Available online at www.scientiaresearchlibrary.com

Scientia Research Library

ISSN 2348-0424
USA CODEN: JETRB4

Journal of Engineering And Technology Research,
2020, 8 (2):1-7

(http://www.scientiaresearchlibrary.com/arhcive.php)

Technological Advancement Challenges: Addressing the Problem of Hacking as the Common Form of Cybercrime

John Roldan Pacsoderon Torres

Fernandez College of Arts and Technology Baliuag, Bulacan, Philippines

ABSTRACT

This literature review explores the problem of hacking, a significant form of cybercrime in the digital age. The review examines the types of hacking, including websites, networks, and email. It also discusses the causes of hacking, including financial gain, political motivations, and notoriety seeking. The review examines the impacts of hacking, including the theft of sensitive information, disruption of critical infrastructure, and psychological impacts on victims. Finally, the review discusses potential countermeasures to mitigate the risks of hacking, including strong passwords and encryption, security software, and education and training programs. This literature review highlights the need for continued research and development of countermeasures to prevent hackers from carrying out their attacks.

Keywords: hacking, cybercrime.

INTRODUCTION

The rise of technology and the increasing reliance on the internet have led to the emergence of a new form of crime known as cybercrime. Cybercrime refers to criminal activities that are committed using digital devices, computer networks, and the internet. It includes a range of activities such as hacking, cyberstalking, identity theft, online scams, cyberbullying, and cyber espionage. The impact of cybercrime can be significant, resulting in financial losses, damage to reputation, and even physical harm. This paper aims to explore the problem of cybercrime, including its types, causes, impacts, and countermeasures [1]–[3].

Cybercrime has become a significant issue in the digital age, with numerous types of crimes and an ever-increasing number of incidents. One form of cybercrime that has garnered significant attention is hacking. Hacking involves gaining unauthorized access to digital systems or networks, with various motives behind such actions. The impacts of hacking can be severe, leading to the theft of sensitive information, disruption of critical infrastructure, and psychological impacts on victims. Therefore, it is essential to explore the problem of hacking in depth, examining the types and causes of hacking, as well as its impacts and potential countermeasures [2]–[6]. This paper aims to provide a comprehensive analysis of the problem of hacking, delving into the different types of hacking, including website hacking, network hacking, and email hacking. It also examines the causes of hacking, including financial gain, political motivations, and notoriety seeking. Furthermore, this paper analyzes the impacts of hacking on individuals, businesses, and society as a whole. Finally, the paper explores potential countermeasures to mitigate the risks of hacking, including strong passwords and encryption, security software, and education and training programs. By providing a thorough investigation of the problem of hacking, this paper aims to contribute to the development of effective countermeasures to prevent hackers from carrying out their attacks and protect digital systems and networks from unauthorized access.

One study conducted a qualitative analysis of 32 convicted hackers to identify the motivations and characteristics of hackers. The study found that hackers were often motivated by a combination of financial gain, curiosity, and notoriety-seeking, and that they tended to exhibit traits such as high intelligence, impulsivity, and a lack of empathy. Another study analyzed the hacking of the 2016 United States presidential election and found evidence of both state-sponsored and non-state-sponsored hacking attempts. The study also identified the use of social media manipulation and fake news dissemination as techniques used by hackers to influence public opinion. Another explored the use of machine learning algorithms for detecting and preventing hacking attacks. The study found that machine learning techniques were effective in identifying anomalies and patterns in network traffic that could indicate a hacking attempt. A similar study examined the use of forensic techniques for investigating hacking incidents. The study found that digital forensics tools and techniques could be used to identify the source of a hacking attack and the methods used by the attacker [4], [5], [7]–[9]. In summary, these studies demonstrate the multifaceted nature of hacking and the various approaches used to prevent, detect, and investigate hacking incidents. By analyzing the motivations, characteristics, and techniques used by hackers, researchers and practitioners can develop effective countermeasures to mitigate the risks of hacking in today's digital landscape.

Methodology

The methodology for this study is a short literature review. Various academic and professional sources, including books, journal articles, and online resources, were used to collect information on the problem of hacking in cybercrime. The search terms used included "hacking," "cybercrime," "types of hacking," "causes of hacking," "impacts of hacking," and "countermeasures for hacking." The collected information was then analyzed and synthesized to create a comprehensive understanding of the problem of hacking in cybercrime. The literature review methodology allowed for the exploration of a wide range of perspectives and expert opinions on the topic, providing a well-rounded analysis of the problem of hacking.

RESULT AND DISCUSSION

Cybercrime can take many forms, and cybercriminals use a range of techniques to target their victims. Hacking refers to the unauthorized access of computer systems, networks, and devices. Hackers use various techniques such as phishing, malware, and social engineering to gain access to sensitive information. Hacking has become a significant problem in the digital age. The number of incidents of hacking has increased in recent years, and the impact of these incidents can be significant. There are several types of hacking, including website hacking, network hacking, and email hacking. Website hacking involves gaining unauthorized access to websites and web applications. Hackers can exploit vulnerabilities in website software or use brute force attacks to gain access to restricted areas of websites. Network hacking involves gaining unauthorized access to computer networks. Hackers can exploit vulnerabilities in network security protocols or use social engineering techniques to gain access to sensitive information. Email hacking involves gaining unauthorized access to email accounts. Hackers can use phishing attacks or other social engineering techniques to gain access to email accounts, which can then be used to send spam or carry out other nefarious activities [10], [11].

The causes of hacking are varied. Some hackers may be motivated by financial gain, using their access to digital systems to steal sensitive information or carry out other types of fraud. Other hackers may be motivated by political or ideological reasons, using their access to digital systems to gather intelligence or carry out cyberattacks against their perceived enemies. Still, others may be motivated by a desire for recognition or notoriety, using their hacking skills to gain attention or notoriety within the hacker community [11]–[13].

The impacts of hacking can be significant. Hacking can lead to the theft of sensitive information, including personal data and financial information. Hacking can also lead to the disruption of critical infrastructure, such as power grids and transportation systems, leading to significant economic and social consequences. Hacking can also have psychological impacts, with victims experiencing anxiety, fear, and other emotional problems [2], [14]–[17].

To mitigate the risks of hacking, various countermeasures can be taken. Strong passwords and encryption can be used to prevent unauthorized access to digital systems. Security software such as antivirus software and firewalls can be used to protect digital devices and networks. Education and training programs can help individuals and organizations understand the risks of hacking and how to prevent it. It is essential to continue to explore the problem of hacking and develop new countermeasures to prevent hackers from carrying out their attacks.

Causes of Cybercrime

There are several factors that contribute to the rise of cybercrime. The anonymity of the internet makes it easy for cybercriminals to launch attacks without fear of being caught. This anonymity also makes it difficult for law enforcement agencies to identify and prosecute cybercriminals. The increasing availability and accessibility of digital devices and networks have made it easy for cybercriminals to launch attacks. Cybercriminals can use a range of devices such as smartphones, laptops, and tablets to carry out their attacks. The increasing reliance on technology for communication, commerce, and other activities has made individuals and organizations more vulnerable to cybercrime. Cybercriminals take advantage of this reliance on technology to launch attacks. Cybercrime can be a lucrative business, with cybercriminals making significant amounts of money from their criminal activities. This potential financial reward is a significant factor that drives cybercriminals to carry out their attacks [18]–[20].

Impacts of Cybercrime:

The impacts of cybercrime can be significant and far-reaching. Individuals and organizations can suffer significant financial losses as a result of cybercrime. Cybercriminals can steal money, commit fraud, and extort victims for money. Cybercrime can damage an individual's or organization's reputation. For example, a data breach can result in the loss of trust from customers, which can be difficult to regain. Cybercrime can cause emotional distress to victims. Cyberbullying, cyberstalking, and other forms of cybercrime can cause anxiety, depression, and other emotional problems for victims. In some cases, cybercrime can result in physical harm. For example, cybercriminals can launch attacks on critical infrastructure such as power grids, resulting in power outages and other physical harm [21]–[23].

Countermeasures

To mitigate the risks of cybercrime, various countermeasures can be taken. Individuals and organizations should use strong passwords that are difficult to guess. Passwords should be changed regularly to prevent unauthorized access. Sensitive information should be encrypted to prevent unauthorized access. Encryption scrambles information, making it unreadable to anyone who does not have the encryption key. Individuals and organizations should use security software such as antivirus software and firewalls to protect their digital devices and networks. Education and training programs can help individuals and organizations understand the risks of cybercrime and how to prevent it. Education and training programs can teach individuals how to recognize and respond to cyber threats [21], [24]–[30].

Hacking has become a significant threat to individuals, organizations, and even governments in today's digital world. Hackers employ a wide range of techniques to gain unauthorized access to computer systems, networks, and data, causing data breaches, financial losses, and reputational damage. To address this issue, a comprehensive solution to hacking is necessary, which involves a combination of technical, legal, and educational measures.

One of the technical measures to prevent hacking is the use of strong passwords and encryption techniques. Passwords should be complex and not easy to guess, and they should be changed periodically. Encryption techniques can protect sensitive data from being intercepted and accessed by unauthorized persons. Additionally, firewalls and intrusion detection systems can be implemented to monitor network traffic and identify any suspicious activities.

Another essential component of a comprehensive solution to hacking is the legal framework that governs cybersecurity. Laws and regulations should be put in place to criminalize hacking activities and impose strict penalties on offenders. Cybersecurity regulations should also be enforced to ensure that organizations and individuals take the necessary measures to protect their systems and data. Government agencies should also collaborate with the private sector to share intelligence on emerging threats and develop strategies to mitigate them.

Education and awareness programs can also be effective in preventing hacking. Individuals and organizations should be educated on the best practices for securing their systems and data, such as avoiding phishing scams and keeping software up to date. Additionally, cybersecurity training should be incorporated into school curriculums to equip students with the knowledge and skills necessary to protect themselves in the digital world.

A comprehensive solution to hacking also requires collaboration among stakeholders. Governments, organizations, and individuals must work together to share information, resources, and best practices. Collaboration can help identify emerging threats and vulnerabilities and develop effective strategies to mitigate them. Public-private partnerships can also be formed to leverage the strengths of both sectors in addressing the challenges of cybersecurity.

Another critical aspect of a comprehensive solution to hacking is the development of a robust incident response plan. Organizations should have a well-defined plan in place to respond quickly and effectively to any security incidents. Incident response plans should include procedures for identifying and containing the breach, assessing the damage, and restoring systems and data. Regular testing of the incident response plan can help identify weaknesses and ensure that the plan is up to date and effective.

CONCLUSION

Cybercrime is a growing problem that affects individuals and organizations worldwide. Cybercriminals use a range of techniques to target their victims, and the impact of cybercrime can be significant. There are several causes of cybercrime, including the anonymity of the internet, ease of access to digital devices and networks, increasing reliance on technology, and potential financial rewards. To mitigate the risks of cybercrime, various countermeasures can be taken, including strong passwords, encryption, security software, and education and training. It is essential to continue to explore the problem of cybercrime and develop new countermeasures to prevent cybercriminals from carrying out their attacks. In conclusion, a comprehensive solution to hacking involves a combination of technical, legal, and educational measures, as well as collaboration among stakeholders. The technical measures include the use of strong passwords, encryption, firewalls, and intrusion detection systems. The legal framework should include criminalizing hacking activities and enforcing cybersecurity regulations. Education and awareness programs can equip individuals and organizations with the knowledge and skills necessary to protect themselves in the digital world. Collaboration among stakeholders can help identify emerging threats and vulnerabilities and develop effective strategies to mitigate them. Finally, a robust incident response plan is critical to responding quickly and effectively to any security incidents. A comprehensive approach to hacking is necessary to address this critical threat to the digital world.

REFERENCE

[1] X. Jin, B. W. Wah, X. Cheng, and Y. Wang, "Significance and Challenges of Big Data Research," Big Data Research, vol. 2, no. 2, pp. 59–64, Jun. **2015**, doi: 10.1016/J.BDR.2015.01.006.

[2] T. J. Holt, "Computer hacking and the hacker subculture," The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp. 725–742, Jan. **2020**, doi: 10.1007/978-3-319-78440-3_31/COVER.

[3] R. J. González, "Hacking the citizenry?: Personality profiling, 'big data' and the election of Donald Trump," *Anthropol Today*, vol. 33, no. 3, pp. 9–12, Jun. **2017**, doi: 10.1111/1467-8322.12348.

[4] J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," *EURASIP J Adv Signal Process*, vol. **2016**, no. 1, pp. 1–16, Dec. 2016, doi: 10.1186/S13634-016-0355-X/FIGURES/5.

[5] D. Décary-Hétu, C. Morselli, and S. Leman-Langlois, "Welcome to the Scene," *http://dx.doi.org/10.1177/0022427811420876*, vol. 49, no. 3, pp. 359–382, Oct. **2011**, doi: 10.1177/0022427811420876.

[6] N. Kshetri, "Positive externality, increasing returns, and the rise in cybercrimes," *Commun ACM*, vol. 52, no. 12, pp. 141–144, Dec. **2009**, doi: 10.1145/1610252.1610288.

[7] N. Kshetri, "Pattern of global cyber war and crime: A conceptual framework," *Journal of International Management*, vol. 11, no. 4, pp. 541–562, Dec. **2005**, doi: 10.1016/J.INTMAN.2005.09.009.

[8] L. L. G. Tummers, V. Bekkers, E. Vink, and M. Musheno, "Coping During Public Service

Delivery: A Conceptualization and Systematic Review of the Literature," *Journal of Public Administration Research and Theory*, vol. 25, no. 4, pp. 1099–1126, Oct. **2015**, doi: 10.1093/JOPART/MUU056.

[9] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J Big Data*, vol. 7, no. 1, pp. 1–29, Dec. **2020**, doi: 10.1186/S40537-020-00318-5/FIGURES/3.

[10] K. Pavlik, "Cybercrime, Hacking, And Legislation," *Journal of Cybersecurity Research (JCR)*, vol. 2, no. 1, pp. 13–16, May **2017**, doi: 10.19030/JCR.V2I1.9966.

[11] J. Kennedy, T. Holt, and B. Cheng, "Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking," *https://doi.org/10.1080/0735648X.2019.1692425*, vol. 42, no. 5, pp. 632–645, Oct. **2019**, doi: 10.1080/0735648X.2019.1692425.

[12] A. M. Bossler and G. W. Burruss, "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-61350-323-2.ch707*, pp. 1499–1527, Jan. 1AD, doi: 10.4018/978-1-61350-323-2.CH707.

[13] T.J.Holt,"Examining the Forces Shaping Cybercrime Markets Online," *http://dx.doi.org/10.1177/0894439312452998*, vol. 31, no. 2, pp. 165–177, Sep. **2012**, doi: 10.1177/0894439312452998.

[14] C. D. Marcum, G. E. Higgins, M. L. Ricketts, and S. E. Wolfe, "Hacking in High School: Cybercrime Perpetration by Juveniles," *http://dx.doi.org/10.1080/01639625.2013.867721*, vol. 35, no. 7, pp. 581–591, 2014, doi: 10.1080/01639625.2013.867721.

[15] I. Gandhi, "ETHICAL HACKING & SECURITY AGAINST CYBER CRIME," **2016**, doi: 10.26634/JIT.5.1.4796.

[16] N. B. Sukhai, "Hacking and cybercrime," *2004 Information Security Curriculum Development Conference, InfoSecCD **2004***, pp. 128–132, Oct. 2004, doi: 10.1145/1059524.1059553.

[17] S. G. A. van de Weijer, R. Leukfeldt, and W. Bernasco, "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking," *https://doi.org/10.1177/1477370818773610*, vol. 16, no. 4, pp. 486–508, May **2018**, doi: 10.1177/1477370818773610.

[18] T. Cymru, "Cybercrime: An Epidemic," *Queue*, vol. 4, no. 9, pp. 24–28, Nov. **2006**, doi: 10.1145/1180176.1180190.

[19] S. Ibrahim, "Causes of socioeconomic cybercrime in Nigeria," *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016*, Nov. **2016**, doi: 10.1109/ICCCF.2016.7740439.

[20] L.Pasculli, "The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory," *Journal of Ethics and Legal Technologies*, vol. 2, no. 1, **2020**, doi: 10.14658/pupj-jelt-2020-1-3.

[21] Y. S. Rao, "Cyber-Crimes and their Impacts: A Review," vol. 2, pp. 202–209, Accessed: Mar. 05, **2020**. [Online]. Available: www.ijera.com

[22] N. Setiawan *et al.*, "The use of audiovisual learning media in Islamic religious education

subjects at SMPIT Al-Fityan Medan View project IMPACT OF CYBERCRIME IN E-BUSINESS AND TRUST,” *International Journal of Civil Engineering and Technology (IJCIET*, vol. 9, no. 7, pp. 652–656, 2018, Accessed: Mar. 05, **2020**. [Online]. Available: http://www.iaeme.com/IJCIET/index.asp652http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=7http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=7

[23] C. H. Gañán, M. Ciere, and M. van Eeten, “Beyond the pretty penny: The Economic Impact of Cybercrime,” *ACM International Conference Proceeding Series*, pp. 35–45, Oct. **2017**, doi: 10.1145/3171533.3171535.

[24] G. Cascavilla, D. A. Tamburri, and W. J. van den Heuvel, “Cybercrime threat intelligence: A systematic multi-vocal literature review,” *Comput Secur*, vol. 105, p. 102258, Jun. **2021**, doi: 10.1016/J.COSE.2021.102258.

[25] B. Akhgar and B. Brewster, “Combatting cybercrime and cyberterrorism : challenges, trends and priorities,” p. 321.

[26] B. Akhgar and B. Brewster, “Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities,” **2016**, doi: 10.1007/978-3-319-38930-1.

[27] “COMBATTING CYBERCRIME AND CYBERTERRORISM : challenges, trends and priorities.,” **2018**.

[28] J. Armin, B. Thompson, and P. Kijewski, “Cybercrime economic costs: No measure no solution,” *Advanced Sciences and Technologies for Security Applications*, pp. 135–155, 2016, doi: 10.1007/978-3-319-38930-1_8/COVER.

[29]“The Council of Europe’s Convention on Cybercrime on JSTOR.” https://www.jstor.org/stable/24120528 (accessed Mar. 05, **2020**).

[30] T. Maung Maung and M. Mie Su Thwin, “Proposed Effective Solution for Cybercrime Investigation in Myanmar”, doi: 10.9790/1813-0601030107.