MEDICINE, LAW & SOCIETY
Vol. 15, No. 1, pp. 89–106, April 2022

A CRITICAL ANALYSIS OF CYBER SECURITY THREATS POSED BY COVID- 19 :DESIGNING A ROADMAP FOR FUTURE

NITEESH KUMAR UPADHYAY,[1, 2] MAHAK RATHEE[3]

[1] South Ural State University, Chelyabinsk, Russia, niteesh_marshal@yahoo.co.in
[2] Galgotias University, Faculty of Law, Uttar Pradesh, India, niteesh_marshal@yahoo.co.in
[3] Supreme Court of India, Tilak Marg, Mandi House, New Delhi, ratheemahak@gmail.com

CORRESPONDING AUTHOR
niteesh_marshal@yahoo.co.in

Accepted
20. 10. 2021

Revised
28. 11. 2021

Published
26. 4. 2022

Abstract The entire world has been impacted by Covid-19, which has forced the nations to undergo lockdowns, which have opened the new horizons of virtual learning and work from home culture. Though virtual learning and online meetings were available prior to the lockdowns, use of these platforms have intensified. There is a lack of awareness among many in the public concerning the perils of using these platforms which makes them susceptible to cyber-crime attacks phishing, sexual or verbal abuse, eve teasing etc. Lockdowns have provided cyber criminals with new criminal opportunities and evidence shows that there has been a rampant increase in the number of cyber-crimes during this period. Public lack of awareness has led to innocent people falling prey in the hands of attackers. Since the pandemic and ensuing lockdowns came as a surprise, public and private authorities lacked the opportunity to make appropriate arrangements for training people and making these platforms secure. There is no question that if these platforms are made secure, then they will prove to be as an asset to the society but much work must be done to achieve the goal of complete cyber security.

Keywords
attacks, Covid-19, Cyber Law, hacking, pandemic

https://doi.org/10.18690/mls.15.1.89-106.2022

University of Maribor Press

1 Introduction

A virus which originated in Wuhan in China, which was soon declared as a pandemic by the World Health Organisation, has impacted the entire world.[1] All the countries are fighting their battle against Covid-19 and the super powers and the countries with the best health care facilities like the U.S., Italy, China etc. have also been severely affected by this virus (Lallie, 2020). The impact of this virus is multifaceted. It is one of the most contagious viruses the world has ever witnessed, causing economic recession in many nations. The negative impacts caused by the virus will be felt by developing and under-developed countries long after the pandemic is over.[2]

India, too, is struggling to win the battle against the corona virus. India's government faces the additional responsibility of tackling the situation in a highly populated country where the majority of the population is poor (Earley, 2020).

There is no question that every sector has been impacted by this virus; however, the virus has precipitated an enhanced use of e-learning and virtual classroom education. Though these platforms were available to us prior to pandemic, they were used to a much lesser extent. The lockdowns necessitated by the pandemic have intensified the use of these platforms by an ever-increasing number of people and in ever-more settings. Be it an employee who has been working from home or a student attending classes, webinars and many other events through these platforms, they have been used like never before. Many companies like Google even extended their work from home policies until 2021.[3] Indeed, almost all companies have had to take measures to continue their operations through work from home mode. Consequently, the usage graphs of these virtual learning or online meeting platforms like zoom, google meet, Microsoft teams etc. have seen a tremendous rise during this time and there is no doubt that these platforms have proved to be the silver lining in the cloud for many of us. However, everything comes with its pros and cons and so is the case of use of these virtual meeting platforms (Desair, 2020).

[1] World Health Organisation on Coronavirus (2020) https://www.who.int/health-topics/coronavirus#tab=tab_1
[2] Id.
[3] Anonymous (2020), The impact of COVID-19 on higher education worldwide Resources for Higher Education Institutions, https://www.iau-aiu.net/IMG/pdf/covid-19_and_he_resources.pdf

While on the one hand these platforms provide a convenient mode of learning and working for many, the downside is that they have spawned an alarming increase in the number of cyber-crimes (ILO, 2020) and led to breaches of privacy (Walker, 2020). Since the Covid-19 pandemic was unforeseen, and the no one anticipated the breadth of the havoc it would cause, there was inadequate time to remove all the technical lacunas in these platforms and make them fully secure to use (Nappinai, 2017).

The cyber-crimes have increased since the lockdown and the incidents of data theft (Gayal, 2020), cyber-bullying, sexual and verbal abuse are being witnessed daily and regrettably the majority of the population is not aware of the various cyber-crimes (Chowdhary, 2020) that they might face using these platforms; or by the use of the internet in general; and, that there is a need to urgently develop and institute measures to tackle these situations (Wolters, 2020). We aim to analyse in detail the kind of cyber-crimes which can occur due to usage of the virtual learning platforms and we will suggest various solutions to mitigate the problems (Gayal, 2020).

2 Covid-19 and Effects on working and learning environments

There are numerous effects of Covid-19 which are negatively impacting the working and learning environments around the globe. The entire world has shifted to online mode and scenarios like work from home have become the new normal. Infrastructure, unfortunately, was not well-equipped to take the work or teaching and learning process online and hence has exposed people with cyber-crimes and threat. Relatively early in the pandemic, various emails started to circulate related to Covid-19 precautions and preventions and in March 2020 camouflaged spam emails targeted Italian email intrusion detection systems to infect them by delivering a weaponised Word document embedded with a Visual Basic for Application (VBA) script that eventually dropped a new TrickBot variant (Saleh, 2020). In one other case, a new ransomware strain dubbed as CovidLock was camouflaged as a Covid-19 tracking app and was widely distributed and downloaded (Anonymous, 2020).

Increased reliance on digital platforms has had negative side effects. Since lockdowns have effected both virtual learning and a work from home (Wallender, 2020) culture, there now is extreme reliance on the digital platforms available. The internet, as the only means of connecting, learning and working available at present,

means that everyone has resorted to the only mode of connectivity available to them. Admittedly, the internet also played a crucial role prior to lockdowns, but its usage and reliance has increased drastically as almost everything has gone online. Even government work, court work, medical consultations, meetings and negotiations have gone online. Even United Nations negotiations have gone online during this pandemic (Mani, 2020).

The lockdowns have caused hardships for individuals not well-equipped with technology. There are many people who have never used technology and this entire shift to the digital platforms has made it difficult for them to keep up. Many people have had a difficult time adjusting to the work from home culture. That section of society cannot be ignored which is not so much financially sound to own a smartphone and the education of children studying in government schools have been impacted a lot because of this. We need to remember that a considerable part of the population in India (and of course elsewhere in the world) reside in rural areas and villages where power outages are commonplace, making it impossible to work or study from home (Bedi, 2020). Many households have only one or two smartphones and laptops sometimes become a requirement because of online classes and work. It is difficult to operate from phones (Crisanto, 2020).

Companies worldwide are reducing their workforces in order to deal with the negative impacts wrought by Covid-19. Since lockdowns were imposed in many nations, the movement of people became restricted and as a result many people lost their livelihoods. This created a perfect storm of sorts, as many people who lost their jobs due to Covid-19 used the situation as an opportunity to make money illegally through cyber-crimes. In order to help avoid or at least minimize cyber-crimes in the future, companies which are seeking to downsize should implement proper plans including structured exit plans. Efforts should also be made to encourage people who have lost their jobs to enhance their skills through, for example, further education and perhaps even start their own start up.

Inadequate training and knowledge regarding use of digital platforms is also problematic. As mentioned earlier, people have been using the digital platforms at rates previously unknown and the entire Edutech industry and online meeting companies have witnessed a boom after the lockdowns as everyone resorted to these platforms (ESCO, 2020). However, a majority of the population is not well-equipped

to use these platforms due to either a lack of or inadequate training. Further, many people lack awareness concerning cyber-security. Parents also lack knowledge and experience regarding how to provide proper guidance to their wards for a better online learning experience and how to make online learning safe and possible, especially for kids below 6th standard.

There is a general lack of awareness among the population regarding cyber-crimes, cyber-security, misuse of the digital platforms, data theft and privacy issues. Hackers/cyber-criminals have seized upon this lack of knowledge to prey on the public for their financial gain (Mittal, 2020). This lack of public awareness is the main reason for the increase in cases of cyber-crimes during this pandemic (UNODC, 2020). Too many users are, regrettably, using these platforms without considering the permissions we are giving to these softwares to gain access to our devices. The cyber-criminals sell or manipulate a lot of data related to users for their personal financial gain (Gayal, 2020).

Targeting young people involved with virtual education is another serious problem. The Edtech Industry has grown many folds during the lockdowns and the audience involved are young school and college students having little knowledge of the lacunas of these digital platforms. This population is particularly susceptible and easy prey for cyber-criminals. A particularly disgusting example involved the case of Nirma University, wherein it has been alleged that during an online class utilizing the zoom platform a hacker entered the session and started masturbating. The National Commission for Women has already taken cognizance of the case (Rama, 2020). Such instances illustrate that, while these platforms provide a great means to connect, there is a lot more work to be done to make them secure to use (UNODC, 2020).

The issues of data protection and privacy are also of prime importance. In the process of utilizing these platforms and remote working, users unfortunately tend to give away a lot of data and permissions to these platforms and mobile applications, so much so that our private information available on our devices is easily accessible to these platforms. It has also been stated that the over passwords of these accounts are available at throw away prices on the dark web. The shift to technology in which the public use all these virtual platforms and other kinds of applications, has given rise to the reality that we tend to grant many permissions to these applications such

as screen recording, access to contacts, cameras, etc. without checking the permissions that we are granting to a particular application. Hence, to avoid or minimize the risk of placing our personal data in the hands of the wrong people, it is imperative that we are cautious while using any application or providing our details anywhere.

3 Increase in the cyber-crime cases during Covid-19 Lockdown

The Covid-19 crisis took India and the rest of the world by surprise and the simple reality is that no one was prepared to deal with education and work from home (Moreno, 2020) during lockdown. Immediately after the lockdown everyone started using these platforms with little (or sometimes even no) knowledge of the threats that may be posed by such platforms or the cyber-crimes which one may face. Cyber-crime cases flourished as a result of this ignorance. Even now, there is still a lack of awareness among many people regarding cyber-security, leaving them at substantial risk.

The current situation has underscored the issue of cyber-security and why it is crucial for everyone to be aware of the problem and to understand and to take the measures that that are prudent in order to avoid falling prey to cyber-criminals. These crimes can be divided into various categories. Some of the most common crimes witnessed presently are discussed next.

3.1 Phishing

Phishing is the most common kind of cyber-crime being experienced presently. Although not a new crime it continues to increase. Phishing happens when the victim is contacted by the attacker through a mobile, email or a text message in which the attacker poses as a legitimate institution attempting to gather private and sensitive data. It is difficult for a lay person to detect a phishing attack because it is generally guised in a different and credible form making it hard for the victim to doubt the veracity of the message. Microsoft issued an alert to its users pertaining to phishing attacks wherein emails were sent to gain remote access. There have been innumerable cases like this (Finklea, 2020).

The number of cases of phishing have increased dramatically during the pandemic (IANS, 2020) because people are in a lockdown and are fearful (Kumar, 2020) of a highly contagious virus and hence they often believe that any information (Lentchner, 2020) (mostly in forms of links) (Ahmad, 2020) they receive is valid and truthful and so they fail to check the authenticity of the information.

In the case of phishing, the username of the attacker has descriptive similarity (Pandey, 2014) to that of any reputed organisation. In addition to the Microsoft situation, another example involved emails sent in the name of WHO (World Health Organisation, 2020) (wherein a few letters were either added or a different domain listed) asking the recipient for sensitive information (World Health Organisation, 2020). In order to avoid falling prey to any such attack, one must ensure to verify the email account or website and check the information from the authentic website and report the matter in case of even slight doubt and above all, do not click on the attachment.

3.2 Fake and Fabricated URLs

There has been an increase in false URLs seeking to secure donations in the name of Covid-19 and people have been fooled into believing these URLs belong to a genuine organisation.

In one such case, the cyber-criminals or the attackers requested the victims to make donations in bitcoins. The cleverly designed plan was with the mala fide intent that tracing of bitcoins is nearly impossible and it is comparatively quite difficult to catch such attackers (Partz, 2020). Hence it is always advisable to check the link before clicking on it.

There have been instances where scams have been done by creating a post or a message stating the device owner qualifies for a Covid-19 governmental grant. The user is asked to click on a link to provide necessary (i.e. personal) details. The scam (theft) is completed when the duped user provides vital, personal information. To avoid the scam, we advise the user not to click on any link that is unexpected or is suspicious. These sites not only abscond with personal/private information but might also steal the user's money and/or may download a malware into the user's system.

3.3 Misinformation

People are under constant fear because of the pandemic (Chappell, 2020) and tend to believe any kind of news or information (whether true or false) that is circulated pertaining to the virus (Fernandes, 2020). There have been many articles and videos which went viral which either were related to some false information pertaining to the virus or which provided remedies or methods to cure the virus which were neither based upon any research nor coming from any reliable source. Criminals are often opportunists. The cyber-crime groups have seized upon this pandemic as an opportunity for themselves by exploiting peoples' fears and anxieties and providing them information which they will receive directly and which they will believe immediately like home remedies for corona virus, cures for the virus, purported benefits by the governments (Tejaswi, 2020). Such information often takes the form of false information designed to misguide the public but many times it also can take the form of phishing or fake URLs (World Health Organisation, 2020).

The public is being flooded with information from all kind of sources and it is extremely dangerous to rely upon any information except that which is coming from authentic and trusted sources (Gercke, 2012). Hence, there is a need both to create awareness among the public and to penalise the persons/institutions spreading any kind of false information.

3.4 Sexual and Verbal Abuse

The media has reported various cases on a regular basis wherein these digital platforms have been taken over by the cyber criminals/hackers for "Zoom Bombing".[4] Given the increased use by workers, students and others of video conferencing, the students, employees and all others who are using these platforms have been targeted by hackers and often face abuse online either through content which is indecent and/or through words or acts constituting online sexual abuse (Panakal, 2020).

[4] Zoom Bombing is a new term that has become prevalent only recently wherein one person tries to enter an online platform where a meeting or class is going on and interrupts the same by doing various acts such as hurling abuses, showing pornography or any other indecent image, using words or gestures to disrupt the normal functioning of the meeting or class.

The schools are making their best efforts to bring learning into students' homes and to ensure that education is not adversely impacted by this virus. Unfortunately, by using these online platforms, hackers who gain access to the online discussions are exposing students to content unsuitable for them, such as child pornography (Morris, 2020), and subjecting them to abuse (Dayton, 2020). The troubling incident that occurred Nirma University (Mehta, 2020), mentioned above, wherein the hacker entered the online class and started performing an indecent act of masturbation created headlines. Unfortunately, however, that was hardly an isolated incident and there have been multiple similar events that have created fear in the minds of audiences viewing them (Hamilton, 2020).

3.5 Online Eve Teasing

Eve teasing is a common euphemism in South Asia for sexual harassment of women in public areas by men. Since educational classes are being conducted online for both school and colleges students, there is a common practice of forming a whatsapp group of all the students for updating each other about the classes, exams etc. and such groups easily give access to the phone numbers of the girls present in the group to others (India.com, 2020). These phone numbers, which ordinarily are private, now are easily accessible at the touch of a finger. This has resulted in an increasing number of unwanted messages and calls being made at odd hours to girls and women with the intention of troubling the person receiving the message or call. This practice has also intensified during this period and left unabated may increase further in the future.

The fact that contact details and other data of people have become so readily available during this lockdown means that this private data is landing into the wrong hands and hence causing a lot of inconvenience to people, especially to females. Young girls, in particular, have seen their privacy breached and they have been bombarded with unwanted calls and text messages at odd hours (Mittal, 2020). Needless to say, this is very stressful for the recipients of this content.

3.6 Sextortion

Sextortion is a crime that occurs when someone threatens to distribute another person's private and sensitive material if that person refuses to provide them images of a sexual nature, sexual favours, and/or money. The instances of sextortion also have increased dramatically recently. The attackers in this form of crime send nude/semi-nude images of females to the victim and then start a video call with the victim. Once the call is answered, the victim would see a female on the other side of the screen who is naked or is showing some of her body part. The attacker then captures screenshots of the call. Another mode adopted by the attackers is to first befriend the victim on social media and then exchange phone numbers and after talking for a few weeks, they ask the victim for virtual sex which is then recorded without knowledge of the victim (Shinde, 2020). These screenshots/recordings are then used by the attackers to blackmail the victim in order to extort money and/or sex (TNN, 2021). These attackers specifically target wealthy businessmen or the senior officials of firms who are likely to give in to their demands easily.

3.7 Cyber-Bullying

The impact of cyber-bullying on the victim can range from mild to severe. The severe variety can cause the victim so much stress and anxiety as to lead to suicide. Schools, colleges and other organisations have been actively conducting workshops and online programs to create awareness regarding cyber-abuse and cyber- bullying (Asam & Samara, 2016). Such efforts are commendable and must continue.

In May 2020, the Bois Locker Room case generated massive headlines after a schoolgirl on social media alleged the she was sexually harassed by her classmate. The death of a seventeen-year-old in Gurugram has also been linked to the controversy. This has led to many debates concerning the reasons behind such incidents and how best to combat them. Some psychologists have suggested cyber-bullying is the result of a lack of sex education, which unfortunately is still considered as a taboo in India. (Ravi, 2020) Unquestionably, the current lack of sex education is the prime reason for such incidents and there is definitely a need of sex education among teenagers; however, another key factor is that young children are also exposed to unfiltered information not appropriate for them (Binder, 2016).

Due to the lockdown, the young generation has easy access to mobile devices and to other forms of technology as their classes and many other activities are being held online. In the past, parents were able to better limit young peoples' usage of this technology. The pandemic and resulting lockdowns has made parents' job in this respect much more difficult, if not impossible. Consequently, our children now have easy access to all sort of unfiltered content and too often build communication channels with others offering all kind of wrong influences. For example, children often connect with unknown people over the internet who might tutor them or threaten them to either get sensitive information regarding their family or make them commit some act.

Hence, there is a need of constant awareness (Notar & Roden, 2013) workshops by schools (Ludlow, 2010) and other organisations for students as well as parents. There also is a need to monitor the students and provide them with regular counselling because in this virtual mode of teaching it is difficult to constantly monitor the behaviour of any child.

3.8 Malware Attacks

This is kind of a cyber-crime in which a malicious link or software performs actions on the victim's system without the victim's knowledge. The modus operandi of these is similar to that of computer viruses. Anyone can fall prey to such attacks merely by clicking on infected email attachments or links (Interpol, 2020) and these attacks are sometimes precursor's to more serious cyber-crimes.

3.9 Ransomware

Ransomware falls into the category of malware attacks. Ransomware constitutes a specific kind of malware wherein the attackers encrypt the system or the files of the victim, thereby corrupting the system, and then demands ransom to restore the victim's system. Hospitals and other medical institutions are at highest risk for these attackers because of the medical emergent situation going on in India (and the rest of the world) and because the services rendered by hospitals are urgently required and accordingly they simply cannot afford to remain paralyzed and without use of their data and system for any extended period of time. In other words, attackers fully realize that through ransomware they essentially are placing a gun at the head of the

victim (hospital) and can easily extort money from them. Obviously, however, hospitals are not the only large institutions at risk. Attackers are indiscriminate and prey on any vulnerable victims.

4 Legal Aspect of Cyber-Crimes

The IT Act 2000 is the legislation in India which presently deals with cyber-crimes apart from certain provisions which are available in the Indian Penal Code. Though the Act attempts to address the issues of cyber-crimes, it unfortunately contains many loopholes and lacunas that permit bad actors to continue preying upon internet users. The Act quite simply needs urgent reform in order to better address and cope with modern day technologies such as artificial intelligence, cloud, quantum computing etc. (Ghosh, 2019). Apart from that already mentioned above, the cyber-criminals are constantly recalibrating their methodologies and developing new ways and loopholes to commit crimes. The provisions of the now-outdated Act are inadequate to deal with these new methodologies and the new modes of crimes. Hence the present Act needs to be amended to comprehensively address the matters discussed in this article, among other things, and to close the loopholes and the lacunas which exist in the now outdated (over twenty-year-old) Act. There is also a need to spread awareness pertaining to the legal remedies which are available to people who have been victims of cyber-crimes and also to toughen penalties and liberalize the remedies.

5 Conclusion

The pandemic has impacted everyone's life in various ways and uncertainty remains as to how long it will take for normal life to return. The pandemic has made one thing clear. The entire concept of going digital, including virtual learning and work from home, is here to stay and it will be the new normal. It cannot be denied that the virtual learning and online meetings, i.e. work from home, is still an evolving process and there is much more to learn about the process. Clearly, these platforms provide great benefits and if made secure can prove to be great assets for everyone. However, there is a need to make these platforms secure for use and measures must be taken to help curb the cyber-crimes mentioned hereinabove (not to mention likely future crimes that industrious hackers will no doubt devise given the benefit of time).

The primary step should be intensifying efforts to raise awareness in the society regarding cyber-security, to everyone, but especially among the most vulnerable sectors of the society like children, the elderly, and novices to the use of technology who are completely unaware of the threats that accompany these lucrative digital platforms. Businesses, government agencies and other organisations also need to corroborate and to take appropriate initiatives to provide cyber-security training for their employees. We must recognize that the traditional workplace has now moved beyond the four walls of the formal office used in the past to online work and hence adequate training and measures need to be imparted as a necessary first step towards cyber-security.

Secondly, more robust mechanisms must be established to deal with the cases of cyber-crime because in many cases it is difficult to trace the real culprits and mitigate the damages done. Appropriate mechanisms must be instituted in order to prevent and track cyber-crimes. We recommend that a committee of qualified professionals should be formed in order to develop specific strategies to tackle the situation.[5]

Thirdly, since the cyber-crimes have grown exponentially recently and there are new crimes constantly evolving, there is an urgent need to strengthen the existing, outdated legislations to tackle the present situation. Additionally, the cyber cells present needs to be more active (Gercke, 2012).

Fourthly, there must be appropriate monitoring on the spreading of false information because such information not only misleads the public but also creates fear in their minds. Especially during the time that we are going through at present, any false information which is coming from unreliable sources should be filtered and strict penalties should be imposed on persons or organizations spreading such news. Everyone is already in a state of fear due to the pandemic and false and misleading information impacts people more negatively at present.

[5] Importance of Cyber Security, (January 10, 2020), https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf

Fifthly, what is most important is that anyone who encounters instances of cyber-attacks should report them immediately to the authorities because many such cases go unreported and hence provide cyber-criminals with further opportunities to carry on with their nefarious deeds (Dhupdale, 2011).

Lastly, each of us should be alert and should also take adequate measures to avoid any kind of cyber-crime. Simple measures like disabling the permissions of the softwares, checking authenticity of the information before sending it forward to others, not providing our personal sensitive information to anyone - especially over a phone call or email - creating awareness among children and other vulnerable users by providing them counselling in order to help prevent them from falling prey to cyberbullying and other crimes. These relatively small measures that we can all take, and also by constantly maintaining our vigilance, will help us greatly in achieving cyber-security.

In conclusion, both the Edtech industry and work from home culture are here to stay as a result of the pandemic, which has introduced us to this entire culture. Virtual learning and meeting platforms have been crucial in enabling everyone to carry on their work to a large extent. However, we each must be mindful of the threats posed by use of these platforms. There needs to be better public awareness of problems associated with the online platforms and steps we call can take to help combat them. Of course, industry must take appropriate steps to help make these platforms more secure. Going forward, these platforms will continue to prove to be valuable assets to the entire education and corporate sectors.

Declaration

We, Niteesh Kumar Upadhyay and Mahak Rathee declare that this paper entitled is our original work and has neither been published nor is under consideration for publication anywhere else in any form.

References

Ahmad, T. (2020) Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity, retrieved from: https://www.researchgate.net/publication/340443250_Corona_Virus_COVID-19_Pandemic_and_Work_from_Home_Challenges_of_Cybercrimes_and_Cybersecurity (11 November 2021).

Asam, A. & Samara, M. (2016) Cyberbullying and the law: A review of psychological and legal challenges, *Computers in Human Behavior*, 65, pp. 127-141, doi: 10.1016/j.chb.2016.08.012,

retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0747563216305775 (November 10, 2021).

Anonymous (2020) Coronavirus impact: Amid 'work from home' trend cyber security risk increases, *Livemint*, 28. 3. 2020, retrieved from: https://www.livemint.com/news/india/coronavirus-impact-amid-work-from-home-trend-cyber-security-risk-increases-11585391974998.html (December 13, 2021)

Anonymous (2020) Bois Locker Room chat group questioned, *Hindustan Times*, 5. 5. 2020, retrieved from: https://www.hindustantimes.com/cities/police-take-note-of-rape-threats-on-social-media-group-of-schoolboys/story-loYqRytz0h5PMSIfsirVKI.html (November 21, 2021)

Anonymous (2020) Work-from-home checklist during the Coronavirus Pandemic, *The National Law review*, 22(80), retrieved from: https://www.natlawreview.com/article/work-home-checklist-during-coronavirus-pandemic (November 21, 2021).

Bedi, A. (2020) No gadgets, no studies: What online classes mean for 16 lakh poor students in Delhi schools, retrieved from: *The Print*, 22. 4. 2020, retrieved from: https://theprint.in/india/education/no-gadgets-no-studies-what-online-classes-mean-for-16-lakh-poor-students-in-delhi-schools/406837/ (November 17, 2021).

Binder, D. (2016) A Tort Perspective on Cyberbullying, *Chapman Law Review*, 19(2), pp. 359-372, retrieved from: https://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1372&context=chapman-law-review (November 11, 2021).

Chappell, B. (2020) U.N. Chief Targets 'Dangerous Epidemic of Misinformation' on Coronavirus, *NPR*, 14. 4. 2020, retrieved from: https://www.npr.org/sections/coronavirus-live-updates/2020/04/14/834287961/u-n-chief-targets-dangerous-epidemic-of-misinformation-on-coronavirus (November 11, 2021).

Chowdhary, S. (2020) Cybercrime in the time of Covid- what firms need to do for security, *Financial Express*, 6. 5. 2020, retrieved from: https://www.financialexpress.com/industry/technology/cybercrime-in-the-time-of-covid-what-firms-need-to-do-for-security/1949190/ (November 12, 2021).

Crisanto, J. & Prenio, J. (2020) Financial crime in times of Covid-19-AML and cyber resilience measures, *BIS*, retrieved from: https://www.bis.org/fsi/fsibriefs7.pdf (November 12, 2021).

Dayton, J. (2020) Zoom Bombing and Online Sexual Misconduct: What are your options?, *ADZ Law*, 16. 4. 2020, retrieved from: https://www.adzlaw.com/victim-advocacy/2020/04/16/zoom-bombing-and-online-sexual-misconduct-what-are-your-options/ (November 12, 2021).

Desair, R. (2020) Cybercrime in India Surges Amidst Coronavirus Lockdown, *Forbes*, 14. 5. 2020, retrieved from: https://www.forbes.com/sites/ronakdesai/2020/05/14/cybercrime-in-india-surges-amidst-coronavirus-lockdown/#6e110690392e (November 11, 2021).

Dhupdale, V. (2011) Cyber Crime and Challenge Ahead, retrieved from: https://www.researchgate.net/publication/265166983_Cyber_Crime_and_Challenges_Ahead (November 11, 2021).

ECSO (2020) ECSO Barometer 2020: "Cybersecurity in light of Covid-19", *European Cyber Security Organisation*, retrieved from: https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf (November 13, 2021).

Earley, K. (2020) Google and Facebook extend work from-home policies to 2021, *Silicon Republic*, 11. 5. 2020, retrieved from: https://www.siliconrepublic.com/companies/google-facebook-remote-work-until-2021 (November 13, 2021).

Fernandes, S. (2020) Scientists discuss ways to bust misinformation and fake news about Covid-19, *Hindustan Times*, 27. 3. 2020, retrieved from: https://www.hindustantimes.com/mumbai-news/scientists-discuss-ways-to-bust-misinformation-and-fake-news-about-covid-19/story-CB3npfRhR7PVcKmI3iZuQL.html (November 13, 2021).

Finklea, K. (2020) Covid-19: Cybercrime Opportunities and Law Enforcement Response, *Congressional Research Service*, retrieved from: https://crsreports.congress.gov/product/pdf/IN/IN11257 (November 13, 2021).

Gayal, S. & Maniar, P. (2020) Covid-19 crisis- the impact of cyber security on Indian Organisations, *PWC*, retrieved from: https://www.pwc.in/assets/pdfs/services/crisis-management/covid-19/covid-19-crisis-the-impact-of-cyber-security-on-indian-organisations.pdf (November 21, 2021).

Gercke, M. (2012) Understanding CyberCrime: Phenomena, Challenges and Legal Responses, *ITU*, retrieved from: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (November 21, 2021).

Ghosh, S. (2019) India's IT Act 2000 a toothless tiger, *CSO*, retrieved from: https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html (November 21, 2021).

Hamilton, I. (2020) Researchers found and bought more than 500,000 Zoom passwords on the dark web for less than a cent each, *Business Insider*, 14. 4. 2020, retrieved from: https://www.businessinsider.in/tech/news/researchers-found-and-bought-more-than-500000-zoom-passwords-on-the-dark-web-for-less-than-a-cent-each/articleshow/75138495.cms (November 21, 2021).

IANS (2020) COVID-19-related phishing attacks up by 667%: Report, *Economic Times*, 27. 3. 2020, retrieved from: https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322 (November 15, 2021).

India.com (2020) Your privacy may be at Risk: WhatsApp Group Chat Links Available on Google Search, *India.com*, 22. 2. 2020, retrieved from: https://www.india.com/technology/your-privacy-may-be-at-risk-whatsapp-group-chat-links-available-on-google-search-3950651/ (November 15, 2021).

Interpol (2020) Cyberthreats are constantly evolving in order to take advantage of online behaviour and tends. The COVID-19 outbreak is no exception, *Interpol*, retrieved from: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (November 15, 2021).

ILO (2020) COVID-19 and the world of work: Impact and policy responses, *ILO*, retrieved from: https://www.ilo.org/wcmsp5/groups/public/---dgreports/dcomm/documents/briefingnote/wcms_738753.pdf (November 15, 2021).

Kumar, A. (2020) Coronavirus pandemic: Cyber criminals and scammers prey on Covid 19 fears to scam people, *India Today*, 22. 4. 2020, retrieved from: https://www.indiatoday.in/technology/features/story/coronavirus-pandemic-cyber-criminals-and-scammers-prey-on-covid-19-fears-to-scam-people-1669926-2020-04-22 (November 12, 2021)

Lallie, H. (2020) Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber- Crime and Cyber- Attacks during the Pandemic, retrieved from: https://www.researchgate.net/publication/342377769_Cyber_Security_in_the_Age_of_COVID-19_A_Timeline_and_Analysis_of_Cyber-Crime_and_Cyber-Attacks_during_the_Pandemic (November 12, 2021)

Lentchner, C. (2020) Technology is not immune to Covid-19 Cyber Fraud, *Pilsbury Law*, retrieved from: https://www.pillsburylaw.com/en/news-and-insights/covid-19-cyber-fraud.html (November 12, 2021).

Ludlow, B. (2010) Cyber Law: Maximiszing Safety and Minimizing Risk in Classrooms, retrieved from: https://www.researchgate.net/publication/286649742_Book_and_Software_Review_Cyber_Law_Maximizing_Safety_and_Minimizing_Risk_in_Classrooms (November 12, 2021)

Mani, G. (2020) Online classes: Poor students in Delhi struggle due to lack of internet connections, *The New Indian Express*, 18. 5. 2020, retrieved from: https://www.newindianexpress.com/cities/delhi/2020/may/18/online-classes-poor-students-in-delhi-struggle-due-to-lack-of-internet-connections-2144781.html (November 18, 2021)

Mehta, O. (2020) Students shaken by hacker's lewd act, *Ahmedabad Mirror*, retrieved from: https://ahmedabadmirror.indiatimes.com/ahmedabad/crime/students-shaken-by-hackers-lewd-act/articleshow/75260597.cms (November 18, 2021).

Mittal, P. & Mathur, V. (2017) Right to Privacy: Data sharing by Google, WhatsApp, Facebook can now be questioned, *Livemint,* retrieved from: https://www.livemint.com/Technology/Vtf6ZybtgIugjQX9U7TMgL/Right-to-Privacy-Data-sharing-by-Google-WhatsApp-Facebook.html (November 18, 2021).

Moreno, J. (2020) Covid-19 Update: Cybersecurity and Data Privacy Best Practices Remain Critical during the Coronavirus Pandemic, *The National Law Review*, 3. 4. 2020, retrieved from: https://www.natlawreview.com/article/covid-19-update-cybersecurity-and-data-privacy-best-practices-remain-critical-during (November 29, 2021).

Morris, S. (2020) Zoom hacker streams child sex abuse footage to Plymouth children, *The Guardian*, 7. 5. 2020, retrieved from: https://www.theguardian.com/society/2020/may/07/zoom-hacker-streams-child-sex-abuse-footage-to-plymouth-children (November 20, 2021)

Nappinai, N. (2017) Cyber Laws Part II: A guide for victims of Cyber Crime, *The Economic Times*, 3. 11. 2011, retrieved from: https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr (November 18, 2021).

Notar, C. & Roden, J. (2013) Cyberbullying: A review of the Literature, *University Journal of Educational Research*, 1(1), pp. 1-9, doi: 10.13189/ujer.2013.010101, retrieved from: https://files.eric.ed.gov/fulltext/EJ1053975.pdf (November 22, 2021).

Panakal, D. (2020) Who's Zoomin Who?, *The National Law Review*, 6. 4. 2020, retrieved from: https://www.natlawreview.com/article/who-s-zoomin-who (November 22, 2021).

Pandey, K. (2014) Laws relating to Cyber Crimes in India, retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412469 (November 17, 2021).

Partz, H. (2020) Scammers impersonate World Health Organisation to steal BTC Covid-19 Donations, *Cointelegraph*, 19. 3. 2020, retrieved from: https://cointelegraph.com/news/scammers-impersonate-world-health-organization-to-steal-btc-covid-19-donations (November 17, 2021)

Rama, N. & Mehta, O. (2020) Nirma Zeroes in on perv hacker's link, *Ahmedabad Mirror*, retrieved from: https://ahmedabadmirror.indiatimes.com/ahmedabad/crime/nirma-zeroes-in-on-perv-hackers-link/articleshow/75281722.cms (November 17, 2021).

Ravi, S. (2020) Bois Locker Room, a reflection of an existing mindset, *The Hindu*, 21. 5. 2020, retrieved from: https://www.thehindu.com/news/cities/Delhi/bois-locker-room-a-reflectionof-an-existing-mindset/article31638044.ece (November 17, 2021).

Saleh, T. (2020) CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware, *Domaintools*, retrieved from: https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware (November 17, 2021).

Shinde, S. (2021) Sextortion cases on rise in Pune, *Hindustan Times*, 18. 8. 2021, retrieved from: https://www.hindustantimes.com/cities/pune-news/sextortion-cases-on-the-rise-in-pune-101629311260646.html (November 21, 2021).

Tejaswi, M. (2020) Organised crime using COVID-19 for launching phishing attacks: KPMG, *The Hindu*, 14. 4. 2020, retrieved from: https://www.thehindu.com/sci-tech/technology/organised-crime-using-covid-19-for-launching-phishing-attacks-kpmg/article31338778.ece (November 20, 2021).

TNN (2021) This extortion gang targeted 200 in 2 years, made Rs 22 crore, *Times of India*, 23. 10. 2021, retrieved from: https://timesofindia.indiatimes.com/city/ghaziabad/this-sextortion-gang-targeted-200-in-2-years-made-rs-22-crore/articleshow/87214650.cms (November 21, 2021).

UNODC (2020) Cyber Crime and Covid19: Risks and Responses, retrieved from: https://www.unodc.org/documents/Advocacy-Section/UNODC__CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf (November 20, 2021).

Walker, S. (2020) Covid-19 and Crime: A response develops at the UN, *Global Initiative*, retrieved from: https://globalinitiative.net/wp-content/uploads/2020/06/Covid-19-and-crime-A-response-develops-at-the-UN.pdf (November 20, 2021).

Wallender, A. (2020) Covid-19 Tests Limits of Union Negotiations via Online Chat, *Bloomberg Law*, 16. 4. 2020, retrieved from: https://news.bloomberglaw.com/daily-labor-report/covid-19-tests-limits-of-union-negotiations-via-online-chat (November 17, 2021).

Wolters, K. (2020) Coronavirus and Cyber Crime, KPMG, *KPMG*, retrieved from: https://assets.kpmg/content/dam/kpmg/nl/pdf/2020/services/coronavirus-and-cyber-security.pdf (November 20, 2021).

World Health Organisation (2020) Beware of criminals pretending to be WHO, *WHO*, retrieved from: https://www.who.int/about/communications/cyber-security(November 17, 2021).

World Health Organisation on Coronavirus, (2020) retrieved from: https://www.who.int/health-topics/coronavirus#tab=tab_1 (November 17, 2021).