Cybercrime Awareness, Vulnerability and Measures Among Higher Education Students and Teachers: An Exploratory Study of India

Noor Alam¹, Osama Qamar² & Ahrar Husain ³
¹²³Department of Teacher Training & Non-Formal Education, (IASE) Faculty of Education, Jamia Millia Islamia New Delhi, INDIA

Abstract: Awareness is the key to enlightenment. It is the light which draws out one’s from the darkness. The present study directed towards getting awareness level regarding cybercrimes in higher education students and teachers. It also reveals the vulnerability and measures that are available is adequate or not. The researchers conducted an interview on 90 participants who belong to a different discipline of higher education. Also, the respondents are from four different classes on the basis of their educational qualification. The data was gathered through a close-ended questionnaire and the researcher was there at the time of interview. The awareness of cybercrime is high on some fronts in research scholar and teachers. Also, teachers are less vulnerable to cybercrime in comparison to others. There are mixed responses on measures to control cybercrime.

Keywords: Cybercrime, Awareness, Vulnerability, Measures, Higher Education.

I. Introduction

Information now a days everything that is considered to be an indispensable part of any progressive thinking. Different media are playing a vital role in the record, publish and dissemination of information both in the form of electronic as well as print. After the invention of the internet especially the (Dennis)World Wide Web(WWW) in 1989 by Sir Tim Berner Lee which gave a new impetus to information dissemination across the globe. Communication these days has become lightning fast due to the availability of handheld gadget, supporting and affordable internet facilities. With the emergence of further technological advancement and the reach of the internet to the people especially the students, which gave birth to a virtual world where time and distance are no longer a barrier to communication. Nevertheless, this also raises serious concern regarding information security, identity authentication, privacy encroachment, data theft apart from hacking and malware attack. It is essential to spread awareness regarding possible cybercrime and measures to counterfeite or to negate their effects. In this paper, the researchers endeavor to purge out information to the public domain regarding cybercrime awareness, vulnerability, and measures pertaining to higher education students and teachers.

Cybercrime

The dictionary meaning of cybercrime is a crime committed over the internet. The general definition of cybercrime is an unlawful act which makes use of the computer either as a tool or a target. Cybercrime can be understood as an unethical act with the use of information technology to sabotage an organization, an individual or both in terms of their privacy encroachment and data theft, phishing, intrusion, thereby making it a serious crime. The nature of the cybercrime act is silent and global. Cybercrime is an umbrella term which includes Email bombing, Data diddling, Hacking, Virus Dissemination, Logic Bomb, Trojan Attack, Denial of Service Attack, Phishing, Web Jacking, Cyberstalking, Obscene mail, Cyberbullying and trolling.

II. Literature Review

(Chawki, 2005) States that legislature would call cybercrime the same old criminal activities with involvement of computer network. (Malhotra, 2017) concluded that the skillfulness of teachers and other users would be effective to combat cybercrime. (Gavekar, 2017) explored that internet users feel insecure during online transactions. (Igba Daniel Igba, 2018) accept that exploitation of human being especially children and economic impact of cybercrime is undisputed. (Muhammad Abdullah Avais, 2014) States that it is the order of the day to study cyber victimization on grass root level. It also found that the awareness is the key to prevent cybercrime. (Varghese, 2016) suggested that cyber law has unique features to develop information security awareness which prove to be powerful technique to remain safe online.

III. Objective of the Study

• To find out the awareness of cybercrime among Higher education students and teachers.
To find out the vulnerability of cybercrime among higher education students and teacher.
To find out the awareness of measures to control cybercrime among higher education students and teachers.

IV. Design of the Study
The existing research is exploratory in nature where the researchers surveyed the higher education students and teachers of Delhi-NCR. The research is directed towards the main questions regarding cybercrime awareness, vulnerability, and measures. The participants are interviewed through a close-ended questionnaire in a single phase. The sample selected is purposive and belongs to the central university situated in south-east Delhi.

V. Sample Composition
The sample consists of 90 respondents out of which 80 were undergraduate, postgraduate and research scholars, and 10 were teachers who belong to diverse discipline and educational qualification. In other words, the sampling is done in such a manner that encompasses a holistic view on the problems. It is both horizontal i.e., the participants from various disciplines like education, engineering, law, dentistry, and social science, and vertical, i.e. undergraduates, postgraduates, research scholars and teachers. It can be visualized through the fig. 1

Figure 1: Sample Composition

<table>
<thead>
<tr>
<th></th>
<th>No. of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate</td>
<td></td>
</tr>
<tr>
<td>Post Graduate</td>
<td></td>
</tr>
<tr>
<td>Research Scholar</td>
<td></td>
</tr>
<tr>
<td>University Teacher</td>
<td></td>
</tr>
<tr>
<td>Total Sample</td>
<td></td>
</tr>
</tbody>
</table>

Tool Employed for Data Collection
The data was collected through a close-ended questionnaire, consisting of 34 questions, in a single phase. The tool is prepared with the consultation of experts in the due guidance of senior academic members as no standard tool was available.

VI. Data Collection Procedure
The questionnaire is sub-divided into three major sections having equal weight to each section. The researcher collected information on many visits as the availability of respondents are ensured through their convenience. The researcher collected data after getting it clear to the respondent about the scopes and demands as well as their vital roles in the study. The privacy of the participants is ensured at every stage of the research. The researcher himself contacted the respondents and collected the information.

VII. Delimitation
The study is delimited to the following parameters.
- The data is collected from a central university situated in Delhi.
- Information for this study is gathered using a self-administered questionnaire.

VIII. Major Finding of the Study
Findings of the research are divided into three major parts and each part is further sub-divided into four sections depending on the objectives and each part is comprehended through a figure 2,3 and 4 respectively.
- **Awareness of cybercrime**

  **Undergraduate**
  Almost all participants belong to the undergraduate category aware of the cybercrime in general. Moreover, awareness regarding hacking is most known to them. The level of awareness regarding virus dissemination, cyberstalking, banking, and credit card fraud, cyber bullying, and identity theft is a bit low i.e. half of the participants know. However, only 15% of undergraduate aware of the logic bomb, Trojan attack, denial of service attack, phishing and data diddling.

  **Postgraduate**
  The level of awareness regarding cybercrime of postgraduate students is lower than undergraduate students in general. However, they are more aware of the Trojan attack, denial of service attack, obscene mail, phishing, email bombing, and cyberbullying. The finding also shows that almost all students belong to the category aware of banking or credit card fraud.

  **Research scholar**
  All participants of this bracket aware of the cybercrime. Hacking is the most known to them. Moreover, most of the scholar aware virus dissimilation, Trojan attack, obscene mail, cyberstalking, banking or credit card fraud, phishing, email bombing, identity theft, and cyberstalking. However, the awareness on some front is very low or negligible, like a logic bomb, denial of service attack, web jacking, and data diddling.

  **University Teacher**
  All the participant of this category aware of the term “cybercrime.” Also hacking is the most known to them. Furthermore, they are high on the awareness of virus dissemination, Trojan attack, obscene mail, cyberstalking, banking and credit card fraud, identity theft and cyberbullying. However, they never come across the word logic bomb. Also, they are low on phishing, web jacking and data diddling.

  ![Figure 2: Awareness of Cybercrime](image)

- **The vulnerability of cybercrime among students and teachers**

  **Undergraduate**
  More than half of the participants under this category believe that memorization of the password is the best practice to remain safe and secure online. However very few of them change their password weekly or monthly. Although more than half of them have installed antivirus in their PC and updates it regularly. Moreover, they access online banking services on a public computer which make them more vulnerable. Also, 36 percent of them faced problems either of improper sign-out or forget to sign-out.

  **Postgraduate**
  More than half of the participants under this category secure their password through memorization. They believe that memorization is the best way to keep one’s password safe and secure. Moreover, half of them have antivirus
on their PC and update it regularly. They only access online banking services through public or shared computers when it is very urgent otherwise they avoid it. However, very few of them change their password weekly or monthly. Most of them are never change their passwords. Almost half of them faced problems either of improper sign-out or forget to sign-out.

Research scholar
They are high on the protection of password as they believe in keeping their password safe and secure through memorization. Also, most of them change their password on yearly basis. Moreover, all research scholars have antivirus on their PC, and they update it regularly. They never access online banking services from shared or public computers. However, they do not practice to change their password weekly or monthly basis. Most of them suffered due to improper and not to sign-out after accessing their email account.

University Teacher
Only half of the teachers keep their password through memorization. Although the majority of them believe that memorization is the best practice to keep one’s password safe and secure. Moreover, few of them change their password weekly or monthly basis, and half of them never changed their password since they have created their email account. Majority of the teachers have antivirus on their PC and they update it regularly. They also avoid public or shared computer for banking services. Moreover, most of them never faced problems due to improper or not to sign-out of their email account after access.

Figure 3: Vulnerability of Cybercrime

- Awareness of measures to control online activities

Undergraduate
More than half of the students under the bracket aware of Information Technology (IT) Act (2000). A chunk of i.e., 34 percent of students believe that Section 43 of the IT Act, that penalize for damage to the computer etc. is adequate and substantial. Although 30 percent of them do not think that it is sufficient and 8 percent hold that penalty is excessive and should be curtailed down. Half of the students think that the section 66 of IT Act (2000), penalize for hacking is adequate. However, 20 percent think that penalty for hacking should be enhanced. The research also shows that 30 percent participant under the category think that the law in effect to control cybercrime is not sufficient.

Postgraduate
Around half of the students under this category aware of the IT Act, 2000 and most of them think that Sec. 43 of IT Act penalize for damage of the computer, etc., is adequate. However, 15 percent think that penalty should be enhanced. Majority of them think that Sec. 66 of IT Act (2000), is penalized for hacking is sufficient. However, 25 percent feel that punishment should be more. The research also revealed that only 25% of students think that the law in effect to curb cybercrime is sufficient.

Research Scholar
Half of the research scholar aware of the IT Act (2000). In the majority opinion, Sec. 43 of the Act that penalizes for damage of computer is adequate. Moreover, 50 percent of the research scholar feel that Sec. 66 of the Act that punishes for hacking is adequate and only a few of them think that law in effect to control cybercrime is sufficient.
University Teacher
They are the only of the above-mentioned categories whose awareness of IT Act (2000) is very high. Majority of them feel that Sec. 43 of the Act, that penalizes for damage of computer is sufficient and only 30 percent of them believe that Sec. 66 of the Act, that punishes for hacking is sufficient and 40 percent feel that the law in effect to curb cybercrime is sufficient.

![Figure 4: Awareness of Measures](chart)

IX. Conclusion
Change is the essential component of any civilization to get advance as time passes. However, change comes with both opportunities and challenges. We have studied many milestones as we go down the history that leads us to the present time. Information and communication technology is one of such landmark development that becomes an indispensable part of our daily life. It is impossible to image life without such technologies. The discomfort as per researcher is the cyber-related crimes. The awareness of these crimes can be the precaution for any individual as we found that the term cybercrime known by most of the respondents. They do aware of the various activities going on cyberspace that harm them directly or indirectly. However, respondents are vulnerable at some fronts and safe on others. We can not conclude in one line that all are safe or not safe in cyberspace. The responses regarding measures to control cybercrime is not either black or white. There is a need to bring all stakeholders together to devise a holistic approach to ironout the problems.

References