INTRODUCTION TO CYBER SECURITY

(BETCK105/205 I)

NOTES

For First/Second Semester B.E[VTU/CBCS, 2023-2024] Syllabus

Syllabus

Course Title: Introduction to Cyber Security **Course Code: :** BETCK105I/205

MODULE-I	Teaching Hours
Introduction to Cybercrime: Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global PerspectivesTextbook:1 Chapter 1 (1.1 to 1.5, 1.7-1.9)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-II	**Teaching Hours**
Cyber Offenses: How Criminals Plan Them: Introduction, How criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercafe & cybercrimes. Botnets: The fuel for cybercrime, Attack Vector. Textbook:1 Chapter 2 (2.1 to 2.7)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-III	**Teaching Hours**
Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spyways, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attackes, Attacks on Wireless networks. Textbook:1 Chapter 4 (4.1 to 4.9, 4.12)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	
MODULE-IV	**Teaching Hours**
Phishing and Identity Theft: Introduction, methods of phishing, phishing, phising techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft Textbook:1 Chapter 5 (5.1. to 5.3)	**8**
Blooms Taxonomy: L1 – Remembering , L2 – Understanding	
MODULE-V	**Teaching Hours**
Understanding Computer Forensics: Introdcution, Historical Background of Cyberforensics, Digital Foresics Science, Need for Computer Foresics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics. Textbook:1 Chapter 7 (7.1. to 7.5, 7.7 to 7.9)	**8**
Blooms Taxonomy: L1 – Remembering, L2 – Understanding	

SL No	Title Of The Book	Name Of the Author/s	Name Of the Publisher	Edition and Year	ISBN
1	, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”	Sunit Belapure and Nina Godbole	Wiley India Pvt Ltd	First Edition (Reprinted 2018)	978-81- 265-21791, 2011,

MODULE 1. INTRODUCTION TO CYBERCRIME

List of Topics:

- Introduction
- Cybercrime: Definition and Origins of the Word
- Cybercrime and Information Security
- Who are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspective
- Cybercrime and the Indian ITA 2000
- A Global Perspective on Cybercrimes
- Cybercrime Era: Survival Mantra for the Netizens

INTRODUCTION

- **"**Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks**"**.
- **"**Cybersecurity**"** means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- Almost everyone is aware of the rapid growth of the Internet.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomena; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend

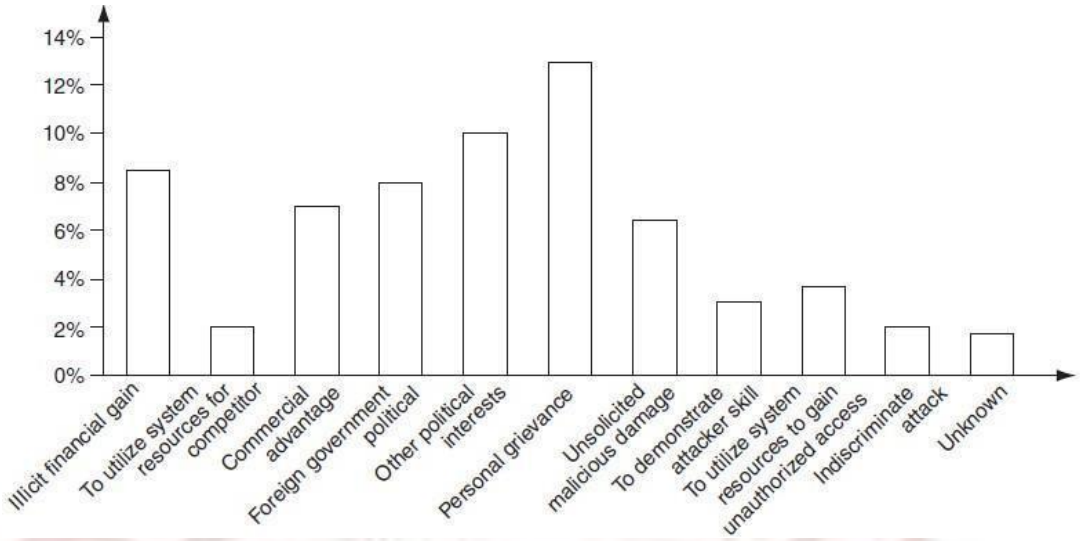

Figure: Cybercrime Trend

- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

Definition:

"A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime."

Alternative definitions of Cybercrime are as follows:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.

4. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.
5. "Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime. The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security, cybercrime is any criminal activity which uses network access to commit a criminal act. Cybercrime may be internal or external, with the former easier to perpetrate. The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. Cybercrime refers to the act of performing a criminal act using cyberspaceas the communications vehicle.

Some people argue that a cybercrime is not a crime as it is a crime against software & not against a person (or) property. However, while the legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:

1. Techno-crime: A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving

few, if any, "finger prints".

2. Techno-vandalism: These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud"; both are punishable. Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways:

a. how to commit them is easier to learn,
b. they require few resources relative to the potential damage caused,
c. they can be committed in a jurisdiction without being physically present in it &
d. they are often not clearly illegal.

Important Definitions related to Cyber Security:

Cyberterrorism:

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

(or)

Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, utilizesaccesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism."

Cybernetics:

Cybernetics deals with information and its use. Cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation. Worldwide, including India, cyberterrorists usually use computer as a tool, target for their unlawful act to gain information.

Internet is one of the means by which the offenders can gain priced sensitive information of companies,

firms, individuals, banks and can lead to intellectual property (IP) crimes, selling illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

Phishing:

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment.

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain & other fraudulent activities.

(or)

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords, credit card information from users etc.

Cyberspace:

This is a term coined by William Gibson, a science fiction writer in 1984. Cyberspace is where users mentally travel through matrices of data. Conceptually, cyberspace is the nebulous place where humans interact over computer networks. The term “cyberspace” is now used to describe the Internet and other computernetworks. In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. Cyberspace is most definitely a place where you chat, explore, research and play.

Cybersquatting:

The term is derived from “squatting” which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.

Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. This term is explained herebecause, in a way, it relates to cybercrime given the intent of cybersquatting.

Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying "domain names" that have existing businesses names.

In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with "Uniform Dispute Resolution Policy" (a contractual obligation to which all domain name registrants are presently subjected to).

Cyberpunk:

This is a term coined by Bruce Bethke, published in science fiction stories magazine in November 1983. According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement."

Cyberwarfare:

Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. These type of Cyber attacks are often presented as threat to military forcesand the Internet has major implications for espionage and warfare.

CYBERCRIME AND INFORMATION SECURITY

Lack of information security gives rise to cybercrimes. Let us refer to the amended Indian Information Technology Act (ITA) 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides a new focus on "Information Security in India". "Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.

Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data),

often some difficulty is faced in estimating the losses because the financial impacts may not be detectedby the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Surveyon computer crime and security supports this. Cybercrimes occupy an important space in information security domain because of their impact. The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (through loss/theft of laptops).

Because of these reasons, reporting of financial losses often remains approximate. In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about **"**security incidents**"** including cybercrime. In general, organizations perception about **"**insider attacks**"** seems to be different thanthat made out by security solution vendor. However, this perception of an organization does not seem to be trueas revealed by the 2008 CSI Survey. Awareness about **"**data privacy**"** too tends to be low in most organizations. When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such **"**crimes**"** may not be detected by the victimized organization and no direct costs may be associated with the theft

Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11

Figure: Cybercrime trend over the years

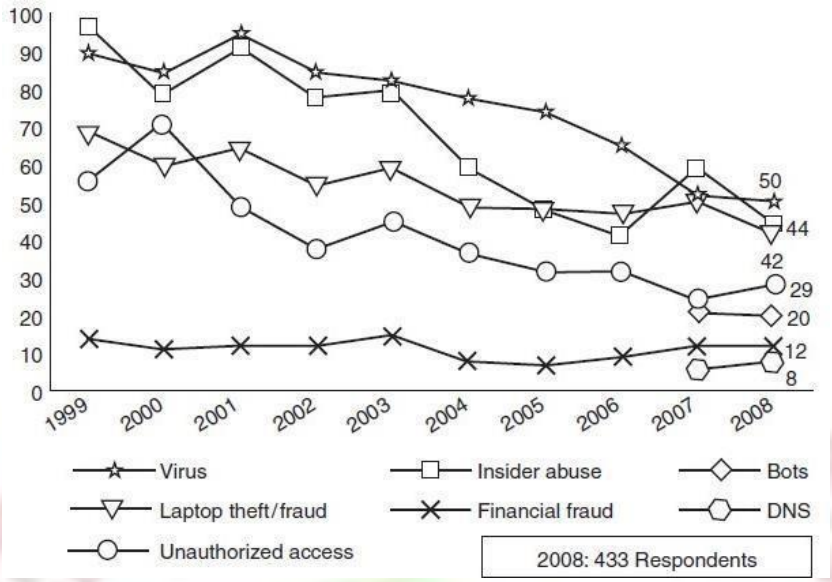

Figure: shows several categories of incidences – viruses, insider abuse, laptop theft and unauthorized access to systems

The Botnet Menace:

A group of computers that are controlled by software containing harmful programs, without their users' knowledge is called as **Botnet**. The term "Botnet" is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Below figure shows how a "zombie" works.