AKTU

CYBER SECURITY

BCC-301 (3rd Sem)
BCC-401 (4th Sem)

Unit :-1

INTRODUCTION TO CYBER CRIME

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

B.Tech 2nd Year Common Courses

(Effective from session 2023-24)

- **BCC301 / BCC401/ BCC301H / BCC401H: Cyber Security**
- **BCC302 / BCC402/ BCC302H / BCC402H : Python programming**

BCC301 / BCC401/ BCC301H / BCC401H:
CYBER SECURITY

Course Outcome (CO)		Bloom's Knowledge Level (KL)
At the end of course , the student will be able to		
CO 1	Understand the basic concepts of cyber security and cybercrimes.	K_1, K_2
CO 2	Understand the security policies and cyber laws.	K_1, K_2
CO 3	Understand the tools and methods used in cyber crime	K_2
CO 4	Understand the concepts of cyber forensics	K_1, K_2
CO 5	Understand the cyber security policies and cyber laws	K_2

DETAILED SYLLABUS

Unit	Topic	Lecture
I	**INTRODUCTION TO CYBER CRIME :** Cybercrime- Definition and Origins of the word Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyber offenses: How Criminals Plan the Attacks, Social Engineering, Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector.	04
II	**CYBER CRIME :** Mobile and Wireless Devices-Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era.	04
III	**TOOLS AND METHODS USED IN CYBERCRIME :** Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft).	04

IV	**UNDERSTANDING COMPUTER FORENSICS:** Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation. Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics.	**04**
V	**INTRODUCTION TO SECURITY POLICIES AND CYBER LAWS :** Need for An Information Security Policy, Introduction to Indian Cyber Law, Objective and Scope of the Digital Personal Data Protection Act 2023, Intellectual Property Issues, Overview of Intellectual Property Related	**04**

	Legislation in India, Patent, Copyright, Trademarks.	

Text books:

1. Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81- 265-21791, Publish Date 2013.
2. Basta, Basta, Brown, Kumar, Cyber Security and Cyber Laws, 1st edition , Cengage Learning publication
3. Dr. Surya PrakashTripathi, RitendraGoyal, Praveen Kumar Shukla, KLSI. "Introduction to information security and cyber laws". Dreamtech Press. ISBN: 9789351194736, 2015.
4. Cyber Security and Date Privacy by Krishan Kumar Goyal , Amit Garg , Saurabh Singhal , HP HAMILTON LIMITED Publication, ISBN-13-978-1913936020
5. Thomas J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing
6. Investigating Intrusions", Copyright © 2014 by John Wiley & Sons, Inc, ISBN: 978 - 1-118 -84965 -1.
7. James Graham, Ryan Olson, Rick Howard, "Cyber Security Essentials", CRC Press, 15-Dec 2010.
8. Anti- Hacker Tool Kit (Indian Edition) by Mike Shema, McGraw-Hill Publication.

What is cybercrime?

Cybercrime is any criminal activity that involves a computer, networked device or a network.

Who are The Cybercriminals?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams.

Cybercriminals are widely available in what is called the “Dark Web” where they mostly provide their illegal services or products.

What is Cyber Crime?

- A generalized definition of cyber crime may be "*unlawful acts wherein the computer is either a tool or target or both*"
- The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking
- The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, Trojan attacks, internet time thefts, theft of computer system, physically damaging the computer system

Origins of the Word

The term “cybercrime” relates to a number of other terms such as:

- *Computer-related crime*
- *Computer crime*
- *Internet crime*
- *E-crime*
- *High-tech crime*

The word “Cybercrime” was first coined in **1982** by William Gibson but it gained popularity in 1984 through his novel 'Neuromancer'.

Akash Arora (1999) was one of the earliest examples of cybercrime in India. (Yahoo Case)

Information Security

- Information is a valuable assets. Security of information is a critical issue which must be addressed properly. Nowdays everyone is dependent on information for personnel as well as professional activities.
- The concept of information security involve maintenance of confidentiality, integrity and availability of information security.

- Information Security focuses on protection of information including confidentiality, integrity, and availability, and includes a variety of protection mechanisms such as policy, training and awareness programs, and technology.

CIA Triad

- **Confidentiality** refers to the protection of information from unauthorised access.
- **Integrity** refers to insurance that information is trustworthy and accurate it protect against unauthorised modification.
- **Availability** means only authorised users should be able to access the information wherever needed.

Who are Cybercriminals?

Cybercriminals are those who conduct activities such as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts.

1. **Type I: Cybercriminals – hungry for recognition**
2. **Type II: Cybercriminals – not interested in recognition**
3. **Type III: Cybercriminals – the insiders**

Types of Cybercrime

We can categories these crimes in given types –

1. Crime against Individual [phishing, spamming, password sniffing, spoofing, cyber stalking, identity theft, data diddling]
2. Crime against property [Credit & debit card fraud, intellectual property theft]
3. Crime against society [Cyber terrorism, child pornography, wed jacking]

Cyber crimes can be categorized based on their targets.

CRIME AGAINST INDIVIDUAL

1. Phishing

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.

Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

2. Spamming

Spamming is the use of messaging systems to send an unsolicited message to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose.

3. Password sniffing

A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

4.Spoofing

An example of spoofing is when an email is sent from a false sender address, that asks the recipient to provide sensitive data. This email could also contain a link to a malicious website that contains malware.

5. Cyberstalking

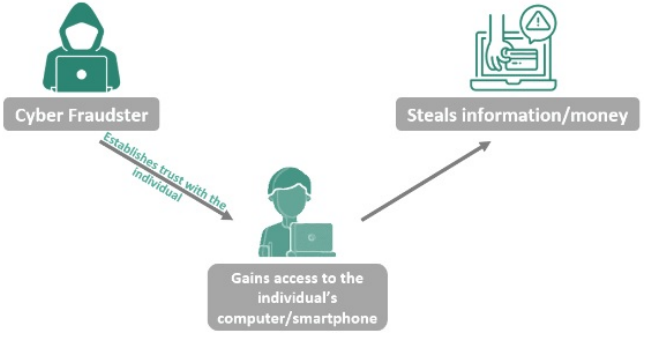
Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. Cyberstalking is stalking or harassment carried out over the internet. It might target individuals, groups, or even organizations and can take different forms including slander, defamation and threats.

6. Identity theft

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964.

7. Data diddling

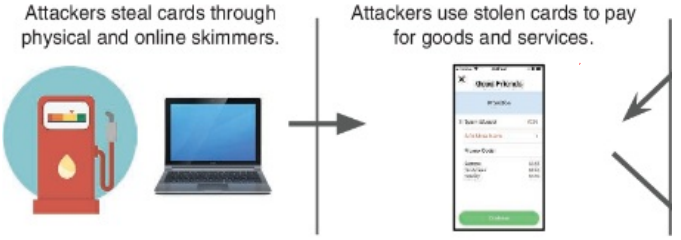
Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus. Computerized processing of the altered data results in a fraudulent benefit.

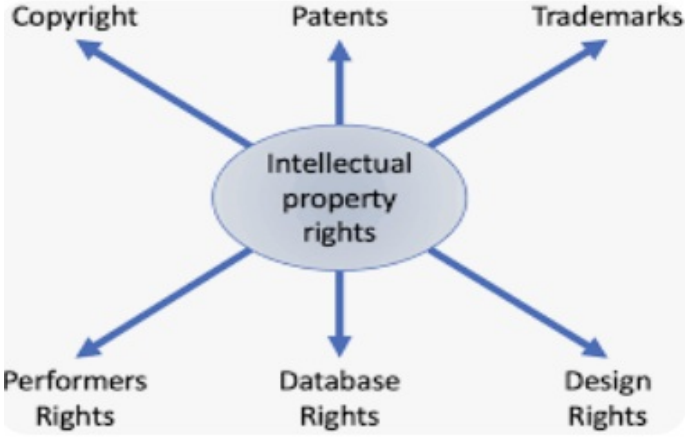


CRIME AGAINST PROPERTY

1. Credit card fraud

Credit and debit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.





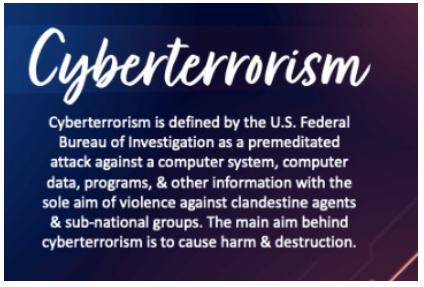
2. Intellectual property theft

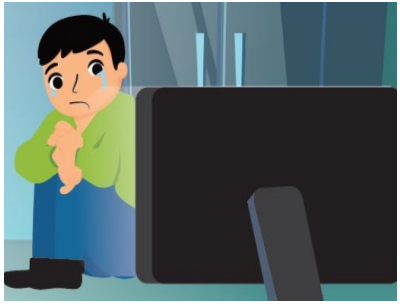
Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions—known as "intellectual property"—which can include everything from trade secrets and proprietary products and parts to movies, music, and software.

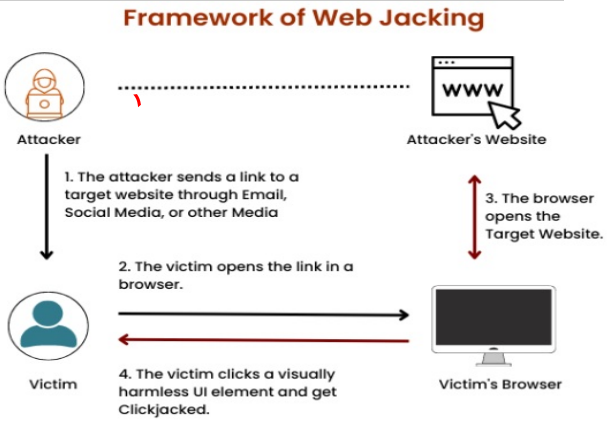
CRIME AGAINST SOCIETY

1. Cyber terrorism

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.







2. Child pornography

If you see sexually explicit images or videos of minors on the web.

3. Web jacking

Web jacking is simply when someone clones your website, and tricks you to believe the cloned site is yours. The malicious link is placed somewhere on your webpage waiting for a click. Immediately, you click on it; a malicious web server replaces it. And that means you have lost complete access to your website.

Cyber – Crime : A Global Perspective

Cybersecurity constitutes one of the top five risks of most firms, especially in Big Tech and Banking & Financial Services. A weekend reading led to some interesting data points from various sources such as AV-Test and Coveware, among others, and that further led to me pondering over the mitigating actions that we can take as individuals and as organisations for some, if not all, of these cybercrime risks. I extend my thanks to the respective experts who shared their knowledge, enabling me to piece together some parts of the larger jigsaw puzzle.

According to the 2020 Cost of Cybercrime Study by Accenture, the average number of security breaches experienced by organizations increased by 11% between 2018 and 2019. **Cybercrime is also becoming more sophisticated, with the emergence of new threats such as ransomware and advanced persistent threats (APTs)**

Global cybercrime damage costs this year are expected to breach US $6 trillion an annum. That is almost one-fourth of the US GDP or twice the GDP of India. This is expected to scale up to US $10.5 trillion an annum by 2025. Cyber attackers are disrupting critical supply chains, at least 4 times more than in 2019.

In conclusion, cybercrime is a growing global issue that requires a concerted effort from individuals, businesses, and governments to prevent and mitigate its impact. By raising awareness about the risks of cybercrime and implementing effective prevention measures, we can help to ensure that the internet remains a safe and secure place for everyone.

A Global Perspective on Cybercrimes

- In Australia, cybercrime has a narrow statutory meaning as used in the *Cyber Crime Act* 2001, which details offenses against computer data and systems.
- In the Council of Europe's (CoE's) *Cyber Crime Treaty*, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses.
- Recently, there have been a number of significant developments such as

  1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime.

  2. In August 18, 2006, there was a news article published "ISPs Wary About 'Drastic Obligations' on Web Site Blocking."

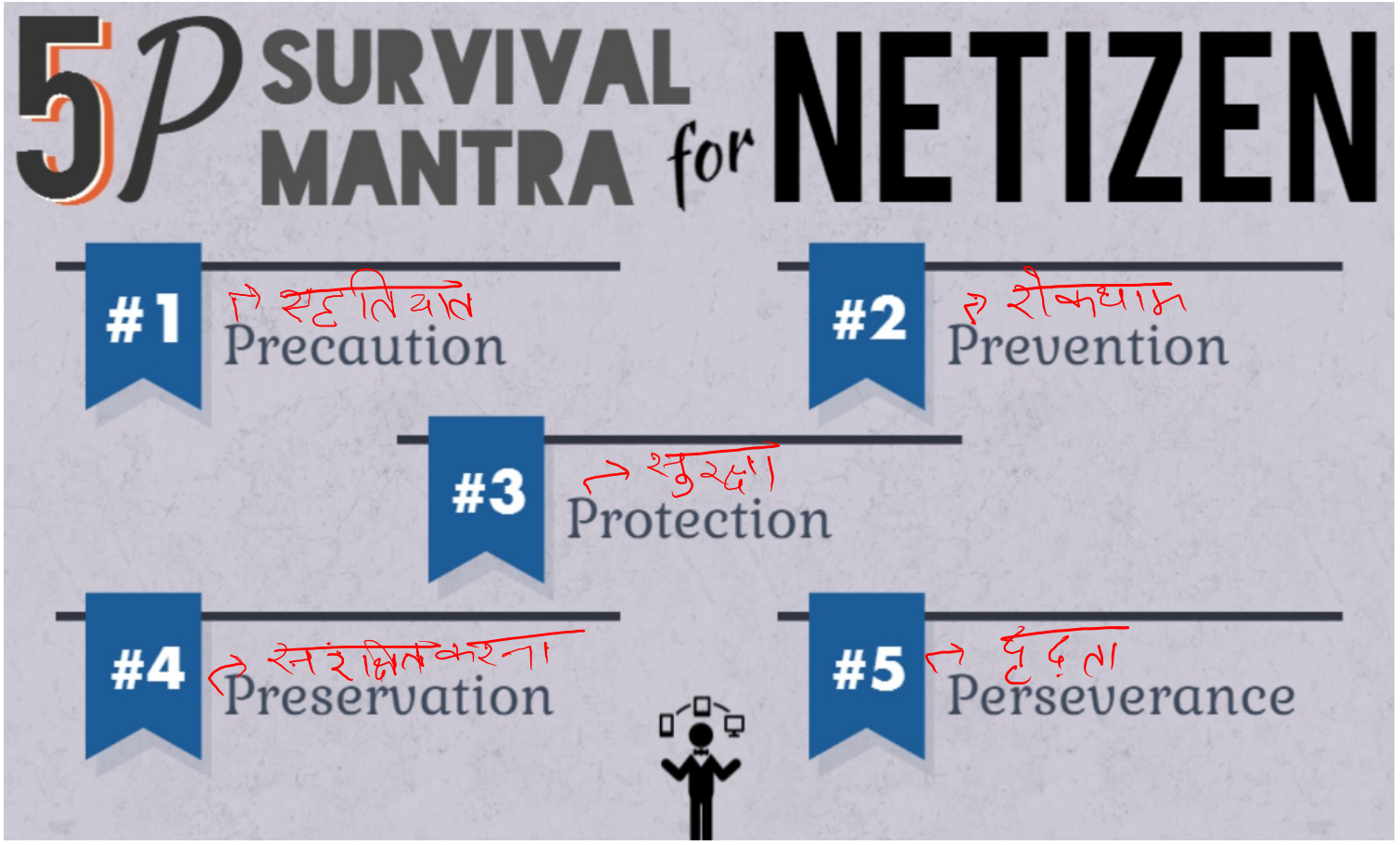
  3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.

Cybercrime Era: Survival Mantra for the Netizens

Cybercrime Era: Survival Mantra for the Netizens

Netizen

- Netizen is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms).
- The 5P Netizen mantra for online security is: (a) Precaution, (b) prevention, (c) Protection, (d) Preservation and (e) Perseverance.
- For ensuring cybersafety, the motto for the "Netizen" should be "Stranger is Danger!"


5P SURVIVAL MANTRA for NETIZEN
#1 Precaution
सतर्कता
#2 Prevention
रोकथाम
#3 Protection
सुरक्षा
#4 Preservation
संरक्षित करना
#5 Perseverance
दृढ़ता

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

How Criminals Plan Them–Introduction

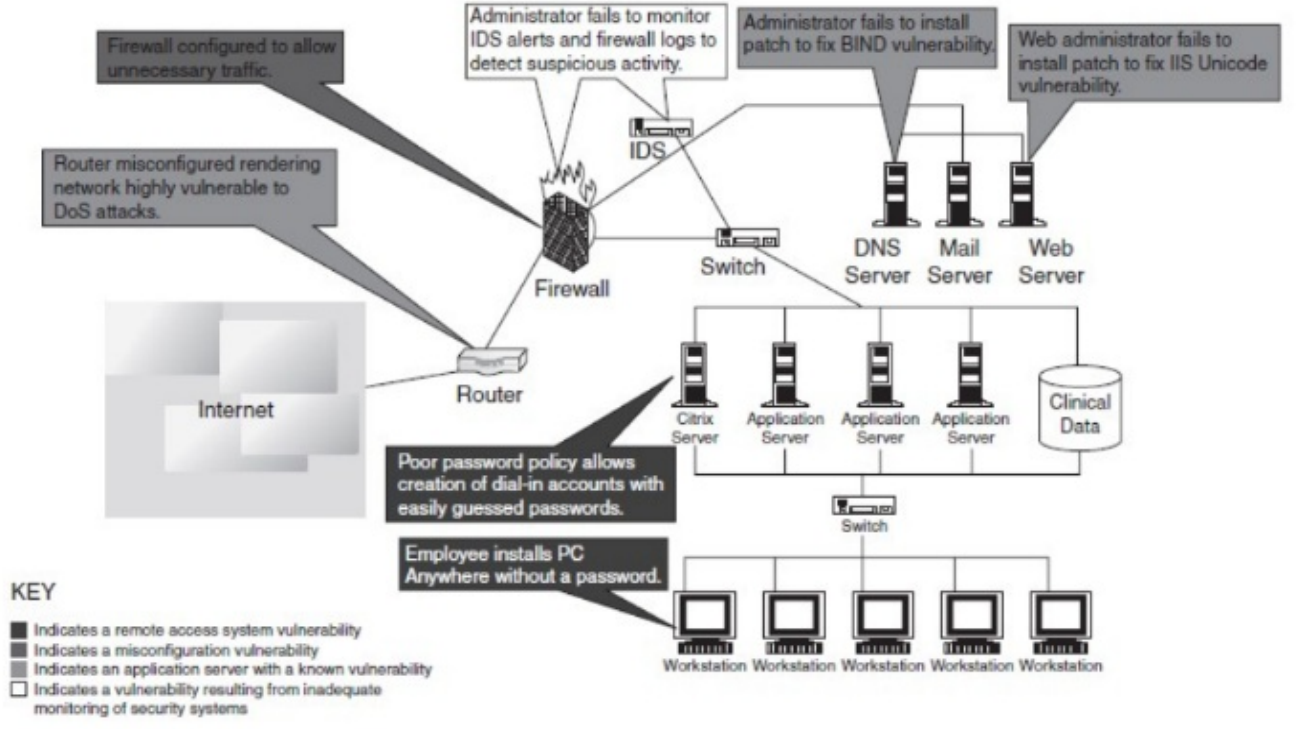
- Technology is a "double-edged sword "as it can be used for both good and bad purposes.
- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter1 provided an over view of *hacking*, *cyber terrorism*, *network intrusions*, *password sniffing*, *computer viruses*, etc. They are the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyber laws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as "Crackers"(Box2.1).

2.2 HowCriminalsPlantheAttacks

- Criminals use many methods and tools to locate the vulnerabilities of their target.
- The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- **Active attacks** are usually used to alter the system (i.e.,computer network) where as **passive attacks** attempt to gain information about the target.
- **Active attacks** may affect the availability, integrity and authenticity of data where as **passive attacks** lead to violation of confidentiality.

Box2.1|Hackers,CrackersandPhreakers
Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who Breaks into computers (refertoBox2.2).
Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force Hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.
Cracker: A cracker is a person who breaks into computers .Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their Crimes include vandalism, theft and snooping in unauthorized areas.
Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the
Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines(called "phreaking").These sites usually display warnings such as "These files are illegal; we are not responsible for what you do with them."
Cracker tools: These are programs used to break into computers. Cracker tools are widely Distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.
Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.
War dialer: It is program that automatically dials phone numbers looking for computers on the Other end. It catalogs numbers so that the hackers can call back and try to break in.

- An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.
- The categories of vulnerabilities that hackers typically search for are the following:
  1. Inadequate border protection(border as in the sense of network periphery);
  2. Remote access servers (RASs)with weak access controls;
  3. Application servers with well-known exploits;
  4. Misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig.2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.



Box2.2 |WhatColorisYour Hatin theSecurity World?

A ***black hat*** is also called a "cracker" or "dark side hacker." Such a person is a malicious or **criminal hacker**. Typically, the term "cracker" is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

A ***white hat hacker*** is considered an ***ethical hacker***. In their aim of IT, a "white hat hacker" is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cow boy hat and the antagonist typically wore a black one. As a simplified explanation, a "white hat" generally focuses on securing IT systems, whereas a "black hat" (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A ***brown hat hacker*** is one who thinks before acting or committing a malice or non-m alice deed. *A grey hat* commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

2.3 Social Engineering

- Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.
- The goal of a social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on…

Box2.6|Social Engineering Example
Mr. Joshi: Hello? **The Caller:** Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few users home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.
Mr. Joshi: Ohh… okay. I will beat my home by then, anyway. **Caller:** Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?
Mr. Joshi: Username is "p joshi. " None of my files will be lost in the move, right? **Caller:** No sir. But we will have to check your account to ensure the same. What is the password of that account?
Mr. Joshi: My password is "ABCD1965," all characters in upper case. **Caller:** Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.
Mr. Joshi: Thank you. Bye. **Caller:** Bye and have a nice day.

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. **Impersonating an employee or valid user:**
   - "Impersonation" is perhaps the greatest technique used by social engineers to deceive people.
   - Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.
2. **Posing as an important user:**
   - The attacker pretends to be an important user– for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
   - The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

3. **Using a third person:**
   - An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
4. **Calling technical support:**
   - Calling the technical support for assistance is a classic social engineering example.
   - Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.
5. **Shoulder surfing:**
   - It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
6. **Dumpster diving:**
   - It involves **looking in the trash for information written on pieces of paper or computer printouts**.
   - This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
   - It is also called dumpstering, binning, trashing, garbing or garbage gleaning.
   - "Scavenging" is another term to describe these habits.
   - In the UK, the practice is referred to as "binning" or "skipping" and the person doing it is a "binner" or a "skipper."

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.
- For example, sending a **fake E-Mail to the user** and asking him/her to re-enter a password in a webpage to confirm it.

1. **Fake E-Mails:**

- The attacker sends fake E-Mails (seeBox2.7)to users in such that the user finds it as a real e-mail.
- This activity is also called "Phishing".
- It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as **usernames, passwords** and **credit card details** by impersonating as a trustworthy and legitimate organization or an individual.
- Banks, financial institutes and payment gateways are the common targets.
- Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website.
- Thus, Phishing is also an example of social engineering techniques used to fool netizens.
- The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails attract to *fish* for passwords and financial data from the sea of Internet users (i.e., netizens).
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

2. **E-Mail attachments:**

- E-mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., key logger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

3. **Pop-up windows:**

- Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

2.4 Cyber stalking

- The dictionary meaning of "stalking" is an "*act or process of following prey stealthily– Trying to approach somebody or something.*"
- Cyber stalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to **harass another individual, group of individuals, or organization**.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- **It involves harassing or threatening behavior that an individual will conduct repeatedly**, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyber stalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. **Online stalkers:**
   - They aim to start the interaction with the victim directly with the help of the Internet.
   - E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
   - The stalker makes sure that the victim recognizes the attack attempted on him/her.
   - The stalker can make use of a third party to harass the victim.

2. **Offline stalkers:**
   - The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
   - Searching on message boards/news groups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
   - The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyber stalking

- The majority of cyber stalkers are men and the majority of their victims are women.
- Some cases also have been reported where women act as cyber stalkers and men as the victims as well as cases of same-sex cyber stalking.
- In many cases, the cyber stalker and the victim hold a prior relationship, and the cyber stalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor.
- However, there also have been many instances of cyber stalking by strangers.

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details(telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone numbers), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to in numerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

2.4.4 Real-Life Incident of Cyber stalking

Case Study
The Indian police have registered first case of cyber stalking in Delhi–the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved,
• Mrs. Joshi received almost 40 calls in 3days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad.
• The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.
• A person was using her ID to chat over the Internet at the website www.mirc.com,mostly in the Delhi channel for four consecutive days.
• This person was chatting on the Internet, using her name and giving her address, talking in obscene language.
• The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.
• This was the first time when a case of cyber stalking was registered.
• Cyber stalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another Person using Internet and other forms of online communication channels as medium.

2.5 Cyber café and Cyber crimes

- In February 2009, Nielsen survey on the profile of cyber cafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and post graduates, though almost over 50% were students.
- Hence, it is extremely important to understand the IT security and governance practiced in the cyber cafes.
- In the past several years, many instances have been reported in India, where cyber cafes are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cyber cafes.
- Cyber cafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cyber cafes, hold two types of risks.

Here are a few tips for safety and security while using the computer in a cyber cafe:

1. Always logout:

2. Stay with the computer:

3. Clear history and temporary files:

4. Be alert:

5. Avoid online financial transactions:

6. Change passwords:

7. Use Virtual keyboard:

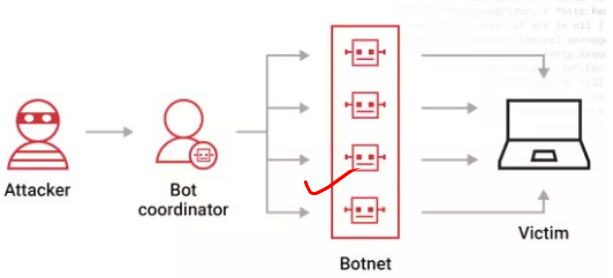
8. Security warnings:

2.6 Botnets:TheFuelforCybercrime

2.6.1 Botnet

- The dictionary meaning of Bot is "(*computing*) *an automated program for doing some particular task, often over a network.*"

- Bot net is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program one can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system may be a part of a Bot net even though it appears to be operating normally.
- Bot nets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service(DoS) attacks
- A Bot net(also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "*Zombie networks*" have become a source of income for entire groups of cyber criminals.



One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date:
2. Set the OS to download and install security patches automatically:
3. Use a fire wall to protect the system from hacking attacks while it is connected on the Internet:

   A fire wall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.

4. Disconnect from the Internet when you are away from your computer:
5. Downloading the free ware only from websites that are known and trustworthy:
6. Check regularly the folders in the mail box– "sent items" or "outgoing"–for those messages you did not send:
7. Take an immediate action if your system is infected:

Box2.9|Technical Terms
Malware: It is malicious *software*, designed to damage a computer system without the owner's Informed consent. Viruses and worms are the examples of malware.
Adware: It is *advertising-supported software*, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.
Spam: It means unsolicited or undesired E-Mail messages
Spam dexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods

2.7 Attack Vector

- **An "attack vector" is a path**, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- **Attack vectors** enable attackers to exploit system vulnerabilities, including the human element.
- **Attack vectors** include viruses, E-Mail attachments, web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.