of Social Network Site Use on Cybercrime Victimization: Trends and Recommendations," *Asian Communication Research*, vol. 21, no. 1, pp. 80–106, 2024.

[13] S. Srivastava and S. Raj, "Cyber Security Assessment and Awareness: A Statistical Modelling Approach," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, IEEE, 2024, pp. 1–6. Available: https://ieeexplore.ieee.org/abstract/document/10482035/

[14] M. Mikkola *et al.*, "Cyberharassment victimization on three continents: an integrative approach," *International journal of environmental research and public health*, vol. 19, no. 19, p. 12138, 2022.

[15] B. Dupont, F. Fortin, and R. Leukfeldt, "Broadening our understanding of cybercrime and its evolution," *Journal of Crime and Justice*, pp. 1–5, Feb. 2024, doi: 10.1080/0735648X.2024.2323872.

[16] C. E. Griffith, M. Tetzlaff-Bemiller, and L. Y. Hunter, "Understanding the cyber-victimization of young people: A test of routine activities theory," *Telematics and Informatics Reports*, vol. 9, p. 100042, 2023.

[17] J. E. Ntsama *et al.*, "Determinants of Cybercrime Victimization: Experiences and Multi-stage Recommendations from a Survey in Cameroon," in *Towards new e-Infrastructure and e-Services for Developing Countries*, vol. 499, R. A. Saeed, A. D. Bakari, and Y. H. Sheikh, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 499. , Cham: Springer Nature Switzerland, 2023, pp. 317–337. doi: 10.1007/978-3-031-34896-9_19.

[18] R. Rughiniș, E. Bran, A. R. Stăiculescu, and A. Radovici, "From Cybercrime to Digital Balance: How Human Development Shapes Digital Risk Cultures," *Information*, vol. 15, no. 1, p. 50, 2024.

[19] S. L. Clevenger and C. D. Marcum, *The Link between Specific Forms of Online and Offline Victimization: A Collaboration Between the ASC Division of Victimology and Division of Cybercrime*. Taylor & Francis, 2023. Available: https://books.google.com/books?hl=en&lr=&id=QObLEAAAQB

AJ&oi=fnd&pg=PT10&dq=Cyber+Risk+and+Cyber+Crimes+on+User%27s+Online+Victimization+2021+to+2024&ots=oBAD2CddWV&sig=ryj0mVsi7vKmqgNis7KLPR55BDg

[20] F. T. Johora, M. S. I. Khan, E. Kanon, M. A. T. Rony, M. Zubair, and I. H. Sarker, "A Data-Driven Predictive Analysis on Cyber Security Threats with Key Risk Factors." arXiv, Mar. 28, 2024. Available: http://arxiv.org/abs/2404.00068

[21] R. Raju, N. H. Abd Rahman, and A. Ahmad, "Cyber security awareness in using digital platforms among students in a higher learning institution," *Asian Journal of University Education*, vol. 18, no. 3, pp. 756–766, 2022.

[22] J. Herrero, A. Torres, P. Vivas, A. Hidalgo, F. J. Rodríguez, and A. Urueña, "Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization," *International journal of environmental research and public health*, vol. 18, no. 7, p. 3763, 2021.

[23] M. S. Van 'T Hoff-de Goede, E. R. Leukfeldt, R. Van Der Kleij, and S. G. A. Van De Weijer, "The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization," in *Cybercrime in Context*, vol. I, M. Weulen Kranenbarg and R. Leukfeldt, Eds., in Crime and Justice in Digital Society, vol. I. , Cham: Springer International Publishing, 2021, pp. 21–41. doi: 10.1007/978-3-030-60527-8_3.

[24] M. Vale, F. Pereira, B. H. Spitzberg, and M. Matos, "Cyber-harassment victimization of Portuguese adolescents: A lifestyle-routine activities theory approach," *Behavioral Sci & The Law*, vol. 40, no. 5, pp. 604–618, Sep. 2022, doi: 10.1002/bsl.2596.

[25] M. Özaşçılar, C. Çalıcı, and Z. Vakhitova, "Examining cybercrime victimisation among Turkish women using routine activity theory," *Crime Prev Community Saf*, vol. 26, no. 1, pp. 112–128, Mar. 2024, doi: 10.1057/s41300-024-00201-y.

[26] J. Curtis and G. Oxburgh, "Understanding cybercrime in 'real world' policing and law enforcement," *The Police Journal: Theory, Practice and Principles*, vol. 96, no. 4, pp. 573–592, Dec. 2023, doi: 10.1177/0032258X221107584.

[27] R. Ch, T. R. Gadekallu, M. H. Abidi, and A. Al-Ahmari, "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, no. 10, p. 4087, 2020.