STUDY ON AWARENESS OF CYBER SECURITY AMONG PRIMARY TEACHER TRAINEES IN ADDALAICHENAI GOVT. TEACHERS' COLLEGE

AM Jazeel
Department of Education and Training, University of Vocational Technology, Ratmalana
amjazeel@yahoo.com

Abstract- Cyber Crime is on the increase everywhere in the world. A large number of people have become victims to this crime. It has affected not only the dealer, but also teachers and students to a great extent. Small children are now using the Internet very often. They can also be victims. In this context, the primary teachers who are teaching small children in schools have more responsibility in educating about cybercrime and cyber security

The present study was conducted to investigate cyber security awareness among primary teacher trainees studying at Government Primary Teachers College, Addalaichenai. A normative survey method was adopted on a sample of 200 Primary teacher trainees selected by stratified random sampling technique. The data were collected by using Cyber Security Awareness Scale and Personal Information Schedule. The major findings of the study have revealed that there is low level of awareness among primary teachers on cyber security and there exists significant differences in cyber Security awareness among Primary Teacher trainees with respect to gender, locality, knowledge of computer, and having own computer.

Keywords- Awareness, Cyber Security, Teacher Trainees

I. INTRODUCTION

Cyber security has emerged one of the major concerns in the world. Many countries are facing a series of cyber security perpetrated by different segment of people. The information in digital form is not secure and that the need of cyber security is the need of the hour.

Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

Application security involves measures or counter-measures that are taken during the development to protect the applications from the threats that can come through flaws in the application design, development, deployment, upgrade or maintenance.

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that is intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Organizations transmit sensitive data across networks and to other devices during the course their doing businesses. Cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, needs to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system such as network security, application security, endpoint security, data security, identity management, database and infrastructure, security, cloud security, mobile security, disaster recovery/business continuity planning and end-user education.

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can cope up with. "As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, National Institute of Standards and Technology issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model" (StaysafeonlineOrganisation).

The National Cyber Security Alliance, through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security man across all business practices. NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information; (Ibid) and outlining the damage the organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others (Ibid). Following a cyber-risk assessment, develop and implement a plan to mitigate cyber risk, protect the "crown jewels" outlined in your assessment, and effectively detect and respond to security incidents. This plan should encompass both the processes and technologies required to build a mature cyber security program. An ever-evolving field, cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by attackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defence against cyber criminals attempting to gain access to the company's sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures (Vipul,2013)

In cyber assessment, Sri Lanka is ranked 72nd in a global ranking of 164 countries that measures the strength of countries in cyber security strategy in terms of Global Cyber Security Index - 2017 released by the UN Telecommunication Agency, the International Telecommunication Union (ITU). The ranking was based on countries' legal, technical and organizational and research capabilities and their cooperation in information sharing networks (*Ibid*). On this ranking, Sri Lanka has been listed in the maturing stage category which refers to 77 countries that have developed complex commitment to cyber security.

In this context, the awareness of cyber security is paramount important not only for the people who are dealing in business, but also for all the segment of people in the country, particularly the students who are using computers for saving and sharing their information. In the absence of previous credible researches about the cyber security among university students, this study is planned to find out the awareness of cyber security among the university students (Jazeel. 2017).

Justification for the Study

The cybercrime rate has increased in the world unprecedentedly. A large number of people have become victims. The main reason for falling victim is, among the other things, lack of awareness about cybercrime and cyber security.

Nowadays, Primary Teachers are mostly using technologies for the purpose of teaching learning process. They need to be contacted with the facilities of Information Communication Technology, particularly the use of the

Internet. The Primary Teachers who interact through the Internet can be one the victims of the cybercrime due to lack of awareness of cyber security (Vipul, 2013).

The review of related literature revealed there is no research found to assess the awareness of cyber security among primary teacher trainees studying at teachers colleges. Hence this study is planned to bridge this gap taking into all these needs.

Objectives of the Study

1. To find out the level of awareness of cyber security among primary teacher trainees
2. To find out whether there is any significant difference in the awareness of cyber security among primary teacher trainees based on gender, locality, qualification, knowledge of computer, and having own computer.

II. METHODOLOGY

In this study, a normative survey method was adopted.

Population of the Study

The population of the study constitutes all the primary teacher trainees studying at Government Teachers College, Addalaichenai

Sample of the Study

A sample of 200 primary teacher trainees following two years in-service teacher training at Government Teachers College, Addalaichenai was selected by using stratified random sampling technique. The strata for the selection were gender, locality, qualification, knowledge of computer and possession of computer

Tools for the Study

The following tools were used for collecting the necessary data for the study

1. Cyber Security Awareness Scale: To measure the awareness of cyber security among the sample, a Cyber Security Awareness Scale developed by Prof. Prema(2010) was used. This Scale consists of 15 items in a five point Likert Scale. Author of the Scale claimed that the instrument has good reliability and it was estimated and reported to be as α = 0.83 and test retest reliability 0.73. The author also claimed the Scale has validity.
2. Personal Information Schedule: The demographic data such as sex, locality, qualification, knowledge of computer and possession of computer of the participants were collected using Personal Information Schedule.

Procedure

The investigator requested their consent after explaining the objective, nature and method of study. After obtaining the participants informed consent, the research instruments were distributed among them. After completion, the instruments were collected back and checked for incomplete or omission. Then the instruments were scored as per the scoring scheme and entered in to a spread sheet for statistical analysis.

III. RESULTS AND DISCUSSION

The data collected by using the tools were calculated and tabulated in the following tables. Mean, Standard Deviation, and t value were calculated and the results are presented in table 1.

Table1. Level of Awareness of Cyber Security among Primary Teacher Trainees

Level of Awareness of Cyber Security	Range of Scores	Number of Primary Teacher Trainees	Percentage
Low	10 -29	112	56
Average	30 -49	56	28
High	50 -69	32	16

From the Table 1, it can be seen that 56 per cent of primary teacher trainees have low level of awareness, 28 per cent of primary teacher trainees have average level of awareness and 16per cent of primary teacher trainees have high level of awareness.

Table2. Differences in Awareness of Cyber Security among Primary Teacher trainees in terms of gender, locality, qualification, knowledge of computer, having own computer

Variable		N	Mean	SD	t-value	Level of Significance
Gender	Male	80	27.23	9.44	5.7	Significant at 0.01
	Female	120	26.39	8.73		
Locality	Rural	142	24.80	11.89	3.6	Significant at 0.01
	Urban	58	28.82	8.33		
Computer knowledge	Yes	122	23.79	7.92	2.9	Significant at 0.01
	No	78	28.98	6.07		
Possession of Own Computer	Yes	90	24.96	8.40	3.7	Significant at 0.01
	No	110	29.09	8.10		

Differences in Awareness of Cyber Securityamong Primary Teacher Trainees in terms of Gender

It is found from the above table that the't' value calculated for the sample with respect to their gender is 5.7. It is found to be more than the table value obtained. This shows there exists significant difference in respect to gender in awareness of cyber Security among Primary Teacher trainees. The mean score of male Primary Teacher trainees is higher than the female Primary Teacher trainees. Hence, it is inferred that malePrimary Teacher trainees have more awareness about cyber Security than the female Primary Teacher trainees.

This result endorses the findings of previous similar studies done. Dilmac, et al.(2009) investigated about cyber bullying. They found that the male students were the victims of cyber bullying at least once in their lifetime and more cyber bullying behavior than females.

Differences in Awareness of Cyber Security among Primary Teacher Trainees in terms of locality

It is also found from the above table that the 't' value calculated for the sample with respect to their locality is 3.6. This value is found to be more than the table value obtained. This shows there exists significant difference in respect to locality in awareness of cyber Security among Primary Teacher trainees. The mean score of urban Primary Teacher trainees is higher than the rural Primary Teacher trainees. Hence, it is inferred that urban Primary Teacher trainees have more awareness about cyber Security than the rural Primary Teacher trainees

From the above table, the 't' value calculated for the sample with respect to their qualification is 0.6. This value is found to be less than the table value obtained. This shows there is no significant difference in respect to qualification in awareness of cyber Security among Primary Teacher trainees. But, the mean score of degree holding Primary Teacher trainees is slightly higher than that of the Primary Teacher trainees with GCE (A/L).

Differences in Awareness of Cyber Security among Primary Teacher Trainees in terms of Knowledge of Computer

It is found from the above table that the 't' value calculated for the sample with respect to their computer knowledge is 2.9. This value is found to be more than the table value obtained. This shows there exists significant difference in respect to computer knowledge in awareness of cyber Security among Primary Teacher trainees. The mean score of Primary Teacher trainees with computer knowledge is higher than that of the Primary Teacher trainees without computer knowledge. Hence, it is inferred that the Primary Teacher trainees with computer knowledge have more awareness about cyber Security than the Primary Teacher trainees without computer knowledge

Differences in Awareness of Cyber Security among Primary Teacher Trainees in terms of Possession of Own Computer

It is found from the above table that the 't' value calculated for the sample with respect to their owing computer is 3.7. This value is found to be more than the table value obtained. This shows there exists significant difference in respect to owing computer in awareness of cyber Security among Primary Teacher trainees. The mean score of the Primary Teacher trainees who own computer is higher than the Primary Teacher trainees without their own computer. Hence, it is inferred that the Primary Teacher trainees having computer on their own have more awareness about cyber Security than the Primary Teacher trainees without owing computer.

IV. DISCUSSION

The findings of the study establish many of the previous studies done on cybercrime and cyber security. Bala Josephine, and Sudharson (2017) in a study conducted on Awareness of Cyber Crime on B.Ed student trainees, revealed that the students who own their own computer at home have more awareness about cybercrime and cyber security than other who use computers in the laboratory. It explains that the students who own their computer at home have more time in using computer. They surf on the Internet. They become known about the crime and the possible security measures with the help of information they receive online.

Similarly the female teacher trainees have less awareness than the male teacher trainees on cyber security. This may be due to the fact that the male teachers are more connected with getting information through newspapers, television news and other advanced technology concepts. The female trainees have only limited opportunities due to the nature of duty they need to perform at home in the capacity of wife and mother (Jazeel, 2017). Urban teacher trainees were found to be significantly higher in cyber Security awareness due to the fact that they have more opportunities in utilizing the advanced technology effectively, and through various sources which create awareness among them than rural students (Rajeswari, and Saravanakumar,2013.

In another study about online security, Vipul, (2013) argues that cyber security is a complex process and the security measures are changing on. Therefore, the awareness of security will only limit out dealing online. This argument does not hold sound water in the case of cyber security. The awareness of security system can prevent possible catastrophe later and keep data safe.

By and large, the findings of the study can create awareness among teacher educators, research workers, and curriculum developers to revise the curriculum and educate teacher trainees on cybercrime and security so that a safer world can be formed in future.

V. CONCLUSION

It is concluded from the analysis of results that most of the Primary Teacher trainees have low level of awareness about cyber security. This show there needs workshops incorporated in the curriculum for educating about cybercrime and cyber security. From the analyses, it was also concluded there are significant differences in the awareness of cyber security in terms of gender, locality and possession their own computer.

VI. REFERENCES

Rajeswari M and Saravanakumar AR (2013). Computing and ICT as a change agent for Education, *International Journal of scientific Research*, India, 2(12), 12 -19.

Jazeel, A M (2016). *Research in Education*, Colombo: Attal Publication

Jazeel A M (2017). A Study on Awareness of Inclusive Education among Parents of Special Need Children, *Journal of Social Welfare and Management*, 9 (1), 24 - 36

Bala Josephine M L and Sudharson (2017). Awareness of Cyber Crime among B.Ed Teacher Trainees, *Bonsecours International Journal on Educational Research (BIJER)* 1(1)

Vipul P (2013). Media role in creating awareness about cyber Security. *International journal of research and development in technology and management sciences*, 9(25), 187-198

Staysafe online Organisation (2018) Safe online, accessed from www. Cyber safe online.com