International Journal of Engineering, Management & Technology (IJEMT)
www.ijemt.com, Volume 1 Issue VI, August 2022, PP 24-44, ISSN (Online): 2583 – 4517

THE BASIC CONCEPT OF CYBER CRIME

Osman Goni[1*]

Designation: Senior Engineer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh.

Md. Haidar Ali[2]

Designation: Senior Scientific Officer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh

Mr. Showrov[3]

Designation: Scientific Officer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh

Md. Mahbub Alam[4]

Designation: Scientific Officer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh

Md. Abu Shameem[5]

Designation: Principal Engineer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh

Corresponding Author: **Osman Goni**, Senior Engineer, Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh
Email: engr.osmangoni@gmail.com

ABSTRACT: Cyber Crime is a common phenomenon in the world. Cyber Crime is that group of activities made by the people by creating disturbance in network, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own. Cyber Crime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Cyber crime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, Trafficking in child pornography and intellectual property, stealing identities, or violating privacy. The cyber crime and they its impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Now a day's Cyber crime is increasing day by day. People have been greatly suffering for it. It is not only creating human suffering but also put effect on it. So Cyber Crime is one of the major crimes done by computer expert. This paper gives the basic concept of cyber crime.

[*] Corresponding Author: Osman Goni
Corresponding Author Email: engr.osmangoni@gmail.com
Published on: August 16, 2022

KEY WORDS: Cyber Crime, Criminal, Child Pornography, Computer Crime, Human Suffering.

1. INTRODUCTION

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both. Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet [1]. Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds [2]. Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime. Just as it is important to understand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way these users fall victim to cybercrime. Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of 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 Internet but there is another side of the coin that is cyber crime by the use of Internet [3]. Cyber crime is a bi-product of the ever-increasing development in the areas of information and communication technology (ICT). The attackers mainly attack the confidential data of the organizations or personal information thereof. The most targeted organizations are hospitals, government offices, police stations, financial. institutions, Research and Development (R&D) organizations and other telecommunication firms etc [4].

2. LITERATURE REVIEW

2.1 Cyber Criminal:

Cyber criminals are an ever-present menace in every country connected to the Internet. The cyber criminals constitute of various groups or category as shown below:

2.1.1 Children and Adolescents:

The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reasons may be to prove themselves to be outstanding amongst other children in their group.

2.1.2 Organized Hackers:

These kinds of hackers are mostly organized together to fulfill certain objective. The reason may be to fulfill their political bias, fundamentalism, etc. The Chinese are said to be one of the best quality hackers in the world. They mainly target the other governments' sites with the purpose to fulfill political objectives.

2.1.3 Professional Hackers/Crackers:

These kinds of hacker's work are motivated by money and mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

2.1.4 Discontented Employees:

This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. Traditionally, internal attacks posed the greatest threat to computer networks, which accounted for about 70 percent of all attempted intrusions [5].

2.2 Cyber Crime:

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS) [6]." The oxford Dictionary defined the term cyber crime as "Criminal activities carried out by means of computers or the Internet [7]." "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime [8]." "Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them [9]." Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds [2].

2.3 Categories of Cyber Crime:

There are a lot of Cyber Crime categories; these categories include different terminology and iconography that create controversy over the computer attacker terms.

2.3.1. Data Crime:

Data Interception, Data Modification, and Data Theft are called Data Crime. An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. Data Theft used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law [2].

2.3.2. Network Crime:

Unauthorized Access and Virus Dissemination are called Network Crime. "Unauthorized Access" is an insider ‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality [10]. Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim [11].

2.3.3. Related Crimes:

Aiding and Abetting Cyber Crimes, Computer-Related Forgery and Fraud and Content-Related Crimes are called Related Crime. There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. Computer forgery and computer-related fraud constitute computer-related offenses. Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries [12] [13] [14].

2.4 Types of Cyber Crime:

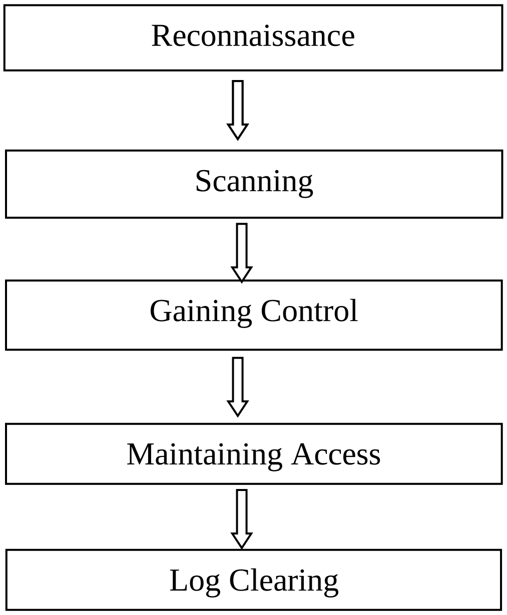
There are many types of Cyber Crime. 1. Hacking, 2. Virus dissemination, 3. Logic bombs, 4. Denial-of-Service attack, 5. Phishing, 6. Email bombing and spamming, 7. Web jacking, 8. Cyber stalking, 9. Data diddling, 10. Identity Theft and Credit Card Fraud, 11. Salami slicing attack, 12. Software Piracy, 13. Cyber Pornography, 14. Sale of illegal articles, 15. Pharming 16.TOR Network

2.4.1. Hacking:

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc. [15].

Now the methodology or the path followed by the Hackers is as follows:

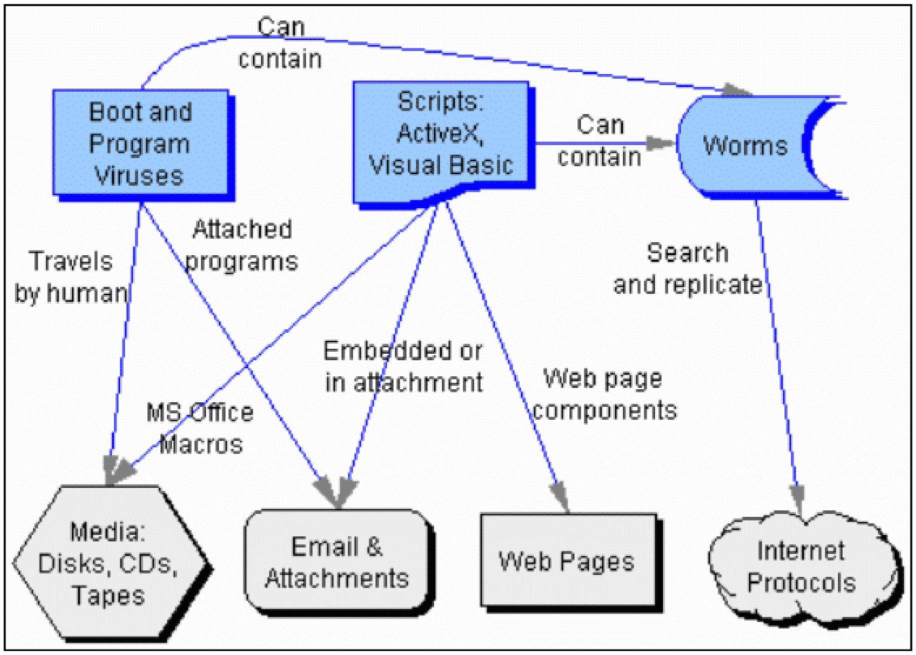
Figure:1. Block Diagram of the methodology or the path followed by the Hackers



2.4.2. Virus dissemination:

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean self-replicating "malware" (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominative current virus scenario. "Trojan horses" are different from viruses in their manner of propagation.

Figure:2. A simple diagram to show how malware can propagate



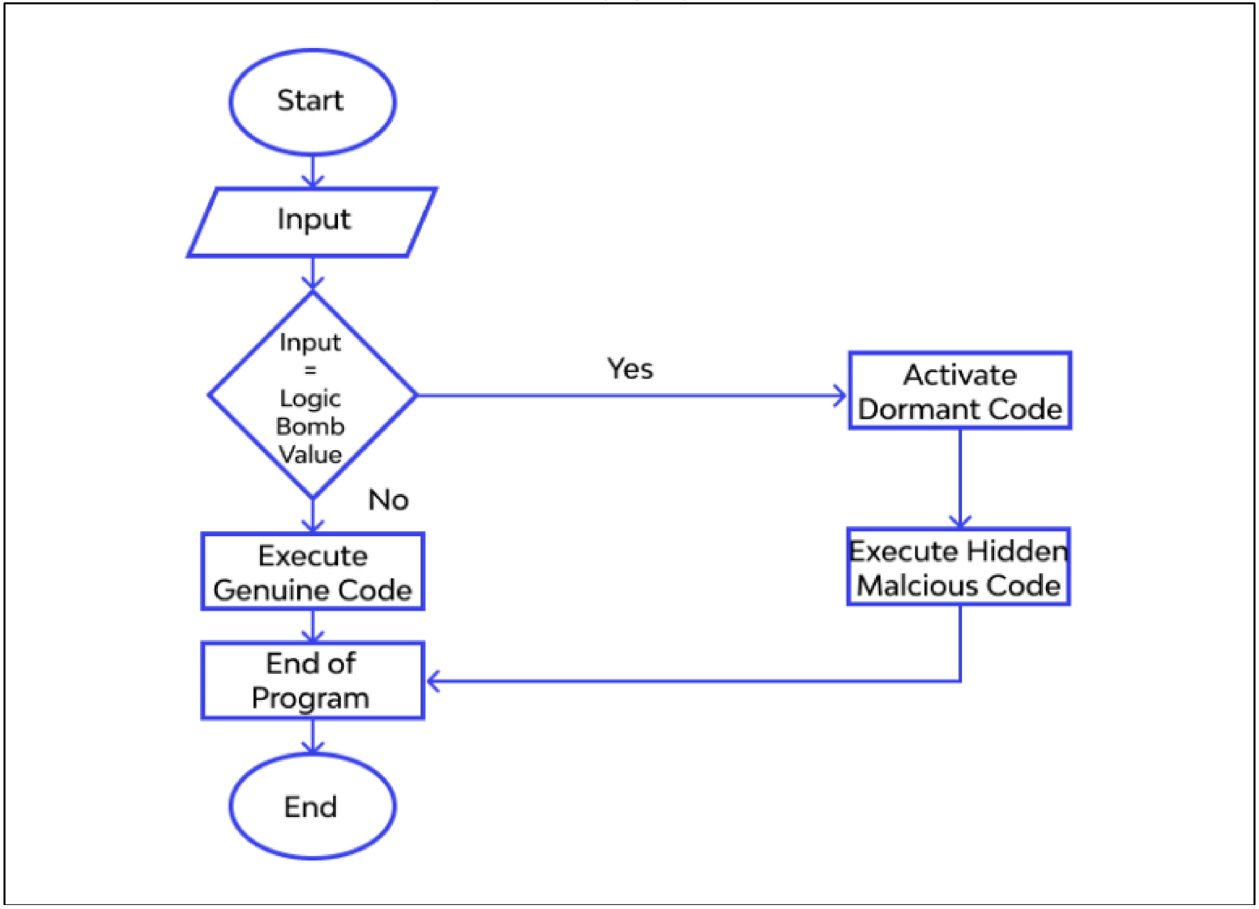
2.4.3. Logic bombs:

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

There's another use for the type of action carried out in a logic bomb "explosion" – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a nondestructive, non-malicious and user-transparent use, and is not typically referred to as one.

A logic bomb is a piece of malicious code that lies dormant and hidden within a legitimate software until a condition is satisfied to trigger its payload. This malware is normally embedded by developers into genuine software. A logic bomb has a flaw that it only works for a software for which it has been designed, it doesn't replicate on other applications. Presence of Logic bomb in system poses great risks to its security and integrity [16]. Working of logic bomb code in a genuine code is shown in figure:

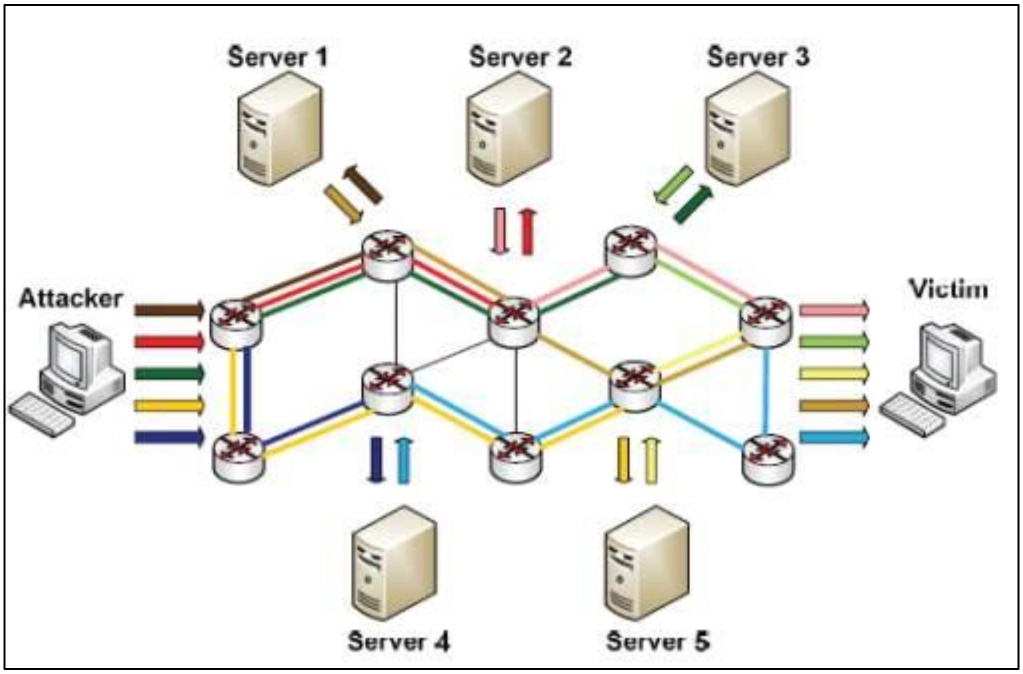
Figure:3. Working of Logic Bomb [16].



2.4.4. Denial-of-Service attack:

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

Figure:4. RDoS Principle [17].

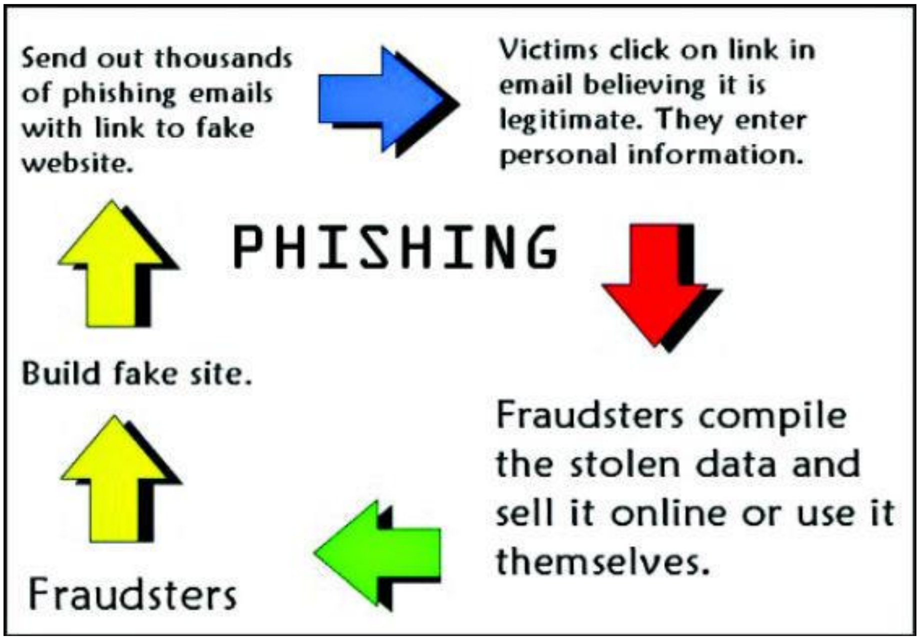


Another variation to a denial-of-service attack is known as a “Distributed Denial of Service” (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

2.4.5. Phishing:

This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You’ve probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn’t click the link. Smart move.

Figure: 5. Phishing Process


Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters

The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.

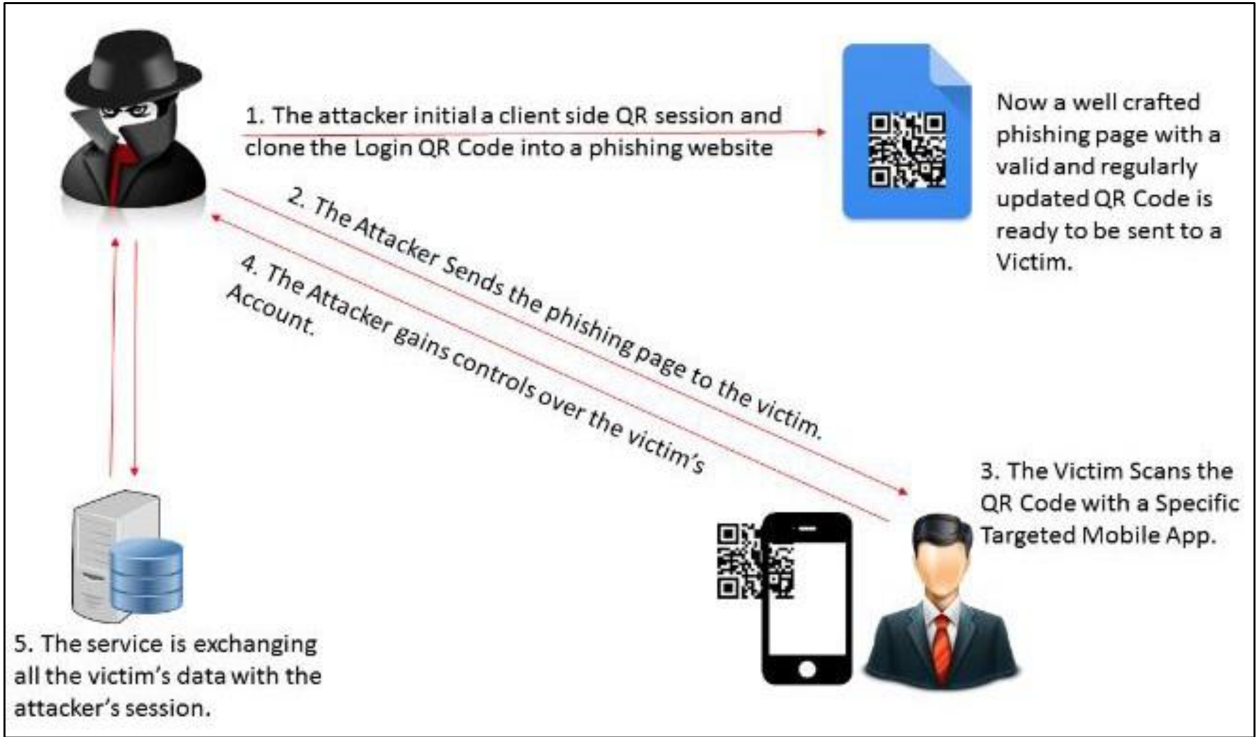
2.4.6. Email bombing and spamming:

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

2.4.7. Web jacking:

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

Figure:6. Detailed Overview of Web Jacking


1. The attacker initial a client side QR session and clone the Login QR Code into a phishing website
Now a well crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.
2. The Attacker Sends the phishing page to the victim.
4. The Attacker gains controls over the victim's Account.
3. The Victim Scans the QR Code with a Specific Targeted Mobile App.
5. The service is exchanging all the victim's data with the attacker's session.

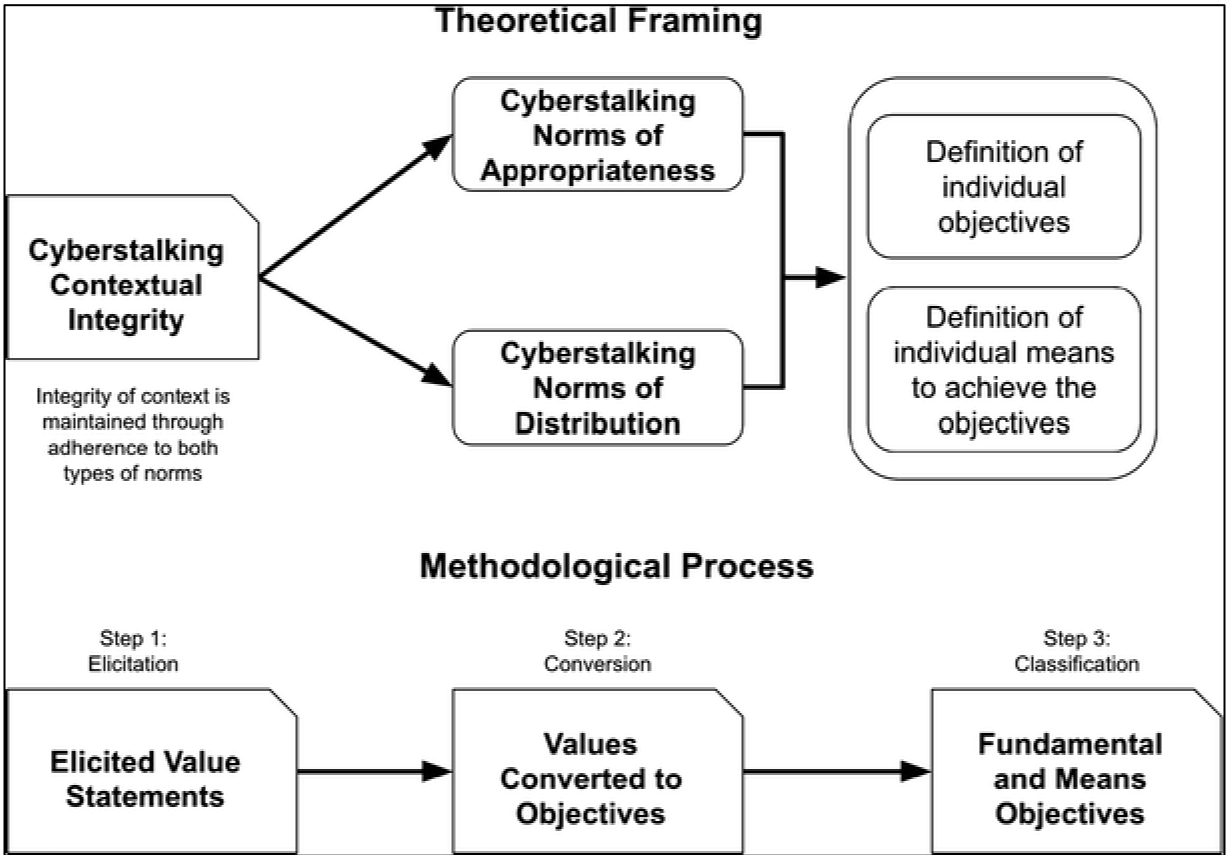
Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the webjacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

2.4.8. Cyberstalking:

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy.

Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

Figure:7. Objectives for preventing Cyberstalking

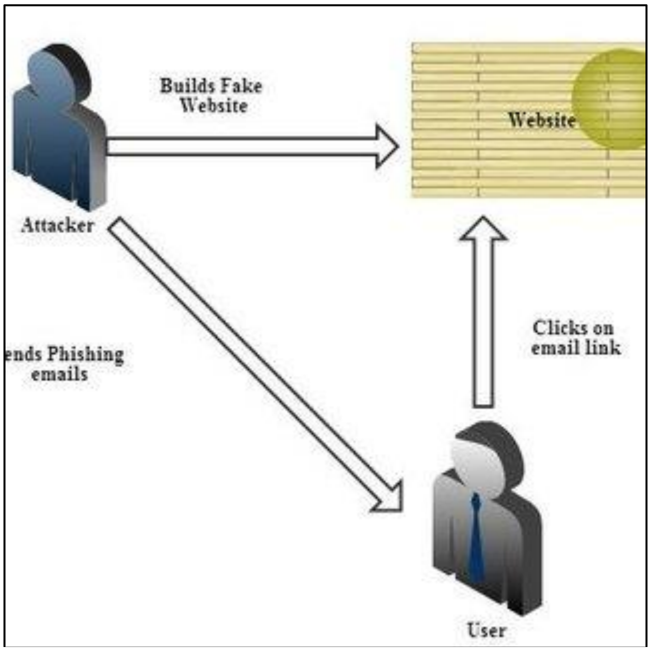

Theoretical Framing
Cyberstalking Contextual Integrity
Integrity of context is maintained through adherence to both types of norms
Cyberstalking Norms of Appropriateness
Cyberstalking Norms of Distribution
Definition of individual objectives
Definition of individual means to achieve the objectives
Methodological Process
Step 1: Elicitation
Step 2: Conversion
Step 3: Classification
Elicited Value Statements
Values Converted to Objectives
Fundamental and Means Objectives

The Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker. The cyber stalker is one who uses the Internet as a weapon or tool of sorts to prey upon, harass, threaten, and generate fear and trepidation in his or her victims through sophisticated stalking tactics, which for the most part, are largely misunderstood and in some cases, legal [18].

2.4.9. Data diddling:

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that’s programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

Figure:8. Data Diddling Attack

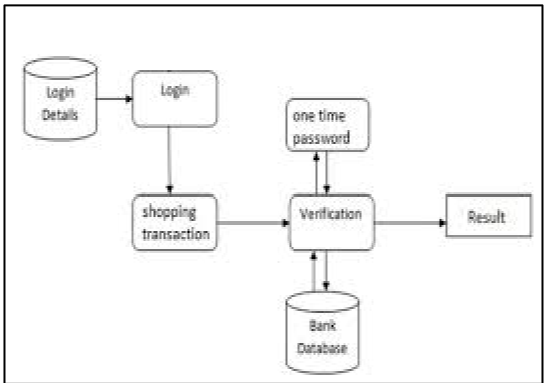


This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full. By altering or failing to enter the information, they're able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

2.4.10. Identity Theft and Credit Card Fraud:

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide-ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.

Figure:9. Credit Card Fraud System hidden Markov Model [19].



With rising cases of credit card fraud, many financial institutions have stepped in with software solutions to monitor your credit and guard your identity. ID theft insurance can be taken to recover lost wages and restore your credit. But before you spend a fortune on these services, apply the no-cost, common sense measures to avert such a crime.

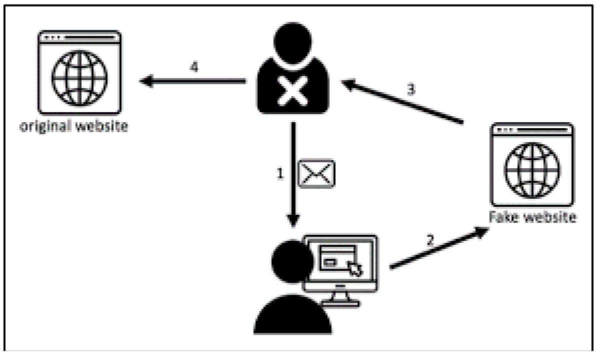
2.4.11. Salami slicing attack:

A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is “collect-the-round off” technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator’s account.

Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their knowhow of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations.

The attackers steal resources or money a little at a time in the salami technique. The important thing here is to make the change meaningless and no one will notice it completely. For example, an employee of bank installs a software into the servers of the bank, which takes a small amount of money from each customer's account. Every account holder isn't likely to notice this illegal deduction, but every month the attacker will make a substantial amount of money. The attacker installs malware on the server so that it performs a specific purpose, such as installing malware on the bank' server and its purpose is to deduct small values of money and send it to the attacker without giving an alert [20].

Figure:10. Salami Slicing Attack and Phishing Attack [20].



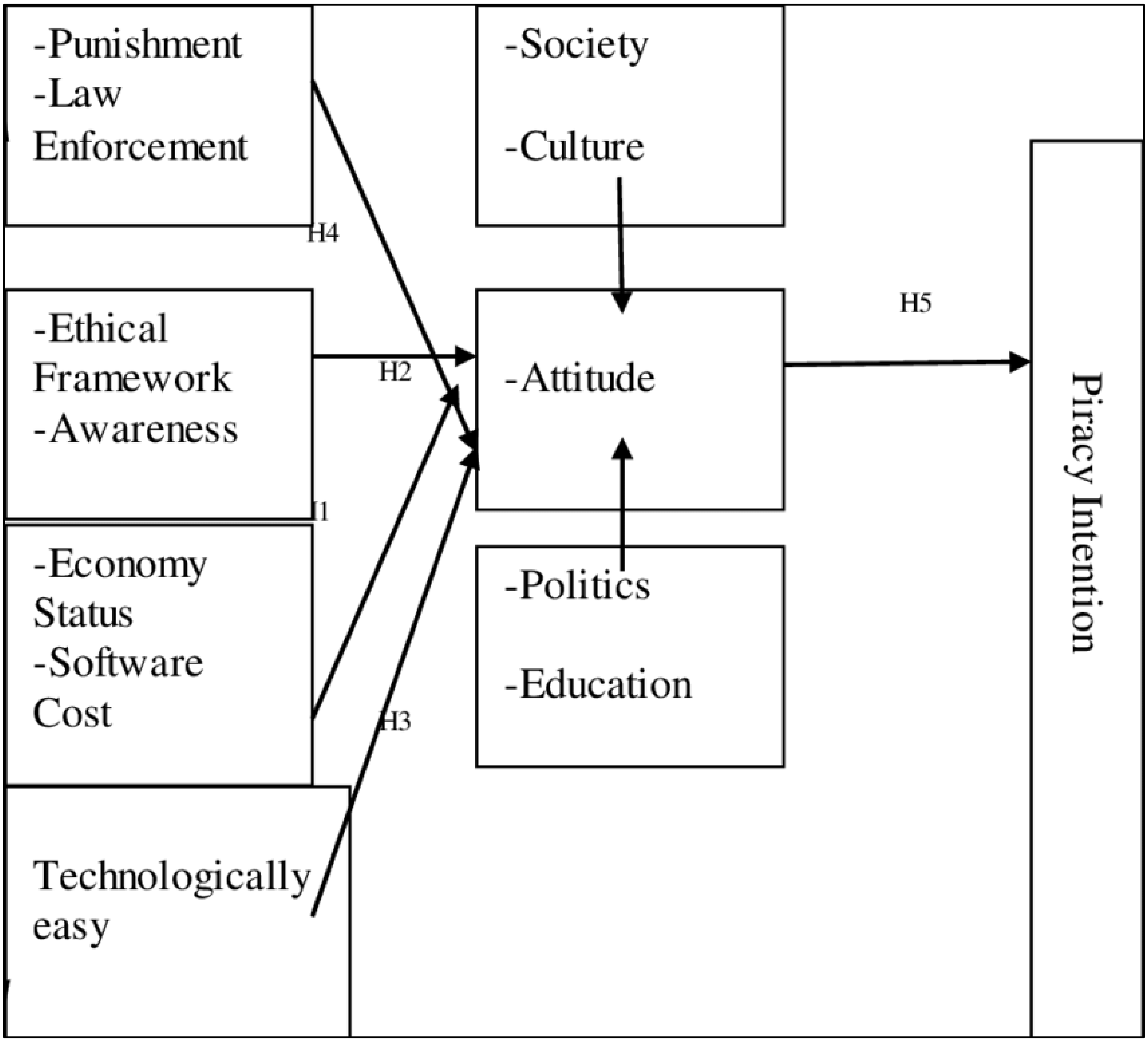
Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering. The salami technique can also be applied together little bits of information over a period of time to deduce an overall picture of an organization. This act of distributed information gathering may be against an individual or an organization.

Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target. Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

2.4.12. Software Piracy:

We can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.

Figure:11. Software Piracy [21].



Software piracy is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

2.4.13. Cyber Pornography:

Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc. There are more than 420 million individual pornographic webpages today. Child pornography is a very unfortunate reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide [22].

Child Sexual Abuse is more severe than any form of exploitation a girl child can encounter. This is because it can leave a severe and lasting impact on a girl child for the rest of their life. Further, Child pornography is considered to be different from adult pornography due to intricacies involved. In child pornography, children are harmed not only in production process but also after publication of such pornography on internet, or via any other media. It attaches a taint on the future of children depicting them in bad light and characterizing them on social networking sites belonging to children who are below 18 years of age. Publication of their nude photos, either with their consent or fraudulently, affects the prospects of their development and it also affects their mental health .Therefore, in a country like India and Bangladesh where a considerable portion of the population consists of women and children, laws made in this regard must be essentially stringent and must at the same time cater to the varied social and cultural scenario pertinent .Moreover, the available statutory measures along with regulatory enforcement mechanism to churn out cyber pornography must be articulated keeping in light the rapid development of the internet and its ill-effects on the society and the innocent minds of the children [23].

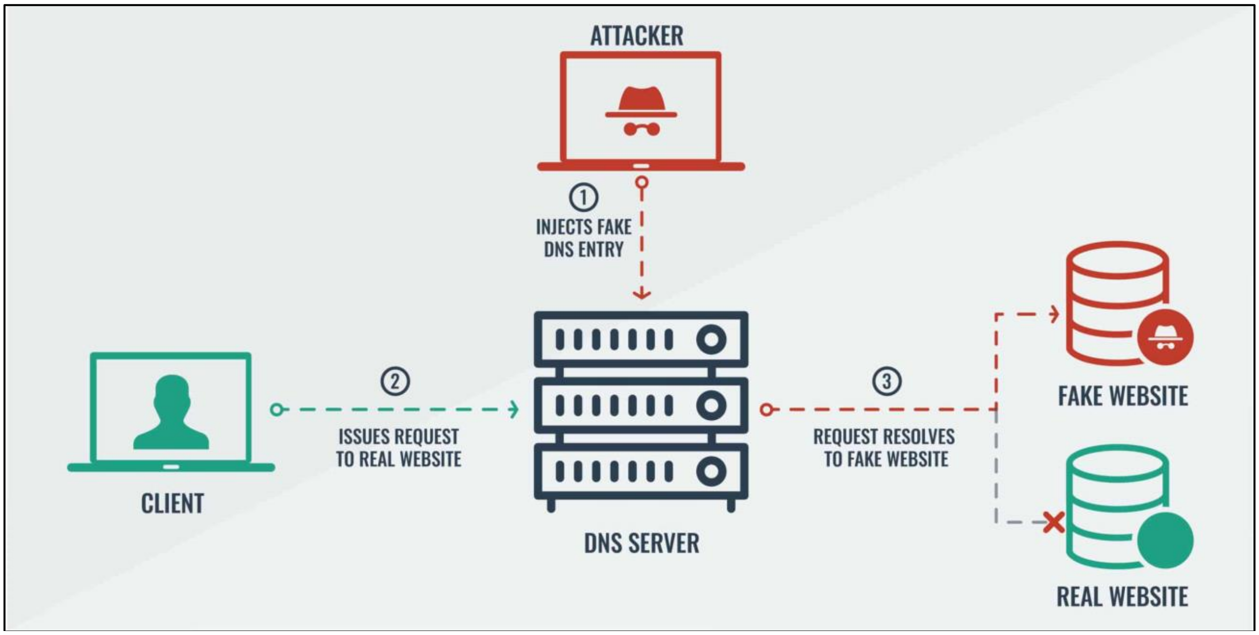
2.4.14. Sale of illegal articles:

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale [22].

2.4.15. Pharming:

Pharming is an attack expected to divert your site traffic to another, presumably false site. Pharming isn't effectively discernible on PC. Pharming is normally done by infecting DNS servers which is beyond control and stays undetectable for a large part. The main way pharming could have been done on your PC is by altering the host's file. In the event that the record contains false entries, at that point some program has attempted to perform pharming on your PC. Some site blocking software use the hosts file to map addresses to the localhost [24].

Figure:12. Pharming Attack.



2.4.16.TOR Network:

This section depicts the noxious business activities recognized in the profound web, especially commercial centers and merchandise cyber-criminal exchange. In spite of the way that the entirety of the previously mentioned systems can possibly bolster unlawful exchanges of each sort, until now, the main system that appears to have increased some footing for underground commercial centers is TOR. The explanation for this might be connected to the way that TOR is relatively more experienced and more created than the opposition and has been endorsed by associations, like the Electronic Frontier Foundation as the first choice among hostile to restriction instruments, putting it under the spotlight as of late. The Deep Web and malware are consummately appropriate for one another, particularly with regards to facilitating order and-control (C&C) system. It is the idea of concealed administrations and destinations like TOR and I2P to shroud the area of servers using solid cryptography. This makes hard for forensic researchers to investigate using conventional methods like looking at a server's IP address, checking enlistment subtleties, etc. What's more, using these locales and administrations isn't especially troublesome. It is then to be expected to see various cybercriminals use TOR for C&C. We've seen the administrators behind predominant malware families use TOR for certain pieces of their arrangement. They basically group the authentic TOR customer with their installation package. Another major malware family that utilizes the Deep Web is Crypto Locker. Crypto Locker alludes to a ransom ware variation that encrypts victims very own reports before redirecting them to a site where they can pay to recover access to their documents. Crypto Locker is likewise keen enough to consequently alter the payment page to represent a victim’s local language and means of payment. It shows why the Deep Web bids to 16 cybercriminals who are eager to make their foundations increasingly powerful to potential takedowns [24].

3. CONCLUSION

The future of the Internet is still up for grabs between criminals and normal users. Our reliance on networks will only continue to grow in the years ahead. This paper concludes with basic information of our privilege society which should aware about cyber crimes. Based on an analysis of existing cyber-Crimes and privacy issues targeting about Cyber Crimes, a comprehensive framework is developed that provides an overview of possible security and privacy threats along with the ways of attacks and countermeasures. In the future, we are planning to apply the proposed framework in Cyber Crime to analyze the impact of the proposed approach in mitigating cyber privacy and security issues. Having identified and understood in clear terms the various cyber-Crimes to cyber security, caution is a watchword for whoever is on the internet. Nevertheless, cyber security is potentially under the mercies of some common factors as explained in this journal article.

REFERENCES:

[1] P. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law," in *An Introduction to Cyber Crime and Cyber law*, Kamal Law House, 2012.

[2] S. D. a. T. Nayak, "IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES," vol. 6, no. 2, October 2013.

[3] Y. S. R. T. Hemraj Saini, "Cyber-Crimes and their Impacts: A Review," vol. 2, no. 2, 2012.

[4] 2. K. A. I. T. T. J. S. R. A. H. I. H. C. Shusmoy Kundu1, "Cyber Crime Trend in Bangladesh, an Analysis and Ways Out to Combat the Threat," Dhaka-1216, Bangladesh, 2018.

[5] n. p. Brigadier General Md. Khurshid Alam, "CYBERCRIME IN BANGLADESH: IMPLICATIONS AND RESPONSE STRATEGY".

[6] 4 January 2016. [Online]. Available: http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf. [Accessed 4 January 2016].

[7] 4 January 2016. [Online]. Available: http://www.oxforddictionaries.com/definition/english/cybercrime. [Accessed 4 January 2016].

[8] 4 January 2016. [Online]. Available: www.naavi.org/pati/pati_cybercrimes_dec03.htm. [Accessed 4 January 2016].

[9] 4 January 2016. [Online]. Available: http://cybercrime.org.za/definition. [Accessed 4 January 2016].

[10] 28 January 2012. [Online]. Available: http://www.imdb.com/title/tt0373414/. [Accessed 28 January 2012].

[11] V. D. Virus Glossary (2006), 28 January 2012. [Online]. Available: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml. [Accessed 28 January 2012].

[12] C. O. a. a. a. o. A. Legal Info (2009), 28 January 2012. [Online]. Available: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html. [Accessed 28 January 2012].

[13] N. I. Shantosh Rout (2008), 28 January 2012. [Online]. Available: http://www.santoshraut.com/forensic/ cybercrime.htm. [Accessed 28 January 2012].

[14] By Jessica Stanicon (2009), 28 January 2012. [Online]. Available: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html. [Accessed 28 January 2012].

[15] A. A. Aman Gupta, "Ethical Hacking and Hacking Attacks," *International Journal Of Engineering And Computer Science,* vol. 6, no. 4, pp. 21042-21050, 4 April 2017.

[16] Y. P. Palash Sandip Dusane1, "Logic Bomb: An Insider Attack," *International Journal of Advanced Trends in Computer Science and Engineering,* vol. 9, no. 3, pp. 3662-3665, May - June 2020.

[17] H. S. Obaid, "Denial of Service Attacks: Tools and Categories," *International Journal of Engineering Research & Technology (IJERT),* vol. 9, no. 03, pp. 631-636, March-2020.

[18] M. L. Pittaro1, "Cyber stalking: An Analysis of Online Harassment and Intimidation," *International Journal of Cyber Criminology. This work is licensed under a under a creative commons Attribution-Noncommercial-Share Alike 2.5 India License,* vol. 1, no. 2, p. 180–197, 2007.

[19] N. P. S. K. S. S. P. A. P. Nabha Kshirsagar1, "Credit Card Fraud Detection System using Hidden Markov Model and Adaptive Communal Detection," *(IJCSIT) International Journal of Computer Science and Information Technologies,* vol. 6, no. 2, pp. 1795-1797, 2015.

[20] M. A. A. B. S. M. M. J. A.-A. Asalah F Altwairqi, "Four Most Famous Cyber Attacks for Financial Gains," *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 9, no. 2, pp. 2131-2139, December, 2019.

[21] M. S.-T. (PhD, "Software Piracy: Some Issues," in *Columbus State University, University Ave, Columbus*, 4225 University Ave, Columbus, GA, 31907, October 2013.

[22] K. C. Vadza, "Cyber Crime & its Categories," vol. 3, no. 5, 2013.

[23] D. M. Joshi, "CYBER PORNOGRAPHY: AN INTERDISCIPLINARY STUDY OF TECHNOLOGY LED CRIME AGAINST WOMEN AND CHILDREN.," *International Journal of Creative Research Thoughts (IJCRT),* vol. 9, no. 12, pp. b297-b301, 2021.

[24] E. a. P. Cyber Crime: Rise, 1 July 2020. [Online]. Available: https://www.researchgate.net/publication/344349620. [Accessed 1 July 2020].

Biography:

Osman Goni was born at Chandpur, Bangladesh in 25th September 1982. He has completed his Diploma-in-Computer Engineering and obtained 3rd place from Bangladesh Technical Education Board (**BTEB**) and B. Sc.in Computer Science & Engineering from the Department of Computer Science and Engineering of World University of Bangladesh (**WUB**) and M. Sc.in Computer Science & Engineering from the Department of Computer Science and Engineering of Jagannath University (**JnU**) in Bangladesh. Currently he is working as Senior Engineer (Computer Science and Engineering) at the institute of Computer Science in Bangladesh Atomic Energy Commission. He is member of Institution of Diploma Engineers, Bangladesh (IDEB) and associate member of Bangladesh Computer Society (BCS). His research interest includes Computer Hardware and Networking, artificial intelligence and Robotics, Cyber Security, E-Commerce etc.

Md. Haidar Ali was born in Kishorgonj, Bangladesh, on 25th January, 1985. He received the B.Sc. Degree in Computer Science and Engineering from the Daffodil International University, Bangladesh in 2010, and in 2012, he received the M.Sc. degree in Computer Science and Engineering from Daffodil International University. He worked at Padma Multipurpose

Bridge Project, Bridge Division under Ministry of Road Transport & Bridges, Bangladesh from 14 October 2014 to 05 November, 2016 as a Assistant Programmer. From 15 November 2016 to still now, He is being a scientific officer of Computer Science Division in Bangladesh Atomic Energy Commission. He is a Life Time Member of Bangladesh Computer Society and Also Life Time Member of IEB. His research interest includes Network and Cyber security, communication Engineering.

Mr. Showrov is currently working as a researcher at the Institute of Computer Science at Bangladesh Atomic Energy Commission. His research interest lies in but not limited to data mining, information retrieval etc. He has completed his undergraduate from Shahjalal University of Science & Technology and graduated from South Asian University.

Md. Mahbub Alam was born in a rural area called Dhamrai of Dhaka in 1991. He has completed his B.Sc & M.Sc from the Department of Computer Science and Engineering,Jahangirnagar University, Savar, Dhaka, Bangladesh. He worked as a lecturer in Gono University at the Dept. of CSE from January 2015 to February 2016. He worked as an Assintant Engineer in WALTON Group at the Computer R&D section from February 2016 to November 2017. Currently he is working as a Scientific Officer at the Institute of Computer Science in Bangladesh Atomic Energy Commission. His research interests include big data analysis, artificial intelligence, pattern recognition and expert system, computer vision, system that can provide distinct service through internet protocol and any system that can be beneficiary for common people. He is also interested in entrepreneurship.

Md. Abu Shameem was born in Bhairab, Kishoregonj, Bangladesh in 1969. He was completed Bachelor of Science in electronics & telecommunications engineering from the department of electronics & telecommunications engineering Prime University, Mirpur, Dhaka and Master of Science in telecommunications engineering from the department of electronics & communications engineering East West University, Dhaka. He worked as a senior instructor in department of youth development from January’1994 to December’ 1995. Currently he is working as a principal engineer & divisional head of computer system & networking division at the institute of computer science in Bangladesh atomic energy commission. His research interest includes communication engineering, networking & security system, server administration and instrumentation & control system etc.