PATNA WOMEN'S COLLEGE 1940

Computer Science (BCA)

Explore–Journal of Research for UG and PG Students
ISSN 2278 – 0297 **(Print)**
ISSN 2278 – 6414 **(Online)**

http://www.patnawomenscollege.in/journal

A Study on the awareness of Cyber Crime and its security issues

• **Ankesha Shree** • **Prachi Priyadarshini**
• **Bhavna Mehrotra** • **Manisha Prasad**

Received : November 2014
Accepted : March 2015
Corresponding Author : Manisha Prasad

Abstract : *The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.*

Hence, awareness of cybercrime is necessary among citizens. In our research paper we have conducted a local survey to guage the level of awareness of Cybercrime. We have also included in our study the types of cyber criminals, the existing cyber laws in India and prevention methods against such crimes.

Keywords : *Cybercrime, Cyberlaws.*

Ankesha Shree
BCA III year, Session: 2012-2015,
Patna Women's College, Patna University, Patna,
Bihar, India

Prachi Priyadarshini
BCA III year, Session: 2012-2015,
Patna Women's College, Patna University, Patna,
Bihar, India

Bhavna Mehrotra
BCA III year, Session: 2012-2015,
Patna Women's College, Patna University, Patna,
Bihar, India

Manisha Prasad
Asst. Professor, Department of BCA,
Patna Women's College, Bailey Road,
Patna – 800 001, Bihar, India
E-mail : manisha_prasad@yahoo.com

Introduction :

All of us are well aware of the fact that computer has become the integral part of our lives, and gradually internet is also emerging as the most needed tool in our life. But all of us know that a coin has two sides, internet facility also comes with a serious threat and that is Cyber Crime.

The purpose of this research is to find out how cyber-crime is advancing; its effect on people and individuals, groups or organizations and on society. This research study will identify the adverse effects of cybercrimes, the approach of the people towards these crimes.

This research will try to identify the approach required to deal with different areas of cybercrime, analyze the problems related to in this approach and the ways adopted to effectively counterattack cybercrime.

Objective :

- to evaluate the awareness among general masses
- to ensure protection of the user over internet and standalone system.

Hypothesis :

This is an era of computerization, and we can say globalization, possible only because of Internet. Most people nowadays use Internet to facilitate their day to day work. In this situation we assume that most of them are aware of cybercrimes and they are well versed with their counter measures. This research work would find out if our assumption is true.

H0: All the internet users are aware of cybercrime and can combat them effectively.

H1: All the users are not aware of cybercrime and cannot handle them effectively.

Methodology :

- **Area of Study :** Different localities of Patna District.
- **Sample size and sampling method :** Around 100 people were considered from different age groups.
- **Tools and Techniques for data collection:** Collecting records, Questionnaires, Personal Interviews, Survey.
- **Method(s) of Data Analysis:** Data way collected and compiled using MS-Excel and a presentation was prepared using MS-PowerPoint.

What is Cybercrime ?

Cybercrime is a criminal activity which is done using computers and the Internet. This includes anything from downloading music files illegally to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Types of Cyber-Crimes

- Hacking
- Theft
- Malware
- Cyber Terrorism

India's Cyber Crime Cases :

In respect of the new IT Act, the cases related to cybercrime filed in 2013 were 4356 and this year it increased by 51 percent compared to the previous year, which means 6577.

Who are the Cyber Criminals ?

Cybercriminals often work in organized groups. Some cybercriminal roles are:

- Programmers
- Distributors
- IT experts
- Hackers
  - Black Hat
  - Blue Hat
  - White Hat
  - Grey Hat
- Fraudsters
- Cashiers
- Money mules

Hackers:

Hackers are not inherently bad—the word "hacker" does not mean "criminal" or "bad guy." Geek writers often refer to "black hat," "white hat," and "gray hat" hackers. These terms define different groups of hackers based on their behaviour.

The definition of the word "hacker" is controversial, and could mean either someone who compromises computer security or a skilled developer in the free software or open-source movements.

Black Hats :

Black-hat hackers, or simply "black hats," are the type of hackers the popular media seems to focus on. Black-hat hackers violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness, (such as creating a botnet and using that botnet to perform DOS attacks against websites they do not like).

Black hats fit the widely-held stereotype that hackers are criminals performing illegal activities for personal gains and attacking others. They are the computer criminals. A black-hat hacker who finds a new, "zeroday" security vulnerability would sell it to criminal organizations on the black market or use it to compromise computer systems.

White Hats :

White-hat hackers are the opposite of the black-hat hackers. They are the "ethical hackers," experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes.

For example, many white-hat hackers are employed to test organizations' computer security systems. The organization authorizes the white-hat hackers to attempt to compromise their systems. However, instead of using their access to steal from the organization or vandalize its systems, the white-hat hackers report back to the organization and inform them of how they gained access, allowing the organization to improve their defences. This is known as "penetration testing," and this is one example of an activity performed by white-hat hackers. Various organizations pay "bounties" or award prizes for revealing such discovered vulnerabilities, compensating white-hats for their work.

Gray Hats :

Very few things in life are clear black-andwhite categories. In reality, there is often a gray area. A gray-hat hacker falls somewhere between a black hat and a white hat. A gray hat does not work for his own personal gain or to cause damage, but he may technically commit crimes and do arguably unethical things.

For example, black hat hackers would compromise a computer system without permission, stealing the data inside for their own personal gain or vandalizing the system. A White-hat hacker would ask for permission before testing the system's security and alert the organization after compromising it. A gray-hat hacker might attempt to compromise a computer system without permission, informing the organization after the fact and allowing them to fix the problem. However, though the gray-hat hacker did not use access for bad purposes, he compromise a security system without permission, which is illegal.

If gray-hat hackers discover a security flaw in a piece of software or on a website, they may disclose the flaw publicly instead of privately disclosing the flaw to the organization and giving them time to fix it. They may not take advantage of the flaw for their own personal gain—that would be black-hat behaviour—but the public disclosure could cause damage as black-hat hackers try to take advantage of the flaw before it is fixed.

Blue Hats :

Blue Hat is a term used to refer to outside computer security consulting firms that are employed to bug test a system prior to its launch, looking for flaws so they can be closed. In particular, Microsoft uses the term to refer to the computer security professionals they invited to find the vulnerability of their products such as windows. An event that is intended to open communication between Microsoft engineers and hackers is called Blue Hat Microsoft Hacker conference. The event has led to both mutual understanding as well as occasional confrontation.

Major Findings of the Study :

- How aware are you of Cyber Crime?

A majority of peopole being surveyed were not much aware of different kinds of cyber crimes. Many of them, though were aware of virus attacks.

- How safe do you feel about your information when you are online?

Most of the people felt that their data was vulnerable when they were online.

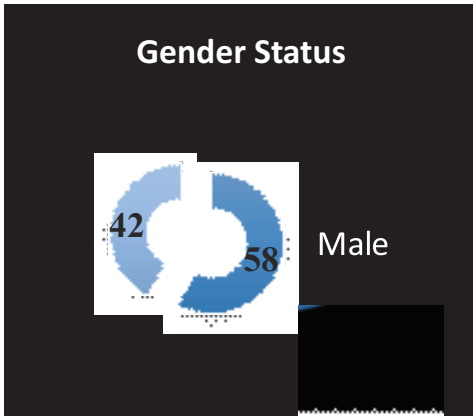
- Do you think password protection related to information security is important.

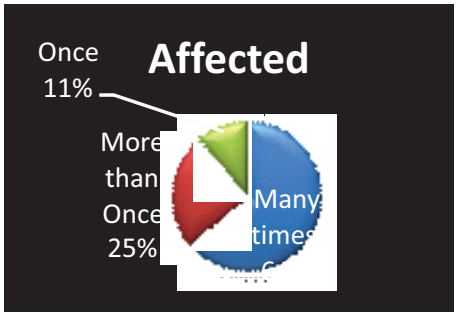
Majority of people confirmed that password was essential feature for keeping the information secure.

- Have you been robbed online unknowingly?

Many people who had been interviewed responded that they were cheated online in matter of their data and information; some of them were robbed online during financial transactions.

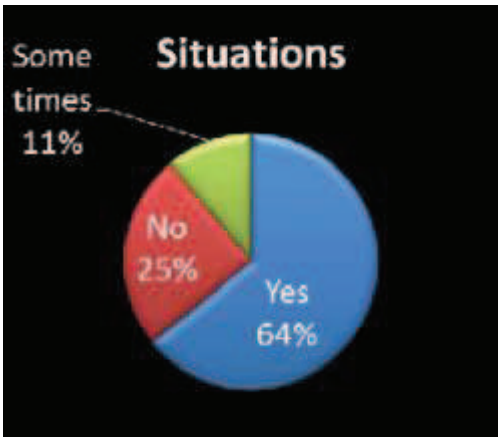
- Do you know about viruses? How severely have they affected you?





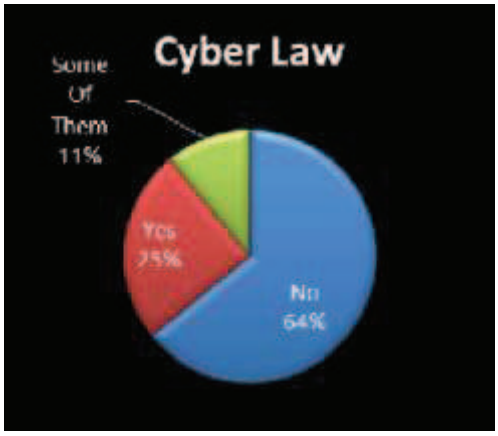
Many of the people using computer systems faced the problems of virus attacks.

- Have you ever experienced any of these situations?
  - Auto generated mails/pop ups to your inbox
  - Publishing of obscure materials to your profile
  - Confidential reports / information being hacked



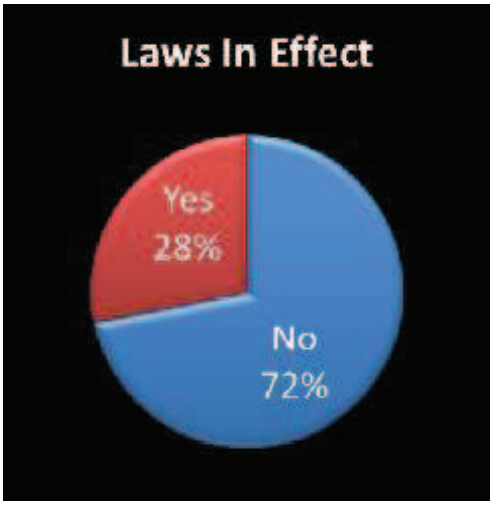
Virus attacks in the form of pop ups and auto generated mails, adwares etc. are a common feature for Internet users.

- Do you know about Cyber Laws?



Majority of people were not aware of the Cyber Laws.

- Do you think that the Laws in effect are able to control Cyber Criminals?



The major problem is the ignorance of the masses regarding the cyber law provisions in our country. A majority of people did not know how to proceed and what to do if they became victims of cyber crimes. Therefore, the biggest challenge is to create awareness about the cyber laws for its successful implementation.

Cyber Law of India:

In simple way we can say that cyber crime is an unlawful act where the computer is either a tool or a target or both. Today, there are many disturbing events happening in cyberspace. It is possible to engage into a variety of criminal activities. Hence there is an urgent need for Cyber laws in India. Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyber space. The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes.

Trends in Cyber security and Latest Counter measures:

A sense of urgency about digital security is fuelled not just by the widespread occurrence of data theft by hackers, but also via the ongoing concern for privacy issues driven by disclosures of extensive National Security Agency (NSA) information gathering. In response to these threats, companies are taking a variety of steps, and the digital security industry is seeing strong growth and innovation. The following trends in 2014 surrounding data protection and cyber security are:

- Enhanced use of encryption
- Use of digital signatures
- Increased scrutiny of internal data use
- Risk assessment and software analysis

Prevention of Cyber crime :

- Use Strong Passwords.
- Activate firewall.
- Use anti-virus/malware software.
- Block spyware attacks.
- Install the latest operating system updates.
- Secure your wireless network.
- Protect your e-identity.
- Call the right person for help.
- Increase awareness about cyber laws.

Conclusion :

The findings of the research project have enhanced our knowledge about Cyber Crime and its effects. Through our survey and study we have realized that many people are not at all aware of the consequences of the use of internet. Due to little or no knowledge about cyber crimes and laws related to it, many people are being tricked very easily and cyber criminals are taking advantage of these people.

We have tried to create awareness among people by informing them about the prevention techniques and basic laws regarding cyber-crime.

References :

Godbole, Nina and Belapure, Sumit. (2011). *Understanding Cyber Crimes, Computer Forensic and Legal Perspectives.* New Delhi : Wiley India Publication.

Wall, David S. (2007). *Cybercrime: The Transformation of Crime in The Information Age.* 1st edition, New Delhi : Wiley India Publication.

Websites :

www.scribd.com
www.slideshare.com
www.timesofindia.com
www.ted.com