International Journal on Emerging Technologies **14**(2): 13-19(2023)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Study on Awareness about Cyber Security Among the Female University Students

Krutika Bhate*
Assistant Professor, Department of Extension and Communication,
Faculty of Family and Community Sciences,
The Maharaja Sayajirao University of Baroda, Vadodara (Gujarat), India.

(Corresponding author: Krutika Bhate)*
(Received 28 June 2023, Revised 29 July 2023, Accepted 31 September 2023)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: All are vulnerable to cyber-attacks on essential infrastructure. Individually, cyber security concerns can put one's wealth, identity, and privacy in danger. To address the cyber security awareness among female students in higher education institutions, there is a need for some cyber security-related awareness program. This survey analyzed Cyber Security awareness among female university students of The Maharaja Sayajirao University of Baroda and enlightens students about the dangers and challenges that are prevalent in cyberspace. It was an experimental research where 167 female students were selected purposively. Data were collected through online survey which need lot of follow up as students were not filling the survey from. The findings of the study revealed that female students were less aware about the various terms related to cybercrime such as phishing, cyber bulling, cyber stalking and so on. The students were aware about password security and social media security whereas they have less awareness about browser security. The awareness session found effective in generating awareness about cyber crime and cyber security among the female university students. Less number of students attended the session; they should understand the importance of cyber security. The study concludes that there is a great need of generating awareness about cyber security among the students. The findings of the study recommend that universities should include curriculum on cyber security for the students.

Keywords: Cyber crime, Cyber Security, Students, Awareness.

INTRODUCTION

Various communication techniques have been developed worldwide. Consequently, public and private sectors have begun to offer more services and adopt new technologies to provide access to information anytime and anywhere upon request from customers. The key reason behind automating services and adopting new technologies is to support and satisfy a wide range of customers, whose number has been increasing rapidly owing to the increase in the usage of the Internet. In response, the number of hackers and organized cybercrime groups has grown exponentially. These cybercriminals have been adopting new methods to carry out cybercrime. The primary motivation for hacking is the financial gain obtained by stealing sensitive information and holding it for ransom. Hackers can also earn money by selling secret data to competitors on the dark web, which makes cyberspace unsafe and poses considerable risks to organizations and their customers (Alharbi and Tassaddiq 2021).

India witnessed 13.91 Lakh cyber security incidents in 2022, Minister of State for Electronics and Information and Technology Rajeev Chandrasekhar informed the Parliament on February 10, 2023. The numbers still do not give an entire picture of cyberattacks on the country as these statistics only include information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In). The number of reported cyberattacks, however, fell in 2022, down from 14.02 Lakhs in 2021. As per government figures, 2.08 Lakh incidents were reported in 2018,

and 11.58 Lakh cybersecurity incidents were reported to CERT-In in 2020 (Thathoo, 2023).

The most common cybercrimes committed against women are cyber blackmail, threats, cyberpornography, posting and publishing of obscene sexual content, stalking, bullying, defamation, morphing, and the establishment of fake profiles. As of 2019, the total cybercrime incidents have gone up by 18.4% but the number of cybercrime cases against women has gone up by 28%, as shown by National Crime Record Bureau. Data showed that 10,730 incidents, or 20.2% of the 52,974 incidents registered in 2021, were reported as crimes against women (Team, 2022).

Protecting the integrity and confidentiality of information in sophisticated network systems is becoming increasingly critical and difficult. And students make up the majority of those who are linked to these networks. Students may engage in cybercrime for a variety of motives, including curiosity and vengeance. The majority of the time, students isunaware of the dangers of cybercrime. The most common victims of cybercrime are women and girls (Senthilkumar & Easwaramoorthy 2017).

The Internet is now used in every area of people's lives. People use the internet to communicate with friends and family, to start businesses and banks, and to use a variety of other services such as virtual healthcare and education, video calls, and so on. As a result, technological linkages have improved. Constant connectivity, on the other hand, increases the hazards. All are vulnerable to cyber-attacks on essential infrastructure. Individually, cyber security concerns can put one's wealth, identity, and privacy in danger. To address the cyber security awareness among female students in higher education institutions, there is a need for some cybersecurity-related awareness program. This survey analyzed Cyber Security awareness among female university students of The Maharaja Sayajirao University of Baroda and enlightens students about the dangers and challenges that are prevalent in cyberspace.

Objectives of the Study

1. To prepare the profile of the female students of the Maharaja Sayajirao University of Baroda.
2. To explore the cyber security awareness level among female students of the Maharaja Sayajirao University of Baroda with respect to general security, password security, browser security, and social media security.
3. To study the differences in the awareness level of the selected aspect of cyber security among female students of the Maharaja Sayajirao University of Baroda in relation to their age, level of study, discipline of study and number of devices use.
4. To enhance cyber security awareness among the selected female students and enlighten them about the hazards and challenges prevailing in cyberspace.
5. To analyze the cyber security awareness level among female students of the Maharaja Sayajirao University of Baroda after the awareness programme.

METHODOLOGY

The present study was conducted in phases

Phase 1: In phase one a survey was conducted through a questionnaire to check cyber security awareness among female students. The population of the study comprised female students of The Maharaja Sayajirao University of Baroda, Vadodara. One hundred and sixty-seven female students were comprised as a sample of the study. The non-probability sampling technique was used to select the sample from the population.

Phase 2: Based on the survey results, an awareness session was organized to strengthen the cyber security knowledge and promote security awareness among the selected female students of The Maharaja Sayajirao University of Baroda. More than 80 students participated in the awareness session. The students from undergraduate and postgraduate programmes participated in the awareness session. Various audio-visual materials were developed and used to generate awareness among the students. The expert from the CyberPeace Foundation conducted an online session on the theme “Data Privacy and Social Media Security” with the students. Based on the findings of the study the topics were covered in the session.

Phase 3: In the third phase post analysis was carried out for the selected students those undergone the awareness session to check their cyber security awareness after attending the session.

Inclusion and Exclusion criteria: The participants had to be 18 years old and above. Participants under the age of 18 were excluded because the focus of this study will be on the cyber security awareness level among adult female students.

Instrument for Research. The research tool is the cornerstone of any kind of study. The construction of good research tools influences the quality of the data and consequently the quality of the research. A questionnaire, and rating scales, was structured to collect quantitative data.

Procedure for Data Collection. The questionnaire was uploaded on "Google Forms" and a web link was created to fill it out. The data was collected through Google Forms by the investigator in December 2022. Before sharing the questionnaire among the respondents, the investigator contacted them and took their consent for the data collection. Those who were ready to give their consent were only selected for the present study. The web link was exchanged via WhatsApp with them. One hundred and sixty-seven questionnaires were selected as data-generating questionnaires.

FINDINGS AND DISCUSSION

A. Profile of the Students

The findings of the study revealed that half of the respondents (50.89%) were from the 17-19 age groups. The data also revealed that 42% of the students were about to get their bachelor's degree as they were from the age group of 20 to 22. The survey results indicated that the majority (62.87%) of the students were from the Social Science discipline whereas more than one-third (37.12%) of the students were from the Humanity discipline. A high majority (81.4%) of the students were undergraduates whereas very few (18.56%) of the students were from Post Graduate. Near to half (49.10%) of the students have access to one device whereas almost equal percentage of the students have access to 2 (32.93%) or 3 (13.17%) devices. It indicates that near to half of the respondents were using more than 1 device hence it becomes very important for them to understand how they can be safe while using these devices.

Table 1: Frequency and Percentage Distribution of the Students according to the Use of devices (n=167).

Use of devices	F	%
Smartphone	166	99.4
Laptop	78	46.7
Tablet	26	15.6
Personal PC	18	10.8
I Pad	1	0.6

**Multiple Choices*

The smartphone has impacted every sphere of human life. Smartphones are popular among youth for the applications they offer to users. Hence, this could be the probable reason for the high use of a smartphone (99.4%) among students. The data also highlight that near to half of the students (46.7%) use laptops whereas very few of them use a tablet (15.6%) and personal PC (10.8%). Laptops are portable and advanced versions of personal PC which provide ease of work and students can work anywhere on the campus on it.

B. Use of Technology

Students nowadays spend a considerable amount of time on their cell phones, computers, and specifically the internet. It has made a significant contribution to the education of students by improving their ability to study and gain knowledge, right from their homes. They use the internet for a variety of purposes, including online lectures, research, the latest information, and more. The finding indicates that almost half of the students (46.1%) spend at least 2 hours on Internet every day. More than one-third (37.7%) of students spend more than 4 hours on the Internet every day. The students use technology most of the time for online chatting (73.05%), listening to music/watching videos (68.86%), and recharging their internet package (67.6%). The data also reflects that the students use technology most of the time to browse the internet to search for information (59.86%), make video calls (55.08%), access social media websites or applications (53.89%), and download applications from play store (50%).

C. Awareness about Cyber Security

This section presents the data related to the awareness about cyber security among the female students of the university. It also highlights the differences in the awareness level in relation to selected variables of the study. The data reflects that 43% of the students reported that they are not well aware of cybercrime whereas little less than half (49.10%) of the students reported that they are very well aware of cybercrime. It reflects that a higher percentage of the students were not aware of or don't know about cybercrime.

Table 2: Percentage Distribution and Item Wise Intensity Indices for the Extent of awareness about the following terms Among the Students (n=167).

Statements	GE	SE	LE	Don't Know	I.I
	%				
Software updates	53.29	21.55	17.36	7.78	3.20
2 step verification	52.69	20.35	14.37	12.57	3.13
Password security management	42.51	32.33	16.76	8.38	3.09
Antivirus	41.91	28.74	19.16	10.17	3.02
Cyberbullying	36.52	31.13	18.56	13.77	2.90
Cyber stalking	31.73	25.14	26.94	16.16	2.72
Secure setting practice	29.34	22.15	22.75	25.74	2.55
Anti-spam	25.14	23.95	25.74	25.14	2.49

Anti-spyware	25.19	23.95	23.35	27.54	2.47
Identity theft	18.56	31.13	26.94	23.35	2.45
Firewall	20.95	25.74	21.55	31.73	2.36
Social engineering	10.17	25.14	30.53	34.13	2.11
Phishing	12.57	21.55	20.35	45.50	2.01

**GE: Great Extent, SE: Some Extent, LE: Less Extent*

The above table presents that a higher percentage of students don't know about phishing (45.50%), social engineering (34.13%), firewall (31.73%), and identity theft (23.35%). They know about anti-spyware (23.95%), anti-spam (23.95%), cyberbullying (31.13%), cyberstalking (25.14%), and security settings (22.15%) to some extent. A higher percentage of the students know about antivirus (41.91%), password security management (42.51%), 2-step verification (52.69%), and software update (53.29%) to a high extent. This indicates that awareness regarding topics that they know to some extent, less extent, and don't know must be created.

The findings reported by Alharbi and Tassaddiq (2021) in their study highlight that 41% of the students could not recognize a situation where their computers were infected with malware or controlled by hackers. A contradictory finding was reported in their study that only 22% of the students were unaware of two-factor authentication and did not know how it added an extra layer of security. They had not enabled this mechanism on their accounts when it became available.

Senthilkumar and Easwaramoorthy (2017) pointed out that the majority of the participants lack the basic knowledge of Two-Factor authentication as is widely applicable to many applications now, and this poses the need for awareness programmes. He also highlighted that respondents are not aware of the concept of phishing emails.

Table 3: Frequency and Percentage Distribution of the students According to their Overall Awareness about Cyber Security (n=167).

Extent of Awareness	F	%
High awareness	89	53.3
Moderate awareness	61	36.5
Less awareness	17	10.2
Total	167	100

The above table represents that more than half (53.3%) of the students had high awareness of cyber security which is a good indication. Near to forty percent (36.5%) and 10% of the students had moderate and less awareness about cyber security respectively. It indicates that near to half of the students had moderate or less awareness. Hence, it is evident that there is a need to generate awareness among the students.

A similar finding was reported by Moallem (2019) that 60% of respondents agreed that they are knowledgeable of cyber security. However, the 40% who do not know about cyber security is significant especially since most are younger college students assumed to have general knowledge of computers. Senthilkumar and Easwaramoorthy (2017) also found a similar finding that the cyber security awareness among college students in Tamil Nadu is measured as 69.45% with which males 38.6% and females 30.85%. Fully fledged cyber awareness will make students protect themselves from hackers and hence the awareness has to be created at a higher level (Moallem, 2019).

Table 4: Frequency and Percentage Distribution of the Students According to their Awareness of Different Aspects of the Cyber Security (n=167).

Aspects	f / %	GE	SE	LE	Don't know
General Safety	Frequency	65	73	13	16
	Percent	38.9	43.7	7.8	9.6
Password Safety	Frequency	104	52	4	7
	Percent	62.3	31.1	2.4	4.2
Browser Security	Frequency	82	62	15	8
	Percent	49.1	37.1	9.0	4.8
Social Media Security	Frequency	118	41	3	5
	Percent	70.7	24.6	1.8	3.0

GE: Great Extent, SE: Some Extent, LE: Less Extent

The above table shows that the majority of the students (70.7%) were aware of social media security, and password security (62.3%) whereas little less than half (49.1%) of them were aware of browser security to a great extent. The use of social media is found high among young students and hence they may have a high awareness of it. The awareness related to password security and social

media security is generally carried out by different print and electronic media hence they may have high awareness about it. On the other hand awareness about general security and browser, security is less covered by media hence a higher percentage of the

Students had moderate awareness about general security (43.7%) and browser security (37.1%). This finding highlights the need of generating awareness about general security and browser security.

Table 5: Analysis of Variance (ANOVA) Indicating Difference between Selected Security Aspects and Use of Number of Devices (n=167).

Security Aspects	Number of Devices	N	Mean	Std. Deviation	Sum of Square	F	Sig. (2-tailed)
General Security	1	82	41.72	12.67	**3, 164**	3.71	0.01*
	2	55	40.84	13.52			
	3	22	48.23	8.65			
	4	8	52.38	6.37			
Password Security	1	82	34.63	8.19	**3, 164**	3.2	0.02*
	2	55	34.07	9.11			
	3	22	39.36	4.77			
	4	8	39.63	5.48			
Browser Security	1	82	20.35	5.77	**3, 164**	3.18	0.02*
	2	55	20.45	5.98			
	3	22	23.05	4.88			
	4	8	25.50	3.12			
Social Media Security	1	82	16.39	4.09	**3, 164**	1.58	0.19
	2	55	16.95	3.79			
	3	22	18.00	2.69			
	4	8	18.50	2.98			
	Total	167	16.89	3.81			

The mean difference is significant at the 0.05 level.

The findings of the study indicate that there was a significant difference in the awareness regarding general security, password security, browser security, and the use of several devices. It highlights that as the use of several devices differs the awareness about selected security aspects also differs. Those who use more devices may have more awareness about selected security aspects. The finding also indicates that there was no significant difference in the awareness about social media security with the use of a number of the device. The probable reason for this could be that they may access social media through their smartphone only hence it is not affecting their awareness level regarding social media security.

The post hoc analysis indicates that the variation occurs in the awareness about password security between the uses of one to four devices. The probable reason for this finding could be that majority of them use more than 2 devices and hence they may feel to keep their devices safe by setting a strong password for them.

There were no significant differences in the awareness level between security parameters, age and, level of study. It reveals that the age group of the students does not affect their awareness about general security, password security, browser security, and social media security. It shows that undergraduate and postgraduate students do not differ in their awareness level about different selected cybersecurity aspects. Hence, the null hypothesis stating that there will be no significant differences in the awareness level concerning their age and level of study is accepted. The findings of the study also highlights that there were no significant differences in the awareness about selected security aspects concerning the discipline of the study. It indicates that their level of awareness about different security aspects does not vary as the variation occurs in their stream of study. Hence, the null hypothesis stating that there will be no significant differences in the awareness level concerning their level of study is accepted (Garba *et al*., 2020).

The findings of the study indicates that a higher percentage of the students were aware of the following statements to a great extent whereas half of them were aware of the same statement to some extent and less extent.

— The importance of shutting down or logging off the device after completing the work.

— Removal of personal or confidential data before giving the device to be repaired or replaced.

— The dangers of installing free software from unreliable and unknown sources.

— The importance of two-factor authentification.

— Rejecting a mobile app request for accessing contacts, cameras, or location.

On the other hand, the following are the statements that need more attention in terms of awareness generation among the students as a higher percentage of them were less aware of it.

— Activating e-mail spam filter
— The encryption when sending email
— Paying attention to the security settings of the web-based software if one uses web-based email or calendar
— Applying security patches to phone if it works slow
— The latest online scam and able to identify it

It is a good indication that a higher percentage of the students were aware about password security to a great extent. One should take note that a higher percentage of the students were aware to some extent (25%) or less extent (13%) that one should not use one strong password across different websites and accounts. It highlights that students were not using a different strong password for their various accounts or maybe using one password for all the accounts. Awareness regarding this aspect should be generated among the students.

It is a very good indication that the majority of the students were aware of the statement related to social media security to a great extent. A similar finding was reported by Alharbi and Tassaddiq (2021) that most of the students shared personal pictures on public social media accounts with no hesitation. This can inadvertently leak sensitive and confidential information, such as personally identifiable information (PII). Notably, 56% of the students kept their location private and never shared it publicly on social media. It is complicated to report harmful and abusive violations on social media; however, in this survey, more than 70% of the respondents knew how to report any threat they faced (Alharbi and Tassaddiq 2021).

D. Post Analysis

Phase two of the study focuses on generating awareness about different aspects of cyber crime and cyber security among the selected students of the university. This section deal with the findings related to the awareness of cyber security among female students after attending the awareness session.

Table 6: Frequency and Percentage Distribution of the Students according to their Awareness of Cyber Crime after Attending the Session (n=85).

Awareness	F	%
Very well	59	69.41
Not so well	17	20.00
Don't know	9	10.58
Total	85	99.99

The data presented in the above table highlights that awareness sessions helped in generated awareness about cybercrime among the selected students of the university as it shows that the majority of them (69.41%) reported that they are very well aware of cybercrime after attending the awareness session.

Table 1: Percentage Distribution and Item Wise Intensity Indices for the Extent of awareness about the following terms Among the Students after Attending the Session (n=85).

Statement	GE	SE	LE	I.I
2 step verification	55	17	13	2.49
Cyber stalking	50	25	10	2.47
Antivirus	53	18	14	2.45
Password security management	47	26	12	2.41
Cyberbullying	44	29	12	2.37
Secure setting practice	43	30	12	2.36
Firewall	30	50	5	2.29
Identity theft	43	26	16	2.20
Software updates	28	43	14	2.16
Social engineering	27	41	17	2.11
Phishing	18	53	14	2.04

The above table shows that awareness sessions helped students in gaining a better understanding of 2-step verification, cyberstalking, antivirus, and password security management to a great extent. It also indicates that more awareness should be generated regarding social engineering and phishing in the future.

CONCLUSIONS

This study aimed to understand the use of technology among female students and generate awareness among the students for cybercrime and cyber security. It also suggests ways of technology used so that the risks and harms associated with it can be mitigated and opportunities and benefits are accentuated. The risk and harms to female students are cyber crimes like- cyber bullying, hacking, phishing, online job, and financial frauds, misuse of online profiles and pictures, morphing of images, etc. The benefits of the technology are helpful in their studies, and activities, make their communication better and establish networks. It is very important to understand the way technology is used, how much it is used, and for what it is used. This decides the balance between opportunities and benefits on the one side and risks and harms on the other.

The findings of this study revealed that female students own their smartphones and they use other technology such as laptops, desktops, and tablets in their daily work. They spend more than 2 hours on different devices per day. They use their mobile data most of the time to access the internet. The majority of them use technology for online chatting, listening to music, watching videos, recharging their

internet package, and browsing information on the internet.

Despite the heavy use of technology, more than half of the students were not aware of cybercrime which is a troublesome situation for them. This is also reflected in the awareness of various terms related to cybercrime and security. As many of them had less awareness or no awareness about phishing, social engineering, firewall, identity theft, etc. the statistical difference was found in awareness about general security, password security, and browser security concerning the use of several devices. The finding also highlighted that the awareness session helped students in gaining information and knowledge regarding cyber security. It is visible that there was a gain in knowledge regarding certain terms associated with cybercrime and security such as phishing, 2 –factor authentification, the importance of antivirus, cyberbullying, etc. after the session.

This indicates that the awareness session not only increased cyber security awareness on the specific topics it addressed but also helped students in general. It indicated that if students are provided with thorough knowledge of this area then they can improve their digital practices and can make sure that they remain safe digitally. As the youth use technology and specifically the internet from multiple devices, there will always be a need for generating awareness and building their capacity to be safe and secure digitally. Real knowledge and skills of using and practicing rules related to digital safety need to be built among female students with the help of teaching and learning. It can be covered in their curriculum. University and academic institutions need to hold comprehensive security awareness and training sessions regularly to recognize the most common cyber security threats and vulnerabilities.

The right to privacy is the fundamental right of every Indian citizen including youth and specifically females and the use of digital media by females should not be used against them or to hamper their future in any way. This concluded that cyber security is highly recommendable to the students in the university and encourages more females to participate in the awareness programme. To minimize the effect of any breach, cyber security awareness through education, workshop, seminars, and other methods within the university is highly encouraged. It should be noted that this research still has several limitations, such as the level of questions reliability,which is still not decent and the limited use of the independent variables. This research also did not always represent another more comprehensive cyber security topic. In future research, it is recommendable to add more variables that might affect cyber security awareness.

FUTURE SCOPE

The present study generated the data of awareness about cyber crime and cyber security among the female university students. The study indicates that awareness session helped students in understanding the concepts better hence, it is concluded that students should get opportunity and trained to use digital media more securely. Curriculum should include courses on cyber security for the students.

Acknowledgements. I would like to express gratitude to all those, who have contributed to this study. I sincerely acknowledge my research partner Cyber Peace Foundation, New Delhi. I am thankful to the team of Cyber Peace Foundation for believing in me and providing funds for conducting this research. I am also thankful to the foundation for having a wonderful and informative awareness session for the students of the university.

REFERENCES

Alharbi, T. and Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah university. *Big Data and Cognitive Computing*, *5(2)*, 23.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *International Journal on Emerging Technologies*, *11*(5), 41-49.

Moallem, A. (2019). Cyber security awareness among college students. In T. Z. Ahram& D. Nicholson (Eds.), *Advances in Human Factors in Cybersecurity* (Vol. 782, pp. 79–87). Springer International Publishing.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamilnadu. *IOP Conference Series: Materials Science and Engineering*, *263*(4), 042043.

Team, C. (2022). Cybercrime against women. *ClearIAS*. https://www.clearias.com/cybercrime-against-women/

Thathoo, C. (2023). India witnessed 13. 9 lakh cybersecurity incidents in 2022: Govt. *Inc42 Media*. https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/

How to cite this article: Krutika Bhate (2023). A Study on Awareness about Cyber Security Among the Female University Students. *International Journal on Emerging Technologies, 14*(2): 13–19.