International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2062156

Cyber Space Crimes and IT Laws in opposition of Cyber Offence

Phalguni Pathak*, Saumya Saraswat , Rahul Yadav
Department of Computer Science Application, ITM University, Gwalior, Madhya Pradesh, India

ABSTRACT

In today's scenario where each activity takes place on Internet, from paying bills to buying groceries and to booking movie tickets to online banking. It is necessary to have the proper knowledge about the trending security threats and laws, in reference of those threats. Use and users of internet is increasing on daily basis, which makes this virtual field, all the more perfect for cybercrime. In this paper, the discussion is based on what are the security threats we face on daily basis, their specific types and nature also what are the Cyber Laws we have against cyber-crimes.

Keywords : Internet, Security, Virtual Space Crime, Cyber Crime, Cyber Law, Cyberspace, Cyber Offence

I. INTRODUCTION

Internet is rapidly growing field, not only in India but around the globe. Internet has made our life easier but also it creates a parallel and virtual world, which is quite new to human kind. We all use internet to solve the one purpose or the other. But the bigger issue is that, not all of us are aware about the term "Cyber Crime" or the security threats we face daily. One fact says, "That in every 3 seconds, there is one **Identity Theft** takes place". As it is already said that this virtual field is quite new for human kind, so the threats and crimes are also quite different from real world. To ensure safety from those cyber crimes, special cyber laws are needed. In other words we can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet [1].

"Cyber law" can also be defined as the law that govern and set jurisdiction rules for the cyber space. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model. [2]

Cyber crime can be categorized as the offences, committed against any person, or organization with some ulterior criminal motive and mal-intention to harm the reputation of individual or organization also to cause mental and social harassment or loss. Victim can be targeted directly or indirectly via various mediums such as E-Mail, through chat-bots, phone calls etc.

Advancement of technology creates a challenging field for Law as well. The biggest challenge is to create and apply laws for various criminal instances taking place over virtual world also known as internet or cyberspace. Virtual world is an area where offenders found new possibilities everyday and still there is a lot of scope for LAW to provide a full proof jurisdiction system for cyber world.

II. METHODS AND MATERIAL

CYBER-CRIME CATEGORIZATION:

There are some of the categories we can divide cyber crime in. For example:

- Copyright infringement
- Theft of personal data
- Pornography and Voyeurism
- Cyber-Stalking
- Fraud
- Bullying

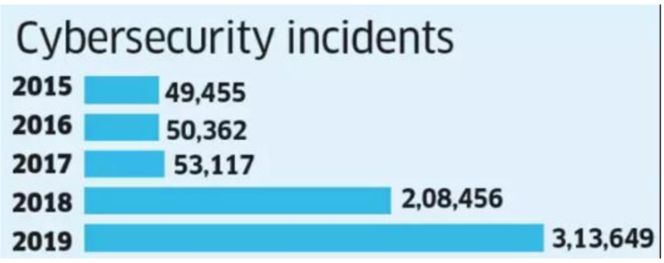


Fig 1. Reported till Oct, 2019[3]

Copyright infringement

Content and data have been uploaded over internet in vast amount every day. But copy of data and content is something that has to be dealt with necessary criteria.

Theft of Personal Data

As we access various services online, we, as individual as well as organization, needs to provide some data to those services. But the question arises **"Are we sure about our data privacy?"** Which means whatever the data user is providing to the application over cyber space is limited to the database of that particular application. And the answer of this question is quite terrifying. Because the data of user is being sometimes sold for marketing purpose or at the other times data thievery is bigger issue.

Pornography and Voyeurism

Internet has users of every age and gender. The biggest risk of them accessing porn websites which are one of the major source of hacking as well as it is socially harmful for the under-age also. Porn-industry grown over a large amount of users because of the easy accessibility of websites through internet, which definitely needs monitoring and restrictions. Whereas voyeurism involves watching others intimate behaviors, considering to be of private in nature such as undressing, or other intimate activities etc.

Cyber-Stalking

Stalking someone's profile on social media is quite normal in today's scenario. But in real terms, it is a crime. Without permission of an individual, keeping tabs on his/her profile is a cyber offence. Stalking someone over internet and gathering information is also a cyber crime. And we keep getting targeted of this cyber crime on daily basis, without even knowing.

Fraud

We all get e-mails saying, "You have won lottery/prize". Do we actually won some prize? No, it is a simplest way of fraudulent. Receiving phone calls, asking for OTP or other debit card and account details are the most common and trending way of Fraud. E-commerce in a trending field which has a lot of scope fraud with various information of individual as well as organization is available over internet (public network).

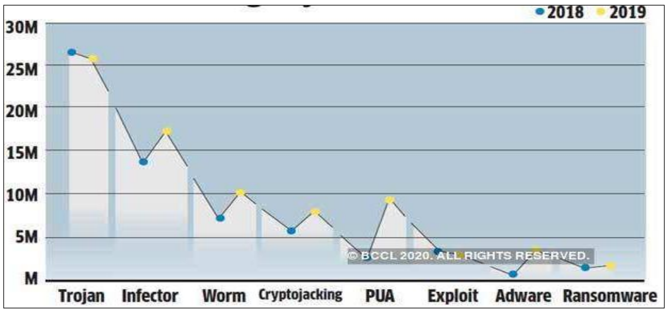
Bullying

Bullying someone over cyber space is also one of the major criminal activity, users face every day. One live example was of a game, that was developed for the purpose to target soft-hearted audience and to make them perform some task by bullying them online, resulting various suicides.

Evolution of Cyber Crime

Years	**Types of Attacks**
1997	Malicious Viruses initiated, which includes Morris Code worm etc.
2004	Torjan, Malicious code etc.
2007	Detect Data theft, Phishing etc.

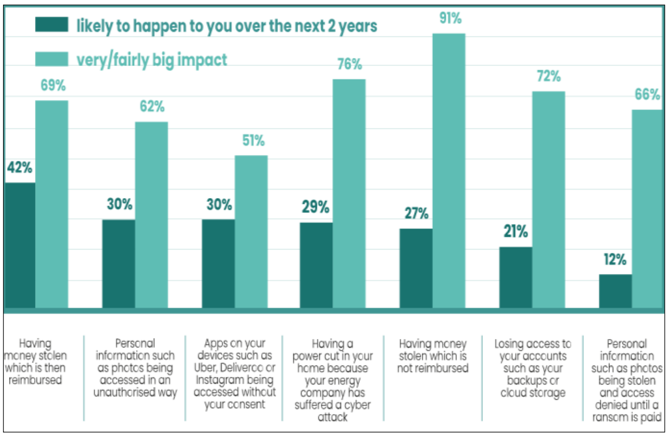
2010	Domain Name Server Attack, Botnets, Database attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack, Cyber warfare etc.



Year-on-Year Malware Detection Statistics-Categorywise[4]

CYBER-CRIME TYPES

- Very common form of cybercrime Type 1 is phishing, here the victim gets an email, supposedly legitimate, with a link that leads to a hostile website [5]. Once the link is clicked, the PC can then be infected with a virus, which leads to data corruption and data stealing.
- Another example could be, when victim downloads any file containing Trojan horse virus, which has hidden keystroke logger program. This keystroke logger program automatically installs in system and allows the hacker to steal private data such as internet banking and email passwords by keeping track of key-strokes.
- Some non-social elements also known as Hackers often use unprotected computer systems or devices in their advantage by placing various malicious viruses such as Trojan horse in the web browser. This also comes under Type 1 cyber Crime. In short any data manipulation or theft via hacking is of this type including bank and e-commerce fraud and identity theft.



III. RESULTS AND DISCUSSION

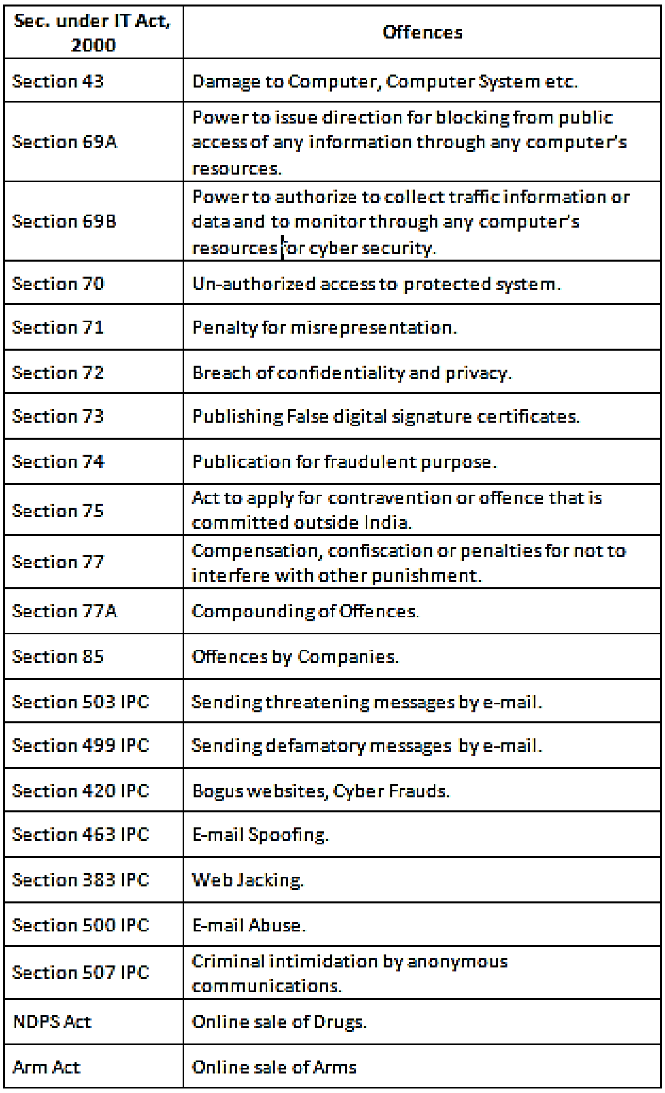
PREAMBLE OF INFORMATION TECHNOLOGY ACT, 2000

- It provides legal recognition for E-Documents.
- It provides legal recognition for Digital Signatures.
- This act explains the Offenses, penalties and Contraventions over cyber space.
- This act gives blueprint of the Justice Dispensation Systems for cyber crimes.
- This Act is also used for providing advice for the constitution of the Cyber Regulations Advisory Committee, whose work will be to advice the government about any rules and regulations related to this act.
- The said Act also proposed to amend to; The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 etc

PLOT OF THE INFORMATION TECHNOLOGY ACT, 2000

The original Act contained **94 sections**, divided into **13 chapters** and **4 schedules**.[6]

But in 2008, two sections; section 66A and section 69 were added by the amendment. The said amendment was passed on Dec 22, 2008 without any debate in Lok Sabha and the very next day, it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on Feb 5, 2009. Section 66A introduced penalty regarding sending "offensive messages". And Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism.



Sec. under IT Act, 2000	Offences
Section 43	Damage to Computer, Computer System etc.
Section 69A	Power to issue direction for blocking from public access of any information through any computer's resources.
Section 69B	Power to authorize to collect traffic information or data and to monitor through any computer's resources for cyber security.
Section 70	Un-authorized access to protected system.
Section 71	Penalty for misrepresentation.
Section 72	Breach of confidentiality and privacy.
Section 73	Publishing False digital signature certificates.
Section 74	Publication for fraudulent purpose.
Section 75	Act to apply for contravention or offence that is committed outside India.
Section 77	Compensation, confiscation or penalties for not to interfere with other punishment.
Section 77A	Compounding of Offences.
Section 85	Offences by Companies.
Section 503 IPC	Sending threatening messages by e-mail.
Section 499 IPC	Sending defamatory messages by e-mail.
Section 420 IPC	Bogus websites, Cyber Frauds.
Section 463 IPC	E-mail Spoofing.
Section 383 IPC	Web Jacking.
Section 500 IPC	E-mail Abuse.
Section 507 IPC	Criminal intimidation by anonymous communications.
NDPS Act	Online sale of Drugs.
Arm Act	Online sale of Arms

Sections of Information Technology ACT, 2000

IV.CONCLUSION

As the number of users are increasing on daily basis over inter, so as the number of cyber crime has become a growing and trending field. Here cybercrime become a great threat to humankind, secrecy and privacy of individual or organization, social and economic environment. So it became necessary for every user to be protected, while using internet. And also to have a keen knowledge about cyber laws.

V. REFERENCES

[1]. https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm

[2]. http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

[3]. https://economictimes.indiatimes.com/news/politics-and-nation/police-in-states-across-india-are-relying-on-private-firms-and-consultants-to-solve-cybercrime-cases/articleshow/72499885.cms?from=mdr

[4]. https://m.economictimes.com/tech/internet/malware-detections-surge-by-48-in-2019/articleshow/73218259.cms

[5]. Kusum Agroiya, Ritu Sharma and Dr. Mukesh Sharma, “Distributed Denial of Service(DDoS): Attacks and Defense Mechanism” , International Conference on Advanced Information Communication Technology and Engineering, 2013.

[6]. https://en.m.wikipedia.org/wiki/Information_Technology_Act,_2000

Cite this article as : Phalguni Pathak, Saumya Saraswat , Rahul Yadav, "Cyber Space Crimes and IT Laws in opposition of Cyber Offence", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 537-540, March-April 2020.
Available at doi :
https://doi.org/10.32628/CSEIT2062156
Journal URL : http://ijsrcseit.com/CSEIT2062156