


Systematic Review

Cybercrime's Threat to Financial Institutions During COVID-19

Abthal Abdajabar¹, Tarik Idbeaa^{2,3,*} 

¹Department of Information Technology, Faculty of Business & Technology, University of Cyberjaya, Cyberjaya, Malaysia

²Department of Computer Science, Faculty of Science, University of Gharyan, Gharyan, Libya

³Department of Information Technology, University of Tripoli Alahlia, Janzur, Libya

ARTICLE INFO

Corresponding Email. tidbeaa@yahoo.com

Received: 18-03-2024

Accepted: 24-05-2024

Published: 26-06-2024

Keywords. COVID-19, Cybersecurity, Financial institutions, Cyberattacks.

Copyright: © 2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>

Cite this article. Abdajabar A, Idbeaa T. Cybercrime's Threat to Financial Institutions During COVID-19. *Alq J Med App Sci*. 2024;7(Supp2):46-52. <https://doi.org/10.54361/ajmas.2472207>

ABSTRACT

This systematic review investigates the impact of the COVID-19 pandemic on cybersecurity by examining the rise of cyberattacks targeting financial institutions. By analyzing over 60 sources including academic research, government reports, and security company data, the review reveals a nearly two-fold increase in cybercrimes targeting financial institutions during the pandemic compared to pre-pandemic levels. Phishing attacks are identified as the most prevalent form of cybercrime within this context. The review delves further by analyzing the differences between phishing and other cyberattacks during COVID-19. Based on the results and observations presented in this paper, the analysis will contribute to enriching strategies to address the growing threat of cybercrime in the financial sector.

INTRODUCTION

The COVID-19 pandemic drastically altered how we connect and work, with social distancing measures leading to a surge in online activity [2]. This rapid shift forced many workers to adopt new communication tools and online platforms [2]. Increased reliance on the internet, however, comes with inherent risks [3]. Financial institutions, which heavily depend on technology for daily operations, require robust cybersecurity measures to protect against cyberattacks [3]. This paper explores the impact of COVID-19 on cybersecurity from a cybercrime perspective. It examines the rise of various cyberattacks targeting financial institutions worldwide during the pandemic, comparing them to pre-pandemic levels. By analyzing over 60 sources including research papers, government reports, and security company analyses, the paper aims to provide a comprehensive understanding of cybersecurity threats during COVID-19. This includes not only the specific tactics used by attackers but also the evolving knowledge base of both financial institutions and their customers regarding cyber threats and security measures [4].

The COVID-19 pandemic wasn't just a health crisis; it was also accompanied by a surge in cybercrime. This "scam pandemic" saw a rise in various cyberattacks, with phishing scams being the most prevalent [6]. Hackers exploited anxieties and uncertainties around COVID-19 to craft more convincing phishing attempts, attracting significant research attention [7]. This new wave of research focused on analyzing the unique cybersecurity challenges brought on by the pandemic, particularly for financial institutions. This paper builds upon existing research on COVID-19 related cyberattacks in finance, but with a key distinction. While advancements in technology have transformed banking processes in recent years, inherent vulnerabilities remain. Financial institutions rely on external platforms for digital services, exposing them to external risks. Hackers, aware of these vulnerabilities, have become more sophisticated. To counter this evolving threat landscape, banks need to continuously evaluate cyberattacks, adapt their security tactics, and improve both their own and their customers' cybersecurity awareness [4].

The pandemic provided a golden opportunity for financially motivated scammers to launch hacking sprees. These attacks targeted various devices connected to the internet, including desktops, mobile phones, and others. Hackers aimed to steal sensitive information like login credentials, financial data, and more. In some alarming instances, they even used this stolen information to directly withdraw money from victims' accounts. Similar to the surge in bank loan scams, many online purchasing scams thrived during lockdowns, with a focus on stealing personal and financial information. With numerous stores forced to close, cybercriminals capitalized on the situation, leading to a reported 42% increase in fraud cases compared to 2019. Some reports even mentioned SMS alerts from a specific bank, falsely advising customers to reschedule a shipment delivery [8].

Phishing remains a prevalent method for infecting smartphones with malware. Hackers lure victims into clicking on malicious links or opening emails disguised as legitimate sources or companies. During the widespread lockdowns caused by COVID-19, attackers ramped up phishing campaigns, targeting a vast number of people. Phishing tactics often involve fake websites designed to harvest user information. Increased reliance on online tools during the pandemic made many people more susceptible to these phishing attempts. Statistics show that while the total number of phishing emails sent in March 2020 was relatively low (less than 2% of all phishing emails), a significant portion (9,163) specifically capitalized on COVID-19 themes [10].

Ransomware attacks, a form of cyber assault, lock companies out of their own IT infrastructure, including computers, networks, and associated systems. Hackers then demand a ransom payment in exchange for regaining access to their data and systems. In some cases, even if a ransom is paid, attackers may never restore access or may even sell the stolen information to other cybercriminals or make it public. The shift to remote work during the pandemic created an ideal environment for ransomware attacks to escalate.

Malware encompasses a broad category of malicious software designed to harm computers in various ways, such as encrypting data, corrupting hardware, hindering software function, stealing data, or gaining unauthorized access. The peak of the COVID-19 pandemic witnessed a significant rise in malware focused on data collection. Hackers increasingly employed data-harvesting tools like spyware, banking Trojans, information stealers, and Remote Access Trojans (RATs). These tools often use COVID-19 related content as bait to lure victims and infiltrate systems. Once inside, attackers can steal information, initiate fraudulent online money transfers, build botnets (networks of hacked devices), and more.

The global financial system faces an ever-growing threat landscape from cyberattacks. A prominent example occurred in February 2017, where hackers attempted to steal a staggering \$1 billion from the central bank of Bangladesh by exploiting vulnerabilities in SWIFT, the primary electronic messaging system for international banking transactions. While most of the attempted transfer was blocked, hackers still managed to steal \$101 million. This incident served as a wake-up call for the banking industry, highlighting the critical need to address systemic cyber risks that had been previously underestimated. The compression of most cybersecurity crimes in the world is highlighted in Table 1.

Table 1 The Most Cybersecurity Crimes in The World

| Authors | Year | Country | Cybersecurity/ crimes |
|--------------------------|------|----------------|---|
| Cyber security in the EU | 2020 | European Union | Cyber War, Cyber espionage, Cybercrime, Phishing, Online Fraud. |
| Computing, etal., | 2015 | India | Phishing, cyber-attacks, Spam email, Fical fraud |
| Malik and Islam, | 2019 | Pakistan | Cybercrimes, fraud |
| Smikle | 2022 | Jamaica | e-fraud, identity theft, credit card forging, Phishing |
| Butler Bank of England | 2017 | UK | Cybercrimes, extortion, blackmail, and fraud |
| SEC | 2018 | USA | cyber-risk, cybercrimes, Phishing. |

EU and Global Risks: In the European Union, a successful cyberattack on banks could trigger a financial crisis. The European Central Bank warns that cyber incidents could be the catalyst for the next financial meltdown. These attacks could disrupt critical financial systems, impacting everything from central bank operations to everyday banking services [15].

Micro and Macroeconomic Consequences: Cyberattacks can have devastating consequences at both the individual and institutional levels. On a microeconomic scale, attacks can lead to stolen funds, data breaches, and disruptions in financial services. Macroeconomically, cybercrime can damage customer trust, lead to legal and regulatory issues, and potentially destabilize entire financial systems [21].

Global Examples: The problem of cybercrime in finance is not limited to a single region. India, for instance, has seen a surge in cybercrimes targeting banks, resulting in both financial losses and data breaches for victims. Similarly, studies in Pakistan highlight the negative impact of cybercrime on organizational performance within the banking sector [28].

The Caribbean and National Security: Jamaica is another country grappling with cybercrime's impact on its financial sector. Cybersecurity vulnerabilities like phishing and denial-of-service attacks pose a significant threat to the country's financial stability. The Jamaican government recognizes cybersecurity as a national security issue due to the potential consequences for the financial system [28].

UK Financial System Risks: The Bank of England's 2018 Systemic Risk Survey identified cyberattacks as the second-highest source of risk facing the UK financial system [15].

The financial sector faces a significant threat from cyberattacks, prompting regulatory bodies to take action. For example, the Bank of England uses the CBEST test to assess the vulnerability of critical financial institutions, acting as a macroprudential policy in response to the perceived systemic risk [5].

Cybercrime's impact is global, with estimates suggesting annual losses of \$450 billion up to UK Finance. In the United States, the Securities and Exchange Commission (SEC) has published guidelines for listed companies on disclosing cyber risks to investors. Updated in 2018, these guidelines provide a framework for reporting cyberattacks and could potentially address existing data gaps in this area. The International Telecommunication Union (ITU) offers a global perspective on cybersecurity preparedness. Their Global Cybersecurity Index considers factors like legal frameworks, technical capabilities, organizational preparedness, capacity building, and international cooperation [24]. Notably, the index shows that almost every nation is represented, with higher ratings for countries that have been targeted by major cyberattacks, such as those in the Baltic states and Bangladesh [5].

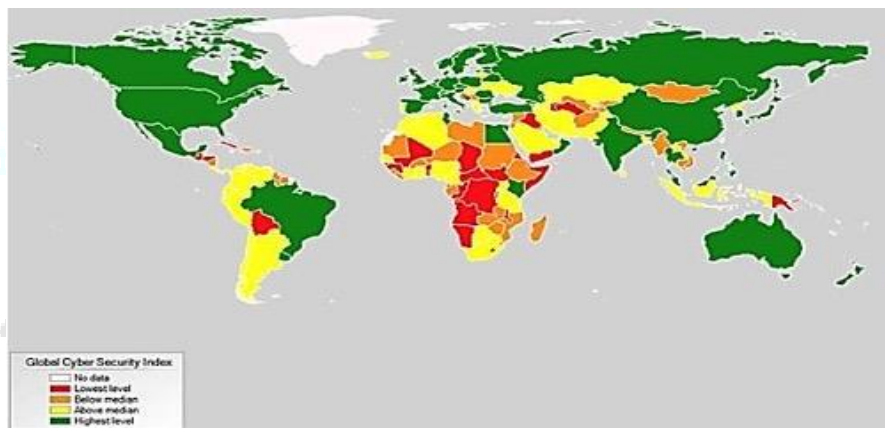


Figure 1. Cybersecurity around the world. Source: ITU (2017).

METHODS

This research utilizes a rapid systematic review methodology to analyze the impact of cybersecurity on financial institutions, particularly in the wake of the COVID-19 pandemic. This approach aims to efficiently summarize existing knowledge on the topic. The first stage involved a comprehensive literature search focused on articles published between 2018 and 2022. We included only English-language, full-text articles with abstracts, restricting the search to published or in-press materials. Review articles were consulted to inform the research direction but excluded from the final analysis. This initial phase established a foundation by defining key terms and exploring common cybercrimes affecting financial institutions.

Following this, the review delved into the impact of COVID-19 on cybersecurity. By summarizing relevant literature published between 2020 and 2022, we aimed to capture the unique challenges posed by the pandemic. Finally, the research differentiates itself by specifically comparing how these cyber threats impact financial institutions, providing focused insights into this critical sector.

Cybersecurity protects our systems, networks, software, and data from unauthorized access and attacks. The field is constantly evolving due to the ever-changing nature of cyber threats. Understanding core concepts like attacks, threats, vulnerabilities, and security measures is crucial for effective information security [16]. The COVID-19 pandemic highlighted our dependence on information technology and the critical need for robust cybersecurity. It also created

fertile ground for a surge in cybercrimes, jeopardizing both personal security and economic stability. Understanding their mechanisms and impact is vital, especially considering the pandemic's disruption of daily routines [17]. Lockdowns across the globe forced people online, increasing reliance on digital services. This period saw a surge in cyber threats targeting the financial sector [21]. Higher education institutions also embraced online learning platforms like WebEx, Zoom, and Google Classroom to facilitate remote learning [22]. Communication tools like social media platforms further connected students, educators, and professionals during this shift. Zoom, for instance, experienced a meteoric rise as video conferencing became essential for remote work. However, its rapid growth also exposed vulnerabilities. With a 355% revenue rise between Q2 2019 and Q2 2020, Zoom faced security incidents like the leak of over 500,000 user credentials on a dark web forum. These compromised credentials were likely used for credential stuffing attacks, highlighting the importance of robust security measures [1]. The COVID-19 pandemic triggered a surge in research on its multifaceted impact. This includes a wave of studies focusing on cybercrime, cyberattacks, and the unique cybersecurity challenges that emerged during the pandemic. While some prior research existed, our work builds upon these earlier efforts by offering a more nuanced analysis. To illustrate this distinction, we briefly review existing studies and highlight the key differences from our current research. A table summarizing relevant past surveys accompanies this review [19].

RESULT AND DISCUSSION

Work Survey Comparison

The COVID-19 pandemic created a prime opportunity for cybercriminals to target financial institutions. The average cost of cybercrime in financial services is a staggering \$5.85 million, making it one of the most expensive business crimes [11-13]. This vulnerability was exacerbated by the shift to remote work, as many employees lacked secure home networks. Common attack methods included distributed denial-of-service (DDoS) attacks, phishing emails, and malware intrusions aimed at stealing bank credentials and accessing ATM transactions [1]. Increased reliance on online banking by customers further amplified these risks [8]. Ransomware attacks also surged, with financial institutions becoming a prime target due to their access to large sums of money [7]. The potential for disrupting critical banking services and the perceived willingness of victims to pay ransoms made these institutions particularly attractive to attackers. Reports suggest that over \$5.2 billion in Bitcoin (BTC) transactions may be linked to ransomware payments by financial institutions [12]. Recent examples highlight the evolving tactics of cybercriminals. In April 2022, a "Fake Calls" banking trojan emerged, impersonating legitimate Korean banks through mobile app imitations and stealing victim information [17]. Similarly, a data breach at the Indian loan app Cashman in April 2022 exposed sensitive customer data due to an unsecured cloud storage bucket [18]. In March 2022, a cyberattack on the South African credit bureau TransUnion SA compromised the personal information of millions of customers [13]. These incidents illustrate the continuous threats faced by financial institutions and the evolving tactics used by cybercriminals.

Table 2. The Summary of The Existing Surveys.

| Study | Year | Cybersecurity relates | Relate/not Relate to Covid |
|--------------------|------|--|----------------------------|
| Hijji & Alam | 2021 | Social engineering-based cyber-attacks | During Covid |
| Lallie et al. | 2021 | Cyber-crime perspective | During Covid |
| Valiyaveedu et al. | 2021 | Focuses on Web phishing attacks | Not relate |
| He et al | 2021 | Highlighted the increase in cyberattacks (e.g., phishing campaigns and ransomware attacks) | During Covid |
| Basit et al. | 2021 | Applications of artificial intelligence to detect phishing attacks | Not relate |
| Salloum et al. | 2021 | Review natural language processing techniques for detecting phishing emails | Not relate |
| Alkhalil et al. | 2021 | Describes the complete process of a phishing attack. | Not relate |
| Hakak et a | 2020 | Malicious cyber activities, focus on Phising | During Covid |
| Korkmaz et al. | 2020 | Analyzes machine learning-based phishing detection systems. | Not relate |
| Choudhary et al. | 2022 | Classified cyber-crimes committed during the pandemic across the world. | During Covid |
| Alawida, M et al. | 2022 | Covered the main types of cyber-attacks such as mobile app, Phishing, email attacks etc. | During Covid |

The COVID-19 pandemic significantly heightened the risk of cybercrime for financial institutions, posing a threat to global economic stability. Lockdowns and increased reliance on online services created fertile ground for cybercriminals to exploit vulnerabilities.

Table 3 details specific cybercrimes that occurred during the peak of the pandemic. However, some concerning examples highlight the evolving tactics used by attackers. In late 2021, researchers identified a new Android banking Trojan called SharkBot. This malware can gain administrative privileges on a device, steal keystrokes, access mobile banking apps, and even transfer funds. Similarly, a surge in phishing attacks targeting Chase Bank in 2021 utilized sophisticated phishing kits designed to gather extensive user information. Data breaches also posed a significant threat. In January 2021, the Reserve Bank of New Zealand experienced unauthorized access to its data through a third-party file-sharing service. Additionally, malicious Android applications targeting Brazilian banking systems emerged in September 2021, with some even containing novel features designed to steal funds through the Pix payment system [25-27].

Botnet attacks targeting banking applications were also documented. In July 2021, researchers identified a botnet campaign leveraging the Oscorp Android malware to steal user passwords from European banking applications [24]. This malware's ability to access confidential data and exfiltrate it back to a remote server further heightened the risk. Large-scale credit card breaches were also reported during the pandemic. In March 2020, over 200,000 credit card numbers from Southeast Asian banks were stolen and posted online. Ransomware attacks also targeted financial institutions in the region, with a notable attack on AXA, a French insurance company, in May 2021. These examples illustrate the evolving landscape of cyber threats faced by financial institutions and the critical need for robust cybersecurity measures [19].

Table 3: Different Cyber Security Crimes Incident in Financial Institution during The Pandemic.

| Event | Date | Target | Incident |
|--|---------------------|---|-----------------------------------|
| Fake calls banking Trojan | April 11, 2022 | South Korea | Cyberattacks, Data breach |
| CashMama data breach (Sharma, B.) | April 06, 2022 | India | Data breach |
| Aon ransomware attack. Jenkinson, A. (2022). | February 25, 2022 | United States | Ransomware |
| OCBC phishing scam Tham, D. (2022) | December 23, 2021 | Singapore | Phishing |
| Banks targeted by SharkBot banking Trojan Dorotik, L. (2021). | October 2021 | UK and Italy | Malware |
| Chase Bank phishing attacks (Rane, S et al, 2022) | May to August, 2021 | United States | Phishing |
| Reserve Bank of New Zealand Data Breach Davtyan, (2022). | January 10, 2021 | New Zealand | Cyber attacks, Data breach |
| PixStealer targets Brazilian banking applications. Wernik & Melnykov, 2021 | September 29, 2021 | Brazil | malware cyber attack, data breach |
| Oscorp malware returns as an Android botnet. (Lakshmanan, R. (2021) | July 27, 2021 | Spain, Poland, Germany, Turkey, United States, Japan, Italy, Australia, France and India. | malware cyber attacks |
| Southeast Asian Banks Credit Card Breach (Sukumaran, T. (2020) | March 06, 2020 | Malaysia, Singapore, Philippines, Vietnam, Indonesia and Thailand | Cyber Attack, Data breach |
| AXA hit by ransomware Kim & Lee (2022) | May 16, 2021 | Thailand, Malaysia, Hong Kong and the Philippines | Ransomware |

CONCLUSION

This systematic review examines the impact of COVID-19 on cybersecurity through the lens of cybercrime. Its focus is on the rise of cyberattacks targeting financial institutions during the pandemic, compared to pre-pandemic levels. The review analyzes existing research and reports on cybersecurity, synthesizes findings from recent studies, and compares cyberattacks before and after COVID-19 to assess their impact. Our analysis reveals a significant increase – nearly doubling – in the number of cybercrimes targeting financial institutions during the pandemic. Furthermore, the review

identifies phishing attacks as the most prevalent form of cybercrime within this context. Analyzing the distinct characteristics of phishing attacks within this context, compared to other cyberattacks, provides valuable insights for developing targeted security strategies. These findings underscore the urgent need for robust cybersecurity measures within the financial sector. By understanding the specific tactics favored by cybercriminals during the pandemic, such as phishing, financial institutions can implement more effective prevention strategies. Additionally, fostering increased awareness among employees and customers regarding these prevalent cyber threats can further bolster overall cybersecurity posture.

This systematic review contributes to the ongoing dialogue on cybersecurity in the financial sector, particularly in the face of evolving threats and vulnerabilities. The significant increase in cyberattacks identified by this review necessitates ongoing research and development of advanced security measures to protect financial institutions and their customers.

Conflict of interest. Nil

REFERENCES

1. Alawida M, Omolara A, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: a survey. *Journal of King Saud University-Computer and Information Sciences*. 2022;34(12):8176-8206.
2. World Health Organization. Coronavirus disease (COVID-19) pandemic situation [Internet]. 2020 [cited 2024 May 27]. Available from: <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>
3. Khweiled AA, Al-Hadidi M, Al-Naeem TM. The impact of COVID-19 on cybersecurity threats and risk management practices in organizations. *Int J Inf Secur Priv*. 2021;15(3):249-67.
4. Alaawi AI, Bassam SA. Implementing computational intelligence techniques for security systems: A review of applications and challenges. *J King Saud Univ Comput Sci*. 2020;32(7):1633-42.
5. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment [Internet]. International Monetary Fund; 2018 [cited 2024 May 27].
6. Lallie HC, Belo IE, Rodrigo MSE. Research synthesis of cybercrime laws and COVID-19 in Indonesia: Lessons for developed and developing countries. *Secur J*. 2021;10(1):1289-303.
7. He Q, Zhao L, Zhang J, Tang Y, Zhou Y. Phishing attacks exploiting COVID-19 pandemic. In: 2021 International Conference on Big Data and Smart Computing (BigDataSmart). IEEE; 2021:1-5.
8. Calliess C, Baumgarten A. Cybersecurity in the EU the example of the financial sector: a legal perspective. *Ger Law J*. 2020;21(6):1149-79.
9. Computing C. International Journal of Advanced Research in Computer Science and Software Engineering [Internet]. 2015 [cited 2024 May 27];5(6). Available from: [invalid URL removed]
10. Davtyan A. Cyber Vulnerability of Japanese Banking/Financial System. The EURASEANs: journal on global socio-economic dynamics. 2022;1(32):53-9.
11. Dorotík L. Analýza datových sad umožňujících detekci mobilního malwaru [Analysis of datasets enabling the detection of mobile malware] [Internet]. 2021 [cited 2024 May 27]. In Slovak.
12. Gobeo A, Fowler C, Buchanan WJ. GDPR and Cyber Security for Business Information Systems. CRC Press; 2022.
13. Jenkinson A. Ransomware and Cybercrime. CRC Press; 2022.
14. Kamiya S, Kang JK, Kim J, Milidonis A, Stulz RM. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *J Financ Econ*. 2021;139:719-49.
15. Bank of England. Systemic Risk Survey results | 2018 H2 [PDF] [Internet]. 2023 [cited 2024 May 27]. Available from: <https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h1>
16. Stallings W, Brown L. Computer security concepts and principles. Pearson Education Limited; 2016:10-17.
17. Kim J, Kim J, Wi S, Kim Y, Son S. HearMeOut: detecting voice phishing activities in Android. In: Proceedings of the 20th Annual International Conference on Mobile Systems, Applications, and Services. 2022:422-35.
18. Kopp E, Kaffenberger L, Wilson C. Cyber risk, market failures, and financial stability [Internet]. International Monetary Fund; 2017 [cited 2024 May 27].
19. Kost E. Biggest Cyber Threats for Financial Services in 2022 | UpGuard. Third-Party Risk and Attack Surface Management Software | UpGuard [Internet]. 2022 [cited 2024 May 27]. Available from: <https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services>
20. Lakshmanan R. Ubel is the new Oscorp - android credential stealing malware active in the wild [Internet]. The Hacker News. 2021 [cited 2024 May 27]. Available from: <https://thehackernews.com/2021/07/ubel-is-new-oscorp-android-credential.html>
21. Bak A. The economic impact of cybercrime. *Security Journal*. 2017;6(3):437-51.

22. Malik MS, Islam U. Cybercrime: an emerging threat to the banking sector of Pakistan. Journal of Financial Crime. 2019;26(2):325-43.
23. Mallet V, Chilkoti A. How cyber criminals targeted almost \$1 bn in Bangladesh bank heist. Financial Times. 2016;08:18.
24. Prenio J, Yong J, Kleijmeer R. Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions. FSI Insights. 2019;(21).
25. Rane S, Devi G, Wagh S. Cyber Threats: Fears for Industry. In: Cyber Security Threats and Challenges Facing Human Life. Chapman and Hall/CRC; 2021:43-54.
26. Silver-Greenberg J, Goldstein M, Perlroth N. Jpmorgan chase hack affects 76 million households. New York Times. 2014; Oct 02(Section A):1.
27. Smikle L. The impact of cybersecurity on the financial sector in Jamaica. Journal of Financial Crime. 2022;29(1):217-34.

تهديد الجرائم الإلكترونية للمؤسسات المالية خلال أزمة كوفيد-19

ابتهاال عبد الجبار^{1*}، طارق الضبيغ^{2,3}

¹قسم تقنية المعلومات، كلية الأعمال والتقنية، جامعة سيرجايا، سيرجايا، ماليزيا

²قسم علوم الحاسب، كلية العلوم، جامعة غريان، غريان، ليبيا

³قسم تقنية المعلومات، جامعة طرابلس الأهلية، جنزور، ليبيا

المستخلص

تبحث هذه المراجعة المنهجية في تأثير جائحة كوفيد-19 على الأمن السيبراني من خلال دراسة صعود الهجمات السيبرانية التي تستهدف المؤسسات المالية. ومن خلال تحليل أكثر من 60 مصدرًا بما في ذلك الأبحاث الأكاديمية والتقارير الحكومية وبيانات شركات الأمن، تكشف المراجعة عن زيادة تقارب الضعف في الجرائم الإلكترونية التي تستهدف المؤسسات المالية أثناء الوباء مقارنة بمستويات ما قبل الوباء. وتعتبر هجمات التصيد الاحتيالي أكثر أشكال الجرائم الإلكترونية انتشارًا في هذا السياق. تتعمق المراجعة بشكل أكبر من خلال تحليل الاختلافات بين التصيد الاحتيالي والهجمات الإلكترونية الأخرى أثناء تفشي فيروس كورونا (COVID-19) وبناء على النتائج والملاحظات المقدمة في هذه الورقة، فإن التحليل سيسهم في إثراء استراتيجيات التصدي للتهديد المتزايد للجرائم الإلكترونية في القطاع المالي.

الكلمات الدالة: كوفيد-19، الأمن السيبراني، المؤسسات المالية، الهجمات السيبراني.