engineering proceedings

MDPI

Proceeding Paper

Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime †

Gagandeep Kaur [1,*], Utkarsha Bonde [1], Kunjal Lalit Pise [1], Shruti Yewale [1], Poorva Agrawal [1], Purushottam Shobhane [1], Shruti Maheshwari [2], Latika Pinjarkar [1] and Rupali Gangarde [2]

[1] Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune 440008, India; utkarsha.bonde.btech2023@sitnagpur.siu.edu.in (U.B.); kunjal.pise.btech2023@sitnagpur.siu.edu.in (K.L.P.); shruti.yewale.btech2023@sitnagpur.siu.edu.in (S.Y.); poorva.agrawal@sitnagpur.siu.edu.in (P.A.); purushottam.shobhane@sitnagpur.siu.edu.in (P.S.); latika.pinjarkar@sitnagpur.siu.edu.in (L.P.)

[2] Symbiosis Institute of Technology, Pune, Symbiosis International (Deemed University), Pune 412115, India; shruti.maheshwari@sitpune.edu.in (S.M.); rupali.gangarde@sitpune.edu.in (R.G.)

* Correspondence: gagandeep.kaur@sitnagpur.siu.edu.in

† Presented at the 2nd Computing Congress 2023, Chennai, India, 28–29 December 2023.

Abstract: There are very renowned social media platforms like Instagram, Twitter, Facebook, etc., with each of which being used by different shareholders across the world to communicate with each other. Social media is a pool of online communication platforms that are based on community input, content sharing, and collaborations. The way we communicate, share information, and connect with other people has been revolutionized by social media. This has led to a series of benefits but also posed many challenges, especially in cybersecurity. This paper investigates the varied influences of social media, examining both its good and negative consequences across a variety of industries. It focuses specifically on the cybersecurity concerns posed by the growing usage of social media, shedding light on the vulnerabilities encountered by individuals and organizations. This investigation includes a study of common cybercrimes like phishing, social engineering, burglary via social networking, virus attacks, cyberstalking, identity theft, and cybercasing. This study emphasizes the importance of a complete and targeted cybersecurity approach that includes preventive measures such as privacy enhancements, user training, sophisticated email filtering, robust authentication, and encryption technologies. Individuals and organizations can traverse the evolving social media ecosystem with greater cyber resilience by addressing these challenges and using proactive tactics.

Keywords: social media; cybercrime; burglary; phishing; cyberstalking; cybercrime prevention

Citation: Kaur, G.; Bonde, U.; Pise, K.L.; Yewale, S.; Agrawal, P.; Shobhane, P.; Maheshwari, S.; Pinjarkar, L.; Gangarde, R. Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Eng. Proc.* **2024**, *62*, 6. https://doi.org/10.3390/engproc2024062006

Academic Editors: Geetha Ganesan, Xiaochun Cheng and Valentina Emilia Balas

Published: 1 March 2024

1. Introduction

Social media is the most widely used platform and it is where most of the popular online activities around the world occur. There is a huge craze for social media among the young generation. Day by day, the usage of electrical gadgets has increased rapidly; not only the current generation but also the upcoming generation will be dependent on social media. Due to high demands, social media is becoming more diverse. Social media has played a very important role in education and learning [1].

Social media is used for connecting and networking with people around the globe through Facebook, LinkedIn, Twitter, Instagram, etc. Networking involves professional as well as personal connections via different social media platforms [2] through the sharing of content, stories, photos, video messages, etc. A crucial component of the innovation process is the use of social media to form new perspectives on established innovations [3]. Figure 1 explains the role of social media.

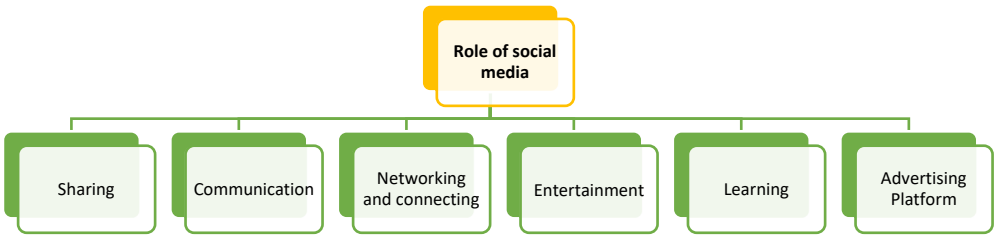

Figure 1. Role of social media.

Social media is used for various purposes in professional fields like providing and acquiring jobs, online meetings, and affiliate marketing [4]. Social media is used for promoting various things like product advertisements, movies, songs, music videos, online shopping brands, and services through various online websites. Additionally, marketers can rely on positive e-WOM from current customers to spread their brand's image [4]. From the inception of the Internet, there has been much discussion about its impact on politics [5].

Social media has its own positive and negative sides. Social media is beneficial in various aspects like connecting to different people, sharing information, spreading awareness, and for entertainment purposes. When we look through an emotional point of view, we find happiness using social media platforms by watching movies and listening to music, and people love watching and making content on social media platforms [6]. Social media hurts people's lives: it affects their mental wellbeing, and people compare their lives with others and start blaming themselves for various things—leading to depression, loneliness, self-harm, and even suicidal thoughts [7]. Today's generation is becoming widely addicted to social media. One of the biggest disadvantages of social media is that it places people's personal information at risk, which further leads to cyberbullying; it is also the biggest platform that can easily spread fake news [8]. The introduction of social media was carried out to facilitate knowledge diffusion, the sharing of creativity across organizational boundaries, and to create a platform where everybody can share their talents [9].

2. Impacts of Social Media in Different Sectors

2.1. Impacts of Social Media on Business

Social media is the latest buzz in the market because it brings organizations, businesses, and brands together to generate news, influence people, form connections, and grow groupings. Companies utilize online social networking platforms for their brand's value. Social media via the Internet has the advantage of a correspondence step that encourages communication between a business and its financiers. The business might be advanced through several distant unauthorized places where one may communicate [10]. A significant amount of the promotion is a tool used by an organization to expand social media networks to draw the finest clients [6].

Some advantages are as follows:

- It is easier to comprehend client needs when social media is used.
- Social media helps businesses promote themselves all over the world.
- Social media builds deals and maintains clients through a standard connection and a lucky client benefit.
- A social networking site will help to attract new customers by offering a wide range of services.
- Internet networking can help to gain insight into the market and expand further in comparison with its competitors.

Some disadvantages are as follows:

- In a business context, social media is not at all risk because many fans and supporters are allowed to comment on specific associations; negative comments can cause an association with disappointment.
- Negative customer reviews are harmful.
- Highly time-consuming.
- There is more and more content on the web.
- It is very difficult to undo a mistake made on social media.

2.2. Impacts of Social Media on Health

Social media is a routine movement that improves social association, communication, and even abilities through participation in various forms of digital networking. There are several opportunities to connect with classmates, businesses, and people who have similar experiences through social networking sites [11]. A survey found that 71% of teenagers claimed they use YouTube at least once a day and 16% said they use it continuously. The use of various social media platforms, like YouTube and Instagram, is more common among older teens than younger teens. Among teenagers aged 13 and 14, for instance, just 45% of respondents claim to use Instagram, compared to 68% of those aged 15 to 17 [12]. Therefore, a significant portion of the social and technological growth of this day and age occurs on the Internet and mobile devices [13]. Digital networking sites have recently been linked by some experts to mental illnesses such as anxiety, loneliness, and depression [11]. Given the relative novelty of digital networking sites, several questions about their possible impact on mental health have not yet been satisfactorily addressed [14].

2.3. Impacts of Social Media on Marketing

Instead of sending people a bundle of information from a company, social media marketing emphasizes user interaction, peer-to-peer contact, and user-generated content. Thus, it raises consumer confidence in brands [4]. There are many different marketing platforms, such as company marketing (HubSpot, active campaign), shopping apps (Amazon, Flipkart, etc.), and promotion platforms (Instagram, Pinterest, etc.). The use of social media allows for easy communication among users and allows marketers to communicate with customers through a variety of channels [2]. SSM brands may find more customers for their goods and services by establishing direct connections with their audience, which offers various advantages [15].

2.4. Impacts of Social Media on Politics

The Internet can be used to influence politics in a variety of ways. With the rapid growth of social media politicians use social networking sites to communicate with people and to build their campaigns. It is generally presumed that social media plays a vital role in diffusing information and the claims of political parties [5]. Through the Internet, people can share and discuss political claims or debate about it. Social media is used to influence people's opinions due to different thoughts and ideas. In addition to being seen as an opportunity to create new forms of participation in politics, the Internet has also been described as an instrument that provides citizens with better access to the political process.

2.5. Impacts of Social Media on Finance

Establishing solid contact with customers and learning more about their evaluations can be achieved through social media accounts. The financial services sector has fallen behind other industries when it comes to social media [16]. Financial institutions can lower their operational risks by fostering transparency through knowledge transfer and sharing [9]. Social media poses many dangers in the finance industry and can impact legislation, policies, and compliance.

3. Challenges of Social Media

Social media has become a fundamental part of modern communication in the digital age, linking individuals all over the world and making information easier to share. However, social media's widespread influence also presents several issues that need to be carefully considered. Below are some of the most prevalent problems with social media.

Disinformation and fake news' proliferation: In the digital age, disinformation and fake news are spreading alarmingly more frequently due to the quick information sharing provided by social media platforms. Vosoughi et al. [17] have conducted recent research that highlights the hasty transmission of inaccurate information on social media platforms like Twitter. This highlights the requirement for efficient ways to thwart this challenge. Widespread intrusions are needed to safeguard the reliability of online information due to the substantial threat that misinformation poses to public discourse and decision making.

Data exploitation and privacy concerns: Social media platforms gather and use substantial amounts of personal information about their users, raising important privacy concerns. An assessment of the likelihood of political misuse of personal data is provided by the Cambridge Analytica incident [18]. For social media platforms, maintaining user privacy while delivering personalized information is a challenging task. The digital environment must undergo a continuous revolution in privacy protections to ensure customer trust and belief.

Psychological effects and mental health concerns: According to Twenge and Campbell [19], teenagers are experiencing a worrying increase in depression symptoms related to enhanced social media usage. These platforms, which use algorithms to extend user interaction, aggravate mental health issues due to their addictive nature. Efforts must be made at both the individual and platform levels to promote a better digital environment in order to effectively mitigate social media's negative psychological impacts.

Cybersecurity vulnerabilities: The interrelated structure of social media platforms exposes users to several forms of cybercrime, like identity theft and phishing attempts. Recent incidents, like the Twitter Bitcoin scam 2020 [20], highlight the defects in even the most prevalent sites. To successfully control cybersecurity concerns, persistent attempts to improve security measures, educate users about online threats, and establish coordination between platforms and law enforcement agencies are needed.

4. Social Media and Cybercrime

The National White Collar Crime Center's "Criminal Use of Social Media" white paper asserts that social media's recent emergence has drastically changed the communication landscape. Every day, millions of people use social media platforms, including Instagram, Facebook, LinkedIn, YouTube, and Twitter. Through these platforms, individuals communicate with one another. People use these channels for everyday communication inside the public sector, as well as for advertising and hiring new staff. Figure 2 displays Statista's data on the most widely used social media networks as of October 2023 [21], sorted by the number of monthly active users.

According to the report [21], social media surfing is the most popular online activity. Social media networking takes up over 12 min per hour on a PC, and social media surfing takes up over 18 min per hour on a mobile phone. Due to the changing nature of communication, malefactors are exploiting social media channels for nefarious purposes. The NW3C report identified five types of social media-related crimes.

(1) Burglary using social networking.
(2) Social engineering and phishing.
(3) Malicious software.
(4) Identity thieving.
(5) Cyberstalking [21].

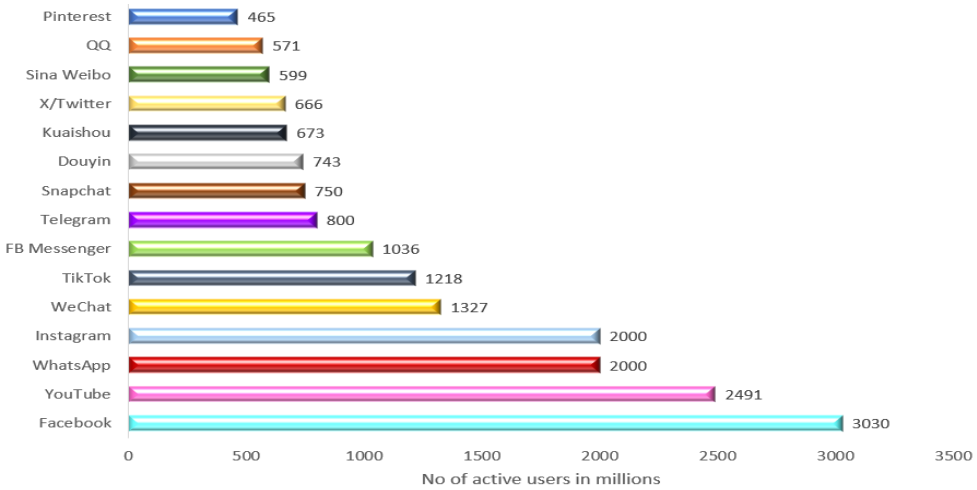

Figure 2. Social media users as of October 2023 [18].

4.1. Burglary through Social Networking

Burglary via social media involves criminals scouring social media for prospective burglary targets. Social media users usually post about their lifestyles, such as having dinner or going on a vacation [22]. These activities provide criminals with information for finding easy targets, allowing them to plan burglaries over an extended period [23].

Social Engineering and Phishing

Social engineering uses coercive control to acquire sensitive data. It is common for people to receive messages from friends asking for immediate financial assistance via social networking platforms [21]. Normally, these messages are not sent with any password protection to prevent crime. As it is very easy to assess the information related to bank accounts, cybercriminals use various tricks and tactics to gather information about any individual with the help of social engineering [10]. Phishing emails look very professional, like tax refund scams, false iCloud update notifications, human resource survey scams, and owners asking employees for login credentials or bank details. Cybercriminals try to scare their targets so that they do not inform any organization which deals with cybercrime. Criminals sent millions of emails to gather details. The most common type of phishing is deceptive phishing. Here, fraudsters pretend to be a legitimate body to steal personal details or login credentials. There were 34% more phishing incidents in 2021 than in 2020, and almost 13 times more compared to 2017 [24]. Figure 3 below shows the number of cybercrime victims in 2021 [23].

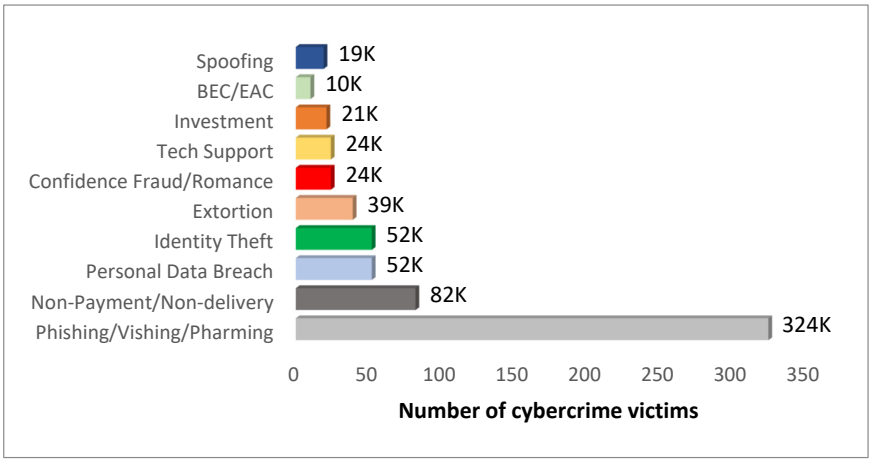

Figure 3. Cybercrime victims in 2021 [23].

4.2. Malicious Software

Social media is a great platform for spreading malicious software and viruses. Malicious software is software designed with an evil intent to harm our systems' users [25]. The malware infects the victims' machines without their knowledge or consent after they reply to them [21]. While there was a noticeable decrease in new malware variations in 2018, the Symantec ISTR 2019 [26] reports that Emotet [21], a banking Trojan virus kind, is one of the most costly and damaging malwares that affects the government and private sectors. The number of malware cases over the recent ten years is displayed in Figure 4 [27].

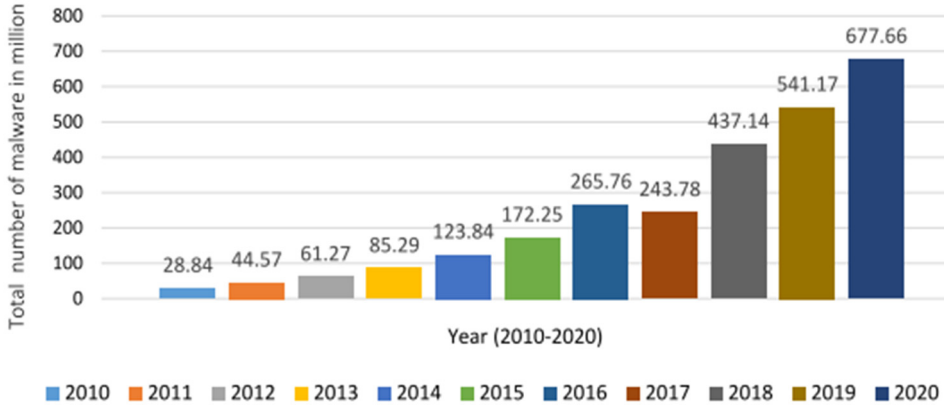

Figure 4. Total number of malware cases in the recent ten years [27].

4.3. Identity Thieving

Identity theft is defined by investigators as an attempt to obtain a person's personal information for illegal purposes [28]. Identity theft is described by research as the deliberate use of the victim's info for illegal purposes without regard for the law [29]. According to a Statista report from 2022, identity theft incidents worldwide rated India as the top country, with an estimated 27.2 million adult victims during that time. The Consumer Sentinel Network Data Book 2018 [21] provides statistics from 2002 to 2018 on identity theft complaints. These figures are displayed in Figure 5.

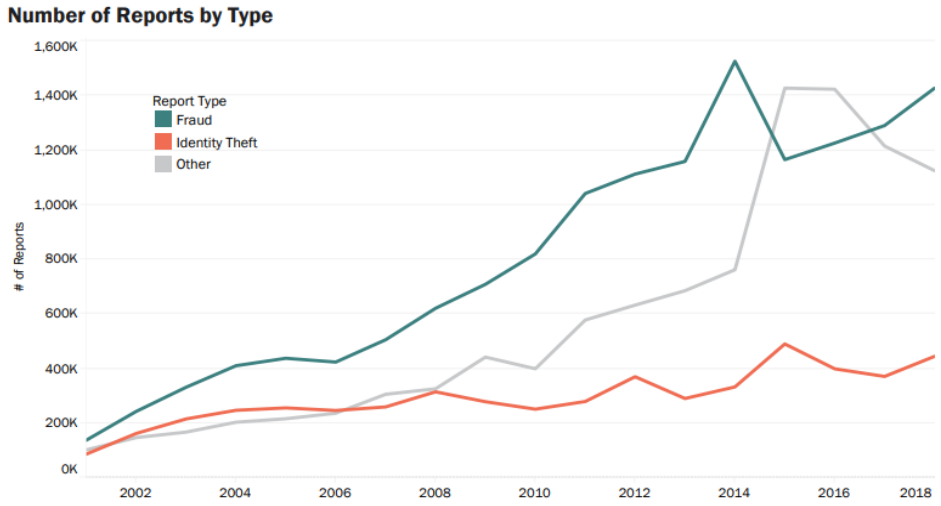

Figure 5. Identity theft complaints from 2002 to 2018 [21].

5. Cybercrime Prevention Techniques

Table 1 below completely describes numerous categories of cybercrime as well as their relevant preventative techniques. It includes a wide range of cyber risks, like burglary via social networking, phishing and social engineering, virus attacks, cyberstalking, identity

theft, and cybercasing. The preventative measures provided cover a wide range of topics, from user education and privacy protections to the employment of advanced technology like firewalls and encryption. Each sort of cybercrime is addressed with a specific set of measures, emphasizing the significance of a diversified approach to cybersecurity.

Table 1. Cybercrime prevention techniques.

Cybercrime	Prevention Techniques
Burglary via social networking	1. Privacy settings: regularly reviewing and adjusting privacy settings on social media platforms can help limit access to personal information. 2. Network security: the use of strong, unique passwords and enabling two-factor authentication to secure social media prevents unauthorized access. 3. Educate users: promote awareness among users about the risks linked with oversharing and the importance of securing personal information online. 4. Using techniques: genetic algorithms, random forest-based model, time series approach, rule induction, multi-layer perceptron, case-based reasoning, and self-organizing map [30].
Social engineering and phishing	1. Email filters: implement advanced email filtering systems to identify and block phishing emails. 2. Multi-factor authentication: enforce the use of multi-factor authentication to add an extra layer of security and prevent unauthorized access. 3. Regular updates: keep software and systems up to date to patch known vulnerabilities exploited by cybercriminals for social engineering attacks. 4. Using techniques: C4.5 algorithm, iREP security, and neural networks [31].
Malware	1. Antivirus software: it is important to install reputable antivirus software and keep it updated to ensure your devices are protected against malware. 2. Firewalls: implementation of firewalls to monitor and control incoming and outgoing network traffic, providing an additional cover of defense against malware. 3. Network segmentation: implement network segmentation to isolate and contain the spread of malware within a network, minimizing potential damage. 4. Using techniques: anomaly-based malware detection, API/system calls, signature-based malware detection, assembly instructions, and n-grams [32].
Identity theft	1. Strong authentication: encourage the use of strong, unique passwords and biometric authentication methods to protect user accounts from unauthorized access. 2. Credit monitoring services: utilize credit monitoring services to detect and alert users to any suspicious or unauthorized activities related to their financial accounts. 3. Secure Wi-Fi networks: ensure the use of secure, encrypted Wi-Fi networks to prevent unauthorized access and data interception by cybercriminals. 4. Using techniques: three-factor authentication (3FA), hidden Markov model, genetic algorithm, SD and CD algorithms, outlier detection, and logistic regression [33].
Cyberstalking	1. Digital footprint management: minimize the online presence by limiting the personal information shared on social media and other online platforms. 2. Privacy settings: adjust privacy settings on social media accounts to restrict access to personal information and control who can view or contact the user. 3. Report and block: encourage users to report instances of cyberstalking and block individuals engaging in such activities. 4. Using techniques: cyberstalking detection framework, signature-based data mining, association rule mining algorithm [34].
Cybercasing	1. Digital footprint awareness: encourage users to be aware of their digital footprint, limiting the information available online about their routines and activities. 2. Location privacy settings: review and adjust location privacy settings on devices and applications to restrict unnecessary sharing of location information. 3. Use of encryption: utilize encryption technologies to protect sensitive information and communications from potential cybercasing attempts. 4. Using techniques: with SVM classifiers, check and delete geolocations from images using a tool like tool.geoimgr.com [35].

6. Conclusions

This review paper provides a thorough examination of the pervasive role that social media plays in contemporary society. The analysis performed here has underscored

the ubiquity of web-based social networking, emphasizing its integral position in the daily lives of individuals, particularly within the age group of 20–29 years. With the continuous advancement of technology, social media is becoming an essential tool for communication, information dissemination, and business enhancement. However, in addition to its revolutionary power, social media brings with it a set of obstacles that must be carefully considered. Social media presents a wide range of difficulties, from the quick spread of misinformation and fake news to serious privacy concerns and data theft. These difficulties are exacerbated by the addictive nature of these platforms, which is amplified by algorithms designed for maximum user involvement. Furthermore, the interconnected structure of social media platforms exposes users to several types of cybercrime, such as identity theft and phishing assaults. To address these problems, a systematic and directed methodology is required.

Policymakers, technology developers, and consumers must collaborate to address misinformation, privacy concerns, psychological effects, and cybersecurity risks. Collaboration is the key to managing the digital age effectively, ensuring that social media's positive impact on worldwide interaction lasts while addressing its challenges.

The sphere of social media presents several research possibilities. To begin with, social media platforms need to be examined more closely in terms of cybersecurity. As cybercrime and misinformation are on the rise, researchers should explore innovative strategies to enhance security measures, protect user data, and mitigate its spread. Additionally, considering the demographic trends highlighted in this review, further studies should investigate how financial institutions and companies can tailor their social media initiatives to better align with the characteristics and requirements of the age groups predominantly using these platforms.

Furthermore, research efforts should be directed toward developing and implementing frameworks for digital literacy and responsible social media usage. Considering the potential negative impacts of social media that this paper emphasized, it is therefore crucial to educate users about discerning credible information, online etiquette, and privacy protection for fostering a safer and more informed digital society.

Author Contributions: Conceptualization, G.K., U.B., K.L.P. and S.Y.; investigation, G.K., U.B., K.L.P. and S.Y.; methodology, G.K., U.B., K.L.P., S.Y., P.A. and P.S.; project administration, L.P. and R.G.; supervision, L.P. and R.G.; validation, S.M.; visualization, G.K. and S.M.; writing—original draft preparation, G.K., U.B., K.L.P. and S.Y.; writing—review and editing, P.A., P.S., L.P., R.G. and S.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: We would like to thank Symbiosis International (Deemed University) for providing research facilities.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Fard, A.E.; Verma, T. A comprehensive review on countering rumours in the age of online social media platforms. In *Causes and Symptoms of Socio-Cultural Polarization: Role of Information and Communication Technologies*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 253–284. [CrossRef]
2. Appel, G.; Grewal, L.; Hadi, R.; Stephen, A.T. The future of social media in marketing. *J. Acad. Mark. Sci.* **2020**, *48*, 79–95. [CrossRef]
3. Testa, S.; Massa, S.; Martini, A.; Appio, F.P. Social media-based innovation: A review of trends and a research agenda. *Inf. Manag.* **2020**, *57*, 103196. [CrossRef]

4. Xiong, L.; Alsadoon, A.; Maag, A.; Prasad, P.W.C.; Hoe, L.S.; Elchouemi, A. Rise of social media marketing: A perspective on higher education. In Proceedings of the 2018 13th International Conference on Computer Science & Education (ICCSE), Colombo, Sri Lanka, 8–11 August 2018.
5. Calderaro, A. Social Media and Politics. 2018. Available online: https://api.semanticscholar.org/CorpusID:155809729 (accessed on 7 October 2017).
6. Akram, W.; Kumar, R. A study on positive and negative effects of social media on society. *Int. J. Comput. Sci. Eng.* **2017**, *5*, 351–354. [CrossRef]
7. Boer, M.; Stevens, G.W.; Finkenauer, C.; de Looze, M.E.; van den Eijnden, R.J. Social media use intensity, social media use problems, and mental health among adolescents: Investigating directionality and mediating processes. *Comput. Hum. Behav.* **2021**, *116*, 106645. [CrossRef]
8. NW3C. Cyberstalking (March 2015). NW3C. 2015. Available online: https://www.nw3c.org/UI/Index.html (accessed on 10 July 2017).
9. Sarigianni, C.; Thalmann, S.; Manhart, M. Knowledge Risks of Social Media in the Financial Industry. *Int. J. Knowl. Manag.* **2015**, *11*, 19–34. [CrossRef]
10. Soomro, T.R.; Hussain, M. Social Media-Related Cybercrimes and Techniques for Their Prevention. *Appl. Comput. Syst.* **2019**, *24*, 9–17. [CrossRef]
11. Rajesh, D.; Priya, V.K. Impact of Social Media on Mental Health of Students. *Int. J. Sci. Technol. Res.* **2020**, *9*, 3796.
12. Anderson, M.; Jiang, J. Teens, social media & technology 2018. *Pew Res. Cent.* **2018**, *31*, 1673–1689.
13. Patchin, J.; Hinduja, S. Trends in online social networking: Adolescent use of MySpace over time. *New Media Soc.* **2010**, *12*, 197–216. [CrossRef]
14. Pantic, I. Online Social Networking and Mental Health. *Cyberpsychol. Behav. Soc. Netw.* **2014**, *17*, 1089. [CrossRef]
15. Kapoor, K.K.; Tamilmani, K.; Rana, N.P.; Patil, P.; Dwivedi, Y.K.; Nerur, S. Advances in Social Media Research: Past, Present and Future. *Inf. Syst. Front.* **2018**, *20*, 531–558. [CrossRef]
16. Venkateswara Kumara, K.S.; Rama Devib, V. Social Media in Financial Services–A Theoretical Perspective. *Procedia Econ. Financ.* **2014**, *11*, 306–313.
17. Olan, F.; Jayawickrama, U.; Arakpogun, E.O.; Suklan, J.; Liu, S. Fake news on Social Media: The Impact on Society. *Inf. Syst. Front.* **2022**. [CrossRef]
18. Cadwalladr, C.; Graham-Harrison, E. Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. The Guardian. 2018. Available online: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed on 17 March 2018).
19. Wenge, J.M.; Campbell, W.K. Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study. *JAMA Pediatr.* **2018**, *172*, 557–565.
20. BBC News. Twitter Hack: Staff Tricked by Phone Spear-Phishing Scam. [Online]. 2020. Available online: https://www.bbc.com/news/technology-53553247 (accessed on 31 July 2020).
21. Mudassir, K.; Haque, S. Cyber Security and Ethics on Social Media. *J. Mod. Dev. Appl. Eng. Technol. Res.* **2017**, *1*, 51–58.
22. Chen, Y.; Sherren, K.; Smit, M.; Lee, K.Y. Using social media images as data in social science research. *New Media Soc.* **2023**, *25*, 849–871. [CrossRef]
23. NW3C. *Criminal Use of Social Media*; NW3C: Fairmont, WV, USA, 2013.
24. AntivirusGuide.com. Phishing Statistics. [Online]. Available online: https://www.antivirusguide.com/cybersecurity/phishing-statistics/ (accessed on 31 July 2020).
25. Ngo, F.T.; Agarwal, A.; Govindu, R.; MacDonald, C. Malicious software threats. *Palgrave Handb. Int. Cybercrime Cyberdeviance* **2020**, 793–813. [CrossRef]
26. Symantec. *Internet Security Threat Report*; Symantec Corporation: Sunnyvale, CA, USA, 2019.
27. Maniriho, P.; Mahmood, A.N.; Chowdhury, M.J.M. A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges. *Future Gener. Comput. Syst.* **2022**, *130*, 1–18. [CrossRef]
28. Dadkhah, M.; Lagzian, M.; Borchardt, G. Identity Theft in the Academic World Leads to Junk. *Sci. Eng. Ethics* **2018**, *24*, 287–290. [CrossRef] [PubMed]
29. Irshad, S.; Soomro, T.R. Identity Theft and Social Media. *Int. J. Comput. Sci. Netw. Secur.* **2018**, *18*, 43–55.
30. Alghamdi, D.M. A Data Mining Based Approach for Burglary Crime Rate Prediction. Ph.D. Dissertation, University of Illinois at Chicago, Chicago, IL, USA, 2017.
31. Priya, A.; Meenakshi, E. Detection of phishing websites using C4. 5 data mining algorithm. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 1468–1472.
32. Ye, Y.; Li, T.; Adjeroh, D.; Iyengar, S.S. A survey on malware detection using data mining techniques. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 1–40. [CrossRef]
33. Kshirsagar, A.; Dole, L. A review on data mining methods for identity crime detection. *Int. J. Electr. Electron. Comput. Syst.* **2014**, *2*, 51–55.
34. Lekha, C.; Prakasam, S. Implementation of Data Mining Techniques for Cyber Crime Detection. *Int. J. Eng. Sci. Math.* **2018**, *7*, 607–613.

35. Spyrou, E.; Mylonas, P. A survey of geo-tagged multimedia content analysis within flickr. In *Artificial Intelligence Applications and Innovations: AIAI 2014 Workshops: CoPA, MHDW, IIVC, and MT4BD, Rhodes, Greece, 19–21 September 2014, Proceedings 10*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 126–135.