

EVALUATION OF AWARENESS OF CYBERCRIME IN MEDICAL STUDENTS

Sagar Lande*¹ and Sandeep Kadu²

¹3rd Year MBBS, Undergraduate Student, DVVPF's Medical College, Ahmednagar, Maharashtra 414111, India.

²Professor and Head, Department of Forensic Medicine and Toxicology, DVVPF's Medical College, Ahmednagar, Maharashtra 414111, India.

Received date: 25 February 2020

Revised date: 15 March 2020

Accepted date: 05 April 2020

*Corresponding author: Sagar Lande

3rd Year MBBS, Undergraduate Student, DVVPF's Medical College, Ahmednagar, Maharashtra 414111, India.

ABSTRACT

Cybercrime is one of the vast growing area of criminality, all over the world. Definitions of cybercrime are variable, depends on purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. *Aim and objective:* 1) To assess the awareness about cybercrime and its related laws. 2) Assessment of precautions taken by respondents to prevent from being cyber victim. 3) Evaluation of cybercrime related knowledge. *Materials and methods:* The cross sectional questionnaire based descriptive study was performed in DVVPF's Medical College and Hospital, Ahmednagar (M.S). The structured questionnaire to gather relevant information pertaining to the research topic was designed and distributed among the participants. The data was collected and analysed statistically under expert guidance for number and percentage. *Results:* In our study 200 individuals were participated of which with 98% response rate 196 individuals responded. Our study reveals that 98(50%) individuals access their social networking account when they get bored. The Majority 140(71.4%) individuals don't use same password for different accounts while 168(85.7%) don't share their passwords with friends and relatives. Most of the participants, 153(78.1%) knows about strong password and aware about its use. For security purpose most of individuals 133(67.8%) have installed Antivirus on their devices. *Conclusion:* The study found that most of the individuals are aware of judicious use of social media, security and of privacy during its use. But the individuals needed to be informed about cybercrime laws and acts and about the various cybercrime related terms.

KEYWORDS: Cybercrime, cyberspace, cyber law, IT act, social media, cyber-attacks.

INTRODUCTION

A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime.^[1] The term "cyber" is a prefix used to describe an idea as part of the computer, laptop, smartphone and information age and "crime" can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. The Commonwealth of Independent States Agreement, without using the term 'cybercrime',^[2] defines an 'offence relating to computer information' as a 'criminal act of which the target is computer information'.^[3] Similarly, the Shanghai Cooperation organization Agreement defines 'information offences' as 'the use of information resources and (or) the impact on them in the informational sphere for illegal purposes'.^[4] Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years.^[5]

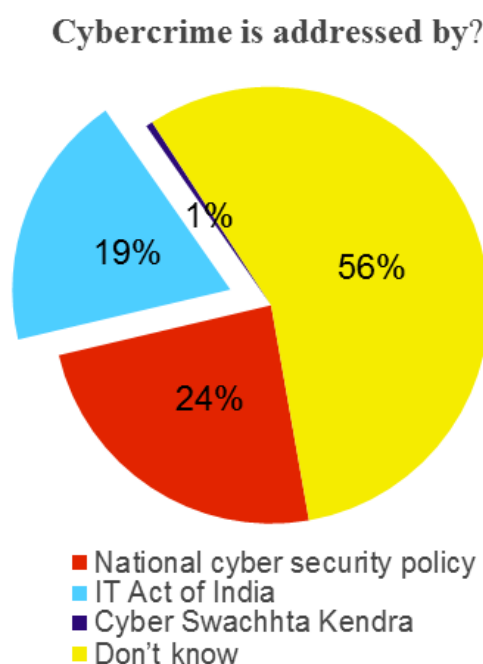
Cyber related risks are worldwide threat of bloodless war. Earlier Cybercrime was considered as only the crime related to computer and hacking. Cybercrime includes phishing, vishing, cyber stalking, carding, spoofing, hacking, cyber harassment, etc. Cybercrime in all of its forms is one of the fastest growing areas of criminality all over the world. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, as well as the deployment of viruses, and various email scams such as phishing.^[6,7]

Cybercrime is an innovative weapon used by modern criminals for crime in this era of technology. It can only be tackled by using the new innovative methods and creating awareness it. There is need of educating people about the technology and it's safe use. A social networking site is the phrase used to describe any

website that enables users to create public profiles within that web site and form relationships with other users of the same website who access their profile.^[8] The present study throws light on the awareness of medical graduates about cybercrime, cybercrime related laws and precautions taken by them.

MATERIALS AND METHODS

A Cross sectional descriptive study with sample size of 200 with Non Proportional Quota Purposive Random Sampling method was carried out with a questionnaire. The questionnaire was designed and validated for our study. In our study 200 individuals were participated. *Inclusion criteria:* Medical students between 17-25 years of age willing to participate in the study and able to give informed consent. *Exclusion criteria:* Medical students of above 25 and below 17 years of age and those who never used any electronic device. The study was performed in DVVPF's Medical college and Hospital, Ahmednagar, Maharashtra. IEC approval was taken prior to the study. Expert statistical guidance was obtained to analyze the data gathered in this study. The confidentiality about research data and identity of an individual is maintained according to ICMR guidelines.



RESULT

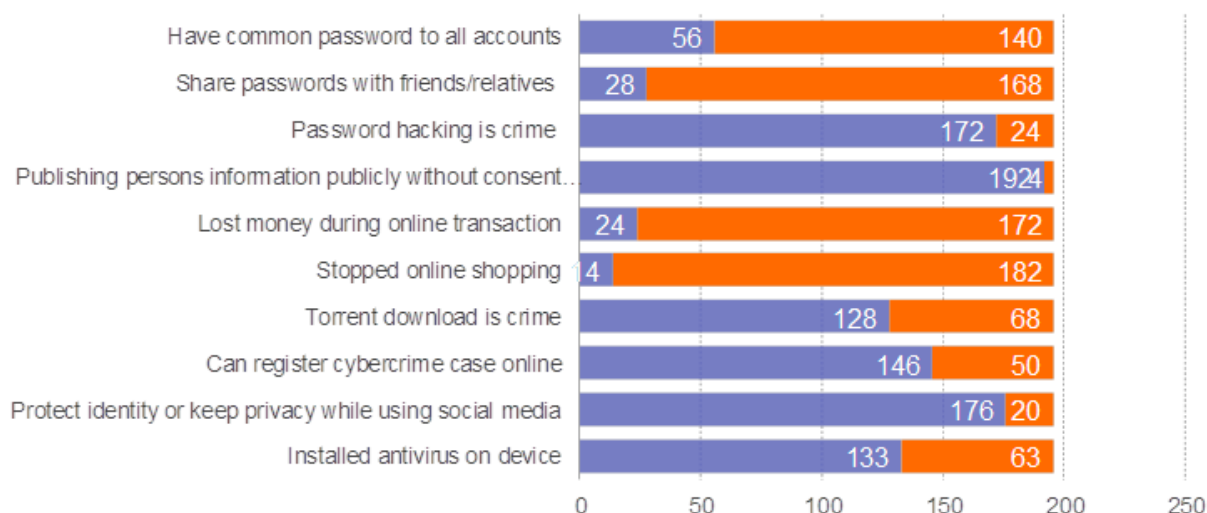
In our study 200 individuals were participated of which with 98% response rate 196 individuals responded. Among participants, 110 were Female and 86 were Male of the 17 to 25 age group. From the results almost everyone have been using smartphone and most of them have been using/ used laptops and computers. Majority of individuals use Internet for surfing, followed by for watching educational videos, YouTube, music, downloads and other purposes. Most of the individuals prefer to download educational videos followed by

Entertainment videos, Music and others. Almost every individual uses WhatsApp, Facebook and Instagram, snapchat, Twitter, Google plus, yahoo, tiktok.

Our study reveals that 98(50%) individuals access their social networking account when they get bored, 69(35.2%) individuals access whenever they gets time while rest 29(14.8%) individuals rarely access in a day. Almost, nearly three-fourth of individuals 139(70.9%) reported that, they access their social media after 9pm onwards, while 54(27.6%) individuals access between 5 pm to 9 pm and remaining 1.5 percent individuals assess during rest of the time. Study also reveals that, 131(66.8 %) individuals spend less than 2 hrs on social media, 62(31.6%) spend between 2-6 hrs, while remaining spend 6-10 hrs on social media. Nearly three-fourth, 140(71.4%) individuals don't use same password for different accounts while 168(85.7%) individuals don't share their passwords with friends and relatives. Study also reveals that majority, 153(78.1%) individuals knows about strong password and aware about its use. Most of individuals 172(87.8%) are aware about password hacking and knows it is a crime. Almost every individual 192(97.9%) are aware that publishing publicly person's information without his consent is a crime. A minority of participants 24(12.2%) reported that, they have lost money during online transactions and 14(7.1%) of them have stopped online shopping due to this issue. Majority of individuals 128(65.3%) are aware that the torrent download is a crime. Surprisingly, only 37(19%) individual have knowledge that cybercrime is addressed, according to IT Act of India, 2000 while majority of them, i .e. 110(56.1%) individuals are not known about any of the Cyber Act (See Pie diagram). Almost three-fourth, 146(74.5%) individuals are aware that they can register cyber case online. Almost half 89(45.4%) individuals Rarely, 33(16.8%) individuals Never, 28(14.3%) individuals Quarterly, 24(12.2%) individual yearly, 17(8.7%) individuals monthly and almost negligible 5(2.6%) individuals weekly change login details of their online accounts. Our study also reveals that 176(89.8%) individuals protect their identity and keeps privacy while using social media. It also reveals 84(42.9%) individuals Every-time, 71(36.2%) individuals sometime, 33(16.8%) individuals rarely and 8(4.1%) individuals never check security setting while posting on social media. For security 133(67.8%) individuals have installed Antivirus on their devices. Result of terms related to cybercrime and level of understanding is given in Table below.

Terms related to Cybercrime and level of understanding					
Terms	Whether Knows the term		If yes, level of understanding?		
	Yes	No	Heard	Superficial	Deep
Online Harassment	172(87.8%)	24(12.2%)	34(17.3%)	110(56.1%)	28(14.3%)
Cyber stalking	173(88.3%)	23(11.7%)	40(20.4%)	109(55.6%)	24(12.2%)
Hacking	188(95.9%)	8(4.1%)	32(16.3%)	105(53.6%)	51(26%)
Spoofing	96(48.5%)	100(51.5%)	64(32.7%)	22(11.2%)	10(5.1%)
Carding	72(36.7%)	124(63.3%)	50(25.5%)	15(7.6%)	7(3.6%)
Virus/ Trojan attack	174(88.8%)	22(11.2%)	56(28.6%)	85(43.4%)	33(16.8%)
Spamming	159(81.1%)	37(18.9%)	44(22.4%)	75(38.3%)	40(20.4%)
Child pornography/ child sexual abuse material	168(85.7%)	28(14.3%)	41(20.9%)	87(44.4%)	40(20.4%)
Cyber bullying	141(71.9%)	55(28.1%)	40(20.4%)	63(32.1%)	28(14.4%)
Sextortion	118(60.2%)	78(39.8%)	51(26%)	48(24.5%)	19(9.7%)
Cryptojacking	69(35.2%)	127(64.8%)	39(19.9%)	24(12.2%)	6(3.1%)
Pharming	58(29.6%)	138(70.4%)	33(16.8%)	15(7.6%)	10(5.1%)
Phishing	70(35.7%)	126(64.3%)	35(17.9%)	21(10.7%)	14(7.1%)
Vishing	47(24%)	149(76%)	26(13.3%)	17(8.7%)	4(2%)
Ransomware	73(37.2%)	123(62.8%)	36(18.4%)	27(13.8%)	10(5.1%)
Cyber Grooming	78(39.8%)	118(60.2%)	44(22.4%)	25(12.8%)	9(4.6%)
Website Defacement	68(34.7%)	128(65.3%)	34(17.3%)	28(14.3%)	6(3.1%)

Graph 1



DISCUSSION

Cybercrime's in India almost doubled in 2017, according to statistics released by the National Crime Record Bureau (NCRB) on October 22, 2019. Karnataka had the highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttar Pradesh. The total number of offences under the IT Act was the highest in Uttar Pradesh, followed by Karnataka (3,152), Rajasthan (950), Assam (941) and Maharashtra (586). Highest number of cases have been reported in Maharashtra related to Cyberstalking and Cyberbullying.^[9]

Nowadays every individual is having smartphone, from teenager to elder. Most of the families have laptops or computers at their home. Due to this there is easy access to internet which have increased the risk of cybercrime. Internet has made this world "The Global Village", but along with pros it also have cons. Study shows that the

individuals are very much active on social media. But as the study sample was Indian medical graduates they along with social media also use Internet for educational purposes and downloading the files related to academics. Every individual have the access WhatsApp or other social media account. Most of the respondents access their social media accounts whenever they gets bored, while some access rarely in a day. Due to their studies and posting schedule usually uses internet after 9pm onwards, while use to spend less than 2 hrs daily on social media.

For security reasons majority of individuals don't use same passwords for different accounts, keep passwords private and aware about the use of strong password. Majority of them are aware, password hacking and publishing person's information publicly without his consent is a crime. Very few have been victim of

cybercrime. Most of the individuals have very poor knowledge about the cybercrime related laws and Acts. But are aware about reporting case online. Login details should be changed monthly, but very few individuals are aware about this. Most of them are aware of keeping privacy and protecting identity. Majority of individuals tend to check their security setting every-time before posting on social media. More than half of individuals have installed antivirus on their devices. Almost half of the cybercrime related terms were unknown and most of them were having superficial understanding.

CONCLUSION

Cybercrime in any of its form is a fastest growing area of criminality. Today's cybercrime policy is concerned with particular online risks adolescents are exposed and other issues such as exposure to harmful or illegal content.

The younger generations,^[10] which use the internet and other online technologies extensively for staying connected for all day to day work and entertainment, including information, e-mails, social networking, e-banking, e-shopping, web-TV, news, education, home-work research, online gaming, downloading music, videos, movies and other contents etc., are more vulnerable to targeted cyber-crime. Most of the individuals are aware of judicious use of social media, security and of privacy during its use. Majority are aware of password safety, keeping of strong password and changing login details. But the individuals needed to be informed about cybercrime laws and acts and about the various cybercrime related terms.

Future scope: 1) Based on current studies, much more studies regarding this should be carried out by giving proper time and interventional lecture and results should be compared with previous studies 2) This study also provides new knowledge and adds to the scientific pool on this topic of research. 3) Actually there is not much study on this research topic, so results obtained by this study will be helpful to future researchers who may be interested in their region. 4) Nowadays the cybercrime is the newly evolving area of criminality in the world, which have increased challenges before the experts to deal with it. So there is much more need to do research in this area and to literate and provide necessary information about precautions to be taken to the society.

REFERENCES

1. Comprehensive study on Cybercrime. United Nations Office on Drug and Crime, 2013 Feb
2. The original agreement is in Russian language and uses the term 'преступление в сфере компьютерной информации', rather than the contemporary equivalent to 'cybercrime': киберпреступности'.
3. Commonwealth of Independent States Agreement, Art., 1(a).
4. Shanghai Cooperation Organization Agreement, Annex, 1.
5. Rajesh D Kharat, Rahul V Kedare. Study of Awareness about Cybercrime among Medical Undergraduates. Indian J Forensic Med Pathol, 2019; 12(3): 189-193.
6. Mohammad MK. Nature of cybercrime and its impacts on young people: A case from Bangladesh. Asian Social Science, 2012; 8(15): 171-83.
7. <https://www.colorado.gov/pacific/dhsem/cyber-crime>.
8. Gupta S. Impact of cybercrime on adolescents through social networking sites. International Journal of Law, 2012; 3(6): 104-7.
9. <http://ncrb.gov.in/StatPublications/CII/CII2017/pdfs/CII2017-Full.pdf>.
10. D.Mahalakshmi, Dr.D.Prabhakaran, Dr.A. Sivalingam and Dr.M.Thirumarimurugan, "A Study on Cyberspace and its Impact in Society", IRACST-International Journal of Research in Management & Technology (IJRMT), ISSN: 2249-9563, 2016; 6(1).