

## unit-2

# Security and legal aspects of e-business

1. what are the threats in e-business

Ans:- Following are the threats in e-business -

(i) Hacking and data breaches:- Hackers can infiltrate e-business platforms to steal sensitive data such as customer information, financial details or intellectual property.

(ii) payment fraud:- online payment systems are vulnerable to credit card fraud, identity theft and charge backs which can result in financial losses.

(iii) Data misuse:- Strong customer data can lead to privacy concerns, especially if their data is mishandled or sold without consent.

(iv) System downtime:- Technical issues such as server outages or software malfunctions can lead to disruption

in service, lost sales and dis-satisfied customers.

⑤ Intense competition :- E-businesses face global competition which can drive down prices and affect profit margins.

⑥ Supply chain disruptions :- problems in the supplychain such as delays in shipping or product shortages can hinder the timely delivery of goods & services.

Q: Why are digital signatures?

Ans:- A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital document, message or software. It ~~seems~~ serves as an electronic equivalent of a handwritten signature or a stamped seal, providing a secure way to ensure that a document has not been altered and that it comes from a verified source.

3. What are the uses of digital sig.

Ans:- ① E-commerce transactions :- Digital signatures ensure that online payments and orders are secure, authentic.



-ticated and verified, reducing fraud.

(ii) Banking and financial services:- These are used to authorised high value transactions, secure communication between banks and authenticate users in online banking.

(iii) E-mail security:- Digital signatures are used to verify ~~sa~~ senders identify and ensure that email content has not been altered in transit.

(iv) Digital identification:- National ID systems or digital identity platforms may use digital signatures for authentication and secure access to services.

(v) Electronic voting:- Digital signatures can authenticate voters identify and ensure the integrity of voters in secure electronic voting system.

4.) write a note on security of clients and service providers.

Ans:- The security of both clients & service providers in an

foundation especially in e-business or online services is crucial to building trust, preventing ~~to~~ business data breaches and ensuring smooth transactions. There are several practices, technologies and policies that help protect both parties -



ChatGPT



## Security of Clients:

1. **Data Encryption:** Protects client data during transmission to prevent unauthorized access.
2. **Authentication:** Requires strong passwords, multi-factor authentication (MFA), or biometrics to verify client identity.
3. **Privacy Protection:** Ensures compliance with data protection laws (e.g., GDPR) to safeguard personal information.
4. **Secure Payments:** Uses encryption and tokenization to protect financial data during transactions.
5. **Regular Updates:** Ensures that client-side applications are patched and updated regularly to address security vulnerabilities.
6. **Access Control:** Limits access to sensitive data based on roles and permissions.

## Security of Service Providers:

1. **Data Encryption:** Encrypts stored data and communication with clients to prevent



Message ChatGPT







ChatGPT



## Security of Service Providers:

1. **Data Encryption:** Encrypts stored data and communication with clients to prevent breaches.
2. **Server Security:** Protects servers with firewalls, intrusion detection systems (IDS), and regular security audits.
3. **Incident Response Plan:** Establishes protocols to quickly address and mitigate security breaches.
4. **Compliance and Certification:** Adheres to industry standards (e.g., ISO, SOC) for data security and privacy.
5. **Regular Security Audits:** Conducts frequent vulnerability assessments and penetration testing.
6. **Access Management:** Implements strict controls on who can access critical systems and data within the organization.



Message ChatGPT



5. What are the features of IT Act 2000

Ans: (i) Legal recognition of electronic records: The IT Act 2000 <sup>grant</sup> legal recognition to electronic documents, making them equivalent to physical documents, provided they are digitally ~~sign~~ signed.

(ii) Digital signature: The Act provides a legal framework for the use of digital signature, which are used to authenticate electronic records.

(iii) Protection of data & privacy: It contains provision related to the protection of sensitive personal data and information ~~from~~ from unauthorised access or misuse.

(iv) Cyber tribunals: The act provided

for the establishment of cyber appellate tribunals to handle disputes arising from the use of information technology.

- ① E-commerce provision: It facilitates the development of e-commerce by allowing secure electronic transaction, contracts and records.
- 

6. Explain the relevant provision of IT Act 2000.

Ans:- The IT act 2000 is a comprehensive legal framework that addresses various aspects of cyber law in India. Following are the important provisions of IT Act 2000:

- ① Section 3 (authentication of electronic records): provides the legal framework for the authentication of electronic records through digital



signature.

① Sec. 4 (Legal recognition of electronic records): Grants legal recognition to electronic records, making them equivalent to paper based document.

② Sec 5 (Legal recognition of digital signature): specified that a digital signature is legally valid and can be used to authenticate & electronic document

④ Sec 10 A (Validity of e-contracts)  
Recognises contracts <sup>form</sup> through electronic means as legally valid.

⑤ Sec 66 (computer related offenses): It Imposes penalties & imprisonment for hacking, unauthorised access & data theft. It includes imprisonment of upto three years or a

fine of upto rupees 5 lakh

- (vi) Sec 70 (protected system): Authorises the govt. to declare any computer, computer system, or network as a protected system. Any unauthorised access to such system is punishable imprisonment
- 

7. What are the different ways of securing electronic records?

Ans:- (i) Encryption: It is the process of converting data into a coded format that can only be accessed by those who possess the decryption key.

(ii) Digital signature: Given

(iii) Access control: Proper access control mechanism such as authentication and authorisation help ensure that only authorised personnel can access or modify electronic records.



④ Data integrity: Ensuring the integrity of electronic records means protecting them from unauthorised modification or tampering.

⑤ Data backup & recovery: Regular backups are essential to protect electronic records against data loss caused by system failure, cyber attacks or natural disasters.

8. Explain the various cyber law offences.

Ans:- ① Hacking: It involves unauthorised access to a computer system or network with the intent to steal, alter or destroy data.

② Data theft: Unauthorised access, downloading, copying or extracting data from a computer system including data bases or file, without permission.

(iii) Identity theft: The fraudulent use of another person's identity information such as passwords, digital signatures or biometric data to gain unauthorized access or ~~commit~~ <sup>commit</sup> fraud.

(iv) Phishing and online fraud: Impersonation using electronic means to ~~deceit~~ <sup>deceive</sup> an individual into providing personal or financial information.

(v) Spamming: Sending unsolicited bulk messages or e-mails often for commercial purposes which can lead to system overload or privacy violation.

3. What are the penalties for various cyber law offenses?

Ans: ① Hacking (Sec 66): \* Imprisonment up to 3 years

\* Fine upto ₹ 5 lakh.



② Data Theft (sec 43): Compensation upto ₹ 1 crore.

③ Identity Theft (sec 66C):

\* Imprisonment up to 3 years

\* Fine up to ₹ 1 lakh.

④ Phishing / Impersonation (sec 66D):

\* Imprisonment up to 3 years

\* Fine up to ₹ 1 lakh.

⑤ Violation of privacy (sec 66E):

\* Imprisonment up to 3 years.

\* Fine up to ₹ 2 lakh.

⑥ Publishing obscene material (sec 67):

\* First offense: Imprisonment up to 3 years and fine upto ₹ 5 lakh

\* Subsequent offense: Imprisonment up to 5 years and fine up to ₹ 10 lakh.

⑦ Publishing sexually explicit content (sec 67A):

\* Imprisonment up to 5 years.

\*. Fine up to ₹ 10 lakh

(viii) Child pornography (sec 67B) :

\*. First offense : Imprisonment up to 5 years and fine up to ₹ 10 lakh

\*. Subsequent offense : Imprisonment up to 7 years and fine up to ₹ 10 lakh

(iv) Cyber terrorism (Sec 66F) : Imprisonment for life.

(x) Unauthorized Access to protected system (sec 70) :

\*. Imprisonment up to 10 years.

\*. Fine (<sup>unspecified</sup> ~~unspecified~~ amount).

(xi) Tampering with source code (sec 65)

\*. Imprisonment up to 3 years

\*. Fine up to ₹ 2 lakh.

(xii) Breach of confidentiality and privacy (sec 71) :

\*. Imprisonment up to 2 years

\*. Fine up to ₹ 1 lakh.