DOI: http://dx.doi.org/10.18203/2394-6040.ijcmph20195868

Original Research Article

Knowledge, attitude and practice study on awareness and preventing cyber threats among the electronic devices used by the doctors of government medical college Vellore, Tamil Nadu, India

Balaji J.*, Ganesh G.

Department of Community Medicine, Government Medical College Vellore, Tamil Nadu, India

Received: 12 November 2019
Revised: 11 December 2019
Accepted: 12 December 2019

***Correspondence:**
Dr. Balaji J.,
E-mail: balajij83@gmail.com

ABSTRACT

Background: Now a days the whole World is submerged with digital electronics devices round the clock for all utilities. Even the doctor community also is not spared by these digital gadgets. Almost every doctor in India is permanently having and operating a smart phone and laptops or desktops plus vide computer applications.

Methods: This cross-sectional study was conducted among 45 doctors across 7 departments of Government Medical College, Vellore. Mean, median, mode, standard deviation was used for quantitative data and Pearson chi square test and logistic regression was used for qualitative data using trial version of SPSS 22.

Results: The mean score was 11.2±2.8 with mean scoring percentile of 38.8±6.5. There was Pearsons Chi square significance for Variables like exposure to external resources and, Books related to cyber security, age less than 34 years and average spending time with electronic devices >2.5 hours per day, designation MD versus MBBS, gender difference.

Conclusions: On running logistic regression the multivariate analysis for study variables with statistical significance was seen for four variables- exposure to external resources, and books related to cyber security, age <34 years, average spending time with electronic devices >2.5 hours per day. Designation and gender variables lost their significance on logistic regression analysis.

Keywords: KAP, Cyber threats, Cyber security, Vellore Medical College, Tamil Nadu

INTRODUCTION

Daily all over the world - digital supremacy or rapid advances in technology and digital field is actively playing a special role in each of our lives. There is a Callous attitude that all these digital and electronic Knowledge is attributable to the technical or a closed group in parallel with computer and allied science field and its working members alone. But now it’s time even for medical fraternity to have a basic sound knowledge on gadgets, cyber security, cyber threats, current looming online cheats, and more over the different ways to safe guard our devices form intruders and safe guard our patients medical data which is of utmost priority at all times to all doctors always.

Lot’s of studies in our medical world focuses on Stiff neck syndrome, dry eye syndrome, insomnia or mood disorders for over usage of digital world. Only a very few or rare studies concentrate on KAP model to prevent our gadgets from malicious and hacking programs or malwares - particularly among doctors.

So, this study will be concentrating on the basic levels of Securing our digital devices and medical data of our precious patients that is generated day to day in our medical world at all levels, right from the primary level (PHC) to tertiary level (research institutes).

India is the third most vulnerable country to cyber threats like malware, spam and ransomware United states with 26% stands globally first followed by China with 11% in 2017.[1]

METHODS

This study is a cross sectional study. This study was conducted among 45 doctors of seven (7) non-clinical departments (anatomy, physiology, bio chemistry, pathology, microbiology, pharmacology and forensic medicine) of government medical college Vellore. During the period of May 2018 to August 2018.

Inclusion criteria

All the willing doctors, particularly the teaching Faculties in all cadres were included in my study.

Exclusion criteria

Those who did not want to participate in this study were excluded.

Sampling technique

Convenient sampling technique was used for sampling.

Study tool

A pre structured questionnaire on basics of day to day using electronic devices, operations and cyberthreats in multiple choice questionnaire format framed from (CyberSwachhtakendra.gov.in - Indian Government Website Nodal and Support Centre).

Data collection

Participants were strictly advised not to refer or Google the answers while filling and answer keys was given at their submission of filled data forms along with reference from Cyber Swachhtakendra.gov.in with Appropriate keys. The pre structured questionnaire with 25 objective type multiple choice question format, carefully framed questions on day to day using electronic devices operations and cyber threats was selected. Total of 25 marks allotted and the percentile also calculated to 100.

Data analysis

Trail version of SPSS 22 was used for statistical software. All the quantitative Variables were calculated as mean±Standard deviation, Pearson Chi square test was used to assess the statistical significance. P-value of less than or equal to 0.05 indicates significance. Logistic regression - co-efficient of Beta (r2) was also done as multi variate analysis.

RESULTS

Mean age group of this study subjects was 29.8±5.4 (mean ±2 SD) in years.

Table 1: Gender distribution among study subjects.

Gender	Frequency	Percentile (%)
Male	22	55
Female	18	45
Total	40	100

Mean years of service or teaching experience of study subjects is 4.8±4 (mean±2 SD) in years.

On gender distribution pattern in this study - males constituted 55% (n=22) and Females constituted 45% (n=18).

Table 2: Distribution of residence among study subjects.

Place of residence	Frequency	Percentile
Urban	24	60
Rural	10	25
Not clear	6	15
Total	40	100

On the distribution of residence pattern in this study - subjects from urban constituted 60% (n=24) and subjects from Rural constituted 25% (n=10).

On the distribution of designation or cadre wise of study subjects

Subjects from Senior Assistant Professor cadre constituted 37.5% (n=15) and tutors constituted 27.5% (n=11), the professor cadre constituted 7.5% (n=3).

Table 3: Distribution of designation of study subjects.

Designation	Frequency	Percentile
Professor	3	7.5
Associate	8	20
Senior assistant	15	37.5
Assistant	3	7.5
Tutor	11	27.5
Total	40	100

Only 12.5% (n=5) of the study subjects has read books and articles related to cyber security context.

Only 15 % (n=6) of the study subjects had exposed to external resources related to cyber security context. Here the external resources included are videos, talk shows, conclave, panel discussion with concerned experts or any other training programs or activities related to this study outcome variable or independent variable (cyber security and threats).

Table 4: Books imbibed or read related to cyber threats and security among the study subjects.

	Frequency	Percentile
Yes	5	12.5
No	35	87.5
Total	40	100

Table 5: Other external resources exposed related to cyber threats and security among the study subjects.

	Frequency	Percentile
Yes	6	15
No	34	85
Total	40	100

Out of the total 25 multiple choice questions related to cyber security knowledge. Each right answer carries one mark and Maximum total per subject is 25. 70% (n=28) scored less than 8 marks, 30% (n=12) scored more than 8 marks.

In this study 40% (n=16) spend more than 2.5 hours a day with electronic devices and 60% (n=24) spend less than 2.5 hours a day.

Table 6: Spending time with electronic devices (average in hours per day of study subjects).

	Frequency	Percentile
Less than 2.5 hours per day	24	60
More than 2.5 hours per day	16	40
Total	40	100

Table 7: Scoring marks and percentile of study subjects.

	Frequency	Percentile
Less than 8 (total 25)	28	70
More than 8 (total 25)	12	30
Total	40	100

Table 8: Univariate analysis for study variables with Pearson chi square significance.

Study variables	DF	P value
Exposure to external resources related to cyber security	1	0.02
Books read related to cyber security	1	0.05
Masters verses non masters (qualification)	2	0.03
Age <34 years verses age >35 years	2	0.05
Spending time with electronic devices (>2.5 hours per day)	2	0.01
Gender wise (male versus female)	2	0.04

Table 9: Multi variate analysis for study variables with statistical significance on logistic regression.

Study variables	Df	P value	R^2 beta co-efficient	95 % confidence interval (C.I)	
				Lower	Higher
Exposure to external resources related to cyber security	1	0.03	0.70	0.40	0.92
Books related to cyber security	1	0.05	0.66	1.2	2.6
Age <34 years verses age >35 years	2	0.05	0.77	1.0	3.4
Spending time with electronic devices (> 2.5 hours per day)	2	0.02	0.86	1.45	1.88
Gender wise (male versus female)	2	2.09	0.40	0.30	1.88
Masters verses non masters	2	3.85	0.22	0.7	2.09

On running the univariate analysis for study variables with statistical significance on Pearson s chi square test (p value <or=5) was seen for six variables - 1. Exposure to external resources, 2. books related to cyber security 3. age less than 34 years and 4. spending time with electronic devices >2.5 hours per day, 5. designation of masters (MD) verses non masters (MBBS) and 6. gender difference (males versus females).

On running the multivariate analysis for study variables with statistical significance on logistic regression was seen for four variables exposure to external resources, books related to cyber security, age less than 34 years and spending time with electronic devices >2.5 hours per day. Variables that lost statistical significance are designation of masters (MD) verses Non masters (MBBS) and gender difference (male versus female).

DISCUSSION

In this study males out number females by participation, males contributed 55% (n=22) and females (n=18) were 45% only.

The study variable of residence of study subjects, both urban and rural did not show any difference to the outcome variable knowledge attitude and practice, cyber threats and cyber security knowledge.

Even the cadre or post wise divisions of study subjects also did not show any difference to the outcome variable knowledge attitude and practice, cyber threats and cyber security knowledge.

The variable denoting MBBS and post graduate perused in both same and allied state had also no Statistical significance both in univariate and multi variate analysis (p=0.05) with the outcome variable knowledge attitude and practice, cyber threats and cyber security knowledge.

Univariate analysis and significance ($p<0.05$) was seen in six study variables namely exposure to external resources related to cyber threats, books read of imbibed related to cyber threats, masters verses non master's qualification, age group <34 years, average spending time with electronic devices per day and gender difference favoring higher scores in male gender and outcome variable.

Multi variate analysis and r^2 (exponent of beta value) significance was seen in four study variables namely exposure to external resources related to cyber threats, books read of imbibed related to cyber threats, age group <34 years, average spending time with electronic devices per day.

In the questionnaire and scoring only 30% (n=12) had more than 8 and only 70% (n=28) had less than 8 for total of 25 marks. This stresses more on to improve the outcome variable knowledge attitude and practice, and awareness of cyber threats and cyber security knowledge for the medical fraternity of current times.

The global cyber threat ranking was based on eight metrics - malware, spam, phishing, bots, network attacks, web attacks, ransome ware and cryptominers.[2] india continues be second impacted by spam and bots, third by network attacks, fourth by ransomewares globally.[3]

A malicious software infiltration in United States health firm - the month of January 2015 was a historically bad month for healthcare data breaches. In the biggest healthcare breach to date disclosed that 78.8 million patient records had been stolen on January 29, 2015. An unknown hacker had accessed a database containing personal information, including names, birthdays, social security numbers, addresses, email addresses and employment and income information. The attack did not compromise credit card information or medical information, the company said.

In late June 2017 they had agreed to settle litigation over hacking in 2015 for $115 million, which lawyers said would be the largest settlement ever for a data breach. The breach is one of a series of high-profile data breaches that resulted in losses of hundreds of millions of dollars to U.S. Medical Fraternity in recent years.

Vital reasons for cyber threats in medical field

- The healthcare industry is one of the lowest performing industries in terms of endpoint security, posing a threat to patient data and potentially patient lives
- Social engineering attacks continue to put patient data at risk
- 60 percent of the most common cyber security issues in the healthcare industry relate to poor patching cadence
- Many healthcare organizations struggled with patching cadence and network security algorithms.

The motive seems clear from the above analysis. The thing with the healthcare industry is be it hospitals, doctors, clinics, nursing homes and assisted living facilities, outpatient clinics and other healthcare providers, they all have one thing in common the juicy details of patient information. These details include personally identifiable information such as social security numbers, names, and addresses to sensitive health data such as medicaid ID numbers, health insurance information, and patients' medical histories. These can then be used for identity theft.[4]

The largest breach penalty was against another medical university in United Kingdom was fined Â£325,000 for a breach involving hard drives containing healthcare information on tens of thousands of individuals that were sold on the Internet. That fine has since been appealed by the trust on the grounds that they had arranged for an experienced IT service provider to dispose of the hard drives and that it acted swiftly to recover and prevented the hard drives to be for sale online.

Another community healthcare in U.K was fined Â£90,000 in May for a breach involving patient lists and drug medications repeatedly faxed to the wrong recipient.[5] Another private software security firm continues to witness a concerted focus on acquiring healthcare research by multiple Chinese advanced persistent threat (APT) groups. In particular, it is likely that an area of unique interest is cancer-related research, reflective of China's growing concern over increasing cancer and mortality rates, and the accompanying national health care costs the cyber security agency noted.[6]

On March 7 by a security researcher of a cyber-security consulting firm, wrote in a blog post that authorities in India took three weeks - until March 29 - to remove the sensitive information from the database. It's worth noting that the database is still available online without a password, which is why the state name has been withheld. The database had patients' records, doctors' details, children's details, admin passwords and logins, all of which were collected as part of the Indian pre-conception and pre-natal diagnostic techniques (PCPNDT) Act, which was introduced in 1994 to prevent sex selection and female infanticide.[7]

In April 2018, it was found that a South Indian Government Health Care Website were leaking Aadhaar numbers of women, their reproductive history from pregnancy to delivery, whether they had had an abortion, and so on. It also tracked the infants' early years and vaccinations. In June 2018, a public Health care website tracked state-run ambulances in real time, allowing anyone with an internet connection to monitor the movement of these vehicles and obtain sensitive information about the patient - such as the pick-up point, why the ambulance was called, and the hospital to which the patient was taken.

The same month, another public health care website exposed the names and numbers of every person who purchased medicines, including those who bought Suhagra (a medicine for erectile dysfunction) from government-run stores. A dashboard on the main health care website allowed anyone with an Internet connection to access details including the names and phone numbers of every person who bought medicines from every single such store.[8]

Public configuration allows the possibility of cyber-criminals to manage the whole system with full administrative privileges. Once the malware is in place, criminals could remotely access the server resources and even launch a code execution to steal or completely destroy any saved data the server contains.[9]

The above epidemiology and real life scenarios quoting cyber security and cyber threats of medical data being compromised globally in all Continents and countries - United States, United Kingdom, China, Brazil, North India, South India, only shows that this is a universal problem and looming threat, where personal virtual etiquette like constantly updating our using electrical devices and their software's, internet security systems, patching our operating systems, changing our login ID s and passwords in regular pattern, will defend and protect our precious patients medical data and a healthy convalescence can be predicted by the treating physician in all setups.[10]

Post data collection and beneficence to study subjects

After getting the Filled data sheets from the study participants, all of there working electronic gadgets have been installed with BOT remover and malware patrolling softwares, APPSAMVID - desktop based application and white listing solution Windows OS, M KAVACH - For mobile devices security solutions for android OS, browser JS guard - Defends and protects from malicious HTML and JavaScript Attacks based on Heuristics, All these software's were designed and sourced from CERT IN - computer emergency response team India - An Indian Government initiative to safeguard electronic digital devices against cyber security and threats.

Limitations of this study were the total Sample size was 45 and non-respondent rate was 11.1% (n=5), 2 of the study subjects did not returned the data sheet and 3 of the data sheets was not properly filled. Study variables like books imbibed and external resources on cyber threats and basic operating system components were not accurately recorded as the study subjects had a lot of recall bias. After collecting the data sheets from the study subjects, and giving them their answer keys - subjects were too much concerned about their performance results. Data collected on favorite or more time spending pattern among websites, Software's, Applications was collected, but since they are all private parties, that data was not considered into analysis or discussion. Side effects of continuous using electronic devices like dry eye syndrome, net addiction, stiff neck syndrome, thumb stiffness, mental changes, psychological effects etc. we're not focused since they all are separate specialties with their own diagnosis and require diverse Specialty approach to fix and requires multiple follow ups.

CONCLUSION

In this study the following variables 1. Exposure to external resources related to cyber security and threats, 2. books read or imbibed related to cyber security and threats 3. age less than 35 years and 4. spending time with electronic devices > 2.5 hours per day. Had a positive outcome and more scores with the independent variable of cyber threat knowledge and awareness. Variables that lost statistical significance are designation of masters (MD) verses non masters (MBBS) and gender difference (male versus female), residence pattern (Urban versus Rural), under graduate (MBBS) and post graduate (MD) persuasion parameters.

Simply to conclude, the current medical fraternity should know more and update current trends in Electronic digital devices both hardware and software's domains both for their academic and professional growth and of utmost is the privacy of medical data of our precious patients or subjects with disease or any other form of illness that needs care and holistic recovery.

ACKNOWLEDGEMENTS

Authors would like to thanks Dean, Vice Principal and the HOD s and faculties of anatomy, physiology, bio chemistry, pathology, microbiology, pharmacology, forensic medicine for their support and contribution to this study.

Funding: No funding sources
Conflict of interest: None declared
Ethical approval: The study was approved by the Institutional Ethics Committee

REFERENCES

1. The Hindu e-Paper, Chennai Edition Dated 18.04.18 Page 12 - Symantec Internet Threat Report - 2017 Global data. Archives /18.4.19/Chennai edition/Symantec ITR 2017. Available at: www.hinduepaper.in /. Accessed on 5 May 2019.
2. National Crime Records Bureau - 2017, Sumanth sen on Vulnerability of Indian Cyber security and threats. Sumanth Sen on Vulnerability of Indian Cyber security and threats. Available at: www.ncrb.in/. Accessed on 25 September 2018.
3. Computer emergency response team / Indian ranking in cyberthreats and cybersecurity 2016 data. Indian ranking in cyberthreats and cybersecurity 2016 data. Available at: www.cert.in. Accessed on 15 October 2018.
4. Top Health care Breaches of United states Fact sheet 2015. Available at: https://www.appknox.com/blog/top-healthcare-data-breaches. Accessed on 19 October 2018.
5. Medical Data Breaches of NHS United Kingdom – 2012. Available at: https://www.databreachtoday.co.uk/uk-health-records-breached-18-million-a-5261 - UK Nov 6/ 2012. Accessed on 25 October 2018.
6. Medical Indo Asian News Service - India Today Article. Available at: https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22. Accessed on 22 August 2019.
7. Medical Data Breaches of Indian Health Data s and information - 2019. Available at: https://www.medianama.com/2019/04/223-health-department-indian-state-pregnant-women-data-leak/. Accessed on 3 April 2019.
8. Indian Medical Data Leak, special report Bulletin news18 India. Available at: https://www.news18.com/news/tech/indias-leaked-medical-data-could-have-been-sold-or-damaged-bob-diachenko-2089351.html. Accessed on 6 June 2019.
9. Sharp WG. The use of armed force against terrorism: American hegemony or impotence. Chi J Int'l L. 2000;1:37.
10. Libicki MC. Cyberdeterrence and cyberwar. Rand Corporation. 2010;26(14):144-52.

Cite this article as: Balaji J, Ganesh G. Knowledge, attitude and practice study on awareness and preventing cyber threats among the electronic devices used by the doctors of government medical college Vellore, Tamil Nadu, India. Int J Community Med Public Health 2020;7:283-8.