CREDIT -III Electronic Payment System: EPS Models, EPS Processing, Digital token based(02), debit card, smart card, Credit Card, risk in electronic payment system(03), E-auction: Introduction, Overview, Electronic trading(02), Online Banking: origin, advantages, disadvantages, Services (03). Lectures: 10
CREDIT -IV Web Security factors, E-Commerce security threats, security schemes, Protocols, Digital Certificates(03), Cyber law in India, Supply Chain Management (SCM): Components and issues(03), Customer Relationship Management (CRM): definition, Components, Benefits, ECRM: concept, impact, ECRM v/s CRM(04) Lectures: 10

E-commerce security is the protection of **e-commerce** assets from unauthorized access, use, alteration, or destruction.Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

- **Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever required within a time limit specified.
- **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
- **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
- **Encryption** − Information should be encrypted and decrypted only by an authorized user.
- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

Cyber-security represents maybe the most **important eCommerce** feature. Without the existence and implementation of proper protocols, online store owners put themselves and also their customers at risk for payment fraud. ... More than financial consequences, data breaches harm an **eCommerce** website's reputation.

Security issues in **e**-commerce such as integrity, authentication and non-repudiation must be dealt with effectively for any online business to be successful. Data integrity is the assurance that data transmitted is consistent and correct.

Electronic security system refers to any **electronic** equipment that could perform **security** operations like surveillance, access control, alarming or an intrusion control to a facility or an area which uses a power from mains and also a power backup like battery etc.

Computer Security – Threats & Solutions

Types of threats:

- Physical damage: fire, water, pollution.
- Natural events: climatic, seismic, volcanic.
- Loss of essential services: electrical power, air conditioning, telecommunication.
    - Compromise of information: eavesdropping, theft of media, retrieval of discarded materials.
    - Technical failures: equipment, software, capacity saturation,
    - Compromise of functions: error in use, abuse of rights, denial of actions

Solutions

- Install Anti-Virus Software.
- Ensure that the anti-virus software is up to date.
- Employ a firewall to protect networks.
- Filter all email traffic.
- Educate all users to be careful of suspicious e-mails.
- Scan Internet Downloads.
- Don't run programs of unknown origin.
- Implement a vulnerability management program.
- Make regular backups of critical data.
- Develop an Information Security Policy.
- Monitor logs and systems.
- Develop an Incident Response Plan.
- Restrict end user access to systems

Security Protocols

Security protocol In the today most e-business, many protocols are widely used such as Secure Socket Layers (SSL) and Secure Electronic Transactions (SET). So we would like to explore about these protocols. We will discuss the various methods that are used in the e-commerce such as Digital certificates, Digital signatures, Secure Socket Layer (SSL), Secure Electronic Transactions (SET).

1. **Digital Signatures and Certificates**

(DISCUSSED IN PREVIOUS LECTURES)

2. **Secure Socket Layers (SSL)** The Secure Socket Layer (SSL) was developed by Netscape to provide secure communication between Web servers and clients. Information sent over the Internet commonly uses the set of rules called TCP/IP (Transmission Control Protocol / Internet Protocol). The information is broken into packets, numbered

sequentially, and an error control attached. Individual packets are sent by different routes. TCP/IP reassembles them in order and resubmits any packet showing errors. SSL uses PKI and digital certificates to ensure privacy and authentication. The procedure is something like this: the client sends a message to the server, which replies with a digital certificate. Using PKI, server and client negotiate to create session keys, which are symmetrical secret keys specially created for that particular transmission. Once the session keys are agreed, communication continues with these session keys and the digital certificates.

3. **Secure Electronic Transactions (SET)** The SET Secure Electronic Transaction TM protocol is an open industry standard developed for the secure transmission of payment information over the Internet and other electronic networks. SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of "encrypting" or scrambling the information exchanged between the shopper and the online store, SET ensures a payment process that is convenient, private and most of all secure.

There are some advantages of SET as shown below:

• Establishes industry standards to keep your order and payment information confidential.

• Increases integrity for all transmitted data through encryption.

• Provides authentication that a cardholder is a legitimate user of a branded payment card account.

• Provides authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.

• Allows the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.

4. HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site. Users expect a secure and private online experience when using a website.Data sent using HTTPS is secured via *Transport Layer Security* protocol (TLS), which provides three key layers of protection:

1. Encryption—encrypting the exchanged data to keep it secure from eavesdroppers. That means that while the user is browsing a website, nobody can "listen" to their conversations, track their activities across multiple pages, or steal their information.
2. Data integrity—data cannot be modified or corrupted during transfer, intentionally or otherwise, without being detected.

3. Authentication—proves that your users communicate with the intended website. It protects against man-in-the-middle attacks and builds user trust, which translates into other business benefits.

Cyber Law (IT Law) in India

Cyber Crime

The **Information Technology Act 2000** or any legislation in the Country does not describe or mention the term **Cyber Crime**. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime related to computers.

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.
IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software licence is controversial and still evolving in Europe and elsewhere.

Importance of Cyber Law:

1. It covers all transaction over internet.
2. It keeps eyes on all activities over internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. ***Copyright*:**
   The internet has made copyright violations easier. In early days of online communication, copyright violations was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.
3. ***Defamation*:**
   Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. ***Harassment and Stalking*:**
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.
5. ***Freedom of Speech*:**
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

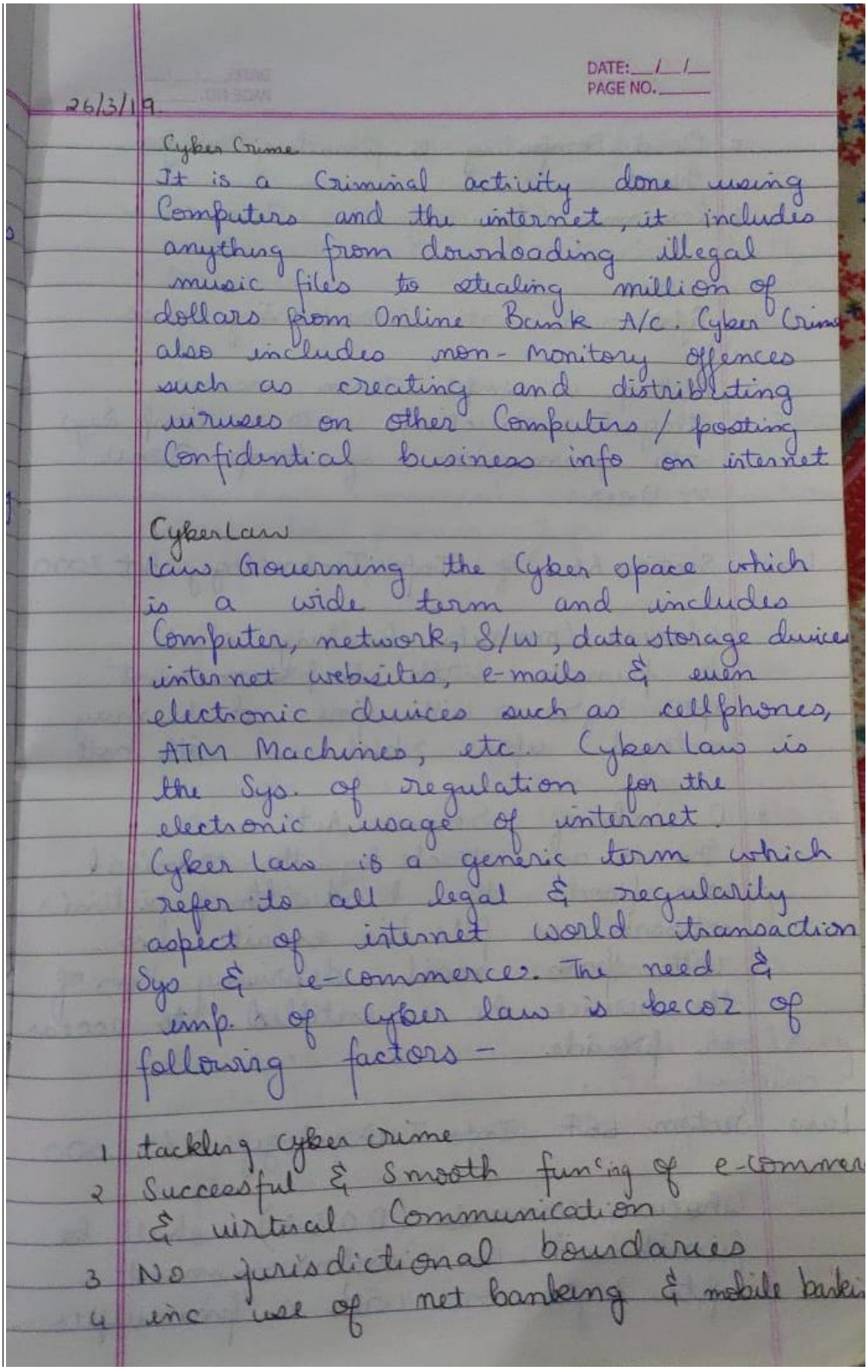
6. ***Trade Secrets*:**
   Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

7. ***Contracts and Employment Law*:**
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

1. Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
2. Digital signatures have been given legal validity and sanction in the Act.
3. It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
4. It allows Government to issue notification on the web thus heralding e-governance.
5. It gives authority to the companies or organizations to file any form, application or any other document with any office, authority, body or agency owned or controlled by the suitable Government in e-form by means of such e-form as may be prescribed by the suitable Government.
6. The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

Cybercrimes and the corresponding Cyber Laws:



DATE: __/__/__
PAGE NO. _____

26/3/19.

Cyber Crime

It is a Criminal activity done using Computers and the internet, it includes anything from downloading illegal music files to stealing million of dollars from Online Bank A/c. Cyber Crime also includes non-Monitory offences such as creating and distributing viruses on other Computers / posting Confidential business info on internet

CyberLaw

Laws Governing the Cyber space which is a wide term and includes Computer, network, S/W, data storage devices internet websites, e-mails & even electronic devices such as cellphones, ATM Machines, etc. Cyber law is the Sys. of regulation for the electronic usage of internet. Cyber Laws is a generic term which refer to all legal & regularity aspect of internet world transaction Sys & e-commerces. The need & imp. of Cyber law is becoz of following factors -

1 tackling cyber crime
2 Successful & Smooth funcing of e-commer & virtual Communication
3 No jurisdictional boundaries
4 inc use of net banking & mobile banki

PAGE NO.

5 Cloud Computing is providing major threat
6 Economic Efficiency

- Cyber Crime with Corresponding Laws

1 Hacking in simple term means illegal instructions into a Comp device with permission of Comp Owner or User

Law Section 66 of Info Technology Act 2000

Whoever commits hacking shall be punish with imprisonment upto 3 yrs or with fine which may extend upto 2 lakh or with both

2 Denial of Service Act
This is an attack by the criminal who floods the bandwidth of victim's network or fills his email box with spam mail depriving him of the service he is entitled to access or provide

Law Section 66F Info Technology Act 2000

Whoever commits (DOSA) shall be punish with an imprisonment upto 2 yrs or with a fine upto

DATE: / /
PAGE NO.

5 lakhs

3 Virus Dissimination

mallacious S/w that attaches itself to other S/w for eg virus, worms trojan horse, time bomb, logic bomb, rabbit are the mallacious S/w

Section 66C Info Technology Act 2000

law Who ever commint virus Dissimiation shall be punish 2 yrs imprisonment or fine upto 5 lakh

4 Cyber Stalking

It can be define as repetative act of harrasment or threatning behaviour of Cyber Criminal towards the victim by using internet services. Criminal follows victim by sending email & entring chat room frequently

Section 66 H Info Tech. Act 2000

Who ever commits Cyber Stalking shall be punish with imprisonment upto 2 yrs or fine upto 5 lakhs.

DATE: / /
PAGE NO.

5 S/w piracy
Theft of S/w through illegal Copying of genuine prog or counter fitting & distribution of products intnd intended to pass for the original.

law Section 66 B Info. Tech. Act 2000

Whoever commits S/w piracy shall be punish with imprisonment upto 2yrs and a fine upto 5 lakh

6 Fishing
it is technique of pulling out confidential info from bank of financial A/c holder by deceptive means.

Cyber Law

Section 66 A Info. Tech. Act 2000

Whoever commits phishing shall be commiat with imprisonment upto 3yrs. plus 2 lakh as a part of section 66.
or with a fine upto 5 lakhs.

7 Spoofing
getting one comp on network to pretend to have identity of

DATE: / /
PAGE NO.

another comp. usually one with special access permission so as to obtain access to other comp. or network

Law Section 66 D Info Tech. Act 2000

Whoever commits Spoofing shall be imprisonment upto 3yrs + rupees 2 lakh as part of section 66 and / or with a fine upto 5 lakhs.