CYBER SECURITY AWARENESS- A NECESSITY FOR MORE PRODUCTIVE DIGITAL EXPERIENCE

Dr. Noora Abdul Kader
Assistant Professor, Department of Education, Aligarh Muslim University, Aligarh, Uttar Pradesh.

Received: March 18, 2020 Accepted: April 21, 2020

ABSTRACT: *It is an urgent necessity in the present scenario to protect ourselves from cyber attack and prevent ourselves from cybercrimes. Reports of the surveys conducted by National Crime Report Bureau (NCRB) is shocking as our younger generation are much involved in cybercrimes evolved out of peer revenge, sibling rivalry and also for getting quick money. Both males and females are victims of cybercrimes in one way or the other way. Phishing emails, hacking, cyber pornography and child pornography are common cases of cybercrimes in India. The present study is checking the awareness on cybercrimes among post graduate prospective teachers of Aligarh Muslim University, Uttar Pradesh. A total of 100 sample have been selected, 40 males and 60 females, through purposive random sampling technique. Data was collected using Cyber security awareness questionnaire and percentage analysis was the statistical technique used. The data was collected on certain dimensions of Password Hacking, Virus Attack, Cybercrime, Use of social media and Misuse of Social network.*

Key Words:

Introduction

In the present technetronic world, protecting ourselves from the cyberattacks and taking right steps to prevent them is an urgent necessity. Simply getting knowledge won't do anything unless and until we pay attention in changing our attitudes and behaviours. It is the responsibility of each and every citizen to take better initiatives for reducing human error and help the world to develop a safer and productive experience in digital world. "In today's life, there are continuous attacks on a big organization that allow access to the internal network, therefore resulting in the economic meltdown which causes loss of reputation and prestige as a company" (McCrohan, Engel, & Harvey, 2010; Troia, 2018). In the present scenario, there is much more cyber world do for everyone. Students access internet facilities much more for entertainment and also for work and pleasure. Its an aid to help them in completing the assigned research works, assignments, projects and proposals. Keeping in touch with social media is like a necessity of life. nothing is private nowadays among the new generation. Vlogs are controlling and maintaining their life. daily routine and household activities are open for all to view and comment. The negligence and ignorance in dealing with cyber horizons are met with cybersecurity threats for which they will have to pay and suffer a lot. Online banking sessions are hijacked with certain hidden malwares that log on to our keystrokes using an infected link, without our consent and knowledge. Access to personal information has become much easier nowadays using spoof websites. Information like email passwords, social media profiles are hacked by phishers using spoof websites.Data compromise, financial loss, and identity theft could be done through services like WIFI, ATM facility and public computers.Digitalizing ourself more and more in the community, may have serious setbacks by putting ourselves at greater risk. It is a great necessity to have good awareness on internet safety and security. The best way to overcome cybercrime is through prevention. Using of weak passwords for storing personal information and profile, re using the password and sharing of password etc. are keeping everyone at risk of cyber threat.

It is very difficult to keep us away from all the techniques of the hackers. They may use variety of techniques like crack passwords, brute force attacks, keylogger software and many more. At least we could prevent ourselves from such cyberattacks to some extent with proper awareness. Social media platforms like YouTube, Instagram, Facebook, Twitter are the most popular through which our younger generation are really fond of. Poor password habits can make it too easy for anyone to access our profile and even make financial and personal loss. Apart from the benefits, social media is directing the users to a world of fascination in which everyone is spending a lot of time. Cases are being reported every day related to bullying, harassing, black mailing, child pornography, leaked videos of private conversation etc. We have also noticed many cases in which friends, family members or even partners are found to be guilty of the cybercrime.

Need and significance of the study

Digital world is becoming smart and hackers are also becoming much smarter in retrieving the data. The whole world has moved themselves to a pocket computer. Increased use of social media, cloud storage, online payments are in turn increasing cybercrime around the globe. We cannot cease ourselves from digitalizing, it is essential that we have to move with the flow. But, being vigilant and protecting ourselves are equally important. How much we try to conceal our password, hackers are that much crooked to disclose it. The personal and financial data of the consumers are everywhere. The computers and laptops that we are using is not away from the attack of malware, ransomware and phishing. Phishing attacks are mainly targeting social security numbers, credit card information, and bank account data of the customers.It is also a necessity to highlight that education sector ranked the last in terms of cyber security performance, as compared to other major sectors or industries. And there lies the need for the students to develop a self-responsibility to enhance their safety. “Uttar Pradesh has reported an over 90% rise in the involvement of students in Cyber-related crimes since 2012” Time of India. According to NCRB (National Crime Report Bureau) “out of 812 students alleged involvement in cases related to cybercrime in the country, 318 were from UP. In 2012, 30 were involved in cybercrime which rose to 40 in 2013”.Similarly, the number went up to 62 out of 1223 arrest”. It was shocking that the majority cases of cybercrimes are of sexual in nature from the classmates or girl/boyfriends on social media for taking revenge. It is also a fact that the actual number of cases are much high compared to the reported cases. Most of the parents of the victims are showing reluctance to report cases against the accused, as they don’t want to risk their name and fame in the society. Quoting the words of famous cyber security expert, Rakshit Tandon, “The maximum number of arresting across India in cybercrime cases are of school and college going students. Since the current generation youth is champions of cyber or web, we find a trend of revenge, sexual exploitation, blackmailing and others in cyber crime committed by them. The problem is, our education system has not taught them cyber hygiene, netiquettes and ethics. They have just been left open to high end technology and devices to play”.“A total of 2,208 cases of cybercrimes were reported in Uttar Pradesh of which 186 cases were of online prank followed by cyber extortion 171, sexual exploitation 139, 112 of disrepute or humiliation, 115 for inciting hate crimes against community, 59 of piracy and 41 for blackmailing. But the highest number of cases were online fraud for financial gain cases was 1154 in the state” Times of India.

Literature review

Network traffic, phishing emailsand user profiling are mostly used by the criminals for cyberattack in launching an attack,(Moallem, 2019). An approximate of 4.9% of students had perpetrated cyberstalking (Reyns, Henson, & Fisher, 2012). “The availability of technology has provided an application for educations either online or offline, university students can access much information unlimitedly, which also helps them to expand their learning (Al-Janabi& Al-Shourbaji, 2016)”. “There is a direct relationship between preventive measures and information security awareness, which increase the security performance”(Knapp, Marshall, Rainer, & Ford, 2006). “There is a strong relationship between knowledge of information security and the behavior of people” (Kruger, Drevin, & Steyn, 2010). Cyberattack can be minimized with maximizing the awareness on cyber security. “Cybersecurity awareness programs should be developed in such a way that such elements must be included, these elements security policies and rules designed by the organization to achieve the desired outcome” (McDaniel, 2013). “University systems have continuously been attacked as a result of open access to information and also a vast amount of power worth connecting” (Katz, 2005).

Objective

- To identify the level of basic knowledge of cybersecurity among prospective teachers

Methodology

The study is descriptive survey in which data has been collected from prospective teachers of Aligarh Muslim University using Cyber security awareness questionnaire. The sample was collected through purposive sampling technique.

Sample

100 postgraduate prospective teachers, 60 females and 40 males, were selected through purposive sampling technique from the Department of Education, Aligarh Muslim University for collecting the data.

Tool

Survey questions are framed based on various cyber security issues like password strength, Virus attack, Cybercrimes and using of social media. These survey questions were sent by Google forms online survey to the students. The survey question covers on User ID's, Passwords, malicious protection, computer viruses, phishing, pop-up windows and fake friends on social media.

Analysis

The responses of the participants were analysed and described under the following heads

- **Use of social media:**

From the responses of the prospective teachers, it is revealed that, 67.3% of them are using their gadgets during day time and 32.7 % of them are using it mostly at night. WhatsApp and facebook are the most widely used social platforms by the prospective teachers. As per the result revealed, 57% of the prospective teachers are using internet for entertainment, 25% of them are using internet mainly for studies, 18% for getting awareness on happenings in and around the world.

- **Password strength:**

Password strength	Yes (in %)	No (in %)
Changing password periodically	53.8	46.2
Re using previous password	46.2	53.8
Using same password for each account	44.5	55.5
Sharing password with any one	15.4	84.6
Trying hint to recover password	61.5	38.5
Accepting prompt to save password	51	49
Using common dictionary word as password	17.3	82.7
Changing password, when it is compromised	90.4	9.6

Among the prospective teachers, 53.8% change their password periodically and 46.2% of them re uses their previous password. It is also revealed that 44.5 % of the sample use same password for each account and 55.5 % use different password for each account. 15.4 % of the respondents share their password and 61.5% of them are trying 'hint' to recover password if forgot. 51% of the sample are accepting prompt to save password and 49% do not. 17.3% of the prospective teachers use common dictionary word as password and 82.7 % do not do the same. It is also revealed that 9.6% of the prospective teachers do not change their password, when it is compromised.

- **Virus Attack**

Virus Attack	Yes (in%)	No (in%)
Laptop Anti virus protected	79.6	29.4
Knowledge of copyright	64.7	35.3
Reading terms and conditions before installing app	42.3	57.7
Checking viruses with a virus scanner	52	48
Downloading free software from untrusted source	22	78
Software in auto update mode	54.9	45.1

When questions were asked related to the dimension 'virus attack', 79.6% of the respondents revealed that their laptop is antivirus protected. 64.7% of the sample have the knowledge of copyright and 42.3 % of the prospective teachers read terms and conditions before installing app in their gadgets. 57.7% of the prospective teachers do not read terms and conditions before installing app in their gadgets and 22% of the respondents are checking, before implementing or using software from any source, for viruses with a current virus scanner. 52% of the respondents revealed that they are checking viruses with a virus scanner and 48 % do not. Software and operating systems are in auto update mode of the 54.9% of the respondents. 78% of them revealed that they do not download from untrusted source while 22 % does the same.

- **Cyber crime**

Cyber crime	Yes (in %)	No (in %)
Ever been to cyberattack	11.8	88.2
Reporting the same to the authorities	2	98
Awareness on phishing	58.8	41.2
Awareness on cyber pornography	52.9	47.1
Knowledge on cybercrime investigation cell	32	68

Knowledge on registration of cyber crime	22	78
Knowledge on information technology act	21.6	78.4

It is evident from the responses that 11.8 % of the respondents where been to one or the other mode of cyber attack and all of them were female prospective teachers. Among them only 2% reported it to the concerned authorities or in the police station. 58.8% of them reported that they are aware about phishing and 52.9% were aware about cyber pornography and its related punishment under Indian judiciary. Only 32% of the prospective teachers are aware about the nearby cybercrime investigation cell or police station. It is really pathetic that 78% of the respondents even do not know that cybercrime could be registration online and 78.4% of them didn't read or have information related to Information Technology Act, 2000.

- **Misuse of Social Network**

Misuse of Social Network	**Yes (in %)**	**No(in %)**
Loosing money through internet transaction	19.2	80.8
Connecting to public WIFI without authentication	51.9	48.1
Giving gadget to any centre for repair	66.7	33.3
Sharing photos in social media	62.7	37.3
Unknown friends in social media	52.9	47.1
Sharing personal information on internet	23.5	76.5

Due to lack of knowledge, 19.2% of the sample lost money in internet transactions and 51.9% of the sample connect themselves to any public WIFI without any proper authentication. 33.3% of the respondents give their laptop or mobile in any of the centres for repair. 37.3% of the prospective teachers share their personal photos in social media and 47.1% of them have unknown friends or strangers as friends in social media. Only 23.5 % of the respondents share their personal information on internet, as revealed from the analysis.

Conclusion

Awareness through better prevention is always a necessity at this juncture. Literacy rate of women is not equal to that of men. Cyber literacy is much less among women compared to men. The fact that should not be neglected is that both men and women are prone to cyberattacks, with women more victimized than men. Irrespective of age, our country has witnessed cyber crimes in all nook and corners. Proper campaign should be there for giving knowledge and awareness related to using of media in social platforms and disclosing their privacy through various social platforms.

References

- Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information and Knowledge Management, 15(1). https://doi.org/10.1142/S0219649216500076.
- Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD '05, 43–48. https://doi.org/10.1145/1107622.1107633.
- Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316–327. https://doi.org/10.1108/09685221011095236.
- McDaniel, E. (2013, July). Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness. In Proceedings of the Informing Science and Information Technology Education Conference.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students. Deviant Behavior, 33(1), 1–25. https://doi.org/10.1080/01639625.2010.538364.