Cyber Crime in India

Ritesh Verma*
Bharat Bhatt*
*Assistant Professor, Maharaja Agrasen College, University of Delhi
* Assistant Professor, Zakir Husain Delhi College, University of Delhi

Abstract

Cybercrime has grown in leaps and bounds as the computer has become central to trade and commerce, leisure, entertainment, and government.
Cybercrime involves an attack on information about individuals, groups, corporations, or governments.

An important aspect of cybercrime is its international character. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation.

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, midway along with the spectrum lie transaction-based crimes, and at the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet.
Cybercrime in India has been examined in this study. There are several sources of information used in this study including National Crime Records Bureau (ncrb) records as well as the internet and media articles. Keywords: Internet, Technology, hacking, Crime, Phishing, Cyber Stalking

INTRODUCTION

Cybercrime includes fraud, phishing, child pornography trafficking, identity theft, and invasion of privacy. Criminal activity related to the Internet has grown in recent years due to the rising importance of computers for trade and business as well in the areas of leisure and entertainment.

Today, cybercrime can be found virtually anywhere due to the widespread usage of computers and the Internet. New criminal opportunities have arisen as a result of current technological advancements. The usage of a digital computer is in between traditional criminal behaviour and cybercrime. If you ask the FBI, online criminal activity is a continuation of present criminal behaviour, along with certain novel illegal behaviours.

Cybercrime can be committed in a variety of ways. In this case, the attacks are aimed at a person's or company's virtual body. There is also an emphasis on computer networks, as well as the fragility of supposedly solid things like personal identity.

Because cybercrime is a global problem, it is difficult to combat. To combat local or even national crimes, law enforcement authorities must now work with other countries. Since the Internet is a worldwide network, cybercriminals have various hiding places on the Internet and in the real world. A good tracker can find proof of hackers' identities and whereabouts, just as a person walking on the ground can. International cybercrime treaties must be approved in order to pursue these suggestions beyond national borders.
When it comes to cybercrime, there are several types of crimes. Examples of crimes that violate personal or corporate privacy include assaults on digital depositories and the exploitation of illegally obtained digital information to blackmail a corporation or persons. In this sector, identity theft is also on the rise. Crimes such as fraud, trafficking in child pornography, piracy and counterfeiting fall in the centre of the spectrum. Since the offenders are anonymous online, they are able to perpetrate these crimes against specific victims in perfect privacy. Then there are others who deliberately falsify data for financial or political gain. Attempts to tamper with the functioning of the Internet are also crimes. Spam, hacking, denial-of-service attacks on specific websites are all examples of cybercrime or

cyberterrorist acts.

United States' judicial institutions and law enforcement organisations are challenged by crime. Cybercrime has been reported all around the world. According to Frost & Sullivan industry expert Katie Gotzen, it is presently one of the most important funding sources for international criminal organisations. As a result, the dangers associated with malware have increased. Because of this new technology infrastructure is not only used to do a criminal act, but it is also the target of a criminal conduct. As a result of the events of September 11, 2001, cybercrime would take on new forms.

Variants of technology that are used for cybercrime

Following are various variants of technology that are used for cybercrime.

Hacking

Hacking is the term used to describe the unauthorised use of computer or network resources. Common definition of hacking is to gain access to computer or network without authorization. To begin, cybercriminals target a vulnerable site before moving on to more secure sites. By gaining control of the "super-user" account, the majority of assaults are aimed to seize complete control of the system and take full use of it. It allows full access to the site as well as the ability to hide your identify. When it came to spotting weaknesses in operating systems and manuals, first-generation hackers sometimes had to create their own programmes to exploit them.As a result, they had to remain abreast of the latest developments in their field. This allowed them to grow increasingly dependent on the hacking community to identify flaws and build programmes that could be adapted to their specific requirements.

Phishing

In an electronic discussion, phishing is an attempt to get sensitive information such as usernames, passwords, and credit card details by appearing to be a trustworthy person. Communication from reputable social media platforms, auction sites, or online payment processors is often used as a ruse to deceive gullible individuals. E-mail and instant messaging pseudonymity is a frequent technique used to mislead consumers into entering their personal information on an imposter site, which has a similar appearance and feel. A common social engineering method, Phishing takes advantage of the inability of existing online security systems to be utilised to fool its victims. Phishing was originally reported in 1987, and the term "phishing" was used for the first time in 1996. "Phreaking" is a variation of fishing that refers to "bait" used in hopes that a potential victim would "bite" on a malicious link or malicious file, leading to the theft of their financial information and passwords A phoney website isn't required in every phishing operation. Users received messages claiming to be from a bank instructing them to call a phone number if they had difficulties with their bank accounts. After dialling the phone number, prompts instructed customers to input their account numbers and PIN. Vishing (voice phishing) makes use of false caller-ID data to make it look as though calls are coming from a reputable company.trusted organization.

Spamming

Spam is the indiscriminate distribution of unwanted mass communications via electronic messaging. Spam is a word that refers to comparable abuses in various media, such as instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified advertisements spam, mobile phone messaging spam, Internet forum spam, and social networking spam. Spamming is still profitable since marketers don't have any running costs other than managing

their mailing lists, and it's impossible to hold senders accountable for bulk mailings. Because the entrance hurdle is so low, spammers abound, and the amount of unwanted mail has skyrocketed. The total number of spam messages sent in 2011 is expected to be approximately seven trillion. The public and Internet service providers, who have been obliged to build extra capacity to cope with the flood, bear the consequences of missed productivity and fraud. Spamming has been made illegal in a number of jurisdictions.

Cyber Stalking

Cyberstalking is the stalking or harassment of a person, a group of individuals, or an organisation via the Internet or other technological methods. False allegations, monitoring, threats, identity theft, data or equipment damage, the recruitment of children for sex, or gathering information to harass are all examples. "Stalking is a type of mental abuse in which the offender frequently, unwantedly, and disruptively enters into the life-world of the victim, with motivations that are directly or indirectly traceable to the affective domain," argues technology ethics professor Lambèr Royakkers.

Cyber Defamation

Cyber Defamation is a crime that takes place in cyberspace, generally through the Internet, with the aim of defaming people. A person's reputation is harmed through defamation. If a person damages another's reputation, he does so at his own risk, just as if he interferes with their property. A person's reputation is his property, and it is potentially more valuable than his other assets. Except for the use of a virtual medium, cyber defamation is similar to traditional defamation.
site-to-site scripting

Cross-site scripting (XSS)

Cross-site scripting (XSS) is a form of online application security vulnerability that allows malevolent web users to insert code into web pages being viewed by other users. HTML code and client-side scripts are two examples of this type of code. Attackers can bypass access restrictions by exploiting a cross-site scripting vulnerability.

Cyber Terrorism

The use of Internet-based assaults in terrorist operations includes acts of planned, large-scale disruption of computer networks, particularly personal computers connected to the Internet, using tools such as computer viruses. Any computer crime that targets computer networks without necessarily impacting real-world infrastructure, property, or life is referred to as cyber terrorism. Terrorist organisations and individuals utilise information technology to achieve their goals.. Hacking into computer systems, injecting viruses into susceptible networks, website defacing, denial-of-service assaults, and terroristic threats sent via electronic communication are all examples of cybercrime. Attacks against Internet businesses can be considered cyber terrorism, although they are usually classified as cybercrime when they are carried out for commercial reasons rather than ideological ones.

Cyber Pornography

Pornography that is spread via the Internet, typically through websites, file sharing, or Usenet newsgroups, is known as cyber pornography. While pornography has been traded over the Internet since the 1980s, the World Wide Web's creation in 1991, as well as the general public's access to the Internet around the same time, resulted in a surge in online pornography. The Internet, like videotapes and DVDs, has become popular for disseminating pornography because it allows individuals to see pornography in the comfort and privacy of their own homes. Pornography is frequently cited as one of the driving reasons behind the early growth of the Internet. Pornographic images were previously

communicated over the Internet as ASCII porn, but sending images over the network necessitated the use of computers with graphics capabilities as well as more network capacity. In the late 1980s and early 1990s, this was feasible thanks to anonymous FTP servers and Gopher. This tiny picture repository included some low-quality scanned pornographic photos that were originally made anonymously available to anybody. In the early 1990s, Usenet newsgroups also served as a means of exchanging photos over the limited bandwidth available. Images scanned from pornographic magazines were converted to ASCII text before being divided into parts and submitted to Usenet's Alt. Binaries hierarchy. These data may then be retrieved, reconstructed, and finally decoded back into pictures. Automated software like aub made it possible to download and assemble all of the photos from a newsgroup automatically. In the early 1990s, the number of posts increased rapidly, but image quality was limited by the amount of files that could be uploaded. This method of dissemination was usually free and offered a high level of secrecy. The anonymity made it safe and simple to circumvent copyright limitations while also safeguarding uploaders and downloaders' identities.

Vishing

Vishing is a criminal activity that involves utilising social engineering and Voice over IP (VoIP) to get private, personal, and financial information from the general public in exchange for a monetary incentive. The name is a hybrid of the words "voice" and "phishing." Vishing takes advantage of the public's confidence in landline telephone services, which have historically terminated in known-to-the-telephone-company physical locations connected with a bill-payer. The victim is frequently unaware that VoIP enables caller ID spoofing, low-cost, complicated automated systems, and bill-payer anonymity.. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Bot Networks

Bot Networks, a type of cybercrime in which spammers and other cybercriminals remotely take control of computers without the owners' knowledge, is on the rise at an alarming rate.
Users inadvertently download dangerous software such as Trojan horses provided as e-mail attachments, which connects their computers to Bot Networks. When the malicious code within these machines is triggered, the afflicted computers, known as zombies, can operate together, giving those behind Bot Networks attacks access to the processing capacity of thousands of systems. The trojan horse instals a backdoor on the machines that have been hacked. The 'backdoor' "is a means of circumventing traditional authentication or securing remote access to a computer while remaining concealed from casual inspection. The backdoor might be a software that is installed or a change to a legitimate programme.
Bot networks pose a unique set of challenges for businesses since they may be remotely updated with new flaws at any time." "As a result, attackers may be able to anticipate security measures.

Cyber Crime

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Hacking	12	25	20	35	45	39	75	87	123	145
Phishing	8	14	26	54	40	58	103	92	97	109
Spamming	4	17	19	29	43	67	86	94	89	105
Stalking	2	8	6	15	19	27	34	29	47	58
Defamation	3	11	9	13	17	24	32	37	59	46
Pornography	0	0	2	7	3	23	27	15	35	42

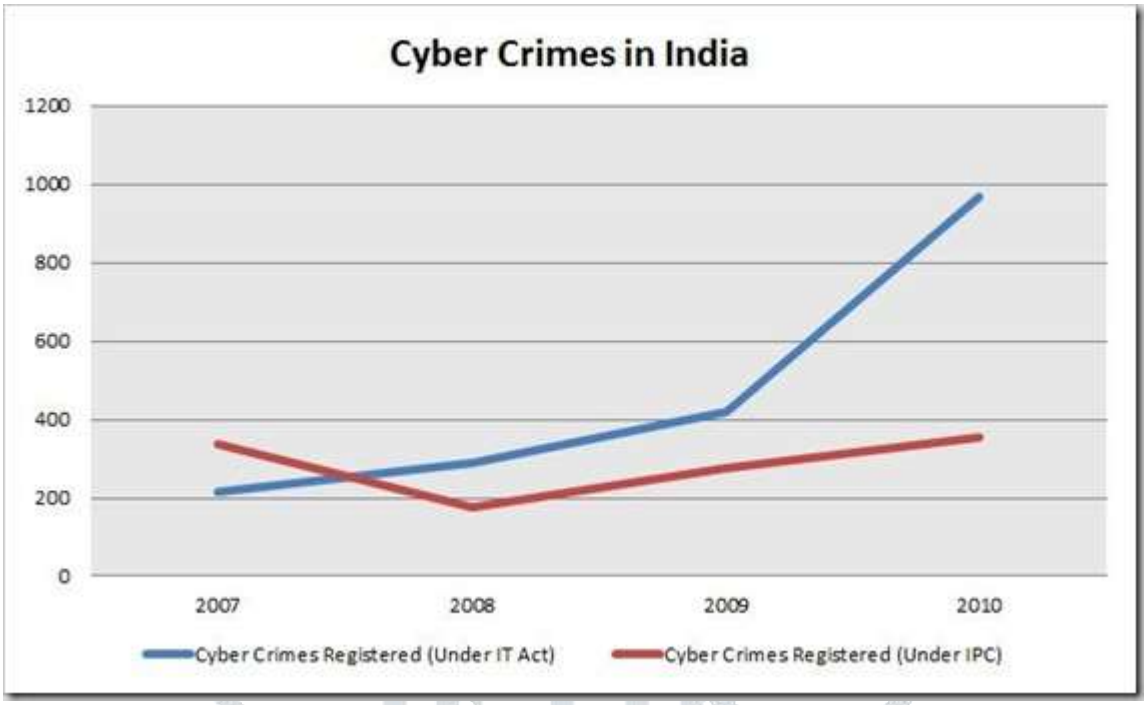
Source:CRBI Table 1

Source:CRBI Figure1

Graphical representation of Reported cases

Here we can see that all the variants of cybercrime are on the rise since 2001. In the early years, the growth rate of reported cases was not so high but after 2005 the growth rate of reported cases increased suddenly because of an increase in computer literacy and the spread of the internet.

Crime is no longer limited to space, time, or a group of people. Cyberspace creates moral, civil, and criminal wrongs. It has now given a new way to express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 1000 million people are hooked up to surf the net around the globe. According to the most recent data, cybercrime is on the rise. However, it is true that cybercrime is not often reported in India. As a result, there is a false sense of security in believing that cybercrime does not exist and that society is immune from it. This is not a true representation of the situation. People in our nation do not report cybercrime for a variety of reasons. Many people do not want to be harassed by the cops. There's also the worry of negative media coverage, which might harm their reputation and social standing. . According to a recent survey, just 50 out of every 500 cybercrime instances are reported to the police, and only one of those is recorded. These data demonstrate how difficult it is to persuade law enforcement to report a cybercrime. It was hoped that the formation of cybercrime units in various regions of the country would increase cybercrime reporting and prosecution. These cells, on the other hand, haven't exactly met expectations. People should not believe that cybercrime is going away, and they should be aware that with each passing day, cyberspace becomes a more hazardous environment to be in, where criminals walk free to carry out their illegal plans, aided by the internet's so-called anonymity. The country's extremely low percentage of cybercrime convictions hasn't benefited the cause of cybercrime regulation. We need to make sure that our system punishes cybercrime and cybercriminals harshly enough to serve as a deterrence to others. The Information Technology (IT) Act of 2008 defines the offences that are punished. Because the major goal of this Act is to establish a conducive environment for business I.T. use, some criminal omissions and commissions while using computers have been excluded.



The government is aware of anti-social groups and criminals abusing the Internet and email. During the examination of some terror cases, the National Investigation Agency discovered that terrorists were utilising the Internet and communicating via email to carry out their acts of terror.

The Internet has evolved into a platform for people to exchange ideas, activities, and events, as well as express their thoughts and opinions on certain topics and events. Several organisations and individuals have placed material on the Internet for a variety of reasons, which may be enjoyed by one segment of the population and profitably utilised by another. Users from various walks of life can access such sites. The Internet is used by millions of people from all walks of life across the world. Users can automatically upload material of their choosing after registering with such sites, without the involvement of service providers who host such sites, thanks to the technology and accompanying apps. Because of the enormous number of people that log on to these sites and the millions of pages they contain, it is nearly impossible to keep track of everything that is uploaded or published on them. The majority of the websites are hosted outside of the United States. Furthermore, the content of such websites stored on the Internet is not regulated by the government.

In 2008, 2009, 2010, and 2011, the Indian Computer Emergency Response Team (CERT-In) reported and tracked a total of 90, 119, 252, and 219 government websites that were hacked by various hacker organisations.

Under Section 79 of the Information Technology Act of 2000, the government has published the Intermediary Guidelines Rules, 2011. The intermediaries are required to follow these guidelines in order to self-regulate. Any individual who has been harmed by the abuse of social networking sites can contact the intermediary that hosts these sites and request that erroneous information or objectionable content be removed or disabled. The intermediaries must also appoint a grievance officer to deal with the impacted person's requests.

The Information Technology Act of 2000 was revised on October 27, 2009, by the Information Technology (Amendment) Act of 2008. The revised Act is comprehensive, and it establishes a legal foundation for combating all types of common cybercrime. For different crimes of cybercrime, harsh penalties have been enacted, ranging from three years in jail to life in prison and a fine.

CONCLUSION

The current article examines the cybercrime situation in India. We are attempting to usher in a new age by inventing cutting-edge technology, yet the same technology is being misused. Cybercrime has been

discovered to be on the rise and has an impact on human civilization. Although cybercrime units have been established in major cities, most incidents get unreported owing to a lack of knowledge. Because there is such a high risk of harm to our national security, our cyber intelligence services must prepare for these attacks. Cybercrime is more deadly than traditional crime since it is an unseen crime that is far more damaging than the apparent one. By sensitising and raising awareness among internet users, we can help to avoid cybercrime.

References

1." Phishing". Language Log, September 22, 2004. Retrieved August 9, 2006.

2. Gonsalves, Antone (April 25, 2006). "Phishers Snare Victims With VoIP". Techweb.

3."Identity thieves take advantage of VoIP". Silicon.com.March 21, 2005.

4. The Spamhaus Project - The Definition Of Spam.

5. Royakkers 2000:7, cited in CyberStalking: menaced on the internet.

6. http://delhicourts.nic.in/CYBER%20LAW.pdf

7. Nasik Police play big boss for internet voyeurs, Hindustan Times, Sunday, Oct 28, 2007
.
8. Losses due to cybercrime can be as high as $40 billion, The Hindu Business line dated May 21 2007downloaded 20 Oct2007

9. Kolkata man threatens to blow up Stock exchanges arrested. Express India.com Sun 28 Oct 2007

10. Mutton, Paul. "Fraudsters seek to make phishing sites undetectable by content filters".Netcraft.

11.http://news.netcraft.com/archives/2005/05/12/fraudsters_seek_to_make_phishing_sites_undetectable_by_content_filters.html.

11. Peter Likarish, Don Dunbar, Juan Pablo Hourcade, Eunjin Jung, BayeShield: Conversational Anti-phishing User Interface, Symposium On Usable Privacy and Security (SOUPS) 2009, ACM.

12. Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth

13. Cyber Crimes on the rise in the state - Kerala: The Hindu Monday, Oct 30, 2006

14. Nowa Pune base for net's cybercops The Hindu Sunday, Nov 26, 2006

15. Bank Customers face Phishing, The Hindu, Coimbatore, Monday, August 20 2007,