Vidyalankar Institute of Technology

Electronics & Telecommunication Department

Orientation Program : Academic Year 2024– 2025

Subject: ILO1016 - Cyber Security and Laws

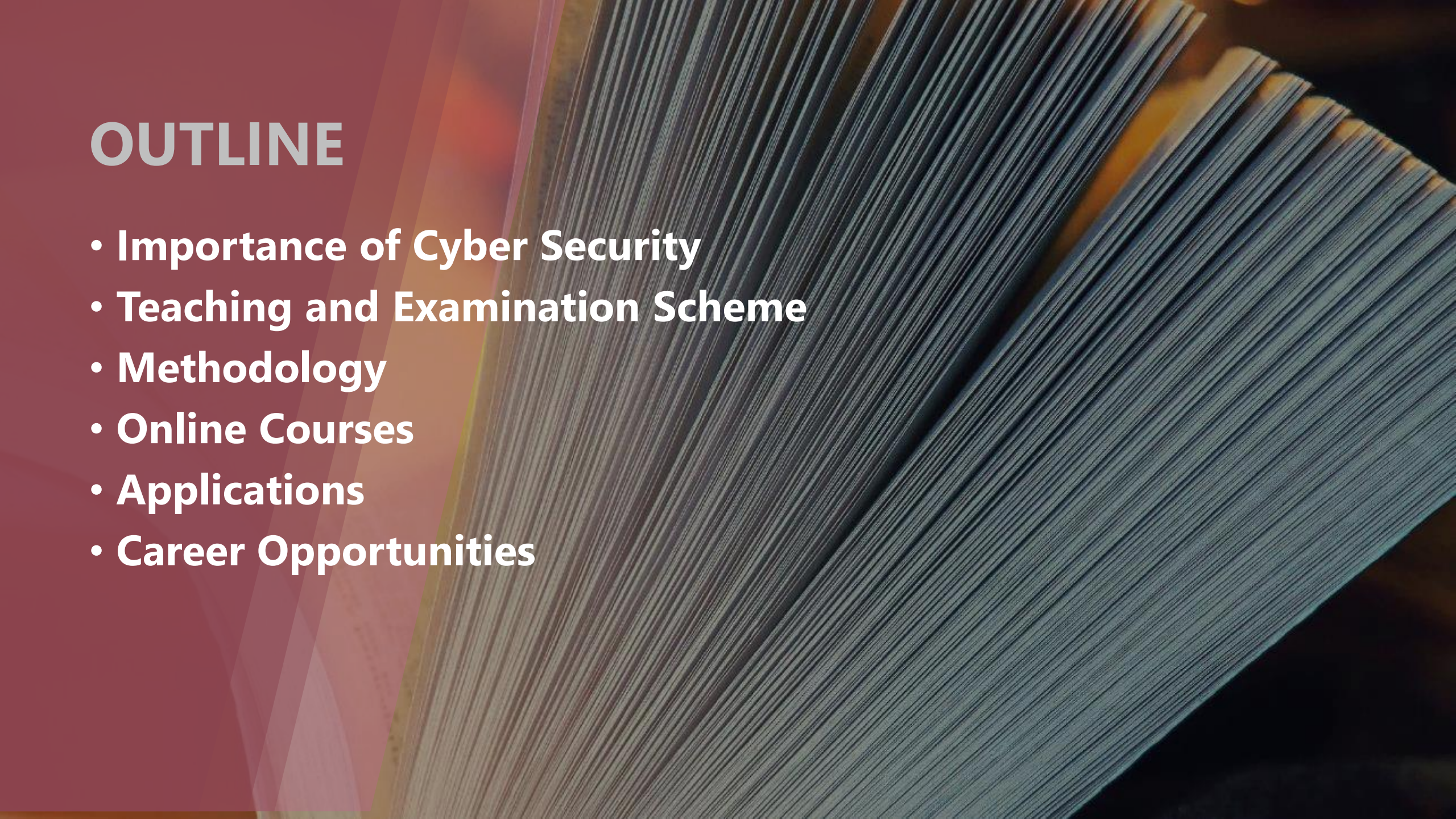
Semester: VII

VIT | Vidyalankar Institute of Technology
Accredited A+ by NAAC

Subject Teacher
Prof. Harshada Rajale

OUTLINE

- Importance of Cyber Security
- Teaching and Examination Scheme
- Methodology
- Online Courses
- Applications
- Career Opportunities



1.Importance of Cyber Security and Laws

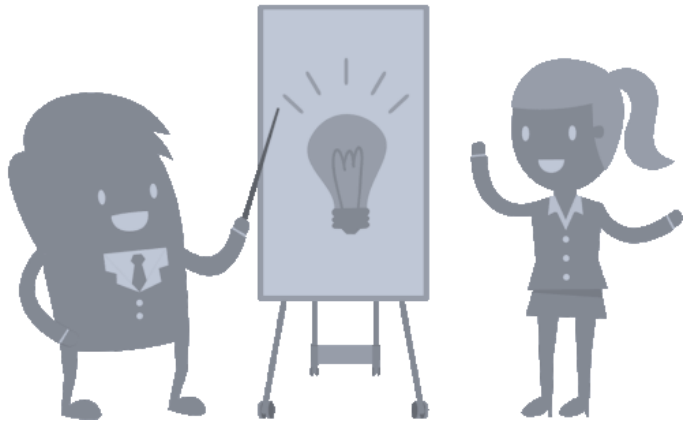

The Indian EXPRESS
Friday, July 31, 2020
Home India Cities Opinion Sports Entertainment Lifestyle Tech Videos Explained Audio Epaper SUBSCRIBE
square yards
Sign in
TOP NEWS
Follow Andhra Pradesh, Telangana Coronavirus Live Updates
Home / Technology / Centre now bans 47 clones of Chinese apps banned earlier
Centre now bans 47 clones of Chinese apps banned earlier
India bans Chinese apps: A month since the last ban, sources in the Ministry tells The Indian Express that "the problem is with the operational ethics of certain apps. This is an ongoing process."
ADVERTISEMENT
Sign In

1.1 Why should you learn this course ?

1. Part of Curriculum

2. Enhancing Organizational Efficiency

3. Increasing Job Opportunity



4. Design quality products

5. Personal protection against Cyber threats

2. Teaching and Examination Scheme

2.1 Teaching and Examination Scheme

Subject Code	Subject Name	Teaching Scheme		Credits Assigned		
		Theory	Practical	Theory	TW/ Practical	Total
ILO1016	Cyber Security and Laws	03 hr/ wk	--	03	--	03

Subject Code	Subject Name	Examination Scheme				
		ISA Marks	Mid Sem. Exam Marks	End Sem. Exam Marks	Practical / Oral	Total
ILO1016	Cyber Security and Laws	20	**30**	**50**	--	**100**

2.2 Prerequisite Courses and Relevance to Future Courses

Prerequisite Courses			
No.	Semester	Name of the Course	Topic/s
1	4	Computer Networks	Network layer and Transport layer
2	5	Cryptography and Network Security	IPSEC, SET

Relevance to Future Courses		
No.	Semester	Name of the Course
1	ME EXTC	Network and Cyber Security

2.3 Syllabus

1. Introduction to Cybercrime	4
2. Cyber offenses & Cybercrime	9
3. Tools and Methods Used in Cyber line	6
4. The Concept of Cyberspace E-Commerce	8
5. Indian IT Act. Cyber Crime and Criminal Justice	6
6. Information Security Standard compliances	6

2.4 Course Outcome (CO) Statements and Module-Wise Mapping

CO No.	Statements	Related Module/s
CO1	Understand the concept of cybercrime and its effect on outside world	1,2
CO2	Interpret and apply IT law in various legal issues	3,4
CO3	Distinguish different aspects of cyber law	5
CO4	Apply Information Security Standards compliance during software design and development	6

3. Methodology

....

3.1 Methodology

- Classroom Teaching
- Concept
- Video demonstration
- Discussion on case studies
- Class Notebook
- Modulewise Notes
- Online Quiz
- Assignment

Join **CSL** on MS Teams:

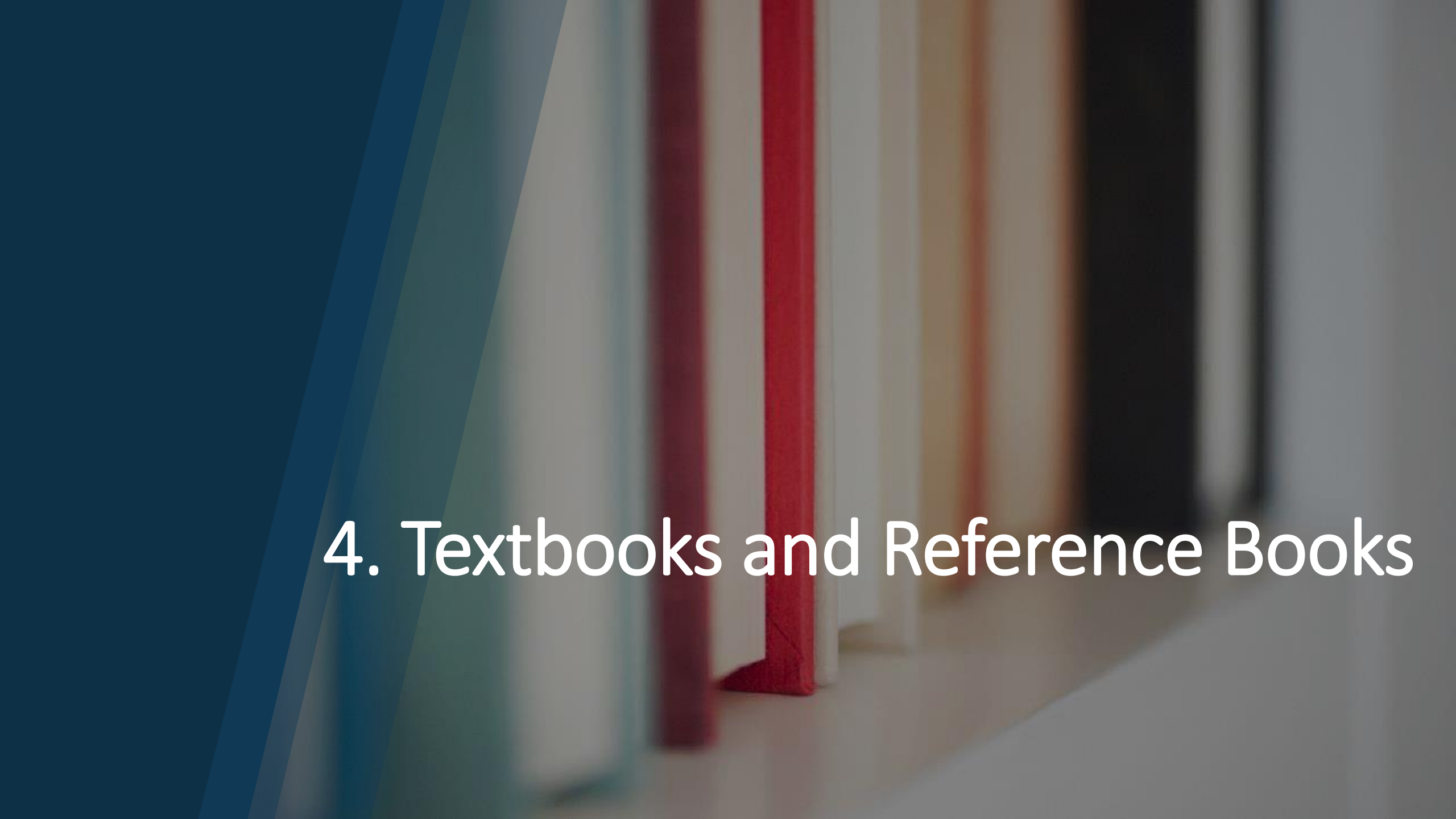
Team Name:

ILE_CyberSecurity&Laws_HarshadaRajale_2023-24

Code: 7f7xost

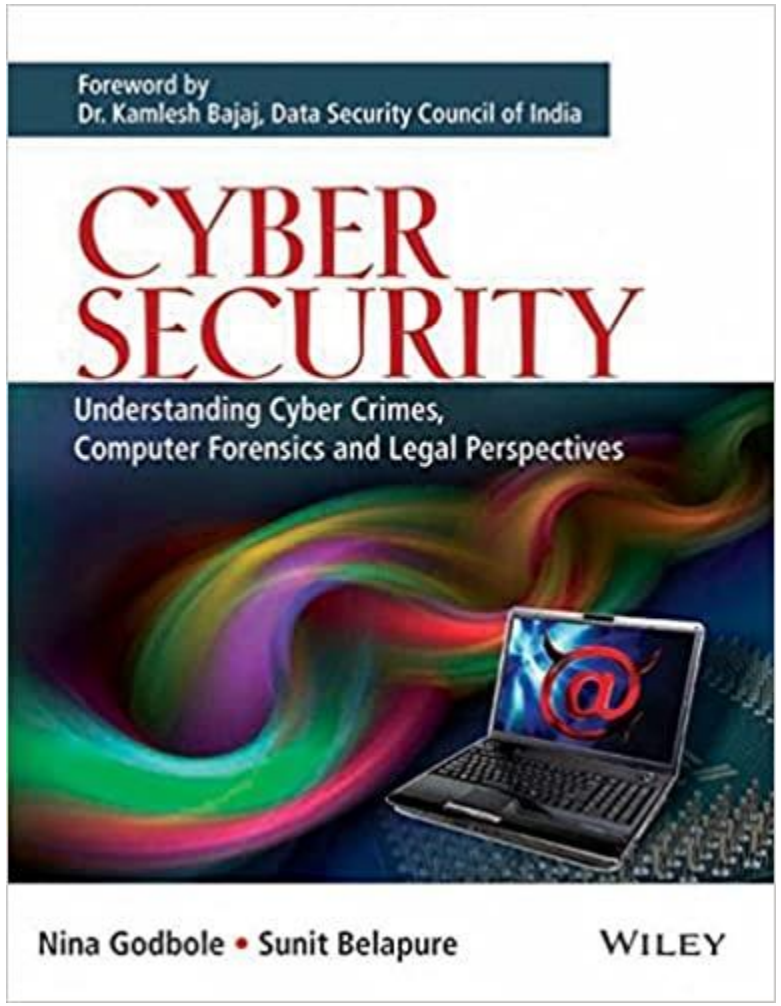
3.2 Rubrics for evaluation

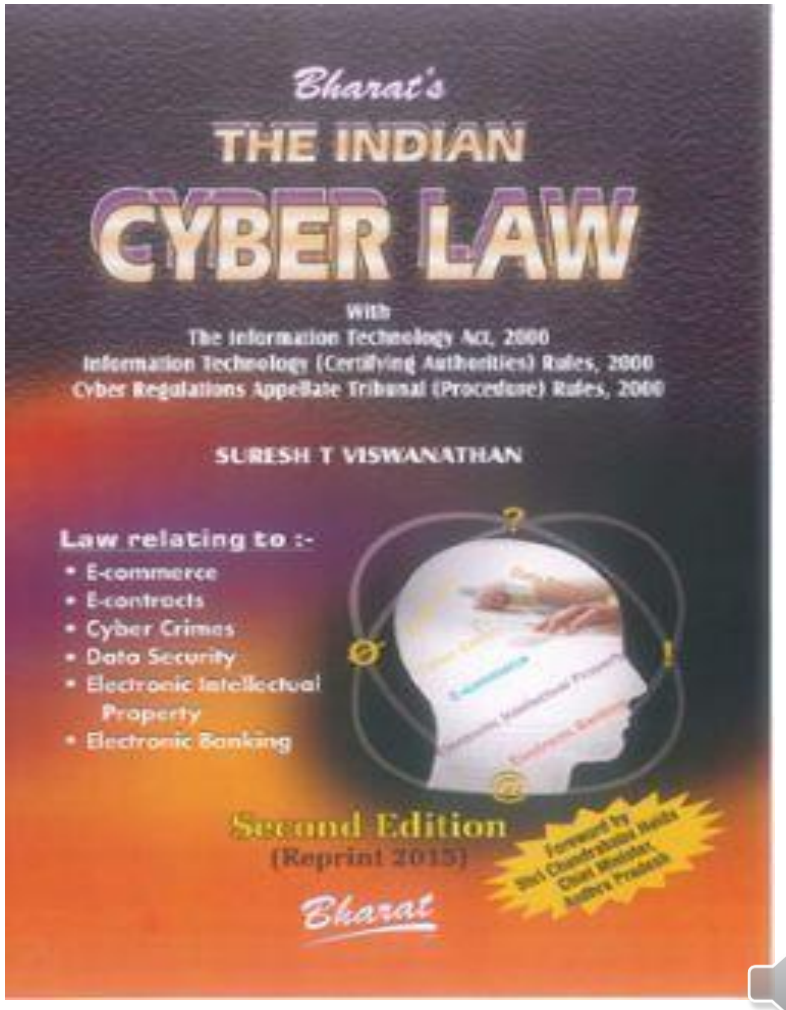
Subject Code	Subject Name	ISA Maks	Mid Sem. Exam Marks	End Sem. Exam Marks	Practical/ Oral	Total
ILO1016	Cyber Security and Laws	**20** 1. Activity 1 based on module 1 and 2 2. Activity 2 based on module 3 and 4 3. Activity 3 based on module 5 and 6 4. Activity 4 based on module 1 to 6 (Each Activity for 5 marks)	**30** **Based on Module 1,2,3 in 7th week**	**50** **Based on Module 1 to 6 as per Institute's final examination timetable**	--	**100**



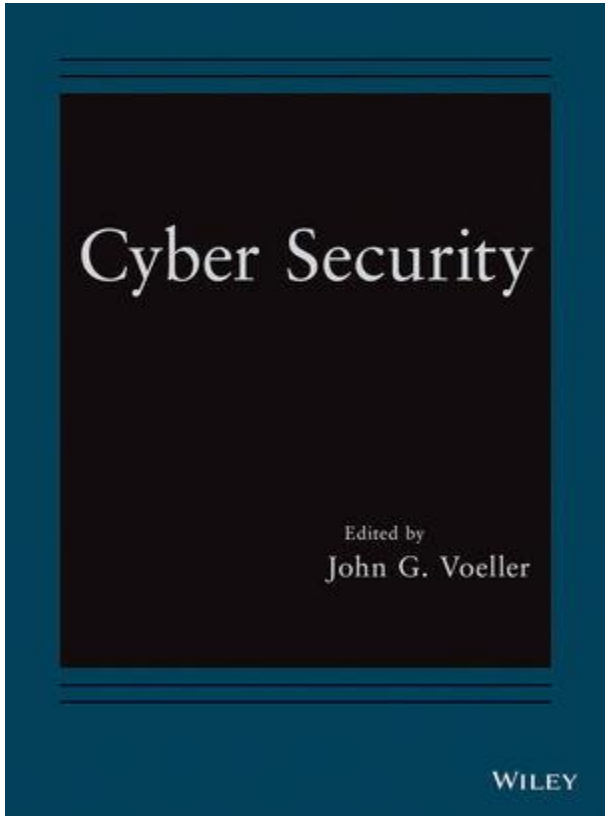
4. Textbooks and Reference Books

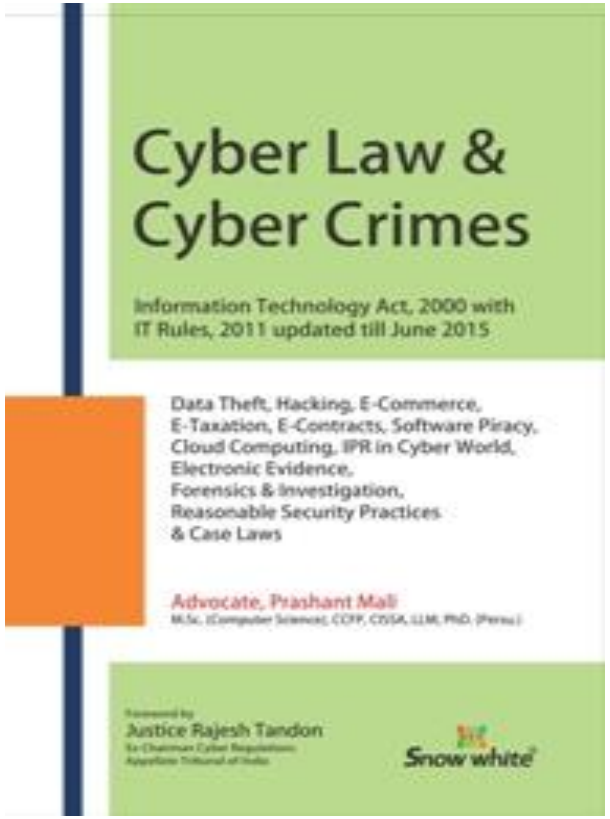
4.1 Textbooks

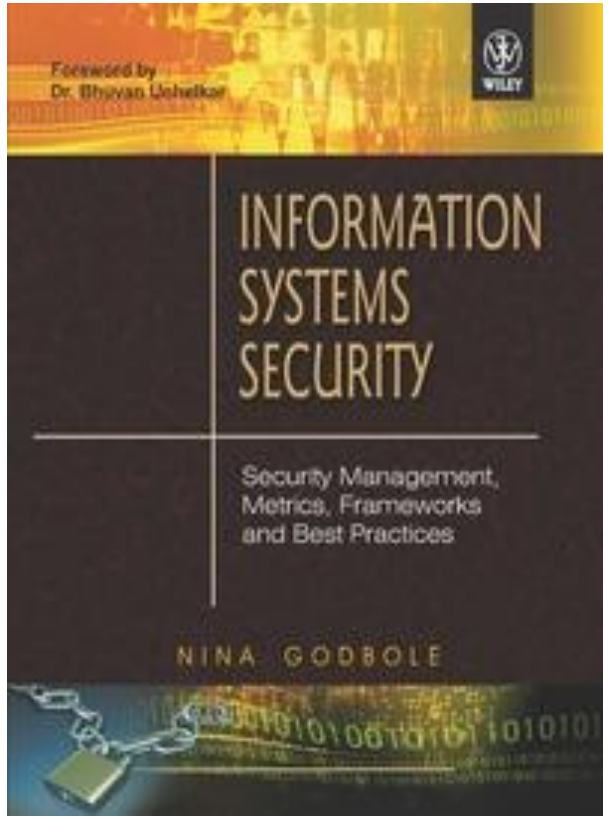




4.2 Reference books

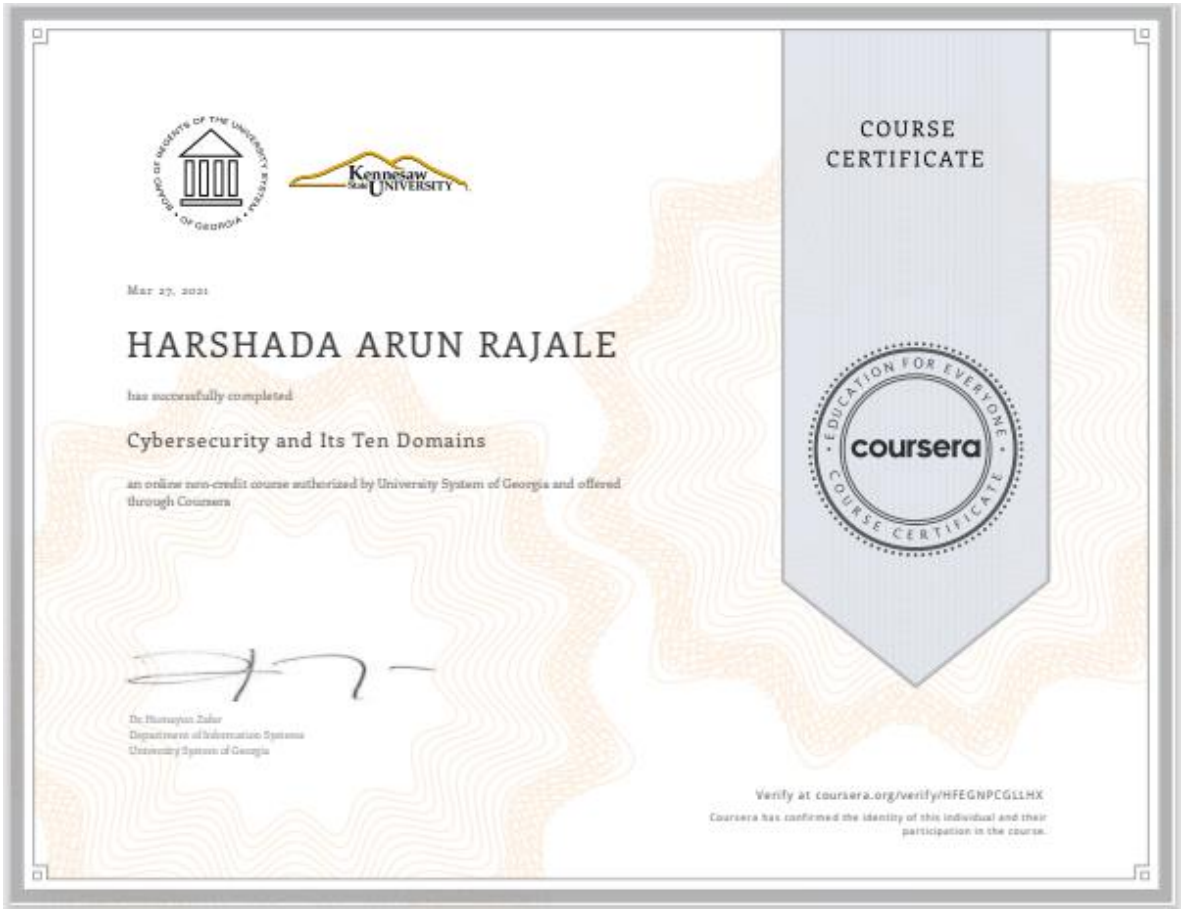







5.ONLINE COURSE

5.1 Online Courses



COURSE CERTIFICATE

May 27, 2021

HARSHADA ARUN RAJALE

has successfully completed

Cybersecurity and Its Ten Domains

an online non-credit course authorized by University System of Georgia and offered through Coursera

Dr. Hamayun Zafar
Department of Information Systems
University System of Georgia

Verify at coursera.org/verify/HFEGNPCGLLHX

Coursera has confirmed the identity of this individual and their participation in the course.

Certificate of Completion

This is to certify that Harshada Rajale successfully completed 4 hours of Introduction to Cyber Security and Information Security 2019 online course on Sept. 26, 2019

e-Learning PRO

e-Learning PRO, Instructor

&

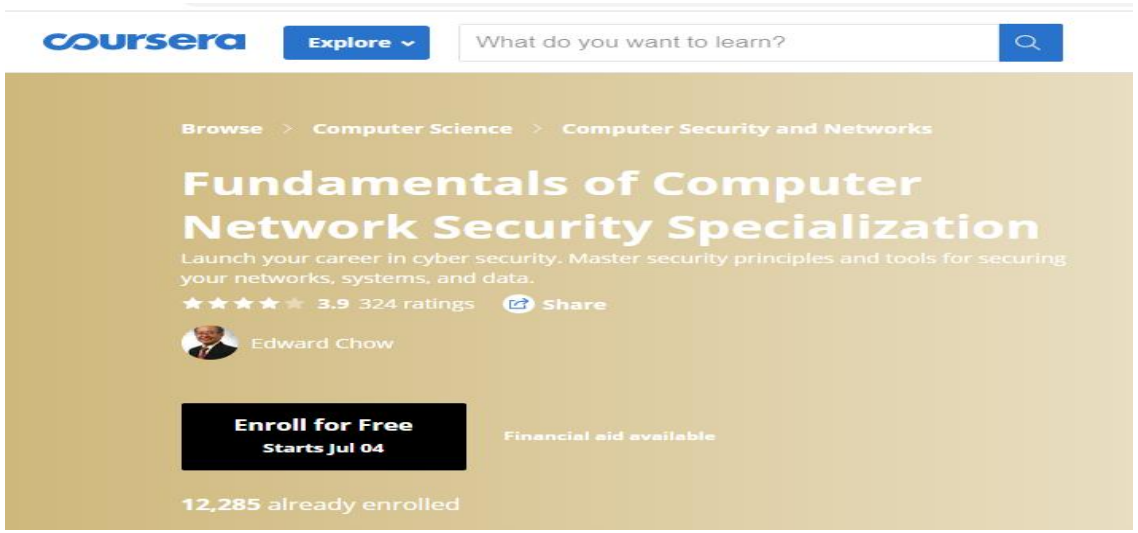
Udemy

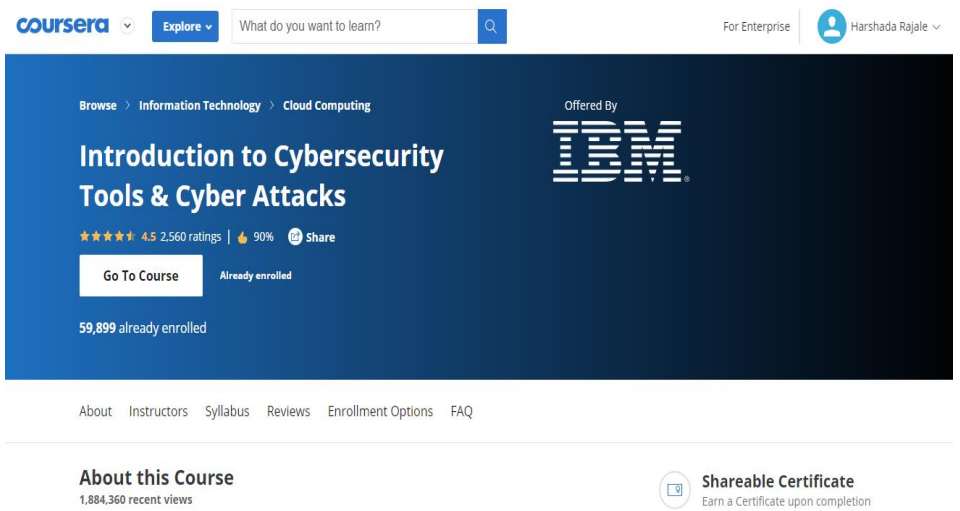
Certificate no: UC-VEUWAD0K
Certificate url: ude.my/UC-VEUWAD0K

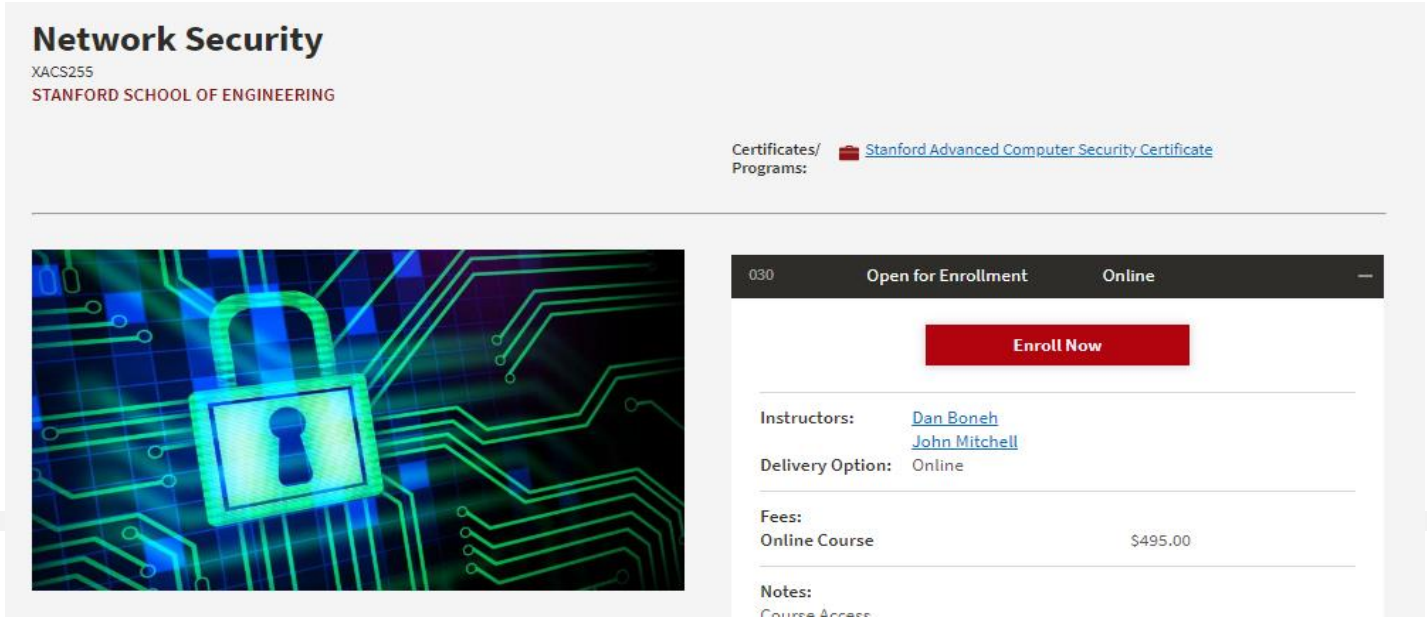
#BeAble

This certificate above verifies that Harshada Rajale successfully completed the course Introduction to Cyber Security and Information Security 2019 on 09/26/2019 as taught by e-Learning PRO on Udemy. The certificate indicates the entire course was

5.1 Online Courses







5.2 Participate in Competitions

5.3 Certification

Certified Information Systems Security Professional (CISSP)

CompTIA Security +

Global Information Assurance Certification (GIAC)

ISACA Certification

5.4 Higher studies

USC University of Southern California

ILLINOIS INSTITUTE OF TECHNOLOGY

ILLINOIS INSTITUTE OF TECHNOLOGY

TEXAS
The University of Texas at Austin

KING'S College LONDON

UNIVERSITY OF Southampton

UNIVERSITY OF BIRMINGHAM

6. Applications

6.1 Applications

7. Career Opportunities

7.1 Potential Careers

- Network Administrator
- Security Administrator
- Cybersecurity Engineer
- Security Compliance Manager
- Chief Risk Officer
- Chief Information Security Officer
- Security Architect
- Security Analyst
- Security Engineer
- Security Software Developer
- Junior Cyber Forensic Consultant
- Senior Cyber Forensic Consultant

The Indian Security Software Market Landscape

Security Landscape

Network security

Firewall
TORRID, SWAN, Quick Heal, INDUSFACE, Cyberoam (A SOPHOS Company)

Threat management
GRIDINFOCOM, AUJAS, Cyberoam, NETMONASTERY

Secure Web Gateway (SWG)
K7, Trinity Futurewin Pvt. Ltd., SHIELDSQUARE, haltDos, Cyberoam

Identity and access management

Advanced authentication
axs, 17networks, magnaquest, INNEFU, iraje, arippal

User Provisioning (UP)
GRIDINFOCOM

Web access management
secugile, TORRID

Data security

Data loss prevention
SHIELDSQUARE, vaultize, iraje, pawaar, druva, SECLORE, GRIDINFOCOM, WRENCH, Klassify

Mobile data protection
vaultize, 1mobility, Quick Heal, GENESIS

Cloud access security
PROACTEYE, CIPHERGRAPH networks, NEVALES, INDUSFACE, Cyberoam (A SOPHOS Company), InstaSafe

7.2 Companies

1. Activity 1

1. Which of the following is a common example of physical IT infrastructure?
   a) Routers and switches
   b) Firewall
   c) Data encryption
   d) Server racks

1. Activity 1

2. What does RAID stand for in the context of data storage?

a) Random Access Integrated Drive

b) Redundant Array of Independent Disks

c) Remote Access and Information Distribution

d) Reliable Archival and Instant Data

1. Activity 1

3. Which of the following is a common type of network attack that involves flooding a network with excessive traffic?

a) Phishing

b) Spoofing

c) Denial-of-Service (DoS)

d) Cross-site scripting (XSS)

1. Activity 1

4. What is the purpose of a firewall in network security?

a) To encrypt data transmission

b) To detect and remove malware

c) To prevent unauthorized access to a network

d) To monitor network traffic

1. Activity 1

5. Which of the following authentication factors is based on a physical characteristic of an individual?

a) Something you know

b) Something you have

c) Something you are

d) Something you do

1. Activity 1

6. What is the primary purpose of a Virtual Private Network (VPN)?

a) To protect against malware attacks

b) To provide secure remote access to a private network

c) To encrypt data stored on a server

d) To monitor network traffic

1. Activity 1

7. What does SSL/TLS stand for in the context of web security?

   a) Secure Socket Layer/Transport Layer Security

   b) Secure System Link/Transmission Layer Service

   c) Secure Storage Layer/Transportation Link System

   d) Secure Security Layer/Transmission Link Service

1. Activity 1

8. What is the purpose of penetration testing in cybersecurity?

a) To exploit vulnerabilities in a system to gain unauthorized access

b) To test the strength of physical security measures

c) To assess the security of a system by simulating attacks

d) To monitor network traffic for potential threats

1. Activity 1

9. Which of the following is an example of a strong password?

a) "123456"

b) "password"

c) "P@55w0rd!"

d) "abcdef"

1. Activity 1

10. What is the purpose of regular data backups in IT infrastructure?
    a) To prevent physical damage to hardware
    b) To store sensitive data securely
    c) To recover data in the event of data loss or system failure
    d) To encrypt data transmission

1. Activity 1

11. What is the purpose of an Intrusion Detection System (IDS)?

a) To prevent data breaches

b) To encrypt network traffic

c) To detect and alert on unauthorized network activity

d) To scan for vulnerabilities in software applications

1. Activity 1

12. Which of the following is a common authentication protocol used for secure remote access?

a) FTP

b) SSH

c) SMTP

d) HTTP

1. Activity 1

13. What is the primary purpose of a Content Delivery Network (CDN)?

a) To provide secure access to online content

b) To store and manage user authentication data

c) To optimize content delivery and improve website performance

d) To encrypt data during transmission

1. Activity 1

14. What is the difference between a virus and a worm?

a) Viruses can self-replicate, while worms cannot.

b) Viruses spread through email attachments, while worms spread through network vulnerabilities.

c) Viruses can infect both computers and biological organisms, while worms are computer-specific.

d) Viruses are always malicious, while worms can be either malicious or benign.

1. Activity 1

15. What does the acronym "VPN" stand for in the context of network security?

a) Virtual Private Network

b) Virus Protection Network

c) Virtual Public Network

d) Visible Personal Network

1. Activity 1

16. Which of the following is an example of a symmetric encryption algorithm?

a) RSA

b) AES

c) Diffie-Hellman

d) ECC

1. Activity 1

17. What is the purpose of a Security Information and Event Management (SIEM) system?

a) To manage user access and permissions

b) To secure physical assets and facilities

c) To collect and analyze security logs and events

d) To protect against distributed denial-of-service (DDoS) attacks

1. Activity 1

18. Which of the following is a common method of social engineering?

a) SQL injection

b) Phishing

c) Brute force attack

d) Man-in-the-middle (MitM) attack

1. Activity 1

19. What is the purpose of a data center in IT infrastructure?

a) To store and manage network switches and routers

b) To provide secure remote access to a private network

c) To centralize and store computer servers and related equipment

d) To monitor network traffic for potential threats

1. Activity 1

20. What does the term "BYOD" stand for in the context of IT security?

a) Bring Your Own Device

b) Backup Your Operating Data

c) Build Your Own Database

d) Break Your Online Defense

THANK YOU

HARSHADA ARUN RAJALE

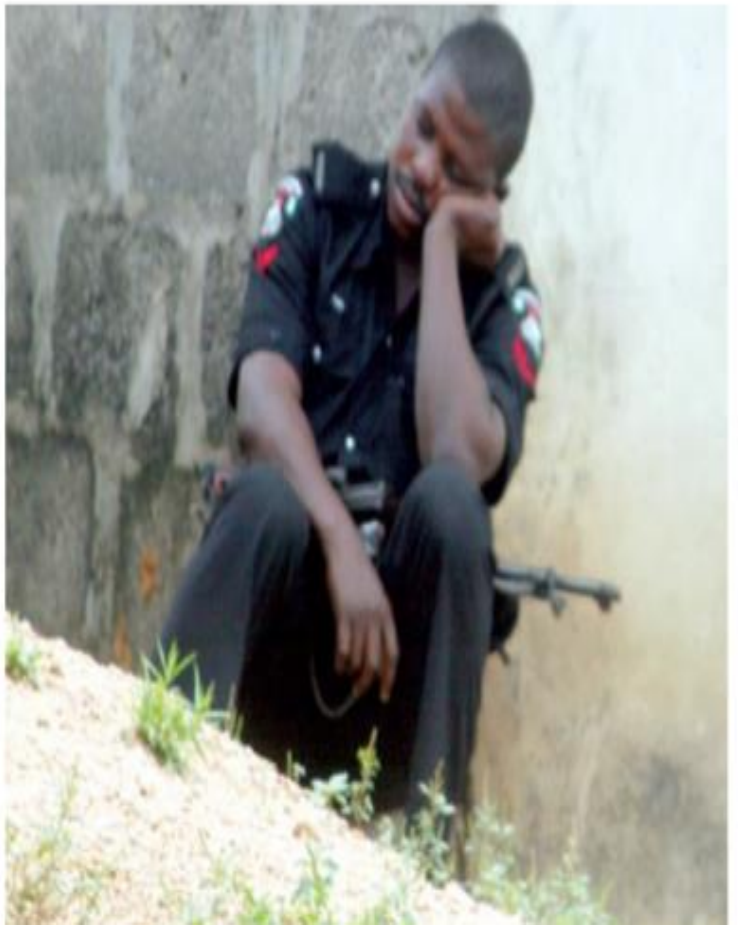
+91 9594146413

Harshada.Rajale@vit.edu.in

Brainstorming

What is Security?

Security according to two boys of 10 years old



Definition Security

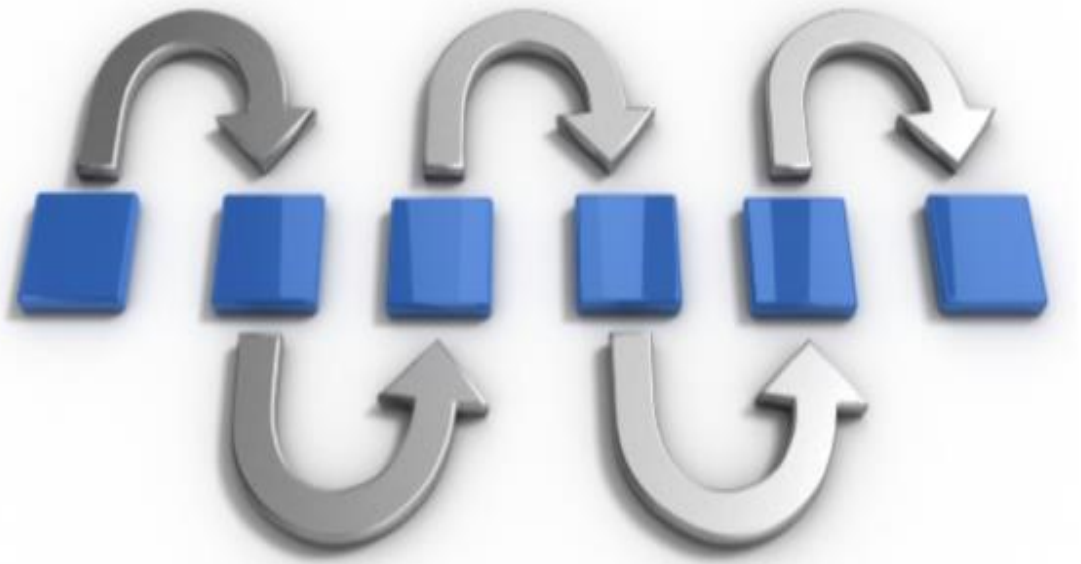
There is no clear cut definition

Security means safety, as well as the measures taken to be safe or protected.

Definition Security

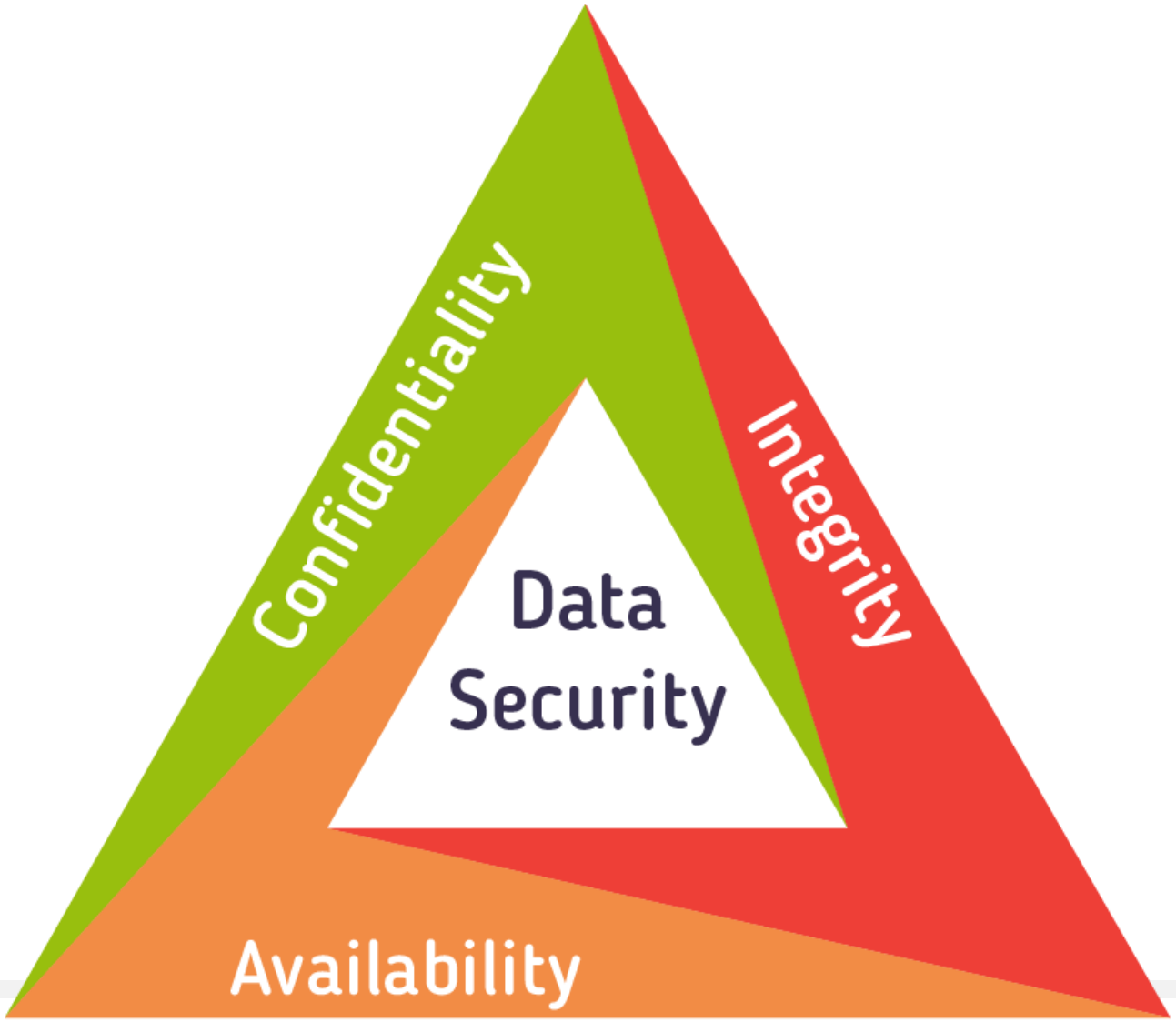
Security is a process, not an end state.

Definition Security



Security is the process of maintaining an acceptable level of perceived risk.

Security Features



Security Features

Confidentiality

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it:

Security Features

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Security Features

Availability

Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Cyber Security and Laws

1.2 Cyber Security

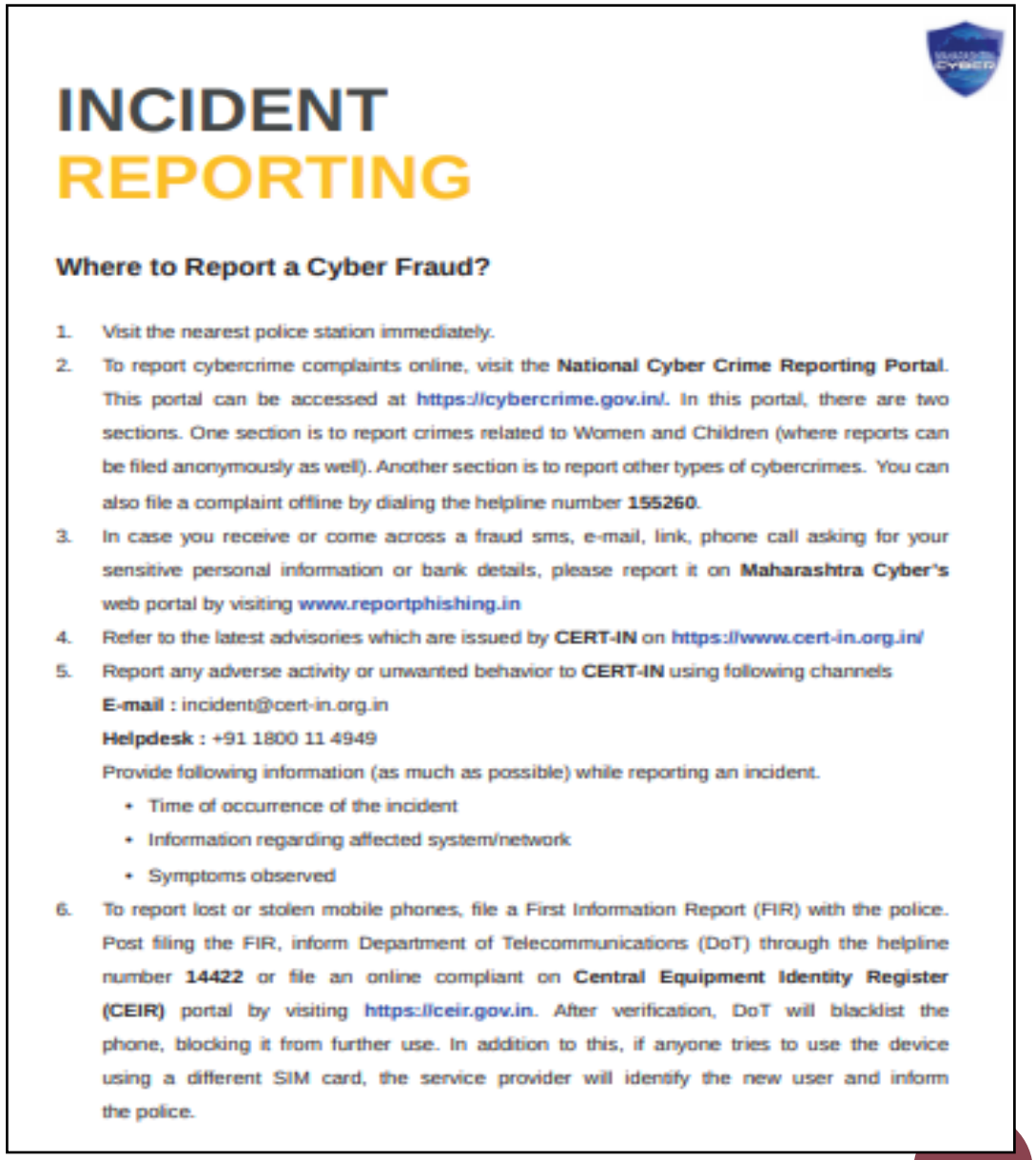
- **Cyber Security** is the protection of
  - computer systems and networks from the theft
  - damage
  - the disruption or misdirection

- Cybersecurity is one of the major challenges in the contemporary world.

1.3 Cyber Laws

- **Cyber law -** legislation focused on the acceptable behavioral use of technology

- It applies to the actions of individuals, groups, the public, government, and private organizations.



INCIDENT REPORTING

Where to Report a Cyber Fraud?

1. Visit the nearest police station immediately.
2. To report cybercrime complaints online, visit the **National Cyber Crime Reporting Portal**. This portal can be accessed at https://cybercrime.gov.in/. In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialing the helpline number **155260**.
3. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on **Maharashtra Cyber's** web portal by visiting **www.reportphishing.in**
4. Refer to the latest advisories which are issued by **CERT-IN** on https://www.cert-in.org.in/
5. Report any adverse activity or unwanted behavior to **CERT-IN** using following channels
   E-mail : incident@cert-in.org.in
   Helpdesk : +91 1800 11 4949
   Provide following information (as much as possible) while reporting an incident.
   - Time of occurrence of the incident
   - Information regarding affected system/network
   - Symptoms observed
6. To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the helpline number **14422** or file an online compliant on **Central Equipment Identity Register (CEIR)** portal by visiting https://ceir.gov.in. After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

Introduction to Computer crime

- A crime conducted in which a computer was directly and significantly instrumental is known as “**Computer Crime”**.

Cyber Crime


Cybercrime is criminal activity that entails the use of a computer system, computer technology, or the internet.
Cyberterrorism
say: "ahhh..."
Computer viruses
CORRECT PASSWORD
Identity theft
Cyberbullying
legaldictionary.net

Cyber Crime

- A crime committed using a computer and the Internet to steal person's identity or sell illegal or smuggled goods or disturb any operations with malicious program is known as **"Cyber Crime"**.

The first Cyber Crime

- **The first recorded cyber crime took place in 1820.**
- *In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom.*

Cyberspace

- Cyberspace is a place where you can chat, explore, research and play (INTERNET).

Cyberpunk

- The word “cyber” and “punk” are two different words which means “disorder via machine”.
- The word cyberpunk was coined by writer Bruce Bethke, who wrote a story with that title in 1982.

- The movies based on cyberpunk are :
  - Terminator I, II and III
  - Until the end of the world
  - Mad MAX I, II and III
  - The Matrix (series)
  - The X-Files
  - Solaris

Cyberwarfare

- Cyberwarfare refers to politically motivated hacking.

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.

Cybercrime and Information Security

- Lack of information security gives rise to cyber crime.
- Cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored in all these from unauthorized access, use, disclosure, disruption, modification or destruction.

Who are Cybercriminals

- Cybercrime involves such activities like
  - Credit card fraud
  - Cyberstalking (irritation)
  - Child pornography
  - Defaming another online
  - Gaining unauthorized access to computer system
  - Overriding encryption to make illegal copies
  - Software piracy
  - Stealing another’s identity to perform criminal act.

Types of Cybercriminals

- Type 1 : Hungry for recognition
- Type 2 : Not interested in recognition
- Type 3 : The insider

Type 1

- Hobby hackers
- IT professionals
- Politically motivated hackers
- Terrorist organizations.

Type 2

- Psychological spoiled
- Financially motivated hackers
- State-sponsored hacking
- Organized criminals

Type 3

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

Classifications of Cybercrimes

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society
- Crimes emanating from Usenet newsgroup

Cybercrime against individual

- Email spoofing
- Phishing
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Pornographic offense
- Password sniffing

Cybercrime against property

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

Cybercrime against organization

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attacks / dissemination of Viruses
- Email bombing

Cybercrime against organization

- Salami attack
- Logic bomb
- Trojan Horse
- Data diddling

Cybercrime against organization

- Crimes emanating from Usenet newsgroup
- Industrial spying
- Computer network disturbance
- Software piracy

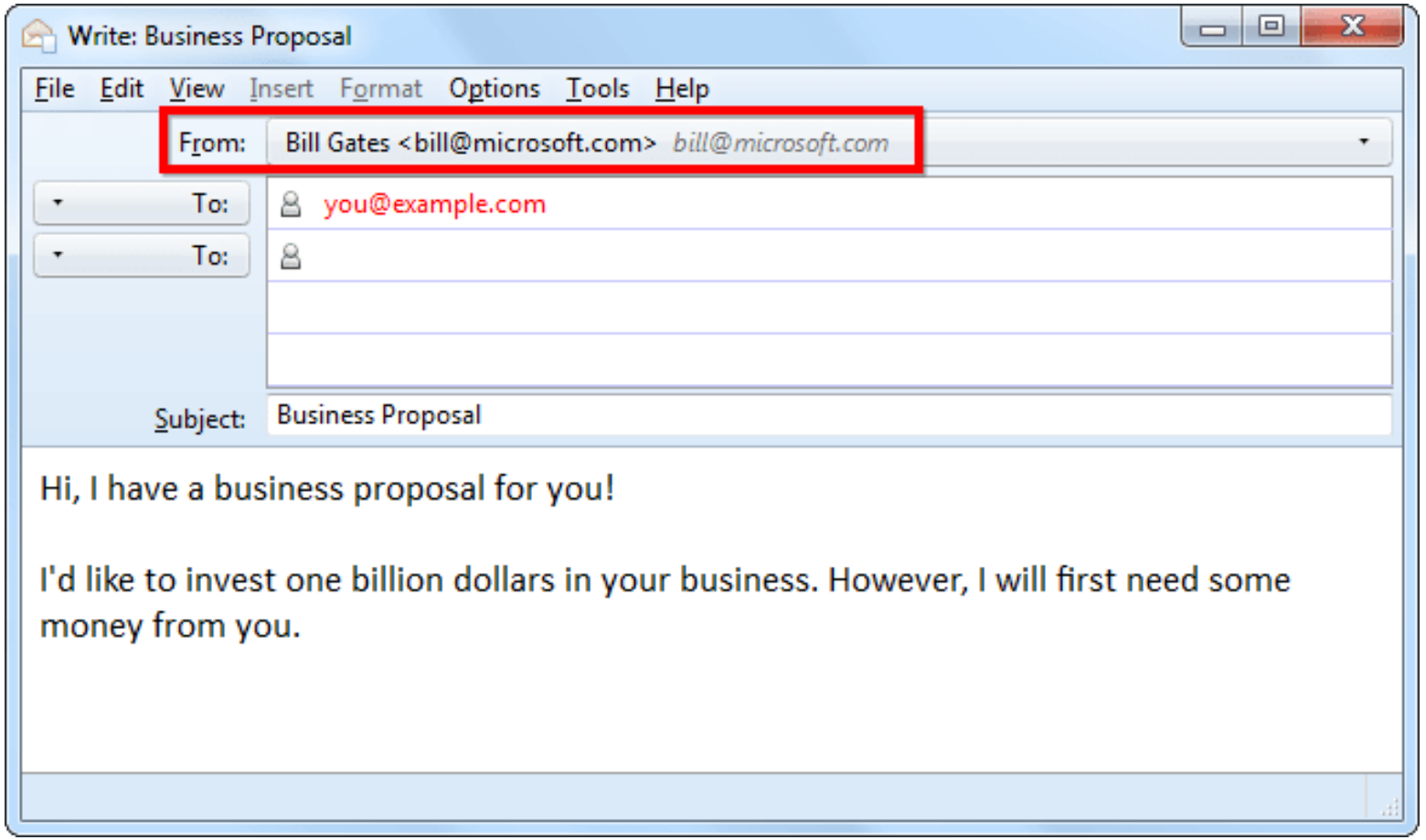
Cybercrime against society

- Forgery
- Cyberterrorism
- Web jacking

Crimes emanating from Usenet newsgroup

- A Usenet newsgroup is a repository usually within the usenet system, for messages posted from many users in different locations using Internet.
- Therefore, it is expected that one uses this with caution and common sense and exercise proper judgment as well as the service at own risk

E-Mail Spoofing



E-Mail Spoofing

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

Example

- A branch of global trust bank experienced a customer spreads out the rumor that bank is not doing well.

Phishing

Phishing

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

Spamming


BEST OFFER!
SPAM
SPAM
SPAM
SPAM
DELETE
STOP SPAM!
BEST OFFER!
BEST OFFER!
• SPAMMING •

Spamming

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

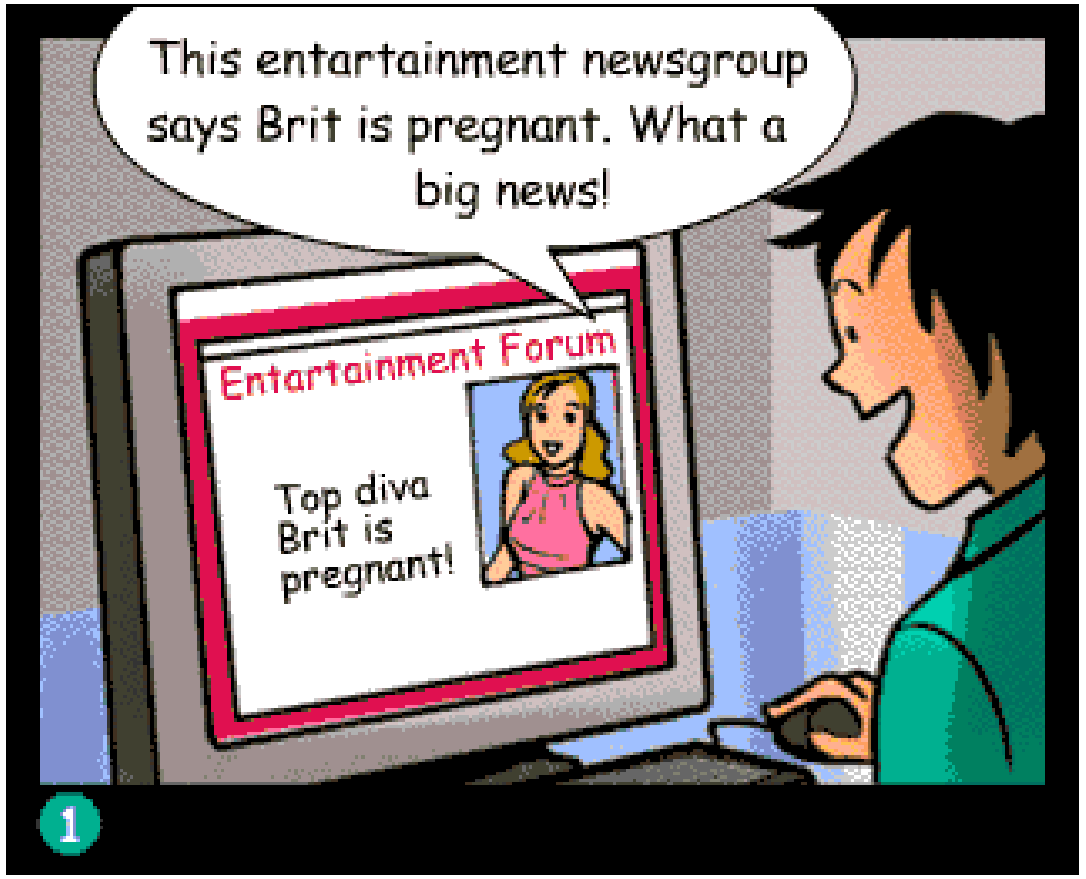
Types Spamming

- E-mail spam(most common)
- Usenet newsgroup spam
- Web search Engine spam
- Spam in blogs
- Online classified ads spam

Types Spamming

- Mobile phone messaging spam
- Internet forum spam
- Social networking spam
- File sharing network spam
- Video sharing sites, etc

Cyberdefamation



Cyberdefamation

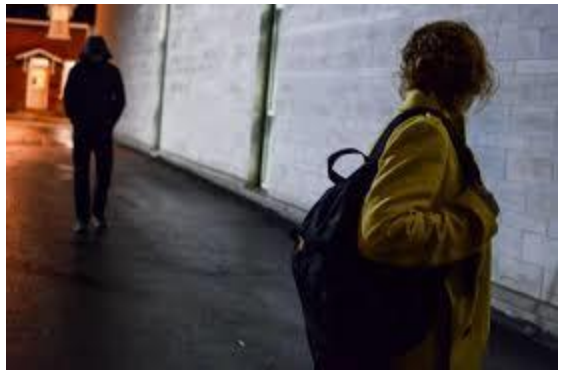
The Indian Penal Code says about defamation is

"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."

Cyberdefamation

- When above happens in electronic form, its known as Cyber defamation
- Cyber defamation occurs when the defamation takes place with the help of computers and/ or Internet
- ***Libel*** is written defamation and ***Slander*** is oral defamation.

Cyber stalking and harassment



Cyber stalking and harassment

- Cyber stalking is the use of internet or other electronic means to stalk or harass an individual , group or organizations
- It may include false accusations, defamation, slander and libel
- It may also include monitoring, identify theft, threats, vandalism, solicitation for sex or gathering information that may be used to threaten , embarrass or harass

Types :Cyber stalking

- Stalking by Strangers
- Gender based stalking
- Of intimate partners
- Of celebrities and public persons
- By anonymous online mobs
- Corporate cyberstalking

Computer Sabotage

Computer Sabotage

- The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses or logic bombs is referred to as computer sabotage
- It is done to gain economic advantage, promote illegal activities, steal data, etc

Computer Sabotage

- A **computer worm** is a standalone malware computer program that replicates itself to spread to other computers
- A **virus** is a type of malicious software comprised of small pieces of code attached to legitimate programs
- **Logic bombs** are event dependent programs created to do something only when a certain event occurs.

Pornographic Offenses

Pornographic Offenses

- 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 .

How they operate?

1. Pedophiles use a false identity to trap the children/teenagers.
2. They seek teens in the kids' areas.
3. They be friend of them.
4. Then they get email address of the child and start making contacts on email too.
5. These emails contains sexually explicit language.

How they operate?

6. They start sending pornographic images/text to the victim to fed to into his/her mind that “This is normal and everybody does it”.
7. At the end of it, the pedophiles set up a meeting with the child out of the house and then use them as a sex object.

Legal Remedies

- Childrens online privacy protection act or **COPPA** is a way of preventing Online pornography
- **Net Nanny** and **Cybersitters** are software originally designed for parents about their childrens unrestricted access to Internet, which can be used to block a user's access to websites containing "dangerous" or "offensive" material

Password Sniffing

Password Sniffing

- Password sniffers are programs that monitor and record the name and password of network users as they login.

Password Sniffing : Case Study

- (1)If you are a fan of siting in public cafes that offer free WIFI and playing on your computer. Make sure you are using sort of encryption and security when sending passwords.
- A person who has a password sniffing program on their computer can easily sit in a public space collecting passwords from the network with ease. These programs are simple to use.
- (2)In a Moll all people are shopping using there smartcard, credit card , debit card etc. at the time of payment customer have to stretch their card into machine. In that machine the attacker can use program to record the user password or sensitive information. And after gaining particular information attacker can misuse the card and amount.

https://securityxploded.com/password-sniffer-spy.php

About

Password Sniffer Spy is the all-in-one Password Sniffing Tool to capture Email, Web and FTP login passwords passing through the network.

It automatically detects the login packets on network for various protocols and instantly decodes the passwords. Here is the list of supported protocols,

- HTTP (BASIC authentication)
- FTP
- POP3
- IMAP
- SMTP

Credit Card Fraud

Credit Card Fraud

- Information security requirements for credit cards have been increased recently.
- The hackers target these online databases to access large databases of credit card information

Credit Card Fraud

- Payment card industry data security standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent card holder data theft and to help combat credit card fraud

Intellectual Property Crimes

Intellectual Property Crimes

- Cyber theft of IP means stealing of copyrights, trade secrets, patents etc using internet and computers.
- Copyrights and trade secrets are the two forms of Intellectual Property that is frequently stolen.

Internet Time Theft

Internet Time Theft

- It occurs when an unauthorized person uses the Internet hours paid by another person.
- Basically, internet time theft comes under hacking because the person gains the access to someone’s user ID and password and then uses it to access Internet without the other person’s knowledge.

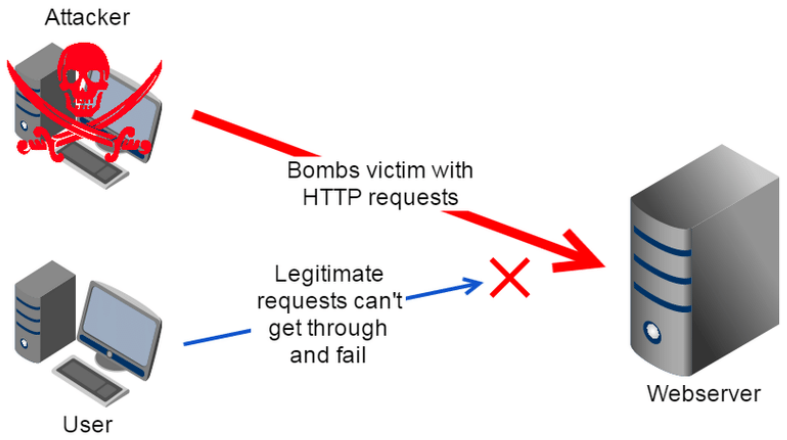
Unauthorized accessing of computer

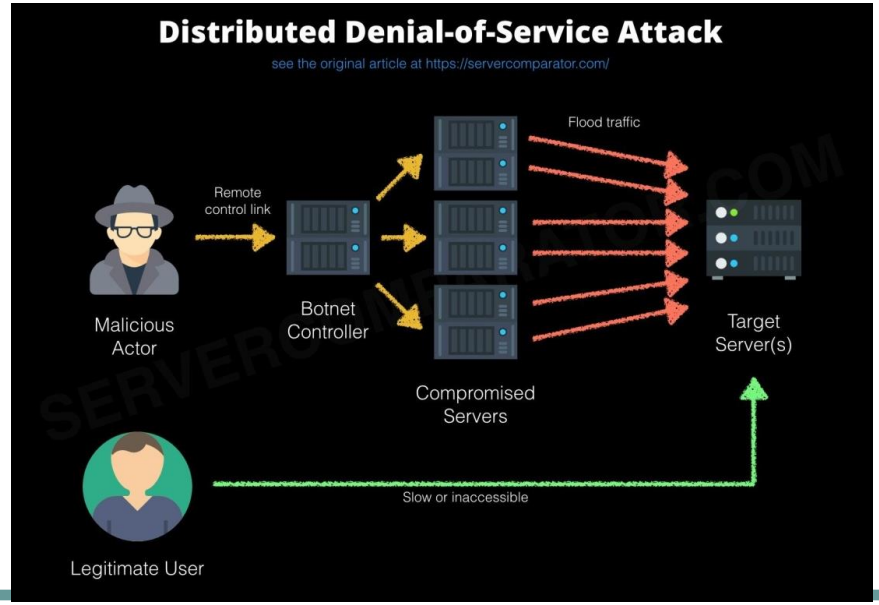
Unauthorized accessing of computer

- Unauthorized access is when someone gains access to a website, program, server, service or other system using someone else’s account or other methods

- Eg: If someone kept guessing a password or username for an account that as not theirs until they gained access, it is considered as unauthorized access

Denial of service attack





Denial of service attack

- DOS Attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
- DOS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash.

Virus Attack/ Dissemination of Viruses

Virus Attack/ Dissemination of Viruses

- Viruses are computer programs that attach themselves to or infect a system or file and have a tendency to circulate to other computers on a network.

Email bombing / Mail Bombs

Email bombing / Mail Bombs

- 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 programs can be written to instruct a computer to do such tasks on a repeated basis.

Salami Attack

Salami Attack

- 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.

- For ex. A bank employee inserts a program, into bank’s servers, that deducts a small amount of money from the account of every customer (Rs. 2/-). No account holder will notice this unauthorized debit, but the bank employee will make sizable amount every month.

On a lighter Note…

Salami Attack In Student's Life

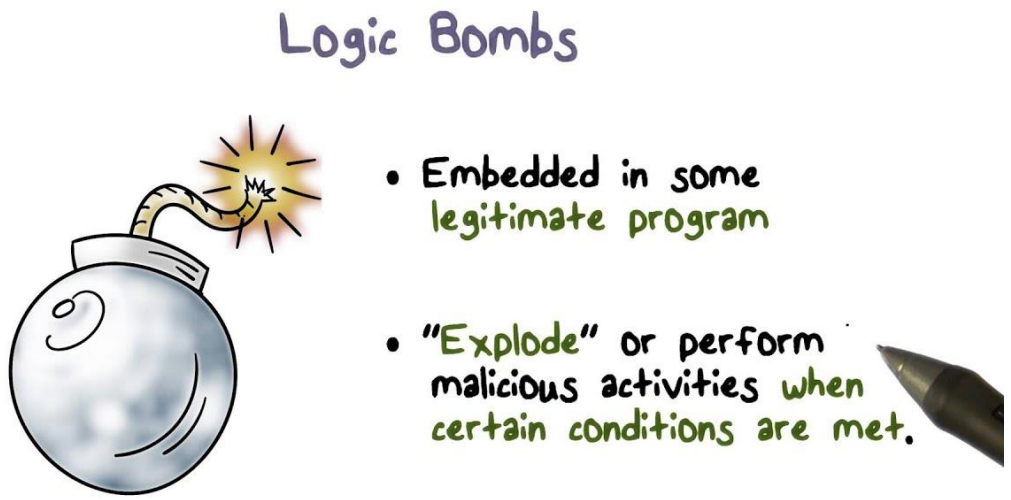
- There is this person who

Eats from everybody's tiffin
Leaving his own at home, its kind of Partial Salami Attack, but it is definitely an Attack.

Logic Bomb

Logic Bomb

- Logic bombs are event dependent programs created to do something only when a certain event known as Trigger event occurs.



- Some viruses may be termed as Logic Bombs because they lie dormant all through the year and become active only on a particular date/ event.

Trojan Horse

- Story of Trojan Horse
- https://www.youtube.com/watch?v=Td1uPq9K--E

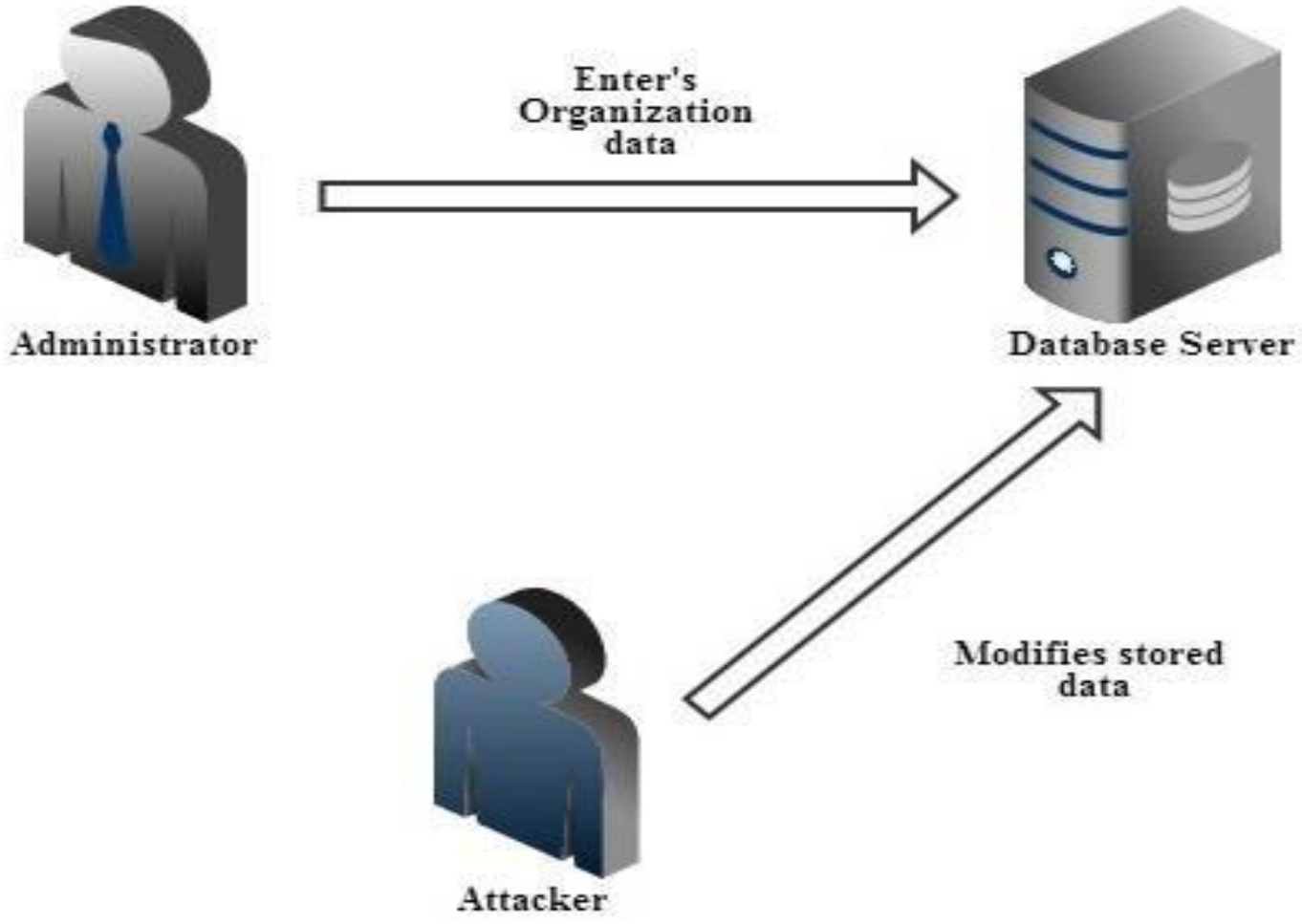
- Beginning in the late 20th century, the name “Trojan horse” was applied to deceptively benign computer codes that seem like legitimate applications but are written to damage or disrupt a computer’s programming or to steal personal information.

Trojan Horse

- It is a destructive program that masquerades as a benign application.
- Unlike viruses, Trojan horses do not replicate themselves but they can be destructive.

- 7 main types of Trojan Horse:
  - Remote access Trojans
  - Data sending Trojans
  - Destructive Trojans
  - Proxy Trojans
  - FTP Trojans
  - Security software disabler Trojans
  - DOS attack Trojans

Data diddling



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.

Crimes emanating from Usenet groups

Crimes emanating from Usenet groups

- Usenet is a popular means of sharing and distributing information on the web with respect to various topics.
- 30,000 different topics
- Practically, no technical method is available to put a control on these groups.
- Specific newsgroup can be blocked...but that is not a correct solution

Usenet group Crimes

- Distribution/ sale of pornographic material.
- Distribution/ sale of pirated software
- Distribution of hacking software
- Sale of stolen credit card numbers
- Sale of stolen data/ stolen property.

Industrial Spying (Espionage)

- Industrial espionage or corporate espionage is a form of spying for commercial purpose instead of purely national security
- Purpose: To gather information about organization
- Example: Stealing of IP, information about manufacture process, ideas, recipes, formula, customer database etc.

- One of the interesting case is about The famous Israeli Trojan story, where a software engineer in London created a Trojan Horse program specifically designed to extract critical data gathered from machines infected by his program.
- He had made a business out of selling his Trojan Horse program to companies in Israel, which would use it for industrial spying by planting it into competitor’s network.

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 passwords.
- The cracker can bypass existing password protection by creating a program to captive logon IDs and Passwords.

Software Piracy

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”***.

Examples of Software piracy

- Friends loaning disks
- Organizations under reporting the number of software licences
- Organization not tracking their software licences
- Illegal download from internet

Disadvantage of piracy

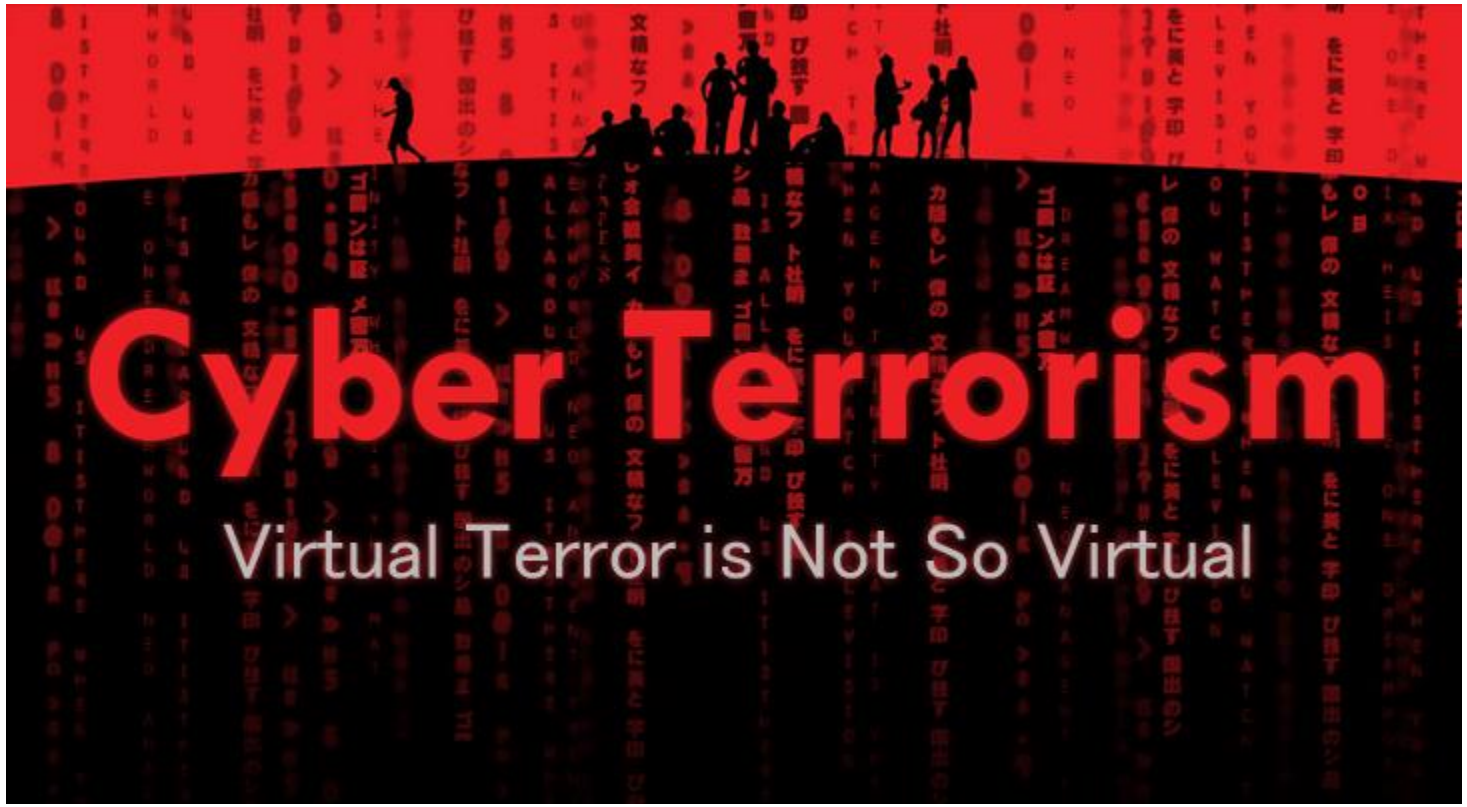
- Getting untested software that have been copied thousands of time over.
- May potentially contain hard-drive infection virus.
- No technical support in the case of software failure.
- No warranty protection
- No legal right to use the product.

Forgery

Forgery

- Fake currency notes, postage and revenue stamps, marksheets can be forged using sophisticated computers, printers and scanners.

Cyber Terrorism



Cyber Terrorism

- It is defined as premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence and cause severe disruption and widespread fear in society.

Web Jacking

Web Jacking

- Web jacking occurs when someone forcefully takes control of a website by cracking the password and later changing it..
- First stage of this crime involves “password sniffing”.

Hacking

Hacking

- Hacking is any act of breaking into computer/ network.
- Purpose of hacking are many, the main ones are as follows :
  - Greed
  - Power
  - Publicity
  - Revenge
  - Adventure
  - Desire to access forbidden information
  - Destructive mindset

- Hackers write or use ready-made computer programs to attack the target computer.
- Government websites are hot on hacker’s target lists and attacks on government websites receive wide press coverage.

- In December 2009, NASA's site was hacked by SQL Injection.
  - SQL injection is a code injection technique that might destroy your database.
  - SQL injection is one of the most common web hacking techniques.
  - SQL injection is the placement of malicious code in SQL statements, via web page input.
- https://www.w3schools.com/sql/sql_injection.asp

A hacker might get access to user names and passwords in a database by simply inserting " OR ""=" into the user name or password text box:

User Name:

" or ""="

Password:

" or ""="

The code at the server will create a valid SQL statement like this:

Result

```
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

The SQL above is valid and will return all rows from the "Users" table, since **OR ""=""** is always TRUE.

Difference between:

Hacker	*Cracker*
Definition - A Hacker is a person who is interested in the working of any computer Operating system. Most often, Hackers are programmers. Hackers obtain advanced knowledge of operating systems and programming languages. They may know various security holes within systems and the reasons for such holes.	Definition - A Cracker is a person who breaks into other people systems, with malicious intentions. Crackers gain unauthorized access, destroy important data, stop services provided by the server, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious.
Hacker constantly seek further knowledge, share what they have discovered, and they never have intentions about damaging or stealing data.	They have intention about damaging or stealing data.
They doesnot work against the law .	They work against law.
They are always find weakpoints of the appln,o.s.,website.& secure it.	They have always bad intension whenever they work.

Online Frauds

- Major types of crimes are:
  - Spoofing website
  - Email security threats
  - Hoax mail about virus threats
  - Lottery fraud
  - Banking frauds

- In spoofing websites and Email security threats, fraudsters create authentic looking websites that are spoof.
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts.

Newsgroup Spam

- This is one form of spamming.
- **Newsgroup spam** is a type of spam where the targets are Usenet newsgroups.
- Spamming of Usenet newsgroups actually pre-dates e-mail spam.

Cyber Crime and Indian ITA 2000

- In India, Information Technology Act, ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in Jan 30, 1997.
- Cybercrimes are punishable under two categories: ITA 2000 and IPC.

ITA 2000

Section Reference	Title	Fine	Imprisonment
Sec 43	Penalty for damage to computer	Rs. 1 Crore	-
Sec 66	Hacking with computer system	Rs. 2,00,000/-	3 years
Sec 67	Publishing of obscene information in E –form	Rs. 1,00,000/-	5 years
Sec 68	Power of controller to give directions	Rs. 2,00,000/-	3 to 10 years
Sec 70	Protected system	-	Upto 10 years
Sec 72	Breach of confidentiality and privacy	Rs. 1,00,000/-	Upto 2 years
Sec 73	False digital signature certificate	Rs. 1,00,000/-	2 years
Sec 74	Publication for fraudulent purpose	Rs. 1,00,000/-	2 years

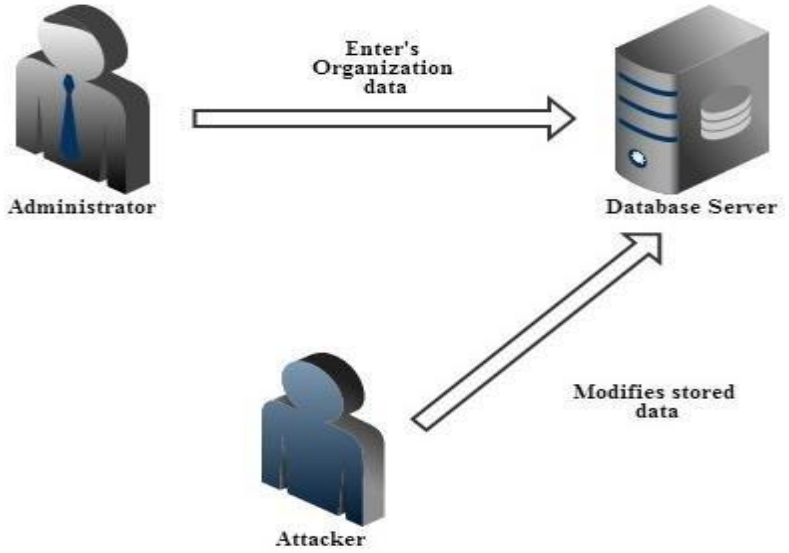
Questions

1. What is CyberCrime? How do you define it?
2. How do we classify cybercrimes? Explain each one briefly.
3. What are the different types of cybercriminals? Explain each one briefly.
4. State the difference between “cybercrime” and “cyberfraud” if any.

5. Define the following terms
    1. Cyberterrorism
    2. Cyberpunk
    3. Cyberdefamation
    4. Cyberwarefare

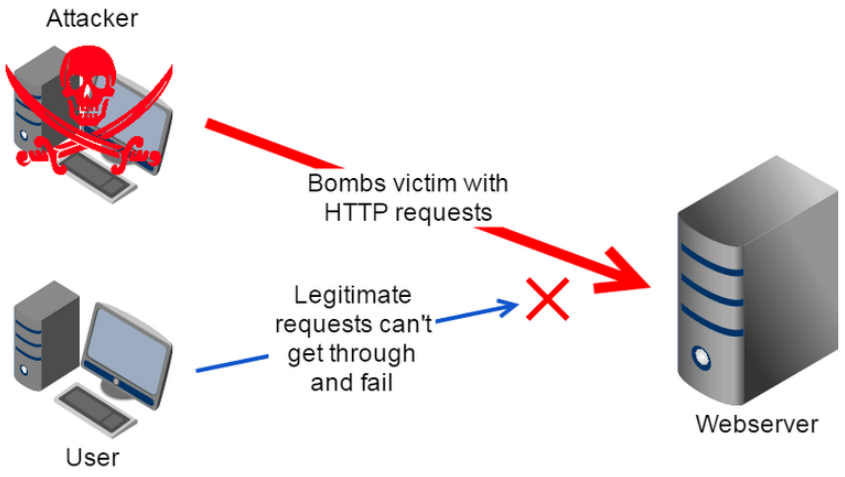

CREDIT CARD
GOLD
0000 1245 7690


YOU'VE
GOT MAIL
xcitefun.net


Enter's
Organization
data
Administrator
Database Server
Modifies stored
data
Attacker


Personal
Data


ack)


Attacker
Bombs victim with
HTTP requests
Legitimate
requests can't
get through
and fail
User
Webserver


SPAM
SPAM
SPAM
SPAM
DELETE
STOP SPAM!
BEST
OFFER!

Questions

1. What is Computer crime and CyberCrime?
2. What are the different types of cybercriminals? Explain each one briefly.
3. How do we classify cybercrimes? Explain each one briefly.

5. Define the following terms
    1. Cyberterrorism
    2. Cyberpunk
    3. Cyberdefamation
    4. Cyberwarefare


Personal
Data


BEST OFFER!
@
@
SPAM
SPAM
@
SPAM
SPAM
DELETE
?
STOP SPAM!
BEST OFFER!
BEST OFFER!

THANK YOU

HARSHADA ARUN RAJALE

+91 9594146413

Harshada.Rajale@vit.edu.in