Global Journal of Medicine & Public Health

Knowledge attitude and practices towards cybercrimes among medical students in Kerala - A cross-sectional study

Pratibha Dabas [1], Remya Ramachandran [2], Neena Priyadarshini A V [3], Ali Zameel B [4], Nirmal C [5], Drisya M [6]*

ABSTRACT

Background

Digitalization, information, and communication technology usage is increasing. The younger generation is vulnerable to cybercrimes. This study was planned to assess the knowledge, attitude, and practice related to cybercrimes among college students across Kerala.

Material and Method

A cross-sectional study was done using a semi-structured questionnaire. Sample size was taken as 663 students. The data were entered into excel sheet and analyzed using SPSS software version 21.0 (IBM Inc). Frequencies and percentages were calculated for all the categorical variables and presented in the form of mean, proportion and percentage. Chi square test was applied to test significant differences with gender and type of academic courses.

Results

Our study showed that all study subjects were aware of the cybercrimes and 54.1% were aware of cyber laws. Practice of various online risk behaviour was high. Higher risk behaviours was found to be associated with male gender and engineering students as compared to the medical students.

Conclusion

There is a need for propagation of awareness regarding cybercrimes and risk behaviours among students.

Key-words: Cybercrimes, Cyber-laws, Online risk behaviour, Social media

GJMEDPH 2023; Vol. 12, issue 4 | OPEN ACCESS

5*Corresponding author:Nirmal C, Assistant Professor, Department of Community Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India; 1-Pratibha Dabas, Professor & HOD, Department of Community Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India; 2.Remya Ramachandran, Assistant Professor, Department of Community Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India; 3.Neena Priyadarshini A V, Associate Professor, Department of Forensic Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India; 4.Ali Zameel B, Associate Professor, Department of Community Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India; 6.Drisya M – Biostatistician, Department of Community Medicine, Malabar Medical College and Research Center, Calicut, Kerala, India

Conflict of Interest—none | **Funding source**: none

INTRODUCTION

Digital technology has interconnected geographies, cultures, and people globally. India is the second-largest internet population in the world. While it helps progress, it also brings new vulnerabilities. Cybercrimes are increasing with increased usage and advancing technologies.(1)Cybercrime is an illegal act committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim via modern communication networks. (2)

Various types of cybercrime are:
Hacking: It means unauthorized access to computer system or network (3), and it is the most predominant form of cyber crime. It is an invasion into the privacy of data.

- Cyber Stalking: behaviour wherein an individual wilfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes that person. (4)
- Harassment via E-mail: It is a form of harassment, which includes blackmailing, threatening, and constant letters in anonymous names or regular sending of embarrassing mails to one's mail box. (4)
- Cyber sexual defamation: It happens between real or virtually known people who out of frustration start publishing defaming stories in obscene languages on various social platforms (4)
- Morphing: it is the editing the original pictures so as to make it look completely or largely different. (4)
- Email spoofing: It is used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. (4)
- Phishing: a malicious individual or group who scam users. They do so by sending emails or creating web-pages that are designed to collect an individual's online bank credit card, or other login information. (5)

Cybercrimes related risk behaviours are (6):

- Psychological reasons: loneliness, insecurity, lack of family support.
- Knowledge of computers: partial computer literacy, difference in gender perspectives related to internet usage
- Sociological perspectives: nurturing practices, patriarchal society, family honour, cyber harassment leads to social harassment.
- Gap between law and technological advancement: lack of awareness about cyber laws, anonymity of miscreants

The Covid-19 induced lockdown saw a spurt in cybercrimes in India with Kerala recording the highest number during the period. A majority of the recorded attacks were phishing attacks with sophisticated campaigns that could easily snare even the most educated users (3).This study aimed to assess the knowledge, attitude, and practice regarding cybercrimes among college students across Kerala.

Material and methods

The cross-sectional study was carried out across the college students of Kerala. Students unwilling to participate were excluded.

The sample size was calculated by using the formula –

$$n = \frac{Z^2_{(1-\alpha/2)} * (p * q)}{d^2}$$

Where, n = sample size, Z^2 (1-α/2) = standard normal deviate for α=95%, value is 1.96
p= prevalence of awareness of cybercrimes
q= (1-p), d = allowable error, which is 5%.
Here p= 50 [unawareness regarding cybercrimes]
Z = 1.96
p= 0.5
d= 0.05
q= 0.5
n = $4 \times 0.03 \times 0.97/(0.015)^2$ = 517
The sample size was calcualted as 517.

- Study tool: Interviewer administered semi structured questionnaire was used to assess the knowledge, attitude and practice regarding cyber crime
- Data collection: After taking informed consent; data were collected using Google form
- Study period was during February, 2021.

The data were entered into excel sheet and analyzed using SPSS software version 21.0 (IBM Inc). Frequencies and percentages were calculated for all the categorical variables and presented in

the form of mean, proportion and percentage. Chi square test was applied to test significant differences with gender and type of academic courses.

RESULTS

Final sample size was 663. In our study, 474 (71.5 %) participants were females and 189 (28.5%) were males. Mean age was 22 years (Range:18 - 26 years). Educational studies being carried out by the paticipants is given in Table 1.

Table 1: Educational studies of the participants (N = 663)

Course	Frequency	Percentage
MBBS	411	61.9
Courses other than medical and engineering	85	12.8
Engineering courses	77	11.6
Medical allied courses other than MBBS	69	10.4
Less than graduate students	21	3.2

Time spent online varied among the students. About one-fifth (110, 16.6%) spent more than six hours, 190 (28.6%) spent 4 to 6 hours, 218 (28.6%) spent 2-4 hours, 127 (19.2%) spent 30 minutes to 2 hours and only 18 (2.7%) spent less than 30 minutes online daily. Social media presence and utilization is given in Table 2.

Table 2: Social media utilization by the participants (N = 663)

Social media site	Users (n,%)	Public profile (n,%)
WhatsApp	660 (99.5%)	71 (10.7%)
Telegram	569 (85.8%)	77 (13.5%)
Instagram	562 (84.8%)	82 (14.1%)
Youtube	528 (79.6%)	108 (20.4%)
Facebook	429 (64.7%)	117 (27.2%)
Snapchat	290 (43.7%)	30 (10.3%)
Pinterest	208 (31.4%)	35 (16.8%)
Twitter	152 (22.9%)	47 (30.9%)
LinkedIn	121 (18.2%)	46 (38.0%)
Discord	97 (14.6%)	22 (22.7%)

Online risk behavior was high. Online risk behaviours are given in Table 3.

Table 3: Online risk behaviours of the participants (N = 663)

Risk Behaviors	Frequency	Percentage
Not always reading privacy guidelines	451	68.0
Not logging out from their accounts after use	393	59.3
Not logging into their accounts for a long time	263	39.6
Downloading files from third party sites	203	30.6
Sharing photos and videos online	190	28.6
Attending spam calls or messages	144	21.7
Interacting with online strangers	138	20.8
Clicking on hyperlink from social networks	111	16.7

Opening email attachments from unknown sources	108	16.3
Sharing their profile/email passwords with others	84	14.5
Visiting restricted sites with adult material	91	13.7
Placing stranges in their buddy list	52	7.8
Shared financial details online	35	5.3
Sharing personal information with the strangers	14	2.1

Of 663 participants, 46 (7%) reported to be victims of a fake account impersonating them. Hundred participants (15.1%) reported to have received messages, images or videos with sexual content. Eleven (1.6%) were threatened of their privacy. Eighty eight (13.3%) reported to have been a victim of online financial fraud.The online risk behaviour was significantly associated with male gender. Males (45.5%) were significantly more likely to share photos, videos and personal details in the public platform as compared to females (21.9%). While females (24.3%) were significantly more likely to interact with strangers as compared to males (12.2%), males (12.7%) were significiantly more likely to add strangers to their buddy list as compared to females (5.9%). Males (29.6 %) were significantly more likely to access restricted sites as compared to females (7.4%). Males were also siginificantly more likely to click on social networks' hyperlinks and download materials from thrid party sites as compared to females. (Table 4)

Table 4: Online risk behaviour association with gender (N = 663)

		Gender		Total	Chi square	p value
		male	female			
Do you read the privacy guidelines of social networking sites?	Yes	48	164	212		
	No	141	310	451	5.26	0.022
Do you share your photos, videos and any other personal details in the public platform?	Yes	86	104	190		
	No	103	370	473	36.69	**0.0001**
What is your attitude when a stranger approaches you online?	No-interaction	166	359	525		
	Interaction	23	115	138	11.988	**0.001**
Placing strangers on buddy list	Yes	24	28	52		
	No	165	446	611	8.622	**0.003**
Sending personal information to strangers	Yes	7	7	14	3.242	0.072
	No	182	467	649		
Visiting restricted sites containing adult material	Yes	56	35	91		
	No	133	439	572	56.469	**0.0001**
Opening email attachments from unknown sources	Yes	32	76	108		
	No	157	398	555	0.08	0.778
	Yes	43	68	111		**0.009**

Clicking on hyperlink from social networks	No	146	406	552	6.849	
Downloading files from third party sites	Yes	95	108	203		
	No	94	366	460	48.031	**0.0001**
Not logging into your account for a long time	Yes	77	186	263		
	No	112	288	400	0.127	0.721
Not logging out from your account after use	Yes	115	278	393		
	No	74	196	270	0.27	0.603
Attended spam calls / messages	Yes	44	100	144		
	No	145	374	519	0.379	0.538
Shared you financial details online	Yes	13	22	35		
	No	176	452	628	1.352	0.245
Allowed others to use your email ID / profile ID / passwords etc	Yes	21	63	84		
	No	168	411	579	0.58	0.446
Have you ever lost money online?	Yes	31	57	88		
	No	158	417	575	2.249	0.134
Are you aware of the existing cyber laws in India?	Yes	91	268	359		
	No	98	206	304	3.833	0.05

Few of the online risk behaviours were found to be signifiantly higher among the engineering students as compared to medical students. Clicking on the hyperlinks was significantly higher among engineering students (28.5%) as compared to Medical allied (21.8%), non-graduates (19%), non-medico / non-engineering graduates (18.8%), and MBBS students (13.1%). Engineering students also had signficant higher prevalence of downloading from unknown sources (48%), not loggin into their accounts for a long period (53.2%), not logging-out of accounts (71.4%) and attending to spam messages (31.1%). (Table 5)

Table 5: Online risk behaviour association with type of academic course (N = 663)

		Academic courses					Total	Chi square	P value
		MBBS	Medical (allied)	Other than medical/ engineering graduate	Engineering	Non graduate students			
Do you read the privacy guidelines of social	Yes	137	22	27	19	7	212		
	No	274	47	58	58	14	451	2.255	0.69

networking sites?									
Do you share your photos, videos and any other personal details in the public platform?	Yes	108	21	25	29	7	190		
	No	303	48	60	48	14	473	4.548	0.34
What is your attitude when a stranger approaches you online?	No-interaction	333	52	64	62	14	525	4.314	0.365
	Interaction	78	17	21	15	7	138		
Placing strangers on buddy list	Yes	28	4	6	11	3	52	6.703	0.152
	No	383	65	79	66	18	611		
Sending personal information to strangers	Yes	11	0	1	2	0	14	3.023	0.554
	No	400	69	84	75	21	649		
Visiting restricted sites containing adult material	Yes	51	12	13	13	2	91	2.523	0.641
	No	360	57	72	64	19	572		
Opening email attachments from unknown sources	Yes	67	13	16	8	4	108	2.812	0.59
	No	344	56	69	69	17	555		
Clicking on hyperlink from social networks	Yes	54	15	16	22	4	111	13.139	0.011
	No	357	54	69	55	17	552		
Downloading files from third party sites	Yes	115	18	27	37	6	203	13.123	0.011
	No	296	51	58	40	15	460		
Not logging into your account for a long time	Yes	166	25	26	41	5	263	11.497	0.022
	No	245	44	59	36	16	400		
Not logging out from your account after use	Yes	243	44	42	55	9	393	11.063	0.026
	No	168	25	43	22	12	270		
	Yes	86	20	13	24	1	144	11.955	0.018

Attended spam calls / messages	No	325	49	72	53	20	519		
Shared you financial details online	Yes	20	5	4	5	1	35	0.968	0.915
	No	391	64	81	72	20	628		
Allowed others to use your email ID / profile ID / passwords etc	Yes	60	7	5	10	2	84	5.513	0.239
	No	351	62	80	67	19	579		
	Prefer not to answer	11	2	1	3	1	18		
Have you ever lost money online?	Yes	51	14	11	6	6	88	9.505	0.05
	No	360	55	74	71	15	575		
Are you aware of the existing cyber laws in India?	Yes	221	39	54	35	10	359	5.898	0.207
	No	190	30	31	42	11	304		

Assessment on awarness of cyber laws

Out of 663 participants of study population, 359 (54.1%) were aware of existing cyber laws in India and 304 (45.9%) were unaware. The awareness about cyberlaws was not significantly different for gender or type of academic study.

DISCUSSION

In our study we assessed the awareness of cybercrime, its prevalence among various social media platforms and identified online risk behaviours among college students. The level of awareness regarding cybercrime was found to be in line with study conducted in Nigeria which was nearly 100%. Our study found males were more likely to adopt high risk online behaviours However, no statistical significance was found between mean scores of male and female students in the Nigerian study. This maybe due to the social differeneces in the two societies.(7)

A study conducted among medical students in Mumbai found that 50% were aware of cybercrimes and 8% shared passwords.(8) Similarly, in our study, password sharing was found to be 14.1 %. However, awareness regarding cybercrime was higher (100%) in our study.

In the study conducted in UK regarding cybercrime prevalence and impact showed that 3% of the population were affected from cybercrimes and losing money online. (9) Whereas in our study, 13.3% reported to have been affected by fiancial fraud online.

CONCLUSION

Our study shows that all study subjects were aware of the cybercrimes and 54.1% were aware of cyber laws. Practice of various online risk behaviour was high. Higher risk behaviours was found to be associated with male gender. Medical students had lower prevelence of online risk practices as compared to the engineering students. We recommend larger scale studies to understand the behaviour towards cyber crime. There is a need for propagation of awareness regarding cybercrimes and risk behaviours among students.

REFERENCES

1. Sandhya Keelery. Cyber crime in India, statistics and facts. July 2020. Statista - the statistics portal [Internet]. Statista. [cited 2023 Oct 10]. Available from: https://www.statista.com

2.Misra R. Cyber crimes against women. Social Science Research Network. 2013.

3.Tanushree GL. Hacking- An In-Depth Analysis. International Journal of Legal Science and Innovation. 1(2).

4.Shobhna Jeet. Cyber crimes against women in India: Information Technology Act. Elixir International Journal. 2000;12.

5. Priyanjali karmakar.types of cyber crimes and causes. Legal service india E. Journal.

6.Saha T, Srivastava A. Indian women at risk in cyber space : a conceptual model of reasons of victimization. International Jouranal of Cyber Criminology. 2014;8(6).

7.Awareness and involvement in cybercrime among undergraduate students in universities in River State. Nigeria, International Journal of humanities and social science invention. 2018;7(7):39–43.

8. Dr.Ashutosh B Potdar and Pratapsingh Ishwar Rathod . Study of awareness of cyber security among medical students. Indian Journal of Forensic Medicine and Toxicology. 2019;(8).

9. Hernandez-Castro J. Eerke Boiten , cyber crime prevalence and impact in the UK. 2014.