

Original Research Article

Are we cyber aware? A cross sectional study on the prevailing cyber practices among adults from Thiruvalla, Kerala

Shaliet Rose Sebastian*, Bichu P. Babu

Department of Community Medicine, Believers Church Medical College Hospital, Kuttapuzha, Tiruvalla, Kerala, India

Received: 23 October 2022

Revised: 05 December 2022

Accepted: 07 December 2022

*Correspondence:

Dr. Shaliet Rose Sebastian,

E-mail: drshaliets@gmail.com

Copyright: © the author(s), publisher and licensee Medip Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT

Background: Cyber-crime is described as any unlawful activity which is committed using any computing devices, like computer/smartphone and which is a part of internet. There are different methods by which cyber-crime is committed which include 1) attacks on computer systems, 2) cyber-bullying, 3) email spam, 4) phishing, 5) identity theft. Breaches in cyber security have become a severe danger to world security and the economy, compromising essential infrastructure and wreaking havoc on company performance, resulting in significant cognitive property loss. It is a sad reality that cybercrime cases have witnessed a steady spike. India has witnessed a significant increase in cases of cyber fraud and various cyber-related incidents in the last three years. The present study was done to assess the prevailing cyber practices among adults from Thiruvalla, Kerala.

Methods: The present cross-sectional study was conducted among 340 adults in Thiruvalla, Kerala from January to June, and 2022. A semi-structured questionnaire was used to elicit information from the study participants after obtaining consent. The quantitative data collected was analysed using the software statistical package for social sciences. The results have been presented as tables and charts showing frequencies and percentages.

Results: 133 out of the 350 study participants (38%) believed that it was important to be aware of cyber security risks in general while 52% (182) of the study participants considered cyber security awareness to be the only solution to the existing online scams.

Conclusions: Widespread awareness campaigns are necessary to improve the cyber awareness of the community and thereby improve their cyber practices.

Keywords: Adults, Cyber practices, Cyber security, Kerala

INTRODUCTION

We are living in the digital age wherein Internet has become an unavoidable part of daily life be it connecting with friends and family, or other transactions like online bank transactions, educational classes, healthcare consultations etc. After the covid era the frequency of online transactions has risen considerably compared to the pre covid era. Ensuring the security of online transactions therefore has become the need of the hour.

Cyber-crime is described in a simpler term as any unlawful activity which is committed using any computing devices, like computer/smartphone and which is a part of internet. There are different methods by which cyber-crime is committed and which include 1) attacks on computer systems, 2) cyber-bullying, 3) email spam, 4) phishing, 5) identity theft. Previous literature has revealed that cyber security, including cyber risk assessment and reporting has become a managerial accounting and auditing matter, subject to cost-benefit analysis, internal

control assessment, and disclosure policy considerations.^{1,2} According to the latest NCRB (National Crime Record Bureau) publication of 2017, there is an increasing incidence of cybercrime in India from 9622 cases in 2014 to 12,317 in 2016 (28%). Maximum number of cases were reported in Uttar Pradesh (2,639 cases) followed by Maharashtra (2380 cases) and Karnataka (1,101 cases).³ Even with knowledge of existence of firewalls, antivirus and many other effective measures to control cyber-crime, India is still far behind in combating cybercrimes.⁴ Breaches in cyber security have become a severe danger to world security and the economy, compromising essential infrastructure and wreaking havoc on company performance, resulting in significant cognitive property loss.⁵ With the advent of 5G and metaverse, previous literature reveals that mitigation of concerns including cybersecurity and privacy positively affects the technology adoption of metaverse.⁶

As we observe yet another world cyber security awareness month in October, it is a sad reality that cybercrime cases have witnessed a steady spike. India has witnessed a significant increase in cases of cyber fraud and various cyber-related incidents in the last three years. India reported 2,08,456 incidents in 2018; 3,94,499 incidents in 2019; 11,58,208 cases in 2020; 14,02,809 cases in 2021; and 2,12,485 incidents in the first two months of 2022 according to data by CERT-In (Indian Computer Emergency Response Team).

There is a paucity of published literature on the prevailing cyber practices in the community. Understanding the practices would help in assessing the current level of awareness and preparedness regarding cybersecurity. Understanding the prevailing practices would enable identification of the gap in knowledge and address the gaps to increase the awareness in the community on cyber security.

Objective of the study

To assess the prevailing cyber practices among adults from Thiruvalla, Kerala.

METHODS

The present cross-sectional study was conducted among 340 adults in Thiruvalla, Kerala from January to June, and 2022. The sample size was calculated using cyber security awareness from a similar study.⁷ Multi stage sampling was used to collect the study data. Out of the 5 taluks in Pathanamthitta district, Thiruvalla was randomly selected using Lottery method. Tiruvalla municipality was randomly selected for the study.

A house-to-house visit was made in the selected area, and after establishing a rapport with the family, the nature, purpose and objectives of the study were explained. A semi-structured questionnaire was used to elicit information from the study participants after obtaining consent. The first house was selected randomly and consecutive houses was surveyed till 340 study participants were surveyed.

The quantitative data collected was analysed using the software statistical package for social sciences version 20. The results have been presented as tables and charts showing frequencies and percentages.

RESULTS

General characteristics of the study population

The 340 study participants were aged between 18 and 68 years (mean- 37.6, SD=14.4). The majority of study participants were males (52%). The general characteristics are shown in Table 1.

Table 1: General characteristics of the study population.

Variables	Frequency (%)
Gender distribution	
Males	182 (52)
Females	168 (48)
Education of the participant	
Below 10 th standard	85 (24.3)
Between 10 th standard and 12 th standard	85 (24.3)
Graduate	90 (25.7)
Post graduate	90 (25.7)
Occupation of participant	
Unemployed	48 (13.8)
Semiskilled	35 (10)
Skilled	70 (20)
Semi professional	84 (24)
Professional	85 (24.2)
Retired	28 (8)
Place of residence	
Rural	210 (60)
Urban	140 (40)

133 out of the 350 study participants (38%) believed that it was important to be aware of cyber security risks in general while 52% (182) of the study participants considered cyber security awareness to be the only solution to the existing online scams. The cyber practices of the participants are given in Table 2.

Table 2: Cyber practices of the study population.

Question	Frequency (%)
Do you have a social media account?	
Yes	322 (92)
No	28 (8)
Who has access to your profile details?	
Visible to everyone	119 (34)
Visible to my friends only	161 (46)
Visible to me only	35 (10)
I don't know	35 (10)
Do you accept friend request from persons who you do not know personally?	
Yes	77 (22)
No	273 (78)
Do you update your career progress, current location, family photographs etc. on social media?	
Yes	175 (50)
No	175 (50)
How do you update your device?	
Automatic update	119 (34)
Manual update	133 (38)
No update	56 (16)
I neglect update	42 (12)
Do you use antivirus software on your device?	
Yes	161 (46)
No	189 (54)
Do you update the anti-virus software at regular intervals?	
Yes	133 (38)
No	217 (62)
Have you ever received phishing emails/messages?	
Yes	259 (74)
No	91 (26)
How many phishing emails/messages containing unknown links do you receive on an average?	
Less than 5 per year	154 (44)
Between 5 and 10 per year	98 (28)
More than 10 per year	98 (28)
Have you ever clicked on unknown links in email/messages?	
Yes	126 (36)
No	224 (64)
Do you change your password periodically?	
Yes	112 (32)
No	238 (68)
Do you use previously used passwords?	
Yes	210 (60)
No	140 (40)
Do you use alphanumeric characters, special characters and more than eight characters in your password?	
Yes	217 (62)
No	133 (38)
Do you share your passwords with others?	
Yes	77 (22)
No	273 (78)
Do you pay attention to web browser's privacy controls and parameters regularly?	
Yes	70 (20)
No	280 (80)

DISCUSSION

The present study was done to assess the prevailing cyber practices among adults. The study found that although 92% of study participants had social media accounts, less than half of them only used an anti-virus software on their device. In a study conducted in Tamil Nadu on cyber security awareness among college students, more than 70% of students were conscious about the basic virus attacks and were using antivirus software (updating frequently).⁷ This disparity could be due to the difference in age groups of the study population involved in both studies. Our study found that a good percentage of the study population (78%) were careful about sharing their social media passwords with others and accepting friend requests from strangers. However, almost half of the study participants regularly updated their carrier progress, current location and family photographs on social media. A similar study conducted in Gujarat among youth revealed that 48% of respondents share their personal details with other persons even they don't know them closely, whereas, 42% of respondents think that sharing photographs on social networking sites is not a risky activity.⁸

The present revealed that a good majority of the study population did not change their passwords regularly (68%). 60% of the study participants were in the habit of reusing previously used passwords. A similar study conducted among medical students revealed that most of students (56%) rarely changed their password; some of them (12%) never even changed it.⁹ Contrary to this in study done on MSW students showed that 33% never changed the password this may be due lack of awareness among them. Some of the students were even sharing the password (8%) with others, some with family members (26%), which increases their risk of identity theft and loss of personal data.¹⁰ The present study revealed that 74% of the study participants had received phishing messages at least once. A similar study revealed that 66% of respondents have become the victim of cyber threat such as cyber bully and scam but only 8 respondents have actually contacted the responsible agency for cyber threat.¹¹ Another study observed that over 60% of the respondents experienced an increase in fraudulent emails, Phishing attempts, and spam to corporate email, since start of COVID-19 pandemic.¹² The present study found that although majority of study participants used internet and were active on social media, 80% of them did not pay any attention to web browser's privacy controls and parameters regularly. This points towards the lack of awareness in the society regarding the issue of cybercrime. Risk and controls including adequate policy documentation and display of privacy policies is mandated by law. A research found that using video visualizations greatly improves the readability of Privacy Policies.¹³

There were some limitations. The responses of the study participants were self-reported and hence could have been

influenced by social desirability bias and recall bias. Direct observation of the practices by the study participants was not done in the study.

CONCLUSION

The present study has discovered a gap in the cyber security awareness of the community by assessing their cyber practices. Widespread awareness campaigns are necessary to improve the cyber awareness of the community and thereby improve their cyber practices.

Funding: No funding sources

Conflict of interest: None declared

Ethical approval: The study was approved by the Institutional Ethics Committee

REFERENCES

- Gordon LA, Loeb MP. Managing cyber security resources: a cost-benefit analysis. Vol 1. Mc-Graw-Hill, New York; 2006.
- Sebastian G. Could incorporating cybersecurity reporting into SOX have prevented most data breaches at US publicly traded companies? An exploratory study. *Int Cybersecur Law Rev*. 2022;3(2):367-83.
- Crime in India 2016 Statistics National Crime Records Bureau (Ministry of Home Affairs) Government of India. Available from: <https://ncrb.gov.in/sites/default/files/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf>. Accessed on 20 August 2022.
- Mehta S, Singh V. A study of awareness about cyber laws in the Indian society. *Int J Comput Business Res*. 2013;4(1):1-8.
- Garg A, Curtis J, Halper H. Quantifying the financial impact of IT security breaches. *Inf Manag Comput Secur*. 2003;11:74.
- Sebastian G. A study on metaverse awareness, cyber risks, and steps for increased adoption. *Int J Secur Priv Pervas Comput*. 2022;14(1):1-11.
- Senthilkumar K, Easwaramoorthy S. A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conf Ser Mater Sci Eng*. 2017;263:042043.
- Shah J. A study of awareness about cyber laws for Indian youth. *Int J Trend Scient Res Develop*. 2016;1(1).
- Rathod P, Potdar AB. (2019). Study of awareness of cyber-security among medical students. *Indian J Forens Med Toxicol*. 2019;13(1):196.
- Afrozulla KZ, Vaishnavi RT, Arjun. Cyber crime awareness among msw students, school of social work, Mangaluru. *J Forens Sci Crimin Invest*. 2018;9(2):555757.
- Hamzah S. Level of Awareness of social media users on cyber security: case study among students of university Tun Hussein Onn Malaysia. *Turkish J Comput Math Educ*. 2021;12(2):694-8.

12. Sebastian G. A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. *Communicat IBIMA*. 2021;2:2-7.
13. SEBASTIAN G. A Cross-sectional Study on Improving Privacy Policy Read Rate and Comprehension via Better UX/UI Design. *Communicat IBIMA*. 2021: 2021.

Cite this article as: Sebastian SR, Babu BP. Are we cyber aware? A cross sectional study on the prevailing cyber practices among adults from Thiruvalla, Kerala. *Int J Community Med Public Health* 2023;10:235-9.