RISING CYBERCRIME ON SOCIAL MEDIA DURING COVID PANDEMIC AND ITS IMPACT ON DIGITAL MARKETING

Sakshi Tiwari, IMS Unison University
Sushil Kumar Rai, IMS Unison University
Varsha Sisodia, Bennett University

ABSTRACT

Covid pandemic brought a significant change in the way people learn, entertain, interact, and conduct business. With people working and socializing remotely, social media usage skyrocketed and provided a fertile ground to cybercriminals to exploit the platforms and its users. This paper will explore the rising trend of cybercrime on social media, including specific types of cybercrime such as phishing scams, impersonation, and misinformation. The paper will also discuss about the parties mostly affected by cybercrimes. Additionally, the paper will delve into the impact of increase in cybercrime on digital marketing, including the challenges faced by businesses. Overall, the paper aims to provide a comprehensive overview of the current state of cybercrime media during the covid pandemic and how it is impacting the overall society and digital markets all together.

Keywords: Covid-19, Digital channels, Social media usage, Cybercrimes, Phishing, Privacy, Online market.

INTRODUCTION

The start of 2020 was dominated by covid, a terrible and obscure virus that wreaked havoc across the globe and putted everything to a halt. Travelling was banned, educational institutions and workplaces were closed, and people were restricted to four walls of their homes, leading to global communication crisis. But, at this point digital channels stepped in to bridge the gap left by covid prevention measures, and an inevitable surge was seen in the usage of digital technologies and social platforms became one of the mediums that allowed individuals to communicate in real-time (Kanekar & Sharma, 2020). Though, increased use of digital technologies led to online fraud, scams, intrusions, and security breaches (Pandey & Pal, 2020). Due to social distancing norms, there was lack of physical interaction therefore, people were entirely dependent on virtual form of interaction and were spending 50% of their time on social media (Beech, 2020). Undoubtedly, social media during the crisis had always redefined communication and made it far better, for instance, when in 2015 Nepal experienced its worst earthquake, Facebook activated its Safety feature, which helped various families to locate their near and dear ones. Similarly, during the covid pandemic Facebook launched a feature 'Community Help' which provided users with a mechanism to offer or receive help in the wake of the crisis. However, at the same time, social media was excessively exploited by cybercriminals, and massive surge in cybercrime cases was observed in many countries around the world (Monteith et.al, 2021).

Additionally, cybercrime cases that were resulting due to COVID-19 pandemic posed serious threats to the global population safety and economy (Lallie et al., 2021). Although, cyber-violence was pervasive within social media platforms, like Twitter and

Citation Information: Tiwari, S., Kumar Rai, S., & Sisodia., V. (2023). Rising cybercrime on social media during covid pandemic and its impact on digital marketing. *Academy of Marketing Studies Journal, 27*(S4), 1-8.

Facebook before the pandemic but, covid situation provided more boost to it. Cyber criminals started using social media for their own malicious purposes and misinformation and disinformation was continuously spread via social media and encrypted messaging services (UNODC, 2020). It was during this phase that fake websites and social media pages were created which further were used to steal personal data. All in all, the shift to remote work, online learning, made it easier for cybercriminals to target individuals and organizations, and the pandemic has created new opportunities for them to take advantage of people's fears and uncertainty.

A major shift at this point was observed in the consumer behaviour and purchasing patterns. As people were forced to stay at home, many turned to online shopping this led to an increase in e-commerce sales and a spike in social media usage, which in turn led to an increase in the importance of digital marketing. Businesses increased investment in digital marketing and social media to support these changes, and also led to more businesses creating digital and social media teams in-house. However, it got easier for cybercriminals to target individuals and businesses, as many people were accessing sensitive information and conducting transactions online from home.

REVIEW OF LITERATURE

Social media usage and Cybercrime

Cybercrime is a broad term that refers to criminal activity that uses computers or computer networks as a tool. These attacks are processed knowingly and have serious impacts over the society for suppose it can be a threat to National Defence, it can lead to psychological disorder and can even cause economic disruption (Saini et al., 2012) further, cybercrime is evolving as a serious issue in today’s scenario. The NW3C in their report discussed six types of crime committed using social media such as social networking burglary, phishing and social engineering, virus, Identity theft, cyber-stalking.

During the COVID-19 outbreak, cybercrime and online fraud have increased, and rates of cybercrime were high during months with the strictest lockdown policies (Buil-Gil, 2021). As the time spent on social media was increasing concerns were raised about its use due to the adverse effects reported by the health experts. Several health reports highlighted that excessive use of social media has resulted in mental health issues, information overload, and social media fatigue (Khan et al., 2020). According to the cyber security firm Bromium, social media platforms which primarily were used to keep in touch with friends and family gave rise to a massive global cybercriminal network. As people were continuously posting about day-to-day activities on social networks therefore, Facebook, WhatsApp, and Instagram become places where anyone can easily get information about someone’s location and personal life (Sharma & Sharma, 2020). Additionally, with COVID-19 unfolding, it was seen that growing use of social media was resulting in massive surge in cybercrime incidents worldwide According to Verizon 2021 Data Breach Investigations Report, Phishing attacks climbed by 11% during the global pandemic in addition, there was a considerable spike in the cases related to registration of fraudulent domains, websites, and spam emails. The cybercriminals targeted children, government, and health-care officials, around the world·

Cybercrimes against Children during Covid-19

Cybercrimes among children penetrated largely during the digital transformation of education that facilitated children to access cyberspace unconditionally (AlShabibi & Al-Suqri, 2021). Though children were gaining immensely from e-schooling still, they were most susceptible to hazards offered by the internet and social media platforms. Children's use of social media during the pandemic made them more vulnerable to becoming victims of cybercrimes (Mkhize & Gopal, 2021). Especially in India, the situation was gruesome as a 400% increase in cybercrime cases against children was reported by the National Crime Record Bureau in 2020 and nearly 90% of these offences involved the dissemination of materials that showed youngsters engaging in sexually explicit behaviour. Since India has the world's largest youth population, this is an alarming situation. Also, during this time, most children were turning to social media platforms and online games to escape the stresses of family life and social isolation without realizing that these platforms are vulnerable to online predation and offenders can easily exploit them on these platforms with false promises of friendship and security (Manganaro, 2021). A report by Pew Research Centre also highlights that teen share a wide range of information on social media

Cybercrimes against Government and Health-Care Officials during Covid-19

During covid lockdown to address public, governments and health-care officials worldwide increased the use of social networks like Twitter, Facebook, and YouTube (Padeiro et.al, 2021). These networks were primarily used to interact with people, circulate health-related information, and pandemic status. Though it was not for the first time that governments worldwide were using social media platforms, in the past also under such crisis governments had used these platforms significantly; such as, in the year 2015-2016 when the United States witnessed outbreak of Zika virus the, government at all levels used Twitter to deliver the information to people effectively (Hagen, et al., 2020).

However, during this pandemic, an obvious link was observed between government policy announcements and cybercrime activities. According to cybersecurity experts, health-care organisations and hospitals were prime targets for attackers (Warnick, 2021). Since the pandemic breakout, official agencies like the World Health Organization were targeted by cybercriminals. In April 2020 approximately 450 WHO members email addresses and passwords were leaked online. Also, under many instances of cybercrime scammers impersonated themselves as public authorities and promised Covid-19 cures to public (Miller, 2021). Nonetheless, in contemporary times, committing any other form of cybercrime is not challenging for scammers because much of the information that they need about an organization is readily available on social networks. Despite the existing threats, people continue to reveal massive amounts of personal information on online social networks, and third parties may benefit from users publicly disclosed personal information.

Cybercrime and Digital Marketing

Online services offer substantial personal and societal advantages to contemporary society (Riek, M. et al., 2015). Unfortunately, the expanding internet environment also exposes people to several dangers. According to consumer polls, consumers consider internet as an important market channel due to the convenience it offers but security and privacy concerns are influencing their buying decisions (Saban, et al., 2002). Due to features like large scalability, anonymity, and global reach, of internet a new type of crime called cybercrime has developed into a significant industry with professional attackers (Moore. et al. 2009). Accessing these online services has become perilous due to consumer-focused cybercrime such identity theft, credit card fraud, and phishing (Hunton, 2009). In the modern business environment, it has been determined that one of the biggest issues facing internet enterprises is the influx of criminal elements into the cyber domain. Also considering that, the success of any e-commerce sites in contemporary time depends on how these cyber challenges are addressed (Ugbomah, et al.). Given the increasing frequency of cyberattacks and data breaches, it is not unexpected that one of the biggest threats facing businesses over the next ten years is cybercrime (Dalpini, 2021).

Reasons behind Spiking Cybercrime

Due to government bans and people staying at home, there was an increase in Internet use, leading to increased cybercrimes. The work from home obligation too increased the potential of becoming a victim of cybercrime. According to a report in the Times of India (an English newspaper), 80% of cybercrime frauds occurred due to lack of cyber hygiene practiced by the users. Another report highlights that falling for a scam is induced due to a lapse in judgement (Lea et al. 2009). In some studies, the proliferation of cybercriminal activities during pandemic is partially attributed to offenders' boredom due to more leisure time at home (Regalado et al. 2022). Another critical factor is the low-risk perception of cybercrime. The globalisation of technology and revolutionary advancements in information technologies also have resulted in an increase in criminal activity (Cerezo et al. 2007).

DISCUSSION

Social Media usage and Cybercrime

The growing dependence of people on social media for everyday activities and communication offered cyber criminals with opportunity to take advantage of vulnerabilities present in these platforms to commit cybercrimes. These crimes range from simple scams to more complex attacks. These crimes even take different forms, such as identity theft, phishing scams, distribution of malware etc., these crimes also involve misuse of personal information, creation of fake accounts and manipulation of content for nefarious purpose.

The most common cybercrime on social media, which saw a huge spike during the covid phase is Phishing scams. These scams involve sending of fake messages or links to users by pretending to be from legitimate sources such as banks, government agencies. The aim of these scams is to trick the users into providing sensitive information such as login details or financial information. These scams can easily be spread through direct messages, posts or even fake profiles.

Another serious cybercrime identified on social media is identity theft which involves stealing someone’s personal information and using it to impersonate them online. This information is further used to access accounts, request money, or even commit crimes in victim’s name. This crime has long-term consequences for victims, including financial losses and damage to their reputation.

Children also face the brunt of the present technology. Online sexual exploitation of children is another serious problem that has grown in the recent years.

With such crimes it has also become important for parents and educators to be aware of these risks and brief children about how to stay safe online.

Governments and law enforcement agencies are even struggles to keep up with the constantly evolving threat to landscape. As cybercriminals are becoming more sophisticated, it is increasingly becoming difficult to track and prosecute them. Therefore, the need of the hour is to equip people with proper knowledge of how to take care of their personal data, how to access appropriate resources; how to report/prevent/stop these kinds of activities, and how to use privacy tools when using the internet. Also, it is important for users to be careful about sharing personal information, avoid responding to mean or aggressive messages, and report they encounter anything that makes them feel uncomfortable

Cybercrimes on Social Media and Digital Marketing

Cybercrimes on social media have a significant impact on marketing on the platform. One of the main ways that cybercrimes on social media can impact digital marketing is by undermining trust in the platform. If users feel that their personal information is at risk or that they are being targeted by scams, they may be less likely to engage with brands and businesses on the platform. This lack of trust will lead to decrease in people using online marketplaces, which can have a negative impact on the overall online market. One of the ways that cybercriminals are taking advantage of social media is using bots and fake accounts. These accounts are used to spread spam and scams, or to manipulate online discussions and influence public opinion further, which is particularly damaging businesses that rely on social media to reach customers, and leading to loss of trust and credibility.

The users presently encounter false or misleading information in large quantity on a social media platform, which make it more difficult for them to differentiate between genuine content and marketing messages. This further leads to a decline in the effectiveness of digital marketing campaigns and damage the credibility of the companies and organizations that are promoting their products or services.

Data breaches have also become a major cause of concern in the digital market. Due to these attack hackers gain access to a company's database and steal sensitive information such as customer data, financial records, and intellectual property. These breaches are having significant consequences for businesses, including financial losses, damage to their reputation, and legal consequences.

It is important for companies and organizations to be aware of these risks and to take steps to protect themselves and their customers from cybercrimes on social media. This can include educating employees about the risks of phishing scams and other types of cyber-attacks, implementing strong security measures, and working with trusted partners to ensure that their marketing campaigns are effective and legitimate.

Coping from Cybercrime in the Post Pandemic World

The challenges posed by COVID and cybercrimes during this communication crisis are global, so the responses should be. Public diplomacy and awareness-raising campaigns are vital during these years for the safety of vulnerable populations, particularly children. Also, legal measures are unquestionably crucial in combating cybercrime Law enforcement agencies also have an essential role in fighting crime (Boes & Leukfeldt, 2017). Harmonization of cyber laws and regulations also developing international cooperation and comity are critical countermeasures to fight cybercrime (Broadhurst & Chang, 2013). Further, it is essential to be wary of phishing emails and websites and practice proper cyber hygiene. Also, before transferring sensitive data or downloading any file from an email or text, a user should always check the source's legitimacy; it is also a good idea to use two channels of communication with counterparts, especially during pandemics.

Need to Rethink Privacy on Social Media to Fight Cybercrime

There has been a disconnect between people's beliefs about privacy and their internet privacy practises. (Norberg et al. 2007) Studies have indicated that social media users appear to care about their privacy, however, they do not act on that concern, disclosing personal information which further can be used by several entities (Barnes, 2006) Similarly, social media, though, is considered a private space by the users; yet, it is not as intimate as one would like to believe. Once information is on social media, it comes into the public domain. Still, many users opt to publicize their personal information to achieve different motives. Moreover, to gain access to any social media, one creates an account that requires them to give out their personal information like email IDs, contact numbers, addresses, and photos and this revelation of personal information leads to loss of privacy and increased chances of becoming a victim of cybercrime. Cybercriminals also use this information to create a secret dossier of users to exploit them in several ways. Therefore, social media platforms can reconsider privacy in several ways in order to combat cybercrime. One strategy is to impose more stringent restrictions on the kinds of personal data users are allowed to publish on their networks. Limiting the types of data that can be gathered, such as financial or locational data, and making it more challenging for hackers to obtain this data are two examples of how to do this. Enhancing user account security through the use of two-factor authentication or other identity verification methods is an additional strategy. Social media businesses can also collaborate closely with law enforcement and security professionals to spot and dismantle criminal operations that use their platforms.

CONCLUSION

Social media has evolved into a powerful platform for personal and international contact, exchanging ideas and information, expressing opinions, and amusement, the people accessing it will grow every year. Moreover, features such as interactivity, user-generated content, instant communication, and collaboration will set it apart from traditional forms of communication. Since cybercrime is currently one of humanity's most serious problems because anyone with an e-mail address, a bank account, or any sensitive information is vulnerable. Anyone can become a target, and the societal impact of cybercrime is reflected in the numbers. Most internet users are unaware of cybercrime, how to face it, to protect themselves from it. Therefore, social media users should learn to balance their personal information and privacy online and should practice proper cyber hygiene. Also, social media users should possess technical skills that will help them create, navigate, organize, produce, and share content. Similarly, cognitive skills for analysing and evaluating social media content and critically understanding the content in its context, relevance, and trustworthiness to safeguard themselves and make the best use of social media platforms and the internet.

In conclusion, cybercrimes on social media are having a significant impact on the online market. They are undermining trust in online marketplaces, leading to fewer people using these platforms. Governments and law enforcement agencies are also struggling to keep up with the constantly evolving threat landscape, leading to a sense of helplessness and frustration among those who have been affected. It is crucial for businesses, governments and individuals to take steps to protect themselves from these crimes, including using strong passwords, being cautious about giving out personal information, and staying up-to-date on the latest security measures.

REFERENCES

AlShabibi, A., & Al-Suqri, M. (2021). Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. In 2021 22nd International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE.

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday*.

Beech, M. (2020). COVID-19 Pushes Up Internet Use 70% and Streaming More Than 12%, First Figures Reveal.

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. In *Cyber-physical security* (pp. 185-203). Springer, Cham.

Broadhurst, R., & Chang, L.Y. (2013). Cybercrime in Asia: Trends and challenges. In *Handbook of Asian criminology* (pp. 49-63). Springer, New York, NY.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Burbidge, T. (2021). Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report.

Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* (pp. 13-27). IEEE.

Dalpini, N. (2021). *Cybercrime Protection in E-Commerce During the COVID-19 Pandemic* (Doctoral dissertation, Utica College).

Hagen, L., Neely, S., Scharf, R., & Keller, T. E. (2020). Social media use for crisis and emergency risk communications during the Zika health crisis. *Digital Government: Research and Practice*, *1*(2), 1-21.

Hunton, P. (2009) "The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model," Comput. Law Secur. Rev., vol. 25, no. 6, pp. 528–535.

Kanekar, A., & Sharma, M. (2020, September). COVID-19 and mental well-being: guidance on the application of behavioral and positive well-being strategies. In *Healthcare* (Vol. 8, No. 3, p. 336). Multidisciplinary Digital Publishing Institute.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Lallie, H. S., Shepherd, L.A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lea, S.E., Fischer, P., & Evans, K.M. (2009). The psychology of scams: Provoking and committing errors of judgement.

Manganaro, F. (2021). Children, Cyber Crime and COVID-19: Cyber Criminals Are Targeting Children During Lockdown.

Miller, O. (2021). Covid-19 related cyber-attacks leveraged Government announcements.

Mkhize, S., & Gopal, N. (2021). Cyberbullying perpetration: Children and youth at risk of victimization during Covid-19 lockdown. International Journal of Criminology and Sociology, 10, 525-537.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports, 23*(4), 1-9.

Moore, T., Clayton, R., & Anderson. R. (2009) "The economics of online crime," J. Econ. Perspect., vol. 23, no. 3, pp. 3–20, 2009.

NCRB report (2020) Over 400% rise in cyber crime cases against children in 2020: NCRB data.

Norberg, P.A., Horne, D.R., & Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, *41*(1), 100-126.

NW3C, "Criminal Use of Social Media (2013)," NW3C, 2013

Padeiro, M., Bueno-Larraz, B., & Freitas, Â. (2021). Local governments' use of social media during the COVID-19 pandemic: The case of Portugal. *Government information quarterly*, *38*(4), 101620.

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171.

Citation Information: Tiwari, S., Kumar Rai, S., & Sisodia., V. (2023). Rising cybercrime on social media during covid pandemic and its impact on digital marketing. *Academy of Marketing Studies Journal, 27*(S4), 1-8.

Regalado, J., Timmer, A., & Jawaid, A. (2022). Crime and deviance during the COVID-19 pandemic. *Sociology Compass*, e12974.

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Saban, K.A., McGivern, E., & Saykiewicz, J.N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. *Journal of Marketing Theory and Practice*, *10*(2), 29-37.

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.

Sharma, S. & Sharma, K. V. (2020) Cyber Crime analysis on Social Media. BSSS Journal of Computer: ISSN(Print)-0975-7228, E-ISSN - 2582-4880, Vol. XI, Issue-I.

Stock, J. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19.

Ugbomah, N., Omede, N., & Ugochukwu, O.C. Cybercrime: predictive impact on e-commerce in nigeria.

UNODC (2020). CYBERCRIME AND COVID19: Risks and Responses.

Warnick. A. (2021). Public health vulnerable to cyberattacks during COVID-19 outbreak: US alert issued.

Received: 13-Jan-2023, Manuscript No. AMSJ-23-13129; **Editor assigned:** 16-Jan-2023, PreQC No. AMSJ-23-13129(PQ); **Reviewed:** 27-Feb-2023, QC No. AMSJ-23-13129; **Revised:** 25-Mar-2023, Manuscript No. AMSJ-23-13129(R); **Published:** 06-Apr-2023