Horizons of Holistic Education
April-June-2021, 8 (2), 64-72

p ISSN : 2349-8811
eISSN : 2349-9133

A Review on Cyber Crime: Some Educational Suggestions to Overcome

Prof. Manoj Kumar Saxena
School of Education
Central University of Himachal Pradesh
Dharamshala (HP)
drmanojksaxena@gmail.com

Nitika Sharma
Research Scholar
School of Education
Central University of Himachal Pradesh
Dharamshala

Received: 10.06.2021 Accepted: 25.06.2021

Abstract

In the modern era, advancement in technology made people's life easy and comfortable as well as make prone to cybercrime. The young generation who frequently entering in to the cyber world, fail to understand the harms of internet, are most susceptible to become the victim of cybercrime or may be indulged in it unknowingly. There can be some motivating factors behind the decline of cybercrimes or such crimes can also happen inadvertently. Cybercrimes are seriously affecting today's younger generation and society in various forms such as: economically, psychologically and educationally. To prevent cybercrimes, it is necessary to analyze each type of cybercrime and understand their impact on different areas of the society. So, the present paper will provide an understanding of awareness of cybercrimes and cybersecurity, its impacts on youth. An attempt has also been made to give some preventive measures to overcome this serious issue.

Keywords: *Cybercrime, Cybersecurity, Awareness, Youth, Educational Suggestions*

Introduction

Due to the technological revolution, human life has changed upto great extent (Gihar, 2006). In the 21st century, Indian youth is living in a smart era where all are influenced by the internet. Students use the internet for various purposes such as academic, social, entertainment, shopping etc. The appearance of prevalent, reasonable and wireless networking has led to the extensive distribution of ICT devices that permit to use of social networking sites and the internet anytime and anywhere. ICT devices have become very important devices that are being used in every field such as education, commerce, entertainment, banking, corporate etc. (Saxena et al., 2019). Online behaviour comprises of the capabilities and skills to converse, generate, collaborate, share and expand the information in the form of text messages, pictures and audio-visuals among users of social networking sites. The usage of the internet and social media bring a change in the way of communication, interaction, investigation, sharing and socialization among students in educational institutions. In this stage of living, the digital platform has become a means for every young person to interact and stay busy (Saxena& Singh, 2020). Not only youth and employees have been influenced by this era of digitalization, but new technical devices are also being used by senior citizens on a large scale. There has been a great shift in the skills needed for a successful life in the present times. Work from home is being promoted during the Covid-19 pandemic. Cyberspace provided so many opportunities for people working in different organizations which require a cybersecurity culture. But cybersecurity culture can be affected as cybercrime exploits all online opportunities (Georgiadou et al., 2021). The Internet has entered every realm of life facilitated through smartphones and other devices. Technical factors such as 'google it, download, upload, apps, subscribe, like' are used quite frequently by the young generation. Most college students do not like to spend much time with books in the library. Instead of going library, students prefer suitable online resources to complete the projects or assignments given by the teachers, because they trust in time management more than performance (Mathias et al., 2018). Online availability of study content as per the convenience of the students has cramped their reasoning & logical power and eradicate inventive thoughts. Various inventions in the field of technology have given several benefits to youth but on the other hand, they may be the victim of cybercrime and also due to ignorance or knowingly they may indulge in cybercrime. Cybercrime victimization, online scam or harassment has its concern especially with the younger generation who were active users of the internet (Oksanen&Keipi, 2013). Today's younger generation is mainly victims of cybercrime. All the aspects such as age, economic status, psychological and social status etc. are all related to cybercrime victimization. One of the push factor for a younger generation to get involved in cybercrime is fear of unemployment (Igba et al., 2018). Youth at this innocent age are not aware of cyber offences. The most active segment of the digital population is the youth and also the most susceptible to be attacked through cybercrime as victims. On the other side of the crime, it's again the youth who are in majority as violators and attackers (Khan, 2019). The important thing to note is that cybercrimes are directly free from fear of law enforcement and witnesses. Cyberspace has created an environment where safe and profitable criminal incidents are taking place (Alansari et al., 2019). Cybercrimes take place due to inadvertence and lack of understanding of cybersecurity. In this time of intense and unrestrained digitization of modern lives, it is imperative to be aware of the various threats that one can face. Cybercriminals have taken full advantage of the dreadful economic and social conditions created by the Covid-19 pandemic (Lallie et al., 2020). Platforms offering online space and users of this space both share equal responsibility to protect the digital world.

Cyber Crime

Cybercrime and conventional crime are not much different from each other as both violate the rules of law. Such actions which are against the reliability, privacy and security of computer data or various types of software fall under the category of cybercrimes. In general, cybercrimes are those criminal activities under which ICT devices (computer and digital equipment) are used to commit a crime to damage the corporate sector, government data, business, digital infrastructure and harm the person etc. The Oxford Reference Online defines 'cybercrime' as the crime committed over the Internet. According to Thomas and Loader, (2000) cybercrime is "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".

Different types of cybercrime are:

1. **Online Harassment:** When a person is continually and doggedly harassed or stalked by online mail, messaging or different digital platforms by criminals which can have a bad effect on the victim's life, emotional and psychological state.
2. **Cyber Bullying:** when a person is abused and humiliated by online activities using the internet and electronic media.
3. **Online Child Pornography:** Online child pornography is a type of cybercrime by which pedophile using computer devices to share out prohibited media and sexually exploitation of children.
4. **Hacking:** hacking is an act of digital obstruction in which criminal can hack the personal data of a person, institution, government department etc. through illegal access of electronic equipment or their account on social sites such as Facebook, WhatsApp, Instagram, and Twitter etc.
5. **Identity Theft:** It is a type of cybercrime under which criminals misuse a victim's identical information and cause him personal or financial loss.
6. **Credit/Debit Card Fraud:** In this type of cybercrime the criminal fraudulently steals the credit card/debit card numbers through the insecure website or wrong information and damages the victim's property and money.

Awareness of Cyber Crime and Prior Computer Knowledge

Cybercrime is a serious problem in today's digital world. It is essential to understand different types of cybercrimes and be aware of their future safeguard (May &Bhardwa, 2018 as cited in Hamsa et al., 2018). Árpád (2013) conducted a software (not real) installation test to identify the awareness level of students regarding cybercrimes and found that more than 80% of students agreed to install a harmful application on the computer and surprising fact study examined that most of the students related with the field of computer science**.** In another study it has been observed that even students are proficient in working with computers and fully aware of cybercrimes, it does not mean that they work with attentiveness in the cyber world and can avoid being a victim of cybercrime (Tibi et al., 2019). Lack of awareness is one of the reasons for increasing cyber delinquency in India because most of the youth are unaware that they are violating others' rights for their entertainment e.g. digital piracy or copyright infringement (Kumar and Manhas, 2021). Similarly, Pradeep & Arjun (2018) observed that young internet users have negligence and lack of awareness regarding the security of their laptop, computer or mobile data. Negligence is a feature of human behaviour, so due to negligence and inattention, cybercriminals can hack the computer and pose cyber threats (Kumar &Manhas, 2021).

Influence of Gender, Age and Knowledge on Cyber Crime Awareness

Hasan et al., (2015) reveled that factors such as gender, age and knowledge have a great influence on the awareness level of cybercrimes.Female students have a higher level of awareness about cybercrimes than male students. In addition, the authors also reported that students with an understanding of cyber-crimes were highly aware of cybercrime. Correspondingly, a study proved that the young generation lies between the age group of 15-30, most of the active user of internet and they prefer online services such as; online transaction, online shopping, study material etc. But, most young internet users were felt insecure about their safety while working online (Kumbhar and Gavekar, 2017).

Awareness about Particular Types of Cyber Crime

Most of the students were having an awareness of the specific type of cybercrime rather than other types of cybercrimes. Sreehari et al., (2018) analyzed that college students have no idea about the safety of their information while being online and maximum of them sometimes take delivery of spam messages and calls but hardly anyone tried to report it to the cybercrime police station to prevent it from occurring again. Similarly, in another study, the analysis of data indicated that most of the youth were just aware of what is cybercrime and some of them having awareness of hacking, piracy and phishing but the most dangerous threats like Trojans and Virus attack which can generate wide damage to data including identity disaster as well were not identified much by the students (Khan, 2019). According to Pradeep & Arjun, (2018) "Apart from hacking, many cyber users are not aware of various cybercrimes such as darknet crimes, copyright infringement, cyberbullying, phishing attack, child pornography, spoofing, domain-squatting etc".

Motivational Factors and Indulgence of Youth in Cyber Crime

Along with the awareness of cybercrime, various studies have also found that youth were involved in cybercrime such as online drug trafficking, cyberstalking, online hacking, identity theft, child pornography etc. There are financial and psychological factors that motivated the youth to become a hacker (Árpád, 2013). Okeshola&Adeta,(2013) were of the opinion that the motivational factors that encouraged individuals to involve in cybercrime varies such as financial gain, gratitude, fame, easy to commit, intellectual hunt, frustration, revenge, unsatisfied from what they earn, lack of good moral education from parents and guardians etc. Cybercriminals take advantage of psychological and demographic factors as the terrible Covid-19 pandemic has incited cyber fraud (Monteith et al., 2021). Digital proficiency and ravenousness, unemployment fear, inventiveness, desire to make money and a place to install their technical skill are those factors which motivated the youth to commit the cybercrime. Most of the youth have accepted that unemployment fear acts as a push factor to get involved in cybercrime (Igba et al., 2018).

Impact of Cyber Crime on Youth

As digitalization brought a positive change but it has also a negative impact on youth (Saxena& Chauhan, 2021). There may be some motivating factors behind cybercrime or it can happen without intention, cyber-attacks that are done intentionally are considered as cybercrime and have a profound effect on society such as economic loss, mental stress and fatal to national security etc. (Saini et al., 2012). Cybercrime is an existing trend and most young people reported being victims of cybercrime. Cybercrime victimization deals with offline disturbance or viable psychosocial troubles and it is necessary to understand the possible mental harms of the younger generation which are overlapping with online experiences and approach offline (Oksanen&Keipi,2013). The college student use the Internet for different purposes, mainly classified as e-shopping, web publishing, virtual interaction, and digital downloading. As predictable, these activities were correspondingly related to fear of various types of cybercrime i.e. malware with digital downloading, digital piracy with web publishing, cyberbullying with virtual interaction and, online scam with online shopping (Yu, 2014). Male gender, younger age, urban residence, unemployment and less active offline social life were major predictors for cybercrime victimization (Näsi et al., 2015). The most common risk factors faced by adolescent girls through online media are a violation of body privacy, online sexual harassment, eve-teasing, molestation, cyberstalking, and other harassments like spreading rumours and gossips about the girl child with the help of social media for embarrassing and humiliating her (Johnson &Manickavasagam, 2020).

Cyber Security Awareness & Youth

In this digital age, cybersecurity awareness and protection is very important for youth. The need of the hour is that making individuals aware of cybercrime and cybersecurity and giving them the tools and knowledge that they need to protect themselves. During this struggling era of the Covid-19 pandemic, cybersecurity is also deliberated as a digital pandemic as many people started online working for the very first time (Ramadan et al., 2021). With the development of advanced technology, the field of cybersecurity is facing a variety of challenges. Youth are easily fascinated by this new digital world and cybercriminals tempting them by misusing their personal information and required data (Potgieter, 2019). People must take suitable actions especially in dealing with social media to prevent them from cybercrimes (Reddy & Reddy 2014). Similarly,in another study, it has been examined that most of the students were active users of social media and more unsafe in social networks despite phishing and virus attack because most of the students were aware of virus attack and phishing emails/messages in any form and very few students responded to those E-mails/messages because they are aware of false E-mail/messages (Senthilkumar&Easwaramoorthy, 2017). As students grow older; they were more tending to use the Internet and there is a tendency of how things change in terms of the way students use the Internet and for what; hence, it is essential to educate youth on diverse problems and various usage stages (Zahri et al., 2017). Timing of usage of the internet is increasing among youth and they are constantly revealing their bank details through online money transaction and with negligent behaviour, their susceptibility increased to malware/spyware attack through downloaded content which led to cybercrime victimization and less awareness about cybersecurity (Rathod&Potdar, 2019).

Educational Suggestions to Overcome Cybercrime:

The review made in the paper leads to the conclusion that the cybercrime is a threat for the youths who may be the students or the working persons. These youths may be the victims of cybercrime or the knowingly or unknowingly offenders. To overcome from the cybercrime, the following educational suggestions may be helpful:

- It is necessary to understand the behaviour of a person who addicted to committing cybercrime and their impact on society as it will help to show suitable means to reduce cybercrime. Cyberlaw, cyber education and formulating policies related to cybersecurity, by adopting these three methods cybercrimes can be reduced.
- Education is the most important weapon for literacy, as such workshops and seminars related to cyber safety should be organized as per time and requirement so that the youth can secure their personal information and stay away from cybercrime.
- Awareness of cybersecurity is an incessant process that needs to be supported so that any cybersecurity-related threat can be avoided. It is necessary to carry out a special and planned cybersecurity operation for the younger generation.
- Cybercrime is a dangerous problem and our society is falling victim to it day by day. Education should be seriously involved in its anti-fight and all cybersecurity-related courses should be implemented at all educational levels. Manuals should be written or rewritten to present the current and the upcoming generations to effectively take up the fight against cybercrime.
- Only educational institutions can give a relevant education to the youth on how to engage in online activities safely and avoid being a victim of cybercrime.

- Educating the students, right from the school level about the dangers of cybercrime has to be given prior importance and regulations that deal with cybercriminals should be strengthened to bring a sense of safety among the internet users.
- Educational institutions should aware of students as well as their parents for the accurate and safe use of online gadgets.
- Along with the basics of ICT, cybersecurity should also be a part of the curriculum from school level to higher-level education.
- Internet facilities provided by the government to educational institutions should be secure.
- Coordination should be established between cyber cells and IT professional companies by cyber law enforcers to trace out the cybercriminals.
- It is the responsibility of Academic institutions to educate youth with interesting and useful education related to cybersecurity on regular basis and adopt a conscious culture in the institutions.

Conclusion

The beginning of the latest technologies always presents an early challenge for society, the education sector and law enforcement agencies. Government and our educational system should take proper strategies and techniques about protecting from cybercrime. Youth and people who are using the internet frequently should be taken preventive measure like work safely and carefully, increase awareness level, develop their mental ability and perception level for protecting this criminality. Responsibilities must be given to the website owners or authorities in shielding their sites by improving security system, using password and establishing a monitoring system. By analyzing various studies, it is found that cybercrime can be protected by increasing awareness level among youth through the education system, developing the policing system by the government and punishment enforced by law.

References

Alansari, M. M., Aljazzaf, Z. M., &Sarfraz, M. (2019).On Cyber Crimes and Cyber Security.In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41.IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001. Retrieved from https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Security

Árpád, I. (2013). A greater involvement of education in fight against cybercrime. Procedia-Social and Behavioral Sciences, 83, 371-377. Retrieved fromhttps://www.researchgate.net/publication/271522001_A_Greater_Involvement_of_Education-_in_Fight_Against_Cybercrime

Georgiadou, A., Mouzakitis, S., &Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 1-20. Retrieved from https://link.springer.com/article/10.1057/s41284-021-00286-2

Gihar, Sandhya (2006). Teaching of Environmental Components in Communication Age through Video Intervention Strategy: Guidelines for TTIs, in Dey, Saxena&Gihar (ed.) Teacher Education in Communication Age, Wisdom Publication, Delhi, pp 97 – 103.

Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. Journal of

Social Sciences, 11(4), 395. Retrieved fromhttps://www.researchgate.net/publication/284510743_Perception_and_Awareness_of_Young_Internet_Users_towards_Cybercrime_Evidence_from_Malaysia

Igba, I. D., Igba, E. C., &Nwambam, A. S. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. International Journal of Applied Engineering Research, 13(2), 1144-1154. Retrieved from https://www.ripublication.com/ijaer18/ijaerv13n2_43.pdf

Johnson, J., &Manickavasagam, B. (2020).Cyber Crimes against Female Undergraduate Students of Thiruvananthapuram City, Kerala.Our Heritage, 68(1), 2604-2612. Retrieved from https://archives.ourheritagejournal.com/index.php/oh/login?source=%2Findex.php%2Foh%2Farticle%2Fdownload%2F986%2F945

Khan, Anisa (2019). A Study Of Awareness On Cybercrime Amongst Senior College Students Of Pune City. International Journal of Research and Analytical Reviews (IJRAR),Volume 6, Issue 1, pp.167-172 Retrieved from https://www.researchgate.net/publication/334670442_A_Study_Of_Awareness_On_Cyber-Crime_Amongst_Senior_College_Students_Of_Pune_City

Kumar, Sanjeev&Manhas, Anupam. (2021). Cyber Delinquencies: An Indian Perspective. Vol-44. 1-6. Retrieved from https://www.researchgate.net/publication/349311630_Cyber_Delinquencies_An_Indian_Perspective

Kumbhar, Manisha&GavekarVidya (2017). A Study of Cyber Crime Awareness for Prevention and its Impact. International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 03, Issue 10, October. Retrieved from https://www.ijrter.com/papers/volume-3/issue-10/a-study-of-cyber-crime-awareness-for-prevention-and-its-impact.pdf

Lallie, Harjinder Singh, Shepherd, Lynsay A, Nurse, Jason RC, Erola, Arnau, Epiphaniou, Gregory, Maple, Carsten&Bellekens, Xavier. (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

Mathias, D. Prathima, A, & Suma, B (2018). A Survey Report On Cybercrime Awareness Among Graduate And Postgraduate Students Of Government Institutions In Chickmagaluru, Karnataka, India And A Subsequent Effort To Educate Them Through A Seminar. International Journal of Advanced Research in Engineering and Technology (IJARET), vol.9, issue 6, pp. 214–228. Retrieved from http://www.iaeme.com/MasterAdmin/UploadFolder/IJARET_09_06_023/IJARET_09_06_023.pdf

May, T., &Bhardwa, B. (2018). Introduction.InOrganised Crime Groups involved in Fraud (pp. 1-10). Palgrave Macmillan, Cham. As cited in Hamsa, S., Singh, A., &Panackal, N. (2018). Study on Effect of Social Networking Sites on the Young World of Cyber Crime. Annual

Research Journal of SCMS, Pune. Retrieved from https://www.scmspune.ac.in/journal/pdf/current/Paper%206%20%20Sajeesh%20Hamsa%20et%20al.pdf

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. Retrieved from https://link.springer.com/content/pdf/10.1007/s11920-021-01228-w.pdf

Näsi, M., Oksanen, A., Keipi, T., &Räsänen, P. (2015). Cybercrime Victimization Among Young People: A Multi-Nation Study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/14043858.2015.1046640

Okeshola, F. B., &Adeta, A. K. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114 Retrieved from http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf

Oksanen, A., &Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. Vulnerable children and youth studies, 8(4), 298-309.RetrievedFrom https://www.researchgate.net/publication/234117319_Young_people_as_victims_of_crime_on-_the_internet_A_population-based_study_in_Finland

Potgieter, P. (2019). The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. In Proceedings of 4th International Conference on the (Vol. 12, pp. 272-280). Retrieved from https://easychair.org/publications/paper/wVsR

Pradeep, L M P, Arjun M. (2018) Crime Awareness among Youth in Udupi District J Forensic Sci& Criminal Invest. 2018; 8(5): 555750. DOI: 10.19080/JFSCI.2018.08.555750 Retrieved from https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555750.pdf

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., &Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. Journal of Advanced Transportation, 2021.Retrieved from https://downloads.hindawi.com/journals/jat/2021/6627264.pdf

Rathod, P., &Potdar, A. B. (2019).Study of Awareness of Cyber-Security among Medical Students. Indian Journal of Forensic Medicine & Toxicology, 13(1), 196-198. Retrieved from https://www.researchgate.net/publication/330978587_Study_of_Awareness_of_Cyber-Security_among_Medical_Students

Reddy, G. N.,& Reddy, G. J. (2014). A Study of Cyber Security Challenges and its emerging trends on latest technologies. arXiv preprint arXiv:1402.1842. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_It-s_Emerging_Trends_On_Latest_Technologies

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.

Retrieved from https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review

Saxena, M. K. & Chauhan, S. (2021). Excessive Smartphone Usage by Students: A Review. Edu Tech-e journal of Education & Technology. Retrieved from http://www.edutech.net.in/Articles/2021/Art00004.pdf

Saxena, M. K., & Singh, A. (2020).The Wireless Communication and Rising State of Unrest among Indian Youth.International Journal of Information Dissemination & Technology, 10(3).

Saxena, M. K., Kumar, S., & Singh, A. (2019). Computer Anxiety and Individual Failure in Computer usage among Teacher Educators of Universities and Colleges: A study on FDP participants. International Journal of Information Dissemination and Technology, 9(4), 191-195.

Senthilkumar, K., &Easwaramoorthy, S. (2017, November). A Survey on Cyber Security awareness among college students in Tamil Nadu. In Materials Science and Engineering Conference Series (Vol. 263, No. 4, p. 042043) Retrieved from https://www.researchgate.net/publication/321482508_A_Survey_on_Cyber_Security_awareness_amon-g_college_students_in_Tamil_Nadu

Sreehari, A., Abinanth, K.J., Sujith, B., Unnikuttan, P.S., &Jayashree, (2018) A Study Of Awareness Of Cyber Crime Among College Students With Special Reference To Kochi. International Journal of Pure and Applied Mathematics (vol.119, No. 16, pp. 1353-1360) Retrieved from https://acadpubl.eu/hub/2018-119-16/1/130.pdf

Thomas, D. and Loader, B. (2000) "Cybercrime: Law Enforcement, Security and Surveillance in the Information Age", London: Routledge, Retrieved fromhttps://www.researchgate.net/publication/231861412_Douglas_Thomas_and_Brian_Loader_eds_Cybercrime_law_enforcement_security_and_surveillance_in_the_information_age_2000_Routledge_London_300_pp_1699_pbk

Tibi, M. H, Kholod,H.,Bashier, W.(2019) Cybercrime Awareness among Students at a Teacher Training College.International Journal of Computer Trends and Technology (IJCTT) – Volume 67,Issue6 Retrieved from https://www.researchgate.net/profile/Moanes_Tibi/publication/333718843_Cybercrime_Awareness_among_Students_at_a_Teacher_Training_College_IJCTT/links/5d00a11b299bf13a384ea3b5/Cybercrime-Awareness-among-Students-at-a-Teacher-Training-College-IJCTT.pdf

Yu, S. (2014). Fear of Cyber Crime among College Students in the United States: An Exploratory Study. International Journal of Cyber Criminology (IJCC), Vol 8 (1): 36–46. Retrieved from https://www.semanticscholar.org/paper/Fear-of-Cyber-Crime-among-College-Students-in-the Yu/e862c8be02f4c68e78bf6d1b9f64ed8945225133

Zahri, Y., Ab Hamid, R. S., &Mustaffa, A. (2017). Cyber security situational awareness among students: A case study in Malaysia. World Academy of Science, Engineering and Technology International Journal of Educational and Pedagogical Sciences, 11(7). Retrieved from https://pdfs.semanticscholar.org/28e1/c12f61c2c5aaf55cd48e8218fc919464367f.pdf