Cyber Security

Unit 1 – Introduction to cyber crime

Contents

- Computer crime and cyber crime
- Terminologies
  - Cyber space
  - Cyber punk
  - Cyber squatting
  - Cyber warfare
  - Cyber terrorism
  - Cyber Fraud/ computer fraud
- Cyber criminals
- Classification of cyber crimes
- Categories of cyber crime

Introduction to Computer crime

* A crime conducted in which a computer was directly and significantly instrumental is known as "**Computer Crime**".
  * Other Definitions
  - Any threats to the computer itself, such as theft of hardware or software and demands for money.
  - Any financial dishonesty that takes place in a computer environment.

Cyber Crime

Any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them is known as ***cyber crime.***

* Other definitions –
  * Any illegal activity done through the internet.
  * Any criminal activities done using cyberspace and WWW.

Cyber security

* Cyber security means
  * Protecting information
  * Equipment
  * Devices
  * Computers
  * Computer resources
  * Communication device and information stored in all these from unauthorized access, use, disclosure, trouble, modification or destruction.

The first cyber crime

Recorded year :1820
Victim : Joseph- Marie Jacquard (textile manufacture)
Country - France
Device : loom
Type of crime: sabotage (damage)

Cyberspace

- Cyber space is the internet.
  - Definition
    - *Cyberspace is a world wide network of computer networks that uses the TCP/IP for communication to facilitate transmission and exchange of data*
    - Cyber space is most definitely a place where you chat, explore research and play

Cyber squatting

* Cyber squatting is the act of registering a popular Internet address -- usually a company name -- with the intent of selling it to its rightful owner.
  * It generally refers to the practice o
    names that use the names of exist
    the intent to sell the names for a p
    businesses.

Jeff Burgar : the most notorious cybersquatter

Over the years, he has registered hundreds of famous people's names, all of which redirected to his own website Celebrity1000.com. Those include CelineDion.com, MichaelCrichton.com, KevinSpacey.com and one of the most high profile ones was for TomCruise.com, back in 2006.

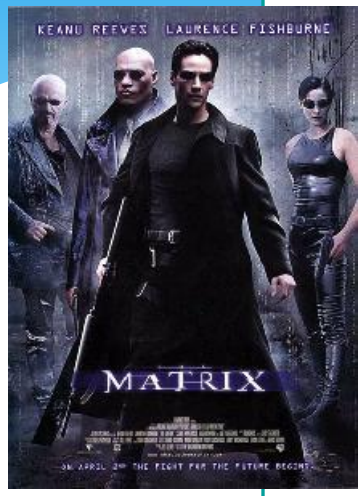
Other examples:

BBC – cyber squatter tried to auction two site named bbc1.com and bbc2.com

Miscrosoft – teenager Mike Rowe set up a website at the domain MikeRoweSoft.com

Cyber punk

* The word “cyber” and “punk” are two different words which means “disorder via machine”.
  * Fast-paced science fiction environment involving innovative computer-based societies
  * Science fiction featuring extensive human interaction with supercomputers and a punk environment .
  * A programmer who breaks into computer systems in order to steal or change or destroy information as a form of cyber-terrorism



Cyber punk movies

- Terminator I, II and III
- Until the end of the world
- Mad MAX I, II and III
- The Matrix (series)
- The X-Files
- Solaris

Cyber warfare

- In 1998, the United States hacked into Serbia's airdefense system to compromise air traffic control and facilitate the bombing of Serbian targets.

- In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.

- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world.

Cyber warfare

* Cyber warfare is information fighters releasing malicious attacks against an unsuspecting opponent's computer network, doing disorder and paralyzing nations.

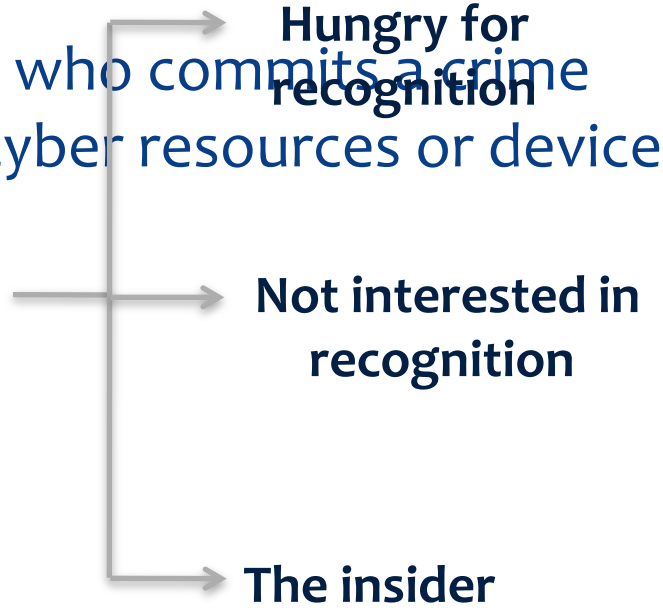
Cyber terrorism

* Cyber terrorism is “any person, group or organization who with terrorist intent, utilizes, accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means and there by knowingly engages in a terrorist act.”

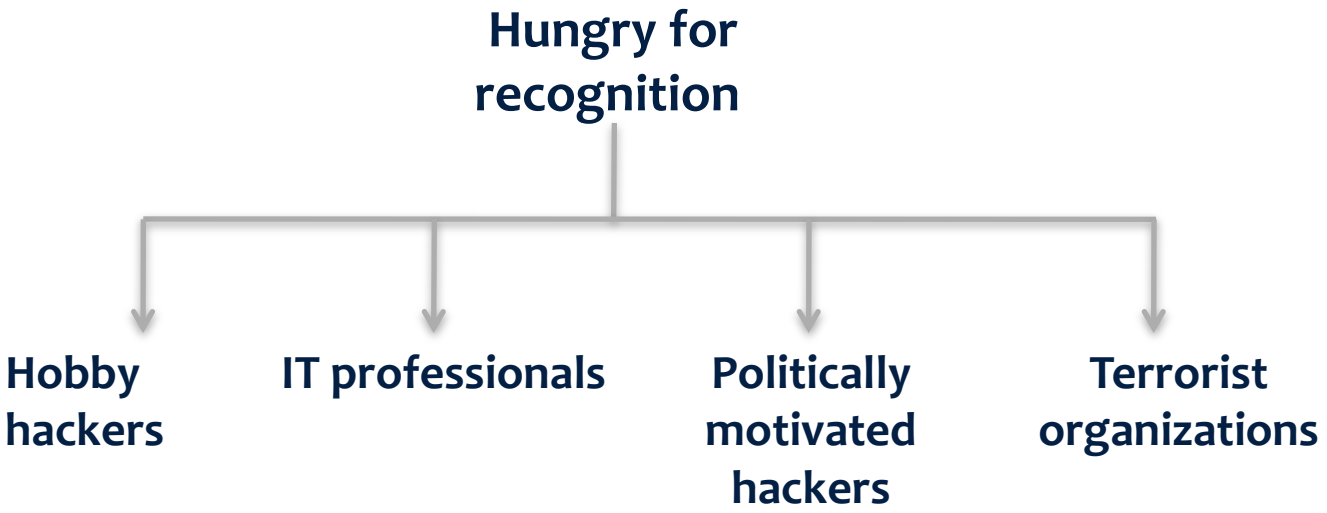
Cyber Criminals

Cyber criminals classification

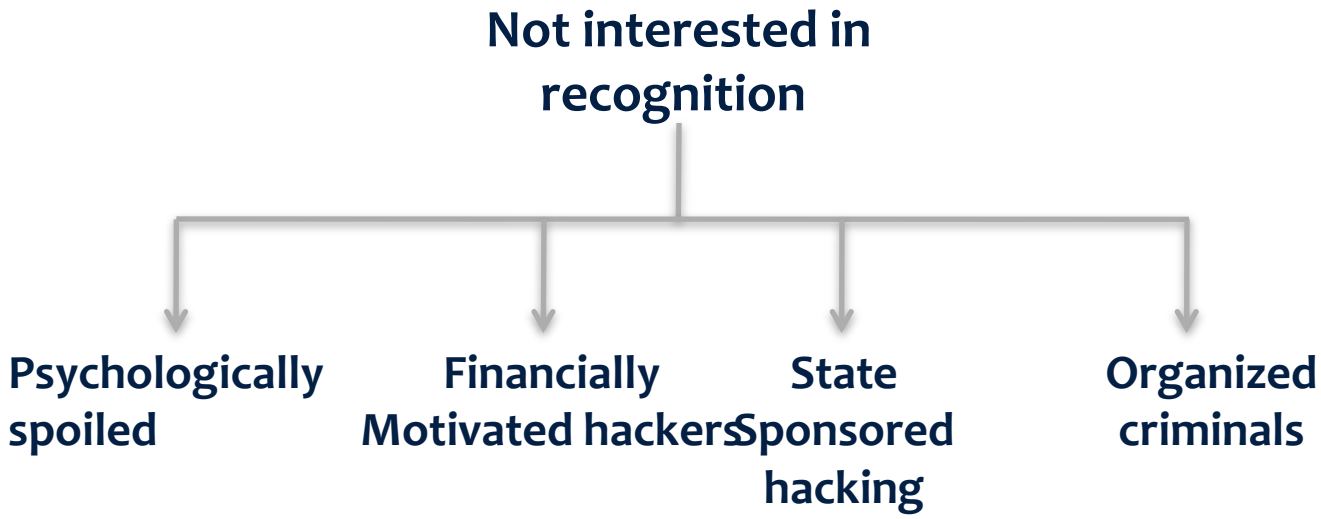
* Cybercriminal is a person who commits a crime through the medium of cyber resources or devices.
  * Type of cyber criminals



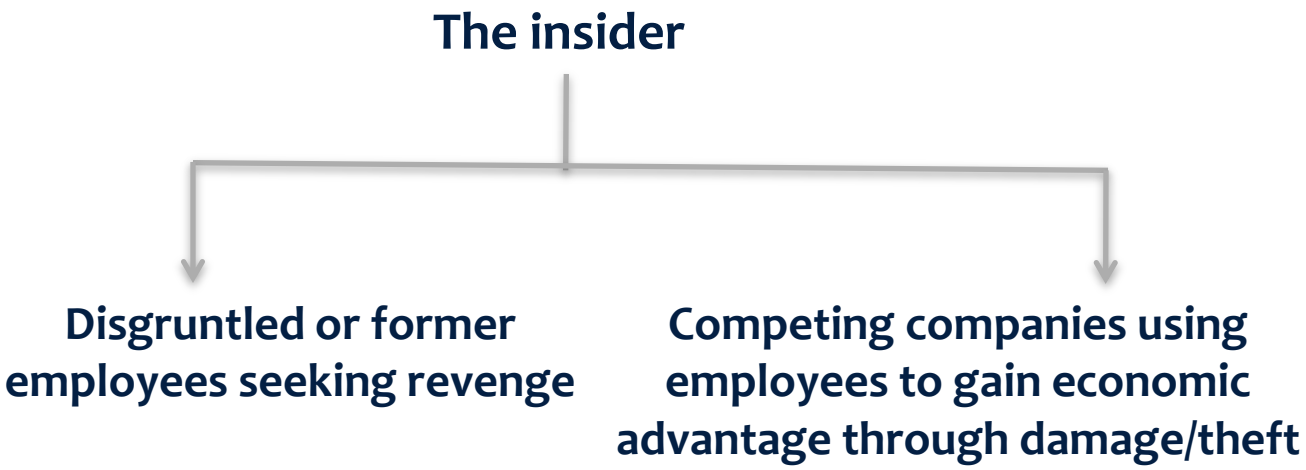
Hungry for recognition



Not interested in recognition



The insider


The insider
Disgruntled or former employees seeking revenge
Competing companies using employees to gain economic advantage through damage/theft

Classification of cyber crimes

I. Cybercrime against **individual**

II. Cybercrime against **property**

III. Cybercrime against **organization**

IV. Cybercrime against **society**

V. Crimes starting from ***Usenet newsgroup***

I. Cybercrime against Individual

* Email spoofing
* Spamming
* Cyber defamation
* Phishing
* Cyber stalking and harassment
* Computer sabotage
* Pornographic offenses (child)
* Password sniffing

Cybercrime against Individual

* Email spoofing
  * A spoofed E-mail is one that appears to originate from one source but actually has been sent from another source.

* Spamming
  * People who create electronic spam are called ***"Spammers"***.
  * Spam is the abuse of e-messaging systems to send unsolicited (unwanted) bulk messages.

    * The another definition of spamming is in the context of "search engine spamming".

Cybercrime against Individual

- To avoid spamming, following web publishing techniques should be avoided.

  - Repeating keywords
  - Use of keywords that do not relate to the content on the site
  - Redirection
  - Duplication of pages with different URLs
  - Hidden links

Cybercrime against Individual

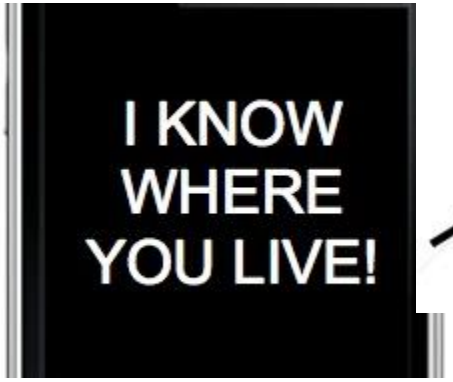
* Cyber defamation
  * **I**ndian **P**enal **C**ode - *Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.*
  * When this takes place in the electronic form, it is cyber defamation.

Cybercrime against Individual - Phishing

Beware of phishing scams.
Don't take the bait! Be suspcious of anyone that asks for your personal information.

Cybercrime against Individual

sn



Cybercrime against Individual

* Computer sabotage
  * Inserting worms, viruses or logic bomb in computer is referred as computer sabotage.
  * Logic bomb is event dependent program created to do something only when a certain event occurs.
  * Example CIH (Chernobyl virus).

Cybercrime against Individual

* Pornographic offenses (child)
  * The internet is being highly used by its abusers to reach and abuse children sexually, worldwide.
  * "*Pedophile*" are people who are sexually attracted to children . They are physically or psychologically forcing minors to engage in sexual activities.

* How do they operate
  * Pedophiles use a false identity to trap the children/teenagers.
  * They seek teens in the kids' areas.
  * They be friend of them.
  * Then they get email address of the child and start making contacts on email too. These emails contains

Cybercrime against Individual

* Password sniffing
  * Password sniffers are programs that monitor and record the name and password of network users as they login.
  * Whoever installs the sniffer can then copy an authorized user and login to access restricted documents.

II. Cybercrime against Property

* Credit card frauds
* Intellectual Property Crime
* Internet time theft

Cybercrime against Property

* Credit card frauds
  * Information security requirements for credit cards have been increased recently.
  * Millions of dollars lost by consumers who have credit card stolen from online database.
* Intellectual property crimes
  * IP crimes include software piracy, copyright infringement, trademarks violation, theft of source

Cybercrime against Property

* Internet time theft
  * Such theft occurs when an unauthorized person uses the Internet hours paid by another person.
  * Basically, internet time theft comes under hacking.

III. Cybercrime against Organization

* Unauthorized accessing of computer
* Password sniffing
* Denial-of-service attacks
* Email bombing
* Salami attack
* Logic bomb
* Trojan Horse
* Data diddling
* Crimes starts from Usenet newsgroup
* Industrial spying
* Computer network disturbance
* Software piracy

Cybercrime against Organization

* Salami Attack/salami Technique
  * These attacks are used for committing financial crimes.
  * The main idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed.
* Data diddling

* Industrial Spying

  * The internet and privately networked systems provide new and better opportunities for spying.
  * “Spies” can get information about product finances, research and development and marketing strategies.
  * This activity is known as **“industrial spying”**.

* Software Piracy
  * This the “The Biggest” challenge area.
  * Software piracy is “*theft of software through the illegal copying of genuine programs or the fake program and distribution of products intended to pass for the original*”.

* Disadvantages
  * The software, if pirated, may potentially contain hard-drive infection virus.
  * There is no technical support in the case of software failure.
  * There is no warranty protection

  * There is no legal right to use the product

* Email bombing
  * It refers to sending a large number of e-mails to the victim to crash victim's email account or to make victim's mail server crash.
* Computer Network intrusions
  * Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, insert trojan horses or change user names and

IV. Cybercrime against Society

* Forgery
* Cyberterrorism
* Web jacking

Cybercrime against Society

* Forgery
  * Fake currency notes, postage and revenue stamps, mark sheets can be forged using sophisticated computers, printers and scanners.

Cybercrime against Society

* Web jacking
  * Web jacking occurs when someone forcefully takes control of a website.
  * First stage of this crime involves “password sniffing”.

Usenet newsgroup

* Usenet is a mechanism that allows sharing information in a many-to-many manner.

* Usenet mainly used for following crime :
  * Distribution/sale of pornographic material
  * Distribution/sale of pirated software
  * Distribution of hacking software
  * Sale of stolen credit card number
  * Sale of stolen data

Categories of cyber crime

* Cybercrime is categorized based on the following
  1. The target of crime
  2. Whether the crime occurs as a single event or series of events

  * Single event
    * Single event from the perspective of a victim like opening mails with virus attachments infect the system immediately.
  * Series of events
    * Involves attacker interacting with the victim repeatedly. Ex. cyber stalking, harassment, defamation, etc