REVIEW ON CYBER CRIME AND SECURITY

Urvashi Sangwan

Abstract: Ever since men began to change their lives by using technology they have found themselves in a series of technology trap. These days computer and internet become very necessary and useful for our daily life. The internet is growing very rapidly. It has given new opportunity in every field like education, business, entertainment etc. It is true that every coin has two sides i.e. positive and negative; In the same way internet has both pros and cons and most disadvantage is cyber crime. Since hackers and other offenders in world are trying to get the most reliable and secret information at minimal cost through viruses and other malicious software’s. Cyber crime is an unlawful act that’s lead to criminal activity. Cyber criminals are targeting consumers as well as public and private organizations. Cyber security is a mechanism by which computer information and equipments are protected from unauthorized and illegal access. This paper focus on cybercrime challenges its impact on society types of threats and cyber security and regulation acts imposed against cyber crime.

Keywords: - Cyber Crimes Cyber Attack Network Security Privacy Computer Security

1. INTRODUCTION
The internet in India is growing very rapidly. In present days people can get information, store information and share information through the internet. The growing world of internet is known as cyber world. Today internet becomes the backbone of social and economic world. Users can access the internet anytime from anywhere but through internet many illegal works may be done. E-mail and website is the most efficient way of data communication [1]. Computer crime is a criminal activity which involves information technology infrastructure unauthorized access illegal interception data interference, abuse of devices, forgery, blackmail and some electronic fraud. Cyber crime cells are there in states to handle these crimes and to punish criminals committing any of the cyber crime [2]. Hundreds of millions of computer are connected to the internet and many computer systems are without adequate protection to prevent illegal access. An unprotected computer system that is connected to the internet is likely to experience attack within less than a minute. The installation of protective measures can lower the risk but successful attacks against well protected computer system prove that technical protection measures can never completely stop attacks [3].

2. CYBER CRIME
Cyber crime also referred as computer crimes electronic crimes; the electronic medium of computer network in which online communication takes place. Cyber crime is regarded as computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducts through global electronics network. Cyber crime was broken into two categories: -
Cybercrime in a narrow sense: Any illegal behavior directed by means of electronic operations that targets the security of computer systems and data processed by them.
Cybercrime in a broader sense: Any illegal behavior committed by means of or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of a computer system or network [4].
Examples of cyber crime are:
Denial of service: - It is an act which criminal sends spam mails to the victim’s mail box depriving him/her of the entitled service to be provided. It is particularly an attempt to make the resources unavailable to users. It is basically produced by unintentional failures of nodes. Denial of Service attack attempts to exhausts the available resources by sending unnecessary packets to the victim node. An attacker may take control of system by taking advantage of security weakness or vulnerabilities [5].
Hacking: - Hacking is gaining unauthorized access to a computer. In hacking criminal’s uses variety of software to enter a person’s computer and person may not be aware that his computer is being accessed from a remote location. This is a type of crime wherein a person’s computer is broken into so that his personal information can be accessed [6]. Some hackers explore for sheer curiosity finding their way into unfamiliar systems for love of the challenge in some cases going so far as to alert system owners to security loopholes. Others hack for their own reasons either to steal information gain control over systems for their own purposes or simply to cause as much damage and chaos as possible.
E-mail bombing: - This is a serious crime in which a person sends a number of emails to the inbox of target system/person.
Mail bombs usually fill allotted space on an e-mail server for the users e-mail and can result in crashing the e-mail server. An

1 Assistant professor, Vaish college of Engg Rohtak
email bomb is an attack against an email inbox or server designed to overwhelm an inbox or inhibit the server’s normal function rendering it unresponsive preventing email communications degrading network performance or causing downtime. The intensity of an email bomb can range from an inconvenience to a complete denial of service. Typically these attacks persist for hours or until the targeted inbox or server implements a mitigation tactic to filter or block the attacking traffic. Such attacks can be carried out intentionally or unintentionally by a single actor or group of actors. There are five common email bomb techniques:

Mass mailing – intentionally or unintentionally sending large quantities of random email traffic to targeted email addresses. This attack is often achieved using a malicious script such as by the automated filling out of online forms with the target email inserted as the requesting/return address.

List linking – signing targeted email addresses up for numerous email subscriptions which indirectly flood the email addresses with subscribed content. Many subscription services do not ask for verification but if they do these emails can be used as the attack emails. This type of attack is difficult to prevent because the traffic originates from multiple legitimate sources.

ZIP bomb – sending very large compressed archive files to an email address which when decompressed consume available server resources to damage performance.

Attachment – sending multiple emails with large attachments designed to overload the storage space on a server and cause the server to stop responding.

Reply-all – responding “Reply All” to large dissemination lists instead of just to the original sender. This inundates inboxes with a cascade of emails which are compounded by automated replies such as out-of-office messages. These are often accidental in nature. This can also occur when a malicious actor spoofs an email address and the automatic replies are directed toward the spoofed address.

Computing Virus: - Viruses are the malicious and harmful computer programs that infect your system or may harm your contact list are sent as an e-mail attachment and sometimes by downloading a file may also infect your system. Visiting a site sometimes starts an automatic download of virus. They can send spam mails may hijack your browser sometimes disable your security setting and display unwanted ads [7].

Phishing: - It refers to steal information like passwords credit card details username etc. over the internet. It is 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.

SMS Spoofing: -SMS spoofing allow changing name or number text messages appear to come from. SMS spoofing is a technique/activity in which people replace or alter the originating mobile number (Sender ID) of a text message [sent via SMS] to an alphanumeric text of their choice. To put it into simple terms the Sender ID of an SMS message is reset to change who the sender appears to be. Spoofing an SMS message completely changes vital information like sender name phone number or even both simultaneously [8].

Identity Theft: - It simply refers to the fraud or cheats others by making wrong identity of others. It involves stealing money or getting other benefits by pretending to someone else. One common form of cyber crime is identity theft. Hackers and scammers may use fake emails to trick victims into giving up passwords and account information they may use specialized programs called key loggers to track what a user types when logging into bank or credit accounts. Once they have this personal information they may be able to access existing accounts or make purchases with the victim’s credit cards. If a hacker can discover a user’s social security number and other identifying information he can parlay that data into credit accounts in the victim’s name and cause considerable damage.

Internet Fraud: -Internet fraud can occur in chat rooms email message boards or on websites. In internet fraud criminal can send fake info to the victim in case like online purchasing real estate pay BAL work at home donation processing etc. If it sounds too good to be true then it probably is. Such scams fool people a little more than expected even in an age where information is so readily available that we’re expected to be wiser. You might get a message from the bank telling you that a large amount of money has been pre-approved and offered to you as a loan. If you see such a scam you should ask yourself how the bank can readily pre-approve such large amounts of money without first evaluating your financial situation. When it comes to credit cards this kind of scam is becoming more and more popular year on year and is leading to the loss of billions by innocent victims. To avoid being a victim watch your online transactions and accounts closely take advantage of consumer protection services and sign up for credit monitoring for free.

Transaction Fraud:- Simple financial fraud is another common crime in the online arena. A scammer may offer an item for sale through an auction site with no intention of delivering once he receives payment. Alternatively a criminal might purchase an item for sale using a stolen credit card or claim a fraudulent chargeback after receiving the goods.

Preventive Measures to Oppose Cybercrime [4]

<table>
<thead>
<tr>
<th>Reduce Opportunities</th>
<th>Reduce opportunities to the criminals. Develop elaborate system design so that hacker does not hack the computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Authentication Technology</td>
<td>Use password bio-metric devices finger print or voice recognition technology and retinal imaging</td>
</tr>
<tr>
<td>Lay a Trap</td>
<td>Bait a trap to catch the attacker in computer</td>
</tr>
<tr>
<td>Understand Cybercrime</td>
<td>For volume impact and legal challenges. Understand the benefits of proper equipment</td>
</tr>
</tbody>
</table>
5. REFERENCES