

CYBER CRIME AND THEIR IMPACTS IN VARIOUS ASPECTS

Ashima Gambhir

Assistant Professor, Amity University Haryana, India

ashima.ashugambhir@gmail.com

Abstract: In the current period of online processing system, maximum number of the people are using internet banking for paying bills, sharing information and online payments etc. Even it makes the life so fast and speedy but this facility of computer technology has not come without drawbacks. Now a days maximum information is online and prone to cyber threats. There are a large number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber crime can involve bonnets, computer viruses, cyber harassment, cyber stalking, cyber violence, cyber pornography, Denial of Service attacks, hacktivism, identity theft, malware, and spam. In This Paper, we will discuss about the understanding of cyber crimes and their impacts on various sectors like Society, Socio-Eco-Political Riders, private industries, teenagers, consumer behavior and business.

Keywords: Cyber Crime, Security, Socio-Eco-Political Riders, DoS.

I INTRODUCTION

Cybercrime refers to any crime that involves a computer, network or any public or private systems. Cyber Crime is only possible due to the internet connection. The internet term can be defined as collection of large number of computer systems that give a connection between the computers. The uses of the internet has both advantages and disadvantages, the most disadvantage of using the internet is cyber crime. Cyber Crime is the most convoluted problem for the cyber world now days[7]. Cyber Crime and Computer Crime both are different things because cyber crime is basically associated with internet and networks, whereas computer crime may or may not involve networks. Most of the Cybercrime issues are related with the problems like security of economic dealings, prohibiting mistreatment of credit/debit card information, providing security for information during online dealings, preserving privacy and secrecy of e-mails and the attack on privacy. The one more major issue which is continuously increasing is the matter of specific companies who are handling billing for the adult website industry. Those companies are progressively more the targets of cyber crooks looking to access credit card details and attack on cash.

II DIFFERENT TYPES OF CYBER CRIME

There are different types of the cyber crime which will give us the comprehensive ideas of the loopholes in the networks and security systems, which can be demoralized by the attackers. Therefore we need to know about the different ways of cyber crime in which our computer can be compromised and our privacy infringed. Figure 1 shows the different kind of the cyber crime.

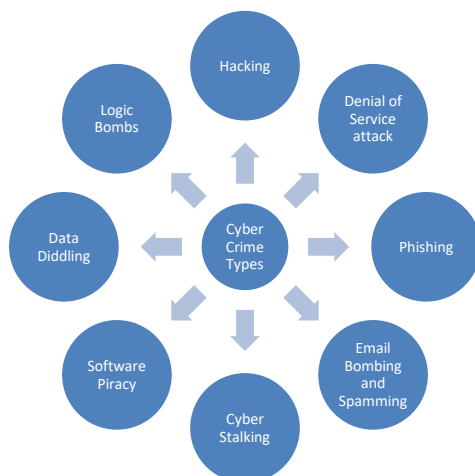


Figure 1 Types of Cyber Crime

1. **Hacking:** Hacking is the most dangerous or serious threat to the e commerce and internet now a days. Hacking refers to an act committed by an interloper by stealing the valuable information (data) from our computer without our permission. Hacking is done by hackers now the question arises who are hackers; hackers are in between client & server and able to take-off the data/information, Duplication the IP address illegally.
2. **Denial of Service attack:** Denial of service attack(DoS) is a type of attack purpose is to make resources or service unavailable is to the projected users. Denial of service attack is also known as the Distributed Denial of service (DDoS) in which number of geologically prevalent perpetrators flood the network traffic. DoS attack basically targets the high profile web site servers related to banks and credit/debit card payment gateways.
3. **Phishing:** Phishing is a technique of extracting the private/confidential information like user name, password and credit card numbers by camouflaged as a legal scheme[8]. This type of attack is usually carried out by email spoofing and instant messaging. In this type of crime hackers make a direct link which directs to the fake page /website which looks and feel like identical to the legitimate one. Figure 2 explains the how phishing can net some really interesting catches.

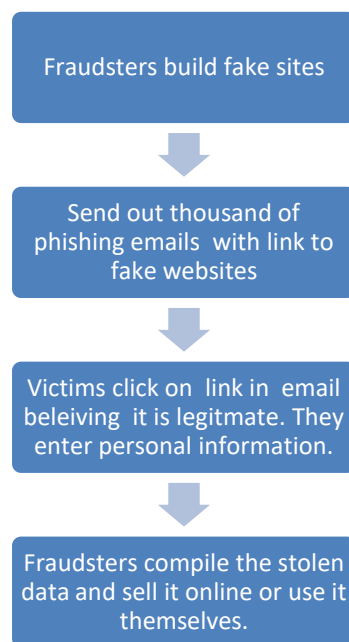


Figure 2 Process of Phishing attack

4. **Email Bombing and Spamming:** Email Bombing is a serious fault in which a person sends a numbers of emails to the inbox of the target system/person. Mail bombs will usually fill the allotted space on an e-mail server for the users e-mail and can result in crashing the e-mail server. Spamming is also a variant of Email Bombing.
5. **Cyber Stalking:** Cyber Stalking ia another main type of cyber crime. Stalkers will repeatedly annoy another online users with bullying messages and emails. Most victims of this type of crime are women and children who are stalked by men. Cyber Stalkers flourish on innocent web users who are not well aware of the rules of internet safety and web security.
6. **Software Piracy:** Software Piracy is the distribution and unauthorised user of computer software. Software piracy is the major issue in the world where major applications are routinely copied by the thousands for resale. Figure 3 explains the methods by which illegal copies of software circulate among computer users..



Figure 3 Types of Software Piracy

7. **Data Diddling:** Data diddling is the unconstitutional changing of data before or during entry into computer systems. In this type, the attacker may modify/update the expected output using the data diddling technique. In India, Electricity boards have been sufferers of data diddling by computer criminals.
8. **Logic Bombs:** Logic Bomb also known as the “Slag code”. Logic Bomb is an event driver attack. This type of attack activates only if certain event occurs. Logic Bombs are embedded in some legitimate program by software developers and explode or performs malicious activities when certain conditions are met or certain event occurs[12]. Logic bomb is not a virus even if it usually behaves in similar manners. This type of attack is very difficult to detect.

III CATEGORIES OF CYBER CRIME

In general, Cyber Crime mainly categories into the three different types as follows.

1. **Data Crime:** Data Crime is classified into the Data Interception, Data Modification and Data Theft.
- a. **Data Interception:** An aggressor screens information streams to or from an objective with a specific end goal to accumulate data. This assault might be attempted to assemble data to help a later assault or the information gathered might be the ultimate objective of the assault. This assault normally includes sniffing system movement, yet may incorporate watching different sorts of information streams, for example, radio[6]. In many assortments of this assault, the aggressor is uninvolved and basically watches general correspondence, however in a few variations the assailant may endeavour to start the foundation of an information stream or impact the idea of the information transmitted. Be that as it may, in all variations of this assault, and recognizing this assault from other information accumulation strategies, the assailant isn't the expected beneficiary of the information stream. Dissimilar to some other information spillage assaults, the assailant is watching express information channels (e.g. arrange movement) and perusing the substance. This varies from assaults that gather more subjective data, for example, correspondence volume, not expressly imparted through an information stream.
- b. **Data Modification:** Security of interchanges is fundamental to guarantee that information can't be changed or seen in travel. Appropriated situations carry with them the likelihood that a vindictive outsider can execute a PC wrongdoing by messing with information as it moves between destinations. In an information alteration assault, an unapproved party on the system blocks information in travel and changes parts of that information before retransmitting it. A case of this is changing the dollar measure of a keeping money exchange from \$100 to \$10,000. In a replay assault, a whole arrangement of legitimate information is over and again interposed onto the system. An illustration is rehash, one thousand times, a legitimate \$100 financial balance exchange.
- c. **Data Theft:** Term used to portray when data is wrongfully replicated or taken from a business or other person. Ordinarily, this data is client data, for example, passwords, standardized savings numbers, charge card data, other individual data, or other private corporate data. Since this data is unlawfully gotten, when the person who stole this data is secured, it is likely he or she will be indicted without bounds degree of the law.

2. **Access Crime:** Access Crime is mainly classified into the unauthorised access and Virus Dissemination.
 - a. **Unauthorised Access:** "Unauthorised Access" is an insider's perspective of the PC saltine underground. The recording occurred the whole way across the United States, Holland and Germany. "Unapproved Access" takes a gander at the identities behind the PCs screens and intends to isolate the media buildup of the 'fugitive programmer' from the truth[10].
 - b. **Virus Dissemination:** Malignant programming that appends itself to other programming. (infection, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are cases of malevolent programming that devastates the arrangement of the victim.

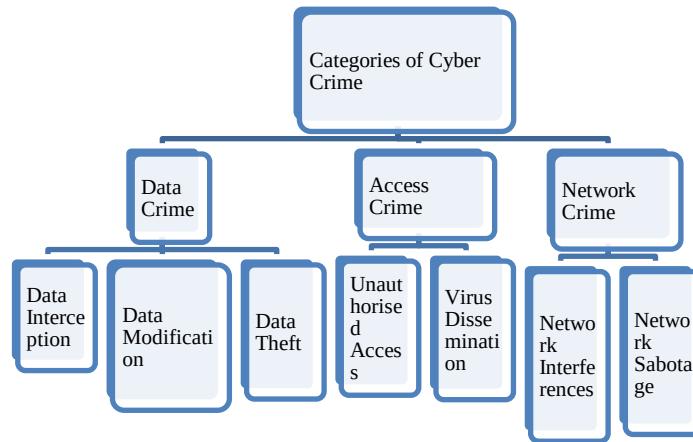


Figure 4 Categories of Software Piracy

3. **Network Crime:** Network Crime is mainly classified into Network Interferences and Network Sabotage.
 - a. **Network Interferences:** System Interfering with the working of a PC Network by contributing, transmitting, harming, erasing, falling apart, modifying or smothering Network information.
 - b. **Network Sabotage:** 'System Sabotage' or clumsy directors endeavouring to carry out the occupations of the general population they regularly are responsible for? It could be the above alone, or a mix of things. In any case, if Verizon is utilizing the assistance the youngsters, thwarting specialists on call line then they may utilize arrange issues as a reason to get the government to mediate in light of a legitimate concern for open security[2]. Obviously if the government powers these individuals back to work what is the reason for unions and strikes anyway.

IV IMPACTS OF CYBER CRIME

1. Impact of Cyber Crime over Society

In spite of crimeless society is myth, wrongdoing is ubiquitous marvel, and it is non-divisible piece of social presence, one may get bother by the inquiry, 'Why there is excessively ado about crime?' No one can deny that wrongdoing is a social wonder, it is inescapable, and there is just the same old thing new in wrongdoing as it is one of the trademark highlights of the all social orders existed up until this point, may it be socialized or savage, and it is one of the essential impulses of all human conduct! Nonetheless, it should remember that the social worry for high wrongdoing rate isn't a direct result of its inclination, yet because of potential unsettling influence it causes to the general public. Furthermore, a few people are casualties of wrongdoing in a more particular sense[1]. The casualties of wrongdoing may lose anything that has esteem. Wellbeing, peace, cash, and property are maybe essential esteems, since they add as per the general inclination of many wishes.

2. Impact of Cyber Crime over Socio-Eco-Political Riders

Thoughtfully, wrongdoing is a dynamic and relative wonder and subjected to the relative sociopolitical and temperate changes happening in existing arrangement of society. Consequently, neither one of the time appropriate far reaching definition enveloping all parts of 'wrongdoing' is conceivable at any snapshot of time nor can a solitary definition be made material to various society. With its dynamicity, it is affected by the progressions happening in the related wonder and esteem framework produced by these progressions. As clear in show situation where cash is more important than values, an unequivocal climb in the defilement related offenses are watched where social profound quality is low which impact the commission of wrongdoing appended less social shame than at any other time. By chance financial wrongdoing is on its pinnacle. This obviously mirrors wrongdoing has its interdependency with other social wonder, monetary frameworks and political hardware. Additionally, the populace is one of the critical elements impacting occurrences of crimes[8]. A positive correlation between the growth in incidences of crime and the population of the country has been observed.

3. Impact of Cyber Crime over Industry

Using three credits to depict cybercrime I would utilize the words nosy, noiseless and unsafe. Simply the quiet method of this sort of violations is a noteworthy issue in fighting the risk, indeed, frequently the organizations understand that they have been casualties of cheats or assaults until the point when long after the occasion happened. The results are incapacitating and recover the circumstance is here and there inconceivable, correctly the time hole between the criminal occasion and its disclosure gives leverage to the individuals who perpetrate wrongdoings regularly unbridgeable that makes unthinkable any activity of oppression. Yet, we are expecting that the occasion is found by the casualties and this isn't generally valid, many organizations are in reality finished the years are casualties of cybercrime, however they don't know, a disease that devastates from inside.

4. Impact of Cyber Crime over Teenagers

Nowadays a most noticeably bad dread in young person's eyes is Cyber Bullying. It is turned out to be basic over recent years, for the most part from the age underneath eighteen are more powerless and dreaded from Cyber Bullying according to review. It is turning into a disturbing pattern in our general public. According to investigation of information, the most exceedingly awful dread of digital wrongdoing is on youngsters female[7]. Digital Bullying is a dread when individual gets dangers, adverse remarks or pessimistic pictures or remarks from other individual. Cyber Bulling can be done through chatting, instant messaging. Users who are using the social networking websites like facebook, twitter, linkedin etc. are more affected from cyber bulling.

5. Impact of Cyber Crime over Buisness

As per the FBI and the Department of Justice, digital wrongdoing is on the ascent among American organizations, and it is costing them profoundly. Digital wrongdoing incorporates a horde of naughty criminal practices intended to break an organization's PC security. The reason for the electronic break and enter can be to take the budgetary data of the business or its clients, to refuse assistance to the organization site or to introduce an infection that screens an organization's online action later on.

Organizations that need to shield themselves from online cheats need to haul out their wallets to do it. There are costs in recognizing dangers, constructing new and more secure working methodology, and purchasing defensive programming and equipment. For organizations with intricate or delicate operations, this frequently includes enlisting a digital security specialist to build up a tweaked arrangement[13]. Not exclusively are the forthright expenses of assurance costly, yet the frameworks must be tried and observed consistently to guarantee that they are as yet compelling against developing digital assaults. These expenses are frequently passed on to the client through higher costs of merchandise and ventures.

IV CONCLUSION

The growth of cyber crime is very high now days and becoming a worldwide issue. The proper education about cybercrime and preventions are required to reduce cybercrimes. This paper puts its eye not only on the understanding the cyber crime, categories of cyber crime but also explain the impacts of cyber crime in various aspects. The main challenge of the cybercrime is the availability of readymade hacking tools that are used for different types of cyber related to crime. It is the responsibility of each individual to take necessary precautions while performing the online transactions.

REFERENCES

- [1] Wow Essay (2009), Top Lycos Networks, Available at: <http://www.wowessays.com/dbase/ab2/nyr90.shtml>, Visited: 28/01/2012.
- [2] Computer Hope (2012), Data Theft, Available at: <http://www.computerhope.com/jargon/d/datathef.htm>, Visited: 28/01/2012.
- [3] PTI Contents (2009), India: A major hub for cybercrime, Available at: <http://business.rediff.com/slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm>, Visited: 28/01/2012.
- [4] Shrivastav et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013, pp. 414-419 201.
- [5] Rupinder Pal Kaur International Journal Of Engineering And Computer Science ISSN:23197242 Volume2 Issue 8 August, 2013 Page No. 2555-2559.
- [6] K. Sreedevi. 2013. "India in top five in cyber crimes". Deccan Chronicle. 23 October. <http://www.deccanchronicle.com/131023/news-current-affairs/article/india-top-five-cybercrimes>.
- [7] Sumanjit Das, Tapaswini Nayak "Impact of Cyber Crime : Issues and Challenges", International Journal of Engineering Sciences & Emerging Technologies", Volume 6 Issue 2 pp 142-153.
- [8] Hemraj Saini, T.C.Panda, "Cyber Crime and their impacts: A Review", International Journal of Engineering Research & Applications", Volume 2 Issue 2, pp 202-209 April 2012.
- [9] Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
- [10] Shubham Kumar, Uday Kumar, "Present Scenario of cybercrime in India and its preventions", International Journal of Scientific & Engineering Research", Volume 6, Issue 4 April-2015.
- [11] P.N. Vijay Kumar, "Growing Cyber Crime in India: A Survey.
- [12] <https://www.emc.com/collateral/white-paper/rsawhite-paper-cybercrime-trends-2015.pdf>.
- [13] Rita Dewanjee, R. Vyas, "Cyber Crime: Critical View", International Journal of Science and Research", ISSN: 2319-7064, 2013.