Chapter 9 – Overview of Cyber Security

Cyber Security क्या है?

Cyber Security वह प्रक्रिया है जिसके द्वारा Computer, Mobile, Network, Software और Digital Data को unauthorized access, चोरी, नुकसान तथा cyber attacks से सुरक्षित रखा जाता है।

सरल शब्दों में, Internet और Digital Devices का सुरक्षित उपयोग करना तथा अपनी जानकारी को hackers और scammers से बचाना Cyber Security कहलाता है।

उदाहरण: Computer में antivirus रखना, Mobile पर screen lock लगाना, Email में 2-Step Verification चालू करना और अनजान links पर click न करना।

Cyber Security की आवश्यकता (Need of Cyber Security)

आज हम Online Banking, UPI, Shopping, Social Media, Email और Government Services का उपयोग करते हैं। इनमें हमारी personal और financial information होती है, इसलिए Cyber Security आवश्यक है।

इसके मुख्य उद्देश्य हैं:

1. **Confidentiality (गोपनीयता):** जानकारी केवल authorized व्यक्ति ही देख सके।
2. **Integrity (अखंडता):** Data में बिना अनुमति बदलाव न हो।
3. **Availability (उपलब्धता):** जरूरत पड़ने पर data और services उपलब्ध रहें।

इन तीनों को **CIA Triad** कहा जाता है।

उदाहरण: Bank account की जानकारी गुप्त रखना Confidentiality है; transaction records में गलत बदलाव न होने देना Integrity है; और जरूरत पर banking service का उपलब्ध होना Availability है।

Cyber Security के अन्य उद्देश्य:

- Personal और financial data की सुरक्षा।
- Identity theft और online fraud को रोकना।

Hi-Tech

- Computer और Mobile को malware से बचाना।
- Privacy तथा digital identity की सुरक्षा।
- Online services को सुरक्षित और भरोसेमंद बनाना।

Cyber Threat, Cyber Attack और Cyber Crime

- **Cyber Threat:** ऐसा संभावित खतरा जो computer, network या data को नुकसान पहुँचा सकता है।
- **Cyber Attack:** Computer system या account को नुकसान पहुँचाने अथवा unauthorized access पाने का प्रयास।
- **Cyber Crime:** Computer, Mobile या Internet का उपयोग करके किया गया अपराध।

उदाहरण: किसी व्यक्ति का password चुराने का प्रयास cyber attack हो सकता है; चोरी किए गए password से उसके account से पैसे निकालना cyber crime हो सकता है।

Malware क्या है?

Malware (Malicious Software) ऐसा software है जिसे computer, mobile या data को नुकसान पहुँचाने, जानकारी चुराने अथवा unauthorized activity करने के लिए बनाया जाता है।

Malware के प्रमुख प्रकार:

1. Virus: ऐसा malicious program जो किसी file या program से जुड़कर फैल सकता है। संक्रमित file चलाने पर यह सक्रिय हो सकता है।

2. Worm: ऐसा malware जो network के माध्यम से स्वयं की copies बनाकर फैल सकता है। इसे फैलने के लिए सामान्यतः किसी दूसरी file से जुड़ना आवश्यक नहीं होता।

3. Trojan Horse: ऐसा malicious program जो उपयोगी या genuine software जैसा दिखाई देता है, लेकिन अंदर से नुकसान पहुँचाता है।

4. Ransomware: ऐसा malware जो files को encrypt करके या system को lock करके उन्हें वापस देने के बदले पैसे माँग सकता है।

5. Spyware: उपयोगकर्ता की गतिविधियों या जानकारी की गुप्त निगरानी करने वाला software।

6. Adware: ऐसा software जो unwanted advertisements दिखाता है। कुछ adware tracking भी कर सकते हैं।

7. Keylogger: ऐसा program या device जो keyboard पर टाइप की गई जानकारी record कर सकता है, जिसमें passwords भी शामिल हो सकते हैं।

8. Rootkit: ऐसा malicious software जो system में अपनी मौजूदगी छिपाने और unauthorized access बनाए रखने का प्रयास कर सकता है।

Exam में याद रखें:

- Files को encrypt करके पैसे माँगना — Ransomware
- खुद की copies बनाकर network में फैलना — Worm
- Genuine software जैसा दिखना — Trojan Horse
- गुप्त रूप से जानकारी इकट्ठा करना — Spyware
- Keystrokes record करना — Keylogger

अन्य प्रमुख Cyber Attacks

1. Phishing: Fake Email, Website या Message के माध्यम से password, OTP या banking details चुराने का प्रयास।

2. Vishing: Voice call के माध्यम से धोखाधड़ी करके जानकारी या पैसे लेना।

3. Smishing: SMS या text message के माध्यम से fake links भेजकर धोखाधड़ी करना।

4. Spoofing: किसी genuine व्यक्ति, Email address, phone number या website की नकली पहचान बनाकर भरोसा जीतने का प्रयास।

5. Brute-Force Attack: बहुत सारे संभावित passwords आजमाकर सही password का पता लगाने का प्रयास।

6. Password Attack / Credential Stuffing: पहले से leak हुए username-password combinations को दूसरी websites पर आजमाना।

7. Denial of Service (DoS): किसी service पर अत्यधिक requests भेजकर उसे सामान्य users के लिए unavailable करना। Distributed रूप को DDoS कहते हैं।

8. Social Engineering: तकनीकी कमजोरी के बजाय इंसान की भावनाओं, डर, लालच या भरोसे का फायदा उठाकर गोपनीय जानकारी प्राप्त करना।

9. Identity Theft: किसी दूसरे व्यक्ति की personal information का गलत उपयोग करके उसकी पहचान अपनाना।

10. Man-in-the-Middle Attack: दो पक्षों के बीच communication को गुप्त रूप से intercept करना या उसमें बदलाव करने का प्रयास।

Cyber Security से जुड़े महत्वपूर्ण शब्द

- **Hacker:** Computer systems की security को समझने या उनमें प्रवेश करने वाला व्यक्ति। हर hacker अपराधी नहीं होता।
- **Ethical Hacker:** अनुमति लेकर system की कमजोरियों की जाँच करने वाला security professional।
- **Firewall:** Incoming और outgoing network traffic को निर्धारित security rules के अनुसार filter करने वाला सुरक्षा तंत्र।
- **Antivirus / Anti-malware:** Malware को detect, block और जहाँ संभव हो remove करने वाला software।
- **Encryption:** Readable data को ऐसी coded form में बदलना जिसे उचित key के बिना पढ़ना कठिन हो।
- **Decryption:** Encrypted data को वापस readable form में बदलना।
- **Backup:** Data की अतिरिक्त copy बनाकर सुरक्षित रखना, ताकि data loss होने पर उसे restore किया जा सके।

- **Patch / Security Update:** Software की security weakness या bug को ठीक करने वाला update।
- **Authentication:** यह सत्यापित करना कि user कौन है।
- **Authorization:** यह निर्धारित करना कि authenticated user क्या कर सकता है।
- **Biometrics:** Fingerprint या Face Recognition जैसी शारीरिक विशेषताओं के आधार पर पहचान सत्यापित करना।

Password Security

Password किसी account या system को access करने के लिए उपयोग किया जाने वाला secret credential है।

Strong Password बनाने के नियम:

1. Password लंबा और अनुमान लगाना कठिन रखें।
2. हर महत्वपूर्ण account के लिए अलग password रखें।
3. नाम, जन्मतिथि, mobile number या 123456 जैसे आसानी से अनुमान लगाए जाने वाले passwords से बचें।
4. Password किसी दूसरे व्यक्ति के साथ share न करें।
5. Password को सुरक्षित रखने के लिए trusted password manager का उपयोग किया जा सकता है।
6. Public या shared computer पर password save न करें।

Weak Password: 12345678, password123

Better Example: कई unrelated words से बना लंबा passphrase, जिसमें जरूरत के अनुसार numbers या symbols शामिल हों।

Two-Factor Authentication (2FA) और MFA

Two-Factor Authentication (2FA) में login के लिए दो अलग-अलग प्रकार के verification factors उपयोग होते हैं।

मुख्य factors:

- **Something you know:** Password या PIN।
- **Something you have:** Registered phone, authenticator app या security key।
- **Something you are:** Fingerprint या Face Recognition।

MFA (Multi-Factor Authentication) में दो या अधिक authentication factors का उपयोग होता है।

उदाहरण: Password के साथ authenticator code माँगना 2FA है।

OTP (One-Time Password): एक बार के verification के लिए बनाया गया temporary code। OTP को किसी अनजान व्यक्ति के साथ share नहीं करना चाहिए—चाहे वह खुद को bank employee या support staff बताए।

Passkey: Sign-in की एक आधुनिक विधि, जो compatible device पर cryptographic credentials और अक्सर device PIN या biometrics का उपयोग करती है। यह पारंपरिक passwords की तुलना में phishing से बेहतर सुरक्षा दे सकती है।

Securing PC (Computer को सुरक्षित रखना)

Computer को सुरक्षित रखने के लिए निम्न उपाय अपनाने चाहिए:

1. Operating System और software को नियमित रूप से update करें।
2. Trusted antivirus या anti-malware protection चालू रखें।
3. Firewall को चालू रखें।
4. केवल trusted sources से software download करें।
5. Pirated software और unknown USB drives से बचें।

6. महत्वपूर्ण files का नियमित backup लें।
7. Strong password या PIN से login सुरक्षित करें।
8. जब computer उपयोग में न हो, तो screen lock करें।
9. Unknown Email attachments और suspicious links न खोलें।
10. Administrator account का उपयोग केवल जरूरत पड़ने पर करें।
11. Public computer पर अपना account logout करना न भूलें।
12. Sensitive data वाली files को जरूरत के अनुसार encrypt करें।

Firewall और Antivirus में अंतर:

- Firewall network traffic को filter करके unauthorized connections रोकने में सहायता करता है।
- Antivirus/Anti-malware malicious files और programs को पहचानने तथा रोकने में सहायता करता है।

दोनों एक-दूसरे के विकल्प नहीं हैं।

Securing Browser (Internet Browser को सुरक्षित रखना)

Browser जैसे Chrome, Firefox और Edge का उपयोग websites खोलने के लिए किया जाता है।

Browser को सुरक्षित रखने के उपाय:

1. Browser को updated रखें।
2. Websites का सही domain name ध्यान से जाँचें।
3. Sensitive information डालने से पहले HTTPS और certificate/security warnings पर ध्यान दें।
4. Unknown websites से files download न करें।
5. Unnecessary extensions install न करें।
6. Pop-ups और suspicious notifications से सावधान रहें।

7. Cookies और site permissions को जरूरत के अनुसार manage करें।
8. Public computer पर काम करने के बाद logout करें और जरूरत के अनुसार browsing data हटाएँ।
9. Browser में passwords save करने से पहले device की security पर विचार करें।
10. Fake login pages पर password या OTP न डालें।

HTTP और HTTPS में अंतर:

- HTTP में connection encryption अपने आप सुनिश्चित नहीं होती।
- HTTPS, HTTP के साथ TLS encryption का उपयोग करता है, जिससे browser और website के बीच data अधिक सुरक्षित तरीके से भेजा जा सकता है।

Important: HTTPS का होना यह guarantee नहीं करता कि website genuine या trustworthy ही है। Fraudulent websites भी HTTPS का उपयोग कर सकती हैं।

Cookies: छोटी data files जिन्हें websites browser में store कर सकती हैं। इनका उपयोग login session, preferences और tracking जैसे कार्यों में हो सकता है।

Private / Incognito Mode: यह मुख्यतः उसी device पर browsing history और कुछ local data के save होने को सीमित करता है। यह user को ISP, employer, school network या हर प्रकार की tracking से पूरी तरह invisible नहीं बनाता।

Securing Email Account

Email account में personal messages, documents और password reset links हो सकते हैं। इसलिए इसे सुरक्षित रखना आवश्यक है।

सुरक्षा के उपाय:

1. Strong और unique password रखें।
2. 2-Step Verification या MFA चालू करें।
3. Sender का Email address ध्यान से जाँचें।

4. Suspicious links और unexpected attachments न खोलें।
5. Urgent payment या confidential information माँगने वाले messages को अलग channel से verify करें।
6. Email account की recovery details updated रखें।
7. Account की recent activity और logged-in devices की जाँच करें।
8. Unknown forwarding rules या filters दिखाई दें तो उनकी जाँच करें।
9. Public computer पर काम के बाद sign out करें।

Spam: Unwanted या unsolicited messages, जो अक्सर bulk में भेजे जाते हैं।

Email Phishing: Fake message के जरिए user को नकली login page पर ले जाकर password या financial information चुराने का प्रयास।

Spear Phishing: किसी खास व्यक्ति या organization को target करके बनाया गया अधिक personalized phishing attack।

Securing Social Media Accounts

Facebook, Instagram और WhatsApp जैसे platforms पर account security के साथ privacy भी महत्वपूर्ण है।

Facebook और Instagram के लिए:

- Strong password और MFA का उपयोग करें।
- Profile की privacy settings की समीक्षा करें।
- Unknown friend requests और suspicious messages से सावधान रहें।
- Unknown apps और websites को account access देने से बचें।
- Login alerts और active sessions की जाँच करें।
- Personal details, location और travel plans को जरूरत से ज्यादा public न करें।

WhatsApp के लिए:

- Two-step verification चालू करें।
- Linked Devices में अनजान device दिखाई दे तो उसे log out करें।
- WhatsApp registration या verification code किसी के साथ share न करें।
- अनजान QR code scan करने या किसी अनजान device को link करने से बचें।
- Suspicious accounts को block और report करें।
- Privacy settings में profile photo, last seen और group permissions को जरूरत के अनुसार सीमित करें।

Impersonation: किसी दूसरे व्यक्ति की नकली profile बनाना या उसकी पहचान का गलत उपयोग करना।

Account Takeover: जब कोई unauthorized व्यक्ति आपके account का control प्राप्त कर लेता है।

Securing Smartphone

आज Smartphone में banking apps, Email, personal photos, contacts और कई accounts जुड़े होते हैं। इसलिए इसकी security बहुत जरूरी है।

मुख्य सुरक्षा उपाय:

1. Screen lock के लिए मजबूत PIN, password या biometric lock लगाएँ।
2. Operating System और apps को updated रखें।
3. Apps केवल trusted official app stores से install करें।
4. App permissions की समीक्षा करें; जरूरत से ज्यादा access न दें।
5. अनजान APK files install करने से बचें।
6. Device खो जाने पर उपलब्ध Find My Device / Find My iPhone जैसे tools का उपयोग करें।
7. Sensitive accounts में MFA चालू रखें।

8. Public Wi-Fi पर sensitive transactions करते समय सावधानी बरतें।
9. Unknown charging accessories या USB connections से बचें, खासकर जब device data access की अनुमति माँगे।
10. जरूरी data का backup रखें।
11. अनजान links और QR codes से सावधान रहें।
12. खोए हुए phone की स्थिति में SIM और important accounts को सुरक्षित करने के लिए संबंधित service provider से संपर्क करें।

App Permissions: Apps को camera, microphone, location, contacts या files जैसी सुविधाओं का access देने की अनुमति।

Public Wi-Fi: ऐसी Wi-Fi service जिसे कई लोग उपयोग कर सकते हैं। इसका उपयोग करते समय network की authenticity verify करें और sensitive कामों में अतिरिक्त सावधानी रखें।

Bluetooth Security: Bluetooth को जरूरत न होने पर बंद रखें और unknown pairing requests स्वीकार न करें।

Online Fraud के आधुनिक तरीके

1. QR Code Scam: Scammer fake QR code भेजकर user को malicious website पर ले जा सकता है या उसे धोखे से payment approve करने के लिए प्रेरित कर सकता है। किसी QR code को scan करने से पहले उसका उद्देश्य समझें।

2. UPI Collect Request Scam: किसी अनजान व्यक्ति के भेजे payment request को ध्यान से पढ़े बिना approve न करें। पैसे प्राप्त करने के लिए सामान्यतः UPI PIN डालने की आवश्यकता नहीं होती।

3. Fake Customer Care Scam: Search results या social media पर मिले नकली customer-care number के जरिए fraud किया जा सकता है। Official app या website से contact details लें।

4. Digital Arrest Scam: Scammer पुलिस, सरकारी अधिकारी या किसी agency का झूठा रूप लेकर गिरफ्तारी का डर दिखा सकता है और पैसे माँग सकता है। घबराकर पैसे न भेजें; स्वतंत्र रूप से संबंधित agency की पहचान verify करें।

5. AI-based Phishing: AI की मदद से बहुत convincing emails, messages और fake websites बनाई जा सकती हैं।

6. Deepfake Voice/Video: AI द्वारा बनाई या बदली गई आवाज या video से किसी परिचित व्यक्ति की नकली पहचान बनाई जा सकती है। पैसे या sensitive information की urgent request को किसी दूसरे विश्वसनीय माध्यम से verify करें।

7. SIM Swap Fraud: Scammer mobile number पर control पाने की कोशिश कर सकता है, जिससे OTP या account recovery प्रभावित हो सकती है। अचानक mobile network बंद होने पर service provider से तुरंत संपर्क करें।

8. Remote Access App Scam: Scammer user को ऐसी app install करने के लिए कह सकता है जिससे device को दूर से access किया जा सके। अनजान व्यक्ति के कहने पर remote access app install न करें।

वर्तमान समय की जरूरी Security Practices

Technology बदल रही है, इसलिए पुराने सुरक्षा नियमों के साथ नए तरीकों को भी समझना जरूरी है।

- **Passkeys:** Supported services पर passkeys का उपयोग password-based phishing के जोखिम को कम कर सकता है।
- **Authenticator Apps / Security Keys:** जहाँ उपलब्ध हों, SMS-only verification के अलावा मजबूत authentication विकल्पों पर विचार करें।
- **AI और Deepfake Awareness:** केवल आवाज, video या profile photo देखकर identity को genuine न मानें।
- **Password Reuse से बचें:** एक website का password leak होने पर दूसरे accounts भी खतरे में पड़ सकते हैं।
- **Session Security:** केवल password बदलना ही पर्याप्त नहीं हो सकता; account के active sessions और linked devices भी जाँचें।
- **Least Privilege:** Apps और users को केवल उतनी permissions दें जितनी आवश्यक हों।

- **Regular Backups:** Ransomware या device failure की स्थिति में backup मदद कर सकता है। महत्वपूर्ण backup की एक copy device से अलग या सुरक्षित location पर रखें।

Cyber Crime होने पर क्या करें?

यदि online financial fraud हो जाए:

1. तुरंत अपने bank, payment provider या संबंधित service को सूचित करें।
2. भारत में financial cyber fraud की तत्काल reporting के लिए **1930** पर संपर्क करें।
3. National Cyber Crime Reporting Portal पर complaint दर्ज करें: **https://cybercrime.gov.in/**
4. Transaction ID, समय, amount, screenshots, messages और suspect details जैसे evidence सुरक्षित रखें।
5. Passwords बदलें, active sessions revoke करें और जरूरत पड़ने पर affected accounts block करवाएँ।
6. संदिग्ध message या call को केवल delete करने के बजाय, reporting के लिए आवश्यक evidence सुरक्षित रखें।

महत्वपूर्ण: जल्दी report करने से संबंधित authorities और financial service providers को कार्रवाई करने का अवसर मिल सकता है, लेकिन पैसे वापस मिलने की guarantee नहीं होती।

Quick Revision – Exam में याद रखने योग्य बातें

Term	**पहचान**
CIA Triad	Confidentiality, Integrity, Availability
Virus	File/program से जुड़कर फैल सकता है
Worm	Network पर स्वयं फैल सकता है
Trojan Horse	Genuine software जैसा दिखने वाला malware
Ransomware	Data lock/encrypt करके ransom माँग सकता है

Hi-Tech

Spyware	गुप्त निगरानी करता है
Phishing	Fake Email/Website/Message
Vishing	Voice call से धोखाधड़ी
Smishing	SMS/Text से धोखाधड़ी
Firewall	Network traffic filter करता है
Antivirus	Malware detection/blocking में मदद करता है
Encryption	Data को coded form में बदलना
2FA	दो अलग authentication factors
Passkey	Password के विकल्प के रूप में secure sign-in method
HTTPS	TLS के माध्यम से connection encryption
Backup	Data की अतिरिक्त सुरक्षित copy
1930	भारत में financial cyber fraud helpline
cybercrime.gov.in	National Cyber Crime Reporting Portal

Hi-Tech