International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 03(I), July - September, 2021, pp 141-144

CYBER CRIMES AND CYBER SECURITY THROUGHOUT COVID-19 PANDEMIC: AN OVERVIEW

Dr. Ajay Kumar Singh*

ABSTRACT

The principal objective of this paper was to guise the furthermost apprehension extent about increasing cybercrimes during the pandemic. Likewise all over the world, people in India had made reliant on the ever excessive internet and digital technology usage during all look-down period. As offices were closed for unprecedented times and work from home culture had completely changed the word situation. No one can disagree that internet and technology has taken over our lives entirely. In a fully digitalized world where we are using all the possible technologies available to us for intended reasons and purposes. So the kinds of dependence upon technologies was the reason the world is experiencing and perceiving the massive cybercrime happenings across the globe. Because of the outbreak of Covid-19, an immense cybercrimes activities and attacks have been perceived by people all across the world. As the pandemic has created so much fright and fretfulness in the lives of people they have agonised some distressing cyber-attacks. This paper explored all the aspects related to the emergent cybercrimes and cyber security actions that should be taken into account. Also discussed cyber teaching and training today and how it must be assimilated in the modern-day times and the effective laws and prevailing precautionary procedures to fight such criminal happenings over the internet.

Keywords: *Cybercrime, Cyber Security, Cyber Journalism, Covid-19, Pandemic.*

Introduction

Internet and new media technologies have become identical in everyone's daily life.Digitalization has taken over all of our daily activities from banking, e-commerce, to social media we are all connected to the internet and all our information is present in cyberspace. The menace of cyber Attacks has not just evolved it is there in every social system for a very long period but we have witnessed a huge hike in terms of number of increasing cases in recent times. Looking at the aspect where the internet has benefited us so much and making life so easier and fast on the other hand it has become a serious concern for those how are not technically sound and have landed up in huge trouble by becoming a victim of cybercrime (Muhammad Kashif, 2020). But the question arises that whether this information is secure or not. Due to the lockdown being implemented and restrictions all across the pandemic, it was only via the internet that everyone was interacting effectively and efficiently which contributed a huge opportunity to cybercriminals to attempt these crimes.

Cybercrime is defined as a crime that is based on or involves a computer as a tool or target to commit a crime. Cybercriminals may utilize computer technology to get to business details, personal information and use a computer to attempt cybercrimes. One of the biggest reason which has hiked the cybercrimes is lack of tutoring about internet usage and technological developments. This was the biggest reason for the major cybercrimes recorded during the pandemic. Phishing is one kind of cybercrime that is done by sending emails claiming one to be a legitimate mail and tries to trick the victim

* Dean, Faculty of Mass Communication, Haridev Joshi University of Journalism and Mass Communication, Jaipur, Rajasthan, India.

and retrieve valuable information from them. In these hard times, the most common practice done by these criminals was by sending emails or messages regarding offers relating to medical help and assistance they were offering to protect themselves from coronavirus. Ransomware is one kind of malicious software that Cybercriminals use to block the victims from using or accessing their own data/information. This is done by encrypting the files on their systems and hold the data hostage until their demand is paid off as the ransom amount. Cyber fraud is a trick that is practiced by hackers to gain dishonest advantages of another person. Mostly the financial frauds are practiced in cyberspace.

Literature Review

Cybercrime Outburst during Covid-19

Kenneth has discussed the most common types of attacks that were practiced were phishing, fraud, ransomware, business email compromise, etc. While the online game has benefited many areas such as online teaching, remote working, and any other important sectors. But the majority have suffered a lot due to the crises (Kenneth Okereafor, 2020). Covid -19 which not only has infected people's health but at the same time has affected their cyberspace too. Due to such a situation, there has been a lot of panic and anxiety which has been suffered by people all across the world which has increased more and more chances to attempt cyber attacks by the offenders by taking the advantage of the current situation (Nawir,2020). Attackers have utilized the weakness of humans knowing their fear towards the virus and all majority attacks which were initiated. A major focus of this paper is on the recommendations which are disused for maintaining cyber safety and protection for the scams. (Mahima Rai 1, 2019) some most harmful cybercrime and how are they performed by the cybercriminals are discussed below and the different types of attacks and what is the motivation of the cybercriminals behind the attack. Girshel has highlighted the different platforms which are used by cybercriminals to achieve their target. Below stated are some most common Covid-19 related attacks (Girshel Chokhonelidze 1, 2020).

The Covid -19 outburst isolated everyone in their home and no one was allowed to go out which resulted in doing everything online (Jolly, 2019). Anjali Jolly in her paper has pointed out that using the internet and technology whether it was groceries, medicine, shopping, etc. every payment or transaction was initiated digitally which one hand was safe for everyone which kept themselves safe from the virus and its spread but on the other hand cybercrime was hiked as everyone was working and paying remotely and were not secure at their networks and were giving out information and personal detail in the cyberspace which gave great chances for hackers to take their information and misuse them (Radoini, 2020).

Cyber Security Challenges

In the present times, the biggest challenge lies with the cyber security of our country to combat cyber attacks. As cyberspace is the least secure in the current times (sadashivam, 2020). People are most vulnerable online and need to be protected. The country has seen some major cyber security loopholes due to which we were not able to combat the cybercrime in the pandemic which was taking place every next second all across the country. In India, we only have one legislation that deals in cybercrime the question that arises is the IT Act sufficient to combat these crimes. With the growing technology and developments and the major shift of society towards online interactions, shopping, business industry education, etc. cyberspace has become very venerable (Jaikaran, 10 April 2020). There is much greater concern regarding the complexity of security of confidential information of state, cyber warfare, cyber terrorism. Living in the digital age it has become very necessary to be prepared for what next is coming our way. It is being observed the existing law and security mechanism need some strong pillars to handle these crimes. India has only one legislation to deal with cybercrimes which is the IT Act 2000 (Information and technology act) and some sections of IPC (Indian penal code). It is not the only security of an individual's cyberspace but a real concern for national security too (Geers, 2011). Therefore, this paper aims to look beyond what can be seen by naked eyes. The article aims to evaluate cyber security strategies for the protection of cyberspace.

Need for Cyber Security Education

Many of us use the internet as a platform to communicate and socialize. The most important and the only thing which one can do before getting trapped into a cyber-threat is to be aware of them. One of the major drawbacks which we have suffered is due to the lack of awareness and defensive strategies among the internet users. Cases like frauds, pornography, phishing, ransomware, are the most practiced attacks in the Covid times. Why is it so common that society is not educated about the risk which is around them by being active in cyberspace? Today's parents are the most concerned about their children as they hold the most potential of being affected by such activities. As the internet is not limited

to only adult's reach, it has its exposure to children also. Online gaming, education, everything is done online these days. Incorporating cyber education and cyber security aspects along with their syllabus at the school and universities level will benefit us to handle these crimes more efficiently (Rahman N. A. A, 2020). Cyber security education is a very crucial aspect in today's time as there are so many social media platforms like Instagram, Facebook, and Twitter etc. due to which children are so much prone to the information which is circulating in the internet world. Children should be protected and this can be done only done if we educated them about these crimes. These challenges have to be dealt with by bringing in new security provisions.

Prevailing Cyber Laws and Regulations to Combat Cybercrimes

In India "Information and Technology Act 2000", is the only legislation that deals with cybercrime. Certain provisions of the Indian penal code also provide some punishments for document-related offenses done online. There have been certain regulations and policies implemented by the government of India to deal with cybercrimes and improve cyber security. (Srivastva, 2017). "CERT-IN" (The Indian computer emergency response team) designated as the National nodal agency is incorporated to deal with cyber security. Its main purpose is for e-publishing security vulnerabilities and security alerts. The latest amendments done are the IntermediateryPolicies,2021 which mainly discusses the due diligence by the intermediary, code of ethics for digital media publishers, social media intermediaries, end-to-end encryption, and few more aspects. But in "Cyber Laws in India: An Overview" (Dr. Sonia Dutt Sharma) it has been rightly pointed out that in order to deal with the cybercrimes and their growing concerns we need to have a better protection mechanism against cyber threats. Hence the governments should take this issue more seriously and should keep a constant check on cyber strategies.

Criticism of the Literature Review

The researcher has reviewed the articles related to cybercrime and cyber security issues in pandemic times. The researcher has found many criticisms in the above literature he has reviewed to write this paper. The author of the cybercrime landscape has explained and encouraged people to be aware of cybercrime and its types and how it is a cyber security challenge but has not addressed the available remedies. Many authors have discussed the rise in cyber activities during the pandemic and the different security policies which prevail to combat these crimes, but have failed to address the inefficiency of the legal regime of our country has lacked to tackle these crimes. In the above article, the author has discussed the lack of cyber education is one of the biggest challenges in today's time to overcome these cyberspace difficulties but has not suggested the ways by which we can improve this lack of education in society. The author also has discussed many times in the above literature review what laws are available in India to give remedies to people if they fall victim to these cybercrimes, but the study did not indicate bringing in more laws to have a better environment and security in the digitalized world. The author has not the how important is it to protect the children from getting affected by the viruses and danger which is present in the technological world. It is a very important issue needs to be addressed. The researcher has looked deeply into matters in this particular area of research for writing this paper where it was found that the government should take initiatives to look into this matter and proved a proper mechanism at different levels of the education system to make everyone aware of these dangerous technological threats.

Research Gap

By going through much-existing available literature the researcher has found a lot of gaps for further study. The researcher found a lot of research gaps in Cyberspace which possesses unpredictable challenge's which need to be explored and taken into account for better safety. (Manjeet Singh, 2017).How has Remote working in the Covid times have made people less secure? There is a need to have more research to figure out to give effective measures to the consequences. (Mariana Toniolo-Barrios, 2020).Many issues regarding cybercrime have been left uncovered with only one legislation. There is a need to rethink more efficient laws for the nation (Kethineni, 2020).Are these new regulations and cyber security policies are sufficient to combat these cyber security issues. The researcher senses that the biggest challenge is that these cybercrimes don't have any boundaries so how will the jurisdiction of these be put through (Maboloc, 2020).The most important gap which has been analyzed by going through a lot many pieces of literature is that there is a lack of cyber education in the society which needs to be made aware to every citizen whether a child or adult and to falling as a victim (Rahman.n.a, 2020).

Concluding Remarks

A potential storm of cyber criminality emerges and if we are ready for that it will destroy our cyberspace. Internet users are must be made aware of the digital hygiene in our country which is the biggest reason for them becoming the victim of cybercrime. These different types of cybercrime and security mechanisms should be introduced to the public and due care should be taken. Hence there is a strong need for cyber education in our society and the researcher has analyzed the existing laws, cyber security policies that need to be revised to combat the current situation. The researcher has thus analyzed the existing laws and regulations to find out the areas in which there is a need for amendments. Moreover, there is a real need to finding out all the loopholes and fill in those with the best remedies the government can bring in by doing this we can give more recommendations and suggestions in this area of research.

References

1. Dr. Sonia Dutt Sharma, P. K. (n.d.). Cyber Laws in India: An Overview.
2. Geers, K. (2011). *Strategic Cyber Security.* CCD COE Publications.
3. Rahman N. A. A, S. I. (2020, May). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology. 10*(5).
4. Girshel Chokhonelidze 1, G. B. (2020). Cyber Threats and Attack Vectors during COVID-19. *International Journal for Research in Applied Science & Engineering Technology (IJRASET), 8*(10).
5. Jolly, M. A. (2019, november). Cyber laws in India. *International Journal of Engineering Research & Technology (IJERT), 8*(11).
6. Jaikaran, c. (10 April,2020). *Federal telework during the Covid-19 pandemic:cybersecurity issues in brief.* CRS report, Congressional research service.
7. Kau, M. S. (2019, April). *Cyber Crimes Becoming Threat to Cyber Security.* Retrieved from www.academia.edu: https://www.academia.edu/39618017/Cyber_Crimes_Becoming_Threat_to_Cyber_Security
8. Kenneth Okereafor, O. A. (2020, February). Tackling The Cybersecurity Impacts Of The Coronavirus Outbreak As A Challenge To Internet Safety. *International Journal in IT & Engineering (IJITE), 8*(2).
9. Kethineni, S. (2020, June 06). *Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms.* Retrieved from https://doi.org/10.1007/978-3-319-78440-3_7.
10. Maboloc, C. R. (2020). Who is the most vulnerable during a pandemic? The social model of disability and the COVID-19 crisis . *Eubios Journal of Asian and International Bioethics*, 158.
11. Mahima Rai 1, H. (2019, July). A Study On Cyber Crimes, Cyber Criminals And Major Security Breaches. *International Research Journal of Engineering and Technology (IRJET) , 06*(07).
12. Manjeet Singh, A. P. (2017, Febuary). A Comprehensive Study of Cyber Law and Cyber Crimes. *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), 3*(2).
13. MarianaToniolo-Barrios. (2020). *Mindfulness and the challenges of working from home in times of crisis* (Vol. 64). Elsevier.
14. Muhammad Kashif, A.-U.-R. M. (2020, august). A Surge in Cyber-Crime during COVID-19. Indonesian Journal of Social and Environmental Issues . *Indonesian Journal of Social and Environmental Issues, 1*(2).
15. Nawir, H. (2020). *Covid-19 Cyber Security Issue*. Retrieved from Academia: https://www.academia.edu/43325959/Covid_19_Cyber_Security_Issue
16. Radoini, M. A. (2020). *freedom from fear magazine.* (M. M. Villadsen, Ed.) Retrieved from F3magazine.unicri.it: http://f3magazine.unicri.it/?p=2085
17. Rahman.n.a, s. H. (2020, Feburary). Importance of cyber security education. *nternational Journal of Research in Engineering and Technology , 2*.
18. Sadashivam, D. T. (2020, April-June). Cyber crime: An analtical study of metropolotan cities in india. *An Intrernational journal bilingual peer reviewed refereed research journal, 10*(38(III)), 72-79.
19. Srivastva, a. (2017, Feburary). analyzing cyber crime & cyber laws in india. *VSRD international journal of technology and non-technical research, VIII*(2).