Study on Effect of Social Networking Sites on the Young World of Cyber Crime

Sajeesh Hamsa

Symbiosis Center for Management Studies,
Symbiosis International (Deemed University), Pune

Dr. Archana Singh

Symbiosis Center for Management Studies
Symbiosis International (Deemed University), Pune

Prof. Nehajoan Panackal

Symbiosis Center for Management Studies
Symbiosis International (Deemed University), Pune.

Abstract

Using this cyber world online transmission of electronic data, electronic commerce, electronic communication as well as electronic governance and mobile communication have become very popular worldwide everyone is using it. The purpose of the paper is to understand the common cybercrimes experienced by individuals and to know about the level of awareness amongst youth. Entire research process is defined and distributed in a systematic manner. It includes extensive literature review. The present paper is based both on primary as well as secondary data & information. As the cyber world digital citizens all of us are instrumented with data obtainable about their location and happenings, privacy seems to vanish. Technological challenges are directly related to security challenges. The paper discusses the cybercrime amongst youth at a macro level in a conceptual manner.

Keywords - Cyber-crime, Youth, Security awareness

Introduction

Today e-mail and websites are means of communication for everyone. (Lane, J., Heus, P., & Mulcahy, T, 2008). It facilitates almost instant exchange and dissemination of data, images and variety of material. It is inclusive of educational and helpful material but undesirable information also. (Mishna, F et.al, (2011).

These begin from inventions in information technology that, to enhance new economic and social opportunities, pose difficulties to our security and prospects of privacy. All of us as humans are already interconnected with information technology. Everyone uses devices and smart gadgets. All social systems are now fully connected as the "Internet of Things." Standards are evolving for all of these potentially connected systems. Quality of life is improving through information technology. Infrastructure is getting automated. Security and privacy are the two major challenges. Disruption and illegal access can be done through attacks (Kugler, R. L., 2009)

In the current online era of cyber threats, a huge number of cyber threats and its impact along with understanding is difficult to restrict at the initial stage of the cyber-attacks. (Hale, C. 2002). The United Nations, for statistical purposes, defines 'youth', as those persons between the ages of 15 and 24 years, without prejudice to other definitions by Member States Almost 27.5% of the Indian population is comprised of Youth in the age group of 15-29 years. It is seen that online risks such as addiction, cyber bullying, and sexual solicitation are associated with negative consequences for youth. It is important to note that not all children information technology users. (Broadhurst et .al 2014). Defining youth with age group is one of the easiest way in are equally susceptible and more research is necessary to identify the youth most at risk as well as to develop effective interventions. (Guan, S. S. A., & Subrahmanyam, K., 2009)

Research Methodology

Entire research process is defined and distributed in a systematic manner. It includes extensive literature review, survey-based research, from Ebsco, Emerald, Scopus, Jstor, Thomson Reuters and Google Scholar.

The present paper is based both on primary as well as secondary data & information. In order to get the primary data from the root source, the structured questionnaires were prepared for respondents. The number of respondents were 100 youth from different states of India.

Review of literature

Cyber Crime

In the modern life cybercrime is an evil. In the cyber world is crime is the most serious threat. It is very important to understand of cybercrimes and to safeguard future from the same (May,T & Bhardwa, B. 2018). Cybercrime is an act for which punishment is imposed upon conviction.

Some of the kinds of Cyber-criminals are mentioned as below-

Crackers are those individuals who are virus creators. Hackers are the one explore others' computer systems for education, Pranksters are individuals who attempt to tricks on others. (Sukhai, N. B, 2004) Career criminals are individuals who earn their income from crime. Harassment is cyber bullying that occurs via the Internet.

Computer spam refers to unsolicited commercial advertisements distributed online via e-mail, which can sometimes carry viruses and other programs that harm computers. Restriction of cybercrimes is dependent on proper analysis of their behavior and accepting of their impacts over different levels of society. (Probst, C. W et.al,2010). Therefore, cybercrimes understanding in the current era and their effects over society with the future trends of cybercrimes are explained. (McGuire, M., & Dowling, S. 2013).

Another type of cybercrime is phishing is just one of the many frauds on the Internet. Vishing is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. A vishing attack can be conducted by voice email, or landline or cellular telephone.

Social networking Sites

The popular social media sites like Facebook and Myspace had studied the views on trust and privacy concern regarding sharing of information and new relationships. It is clear there is no much difference as privacy is concerned. It was found that majority of Facebook members were willing to share information than members of Myspace. Whereas Myspace members are more willing to interact with other new members of the site. This suggests that given in any social media platform, privacy and trust do not really matter when exchange of information or relationship building between the members. (Dwyer, Hiltz, & Passerini.2007).

(Subrahmanyam, Reich, Waechter & Espinoza,2008). study shows that evolving adults also use Social networking sites to connect with family and friends and the pattern disclose that they use online to reinforce their disconnected folks. According to (Lin& Lu,2011) one of the major factor people join social networking sites is for fun or enjoyment, and the other aspect is friends and real benefits of it. It was also known that men and woman have different influencing factors when it comes to joining social networking sites. One of the top reason is, woman is influenced by number of their peers in social media. Whereas men had no impact of friends or families, to join in a social networking site.

(Wilson, Fornasier & White,2010) showed in their study that psychologically, overenthusiastic teenagers trend to spend more time at social networking sites and also higher level of addictive affinities.

Cybercrime and social networking sites

(Williams, Edwards, Horsley, Burnap, Rana, Avis & Sloan, 2013) focuses on social media users with the ability to monitor social media facts streams for signs of high tension which can be examined in order to detect deviancies from the 'norm' (levels of interconnection/low tension). Indicators about neighborhood crime, scarcity and demography, to provide a multifaceted representation of the 'terrestrial' and 'cyber' streets. As a result, this 'neighborhood informatics' allows a means of official foundations of civil unrest through reference to the user generated versions of social media and their connection to other, curated, social and commercial data.

(O'Keeffe & Clarke, 2011) explained spending time in social media Network sites is among the most common activity among the current generation of children and youngsters. Gaming sites, simulated worlds and video sites such as YouTube; and blogs offer youth a gateway for entertainment and interaction. This had grown tremendously in recent years. It is vital that parents become conscious of the environment of social media sites, given that not all of them are safe backgrounds for children and adolescents.

(Wall, 2008) talked about the astounding contrast between the numerous instances of cybercrime supposedly stated each year and the pretty small number of known trials. This distinct evidence leaks a large hole in our understanding of cybercrime and pleads a number of vital queries about the quality of the making of criminological evidence about it. This item takes a serious look at the

means that public insights of cybercrime are made and uncertainties about it are produced. It discovers the varying conceptualizations of cybercrime before finding tensions in the making of criminological awareness that are causing the rhetoric to be chaotic with realism. It then differences the tradition of cybercrime with what is actually going on in direction to know the support gap that has unlocked up between public demands for Internet safety and its delivery.

(Patton, Hong, Ranney, Patel, Kelley, Eschmann& Washington,2014) emphasized on assassination being the second top cause of death for young people, and experience to violence has an adverse effect on youth mental vigor, academic presentation, and interactions. They proved that youth violence, together with victimization, mob violence, and self-directed violence, more and more occurs in the virtual space. Some methods of online violence are inadequate to Internet-based relations; others are directly related to head-on acts of violence.

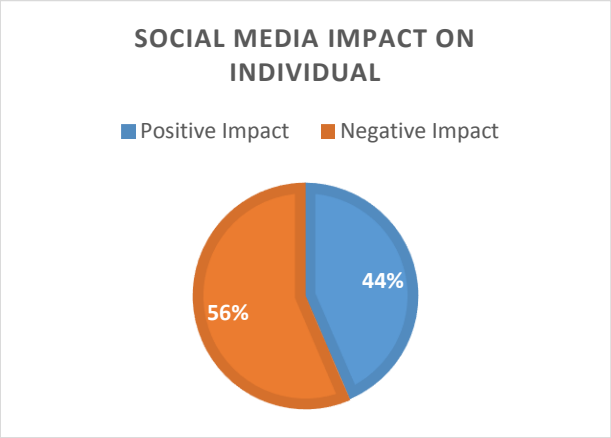
Cybercrime and youth

(Marcum, Higgins, & Ricketts,2010) through their study proved positively more effective policies and plans can be established to teach youth and people about defending themselves while online. Youth should be mindful of who they are communicating with online and abstain from as long as any type of personal information to persons they do not identify and belief. Also, further analysis of the use of social networking websites and the wrong actions of youths, as well as their knowledge with misleading Internet practices, will spread our awareness of the online activities and practices of adolescents. With this understanding, better safety measures and strategies can be established to keep adolescents safe online

(Oksanen & Keipi, 2013) in the study explored cybercrime, which has grown into a major topic within the last two decades. Young societies are more likely to be the targets of cybercrime. In addition to age, other aspects including gender, education, financial status, and forceful victimization relates with cybercrime victimization. Decent offline social networks were a defending aspect against cybercrime harassment among females. Young cybercrime preys were more likely to be bothered about future harassment. They showed the significance of understanding both psychosocial threat elements in offline and patterns of uncertain online actions.

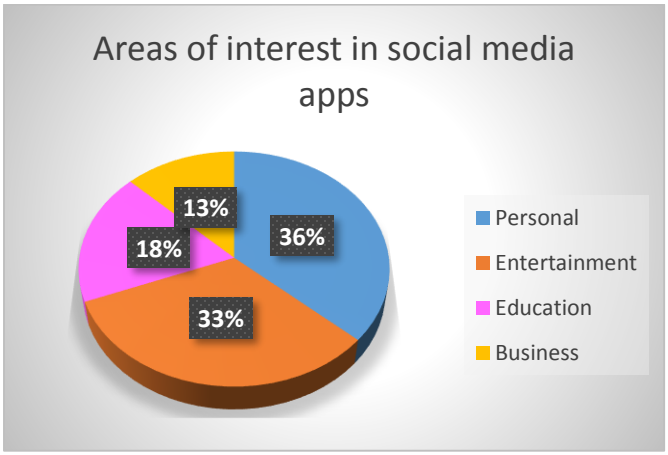
Data Analysis

1. Do you consider social media has more negative or positive effect?



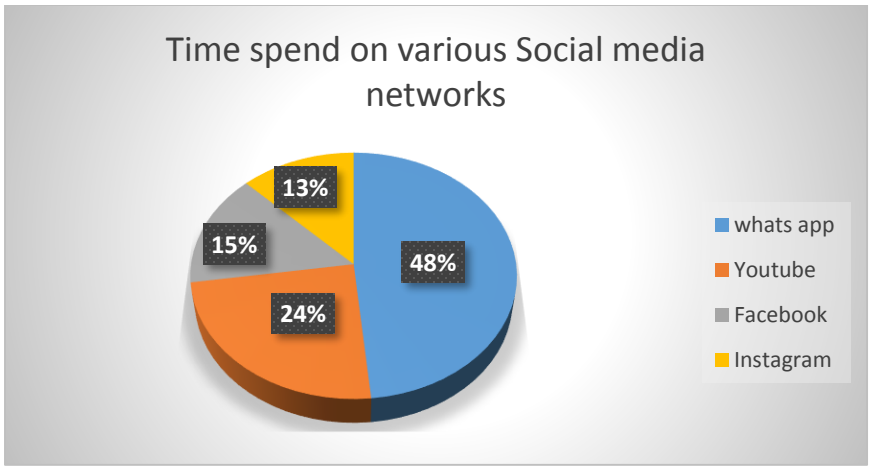
Out of 100 respondents' majority have shown that extensive use of social media can actually cause addiction and negative effects. On the contrary other respondents perceived it as a positive platform.

2. Which types of information interest you in social media apps?



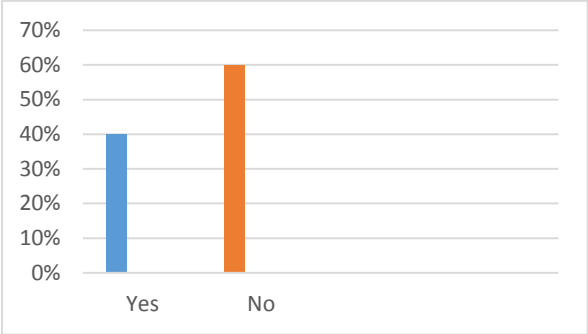
Majority of the respondents were interested in personal and business information. For the purpose of education, it is least preferred. Entertainment is also preferred over education purpose.

3. Which is the social media apps do you most often use?



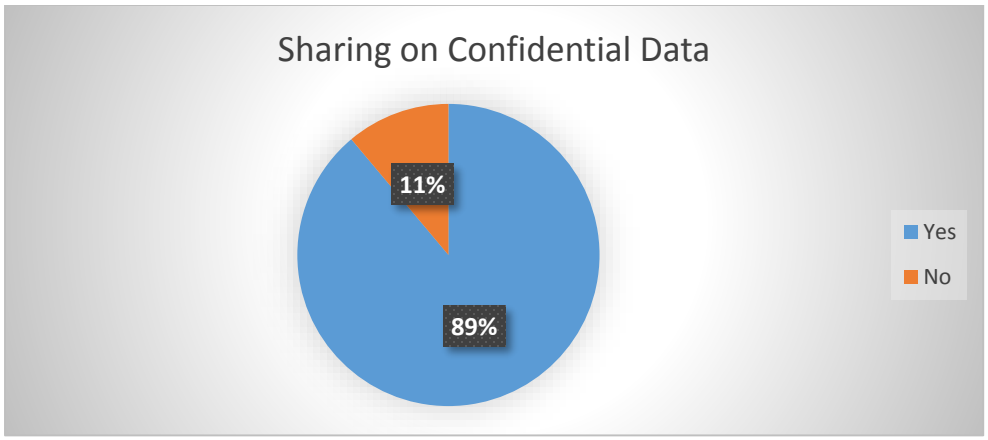
Whatsapp is the most famous application of social media networking followed by Youtube, facebook and Instagram consecutively.

4. Have you ever added an unknown profile from social media?



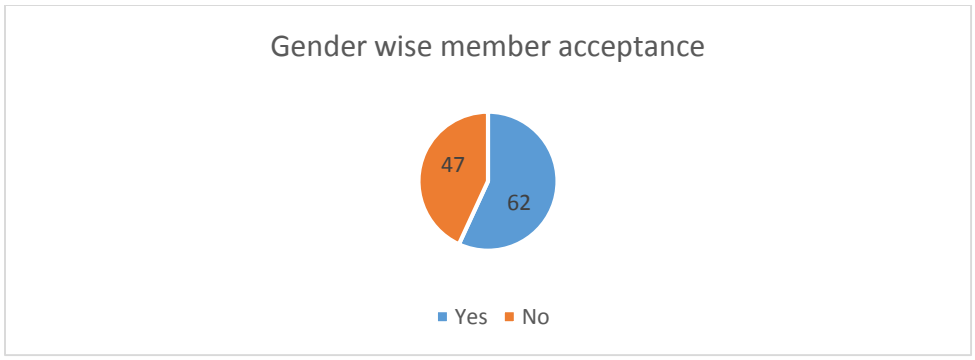
Majority of the respondents are conscious and do not accept any friend request from strangers. 40% respondents believe there is no harm in chatting with strangers.

5. Had you ever shared your passwords among close friends, parents or others?



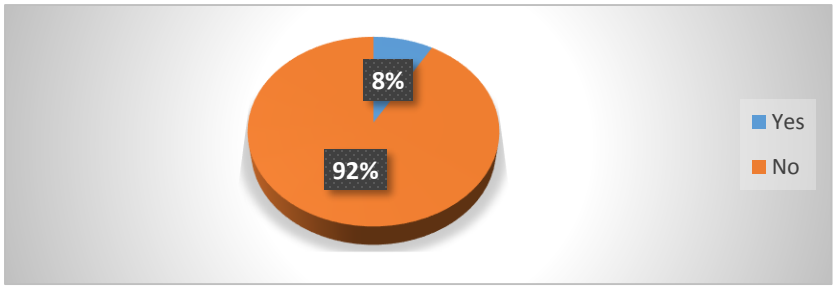
It was astonishing to note that maximum respondents don't mind sharing crucial information like their password amongst family and friends, which shows level of awareness is very low amongst youth.

6. Acceptance on the basis of gender on social networking site



Majority of the youth on social networking sites enjoy having friends of the opposite gender which can be misleading and can cause negative effects.

7. Have you disclosed cybercrime faced by you to your friends or parents?



Majority of respondents have not disclosed details of cybercrime faced by them to their parents

out of fear which again shows that the level of awareness of the consequences of cyber crime needs to be assessed.

Conclusion

There are a wide range of information security awareness delivery methods such as web-based training materials, contextual training and embedded training. In spite of efforts to increase information security awareness, research is scant regarding effective information security awareness delivery methods. (Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. 2011). (Abawajy, J. 2014) suggested that a combined delivery methods are better than individual security awareness delivery method.

In order to prevent cyber stalking, individuals should avoid disclosing any information pertaining to them (Florêncio, D., & Herley, C.2013). This is as good as disclosing your identity to strangers in public place always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. Always use latest and update anti-virus software to guard against virus attacks. always keep back up volumes so that one may not suffer data loss in case of virus contamination Never send your credit card number to any site that is not secured, to guard against frauds.

Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this. It is important to discuss and evaluate the effects of various information security awareness delivery methods used in improving end-users' information security awareness and behavior. (Tadda, G et.al, 2006).

Limitations of the study

Following are the limitations pertaining to the research study-

- It is a descriptive study with close ended questionnaire and hence the potential to capture unique insight is limited.
- Legal aspects of cybercrime and cyber security is not covered in the study.

References

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber-crime.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Ferrell, J. (1997). Youth, crime, and cultural space. *Social Justice*, *24*(4 (70), 21-38.

Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. In Economics of information security and privacy III (pp. 35-53). Springer, New York, NY.

Guan, S. S. A., & Subrahmanyam, K. (2009). Youth Internet use: risks and opportunities. Current opinion in Psychiatry, 22(4), 351-356.

Hale, C. (2002). Cybercrime: Facts & figures concerning this global dilemma. Crime and Justice International, 18(65), 5-6.

Kugler, R. L. (2009). Deterrence of cyber-attacks. Cyberpower and national security, 320.

Lane, J., Heus, P., & Mulcahy, T. (2008). Data Access in a Cyber World: Making Use of Cyberinfrastructure. Trans. Data Privacy, 1(1), 2-16.

Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in human behavior*, *27*(3), 1152-1161.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

May, T., & Bhardwa, B. (2018). Introduction. In Organised Crime Groups involved in Fraud (pp. 1-10). Palgrave Macmillan, Cham.

McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*.

Mishna, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2011). Interventions to prevent and reduce cyber abuse of youth: A systematic review. Research on Social Work Practice, 21(1), 5-14.

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800-804.

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.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior*, *35*, 548-553.

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of insider threats. In Insider Threats in Cyber Security (pp. 1-15). Springer, Boston, MA.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In Proceedings of the 2011 conference on Information technology education (pp. 113-122). ACM.

Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: Use of social networking sites by emerging adults. *Journal of applied developmental psychology*, *29*(6), 420-433.

Sukhai, N. B. (2004, October). Hacking and cybercrime. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 128-132). ACM.

Tadda, G., Salerno, J. J., Boulware, D., Hinman, M., & Gorton, S. (2006). Realizing situation awareness in a cyber-environment. In Proceedings of SPIE-The International Society for Optical Engineering (Vol. 6242, p. 624204).

Wall*, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63.

Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., ... & Sloan, L. (2013). Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and society*, *23*(4), 461-481.

Wilson, K., Fornasier, S., & White, K. M. (2010). Psychological predictors of young adults' use of social networking sites. *Cyberpsychology, behavior, and social networking*, *13*(2), 173-177.