
A study of Cyber Awareness of the College Students

Dr. P.V. Sathe

Asso. Professor,

Brihan Maharashtra College of Commerce, pune

Introduction:

What is cyber security and why should we care? Cyber security has become a new concept in the last decade. We live in a world where technology is integrated into our daily lives. We spend more and more time using the internet for work, education and socializing. Being part of this cyber world is no longer a luxury, but a necessity for many cyber users so it can be said that “*We are becoming the cyber generation*”. While these advances are making our daily lives easier they are also adding extra risks to our personal information. Most people do not think about their identities getting stolen when they make an online transaction, check their email, or use social media. However, each time that you put your personal information on the Internet you are at risk of that information getting stolen. Therefore one needs to understand the possible cyber threats associated with using cyber devices and tools such as mobile phones, tablets and desktops, and connectivity to the Internet. There are many simple ways that these risks can be reduced, but it starts with cyber security awareness. Ideally, all cyber users should understand the technology they use and how to use it properly and safely.

“I dream of a Digital India where cyber security becomes an integral part of our National Security”.
-Narendra Modi

Objectives of the study:

The objective of this research is:

1. To understand the level of awareness regarding security measures adopted by cyber users.
2. To know the direct and indirect issues faced by cyber users.
3. To provide suggestions for safe cyber uses.

This research also investigates a number of current cyber security problems faced by young college-going population, including social acceptance of mobile use and access to inappropriate material.

Methodology:

The present study is taking into consideration college students and their awareness regarding cyber security and cyber issues. A questionnaire has been designed and administered through the internet. The questionnaire was sent to target groups through WhatsApp groups at various levels in college at degree level. The first respondent was requested to forward it to the peer groups. The sampling is largely selective in nature and a snow-balling sampling method is followed.

Review of Literature:

A study conducted in South Africa by Professor Elmarie Kritzinge, from the University of South Africa conducted a web based survey. The questionnaire focused on areas like cell phone and internet

use; access to inappropriate material; cyber-bullying perceptions and experiences. Data was collected from a sample of 503 respondents (278 males) representing mainly high school learners (67% government school). The respondents were between the ages of 16-19, all with access to the internet.

Existing literature and current research repeats the large degree to which technology is integrated in the lives of South African youth. The study observed that high levels of internet access and mobile usage (41% of respondents spend more than 3 hours a day on the internet and 60% of the respondents spend more than 3 hours a day on their cell phones) create a 'cyber-world' in which youth are constantly immersed. Although concerns around online scams and privacy of personal information are indicated as the most notable 'internet threats', over 40% of South African youth in this sample report that cyber-bullying is also an issue and 88% feel that it is a 'big deal'. Despite the moderate levels of involvement by teachers and parents in education around cyber-security awareness, there is a strong desire for this topic to be covered within the school curriculum, particularly within the life-orientation subject. These findings suggest that various educational campaigns addressing cyber-bullying should be implemented in the South African high school environment in order to address a 'new-age' phenomenon that may increase in prevalence as a result of further technological developments and advances.

Studies in India by Parmar and Patel (2016) concluded that most of the netizens, irrespective of being related to IT field were not able to actively keep themselves updated with the latest information related to cyber law and computer security. They felt that the situation could be ever worse among the netizens who are not associated with IT field. They recommended inculcating basic ethics among netizens, while creating awareness on cyber laws in India.

Mehta & Singh (2013) studied the awareness about cyber laws in Indian society and found that there is a significant difference between the awareness level of male and female users of internet services and established that male netizens are more aware of cyber laws compared to women users.

Another study by **Aparna and Chauhan (2012)**, analyses cybercrime awareness in Tricity has revealed that giving more importance to cybercrime awareness can be an efficient tool to decrease or prevent cybercrimes. It remains the responsibility of the net users as well as the government to ensure a safe, secure, and trustworthy computing environment

Analysis of the study:

The survey for the study was carried out through a web based survey which included open-ended responses. Participants were sent a web-link of the survey. The questionnaire focused on several areas including: respondent demographics; usage and access to material; choice regarding adoption of various preventive measures. The final sample included 161 respondents. The respondents were mainly college students between the ages of 18-25 years.

- **Respondents Targeted:**

The main people targeted for this research were between 18 to 25 years (79.1%) while 15.8% were in the age group above 25 years and the remaining from the age group below 18 years.

The younger generation is more into digitalization and carries out most of their functions through mobile phone. It is also necessary for them to have an email id for various purposes. A very small percentage (.96%) reported that they did not have email ids.

- **Usage of Email ID:**

In such a technology oriented world, the security of our personal information becomes a necessity. On the basis of our research, 57.5% of the respondents were not found to be much concerned about their private information and they did not feel it necessary to create different email ids for professional or personal uses.

- **Beware Where You Browse:**

In spite of increasing number of cyber-crimes in India, 30.8% of the respondents prefer browsing as per the availability of the device, whereas 52.2% of the respondents make an attempt to browse on a mobile phone while only 14.5% reported that they browse on a secured device.

Since there is large percentage of respondents who prefer using mobile phones for carrying out their online transactions, there is a need for all of us to take preventive measures as to protect the portable devices from threats. Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it's a friend's phone, a public computer or a net cafe or a free Wi-Fi zone, there is a possibility of your data to be copied or stolen.

- **Beware What You Share:**

A small percentage of respondents (6.2%) did state that they had responded to emails, instant messages, phone calls etc. that could hamper their cyber security.

When someone attempts to gain information through manipulation and calls or emails asking you for sensitive information, one has to refuse such information and it is advisable to call the company reporting such calls and should verify, if possible, the source asking for such information before sharing out any personal information.

- **Change of Passwords:**

Only 26.4% people are cautious about securing their passwords and willing to change it regularly; while 73.6% are exposed to danger as they were not very concerned about the security of their password.

36.3% of the respondents stated that they did not follow instructions given by the operator while designing their password and were exposing themselves to cyber threats.

Practice good password management by keeping longer password which contains more variety and does not spell out any words. Don't use same passwords for every account so that it becomes difficult for a hacker to gain access to all your systems.

- **Perceived dangers and threats due to dependence on the operators:**

85.5% of the respondents are not ready to take their own preventive measures, but rely wholly on the operators. It is also the responsibility of the user to take appropriate security measures.

- **Concerns of Respondents:**

Majority of respondents are more concerned with the possibility of virus threat (36.9%), various threats including protection of personal data which are exposed to online predators and reliability on authentication technology. Back up your data regularly and regular up-date of anti-virus software can keep you protected from threats. Be conscious of where you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smart phones.

- **Tech Oriented people:**

On the basis of responses (58.8%) people are advancing themselves towards a digitalized world by using internet banking /digital banking /Paytm and other e-wallets on a regular basis in their daily lives.

- **Feeling of Insecurity:**

In such a cyber-attack threatening world (36.5%) respondents are not really worried in accessing the internet, while (29.6%) of the respondents are concerned because they feel that the various security measures taken by them against cyber threats are not sufficient to tackle those problems and issues related to cyber threats.

- **Security measures adopted:**

Out of the total respondents, 72.2% prefer to have installed anti-virus software on their devices, while 30.6% of the respondents have installed anti-spam software.

42.7% make use of multiple passwords for each account while only 31.2% of the respondents encrypt their important files.

- **Appropriate Measures taken:**

In spite of the increase in the number of cyber threats in India 35.6% of the total number of respondents are not worried even if the devices are not protected with anti-virus software and other security measures.

36% of the respondents stated that adopting security measures does reduce user-friendliness while majority were of the opinion that it is necessary and much required.

Conclusion:

Cyber security and awareness is more important now than it has ever been before. Therefore the first step is to make individuals aware about the threats to their personal information and stolen identities. The second step is giving users the knowledge and tools that they need to protect themselves. It is our responsibility to make the society aware of the various issues related to cyber threats and knowledge related to cyber security needs to be made more readily available. It is important for us to help

educate individuals on what they can do to stop and prevent potential cyber security attacks as well as recognize the potential threats. Most of the time, people just hope or assume that identity theft and phishing attacks are not going to happen to them. ***Ignorance is bliss after all.*** But, making society aware that even the smallest tasks can pose potential threats is crucial for their safety.

References:

- Archana Chanuvai Narahari & Vrajesh Shah (2016) “Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India), *IJARIE-ISSN(O)-2395-4396, Vol-2 Issue-6*
- Elmarie Kritzinge (2009) “Cyber Security Awareness and Education Research” <http://eagle.unisa.ac.za/elmarie/images/Pdf/r1.pdf>
- Parmar, Aniruddhsinh & Patel Kuntal (2016), *Critical Study and Analysis of Cyber Law Awareness Among Netizens. Conference: International Conference on ICT for Sustainable Development, At http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409*
- Saroj Mehta & Vikram Singh (2013) “A Study Of Awareness About Cyberlaws In The Indian Society” *International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 1 January*

Websites accessed:

- <https://www.globalsign.com/en/blog/cybersecurity-tips-for-business>
- <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/ten-recommendations-for-security-awareness-programs.html>