

Social Media and Undergraduate Students : Issues and Tackling Strategies

Jiji Johnson

Ph.D. Research Scholar, Department of Sociology and Social Work, Annamalai University

Dr. B. Manikavasagam

Associate Professor, Department of Sociology and Social Work, Annamalai University

Abstract

Increasing independence from control of parents and adults tends undergraduates to be a freer person who are in search of wider friendships from different walks of life, for getting spotlighted in gatherings. To expand their friends circle they get hold of a cell phone, a laptop or a computer with internet connection. By using this they come in contact with people around the world without knowing the pros and cons of their friendship. The main aim and specific objectives of this study on the 'Social Media and Undergraduate Students : Issues and Tackling Strategies' is to help in supporting the parents, teachers and elders to be acquainted with the problems faced by undergraduates in using social media. Findings reveal that undergraduates at college level face more problems through social media's like online gaming, cyberbullying, cyber grooming, etc...In order to reduce the risk of falling a victim to cybercrimes, proper awareness should be provided to children even from early age so that they get an insight on the ways how cybercrimes are triggered and about cyber security and the impacts of cybercrimes.

Keywords: Adolescents, Cybercrimes, Social Media, Socio-psychological problems, Undergraduates



Information and communication technology through internet, computers, and smart phones has become an integral part of our everyday life. It has just transformed our ways of communication and means of sharing updates and data like photos, videos, etc. Even the ways of purchase has changed to the platforms of online shopping. e-banking is also widely encouraged for cashless payments of bills, fees, transfer of money from one bank to another, and for other financial transactions using online facilities. The new generation now a days are getting more exposed to cyber space even from a very young age. Children especially teenagers spend most of their time in online games, chatting and in using WhatsApp. With the upcoming of smartphones, the interest in getting engaged in cyber

space has increased significantly. As cyber space connects a person with a virtual world where there are all kinds of people, both good and bad, the cybercrimes has increased rapidly. It is seen that adolescent children in the undergraduate group having a greater quest for experimental knowledge with limited knowledge of cyber threats are more susceptible and vulnerable to cybercrimes. Though experimenting is the ideal way of learning, it is equally important to have a proper guidance of an experienced hand while browsing online so that the children does not get involved in cybercrimes which can help in safeguarding themselves from the adverse impacts of cyber technology. It will help them to be careful cyber citizens.

Social networking websites are profile based websites that permits users to maintain social relationships by viewing and sharing their social connections with other members of the group. It helps in interacting with others as a virtual community by helping in sharing information, ideas, knowledge and common interests through online social network sites which are maintained by social media organisations. This helps in creating a highly interactive platform through which individuals or communities can share their views and discuss matters of common interests. It is entirely different from the traditional media for communications like newspaper, magazines, radio and television broadcastings where only sender can pass the information and the recipients cannot respond back or express their views. This interactivity, accessibility and proximity has made online communication more popular even among children. Whatever a person wants to know is at their fingertips from all around the world. Social media outlets operate in a dialogic transmission method (many sources to many receivers) where as traditional media's operates as mono-logic transmission method (one source to many receivers). Some of the most popular social media websites are Facebook, WhatsApp, Blogs, Instagram, Twitter, YouTube, LinkedIn, emails, chat rooms, social gaming, photos and video sharing, etc. Social media thus facilitates the development of online social network sites by connecting a user's profile with those of other individual groups. It is therefore an electronic communication media through which the user creates or gets connected with online communities to share information, personal messages and knowledge. But it is less known that the information or personal details shared on the internet stay online forever which hackers can use for financial or reputational loss of a person. Hackers usually use malwares, Trojans and viruses for unauthorised access of data from another person's computer or mobile.

It has been noted that there are a varied range of positive and negative impacts of social network sites on teenager's especially undergraduates. In the studies conducted among undergraduates, especially of Trivandrum district, it is seen that by the time a student passes his schooling, he forces his parents to get a computer with internet connection to facilitate his higher studies and also a smart phone to interact with his peer groups. In the beginning the undergraduate students mostly use social networking sites to connect with their friends, family and relatives. But later through these social media's the child gets connected with online communities. These communities share their views with one another, which sometimes could be good or bad, depending on the group in which he gets into, as the user generated contents are the life blood of a social media organisation. The increase in the wide spread use of smart phones for exploring and expanding knowledge for learning the unknown factors has in many times lead teenagers into critical problems and fake friendships in which they get caught. The community based personal websites like chat rooms and other social spaces tend to trap teenagers by using the facilities like messaging, sharing photos and videos as youngsters are the avid users of these sites. Unaware of the shortcomings of sharing the information, under graduate students tends to disclose their personal information which reveals their identity. Later this is used to blackmail them, as security and privacy gets attacked in many cases. Many studies shows that college students spend a great amount of time on social media's like WhatsApp and Facebook as part of their daily routine and as part of their freedom of expression. In some cases this helps students to increase their self-esteem and life satisfaction. They get larger

network of friendship through online communication compared to elder persons, which encourages sociability in them.

Social networking sites being the means for interactive online communication prompts teenagers to join these sites, mainly because their friends invite or compel them to become a part of these sites. Spending a great amount of time on the social networking sites for posting entries, comments, pictures, photographs and videos may negatively affect the academic performance of the students. The studies conducted in the undergraduate students of Trivandrum district shows that students at many times reveal a lot of information about themselves without knowing the privacy options or to permit whom to view their profiles. So the ways to prevent cybercrimes and how to protect themselves from cyber threats has to be taught to children even from adolescent age so that they could use cyber space safer and could share their knowledge with other community without having cyber threats.

Cybercrimes are offences committed with malicious intentions using internet facilities. Cyber criminals use platforms like social networking sites, websites, chatrooms or emails to trap victims for attacking them. Now a day's cyber-attacks are becoming more sophisticated and are being made use for stealing bank details, addresses, photographs, phone numbers, passwords and personal information creating fake profiles for criminal purposes or for cyberbullying. The various ways used for cyber-attacks are email spoofing which is used by send emails which look genuine but actually are not. Through social engineering the cyber criminals gain confidence of the targeted victim to access personal information from him. Depending on the victim's interest, the criminal interact with the person and gains his confidence by collecting his personal information and later using it to harm him. The Cybercriminal sends malicious file applications to the victims system through direct messaging, emails, websites or games and thus gets access to the victim's personal data from his computer or smart phones. Some criminals use the identity of the victim to create fake account and use it to gain financial advantage or some other benefits in the victim's name which causes loss or damage to the victim. One among this is cashless financial transactions which is commonly used for online shopping's and payments.

Cyber bullying is a form of harassment or bullying inflicted through online communications. It is usually used against teenagers where they are bullied and harassed through online media. The bullier sends rude, mean or hurting messages and comments to victim through email or through social media platforms like private chat rooms or as text messages, images/ videos via smart phones to harass him/ her. He might give threat on spreading embarrassing rumours or pictures of the victim to his near and dear. The fear of the cyber-attack could cause physical, emotional and psychological effects on the adolescent child which could reflect in their academic performance or even his routine life.

Cyber grooming is yet another major cyber-attack. It is done by build an emotional bond with adolescent children, through social media, with the aim of gaining their trust for sexual abuse or exploitation. The cyber groomer collects obscene photographs or videos of the teenager with which he blackmails the victim. If his wishes are denied he threatens to spread the collected materials within the victim's family and friends. This deeply affects the psychological and emotional wellbeing of the teenager which could haunt the victims through out his/ her life.

Online gaming is another area which is used to trap adolescent children. As online games can be played even on mobiles, more and more children are getting addicted to it. There are many free online gaming websites. For entering the gaming community one have to create an account for which a lot of personal information has to be provided before creating the account. A web cam and a head phone has also to be used. Through these websites, the child plays with a large online community, where the child shares his/ her views and become befriended with many strangers who can cause risk to the player. Unknowingly viruses, malicious software's and spams gets downloaded while playing online and while downloading games from these sites. Some cyber criminals make friendship with the victimized player and plays these games pretending to be a child giving

clues and by sharing points, coins, etc..., helping the victimised player to improve his/ her performance and helping him to win the game and thus by making friendship with him. Later this friendship will be misused by inviting the child for a one to one meeting or may be asked to share the credit card/debit card details of his parents for payment which could be later be misused by capturing the details of the credit card.

e-mail fraud is yet another means to trap people online. As an email account is needed to open a social media account, online gaming account and other online accounts it has become an essential part of life for online communications. Email address is commonly used for mobile banking and other financial communications also. Email spams are sent from fake accounts to a person's email address which has links which could direct the person to other pages where he would be asked to enter password or personal details for updates which when given ends up by giving personal details to the cybercriminals. Or else an email with malware or virus document in word or excel format will be sent to the targeted victim's email. When such document is opened malware gets installed in the victim's computer or mobile which could be used to access important details like password, login id, phone number and address of the victim by which further criminal activities can be performed. Another way is to inform the targeted victim that he has won a lottery for a lump sum amount for receiving of which he has to give his banking details which will be said is for transferring the prize money. Further for getting the winning amount they might ask to pay as a processing fees or tax deposit which could be a percentage of the huge amount they have promised. Once the cybercriminals receive the cash from the victim they will vanish into thin air. Some hackers send offensive emails to the addresses accessed from the victim's contact details also. They could ask for financial help through the victim's email address book to the victim's family members and friends by saying that it is an emergency and that he cannot contact in person at present. To avoid such situation the email id should be well protected using complex passwords which should be changed at regular intervals so that it could not be hacked. Never use names of family members and their date of birth as passwords. It would be better to use combinations of alphabets, numerals and symbols and make it a bit strong and long so that it may not be recognised easily by others. Also two factor authentication could also be used for login to the email account, the second of which being an OTP number sent to the email holder's mobile phone which could ensure higher level of security. Also it should be ensured that the email id and its password are never shared with others. Links from other unknown users should be never entertained. Make sure that you sign out from your account before you close your account and also not to click 'remember password' button while not using one's own computer. If in any case a person's email address is hacked, send an alert message to all the addresses in the contact list so that they can be warned about any unwanted happenings from this email address. The service provider can also be asked to temporarily block the email account and meanwhile try to retrieve and change the email account immediately. Never respond to emails or messages of winning a lottery or huge prize money as it could be a real trap. Check the genuineness of emails before responding to it. If in any case a person comes across a family member or friend asking for financial assistance through email, that person should be contacted personally and should be ensured that their email address has not been hacked and the request is genuine.

Online transaction fraud could be done through net banking by accessing credit/debit card credentials. It could be done by sending emails or calls as if it is from banks asking for one's bank account details, personal identification number (PIN) which is the unique identification number, card details, card verification value (CVV), date of birth, expiry date, etc. Once this is obtained the person's account can be misused. As mobile number is linked with bank account, mobile numbers could also be used to hack bank details. The hacker would pretend to be the mobile service provider and sends a link or will ask to send an SMS to a number which actually is to obtain a duplicate SIM which the hacker obtains himself and uses for malpractices. To avoid this, if such calls come

disconnect the call and contact the customer care number and check the genuineness of the call. Never install pirated software on the computer or mobile phone. It is not only illegal but may cause in compromising with the security of the system. Avoid using public Wi-Fi or public computers for online transactions. Preferably make it a habit to review the monthly bank statement and credit/debit card details for unrecognized transactions. If bank details are found stolen, inform the bank authorities immediately to freeze the account temporarily and meanwhile lodge a complaint to the nearest police station. All these information should be made available for the children from their teenage itself as they are more prone to online fraud practices.

Conclusion

The studies conducted among undergraduate students of Trivandrum district shows that most of them are not aware of cybercrimes. So awareness programmes should be provided to enlighten students especially teenagers and undergraduates on the risk factors associated with social networking sites, various cyber threats and the ways to safeguard themselves against cybercrimes. They should be taught not to accept friend requests from unknown persons through social media. To avoid falling victim to cybercrimes children should be enlightened not to share their personal details like name, date of birth, age, address and phone numbers with online acquaintance. Further make aware that whatever posted on social media could be seen and accessed by all, until it is restricted for the access of restricted viewers like their near and dear ones. It should be insisted not to download free online games from software developers that are not reputed or should be downloaded by clicking links sent via email or as text message or through pop ups. This could cause viruses or malwares to be downloaded on to the person's computer or his smart phone which could indeed compromise on the security of the software. To avoid this a reliable antivirus software should be installed in the system and should be regularly updated to detect & protect the system from malwares and virus threats. While chatting, only public chat rooms are to be used and never to accept any private chat invitation from unknown persons and also not to reveal one's personal identity to any strangers online. Never keep the webcam on, when the chat partner does not connect himself to the webcam. Before making online friendship it should be verified as to how many others are in the friend's list of the person and whether you know any of them in person. Never try to meet the persons alone who have been befriended though online social media. Be cautious when a person who chats with you gives many compliments within a short period of acquaintance and also when he asks about your sexual interests. Never entertain such talks that are not comfortable to you. Also unwanted software's which could be used to trap you should not be installed. Further never tease or bully peers or such other people leading them to harass you. If any such unfortunate things happen, ask the children to get the assistance of their parents or elders so that they can intervene and support the children by guiding them and not letting them to fall a prey to the cyber-criminal and also to block the access of the bullier. As it is illegal, unethical and punishable offence, if harassing persists, the assistance of cyber cell can be sought or a complaint can be lodged in the local police station. The messages, pictures and videos send by the cybercriminals can be saved as an evidence for taking legal action against them.

Social networking website companies should improve the security and privacy of their sites. Policies and strategies should be established to safeguard the use of personal information in these sites. Further students should be made aware that they should not disclose personal information with strangers online as this could lead to cybercrimes like cyber bullying, cyber grooming and online transaction fraud. It should be made aware to children that the parents or elder's credit card/ debit card details should not be shared online as part of getting points or coins in online games. Likewise the passwords of the bank ATM or email id or e-banking should not be disclosed. The passwords should be made complex

to increase online security and the PIN number of the debit/credit card should be changed at regular intervals to enhance the safety. Use the personal bank account of oneself by themselves to avoid other person's possibility of accessing ones account. Try not to share fake news or messages which could hurt the integrity of another person. Before sharing a news check its authenticity. Also never upload or download copyrighted contents without author's permission as doing so is a punishable offence. It is ideal not to use web cam or voice chat while playing online games which could be helpful in sharing your identity with other players which could in turn lead to cyber bullying, cyber grooming or other cybercrimes. If faced with any such atrocities the child should be encouraged to reveal and disclose the matter to his parents, class teachers or elders at home so that they could support him and guide him by helping him to face the circumstances. It would be better to encourage children to play outdoors with their peer groups to avoid such unnecessary circumstances which could even affect the child's academic performance and even his routine life. This could help to limit the child's exposure to online games. The physical games helps to develop the child's muscle strength and would help him to first-hand experience from real environment and will help him to gain knowledge and gain confidence in doing things on his own which could indeed help in developing his overall personality and could help in their physical, mental and social development.

References

- [1] A to Z of Cyber Crime, Asian School of Cyber Laws, <https://www.dbs.com/act/assets/pdf/ leap-a2z.pdf>
- [2] Akashdeep Bhardwaj , Vinay Avasthi , Sam Goundar. *Impact of Social Networking on Indian Youth - A Survey*, I.J. of Electronics and Information Engineering, Vol.7, No.1, PP.41-51, DOI: [10.6636/IJEIE.201709.7\(1\).05](https://doi.org/10.6636/IJEIE.201709.7(1).05) (2017)
- [3] Almenayes, J. *The Relationship between Cyber bullying Victimization and Depression: The Moderating Effects of Gender and Age*. *Social Networking*, 6, 215-223. <https://doi.org/10.4236/sn.2017.63014> (2017)
- [4] Daria J. Kuss and Mark D. Griffiths. *Adolescent online gaming addiction*, *Education and Health* (2012) Vol.30 No. 1.
- [5] Hinduja SY, Patchin JW. *Bullying, cyberbullying, and suicide*. *Arch Suicide Res*.14(3) (2010) pp.206-221
- [6] Jeanna Mastrodicasa & Paul Metellus. *The Impact of Social Media on College Students*, *Journal of College and Character*, 14:1, 21-30, DOI: [10.1515/jcc-2013-0004](https://doi.org/10.1515/jcc-2013-0004) (2013)
- [7] Kavitha .*The Influence Of Social Media On Indian Students And Teenagers*, *International Journal of Advance Research In Science And Engineering* <http://www.ijarse.com> IJARSE, Vol. No.4, Special Issue (01), April(2015)
- [8] Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. and Tippett, N. *Cyberbullying: Its Nature and Impact in Secondary School Pupils*. *Journal of Child Psychology and Psychiatry* (2008) 376-385. <https://doi.org/10.1111/j.1469-7610.2007.01846.x>
- [9] Van der Hof Simone and Kooops, Bert-Jaap. "Adolescents and Cybercrime: Navigating between Freedom and Control", *Policy & Internet: Vol. 3: Iss. 2, Article 4*. <http://www.psocommons.org/policyandinternet/vol3/iss2/art4>, DOI: 10.2202/1944-2866.1121 (2011)
- [10] Waleed Mugahed Al-rahmi, Akram M. Zeki, Norma Alias & Ali Ali Saged. *Social Media and its Impact on Academic Performance among University Students*, *The Anthropologist*, 28:1-2, 52-68, DOI: [10.1080/09720073.2017.1317962](https://doi.org/10.1080/09720073.2017.1317962)(2017)
- [11] Zhengchuan Xu , Ofir Turel and Yufei Yuan. *Online game addiction among adolescents: motivation and prevention factors*, *European Journal of Information Systems* 21(2012)

About the author



Jiji Johnson is a Ph.D research scholar of the prestigious Annamalai University, Chidambaram, Tamil Nadu. Being a keen observer and a proficient scholar she has presented three papers in National Seminars

and published a paper in the Pramana Research Journal on socio-psychological problems of adolescence among higher secondary students of Thiruvananthapuram city. She focuses on the socio-psychological problems of college student's especially of Thiruvananthapuram district in Kerala



Dr. B. Manickavasagam is an Associate Professor in the Department of Sociology and Social Work, Annamalai University, Tamilnadu. He has completed nineteen years of teaching experience in UG and PG level. His area of specialization is Sociology of Environment. He has published more than 60 research papers in national and international reputed journals. He has successfully completed two Ph.Ds. and now six Ph.D. research scholars doing under his guidance. To his credit he authored a book medical Sociology. He has participated more than fifty-five conferences in national and international level. He has associated with Indian Sociological Society.