Review Article

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Engineering Survey

2020
Vol. 8 No.3:14

Research on Cybercrime and its Policing

Dhaval Chudasama*, Darsh Patel, Abhishek Shah and Nihal Shaikh

Computer Science Department, Indrashil University, Mehsana, Gujarat, India

*Corresponding author: Dhaval Chudasama, Computer Science Department, Indrashil University, Mehsana, Gujarat, India, E-mail: Dhaval.chudasama@indrshiluniversity.edu.in

Citation: Chudasama D, Patel D, Shah A, Shaikh N (2020) Research on Cybercrime and its Policing. Am J Comput Sci Eng Surv Vol. 8 No. 3: 14.

Abstract

Being one among the foremost rapidly expanding sector, internet has become one among the most vital part of our life from work to entertainment there is no other way now but it comes with a price of our privacy and data. Cyber Crime in India has been rapidly evolving since the beginning of the technological era. Cybercrime are often defined as a criminal offense or an unlawful act where the pc is employed either as a tool, a target or both. Cyber-attacks have already caused considerable damage and amount to detail-retail banking, mainly through MasterCard and payment scams. Cybercrimes are affected by way of illegal access into another data base, illegal interception, data interference, and system interference, misuse of devices, forgery and electronic scams.

Keywords: Cybercrime; Cybercrime and policy

Received: November 09, 2020; **Accepted:** November 23, 2020; **Published:** November 30, 2020

Introduction

"Neither the internet nor Cyberspace will ever be a secure haven for people that attempt this type of cyber-crime. The Secret Service in conjunction with our enforcement partners, will hunt you down, keystroke to keystroke."

– Brian Marr

Now a day's people cannot live without internet, smartphones or the modern technologies and due to this cybercrime has grown substantially. Hackers develop methods which can breach into the devices through vulnerabilities and take advantage of this by stealing the data to use it for their own benefits. There are multiple ways by which people are getting scammed and lose their money or sensitive data and this causes serious harm in India and around the world.

It was noted that in India, the IT act isn't intrusive, but Internet service providers (ISPs) are statutorily sure to provide adjacent space for intelligence agencies. Canada, the UK, and Germany were introduced laws that might restrict the liberty of the web. The question of the adequacy of technical methods to police the web was raised, and whether a particular level of compulsion is often introduced, since companies were most reluctant to move in this direction. The 2014 National Crime Records Bureau (NCRB) Statistics Report registered an entire of 9,322 cyber-crime related acts in 29 states and 300 such cases even in Union Territories (UTs). These digits mark a 69.2 surge in States and 62.2 % increase in seven UTs from the previous year. The bulk of the cases have been registered under the IT Act, (Indian Penal Code) IPC and Special and Local Laws (SLL).

Making the online safer and secure (and protecting Internet users) has become integral to the event of latest services also as governmental policy. The battle against cybercrime needs a comprehensive, secure and a safer approach. Given that technical measures alone cannot prevent any crime, it is important that enforcement agencies are allowed to research and prosecute cybercrime effectively [1].

Cyber crime

Cybercrime is criminal activity that either targets or uses a computer, a network or a networked device which can be hacked. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Few of the cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers [2].

Rarely, cybercrime aims to wreck computers for reasons aside from profit. These could be political or personal. It looks legitimate-but with one click on a link, or one download of an attachment, one wrong message, most are locked out of your network. That link downloaded or opened software that holds your data of the hostage. That's a ransom ware attack. The attackers invite money or crypto currency, but albeit you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the knowledge you would like to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransom ware can take a serious toll on your business. As day by day technology is playing in major role during a person's life the cybercrimes also will increase alongside the technological advances.

Rate of cybercrime cases recorded (per 1 lakh population) in 2018 by states/UTs is shown in **Figure 1** where Karnataka has the highest cyber-crime rate [3].

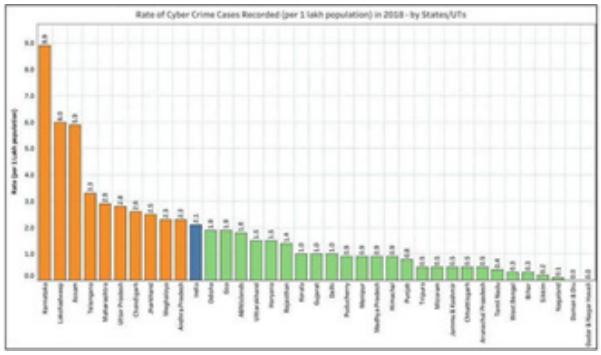

Figure 1: Rate of cybercrime cases recorded (per 1 lakh population) in 2018 by states/UTs.

Techniques cybercriminals use

Internet Fraudsters are everywhere and that they come up with innovative tricks to cheat people and wipe out money from their checking account. There are many techniques which hackers use for committing crime but here we will discuss the most common ways they use.

Phishing or email scam: It is a way employed by fraudsters to steal your personal information. Under this fraud, fraudsters send you send you emails by posting as a genuine or reputed company. The primary intention of sending those emails is to steal your bank details. These emails are to steal your bank details. These emails will usually have a link or attachment. If you click on those links, you'll be taken to a fake website. The fake website will ask you to supply your sensitive information like card details, UPI code and other bank details. Also, clicking on such links will cause an epidemic attack on your computer.

Lottery fraud: Lottery fraud is one of the highest three internet frauds in India. Under lottery fraud, fraudsters call you or send emails and messages stating you have won lottery money, you will be asked to transfer money online in the name of tax. Sometimes you'll be asked to pay money by visiting fake websites. When you attempt to make payment using those websites, all of your card details are going to be stolen.

Identity theft: Under fraud, your personal information is stolen by fraudsters through the web and wont to apply for a private loan, two-wheeler loan or a MasterCard with a bank. When loans are availed in your name, you'll be liable for its repayment. Banks will send you the notice for repayment. If the loan isn't repaid it'll have a nasty impact on your credit score and you'll be marked a loan defaulter [4].

Also, the stolen information of yours is often wont to create fake social media accounts.

Social media scam: with the number of people using social media, social media scams are on the rise. Cyberbullying is one among the most important social media fraud to which many teenagers have fallen prey. Under cyberbullying social media sites are wont to bully people. Also, there are many other social media frauds sort of a Facebook friend fraud.

Online shopping frauds: It is one among the most important internet frauds since the past few years. Under this, fraudsters found out fake online shopping portals with the intention of cheating innocent people of their hard-earned money. In the website, they display attractive product at a really cheap rate. But, after the acquisition is formed by paying the cash, either the fake product is delivered or the merchandise isn't delivered in the least. These websites won't have any return or refund policies and also there'll be no customer support team to contact.

The role of police in fighting cybercrime

It is very hard for police units to start out investigations due to the low visibility of such crimes and therefore the lack of reporting that could happen due to different reasons: from the unwillingness of commercial entities, especially financial companies to report to the police on account of reputational questions and negative publicity to the lack of knowledge that such a criminal activity could be reported or lack of trust in the police department (CSI and FBI, 2004, 19; Wall, 2007, 193). Because of the low reporting rate, lack of resources and under-reporting law-enforcement agencies haven't any possibility to research and prosecute quite a 'tiny fraction' (Vogel, 2007) of what is happening in cyberspace.

Moreover, it is very hard for police units to justify the impact on public interest of initiating an investigation, especially in the case of a low impact, single crime with the one victim (Wall, 2007, p. 191). Since use of internet and ICT technologies provides offenders with the chance to make aggregated revenue with low impact on one victim (e.g. stealing 1 euro millions of times rather than millions of euros only once), one of the most important challenges for the police is the justification of a public order breach and the initiation of investigatory procedures.

Taking into consideration the demand for new skills to investigate crimes in cyberspace, the necessity to review policing concepts, such as the justification of a breach of public order, the applicability of techniques in policing the important world to the upkeep of order in virtual space, implementation of those instruments during a practical environment remains the very best priority. And for this in Karnataka two stages training program on how to deal with hacking, online harassment, credit/debit card fraud, data theft etc., for ranks till the level of constable. Though training Personnel remains the challenge when it comes to dealing with the digital crime.

A number of police agencies have formed partnerships with computing departments at local universities. These partnerships not only provide an opportunity to expertise the police, but also function as a recruiting tool for college kids who have an interest

in cybercrime and policing. A knowledge hub thus are often established which may also attract students to pursue a career as cyber investigators. Also, for enforcement agencies at the national, state, and native level, there should be a central referral mechanism for complaints involving cybercrime. In many cases, private corporations and special branches have more experience with cybercrime investigations than local police agencies and henceforth, the Police can seek cooperation with private corporations without compromising the security [5].

How 'We' as a citizen can prevent cybercrime

Cybercrime is not just Governments responsibility, we as a citizen should also have to stay aware and try to defend ourselves from cybercriminals. And we can achieve that by following some simple steps:

- **Use strong passwords:** Use the various password and username combinations for various accounts and resist the temptation to write down them down [6].
- **Keep your social media accounts private:** Make certain that you simply keep your social networking profiles (Facebook, Twitter, YouTube, etc.) private. Be sure to check your security settings. Be careful of what information you post online. Once it's on the web it's there forever [6].
- **Secure your mobile devices:** Many of us aren't aware that their mobile devices also are susceptible to malicious software, like computer viruses and hackers [6].
- **Protect your data:** Protect your data by using encryption for your most sensitive files such financial records, and tax returns [6].
- **Protect your identity online:** When it involves protecting your identity online it's better to be too cautious than not cautious enough. It is critical that you simply take care when giving out personal ID like your name, address, telephone number and/or financial information on the web [6].

To report cybercrime in India, the first step is to file a complaint at the cybercrime cell in a police station of the city where the crime has taken place, or where the device is located which was affected or attacked by cyber criminals. You can go to the police station of your state or send a mail to the Police as they will forward your complaint to the Cyber Cell or you can directly mail the complaint to cyber cell.

Innovations in cyber security

As technology is advancing rapidly, the IT sector and computer security are getting more fragile and susceptible to risks and threats. Going much beyond their regular activities, the attackers are innovating and advancing their approach to steal much complex data and knowledge. Right from credentials to misconfiguring cloud data, cyber security attacks are making life tough for people within the IT sector. [4] There are few innovations which can be helpful in cyber security sector which are:

Biometric scanning: Payments can be made more secure by using biometric scanning. Biometric scanning can be a good way in opening a new dimension for securing our data. There are multiple biometric scanners available, for instance IRIS scanner, fingerprint scanner and face recognition which can be helpful because currently we use PIN and Mobile Numbers for money transactions and security. This convectional way can be breached easily and so we can use such biometric scanners to make digital signatures which can be unique and cannot be replicate easily and so our privacy will increase, thus resulting in prevention of cybercrime.

Government payment portals: Generally, payments are done using third party applications which attackers use as their advantage by manipulating people to transfer money to them and are scammed easily. Although there are many government portals for money transactions people usually use easier ways, and so if government takeovers these third party applications by keeping records and also by monitoring the transactions which can lead to more transparency and will ultimately result in less crime.

Using AI (Artificial Intelligence) for the identifying threats: AI can be a very powerful defender from the cyber criminals as it can detect the problem in the vulnerability by analyzing its every aspect millions of time within seconds. AI can help checking emails before a person clicks on it by check its link on a fake server and if it a scam emails it can directly go to the spam folder without the user even knowing it. Similarly, an AI can scan the loopholes and identify all the vulnerabilities and if someone tries to attack that vulnerability it can automatically block it before the attacker can breach it.

Conclusion

Computer security may be a vast topic that's becoming more important because the planet is becoming highly interconnected, with networks getting used to hold out critical transactions. It is a well-known incontrovertible fact that terrorists are using the web to speak, extort, intimidate, raise funds and coordinate operations. The degree of our preparedness within the face of these potential threats does leave much to be desired. The Government should also note of this slow but worrying development and put in situ a correct mechanism to curb the misuse.

References

1. Biden JE (2011) Cybercrimes. SSRN Electron J: 1-14.
2. Tips on how to protect yourself against cybercrime. Kaspersky.co.in, 2018.
3. Kancharla B (2020) Almost 45% of the cyber-crimes reported in 2018 are from UP & Karnataka. Factly.in, 2020.
4. Advanced cyber security innovations and updates for 2020. Technology Trends-medium.com, 2019.
5. What is cybercrime and how can you prevent it? avast.com, 2019.
6. Shalini S (2019) How to prevent cybercrime in India? myadvo.in, 2019.