Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0047

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

Cybersecurity Awareness on Cybercrime Among the Youth in India

Dr. Vijay Parasram Tupe
Asst. Professor,
Orange City College of Social Work, Nagpur

Abstract

The increased independence on Internet in India has raised growing concerns that cyber security isbecoming difficult to maintain. Not only do businesses depend on the internetfor all types of electronic transactions, but home users increasingly also experience the immense benefit of the internet especially during the COVID-19 pandemic. The rapid growth in the use of cyber space is not matched by the necessary skills. Therefore, there is a need for broad-based education initiatives on Internet safety and security to tackle the issues of child protection and social security in general. Cyber security and awareness become vital issue because promoting awareness would contribute greatly towards cyber security as a whole. An interpretive research approach was adopted using a qualitative research method. Data was collected from primary sources by the semi-structured interviewswhich conducted with the participants of the SAPS Crime Intelligence Unit and Crime Intelligence Unitfor the youthwho were between the ages of 19 to 35 years. The findings indicated that there are currently no existing initiatives in the field of policing cybercrime in South Africa. There are currently no cyber security awareness programmes or preventive techniques by the SAPS targeting the youth. South Africa is still lacking behind in the strategy development regarding cybercrime and cyber security.

Keywords: Awareness; Cybercrime; Cybersecurity; Cyber-scam; Cyber Awareness; Net Behaviour; Social-Media; Police; Youth.

Introduction:

Information Communication Technology (ICT) has become an integral part of our daily lives, especially during the COVID-19 pandemic. Its seems that almost everything relies on computers and the Internet these days, from communication, entertainment, transportation, shopping, etc. Cyber security is an important aspect of National Security and the safekeeping of a Nation's constituency and resources. Itplays an important role in the ongoing development of Information Technology (IT), as well as Internet services. Enhancing cyber security and protectingcritical information infrastructures are essential toeach nation's security and economic well-being. Cyber security as thecollection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organisation and user assets.

The SAPS and Hawks lack cyber capabilities. Youth concurred that the level of knowledge and awareness regarding the notions of cybercrime is not visible or active reactions of youth in relation with the educational activities, as there were none in the Gauteng Province. Responses paint a bleak picture as the participants from both the SAPS as well from the youth that due to a lack of awareness regarding cybercrime and how the victims should report such incidents. Due to lack of adequate awareness among the youth regarding the risks associated with the use of internet, a majority of the youth had inadequate capacity to be vigilant towards possible attacks. These pose a risk each time they connect to the internet, read an email or

download a free application. The unfortunate part of their ignorance, is that there would become part of the statistics of victims and increase lack of reporting of incidents to the local police. SAPS cannot fight cybercrime alone; they need to collaborate with other stakeholders as well as other countries.

- **Theme 1: Lack of Cyber Security Awareness**

When asked how effective cybercrime awareness campaigns were when targeted to the youth, it emerged from the findings that the majority of the participants concurred that not much has been done to increase educational awareness in the home, or in schools and colleges, particularly for vulnerable young people. The participants also emphasized the need to inform the development of training of the relevant stakeholders regarding the best practice for policing across a range of roles on educating the youth on cybercrime. It became clear during data collection process that the participants spoke with one voice with regards to public awareness remaining a challenge, and secondly.The attacks towards ignorant youth were becoming increasingly sophisticated, which posed a challenge for the public in general. These are some of their responses quoted verbatim, and no corrections of their language.They have targeted the youth enough; they have not made them a priority.

They should be made a priority because that's a target market for criminals as much as you look at fraud and scams where guys will target online banking. Specific type of criminals targets specific market and if you look at child abduction, paedophiles and other child criminals, they target youth. So, youth need to be aware and from SAPS perspective, if we have more resources, more capacity, more training we could do much. The youth does not make aware of proper cyber protocols, strategies and security measures that they can implement to safeguard themselves. It could be disastrous. Youth become victims of cybercrime due to lack of awareness and information about cyber related crimes. The responses above highlighted the lack of knowledge as well as awareness posed by the internet amongst the youth.

- **Cyber-scam and Cyber Victim:**

Most of the factors affecting society, as most of the youth become victims of cyber-crime.The victims affected through various forms, such as but not limited to cyberbullying and identity theft. Lack of knowledge on the dangers lurking in the internet by the youth, could also raise the risks such as unsecure behaviour, which, renders users in South Africa easy targets for cyber criminals. The implications are that, apart from adjustment for well-known scams targeting the youth, law-makers must continuously analyse new and developing types of cybercrime to ensure theireffective criminalisation. Considering the actual level of knowledge, awareness and strategies of the SAPS towards cybercrime targeting the youth, some of the responses from youth.It is given that every victim of crime should report a violation of his or her rights to the local police station. Since the SAPS are silent on the issue of cybercrime, do we have to report such incidents to my local station? Those people are clueless about these things. The state and the SAPS should play an active role in reaching out to the youth regarding how to be vigilant towards cybercrimes.

Currently, there is a lack of clarity for victims about how and where different types of cybercrime should be reported. The SAPS DCI plays active role towards informing the youth

about the dangers of the cybercrime. Therefore, it essential that, in case of victimisation, those who fall victim to cybercrime need to know where to report it and get assistance. The uncertainty about how and where to report can deter victims from reporting, limiting our ability to respond to and understand cybercrime. For now, you bring something to us that is really creating confusion as to whether the SAPS actually, has capacity to even attend to these kinds of challenges, they are more concerned with violent crimes. The youth are left on their own that is why recently, there isolated reports in the media concerning some of the youth involved in acts of terrorism or extremism. If I become a victim, the SAPS should let us know, what to do in order to reduce confusion around cybercrime and how to report it.

- **Theme 2: Lack of Collaboration Among Role Players to Respond Adequately to Cybercrime:**

When asked how effective collaboration was among the role players to respond adequately to cybercrime targeting the youth, the majority of the participants from both the youth and the SAPS lacked effective collaboration. The participants highlighted that there was a huge need for the SAPS to collaborate with other stakeholders. Participants alluded to the fact that cybercrime is different from other traditional crimes, where there is no crime scene, perpetrators may be miles away from the victims and the modusoperandi is much more sophisticated. The participants also indicated that the SAPS lacks sufficient infrastructure for information sharing and international co-operation in relations to share best practices to respond to cybercrime targeting the youth. It also emerged from the majority of the participants from both the SAPS and the youth, that the private companies and organisations, are often the first to become aware of emerging cybercrime threats, are the most at risk of such attacks, and are also best-placed to protect themselves as well as inform the public against such attacks.

The participants were of the view that information sharing arrangements between private-public organisations, especially with the SAPS, must be robust and effective. While there are sound policy reasons for certain barriers to information sharing, including privacy, commercial, and national security concerns, these must be balanced with the importance of sharing information to support our collective efforts to address the cybercrime challenge. The following are the responses from the SAPS officers when asked what could be done to improve the collaboration among role-players to respond adequately to cybercrime in order to reduce victimisation among youth.It is the best way would be to be more transparent, to have public and private negotiations or better working relationships. The private sector has certain skills and values and techniques that the public, for example SAPS, would not have.

Private sector will also have certain techniques that we use or maybe specific training that we use that they don't, so I will always prefer brainstorming sessions, conferences, work sessions, more transparency between the two SAPS and private sectors because you will start benefiting one another when you start working together. For example, banks will have certain threats that SAPS will know about but have not identified or have not gone around the specific technique that the banks would use and vice versa. And as for prosecution, all cybercrime related cases are reported to the police, so who's really doing prosecution, the police. If the banks do not

assist the police and vice versa or do not share their knowledge, skills, you can never fight the battle on your own. They cannot fight it on their own either.

RESEARCH METHODOLOGY

- **Objective:**
  - To know the status of the Cyber security awareness and nature of education in India and the central to any attempt to secure cyber space.
  - To study the types, nature and consequences of cybercrime in India and its solution.
- **Research Materials and Methods**

A qualitative research approach was used for the study for adequate insight into solving and achieving the research problems and objectives. In-depth interviews were conducted with members of the SAPS in order to get an understanding of the level of awareness they provide to the youth in India. The researcher adopted a non-probability purposive sampling comprising of Crime Intelligence Unit who were between the ages of 19and 35 years. Data was analysed inductively and thematically. A qualitative data analysis involves organising the insights of the interviewees, and accounting for and explaining the data gathered. Conclusions were drawn using a more qualitative approach of describing thethemes that emerged, rather than conducting statistical analysis, as this study followed a qualitative research technique as highlighted earlier.

RESULTS AND DISCUSSION

This section focuses on the findings of the study relating to the selected objectives. The aim of presenting the findings is to assess the level of awareness about cybercrime among the youth in the selected policing areas in Gauteng Province. There should be a co-ordinated approach by the SAPS in dealing with youth awareness regarding cybercrime and cybersecurity, in order to educate youth about the dangers of cyber space. Two themes emerged from the data and are presented below.

- **Cyber Threat and Cyber Awareness:**

Cyber security seeks to promote and ensure the overall security of digital information and information systems with a view to securing the information society. Criminal laws regulating the cyberspace tend to result in fewer prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries all over the world. Currently there is lack of research on cyber security awareness initiatives conducted by the South African Police Service (SAPS). Cyber-attacks are launched continuously by cyber criminals because of the gaps in cybersecurity. Various studies and experts' opinions estimate that the direct economic impact of cybercrime to be millions of Rands annually. Yet cybercrime continue tobe an offence that most experts agree thar has just begun stirring and criminals are getting smarter and better equipped. The dangers associated with the lack of cyber awareness among youth render it vital for everyone using technology and all role players to be thoroughly alerted to and educated about cybersecurity. It is also difficult to obtain accurate cybercrime statistics because of the unknown number of crimes that goes undetected and unreported.

It is imperative for everyone using technology to be aware of the potential information safety risks and how to identify and prevent them. In many instances, home users neither understand nor are they aware of the cyber risks associated with cyber space as they are

extremely vulnerable because of their inadequate knowledge and regarding how to protect themselves. They easily fall victim to cyber-attacks because they are ill-prepared to protect themselves in the cyber space. More and more children own mobile devices and these mobile devices have access to the internet, and therefore can be used to connect to social media sites and gain web access. Children's continuous use of social media has raised issues regarding their safety, privacy and abuse. Risks such as cyberbullying can harm children physically and emotionally if they are not protected. It is vital that children are informed of such risks and how to protect themselves while they are cyber space. They should be properly enlightened on how to identify cyber risks and how to avoid or minimise them. It is important that they are encouraged to keep themselves cyber safe. Cyber criminals are enjoying greater degrees of success on social networks because they are easier to target and users are more likely to fall for scams.

- **Cyber Security and Indian Concern:**

The biggest issue is that they are not properly educated on how to operate safely and securely in the technology environment. Lack of cybersecurity awareness can result in a great number of cyber threats that can lead to significant, long-lasting and negative impacts on the youth. Very few studies of this nature were conducted in India addressing cybersecurity awareness among the youth. Other studies generally addressed the lack of cybersecurity skills within the Indian Police Service investigation units. Lifestyle Theory suggests that individual of different ages participate indifferent kinds of lifestyle. These lifestyle differences, therefore, expose individuals of different ages to varying levels of risk of victimisation. It has been persistently reported that the youth are more likely to be victimised than older people.

India needs to create a massive awareness strategy since cybercrime occurs irrespective of age and education level. Awareness programmes are able to give basic knowledge about the safety in the cyber space. Internet users are as young as eight years old. Educating them, right from school is imperative as ignorance has been mooted as one of the main reasons that many people fall victims to cybercrime. There should be awareness raising to inform young people and parents about cybercrime through general awareness raising programs in schools. Children should be taught computer ethics education in schools. The Department of Basic Education can hold workshops for both kids and parents for better understanding of the cyber space. This strategy can be adopted to higher learning institutions. Education, learning and simulation will ensure knowledge of how to respond, what to look for, and why this is important.

India emphasises on the effectiveness of university programmes in promoting knowledge and values about cyber-crime as these programmes could improve future behaviour of students towards cybercrime in terms of safety and security. This would establish norms and adjust prospects for illegal or delinquent behaviours. Based on the review of above literatures it is anticipated that gender, age, and knowledge have significant influences on cybercrime. Children and adolescents represent a vulnerable group of users who spend a lot of time on the web and on social networks. They are exposed to the same threats as adults but the effect on them can be more even more devastating. These days, a worst fear in teenager's eyes is cyber bullying. It is becoming an alarming trend in the society. Youths are using the internet for playing games and communicating with friends, maintaining online blogs concerning their lives and interests, and

using social networking sites to develop and maintain relationships. Each of these behaviours could potentially lead a young person to encounter harassment.

- **Internet Behaviour and Cyber-Bulling**

The internet behaviours of young people could potentially cause them severe harm, with some recent media reports linking cyber bullying and online harassment to suicide-related deaths and attempted suicides among juveniles. Online communication tools open the door for friendships with other teens near and far. The risks that children may encounterwhen online are numerous and rather serious: exposure to inappropriate conversation; unwittingly becoming the subject of sexual fantasy; being sent indecent or obscene images; being asked to send indecent images of themselves or their friends; being engaged in sexually explicit talk; and being encouraged to perform sexually explicit acts on themselves or their friends.

Cyber-bullying is a fear when a person receives threats, negative comments or negative pictures or comments from another person. Cyber bullying is a negative effect of online communication between youth. Victims of cyber bullying often experience rumours, body shaming and lies spread on online social network. Bullies may post inappropriate or embarrassing pictures of their victims. Another aspect of cyber bullying involves using mean text messages as harassment. Cyber communication is society's newest way to interact. Online social networking websites, text messages and emails provide users with an effective, quick way to communicate with people all over the world. Teens, in particular, spend hours online every day, on computers or personal electronic devices. With social networking sites becoming increasingly popular, youth are able to stay connected to real and online friends.

Children and adolescents represent a vulnerable group of users who spend a lot of time on the web and on social networks. They are exposed to the same threats as adults, but the effect on them can even be more devastating. It is point out that the experience of abuse causes long-term effects on a person's later life, both physical, and psychological. The latter includes feelings of guilt or responsibility for the abuse, low self-esteem, feeling of inferiority, and depression. With internet pornography, one must also realise that the child is victimised each time anybody watches material depicting his or hersexual abuse.Due to the ease of disseminating material on the web and the impossibility of removing material once it is published, it is very difficult to stop the cycle of abuse.

- **Social Media and Social Networking:**

On social media platforms, these teens try to take on new personalities to fit the stereotypes around them. The craze of the youth for social media is associated with the psychological effects of adolescence. Adolescence isthe period of self-discovery and awareness. It is also a period of in life when children seek independence from parents. In this phase of life, teens try to create an identity for themselves. They want to be accepted by their peers and respected by others. Many teenagers turn to social networks, using them as safe havens and media for establishing new identity, marketing of self and networking with other users to gain local and if possible, international popularity. Youths use social networks for a variety of purposes ranging from interpersonal connection to entertainment to research. They spend most of the time uploading pictures, posting opinions, obtaining current and social news, downloading

wallpapers, ringtones, soft wares and music among other things. Chatting seems to be a major preoccupation of the adolescents on social networks as Facebook and other networks are used primarily as forums for communication exchange with friends after school and connecting with new ones.

Social networking sites are becoming more and more prone to online attacks as users continue to grow by the day. Addiction to smartphones has led to a spike in the number of people falling victim to cybercrime. Smartphone applications have inherent vulnerabilities, allowing them to be compromised by hackers and security threats. Smartphones have become a gateway for cyber criminals where once technology has been adopted, it is difficult to imagine life without it. Mobile applications are the new frontier for cybercrime. Due to the growing usage of mobile devices worldwide, web threats are no longer limited to conventional personal computers (PCs). App stores now ever as the sites for software download, while mobile apps serve as programmes we download onto our mobile devices.Users, including youth who download from app stores may end up downloading malware instead. Malware, short for malicious software, has become the latest attacking tool of cybercrime.

- **Conclusion**

There is a very lessawareness of cyber security and prevention measures for individuals and businessesin India. There are millions of internet users across the country with more malicious mobile apps emerging at a rapid speed. This rapid growth is facilitating the emergence of new attack vectors and opportunities for cyber criminals. It poses a significant future threat, especially among youth that are constantly exploring the new apps on their mobile devices. The fight against cybercrime and cyber threats requires a partnership between citizens, businesses, and government. There is a need for international collaboration of cybercrime and cyber security experts to enhance effective prevention. International collaboration is critical in securing the cyber space. Collaborating with countries that already have security would be crucial, as SA would learn from them as long as there is open communication and a willingness to give and accept input from others.

The awareness programmes need to be communicated throughout the different media platforms and to all other stakeholders. The model on the next page was adopted from a study conducted in India regarding awareness among youth on cybercrime and cyber security. The model explains how an individual who uses Internet is connected with various stakeholders, which can be schools, retail outlets, social media platforms, private or government sectors or banks for various transactions on a daily basis. The government can take initiative of creating awareness among youth and stakeholders at various levels, with multiple approaches. The government can inform and educate all internet users on cybercrime and what security measures are in place. Banks can alert and educate their customers through their banking websites about the dangers of using internet banking and how to protect themselves. There must be a sharing of information between media, ethical hackers, educational sectors, law enforcement agencies by proving information to reach all members of the society whenever it is required. The government should be up to date in terms of their cyber security measures and make sure that they have an updated information and awareness.

REFERENCES

- Asokhia, M. (2010). Enhancing national development and growth through combating cybercrime internet fraud: A comparative approach. Journal of Social Sciences, 23:13.
- Bele, J.L., Dimc, M., Rozman, D. &Jemec, A.S. (2014). Raising awareness of cybercrime-The use of education as a means of prevention and protection.In: Proceedings of the 10thInternational ConferenceMobile Learning, Feb. 28, March 2, 2014, Madrid, Spain [Online]. https://eric.ed.gov/?id=ED557216.
- Dlamini, Z. & Modise, M. (2012). In: Case studies in information warfare and security.
- Ephraim, P.E. (2013). African youths and the dangers of social networking: A culture-centred approach to using social media. Ethics and Information technology, [Online], 15(4). https://link.springer.com/content/pdf/10.1007/s10676-013-9333-2.pdf.
- Khan, M.F. (2013). End user awareness of cybersecurity challenges. B.Sc. thesis, Oulu University of Applied Sciences.
- Kritzinger, E. (2017). Cultivating a cyber-safety culture among school learners in South Africa. Africa education Review [Online], 14(1).https://www.tandfonline.com/doi/pdf/10.1080/18146627.2016.1224561?needAccess=true.
- Levin, A., Foster, M., West, B., Nicholson, M.J., Hernandez, T., & Cukier, W. (2008). The Next Digital
- Divide: Online Social Network Privacy. RyersonUniversity. Ted Rogers School of Management, Privacy and Cybercrime Institute [Online] March 2008. https://www.ryerson.ca/content/dam/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf.
- Orji, U. J. (2012). Cybersecurity Law and Regulation. Wolf legal publishers. [Online], Sept. 30. http://www.wolfpublishers.com/docs/73.pdf.
- Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety, 12, 99-118.
- Wang, H.S., Chou, C.H. & Tsai, S.N. (2008). A preliminary study of the education ofinternet security implied in a movie based English class in Taiwan's private vocational continuation high school. CNTE2008, Chichu, Taiwan.