International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

The History, Evolution and the Present Scenario of Cyber Crime in India

Anjali Saraswat

Introduction

Cybercrimes or digitalized crimes can be considered as the crimes that are committed using electronic devices namely smart phones or interconnected computers. A cybercrime may be committed for a number of reasons, including retaliation, fraud, or even sexual exploitation. As time goes on, India is seeing an exponential rise in the number of cybercrime cases. This amount is in direct relation to the daily growth in the number of subscribers. In 2020, the Ministry of Home Affairs reported 51,000 or so cases of cybercrime. Current era is too fast to utilize the time factor to improve the performance factor. It is possible only through the use of the Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the Internet. Everyone appreciates the use of the Internet; but there is also a negative aspect to it: criminality committed online. Cybercrime is defined as an act that is committed or omitted in violation of a law that forbids or commands it and that carries a sentence upon conviction. Cybercrime is any criminal behavior that involves the use of computers, including unauthorized access to another person's computer system or database, data alteration or theft, and sabotage of hardware and data. Cyberspace, often known as the Internet, is expanding quickly, which has led to an increase in cybercrimes

What is Cyber-Crime?

"Offences that are committed against individuals or groups of individuals with. a criminal motive to intentionally harm the reputation of the victim or cause."

-Debarati Halder & Dr. K. Jaishankar

Cybercrime, which includes everything from electronic theft to denial-of-service attacks, is a broad term used to describe criminal activities in which computers or computer networks are a tool, a target, or a location. It's a catch-all phrase for crimes like phishing, credit card fraud, bank robbery, illegal downloading, industrial espionage, child porn, kidnapping minors through chat rooms, scams, cyber terrorism, production and/or distribution of viruses, spam, and more. Nowadays, everyone has a social media account, and they frequently post updates about their daily activities as well as personal details like their addresses. It is easy for criminals to hurt that individual by kidnapping them because they now know whereabouts of that person thanks to the personal information that a social media account holder posts on his account. Hacking is another cybercrime that is fairly common. It has now become so common that even the highly secured websites of government bodies get hacked, let alone the social media accounts of common people. The most common method of hacking is that the hacker usually sends some links to the email or any social account of the victim and the moment the user clicks open that link, the hacker gets access to the computer system of that user. We can also witness such cases where we get spam messages in our e-mails reading that we have won some amount of prize money and in return they ask us about our bank details. This is where many people fall into the trap, even the educated ones. The term 'cyber-crime' is used to refer to "any crime that is facilitated or committed using a computer, network or hardware device". Information and communication technologies such as networked computers provide cheap, fast, secure, anonymous communication with multimedia capacity. They may be used as a means of

communication and organization to support existing criminal activities, to provide new ways of conducting criminal activities, to extend the geographic reach of criminal activities or to create new types of criminal activity

History of Cyber crime:

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future. The internet was viewed by the 1990s as a special medium with the quickest speed in human history and a growing dependency on technology.

The first polymorphic virus was released in 1992, the same year as the first cybercrime. One of the earliest cybercrime cases in India was Yahoo v. Akash Arora.

Evolution of Cyber Crime :

The first instance of a cybercrime development occurred in the late 1980s, coinciding with the explosive growth in email usage. When an email began to circulate worldwide in households, a plethora of scams hit the scene. The email was disguised as a genuine request from a Nigerian Prince who asks for financial help so that he can help get millions of people out of Nigeria with a promise that he would return millions of dollars to the email recipient.

In the late 1980s, a cyber form named "**Morris Worm**" attacked nearly (within 24 hours) 6000 of the 60000 computers that were connected to the internet back then. The cyber worm caused a slowdown in the computers. The cyber worm infiltrated the computer systems at many colleges and universities including Harvard, Princeton, Stanford, Johns Hopkins, NASA, and the Lawrence Livermore National laboratory.

When cybercrime start, Cybercrime's history and the evolution of cybercrime did is easy to trace and coincide with the evolution of the Internet itself. The first offenses were, of course, essential hacks from local networks to steak records, but when the Internet became more developed, so did the attacks.

- Although there had been some cybercrime before to that in the late 1980s, the growth of email coincided with the first significant spike in cybercrime.
- It has made it easy to send a host of scams and/or viruses to your inbox.
- With improvements in online browsers, the second phase of the history of cybercrime emerged in the 1990s. There were many users to pick from at the time, many more than now, and most were vulnerable to viruses. Any time dubious websites were accessed, viruses were distributed via Internet connections.
- As social media started to take off in the early 2000s, cybercrime began to accelerate. The influx of people dumping all the information they could into a profile folder led to an influx of personal information and the emergence of ID fraud. The data was utilized by thieves to open bank accounts, create credit cards, and commit other types of financial theft.
- The new wave is the emergence of an annual multinational crime enterprise totaling almost half a trillion dollars. These criminals operate in groups, employ tried-and-true strategies, and prey on anyone with an online presence.

Indian cybercrime situation

Since 2018, the number of cybercrime cases has steadily increased. In 2018, India reported 2,08,456 incidents; in 2019, 3,94,499 incidents; in 2020, 11,58,208 instances; in 2021, 14,02,809 cases; and in 2022's first two months, 2,12,485 incidents.

New Delhi: Earlier this year, certain media reports created a flutter when they claimed that personal data of over 20,000 people were leaked from a government server and put on sale. The data apparently included details such as name, age, address, mobile number and Coved test result.
Similar data breaches have been disclosed from numerous different institutions since last year, including a well-known airline, a popular pizza restaurant, a digital payment platform, and others. This may be a key factor in the Centre's heightened focus on cyber security.

Fraud-Biggest motive of cyber crime

The National Crime Records Bureau (NCRB), however, presents a different set of data. According to NCRB, India reported 50,035 cyber crimes in 2020; 44,546 cases in 2019 and 27,248 cases in 2018.
The year 2020 saw 4,047 cases of online banking fraud; 2,160 cases of ATM fraud; 1,194 credit/debit card fraud and 1,093 OTP frauds. According to NCRB data, there were also 578 instances of fake news on social media and 972 occurrences of cyber bullying and stalking of women and children.
Fraud was determined to be the primary motivation, accounting for 30,142 of the 50,035 cases (60.02 per cent). Following these were extortion (4.9%) and sexual exploitation (6.6%).
Karnataka has the highest rate of cybercrime (16.2%), followed by Telangana (13.4%) and Assam (10.1 per cent).
Government employee training and widespread information security awareness creation

Following table presents the total number of cyber incidents from 2018 to Feb 2022 in India

Year	Total cyber incidents
2018	2,08,456
2019	3,94,499
2020	11,58,208
2021	14,02,809
2022(till Feb)	2,12,485

Cases

i. The Bank NSP Case

In this instance, a bank management trainee became engaged to be married. Using the company's computers, the pair used to send and receive a lot of emails. After some time, they separated, and the young woman sent emails to the boy's international clients using fictitious email addresses like "Indian bar associations.

"She used the banks computer to do this. The boy‘s company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank‘s system.

ii. Bazee.com case

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The CEO was later released on bail after the Mumbai Police and Delhi Police intervened.

iii. Andhra Pradesh Tax Case

The proprietor of the plastics company in Andhra Pradesh was detained, and the Vigilance Department found cash valued at Rs. 22 in his home. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. The fact that the suspect was operating five firms under the guise of a single organization and falsifying sales records with electronic vouchers in order to avoid paying taxes was disguised. Therefore, when department officials got their hands on the computers used by the accused person, the questionable methods of the state businessman were made clear.

iv. Sony.Sambandh.Com Case

First cybercrime conviction in India. In this instance, Sony India Private Limited, which operates the NRI-targeting website www.sony-sambandh.com, filed a complaint. After making an online purchase, the service enables NRIs to mail Sony products to their friends and relatives in India. The company undertakes to deliver the products to the involved recipients. In May 2002, somebody logged onto the web site underneath the identity of Barbara Campa and ordered a Sony color television set and a cordless head phone. She requested to deliver the product to Arif Azim in Noida and gave the number of her credit card for payment. India had its first conviction for cybercrime. This is the situation where Sony India Private Limited, which operates the website www.sony-sambandh.com that targets NRIs, filed a complaint. NRIs can purchase Sony products on the website and then mail them to friends and family in India after making an online payment.

When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The business had complained to the CBI about internet cheating, and the CBI had filed a case in accordance with Sections 418, 419, and 420 of the IPC (Indian Penal Code). Following an investigation, Arif Azim was taken into custody.

Investigations discovered that Arif Azim, whereas acting at a call centre in Noida did gain access to the number of the credit card of an American national which he misused on the company’s site. The

color television and cordless phone were retrieved by the CBI. Because the CBI had evidence to support its claims in this case, the accused confessed to being guilty. Arif Azim had been found guilty by the court under Sections 418, 419, and 420 of the IPC; this was the first instance in which a cybercrime conviction had been made. The court, felt that since the defendant was a boy of 24 years and a first time convict, a compassionate view needed to be taken. Thus, the court discharged the defendant on the probation for one year.

Recent Cyber Attack

i. **Proxy Logon Cyber attack -** One of the most harmful recent cyber attacks involved the infiltration of a Microsoft Exchange server, which led to many zero-day vulnerabilities. Microsoft discovered the Proxy Logon vulnerabilities in January and patched them in March. These flaws were first introduced by the Hafnium hacker organization. However, more groups joined Hafnium in attacking unpatched systems, resulting in thousands of organizations being compromised**.**

ii. **Tether Attack** - Cybercriminals threatened to expose Tether crypto currency documents in March 2021. The attackers wanted a settlement price of about 500 Bit coins ($24 million), claiming the information would "damage the Bit coin ecosystem," but Tether refused to comply.

iii. **Face book Cyber attack -** Data of more than 530 million Face book users, including their names, Face book IDs, dates of birth, and relationship status, was published online in April 2021. Face book, now Meta, said that the data was collected in 2019 by scraping.

iv. **Colonial Pipeline Attack -** The Colonial Pipeline attack in May 2021 brought attention to the growing threat that sophisticated cyber security attacks represent to the world. The fuel pipeline operator suffered a ransom ware attack launched by the Dark Side hacking group, which led to fuel disruption and mass panic buying across the U.S.

v. **Omiai Cyber attack** - A cyber attack with illegal entry in May 2021 exposed the personal information of 1.7 million users of the Japanese dating app Omiai.

vi. **T-Mobile Attack** - In August 2021, telecoms firm T-Mobile suffered a cyber security breach that led to the data of around 50 million existing customers and prospects being stolen. An individual aged 21 stole the information, which included customer addresses, license numbers, and social security numbers. He claimed to have taken almost 106GB of data.

vii. **AP-HP Attack** - The number of cyber security assaults on healthcare companies and medical institutions is also rising. Cybercriminals obtained the personal information of almost 1.4 million persons who underwent COVID-19 testing in 2020 as a result of the hack on the AP-HP system of public hospitals in Paris in September 2021.

viii. **Debt-IN Consultants Cyber attack -** A South African debt recovery company suffered a significant attack that led to client and employee data being illegally accessed from its servers in September 2021. The incident is suspected to have affected the personally identifiable information (PII) including owed debts, of over 1.4 million people.

ix. **Argentinean Government Attack -** A hacker, who claimed to have leaked the entire database of Argentina's National Registry of Persons, has allegedly stolen the data of more than 45 million Argentinean residents. However, the government denied the hack.

x. **Squid Game Cyber attack** - The value of a crypto currency linked to but not officially associate with the Netflix program Squid Game plummeted after a suspected exit scam in November 2021. The crypto currency's value dropped from $2,850 to $0.003028 overnight, which resulted in investors losing millions of dollars.

xi. **Bit Mart cyber attack** - Bit Mart experienced a breach in December 2021 that allowed cybercriminals to steal about $150 million worth of crypto currencies, becoming yet another cyber security attack against digital currencies. Around $200 million in total losses and damages were brought on by the attack.

xii. **WHO Attack-**As the COVID-19 pandemic broke, an attack targeting the World Health Organization (WHO) resulted in the breach of 25,000 email addresses and passwords. The data was leaked online on April 19, 2020, along with information belonging to other groups fighting the pandemic, including the Gates Foundation, the National Institutes of Health (NIH), and the U.S. Centers for Disease Control and Prevention (CDC)

Conclusion

Nobody could dispute the numerous ways in which the Internet has altered our culture, society, and way of life over the past 20 years. In fact, the entire phenomenon is still so young that we have not yet figured out exactly how it affects us and how it will continue to affect us in the future. We cannot say for certain, what new advances the internet will give us, what new art forms, social classes, or subcultures it will engender. So also we cannot predict all the dangers which it introduces. Cyber-crime is also necessarily very new. As soon as there was an internet, there were criminals operating to exploit it, with all new technology. We must do our best to keep one step ahead of cybercrime, in order to protect ourselves. At the very least, we cannot afford to fall too far behind.

References

(Dr.M.Ramasubramani)
https://www.rajalakshmi.org/ijgbmr/downloads/IJGBMRMar15-Paper10.pdf
(fortinet)
https://www.fortinet.com
(ipleaders)
https://blog.ipleaders.in/changes-and-developments-in-crimes-in-cyber-world-since-indian-independence/
https://www.legalserviceindia.com/legal/article-8311
https://www.legalserviceindia.com/legal/article-8382-the-evolution-of-cyber
https://zeenews.india.com/technology/two-months-of-2022