Cyber security

Cyber Crime

It refers to all the criminal activities done using medium of communication devices such as computers, mobile phones, tablets, etc.the internet ,cyber space & the world wide web.Cyber crimes are a new class of crimes that is rapidly expanding due to extensive use of internet.

Eg. Phishing cyberstalking, identify theft, etc.

Cyber Law

The law that governs cyber space. It is the term used to describe legal issues related to the use of communication technology, particularly cyber space i.e the internet. It is an attempt to apply laws designed for physical world, to human activity on the internet.

Cyber security

It means protecting equipment, devices, computers, computer resources, communication devices and information stored there in from un-authorized access, use, disclosure, disruption, modification or destructions. The term incorporates both the physical security of devices as well as the information stored there.

Cyber crimes

1. Email spoofing

   A spoofed email is the one that appears to originate from one source but actually has been sent from another source.
2. Spamming

   Spam is the abuse of electronic messaging system to send unsolicited bulk messages indiscriminately.

3. Internet time theft

   Such theft occurs when an unauthorized person uses the internet hours paid for by another person. It comes under hacking because the person who gets access to someone else's ISP users ID and password either by hacking or by gaining access to it by illegal means, uses it to access the internet without the other persons knowledge.
   One can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent.
   The issue of Internet time theft is related to the crimes conducted through "identity theft".

4. Salami attack

   These attacks are used for committing financial crimes. The idea here is to make the alternations so insignificant that in a single case it would go completely unnoticed.
   e.g A bank employee inserts a program into the bank servers, that deducts a small amount of money say Rs.2 from the account of every customer. No account holder will probably notice this unauthorized debit but the bank employee will make a sizable amount every month.

5. Web Jacking

   Web jacking occurs when someone forcefully takes control of the website (by cracking the password and later changing it). Thus the first stage of this crime involves password sniffing. The actual owner of the website doesn't have any more control over what appears on that website.

6. Hacking

   It may be done for the following reasons:

   a. greed
   b. power
   c. publicity
   d. revenge
   e. adventure

   Every act committed towards breaking into a computer and/or network is hacking and it is an offense. Hackers use readymade computer programs to attack or target the computer. They possess the desire to

destruct and they get enjoyment out of such destruciton. Some hackers hack for personal monetary gains such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature.

7. Software Piracy

   Cyber crime investigation cell of India defined software piracy as theft of software through the illegal copying of genuine programs or the counter feiting the distribution of products intended to pass from the original.

e.g a. End users copying friends loaning disks to each other.

b. hard disk loading with elicit means hard disk vendors load pirated software.

c.Counter feiting – large scale duplication and distribution of illegally copied software.

d.Illegal downloads from the internet – by intrusion,by cracking serial number,etc.

Following problems may be faced on buying pirated software.

a. Getting untested software that may have been copied thousands of times over.
b. The software is pirated may contain hard drive infecting viruses.
c. There is no technical support in the case of software failure that is lack of technical product support available to properly licensed users.
d. There is no warranty protection
e. There is no legal right to use the product

8. Email bombing/Mail bomb

   It refers to sending a large number of emails to the victim to crash victims email account in the case of an individual or to make victims mail serves crash in case of a company or an email service providers computer program can be written to instruct a computer to do such tasks on repeated basis by instructing a computer to repeatedly send email to a specified person’s email address. The

cyber criminal can overwhelm the recipients's personal account and potentially shut down the entire system.

9. Usenet newsgroup as a source of cyber crime

   Usenet is a popular means of sharing and distributing information on the web with respect to a specific topic or subject. Usenet is a mechanism that allows sharing information in a many-to-many manners.it is possible to put usenet to the following criminal use :

   A. Distribution or sale of pirated software package
   B. Distribution of hacking software
   C. Sale of stolen credit card number
   D. Sale of stolen data or stolen property.

10. Computer network intrusions:

    Computer networks pose a problem by way of security threat because people can get into them from anywhere. Hackers can break into computer system from anywhere in the world and steal data, plant viruses, create back doors, insert trojan horses or change username/passwords. Network intrusions are illegal but detection and enforcement are difficult. The cracker can bypass existing password protection creating a program to capture login IDs and passwords. The practice of strong password is therefore important.

11. Password sniffing

    Password sniffers are programs that monitor and record the name and password of network users as they login jeopardizing security at a site. Whoever installs the sniffer can then impersonate an authorized user and login to access restricted documents. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using sniffer programs.

12. Credit card frauds

a. Traditional techniques

This is paper based fraud wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally identifiable information to open an account in someone else's name. Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

b. Modern techniques

Sophisticated techniques enable criminals to produce fake and proctored cards. Skimming is also used to commit frauds. Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another. Site cloning and false merchant sites on the internet are becoming a popular method of fraud. Such bogus or fake sites are designed to handover their credit card details without realizing that they have been directed to a fake weblink or website.

How to prevent credit card frauds?

Do's

1) Put your signature on the card immediately upon its receipt.
2) Change the default personal identification number (PIN) received from the bank before doing any transaction.
3) Always carry the details about contact numbers of your bank in case of loss of your card. Report the loss of card immediately in your bank and at the police station if necessary.
4) Ensure the legitimacy of website before providing any of your card details.
5) Preserve all the receipts to compare with credit card invoice.

Dont's

1) Don't store your card numbers and pins in your cell.
2) Don't lend your card to anyone.
3) Don't give out immediately your account number over the phone.
4) Don't leave cards and transactions receipts lying around.

13. Denial of service attack. (DoS attack)

In this type of attack, the attackers floods the bandwidth of the victims network or fills his email box with spam mails depriving him of the services he is entitled to access or provide. The attackers typically target sites or services hosted on high profile webservers such as banks, credit card payment gateways, mobile phone networks. The goal of DoS is not to gain unauthorized access to systems or data but to prevent legitimate users of service from using it.

A DoS attack may do the following:

A. Flood a network with traffic, thereby preventing legitimate network traffic.
B. Disrupt connections between two systems thereby preventing access to a service.
C. Prevent a particular individual from accessing a service.
D. Disrupt service to a specific system or a person.

14. Distributed denial of service attacks (DDoS)

In DDoS attack , an attacker may use your computer to attack another computer by taking advantage of security vulnerabilities or weaknesses.An attacker could take control of your computer.the attacker could take control of your computer. The attacker could then force your computer to send huge amounts of data to a website or send spam to a particular email address. The attack is distributed because the attacker is using multiple computers including yours to launch the DoS attack. A DDoS attack is a distributed DoS wherein a large no of zombie systems are synchronized to attack a particular system.

How to protect from DoS and DDoS ?

a) Implement router filters which can reduce exposure to certain DoS attacks.
b) Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
c) Invest in redundant and fault tolerant network configuration.
d) Establish and maintain regular backup schedule and policies particulary for important configuration information.
e) Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Microsoft windows NT administrator.

15. Password cracking

It is a process of recovering passwords from data that have been stored in/or transmitted by a computer system. It is categorized into

a) Online attack
An attacker can create a script file that will be executed to try each password in a list and when matches an attacker can gain the access to the system. The most common online attack is the Man-in-the-middle attack.it is a form of active eavesdropping in which the attacker establishes a connection between a victim and server to which a victim is connected. When a victim client connects to the fraudulent server the man-in-the-middle server intercepts the call, hashes the password and passes the connection to the victim's server. This type of attack is used to obtain passwords for email accounts on public website such as Gmail, Yahoo and also used to get the password for financial website that would like to gain the access to banking websites.

b) Offline attacks
Offline attacks are mostly performed from a location other than the target(i.e. either a computer system or while on the network) where these passwords reside or are used. Offline attacks usually require

physical access to the computer and copying the password file from the system onto a removable media.

Types of offline password attacks

a. Dictionary attack
   Attempts to match all the words from the dictionary to get the password

b. Brute-force attack
   Attempts all possible permutations and combination of letters, numbers and special characters.

   Guidelines about password policies

   1. Password and user login identities should be unique.
   2. Password should be kept private i.e they should not be shared with friends, colleagues,etc.
   3. Passwords should be changed every 30-45 days or less. Most operating systems can enforce a password with an automatic expiration and prevent repeated or reused passwords.
   4. Users accounts should be frozen after five or less failed logon attempts. All erroneous passwords entries should be recorded in an audit log for later inspection and action as necessary.
   5. Session should be suspended after 15 min or other specified period of inactivity and require the passwords to be re-entered
   6. Login ID's and passwords should be suspended after a specific period of nonuse.
   7. Passwords used previously should not be used while renewing the password.

16. Software Keyloggers

Keystroke logging often called keylogging is the practice of noting (or logging) the keys struck on a keyboard. Keystroke logger or keyloggers is a quicker and easier way of capturing the passwords. Software keyloggers are software programs installed on the computer systems which usually are located in between the OS and the keyboard hardware and every keystroke is recorded. Software keyloggers are

installed on a computer system by trojans or viruses without the knowledge of the users. Cyber criminals always install such tools on the insecure computer systems available in public places (i.e. cybercafes) and can obtain the required information about the victim very easily.

Hardware keyloggers

To install these keyloggers ,physical access to computer system in required. Hardware keyloggers are small hardware devices connected to the PC and /or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cyber criminals install such devices on ATM machines to capture ATM card PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems, hence bank customers are unaware of their presence.

- Anti-keylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.

17. Spyware

Spyware is a type of malware that is installed on computers which collect information about users without their knowledge. The presence of spyware is typically hidden from the users. It is secretly installed on the user's personal computer. Spyware program collect personal information about the victim such as internet surfing habits and the websites visited. Spyware may also have an ability to change computer settings which may result in slowing of the internet connection speed and slowing of response time that may result into user complaining about the internet speed connection with internet service provide.