International Journal of Life Sciences
International Peer Reviewed Open Access Journal

Special Issue A18, May 2022
ISSN:2320-7817(p) 2320-964X(0)

Original Article Open Access

Cyber crime effects on students’ life during COVID-19

Dombre Maithili[1]* and Mukherjee Anushka[2]

[1]Department of Forensic Science, Lovely Professional University Phagwara Punjab, India
[2]Applied Forensic Research Sciences, India.
Email Id: maithilidombre@gmail.com

Manuscript details:

Available online on http://www.ijlsci.in
ISSN: 2320-964X (Online)
ISSN: 2320-7817 (Print)

Cite this article as:
Dombre Maithili and Mukherjee Anushka (2022) Cybercrime effects on students’ life during COVID-19, *Int. J. of. Life Sciences*, Special Issue, A18: 49-52.

Article published in Special issue of 1st National Conference on Forensic Science & Digital Forensics 2022 organised by Applied Forensic Research Sciences From 18th to 20th March, 2022.

ABSTRACT

The pandemic of covid-19 has changed all the aspects of lifestyle. The imposed lockdown has led millions of students to be confined at home leading to spend hours online every day for various activities which they could do offline. As such, full and direct dependence on the use of the unsafe Internet network in running all aspects of life. Students are fully and directly dependent on the usage of internet for all the various activities. Compounding a global health crisis with a sharp increase in cybercriminal activities related to COVID-19 is putting significant strain on law enforcement communities worldwide. These conditions have created a fertile environment for cybercriminals to grow their activity and exploit the pressures that affected human psychology to increase their attack success, given rise to the growth of cyber criminals. The significance of this research is to highlight how criminals are taking the benefit of this crisis. And for better prevention of cybercrimes.

Keywords: Cybercrimes, COVID-19, Internet surfing, cyber-attacks.

INTRODUCTION

The pandemic of COVID-19 and the imposed lockdown, has led to more people to be confined at home with many more hours to spend online each day and increasingly relying on the Internet to access services, they normally obtain offline. For example, most companies requested their employees to work from home, students moved to online studies, online shopping increased, and social networking activity increased, leading to an increase in Internet users significantly. Although traditional crime rates decreased due to curfews' imposition, cybercrime rates have witnessed a remarkable increase since the beginning of the pandemic.

However, cybercriminals exploit the COVID-19 pandemic. As such, they have increased their attacks and focused on campaigns related to COVID-

19, such as online selling of unlicensed drugs as cure for the disease, sharing fake news on social media, and sending phishing emails to victims (C Sohrabi et all,. 2019) Cyber-attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees working from home and capitalizing on people's strong interest in coronavirus-related news (e.g., malicious fake coronavirus related websites). Hackers also use credential stuffing techniques to gain access to employees' credentials and the stolen data is then sold to other cyber security criminals. One of the consequences is a serious disruption to businesses that rely heavily on videoconferencing platforms. Credential stuffing is a form of cyber-attack whereby hackers use previously-stolen combinations of username and password to gain access to other accounts.

Cybercrime and its techniques

Cybercrime has been there for many years but it has increased during the covid-19 pandemic due to the favorable environment for cybercriminals. The increase in the percentage of the population connected to the Internet and the time spent online, combined with the sense of confinement and the anxiety and fear generated from the lockdown, have provided more opportunities for cybercriminals to take advantage of the situation and make more money or create disruption. With the passage of time and the rapid increase in technology development, the attacker became more experienced and sophisticated in selecting victims in a coordinated manner to increase the likelihood of the attack success. Therefore, we have a term known as opportunistic attacks. Opportunistic attacks can be assumed as attacks focus on selection of victims based on the most vulnerable victim. In other words, attackers search for gaps or weaknesses in the company's system, making it more vulnerable to attack. As a result of the global pandemic, several small and medium sized commercial stores have gone digital in order to sustain their businesses. It was revealed that an estimate of 21% increase in online transaction has been discovered in year 2020 compared with 2019. Most of these websites were set up in such a hurry without much consideration to the security requirements of online businesses which has made them gullible to cyber frauds and attacks. E-Commerce crime entails all fake business deals performed through the internet. Such transactions unlike physical payment do not necessarily needs the card at the point of making payment rather; it only requires necessary information about the card. This information can be extracted by hackers who either use the stolen data to make false transactions or sell it to cybercriminals who defraud innocent people with this confidential information in their custody. Emails are considered as one of the most used tools, as it is used in phishing campaigns, spear phishing, spamming, spreading fake news, fraud, and Fake donation campaigns (A M Abukari and E K Bankas,. 2020). Moreover, emails are considered as the most official communication media between companies and employees, so cybercriminals take advantage of this circumstance to increase their campaigns. There has been a spike in some cybercrime techniques such as phishing. Phishing is the fraudulent practice of inducing individuals to reveal personal information, such as passwords and credit card numbers through fake websites or emails. New data gathered by Google and analyzed by Atlas VPN, a virtual private network (VPN) service provider, is shedding more light on the scope of this. According to the report, in January, Google registered 149k active phishing websites. In February, that number nearly doubled to 293k. In March, though, that number had increased to 522k – a 350% increase since January.

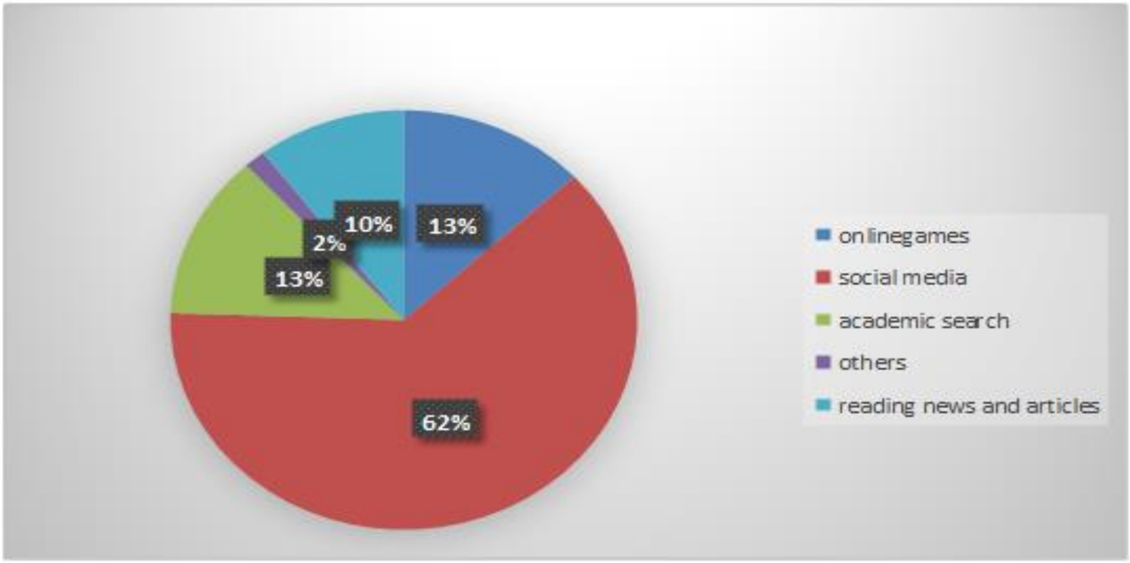
Cases all over the world

Countries all over the globe has reported an increase in various cybercrimes during the covid-19 pandemic. Several kinds of scams and frauds that came in the form of ads, emails, and fake websites and also through phone calls and text messages have been reported Cybercriminals are using malware such as Viruses, Worms, Trojan horses, Ransom ware and spyware to attack, damage and steal personal information of students and their families to blackmail them for their own benefit. There were also several cases reported of websites selling inappropriate or fake pharmaceutical drugs and medical equipment at very high prices in the name of covid-19 treatment. Cybercriminals also organized numerous crowd-funding events across several countries around the globe in the name of helping nobel corona virus warriors and survivors and also to help the families. But it was all a fraud to collect money for their own benefits. Another common scam that took place during the pandemic was promises of fake investments and health insurances. It was reported globally and both INTERPOL and United Nations have warned of such online frauds taking place during the pandemic of covid-19 (Khan N.A et all., 2020). At the same time, the lockdown has also significantly increased concerns about vulnerable persons online. While children, for instance, are greatly benefiting from e-schooling, they are equally more exposed to threats coming from the internet: file-sharing abuse, inappropriate content, and the grooming of children for sexual purposes are some of the dangers their parents should be aware of in these challenging times. The elderly, who usually rely on offline shopping and have now to purchase what they need from the internet, equally find themselves more exposed to cybercrime. There has also been an increase in the use of pornography. The industry has seen an increase in the number of users, but also concerns are being raised about vulnerable categories being pushed into exploitation, including drug addicts and children trafficked by families in need (Clement, J. 2020).

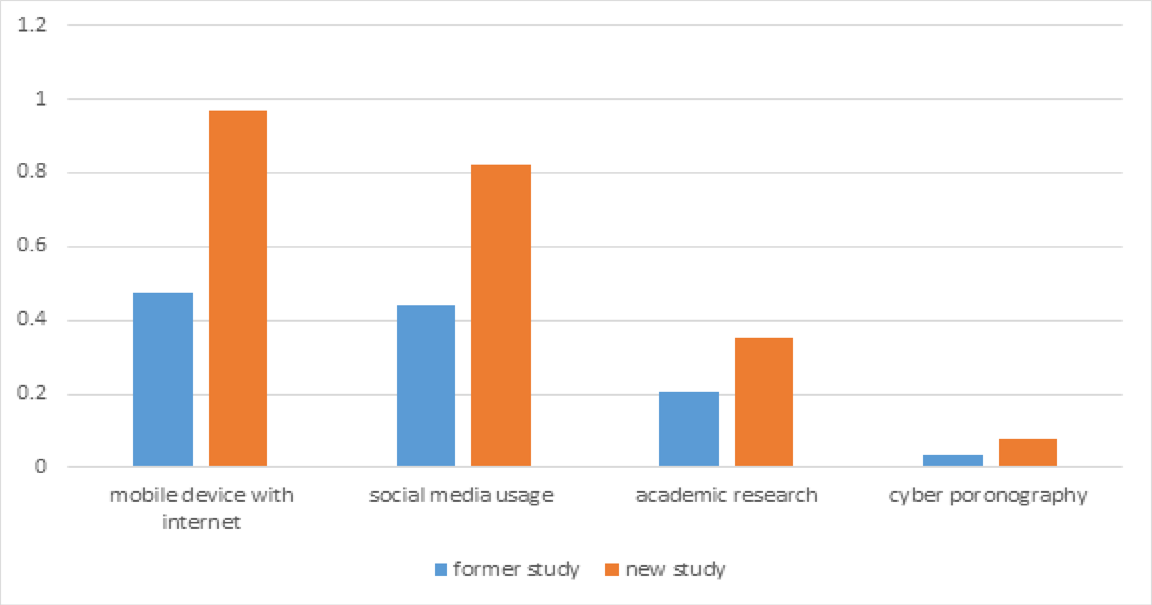
Graphical Studies Result

To analyze the activities that were mostly carried out using the internet, it was discovered that 10.2% spent more time playing online games, 8.3% read news and other articles online, 50.3% browse through different social media platforms such as Facebook, Instagram, Whatsap and others, 10.5% engaged in academic research activities while others were involved in other online activities such as watching videos and listening to songs. The following responses were revealed and a conclusion made from the results that people spend more time on social media than others.

T-test was employed to determine if there is significant difference between the occurrences of these cybercrimes in the two studies. A t-test value was measured between the number of occurrence of the different cybercrimes in the study before the pandemic and the one during the pandemic. The result of the t-test analysis conducted confirmed that the cybercrimes is statistically significant at. The t-test result further validates the fact that more cybercrimes were experienced during the covid -19 pandemic than before the pandemic.



Analyzing factor	Former study	New study
Mobile device with internet	0.475	0.968
Social media usage	0.438	0.82
Academic research	0.205	0.35
Cyber pornography	0.032	0.08



Conclusion

Cyber security is on the agenda of most executive committee meetings, but should perhaps be given extra attention in view of the growing threats during the pandemic. In the midst of the second wave of the coronavirus and concerns about a potential third wave, companies should be proactive in addressing the threats, and plan ways of preventing successful cyber-attacks rather than responding when they occur. However, although prevention measures are important, there is also a need for cyber-attack detection, response and recovery capabilities.

Conflicts of interest: The authors stated that no conflicts of interest.

REFERENCES

Abukari AM, Bankas EK (2020) Some Cyber Security Hygienic Protocols for Teleworkers in Covid-19 Pandemic Period and Beyond International Journal of Scientific & Engineering Research, volume 11, issue 4, p. 1404 - 1407

Clement, J. 2020: "Nigeria: Number of Internet Users 2025 Statista." 2020. https://www.statista.com/statistics/183849/internet-users-nigeria/.

Khan N.A., Brohi S.N. and Zaman N. (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic TechRxiv. Preprint. 2020, 6 p. DOI: 10.36227/techrxiv.12278792.v1

Sohrabi C, Alsafi Z, N Neill, M Khan, A Kerwan, A Al-Jabir, C Iosifidis & Agha R. World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19) International Journal of Surgery, volume 76, p. 71 - 76