Cyber Fraud in the Pandemic Age: Causes and Consequences

Mazurina Mohd Ali[1*], Noor Hasniza Haron[2]

[1,2] Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000260

Received: 08 October 2025; Accepted: 14 October 2025; Published: 10 November 2025

ABSTRACT

The COVID-19 pandemic was an important factor that has reshaped how individuals and organization's function, accelerating global reliance on digital technologies for work, communication, education, and commerce. While this shift ensured continuity during lockdowns, it also created opportunities for cybercriminals. The purpose of this study is to examine the surge in cyber fraud during the pandemic, its causes, and socio-economic impacts. Past studies determine that cyber fraud leads to financial losses and psychological distress. To counter these risks, the paper recommends enhancing cybersecurity literacy, enforcing data protection, maintaining vigilance, and strengthening institutional and governmental measures. It concludes by stressing the need for ongoing public awareness, policy action, and personal responsibility in combating cyber fraud in the post-pandemic digital era.

Keywords: COVID-19 pandemic; cybercrime; online scams; socio-economic impact; preventive measures

INTRODUCTION

Globally, the world had recorded more than 40 million COVID-19 cases by October 2020, with the worldwide death toll surpassing one million (Ryan, 2021). Beyond its devastating health impact, the pandemic became the subject matter that transformed nearly every aspect of daily life, forcing individuals and communities to rethink how they live, work, and interact. In most cases, lockdowns, travel bans, and social distancing measures reshaped social norms and redefined the rhythm of human connection. As homes became workplaces, classrooms, and social hubs, massive reliance on digital technology deepened. Internet usage became very significant across the globe, with people turning to online platforms not only for banking, healthcare, and education but also for entertainment, business continuity, and access to essential public services (Ray et al., 2025). Changes to consumer patterns and government responses have affected the ecosystems and economies of the cyber world (Juneja et al., 2024).

While this digital transformation has supported economic and social continuity, it has also created new vulnerabilities that cybercriminals actively exploit. The unprecedented increase in online activity, coupled with limited cybersecurity awareness among users and organizations, has led to a surge in cyber fraud incidents worldwide (Pandey & Kapoor, 2025). Phishing, scams, fake online profiles, data breaches, and other forms of cybercrime have intensified, targeting individuals and institutions already burdened by the economic and emotional stress of the pandemic (Ma & McKinnon, 2022). Despite the growing number of reported cases and the severe financial and psychological consequences for victims, public awareness and preparedness remain inadequate. Besides, many developing economies face additional challenges such as weak digital infrastructure, limited law enforcement capacity, and lack of coordinated cybersecurity policies (Anazodo, 2025). Primarily, this situation underscores the urgent need to understand the nature, causes, and impacts of cyber fraud during the COVID-19 crisis and to identify effective precautionary measures to mitigate its risks in the post-pandemic digital era.

The main objective of this concept paper is to explore the increasing occurrences and impacts of cyber fraud during the COVID-19 pandemic. This concept paper is significant as it contributes to the growing body of knowledge on cyber security and fraud prevention in the context of the COVID-19 pandemic. The study

highlights the evolving nature of cyber threats and the vulnerabilities created by the rapid shift toward digital dependence. By examining the relationship between pandemic-driven digital transformation and cybercrime, this paper provides valuable insights for policymakers, organizations, and individuals. This study aims to promote a culture of cyber vigilance and resilience, encouraging a proactive rather than reactive approach to cybersecurity. Cyber fraud is inevitable, however, understanding and addressing the implications of cyber fraud in the COVID-19 era is essential not only for protecting financial assets but also for preserving mental well-being, social trust, and the stability of the global digital economy.

DISCUSSION ON GLOBAL ISSUES RELATED TO CYBER FRAUD

It is an unfortunate reality that fraudsters often exploit unforeseen incidents and challenging situations to carry out their fraudulent activities. Fraudsters will always take an opportunity for their interest especially when normality becomes disrupted. This happened during the pandemic COVID-19 when there was a significant increase in fraudulent activity. INTERPOL (2020) highlighted that the growing global reliance on online platforms has opened up new opportunities for cybercriminals, as many individuals and organizations fail to maintain robust and up-to-date cybersecurity measures.

Some of the key findings of the cybercrime landscape in relation to the COVID-19 pandemic merely include phishing, data theft, fake profiles and time theft (Gryszczyńska, 2021; Choudhary et al., 2022; Ma & McKinnon, 2022). Phishing happened when cybercriminals employ deceptive emails that mimic legitimate communications to manipulate individuals (Alkhalil et al., 2021; Ali and Mohd Zaharon, 2024). Such arrangements are made until sensitive information is disclosed or harmful actions are performed. These fraudulent messages often appear to originate from reputable organizations—such as financial institutions—and may prompt recipients to open malicious attachments or contact counterfeit customer service channels designed to harvest personal data (Ali and Mohd Zaharon, 2024). In more severe threats, phishing campaigns may also use cloned websites that perfectly resemble the real platforms (MohamedAli & Abduhameed, 2024), making it difficult for individuals to recognize fraud. Eventually, the goal of phishing is to exploit human trust (Wright et al., 2014) and induce actions that lead to financial loss, data breaches, or unauthorized system access (MohamedAli & Abduhameed, 2024).

Moreover, data theft happens when the shift toward remote working environments has granted employees unsupervised access to organizational data, including highly sensitive client information (Al-Harrasi et al., 2023). This situation presents significant security risks, particularly within sectors such as healthcare and financial services, where data breaches can result in severe financial and legal consequences. Data theft portrays malicious insiders with intentional motives or from well-intentioned employees who exhibit negligence in data handling practices (Homoliak et al., 2019). For instance, leaving computers unlocked or unattended in shared home environments can expose confidential information to unauthorized third parties, such as family members or visitors. Such mistakes in data protection protocols can compromise corporate security, damage client trust, and potentially lead to financial losses or reputational harm.

Furthermore, the propagation of fraudulent profiles on social media platforms has arisen as a prominent form of cyber threat (Ramalingam & Chinnaiah, 2018). Cybercriminals often create counterfeit accounts that mimic legitimate users by incorporating names, photographs, or networks recognizable to the target, to name a few. This is to establish a false sense of trust. Once connection is built, the perpetrator may solicit financial assistance, request personal information, or manipulate the victim into actions that serve the fraudster's interests. Such manipulative practices not only compromise individual privacy and security but also erode trust in online social networks. Similarly, fraudulent profiles activities have become a serious threat since they can cause concerns about the credibility and reliability of the victim.

Finally, time theft, a predominant form of payroll fraud. Time theft occurs in a condition when employees, generally those compensated on an hourly basis or who bill clients for their time, deliberately misreport or falsify their working hours (Harold et al., 2022). This unethical practice may take various forms, including engaging in personal activities during work hours, or failing to inform employers of absences (Harold et al., 2022). Conventionally, organizations could easily monitor employee attendance and productivity through direct supervision and timekeeping systems within physical work settings. Nonetheless, the emergence of remote and

hybrid work arrangements has made supervising mechanisms complicated which significantly create new vulnerabilities for time-related fraud.

The Impact of Cybercrime on Socio-Economic and Political Dimensions

Conceptually, crime is a dynamic and relative phenomenon that evolves in response to social, political, and economic transformations within a society (Bhowmik, 2023). Thus, it is neither feasible to establish an all-encompassing definition of "crime" applicable across all contexts nor to formulate a single definition that remains relevant across different societies or time periods. The nature of crime is influenced by shifts in correlated social phenomena and the value systems shaped by these changes. In contemporary contexts, where monetary gain often supersedes moral values, there has been a noticeable increase in corruption-related offenses, particularly in societies where social morality is diminishing. Such environments tend to reduce the social stigma associated with criminal behavior. Notably, economic crime appears to be at its peak, reflecting the intricate interdependence between crime, social structures, economic systems, and political institutions.

From a theoretical perspective, the incidence of crime is closely intertwined with various demographic, socioeconomic, and political determinants. Population dynamics, in particular, play a significant role in influencing crime rates, as numerous studies have identified a positive correlation between population growth and the frequency of criminal activities (South & Messner, 2000; Kovandzic & Vieraitis, 2006). Beyond population factors, contextual variables such as urbanization rates, migration patterns, unemployment levels, income inequality, and, in the case of cybercrime, computer literacy, have also been found to shape crime incidence (Chen et al, 2023; Singh et al., 2025). In addition, the economic structure of a society exerts a substantial influence on economic and financial crimes, as disparities in wealth distribution and access to resources often substitute conditions conducive to deviant behavior (Ayinla, 2024). Besides, the political system, through its role in formulating norms, instituting legal frameworks, and implementing preventive measures—acts as a crucial moderating force in crime control (Stummvoll, 2012; Stenson, 2012). Subsequently, crime cannot be viewed in isolation but must be understood as a socially constructed phenomenon shaped by the interrelationships among socioeconomic, political, and cultural factors. This theoretical interdependence underscores that the definition and nature of crime are fundamentally contextual, evolving in response to shifts in societal values and institutional structures.

Precautionary Measures Towards Cyber Risks

The exposure and incidence of cyber threats are significantly heightened due to the massive rise in digital dependency during and after the COVID-19 pandemic. Therefore, as people and organizations become more dependent on digital platforms for their daily activities, having strong cybersecurity measures in place has become more important than ever. Hence, three major areas of precautionary measures, namely, (a) developing knowledge and awareness, (b) implementing information security technologies, and (c) sustaining cyber vigilance will be further discussed.

a) The Importance of Knowledge in Preventing Cyber Fraud

The foundational defence mechanism against cybercrime is knowledge and awareness (Mali et al., 2018). Individuals and organizations as users will be able to recognize potential threats and respond efficiently, if they continuously learn cybersecurity. Apart from continuous learning, users' understanding of how to identify and mitigate risks associated with phishing, identity theft, and social engineering could be enhanced by participating in structured cybersecurity courses, professional certifications, and awareness campaigns (Kenneth et al., 2023; Pinjarkar et al., 2024; Wright et al., 2014). Therefore, cybersecurity literacy is particularly essential to promote safe online behavior and protecting sensitive data, (Kont, 2023). Accordingly, a preventive and empowering strategy in modern digital ecosystems is the investment in cybersecurity education.

b) Implementation of Information Security Technologies

To ensure the integrity, confidentiality, and availability of digital resources, robust information security infrastructure is crucial (Nadji, 2024). A multi-layered security strategy, such as the integration between technological solutions and human oversight can effectively deter cyber threats.

Securing Personal Devices and Accounts

To secure all internet-connected devices, reputable antivirus software should be installed and regularly updated. Additionally, the passwords used for e-mail, social media accounts and banking websites must be strong and unique. When available, the passwords should be supported by multifactor authentication. Furthermore, to prevent unauthorized data sharing and strengthen online confidentiality and privacy, the privacy settings must regularly be reviewed.

Mitigating Phishing and Social Engineering Attacks

One of the most prevalent cyber threats is phishing (Ali and Mohd Zaharon, 2024). To reduce phishing, users should avoid opening links or attachments in unsolicited messages or e-mails. This action is important to cease users from sharing financial or personal details via unverified communications. Also, to avoid falling victim to phishing attacks, users should seriously evaluate the legitimacy of digital correspondence. For instance, in an organization, to improve the employees' ability to identify phishing sites and to reduce risks related to that, phishing simulations such as typographical differences between fake and legitimate websites and awareness campaigns should be incorporated (Moreno-Fernández et al., 2017).

Safeguarding Organizational Data During Remote Work

To safeguard organizations especially in remote working environment, they must ensure employees are trained in data protection, confidentiality policies, and the responsible use of digital tools. Accordingly, the security controls, particularly those implemented rapidly during the pandemic should be routinely assessed in terms of its effectiveness. Apart from the technological solutions to detect anomalies or insider threats (Muku et al., 2025), another essential element is continuous monitoring of user activity and device access (Alzaabi & Mehmood, 2024). Furthermore, organizations must evaluate the cybersecurity compliance of external partners and suppliers, as weaknesses in the supply chain can result in extensive data breaches.

c) Sustaining Cyber Vigilance and Scam Awareness

Cyber vigilance involves maintaining a proactive and sceptical stance toward potential scams and fraudulent activities (Button & Whittaker, 2021). Scammers frequently adapt their methods, exploiting uncertainty and public trust through impersonation of legitimate entities such as financial institutions, government agencies, or charitable organizations (Taodang & Gundur, 2023). Users should adopt a habit of verifying the authenticity of requests and conducting independent research before engaging in financial or personal exchanges. For example, individuals should avoid responding to prompts or providing information when receiving suspicious phone calls. Additionally, when dealing with unconventional payment requests, including those involving cryptocurrency, wire transfers, or gift cards, caution should be further exercised. When encounter suspicious incidents, victims of cyber fraud should immediately report that incidents to relevant authorities or cybersecurity agencies, as prompt reporting facilitates investigation, legal recourse, and broader fraud prevention awareness (Chhabra Roy & P, 2024).

In conclusion, a holistic and proactive approach that combines education, technological safeguards, and continuous vigilance are essential in preventing cyber fraud. While robust technological defenses provide critical protection against evolving threats, enhancing cybersecurity literacy equally empowers users to make informed decisions. At the same time, cultivating sustained awareness and scepticism toward potential scams is critical to minimizing personal and institutional vulnerabilities. Eventually, collective responsibilities among individuals, organizations, and governments are needed in fostering a secure and resilient digital ecosystem capable of withstanding future cyber challenges.

CONCEPTUAL FRAMEWORK

Cyber attackers are enjoying a renaissance of the increasing availability of bandwidth, connected devices, and affordable attack tools that allow them to launch more complex and potent attacks against a cyber-security practitioner's residential subscribers and businesses (Mallick & Nath, 2024). The threat to cyber-security is growing at vast rate. Cybercriminals are becoming cleverer and are now targeting consumers as well as public

and private organizations (Saini et al., 2012). The lack of cyber security leads to the arising trend of cybercrimes.

The conceptual framework of this paper is grounded in the understanding that technological dependency, human behaviour, and institutional preparedness interact to influence the prevalence and impact of cyber fraud, particularly during crisis periods such as the COVID-19 pandemic. The framework proposes that the COVID-19 pandemic acted as a catalyst for the digital transformation of daily life, that leads to the increasing online activities such as remote work, digital banking, e-commerce, and online education. While beneficial for social and economic continuity, this rapid digitalization also amplified exposure to cyber risks.

The key determinants identified in this framework include: (1) technological factors such as increased internet usage, weak data protection systems, and rapid adoption of online platforms without adequate cybersecurity measures; (2) behavioural factors such as low cybersecurity awareness, stress, and psychological vulnerability among individuals during the pandemic, making them more susceptible to scams and phishing; and (3) institutional and policy factors such as limited law enforcement capacity, lack of coordinated cybersecurity policies, and weak corporate governance mechanisms. These factors collectively lead to an increase in cyber fraud incidents, resulting in financial losses, psychological distress, and social insecurity. The framework further emphasizes that cybersecurity awareness, education, and preventive strategies can serve as mitigating mechanisms that reduce both the frequency and impact of cybercrimes.

In summary, the conceptual model illustrates a cause-and-effect chain as follows:

Pandemic-Driven Cyber Fraud Dynamics Framework

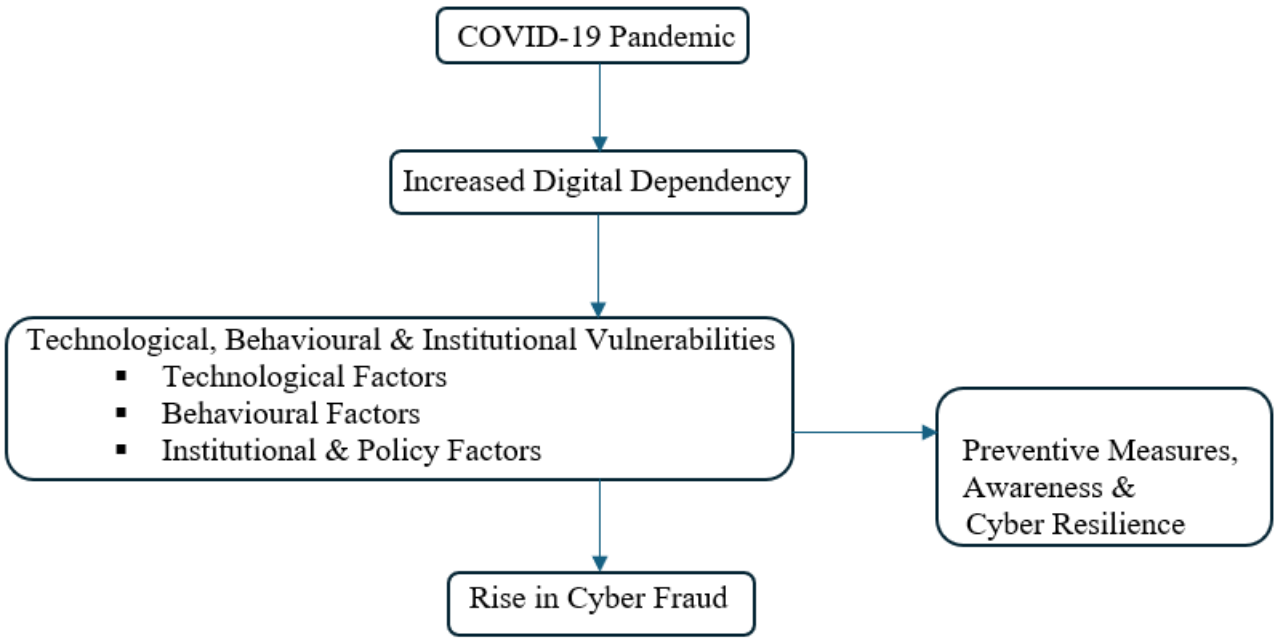

Figure 1. Conceptual Model of Pandemic-Driven Cyber Fraud Dynamics

CONCLUSION

The COVID-19 pandemic and the resulting lockdown measures have confined much of the global population to their homes, leading to a substantial increase in the amount of time people spend online. The reliance on the Internet became unprecedented as individuals sought to maintain access to essential services that were traditionally obtained offline. The pandemic has fundamentally transformed people's routine and their interaction since nowadays, the interactions are largely conducted through digital means. Nonetheless, the incidence of cyber fraud has escalated dramatically, as online engagement has intensified, revealing new vulnerabilities in the digital landscape. The consequences of cyber fraud extend far beyond financial loss, often leaving victims to struggle with profound psychological distress. Therefore, to ensure data integrity, practicing good cybersecurity hygiene may help. By following these preventive measures and promoting cybersecurity awareness, cyberattacks can be significantly reduced.

REFERENCES

1. Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875-888.
2. Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101-121.
3. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.
4. Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, *12*, 30907-30927.
5. Anazodo, R. O. (2025). Cyber Security Administration in Developing Countries: A Nigerian Perspective. *International Journal of Finance, Accounting and Management Studies*, *1*(4), 122-139.
6. Ayinla, O. A. (2024). The Impact of Crime on Economic Hardship In Oyo State, Nigeria. *Journal of Business Development and Management Research*.
7. Bhowmik, S. (2023). The Evolution of Crime: The Dynamic Definition of Crime as per Society. *Issue 3 Int'l JL Mgmt. & Human.*, *6*, 3638.
8. Button, M., & Whittaker, J. (2021). Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation. International Journal of Law, Crime and Justice, 66, 100482.
9. Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*, *26*(6), 678-707.
10. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 1-10.
11. Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., & Dragoni, N. (2022). Emerging cyber security challenges after COVID pandemic: a survey. *Journal of Internet Services and Information Security*, *12*(2), 21-50.
12. Gryszczyńska, A. (2021). The impact of the COVID-19 pandemic on cybercrime. *Bulletin of the Polish Academy of Sciences. Technical Sciences*, *69*(4).
13. Harold, C. M., Hu, B., & Koopman, J. (2022). Employee time theft: Conceptualization, measure development, and validation. *Personnel Psychology*, *75*(2), 347-382.
14. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.
15. INTERPOL. (2020, August 4). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
16. Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: opportunities, growth and challenges. *Journal of technology innovations and energy*, *3*(2), 1-22.
17. Kenneth, A., Hayashi, B. B., Lionardi, J., Richie, S., Achmad, S., & Junior, F. A. (2023, August). Phishing attack awareness among college students. In *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)* (pp. 344-348). IEEE.
18. Kont, K. R. (2023). Cyber literacy skills of Estonians: activities and policies for encouraging knowledge-based cyber security attitudes. *Information & Media*, (96), 80-94.
19. Kovandzic, T. V., & Vieraitis, L. M. (2006). The effect of county-level prison population growth on crime rates. *Criminology & Public Policy*, *5*(2), 213-244.
20. Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2), 433-446.
21. Mali, P., Sodhi, J. S., Singh, T., & Bansal, S. (2018). Analysing the awareness of cybercrime and designing a relevant framework with respect to cyber warfare: an empirical study. *International Journal of Mechanical Engineering and Technology*, *9*(2), 110-124.
22. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.
23. MohamedAli, R. S., & Abduhameed, R. A. (2024, May). Phishing email detection: Survey. In *International Conference on Advanced Engineering, Technology and Applications* (pp. 551-570). Cham: Springer Nature

Switzerland.

24. Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior*, *69*, 421-436.
25. Muku, A., Singh, S. K., Kumar, S., Sharma, A., Rai, P., Upadhyaya, B., ... & Sharma, V. (2025). Phishing prevention solutions and mechanisms. In *Critical Phishing Defense Strategies and Digital Asset Protection* (pp. 49-72). IGI Global Scientific Publishing.
26. Nadji, B. (2024). Data security, integrity, and protection. In *Data, Security, and Trust in Smart Cities* (pp. 59-83). Cham: Springer Nature Switzerland.
27. Pandey, P., & Kapoor, A. (2025). Cybercrime In the Digital Era: Impacts, Awareness, And Strategic Solutions for a Secure Future. *Sachetas*, *4*(1), 32-37.
28. Pinjarkar, L., Hete, P. R., Mattada, M., Nejakar, S., Agrawal, P., & Kaur, G. (2024, July). An Examination of Prevalent Online Scams: Phishing Attacks, Banking Frauds, and E-Commerce Deceptions. In *2024 Second, International Conference on Advances in Information Technology (ICAIT)* (Vol. 1, pp. 1-6). IEEE.
29. Ramalingam, D., & Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165-177.
30. Ray, R. L., Abeysingha, N. S., Deegala, D. M. B. M., Gurau, S., & Dissanayake, S. (2025). Review of the effects of the COVID 19 pandemic on the environmental economy and human wellbeing. *Discover Sustainability*, *6*(1), 965.
31. Ryan, J. M. (2021). Timeline of COVID-19. *COVID-19: Global Pandemic, Societal Responses, Ideological Solutions. Routledge*.
32. Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.
33. Singh, N. K., Behera, B., Dash, D. P., Balsalobre-Lorente, D., & Sethi, N. (2025). What determines crime in tropical and sub-tropical countries? Exploring the dynamics of climate change, corruption, and information & communication technology. *Economic Change and Restructuring*, *58*(4), 71.
34. South, S. J., & Messner, S. F. (2000). Crime and demography: Multiple linkages, reciprocal relations. *Annual Review of Sociology*, *26*(1), 83-106.
35. Stenson, K. (2012). The new politics of crime control. In *Crime, risk and justice* (pp. 15-28). Willan.
36. Stummvoll, G. (2012). Governance through norms and standards: The normative force behind design-led crime prevention. *Criminology & Criminal Justice*, *12*(4), 377-396.
37. Taodang, D., & Gundur, R. V. (2023). How frauds in times of crisis target people. *Victims & Offenders*, *18*(5), 889-914.
38. Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400.