IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON AWARENESS ABOUT CYBER-CRIME AMONG COLLEGE STUDENTS

Arbaz Sayyad, Rutuja Dusane, Aishwarya Hanamghar, Swaraj Bhoite, Dr. B. J. Mohite

Zeal Institute of Business Administration, Computer Application & Research, Narhe, Pune

Abstract:

The aim of the study is to investigate the attention of cyber-crime among students in college. Now days, Internet is becoming an important part of our life. Everyone is very much depending on cyber world which also increase the space for cybercrime. Cybercrime is evolving as a very serious issue in today's scenario. The internet becomes integrated part of our lives because it brings joy or happiness but sometime it becomes nightmare. There is a numerous trick used by cyber criminals to cheat people. Cyber world becomes forte of everyone, government sector to businessmen, school students to college students and teenagers to adults. Thus, the current research paper focuses in finding out the answers to alarming questions "Are the students really aware that he/she is vulnerable to various cyber-crimes?"; "If is aware, to what extent?", "If not aware of cybercrimes, what measures can be adopted to make the students more aware and updated. The paper suggested a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes.

Keywords:
Cyber-Crime, Cyber Security, IT Superpower, IT Act, Awareness

Introduction:

The quantity of persons who have access the information of computers has improved as the communications industry has experienced an upheaval in current ages and unrestrained access to information offers a danger in most commercial and government statistics. Since extremely significant role that computers play in modern life, there is an essential to keep information on machines secure from fiddling, from illegal distribution, and from unlawful elimination. The Oxford Reference Online defines 'cyber-crime' as crime committed over the internet. Cyber-crime could reasonably include a wide variety of criminal offences and activities. A generalized definition of cybercrime may be "unlawful acts where in the computer is either a tool or target or both".

CBI Manual defines cybercrime as:

(i) Crimes committed by using computers as a means, including conventional crimes.

(ii) Crimes in which computers are targets.

As all digital assets present in today's scenario need to follow the CIA triad. Where, CIA refers to Confidentiality, Integrity and Availability. Since most information processing these days depends on the use of information technology, the regulation and investigation of cyber activities is vital to the success of the Organizations, Government's agencies and individuals. The finding and retention of highly skill cybercrime expert by Government and Business Enterprises cannot be overstated. This will ensure compliance with international acceptable standard of usage of computer and other technological devices in the work places. As we know, prevention is better than cure. But, irrespective of the preventive measures to prevent and or control cyber-crime, there may still be breaches, where this occur, Forensics Experts will be called in to conduct a sound digital forensic investigation, analysis, documentation and reconstruction of the crime scene and present the evidence of the findings to the appropriate

authorities or the Jury as the case may be, that can lead to arrest, prosecution and conviction of the culprit.

This paper is broken in two broad categories named as –

(I) Cyber-crime regulation and control.

(II) Cyber-crime investigation.

Cyber-crime regulation and control: -

To control and regulate cyber-crime in cyberspace many government and private organizations are conducting different types of educational workshop and seminars to educate people regarding this vital issue. Apart from this Indian government passed IT Act 2000 based on the United Nations General Assembly resolution of January 30, 1997.

The Government of India passed the Information Technology Act 2000 (Act No.21 of 2000) and notified it on October 17, 2000. The Information Technology Act, 2000, is the first step taken by the Government of India towards promoting the growth of the Ecommerce and it was enacted with a view to provide legal recognition to e-commerce and e-transactions, to facilitate e-governance and prevent computer-based crimes. However, the rapid increase in the use of Internet has led to a series in crime like child pornography, cyber terrorism, publishing sexually explicit content in electronic form and video voyeurism. The need for a comprehensive amendment was consistently felt and after sufficient debate and much deliberation, the I.T. Amendment Act 2008 was passed. The ITAA 2008 got the President's assent in February 2009 and was notified with effect from 27.10.2009. The new IT Amendment Act 2008 has brought a large number of cyber-crimes under the ambit of the law. Some of the significant points in the Amendment Act include introduction of corporate responsibility for data protection with the concept of 'reasonable security practices' (Sec.43A), recognition of Computer Emergency Response Team – India (CERT-In) as the national nodal agency empowered to monitor and even block web-sites under specific circumstances, introduction of technological neutrality replacing digital signatures with electronic signatures etc. This research focuses on the different cyber-crimes and their preventive methods to minimize the future risk.

Cyber-crime Investigation: -

The issue of investigations set in, unravelling the mysteries behind the attack, tracing the hacker through the cyber space. This is a very interesting module as forensic investigation of both network-based attacks and computer systems including mobile devices will be covered. In cyber-crime cases, the investigator's challenge is to establish the crime beyond reasonable doubt using digital evidence that exist in cyber space. This requires Computer or Cyber Forensics special skills, equipment's, lab and capabilities far different from conventional crime detection. Computer forensics is extremely important to track and establish proof in all computer related offences. According to Section 79A of the Information Technology Act, 2000, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, and digital fax machines.

The stages in involved in computer forensic investigation are usually as follows

1. Identifying the achiever of the crime.
2. Locating the means and equipment through which the crime was committed.

Statement of the Research Problem:

In view of the above and taking into consideration necessity of subject researcher has selected the research topic entitled "**A STUDY ON AWARENESS ABOUT CYBER CRIME AMONG COLLEGE STUDENTS"** for in-depth study.

Objectives of the Study:

1. To study the concept of cyber-crime.
2. To examine the level of awareness towards maintaining cyber-crime.
3. To study the positive and negative impact of cyber-crime.
4. To learn and understand cyber-crime laws.
5. To understand the purpose of security in cyber-crime.

Scope of the Study:

1.Geographical Scope: The geographical scope of the present study covers education society's nearby vicinity.

2. Topical Scope: The topical scope of the present study is restricted to study various concepts regarding cyber security, identify current awareness level of selected students.

3. Analytical Scope: The analytical scope of the study focus on the objectives of the study, and on the techniques followed such as classification of data, presentation of data, percentage calculation, comparison, testing of hypothesis through statistical devices.

4. Functional Scope: The functional scope is confined to offering a set of meaningful suggestions about maintaining cyber security and about security policies.

Validity of the Study:

- The proposed research is aimed to focus on the current situation of awareness level of cybercrime concept in the college students.
- This research will facilitate to create awareness of maintaining cyber-crime in professional and social life.
- This research will reflect the present scenario of the awareness level of cyber-crime to the concerned and will prove useful for better professional and social life.

Research Methodology Adopted:

- **Research Type:** Applied Research.
- **Sample Units:** Students in the area of Narhe(Polytechnic, Engineering, MBA & MCA).
- **Sample respondents:** Different department students studying in professional institutes.
- **Sampling Technique:** Stratified Proportionate Random Sampling.
- **Population:** All students studying professional institutes.
- **Size of Population:** about 1500 students.
- **Sampling Units:** Polytechnic, Engineering, MBA & MCA.
- **Sample size:** 50 Respondents.

Parameter of interest: Awareness about cybercrime.

	Polytechnic	**Engineering**	**MBA**	**MCA**	**Total**
Students	300	792	340	68	1500
Sample using proportionate Sampling	20	51	22	7	100
50% sample selected using random method	10	25	11	4	**50**

Data collection source:

a) **Primary Data –**

The primary data will be collected throughout the finding techniques like the personal-**interviews, discussion, on-site observation and administering structured questionnaire.**

b) **Secondary Data –**

In order to avail the secondary data necessary for the study, researcher has personally visited the following departments.

- Departments of Polytechnic, Engineering, MBA & MCA nearby Narhe
- Libraries Professional institutes.
- Websites of related cyber-crime.

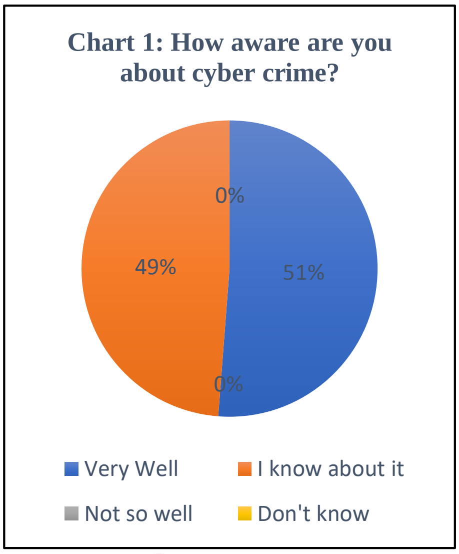
Data Analysis:

The data so collected through varied sources will be analyzed in a systematic way through tabulation, percentage and graphical presentation. Similarly, the hypothesis set will be tested with the help of statistical tools like Chi-square test.

Analysis & interpretation:

Table 1 - Awareness about Cyber-Crime.

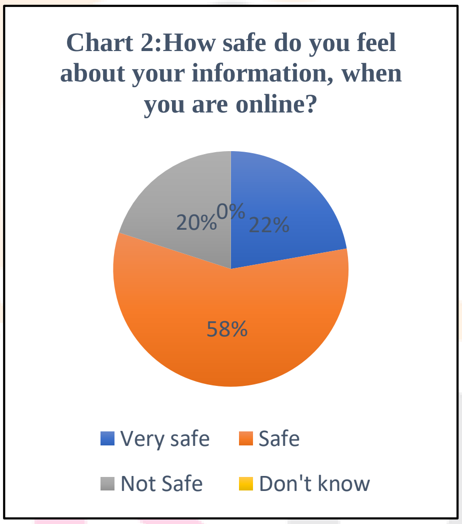
OPTIONS	NO. OF RESPONDENTS	PERCENTAGE
Very Well	21	51
I know about it	20	49
Not so well	0	0
Don't know	0	0
Total	**41**	**100**
Reference (Questionnaire)		



Interpretation:
From the above table and chart, it is observed that 51% respondents are very well aware about cyber-crime and 49% respondents are just know about it, 0% respondents are not so well known about it and only 0% respondents are unknown about it.

Table 2 - Safety of information when you are online.

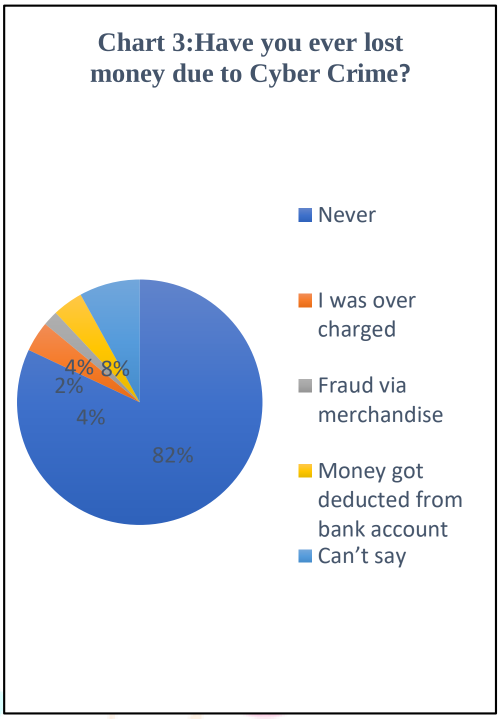
OPTIONS	NO. OF RESPONDENTS	PERCENTAGE
Very safe	10	22
Safe	26	58
Not Safe	9	20
Don't know	0	0
Total	**45**	**100**
Reference (Questionnaire)		



Interpretation:
From the above table and chart, it is observed that 22% respondents feel very safe when they are online and 58% respondents feels only safe when they are online, 20% of respondents are not feel safe when they are online and 0% respondent have don't know about it.

Table 3 - Victim of Cyber Crime.

OPTIONS	NO. OF RESPONDENTS	PERCENTAGE
Never	41	82
I was over charged	2	4
Fraud via merchandise	1	2
Money got deducted from bank account	2	4
Can’t say	4	8
Total	**50**	**100**
Reference (Questionnaire)		

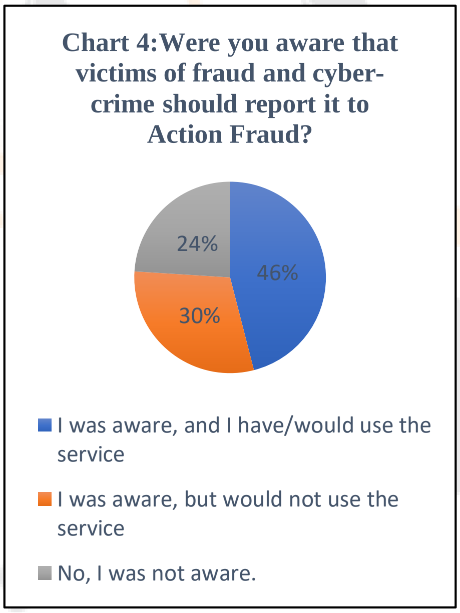


Interpretation:

From the above table and chart, it is observed that 82% respondents have never lost money due to cyber-crime and 4% respondents were over charged, 2% respondents have been facing the fraud via merchandise and 4% respondents have been deducted money from bank account 8% respondents are not known about it.

Table 4 - Awareness about victims of fraud and cyber-crime should report it to Action Fraud.

OPTIONS	NO. OF RESPONDENTS	PERCENTAGE
I was aware, and I have/would use the service	23	46
I was aware, but would not use the service	15	30
No, I was not aware.	12	24
Total	**50**	**100**
Reference (Questionnaire)		

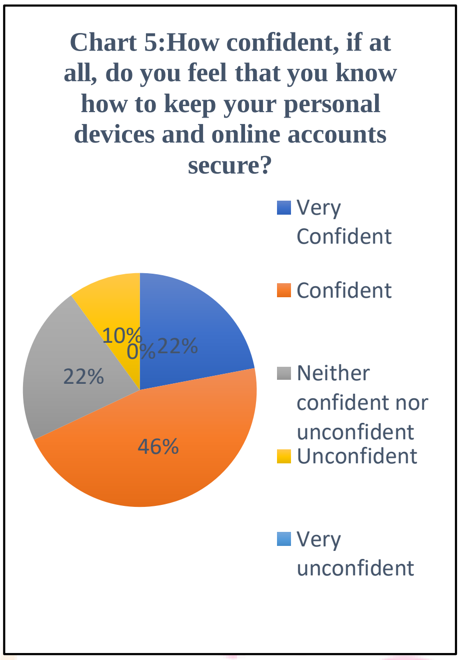


Interpretation:

From the above table, it is observed that 46% respondents were aware, have/would use the service and 30% respondents was aware, but would not use the service and 24% respondent are strongly disagree with law, 10% respondent disagree with law and 22% respondent are neutral with decision.

Table 5 - Assureness when you know how to keep your personal devices secure.

OPTIONS	NO. OF RESPONDENTS	PERCENTAGE
Very Confident	11	22
Confident	23	46
Neither confident nor unconfident	11	22
Unconfident	5	10
Very unconfident	0	0
Total	**50**	**100**
Reference (Questionnaire)		



Interpretation:

From the above table, it is observed that 22% respondents are very confident about how to keep your personal devices and online accounts secure and 46% respondents confident about how to keep your personal devices and online accounts secure and 22% respondent are neither confident nor unconfident about how to keep your personal devices and online accounts secure, 10% respondent are unconfident about how to keep your personal devices and online accounts secure and 0% respondent are very unconfident about how to keep your personal devices and online accounts secure with decision.

Findings:

The following are the major findings of the study:

1. Most of the respondents have antivirus on their PC/Mac.
2. Most of the respondents are known about cyber-crime.
3. Most of the respondents are feel only safe when they are online.
4. Most of the respondents are agree to feel safe online is very essential.
5. Most of the respondents have been never lost money due to cyber-crime.
6. Most of the respondents never face the situation like Trojan or malware, auto generated mails to your inbox, publishing obscure material on your profiles, Confidential reports/information being hacked.
7. Most of the respondents has been shopped on only highly trusted websites.
8. Most of the respondents have never been victim of cyber-crime.
9. Most of the respondents are only agree with the law against cyber-crime.
10. Most of the respondents are confident about how to keep your personal devices and online accounts secure.
11. Most of the respondents were you aware that victims of fraud and cyber-crime should report it to Action Fraud.

Suggestions:

The researcher has made personal contact with the respondents and concluded that most of the respondents think that law is ok in now a day but it will be great and effective also. And based above findings, below are the suggestions:

1. Everyone must have installed an antivirus on their pc/mac to avoid attacks like malware
2. Everyone must be known about what is cyber-crime very well to avoid the online scams.
3. Everyone must keep their information safe during online work it is very essential.
4. People should keep their sensitive information very safe otherwise they will get scammed.
5. People must have report if any of this situation is occurred like Trojan of malware, auto generated mail, obscure material on profile, credential information being hacked.
6. Online shopping is the personal choice of everyone so people must be aware about what we have shopped, quality, is if refundable or not or is its fake site, etc.

7. If people take care of their personal information or any important information very safe then there will be no more cyber-crimes done.
8. People should believe in law; they must have visited the cyber-security department without hesitation if they have faced any of cyber-crime.

References:

Related Research Paper:

1)Vajagathali M*, Navneeth Kumar S and Balaji Narayan B,” Cyber **Crime Awareness among College Students in Mangalore”**, Journal of Forensic Sciences and Criminal Investigation, ISSN: 2476-1311, Volume-12, Issue: July 01, 2019.

2)Prerna& Singh, G. (2014).” **Cyber Crime Awareness Among Prospective Teachers in Relation to Stream and Locale”**, Edubeam Multidisciplinary- Online Research Journal .7(1) ISSN: 2320–6314.

3) JV’n. Dr. Sanjay Bundela, JV’n. Kiran Kumari, **“A Study of Cyber Crime Awareness Among College Students”**, Psychology and Education Journal, VOL.58 NO. 2(2021).

4) Dr. B. J. Mohite, **“Issues and Strategies in Managing E-waste in India”**, Indian Journal of Research in Management, Business and Social Sciences (IJRMBSS), ISSN No.: 2319-6998, Vol. 1, Issue 1, Mar. 2013.

Related Books:

1) **Cybercrime and the Law: Challenges, Issues, and Outcomes (**Susan W. Brenner, 2012, Published by: North-eastern University Press)

2) **Research Methodology: Methods and Techniques** (C. R. Kothari,
2nd Revise Edition:2004, Published by: New Age International (P) Ltd., ISBN (13): 978-81-224-1522-3)

Related Websites:

1)https://en.m.wikipedia.org/wiki/Research_paper

2) http://psychologyandeducation.net/pae/index.php/pae/article/view/3547

3) https://www.scribbr.com/dissertation/methodology/