SIBANI MANDAL MAHAVIDYALAYA

Village + P.O. Namkhana

Dist. South 24 Parganas

West Bengal

Computer Applications

SEC-3, 4-Year Education Major

L8: সাইবার স্টকিং, সাইবার অপরাধ এবং সাইবার নৈতিকতা

Cyber Stalking, Cyber Crimes এবং Cyber Ethics

একটি বিস্তৃত রিভিউ

---

১. ভূমিকা

ডিজিটাল যুগে ইন্টারনেট, সামাজিক যোগাযোগমাধ্যম ও অনলাইন প্ল্যাটফর্ম মানুষের যোগাযোগ, কাজ, শিক্ষা ও বিনোদনের মাধ্যমে বিপুল সুবিধা এনেছে। তবে এই অগ্রগতির সঙ্গে এসেছে নানা ধরনের **সাইবার অপরাধ**, **পরিচয় চুরি**, **অনলাইন হয়রানি**, **গোপনীয়তা লঙ্ঘন** এবং **নৈতিকতার অবক্ষয়**।
বিশেষত **Cyber Stalking**, বিভিন্ন **Cyber Crimes**, এবং **Cyber Ethics** বর্তমান সময়ের গুরুত্বপূর্ণ আলোচনার বিষয়।

---

২. Cyber Stalking – ধারণা, বৈশিষ্ট্য ও প্রকারভেদ

২.১ Cyber Stalking কী?

Cyber Stalking হলো কোনো ব্যক্তিকে অনলাইন বা ডিজিটাল মাধ্যমে **বারবার অনুসরণ, নজরদারি, হুমকি, হয়রানি বা মানসিক চাপ** প্রদান করা।
এটি সাধারণত সামাজিক যোগাযোগমাধ্যম, ইমেল, মেসেঞ্জার, ফোন, GPS ট্র্যাকিং বা ফেক প্রোফাইলের মাধ্যমে করা হয়।

২.২ Cyber Stalking-এর বৈশিষ্ট্য

- বারবার মেসেজ বা ইমেল পাঠানো
- অজ্ঞাত পরিচয়ে হুমকি বা কটূক্তি
- ব্যক্তির অনলাইন কার্যকলাপ নজরদারি
- Location tracking
- ব্যক্তিগত ছবি/তথ্য ব্যবহার করে ব্ল্যাকমেইল
- Fake profile থেকে যোগাযোগ
- ব্যক্তিকে অনলাইনে মানসিকভাবে আক্রমণ/হয়রানি

২.৩ Cyber Stalking-এর প্রধান প্রকারভেদ

১. Direct Stalking:

ভুক্তভোগীর অ্যাকাউন্টে সরাসরি মেসেজ/হুমকি পাঠানো।

২. Cyber Harassment:

গালি, হেনস্তা, কটূক্তি, ট্রোলিং বা অপমানজনক মন্তব্য।

৩. Surveillant Stalking:

ব্যক্তির অনলাইন কার্যকলাপ পর্যবেক্ষণ, যেমন location snooping, profile monitoring।

৪. Impersonation Stalking:

ভুক্তভোগীর নামে **ভুয়া প্রোফাইল তৈরি** করে অপকর্ম করা।

৫. Image-based Stalking:

আপত্তিকর ছবি/ভিডিও দিয়ে ভয় দেখানো বা ব্ল্যাকমেইল (revenge porn সম্পর্কিত)।

২.৪ Cyber Stalking-এর প্রভাব

- মানসিক চাপ, উদ্বেগ, বিষণ্নতা
- সামাজিক বিচ্ছিন্নতা
- আত্মসম্মানহানি
- নিরাপত্তাহীনতা
- আত্মহত্যাপ্রবণতা পর্যন্ত দেখা যায়

---

৩. Cyber Crimes – ধারণা, প্রকারভেদ ও প্রযুক্তিগত পটভূমি

৩.১ Cyber Crime কী?

কম্পিউটার, ইন্টারনেট, নেটওয়ার্ক বা ডিজিটাল প্রযুক্তি ব্যবহার করে সংঘটিত যেকোনো অপরাধকে Cyber Crime বলা হয়।

এটি ব্যক্তি, প্রতিষ্ঠান, সরকার ও সমাজের নিরাপত্তা, গোপনীয়তা ও আর্থিক স্থিতি ক্ষতি করতে পারে।

৩.২ Cyber Crime-এর প্রধান প্রকারভেদ

১. Financial Cyber Crime

- অনলাইন ব্যাংক প্রতারণা
- ATM/credit card fraud
- Phishing ও ভুয়া ওয়েবসাইট
- Ransomware দিয়ে মুক্তিপণ দাবি

২. Identity Theft

- ব্যক্তিগত তথ্য চুরি
- ভুয়া পরিচয় ব্যবহার
- সোশ্যাল মিডিয়া অ্যাকাউন্ট হ্যাক

৩. Hacking Crimes

- Unauthorized access
- Network breach
- Password cracking
- Server penetration

৪. Cyber Terrorism

- সরকার/প্রতিষ্ঠানের ডেটা আক্রমণ
- জাতীয় নিরাপত্তা ঝুঁকি

৫. Cyber Bullying

- অনলাইনে অপমান, ভয় দেখানো
- শিশু/কিশোরদের মানসিক ক্ষতি

৬. Online Sexual Crimes

- Grooming
- Child pornography
- Revenge porn

৭. Malware/Spyware Attack

- ভাইরাস, র‍্যানসমওয়্যার, ট্রোজান
- তথ্য চুরি, সিস্টেম নষ্ট

৮. Fake News & Misinformation

- সামাজিক অস্থিরতা সৃষ্টি
- জনগণকে বিভ্রান্ত করা

৩.৩ Cyber Crime কিভাবে ঘটে? (Tech Mechanisms)

- Keylogging
- Password sniffing
- Social engineering
- Malicious link injection
- Public Wi-Fi exploitation
- Data interception
- Zero-day attack

৩.৪ ভারতের আইনে Cyber Crime

ভারতের মূল সাইবার আইন: **Information Technology Act, 2000 (IT Act 2000)**
এতে রয়েছে—

- Section 66A: Offensive messages
- Section 66C: Identity theft
- Section 66D: Cheating by impersonation
- Section 67: Obscene material publishing
- Section 43, 45: Unauthorized access

অপরাধের মাত্রা অনুযায়ী কারাদণ্ড ও জরিমানার বিধান রয়েছে।

---

৪. Cyber Ethics – সংজ্ঞা, উপাদান ও গুরুত্ব

৪.১ Cyber Ethics কী?

Cyber Ethics হলো ডিজিটাল প্রযুক্তি ব্যবহার করার সময় অনুসরণীয় **নৈতিক নিয়ম, মূল্যবোধ এবং আচরণবিধি**।
এটি সঠিক ব্যবহার, সততা, গোপনীয়তা সম্মান, অন্যের তথ্য নিরাপত্তা রক্ষা ও নৈতিক যোগাযোগ শেখায়।

৪.২ Cyber Ethics-এর মূল নীতি

✔১. Respect & Privacy

অন্যের ব্যক্তিগত তথ্য শেয়ার না করা।
গোপনীয়তা রক্ষা করা।

✔২. Honesty & Authenticity

ভুয়া প্রোফাইল, ভুয়া খবর, ভুয়া পরিচয় ব্যবহার না করা।

✔৩. Non-harmful Behavior

Cyberbullying, trolling, harassment না করা।

✔৪. Intellectual Property Respect

পাইরেসি, কপি–পেস্ট (plagiarism) না করা।

✔৫. Safe Information Sharing

OTP, পাসওয়ার্ড, ব্যাংক তথ্য শেয়ার না করা।

✔৬. Digital Footprint Consciousness

পোস্ট/মন্তব্য যেন ভবিষ্যতে নিজের ক্ষতি না করে।

✔৭. Responsible Social Media Use

দায়িত্বশীল ভাষা, ইতিবাচক যোগাযোগ।

---

৫. Cyber Stalking ও Cyber Crime প্রতিরোধে করণীয়

৫.১ ব্যক্তিগত নিরাপত্তা

- Strong Password + 2FA
- Privacy Settings
- সন্দেহজনক লিঙ্কে ক্লিক না করা
- Public Wi-Fi এড়ানো
- Regular software updates

৫.২ সামাজিক যোগাযোগমাধ্যম নিরাপত্তা

- Friend request যাচাই
- Location sharing বন্ধ
- Profile lock/Restricted mode
- Report/Block ব্যবহার

৫.৩ প্রযুক্তিগত নিরাপত্তা

- Antivirus
- Firewall
- Anti-phishing tools
- VPN
- Backup system

৫.৪ আইনগত করণীয়

- Cyber Crime portal (www.cybercrime.gov.in)
- নিকটস্থ থানায় অভিযোগ
- 1930 হেল্পলাইনে কল

৬. উপসংহার

Cyber Stalking এবং Cyber Crime আজকের ডিজিটাল সমাজে উল্লেখযোগ্য ঝুঁকি তৈরি করেছে। এর মোকাবিলায় ব্যবহারকারীর সতর্কতা, আইনগত সচেতনতা এবং প্রযুক্তিগত সুরক্ষা ব্যবস্থা অত্যন্ত গুরুত্বপূর্ণ।
সেই সঙ্গে Cyber Ethics অর্থাৎ নৈতিক ও দায়িত্বশীল ডিজিটাল আচরণই অনলাইন বিশ্বকে নিরাপদ, সম্মানজনক ও মানবিক করার প্রধান উপায়।

⭐ MCQ Set – 55 Questions

(Cyber Stalking • Cyber Crime • Cyber Ethics)

A. Cyber Stalking – Basics & Concepts

১. Cyber Stalking কী?

A) অফলাইনে অনুসরণ
B) অনলাইনে বারবার হয়রানি/হুমকি
C) ছবি এডিট করা
D) ইন্টারনেট ব্রাউজিং
✔উত্তর: B

২. Cyber Stalking সাধারণত কোথায় ঘটে?

A) ফোন কল
B) সামাজিক যোগাযোগমাধ্যম
C) ইমেল
D) সবগুলো
✔উত্তর: D

৩. কোনটি Cyber Stalking-এর উদাহরণ?

A) Exam result দেখা
B) বারবার মেসেজ/হুমকি পাঠানো
C) নোট শেয়ার করা
D) লগইন করা
✔উত্তর: B

৪. Cyber Stalking-এর উদ্দেশ্য—

A) শিক্ষা প্রদান
B) অনলাইন হয়রানি
C) নেট স্পিড বাড়ানো
D) ফাইল ট্রান্সফার
✔উত্তর: B

৫. Online tracking কোন অপরাধের অন্তর্ভুক্ত?

A) Photo editing
B) Cyber Stalking
C) Gaming
D) Software update
✔উত্তর: B

B. Cyber Harassment & Bullying

৬. Cyberbullying কী?

A) অফলাইন অপমান
B) অনলাইনে অপমান/গালি/হয়রানি
C) বন্ধুত্ব করা

D) ভিডিও আপলোড
✔উত্তর: B

৭. কোনটি Cyberbullying-এর উদাহরণ নয়?

A) বিরক্তিকর মেসেজ
B) ফেক অ্যাকাউন্ট তৈরি
C) ইতিবাচক মন্তব্য করা
D) অপমানজনক ছবি পোস্ট
✔উত্তর: C

৮. Revenge porn কোন অপরাধের শ্রেণীভুক্ত?

A) Cyberbullying
B) Cybercrime
C) Online sexual crime
D) সবগুলো
✔উত্তর: D

C. Identity & Privacy Threats

৯. Identity Theft কী?

A) মোবাইল চুরি
B) ব্যক্তিগত তথ্য চুরি
C) ছবি শেয়ার
D) কল রেকর্ড
✔উত্তর: B

১০. Impersonation বলতে বোঝায়—

A) গান শোনা
B) ভুয়া পরিচয় ব্যবহার
C) ক্যালকুলেট করা
D) ব্রাউজিং
✔উত্তর: B

১১. কোনটি ব্যক্তিগত তথ্য শেয়ার করা উচিত নয়?

A) জন্মতারিখ
B) ATM PIN
C) পাসওয়ার্ড
D) সবগুলো
✔উত্তর: D

১২. Cyber Stalker সাধারণত কোন তথ্য ব্যবহার করে?

A) Public photos
B) Location
C) Contact list
D) সবগুলো
✔উত্তর: D

D. Cyber Crimes – Nature & Types

১৩. Cyber Crime বলতে বোঝায়—

A) ইন্টারনেটে খেলা
B) প্রযুক্তি ব্যবহার করে অপরাধ
C) ভিডিও দেখা
D) ফাইল ডাউনলোড
✔উত্তর: B

১৪. কোনটি Financial cyber crime?

A) Phishing
B) Online fraud
C) Credit card misuse
D) সবগুলো
✔উত্তর: D

১৫. Ransomware কী করে?

A) গান বাজায়
B) ডেটা লক করে মুক্তিপণ দাবি

C) স্পিড বাড়ায়
D) ছবি এডিট
✔উত্তর: B

১৬. Malware-এর উদাহরণ—

A) Virus
B) Trojan
C) Worm
D) সবগুলো
✔উত্তর: D

১৭. Social Engineering বলতে বোঝায়—

A) ডিজাইনের কাজ
B) মানুষকে প্রতারণা করে তথ্য বের করা
C) নেটওয়ার্ক তৈরি
D) সার্ভার রক্ষা
✔উত্তর: B

১৮. কোনটি online scam?

A) Lottery scam
B) Fake job offer
C) Free gift message
D) সবগুলো
✔উত্তর: D

১৯. ATM fraud কোন শ্রেণীতে পড়ে?

A) Hardware error
B) Cyber Crime
C) Social media misuse
D) Spam
✔উত্তর: B

২০. Cyber terrorism-এর লক্ষ্য—

A) গেম তৈরি
B) ব্যক্তিগত বিনোদন
C) জাতীয় নিরাপত্তা ক্ষতি

D) গান প্রকাশ
✔উত্তর: C

E. Cyber Laws & Protection

২১. ভারতীয় সাইবার আইন কোনটি?

A) IT Act 2000
B) RTI Act
C) IPC 302
D) GST Act
✔উত্তর: A

২২. Identity theft কোন সেকশনে শাস্তিযোগ্য?

A) Section 66A
B) Section 66C
C) Section 43
D) Section 75
✔উত্তর: B

২৩. Offensive messages কোন সেকশনে শাস্তিযোগ্য ছিল?

A) 66A
B) 67
C) 43
D) 45
✔উত্তর: A

২৪. Obscene content online কোন সেকশনে নিষিদ্ধ?

A) Section 66D
B) Section 67
C) Section 69
D) Section 46
✔উত্তর: B

২৫. Cybercrime রিপোর্ট করার সরকারি সাইট—

A) india.gov.in
B) cybercrime.gov.in
C) uidai.gov.in
D) crpf.gov.in
✔উত্তর: B

F. Cyber Ethics

২৬. Cyber Ethics কী শেখায়?

A) অবৈধ ব্যবহার
B) দায়িত্বশীল ও নৈতিক ডিজিটাল আচরণ
C) গেম খেলা
D) ভাইরাস বানানো
✔উত্তর: B

২৭. Plagiarism কী?

A) নিজের লেখা
B) অন্যের লেখা কপি করে নিজের নামে ব্যবহার
C) অনলাইন চ্যাট
D) ছবি এডিট
✔উত্তর: B

২৮. কোনটি অনৈতিক কাজ?

A) অনুমতি ছাড়া ছবি পোস্ট
B) অন্যের তথ্য প্রকাশ
C) Cyberbullying
D) সবগুলো
✔উত্তর: D

২৯. Responsible social media behavior অন্তর্ভুক্ত—

A) ভদ্র ভাষা
B) সঠিক তথ্য
C) গোপনীয়তা রক্ষা

D) সবগুলো
✔উত্তর: D

৩০. Piracy বলতে বোঝায়—

A) গান শোনা
B) কপিরাইট লঙ্ঘন
C) পাসওয়ার্ড বদলানো
D) ফাইল rename
✔উত্তর: B

G. Safe Social Networking

৩১. কোনটি Social media safety practice?

A) অজানা রিকোয়েস্ট গ্রহণ
B) Strong privacy settings
C) ATM PIN শেয়ার
D) Location সবসময় ON
✔উত্তর: B

৩২. Fake profile-এর প্রধান উদ্দেশ্য—

A) Account verify
B) তথ্য সংগ্রহ ও প্রতারণা
C) ছবি এডিট
D) পাসওয়ার্ড রিসেট
✔উত্তর: B

৩৩. Location sharing ঝুঁকি বাড়ায়—

A) স্বচ্ছতা
B) নিরাপত্তা
C) Tracking
D) গতি
✔উত্তর: C

৩৪. Social media stalking সহজ হয় যখন—

A) Profile locked
B) Everything Public
C) Limited sharing
D) 2FA সক্রিয়
✔উত্তর: B

৩৫. Blocking ব্যবহার করা হয়—

A) অনলাইন শপিংয়ে
B) অপরাধী বা স্টকারকে বন্ধ করতে
C) ভিডিও এডিট
D) ফাইল ডাউনলোড
✔উত্তর: B

H. Security Tools & Best Practices

৩৬. Antivirus ব্যবহৃত হয়—

A) ব্রাউজার চালাতে
B) ভাইরাস আটকাতে
C) ছবি তুলতে
D) Cables ঠিক করতে
✔উত্তর: B

৩৭. Firewall কাজ করে—

A) গেম চালায়
B) Unauthorized access ব্লক করে
C) ফাইল rename করে
D) স্পিকার চালায়
✔উত্তর: B

৩৮. VPN ব্যবহৃত হয়—

A) নেটওয়ার্ক নিরাপদ করতে
B) স্ক্রিন উজ্জ্বলতা বাড়াতে
C) গেম খেলতে
D) ফাইল ডিলিট
✔উত্তর: A

৩৯. Backup রাখা জরুরি কেন?

A) গান শুনতে
B) ডেটা হারানো প্রতিরোধ
C) স্ক্রিন পরিবর্তন
D) রঙ পরিবর্তন
✔উত্তর: B

৪০. Strong password-এ কী থাকা উচিত?

A) জন্মতারিখ
B) নিজের নাম
C) Symbol + Number + Letters
D) শুধু সংখ্যা
✔উত্তর: C

I. Online Fraud Detection

৪১. Fake email চিনতে সাহায্য করে—

A) ভুল বানান
B) অদ্ভুত URL
C) অজানা sender
D) সবগুলো
✔উত্তর: D

৪২. Phishing link সাধারণত কোথায় দেখা যায়?

A) Spam mail
B) Official website
C) Government portal

D) Textbook
✔উত্তর: A

৪৩. OTP কারো সাথে শেয়ার করা উচিত নয় কারণ—

A) তেমন কিছু হবে না
B) একাউন্ট হ্যাক হতে পারে
C) ফোন নষ্ট হয়
D) স্ক্রিন কালো হয়
✔উত্তর: B

J. Miscellaneous

৪৪. Cyber grooming কাকে বলে?

A) বাড়ি পরিষ্কার
B) অনলাইনে শিশুকে প্ররোচিত করা
C) ট্রাফিক নিয়ন্ত্রণ
D) গেম খেলানো
✔উত্তর: B

৪৫. Spam mail সাধারণত—

A) দরকারি
B) অনাকাঙ্ক্ষিত
C) নিরাপদ
D) সরকারি
✔উত্তর: B

৪৬. Digital footprint হলো—

A) বাস্তব পদচিহ্ন
B) অনলাইনে রেখে যাওয়া তথ্য
C) Birth certificate
D) স্ক্রিন পাসওয়ার্ড
✔উত্তর: B

৪৭. Cybercrime helpline India—

A) 100
B) 1930
C) 108
D) 1098
✔উত্তর: B

৪৮. Cyber Ethics অনুসরণ না করলে—

A) সমাজে সম্মান বাড়ে
B) Cybercrime বেড়ে যায়
C) দ্রুত কাজ হয়
D) গেম খেলা সহজ
✔উত্তর: B

৪৯. কোনটি নিরাপদ নয়?

A) HTTPS browsing
B) Public Wi-Fi banking
C) 2FA enable
D) Limited sharing
✔উত্তর: B

৫০. Fake news ছড়ানো—

A) নৈতিক
B) অপরাধ
C) সামাজিকভাবে ভালো
D) harmless
✔উত্তর: B

⭐ Bonus MCQs (৫টি)

৫১. Cyber awareness program-এর উদ্দেশ্য—

A) অপরাধ শেখানো
B) নিরাপদ ব্যবহার শেখানো

C) ছবি আঁকা
D) গেম শিখানো
✔উত্তর: B

৫২. Hacking হলো—

A) Unauthorized access
B) Painting
C) File rename
D) OS shutdown
✔উত্তর: A

৫৩. Trojan কী?

A) ক্ষতিকর প্রোগ্রাম
B) অ্যান্টিভাইরাস
C) Keyboard
D) Printer
✔উত্তর: A

৫৪. কোনটি নৈতিক আচরণ?

A) Copyright মানা
B) Plagiarism
C) Fake profile
D) Cyberbullying
✔উত্তর: A

৫৫. Cybercrime-এর প্রধান লক্ষ্য—

A) Data
B) Keyboard
C) Monitor
D) Loudspeaker
✔উত্তর: A

✔চাইলে আমি দিতে পারি—

 SAQ + LAQ প্রশ্নব্যাঙ্ক
 এক পাতার সংক্ষিপ্ত নোট
 PDF/Word File

নীচে **“Cyber Stalking, Cyber Crimes এবং Cyber Ethics”** বিষয়ের ওপর **SAQ (৩–৫ নম্বর)** এবং **LAQ (৮–১২ নম্বর) মডেল প্রশ্ন ও উত্তরসহ** একটি পূর্ণাঙ্গ প্রশ্নব্যাঙ্ক প্রদান করা হলো। এটি কলেজ–বিশ্ববিদ্যালয়ের ICT/Computer Awareness কোর্স, সাইবার সেফটি প্রশিক্ষণ এবং পরীক্ষার জন্য যথাযথ।

□ SAQ (Short Answer Questions – ৩–৫ নম্বর)

⋆ *সংক্ষিপ্ত প্রশ্ন + মডেল উত্তর*

SAQ–1: Cyber Stalking কী?

উত্তর:
ডিজিটাল মাধ্যমে কাউকে বারবার অনুসরণ, নজরদারি, হয়রানি বা হুমকি দেওয়াকে Cyber Stalking বলা হয়। এটি সাধারণত ফেসবুক, ইনস্টাগ্রাম, ইমেল, মেসেঞ্জার বা ফেক প্রোফাইলের মাধ্যমে ঘটে।

SAQ–2: Cyberbullying ও Cyber Stalking-এর মধ্যে পার্থক্য লিখো।

উত্তর:

- **Cyberbullying:** অনলাইনে অপমান, গালি, ট্রোল, কটূক্তি বা মানসিক হয়রানি।
- **Cyber Stalking:** দীর্ঘমেয়াদি অনুসরণ, নজরদারি, বারবার মেসেজ/হুমকি পাঠানো। Cyber Stalking বেশি ধারাবাহিক ও পরিকল্পিত।

SAQ–3: Identity Theft কী?

উত্তর:
কোনো ব্যক্তির ব্যক্তিগত পরিচয় বা তথ্য (নাম, ছবি, ফোন, ব্যাংক তথ্য ইত্যাদি) অনুমতি ছাড়া ব্যবহার করে প্রতারণা, অপরাধ বা হ্যাকিং করাকে Identity Theft বলে।

SAQ–4: Phishing কী?

উত্তর:
ভুয়া ইমেল, ফেক লিঙ্ক বা নকল ওয়েবসাইট ব্যবহার করে ব্যবহারকারীর পাসওয়ার্ড, ব্যাংক তথ্য বা ব্যক্তিগত ডেটা প্রতারণামূলকভাবে সংগ্রহ করাকে Phishing বলা হয়।

SAQ–5: Ransomware কী?

উত্তর:
র‍্যানসমওয়্যার একটি ক্ষতিকর সফটওয়্যার যা কম্পিউটারের ডেটা এনক্রিপ্ট করে লক করে দেয় এবং তা মুক্ত করতে অর্থ (ransom) দাবি করে।

SAQ–6: Cyber Terrorism বলতে কী বোঝায়?

উত্তর:
ডিজিটাল প্রযুক্তি ব্যবহার করে জাতীয় অবকাঠামো, সরকারী সংস্থা বা গুরুত্বপূর্ণ তথ্যভান্ডারে আক্রমণকে Cyber Terrorism বলা হয়। এটি জাতীয় নিরাপত্তার জন্য গুরুতর হুমকি।

SAQ–7: Cyber Ethics কী?

উত্তর:
অনলাইনে দায়িত্বশীল, নৈতিক, ভদ্র ও নিরাপদ আচরণ নিশ্চিত করার নিয়ম ও মূল্যবোধকে Cyber Ethics বলা হয়। এটি গোপনীয়তা, সম্মান ও আইন মেনে চলাকে উৎসাহিত করে।

SAQ–8: Plagiarism কী?

উত্তর:
অন্যের লেখা, গবেষণা বা কনটেন্ট কপি করে নিজের নামে ব্যবহার করাকে Plagiarism বলা হয়। এটি একটি গুরুতর নৈতিক অপরাধ।

SAQ–9: Cyber Grooming কী?

উত্তর:
অনলাইনে শিশু বা কিশোরদের বিশ্বাস অর্জন করে তাদের ব্যক্তিগত তথ্য নেওয়া, প্ররোচিত করা বা শোষণ করার প্রক্রিয়াকে Cyber Grooming বলে।

SAQ–10: ঘটনাস্থলে Cybercrime রিপোর্ট করার সরকারি পোর্টাল কোনটি?

উত্তর:
ভারতের সরকারি সাইবার অপরাধ রিপোর্টিং পোর্টাল হলো **www.cybercrime.gov.in** এবং জরুরি হেল্পলাইন নম্বর **1930**।

SAQ–11: Social Engineering কী? একটি উদাহরণ দাও।

উত্তর:
মানুষকে বিভ্রান্ত বা প্ররোচিত করে তার কাছ থেকে সংবেদনশীল তথ্য বের করে নেওয়ার কৌশল।
উদাহরণ: ভুয়া ব্যাংক কর্মীর ফোন করে OTP চাওয়া।

SAQ–12: Cyber Ethics-এ Responsibility বলতে কী বোঝায়?

উত্তর:
দায়িত্বশীলভাবে তথ্য শেয়ার করা, ভুয়া খবর না ছড়ানো, কারও সম্মানহানি না করা এবং অনলাইন আচরণে আইন ও নীতি মেনে চলা।

□ LAQ (Long Answer Questions – ৮–১২ নম্বর)

⋆ *বিশদ প্রশ্ন + মডেল উত্তর*

LAQ–1: Cyber Stalking কী? এর বৈশিষ্ট্য, প্রকারভেদ এবং প্রভাব আলোচনা করো।

উত্তর:
Cyber Stalking হলো ডিজিটাল প্ল্যাটফর্মে কাউকে বারবার অনুসরণ, হয়রানি, হুমকি বা নজরদারি করা। এটি ব্যক্তিগত গোপনীয়তা, মানসিক স্বাস্থ্য ও নিরাপত্তার জন্য গুরুতর হুমকি।

বৈশিষ্ট্য:

- বারবার মেসেজ, কল বা ইমেল
- প্রোফাইল ও ছবি চুরি
- Location tracking
- ব্ল্যাকমেইল বা হুমকি
- Social media monitoring
- Fake profile তৈরি

প্রকারভেদ:

1. **Direct Stalking:** সরাসরি যোগাযোগ করে হয়রানি।
2. **Indirect Stalking:** অন্যের মাধ্যমে হুমকি/মন্তব্য।
3. **Surveillant Stalking:** অনলাইন কার্যকলাপ নজরদারি।
4. **Impersonation Stalking:** ভুক্তভোগীর নামে ভুয়া প্রোফাইল।
5. **Image-based Stalking:** ছবি/ভিডিও দিয়ে চাপ সৃষ্টি।

প্রভাব:

- উদ্বেগ, আতঙ্ক, বিষণ্নতা
- সামাজিক বিচ্ছিন্নতা

- আত্মসম্মানহানি
- ব্যক্তিগত নিরাপত্তাহীনতা
- মানসিক স্বাস্থ্যহানি

Cyber Stalking প্রতিরোধে প্রযুক্তিগত নিরাপত্তা, আইনি ব্যবস্থা ও সচেতনতা অত্যন্ত জরুরি।

LAQ–2: Cyber Crime কী? এর ধরন, কারণ ও প্রতিরোধ ব্যবস্থা আলোচনা করো।

উত্তর:
কম্পিউটার, ইন্টারনেট বা ডিজিটাল সিস্টেম ব্যবহার করে সংঘটিত যেকোনো অপরাধ হলো Cyber Crime।

Cyber Crime-এর ধরন:

- **Financial Crime:** Phishing, credit card fraud, online banking scam
- **Identity Theft:** ভুয়া পরিচয় ব্যবহার
- **Hacking:** Unauthorized access
- **Malware Attack:** Virus, Trojan, Worm
- **Ransomware:** ডেটা লক
- **Cyber Terrorism:** সরকার/সংস্থা আক্রমণ
- **Cyber Bullying:** অপমান/হয়রানি
- **Child exploitation crimes**

কারণ:

- অতিরিক্ত তথ্য শেয়ার
- Password দুর্বলতা
- Public Wi-Fi ব্যবহার
- প্রযুক্তিগত অজ্ঞতা
- নিরাপত্তার ঘাটতি
- Social engineering

প্রতিরোধ ব্যবস্থা:

- Strong password, 2FA
- HTTPS ব্রাউজিং
- Antivirus ও firewall
- Regular software update

- Suspicious link avoid
- Backup রাখা
- Privacy settings সঠিক করা
- Cybercrime.gov.in-এ অভিযোগ

Cyber Crime প্রতিরোধে প্রযুক্তি + সচেতনতা + আইনি পদক্ষেপ একত্রে কাজ করতে হয়।

LAQ–3: Cyber Ethics কী? Cyber Ethics-এর নীতি ও গুরুত্ব ব্যাখ্যা করো।

উত্তর:
Cyber Ethics হলো অনলাইনে নৈতিক, দায়িত্বশীল এবং সচেতন আচরণ বজায় রাখার নিয়ম ও মূল্যবোধের সমষ্টি।

মূল নীতি:

1. **Honesty:** ভুয়া পরিচয়/ফেক প্রোফাইল ব্যবহার না করা
2. **Respect:** অন্যের মতামত ও গোপনীয়তা সম্মান
3. **Responsibility:** ভুয়া খবর, গালি, হুমকি ছড়ানো পরিহার
4. **Privacy:** ব্যক্তিগত তথ্য শেয়ার না করা
5. **Intellectual Property:** Plagiarism ও পাইরেসি এড়ানো
6. **Digital Footprint সচেতনতা:** প্রতিটি পোস্ট ভবিষ্যতে প্রভাব ফেলে

গুরুত্ব:

- নিরাপদ ও সুস্থ ডিজিটাল পরিবেশ
- অনলাইনে পারস্পরিক সম্মান
- সাইবার অপরাধ কমানো
- ব্যক্তিগত পরিচয় সুরক্ষা
- সামাজিক মূল্যবোধ রক্ষা

Cyber Ethics অনলাইন সমাজকে মানবিক ও নিরাপদ রাখে।

LAQ–4: Phishing, Ransomware ও Social Engineering—এই তিনটি সাইবার হুমকি ব্যাখ্যা করো এবং প্রতিরোধ ব্যাখ্যা করো।

উত্তর:

১. Phishing:

ভুয়া লিঙ্ক বা ইমেল ব্যবহার করে ব্যক্তিগত তথ্য সংগ্রহ।
প্রতিরোধ:

- লিঙ্ক যাচাই
- Sender authentic কিনা দেখুন
- OTP/password কখনও শেয়ার নয়

২. Ransomware:

ডেটা লক করে মুক্তিপণ দাবি।
প্রতিরোধ:

- Backup
- Antivirus
- অজানা ফাইল না খোলা

৩. Social Engineering:

মানুষকে প্রতারণা করে তথ্য বের করা।
প্রতিরোধ:

- অচেনা কল/মেসেজ এড়ানো
- পরিচয় যাচাই
- Personal information শেয়ার না করা

এই তিনটি সাইবার আক্রমণ মানুষের সচেতনতা ও প্রযুক্তিগত সুরক্ষা বাড়িয়ে প্রতিরোধ করা যায়।

LAQ–5: Social Media Safety কেন গুরুত্বপূর্ণ? ঝুঁকি ও সুরক্ষা কৌশল ব্যাখ্যা করো।

উত্তর:

ঝুঁকি:

- Fake profile
- Identity theft
- Cyber stalking
- Online blackmail
- Revenge porn
- Phishing attack
- Data leak
- Cyberbullying

সুরক্ষা কৌশল:

- Strong privacy settings
- Friend request যাচাই
- Location sharing বন্ধ
- 2FA enable
- Block/Report ব্যবহার
- Personal info সীমিত শেয়ার
- শিশুদের জন্য parental control
- সন্দেহজনক লিঙ্ক এড়ানো

সোশ্যাল মিডিয়া নিরাপত্তা রক্ষা করা ডিজিটাল জীবনের একটি অপরিহার্য অংশ।

✔চাইলে আমি দিতে পারি—

 এক পাতার সংক্ষিপ্ত নোট
 PDF/Word File
 আরো ৫০+ MCQ

নীচে **"Cyber Stalking, Cyber Crimes এবং Cyber Ethics"** বিষয়ের ওপর **এক পাতার সংক্ষিপ্ত নোট** প্রদান করা হলো।
এটি পরীক্ষার প্রস্তুতি, ক্লাস হ্যান্ডআউট বা সচেতনতা কর্মসূচির জন্য অত্যন্ত উপযোগী।

এক পাতার সংক্ষিপ্ত নোট

Cyber Stalking • Cyber Crimes • Cyber Ethics

---

১. Cyber Stalking – সংক্ষিপ্ত ধারণা

Cyber Stalking হলো ডিজিটাল মাধ্যমে কাউকে **বারবার অনুসরণ, নজরদারি, হয়রানি বা হুমকি** দেওয়া।
সোশ্যাল মিডিয়া, ইমেল, মেসেঞ্জার, ফেক অ্যাকাউন্ট, GPS ট্র্যাকিং ইত্যাদি এর প্রধান মাধ্যম।

বৈশিষ্ট্য:

- বারবার অপ্রয়োজনীয় মেসেজ/ইমেল
- অজ্ঞাত পরিচয়ে হুমকি
- Location tracking
- Fake profile ব্যবহার
- অনলাইন নজরদারি

ফলাফল:

- মানসিক চাপ
- উদ্বেগ/বিষণ্নতা
- সামাজিক বিচ্ছিন্নতা
- নিরাপত্তাহীনতা

---

২. Cyber Crimes – সংক্ষিপ্ত ধারণা

ডিজিটাল প্রযুক্তি, কম্পিউটার, মোবাইল বা নেটওয়ার্ক ব্যবহার করে সংঘটিত অপরাধকে Cyber Crime বলা হয়।

প্রধান ধরনের Cyber Crime:

- **Financial fraud:** Phishing, credit card misuse, online scam
- **Identity theft:** ব্যক্তিগত তথ্য চুরি
- **Hacking:** Unauthorized access

- **Malware attack:** Virus, Trojan, Worm
- **Ransomware:** ডেটা লক করে মুক্তিপণ দাবি
- **Cyberbullying:** অনলাইনে অপমান/হয়রানি
- **Cyber Terrorism:** জাতীয় নিরাপত্তা আক্রমণ
- **Online sexual crime:** Grooming, revenge porn

Cyber Crime-এর কারণ:

- দুর্বল পাসওয়ার্ড
- অতিরিক্ত তথ্য শেয়ার
- Public Wi-Fi ব্যবহার
- Social engineering
- নিরাপত্তা সম্পর্কে অজ্ঞতা

প্রতিরোধ:

- Strong password + 2FA
- Antivirus + Firewall
- HTTPS ব্রাউজিং
- Backup রাখা
- Privacy settings ঠিক করা
- সন্দেহজনক লিঙ্ক এড়ানো
- cybercrime.gov.in-এ অভিযোগ করা

---

৩. Cyber Ethics – সংক্ষিপ্ত ধারণা

Cyber Ethics হলো অনলাইনে **নৈতিক, দায়িত্বশীল ও নিরাপদ আচরণ** করার নিয়ম ও মূল্যবোধের সমষ্টি।

Cyber Ethics-এর নীতি:

- **Honesty:** ভুয়া পরিচয়/প্রোফাইল ব্যবহার নয়
- **Respect:** অন্যের গোপনীয়তা ও মতামত সম্মান করা
- **Responsibility:** ভুয়া খবর, হুমকি, গালি না ছড়ানো
- **Privacy:** ব্যক্তিগত তথ্য সীমিত শেয়ার
- **Intellectual Property Respect:** Plagiarism ও পাইরেসি না করা
- **Digital Footprint সচেতনতা:** প্রতিটি পোস্ট ভবিষ্যতে প্রভাব ফেলে

গুরুত্ব:

- নিরাপদ ডিজিটাল পরিবেশ
- সামাজিক সম্মান বজায় রাখা
- সাইবার অপরাধ কমানো
- নৈতিক অনলাইন সংস্কৃতি গঠন

✔সারাংশ (Summary)

Cyber Stalking ব্যক্তির মানসিক ও ব্যক্তিগত নিরাপত্তার জন্য ঝুঁকিপূর্ণ।
Cyber Crime ডিজিটাল যুগের বড় হুমকি যা ব্যক্তি, প্রতিষ্ঠান ও জাতির ক্ষতি করতে পারে।
Cyber Ethics অনুসরণ করলে অনলাইন বিশ্বে নিরাপত্তা, নৈতিকতা ও সম্মান বজায় থাকে।

⭐ Additional MCQ Set – 55 Questions (with Answers)

(Cyber Stalking • Cyber Crimes • Cyber Ethics • Digital Safety)

A. Cyber Stalking – Additional Questions

১. কোনটি Cyber Stalker-এর সাধারণ কৌশল নয়?

A) Repeated messaging
B) Location tracking
C) Sending gifts online
D) Fake profile ব্যবহার
✔উত্তর: C

২. Cyber Stalking সাধারণত কোন বয়সের মানুষ বেশি ভুক্তভোগী হয়?

A) শিশু ও কিশোর
B) বয়স্ক
C) শুধুই পুরুষ

D) শুধুই নারীরা
✔উত্তর: A

৩. GPS tracking কোন অপরাধের অংশ হতে পারে?

A) Social gaming
B) Cyber stalking
C) Data backup
D) Cloud sync
✔উত্তর: B

৪. কোন ক্ষেত্রে Cyber Stalking বেশি ঘটে?

A) বন্ধ গ্রুপ
B) Public profile
C) Offline stores
D) PDF files
✔উত্তর: B

৫. Image-based stalking মূলত কী কাজে ব্যবহৃত হয়?

A) শিক্ষা
B) ভয় দেখানো/ব্ল্যাকমেইল
C) গেম খেলা
D) বিজ্ঞাপন
✔উত্তর: B

৬. Cyber Stalker সাধারণত কোন তথ্যকে টার্গেট করে?

A) Assignment
B) Personal photos
C) Calculator
D) Song
✔উত্তর: B

৭. Social media stalking কমাতে সবচেয়ে জরুরি—

A) ফ্রেন্ড সংখ্যা বাড়ানো
B) Profile privacy
C) public post

D) Auto location
✔উত্তর: B

B. Cyber Crime – Additional Questions

৮. কোনটি Cyber Crime নয়?

A) Identity theft
B) Online banking fraud
C) Cyber terrorism
D) Textbook reading
✔উত্তর: D

৯. কোন আক্রমণ ডেটা এনক্রিপ্ট করে?

A) Worm
B) Ransomware
C) Keylogger
D) Spyware
✔উত্তর: B

১০. Keylogger ব্যবহৃত হয়—

A) ছবি কপি করতে
B) কী প্রেস রেকর্ড করতে
C) ব্যাটারি বাড়াতে
D) ফাইল ডিলিট করতে
✔উত্তর: B

১১. DoS attack দ্বারা—

A) সার্ভার অচল করা হয়
B) পাসওয়ার্ড লুকানো হয়
C) ফোন কল বাড়ানো হয়
D) ছবি বড় করা হয়
✔উত্তর: A

১২. Zero-day attack ঘটে যখন—

A) নতুন গান বের হয়
B) সফটওয়্যারের দুর্বলতা প্রকাশের আগেই আক্রমণ করা হয়
C) কম্পিউটার নতুন
D) সার্ভার বন্ধ
✔উত্তর: B

১৩. কোনটি Social Engineering-এর উদাহরণ?

A) শক্তিশালী পাসওয়ার্ড
B) Fake bank call
C) Antivirus
D) Firewall
✔উত্তর: B

১৪. Brute force attack হলো—

A) Guessing passwords by repeated attempts
B) ভিডিও এডিট
C) File printing
D) Screenshot
✔উত্তর: A

১৫. Spyware কী?

A) কম্পিউটার পরিষ্কারকারী
B) নজরদারি করা সফটওয়্যার
C) Drawing tool
D) Antivirus
✔উত্তর: B

১৬. 'Botnet' বলতে বোঝায়—

A) খেলনা রোবট
B) নেটওয়ার্কে সংক্রমিত কম্পিউটার গ্রুপ
C) ব্রাউজার প্লাগইন
D) RAM
✔উত্তর: B

১৭. ATM skimming হয়—

A) Data theft via device
B) কম ব্যালেন্স
C) ব্যাঙ্কে ভুল
D) প্রযুক্তিগত ত্রুটি
✔উত্তর: A

C. Online Scams & Fraud

১৮. Phishing-এর মূল অস্ত্র—

A) অজানা লিঙ্ক
B) প্রক্সি
C) USB drive
D) Printer
✔উত্তর: A

১৯. Vishing কী?

A) Voice phishing by fake calls
B) Video sharing
C) Virus installing
D) Voice editing
✔উত্তর: A

২০. Smishing কী?

A) Social messaging
B) SMS phishing
C) Screenshot
D) Social mining
✔উত্তর: B

২১. Lottery scam-এর প্রধান উদ্দেশ্য—

A) পুরস্কার দেওয়া
B) ব্যাংক তথ্য চুরি
C) খেলা

D) শিক্ষা
✔উত্তর: B

২২. Online marketplace scam সাধারণত হয়—

A) Verified sellers
B) Fake buyers/sellers
C) Government portals
D) Library sites
✔উত্তর: B

D. Cyber Law & Governance

২৩. IT Act 2000-এর উদ্দেশ্য—

A) নতুন কর
B) সাইবার অপরাধ নিয়ন্ত্রণ
C) সিনেমা নিয়ন্ত্রণ
D) রাস্তাঘাট
✔উত্তর: B

২৪. Section 66D শাস্তি দেয়—

A) পরিচয় চুরি
B) cheating by impersonation
C) virus spread
D) hacking
✔উত্তর: B

২৫. Section 67 প্রযোজ্য—

A) অশ্লীল কনটেন্ট প্রকাশে
B) পাসওয়ার্ড তৈরি
C) গেম খেলা
D) ছবি আঁকা
✔উত্তর: A

২৬. Cybercrime রিপোর্ট করার emergency helpline India—

A) 911
B) 1930
C) 102
D) 1091
✔উত্তর: B

E. Cyber Ethics – Additional Questions

২৭. Cyber Ethics শেখায়—

A) অবৈধ আচরণ
B) দায়িত্বশীল অনলাইন ব্যবহার
C) গেম খেলা
D) ভিডিও শেয়ার
✔উত্তর: B

২৮. Responsible digital citizenship অন্তর্ভুক্ত—

A) অন্যকে সম্মান
B) গোপনীয়তা রক্ষা
C) ভদ্র ভাষা
D) সবগুলো
✔উত্তর: D

২৯. Copyright মানা হলো—

A) নৈতিকতা
B) অপরাধ
C) ভাইরাস
D) ফোন কল
✔উত্তর: A

৩০. কোনটি অনৈতিক?

A) Plagiarism
B) Privacy respect
C) Strong password

D) Report/block
✔উত্তর: A

৩১. Cyber Ethics অনুযায়ী—

A) হুমকি দেওয়া ঠিক
B) ভুয়া খবর ভুল
C) Identity theft ঠিক
D) DDoS আক্রমণ ভালো
✔উত্তর: B

F. Privacy & Safety

৩২. Privacy settings কেন জরুরি?

A) Battery save
B) Personal info protection
C) Game unlock
D) Internet speed increase
✔উত্তর: B

৩৩. Digital Footprint হলো—

A) পায়ের ছাপ
B) অনলাইনে রেখে যাওয়া তথ্য
C) স্ক্রিনশট
D) কাগজ
✔উত্তর: B

৩৪. কোনটি ব্যক্তিগত তথ্য?

A) Aadhar number
B) PAN
C) Phone number
D) সবগুলো
✔উত্তর: D

৩৫. Incognito mode রক্ষা করে—

A) ব্রাউজার হিস্ট্রি সংরক্ষণ না করে
B) পাসওয়ার্ড বাড়ায়
C) RAM বৃদ্ধি
D) Virus delete
✔উত্তর: A

৩৬. Public Wi-Fi নিরাপদ নয় কারণ—

A) ফ্রি
B) এনক্রিপশন দুর্বল
C) গতি কম
D) স্ক্রিন কালো
✔উত্তর: B

G. Social Media & Online Communication

৩৭. Fake friend request এড়াতে—

A) সব accept
B) Profile verify
C) ফোন কল
D) পোস্ট করা
✔উত্তর: B

৩৮. Cyber grooming টার্গেট—

A) বয়স্ক
B) শিশু-কিশোর
C) সরকারি কর্মচারী
D) ডাক্তার
✔উত্তর: B

৩৯. কোনটি social media crime?

A) Cyberbullying
B) Identity theft
C) Impersonation

D) সবগুলো
✔উত্তর: D

৪০. Online hate speech হলো—

A) নৈতিক
B) অপরাধ
C) harmless
D) আইনসম্মত
✔উত্তর: B

৪১. Location sharing ঝুঁকি বাড়ায়—

A) গতি
B) stalking
C) ছবি
D) নোট
✔উত্তর: B

৪২. Profile lock mainly useful for—

A) Privacy
B) Game speed
C) Storage
D) Charging
✔উত্তর: A

H. Security Tools & Techniques

৪৩. Antivirus রক্ষা করে—

A) ভাইরাস থেকে
B) ফোন চার্জ
C) গান শুনতে
D) ছবি এডিট
✔উত্তর: A

৪৪. Firewall কাজ করে—

A) Unauthorized access ব্লক
B) ভিডিও বানানো
C) ড্রাইভার ইনস্টল
D) ফাইল সাজানো
✔উত্তর: A

৪৫. Encryption ব্যবহৃত হয়—

A) ডেটা সুরক্ষায়
B) গান বানাতে
C) Colour change
D) ক্যালকুলেট
✔উত্তর: A

৪৬. Two-factor authentication হলো—

A) দ্রুত লগইন
B) অধিক নিরাপদ লগইন
C) ছবি এডিট
D) ভাইরাস চালানো
✔উত্তর: B

I. Miscellaneous Cyber Awareness

৪৭. Spam mail সাধারণত—

A) দরকারি
B) অপ্রয়োজনীয়
C) সরকারি
D) textbook
✔উত্তর: B

৪৮. OTP শেয়ার করলে—

A) কিছু হয় না
B) Account hack হতে পারে
C) ফোন বন্ধ হয়

D) রঙ বদলায়
✔উত্তর: B

৪৯. Data breach কী?

A) ডেটা নষ্ট
B) ডেটা দুর্ঘটনাজনিত/অবৈধভাবে ফাঁস
C) ভালো লেনদেন
D) গান ডাউনলোড
✔উত্তর: B

৫০. Cyber safety প্রধানত কার দায়িত্ব?

A) সরকার
B) ব্যবহারকারী
C) বন্ধুরা
D) দোকান
✔উত্তর: B

⭐ Bonus MCQs (৫টি)

৫১. Cookies ব্যবহৃত হয়—

A) ব্যবহারকারীর পছন্দ সংরক্ষণে
B) ভাইরাস ছড়াতে
C) ছবি ছোট করতে
D) ট্রাফিক নিয়ন্ত্রণ
✔উত্তর: A

৫২. Report/Block ব্যবহার করা হয়—

A) Stalker বা অপরাধীকে থামাতে
B) স্ক্রিন বড় করতে
C) Keyboard clean
D) Printer run
✔উত্তর: A

৫৩. Social media addiction-এর ফল—

A) Concentration কমে
B) সময় নষ্ট
C) মানসিক চাপ
D) সবগুলো
✔উত্তর: D

৫৪. Data backup করা উচিত—

A) বছরে ১ বার
B) নিয়মিত
C) কখনও নয়
D) শুধু ফোনে
✔উত্তর: B

৫৫. Cyber ethics না মানলে—

A) নিরাপত্তা বাড়ে
B) সাইবার অপরাধ বাড়ে
C) শিক্ষা উন্নত
D) বন্ধুত্ব বাড়ে
✔উত্তর: B