SIBANI MANDAL MAHAVIDYALAYA

Village + P.O. Namkhana
Dist. South 24 Parganas
West Bengal

Computer Applications

SEC-3, 4-Year Education Major

L7: ইন্টারনেটে নিরাপদ ব্রাউজিং ও সামাজিক যোগাযোগমাধ্যম ব্যবহারের নিরাপত্তা

ইন্টারনেটে নিরাপদ ব্রাউজিং ও সামাজিক যোগাযোগমাধ্যম ব্যবহারের নিরাপত্তা:

পরিচয় সুরক্ষা, ব্যক্তিগত তথ্য রক্ষা ও সঠিক ব্যবহারের একটি বিস্তৃত রিভিউ

১. ভূমিকা

ইন্টারনেট আমাদের তথ্য সংগ্রহ, যোগাযোগ, শিক্ষা, কেনাকাটা, চাকরি অনুসন্ধান এবং সামাজিক মিথস্ক্রিয়ার প্রধান মাধ্যম হয়ে উঠেছে। কিন্তু এই সুবিধার পাশাপাশি রয়েছে **সাইবার অপরাধ**, **ডেটা চুরি**, **ভুয়া পরিচয়**, **ফিশিং**, **হ্যাকিং**, **সাইবার বুলিং** ইত্যাদির ঝুঁকি। অতএব, নিরাপদ ব্রাউজিং ও সামাজিক যোগাযোগমাধ্যমের সঠিক ব্যবহার ডিজিটাল যুগে অত্যন্ত গুরুত্বপূর্ণ।

---

২. নিরাপদ ব্রাউজিং (Safe Web Browsing) – কী এবং কেন?

নিরাপদ ব্রাউজিং বলতে বোঝায়—ইন্টারনেট ব্যবহার করার সময় নিজের **ব্যক্তিগত পরিচয়, নেটওয়ার্ক তথ্য, লগইন ডেটা, ব্রাউজিং ইতিহাস, আর্থিক তথ্য ও ডিভাইস**কে সাইবার বিপদ থেকে রক্ষা করার প্রক্রিয়া।

কেন নিরাপদ ব্রাউজিং জরুরি?

- ব্যক্তিগত তথ্য চুরি প্রতিরোধ
- ব্যাংকিং/লেনদেন সুরক্ষিত রাখা
- ম্যালওয়্যার, ভাইরাস, র‍্যানসমওয়্যার থেকে রক্ষা
- ফিশিং থেকে বাঁচা
- ডিজিটাল পরিচয় সুরক্ষিত রাখা

---

৩. নিরাপদ ব্রাউজিংয়ের মূল নীতি (Key Principles of Safe Browsing)

৩.১ Secure Websites ব্যবহার করুন (HTTPS)

- “HTTPS://” দিয়ে শুরু হওয়া সাইট ব্যবহার করুন।
- ব্রাউজার অ্যাড্রেস বারে □ লকের চিহ্ন আছে কিনা যাচাই করুন।

৩.২ শক্তিশালী পাসওয়ার্ড ব্যবহার করুন

- কমপক্ষে ১২+ অক্ষর
- বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও প্রতীক মিলিয়ে
- একই পাসওয়ার্ড বহু সাইটে ব্যবহার করবেন না
- Password Manager ব্যবহার করা নিরাপদ

৩.৩ Browser Update ও Antivirus Update করতে ভুলবেন না

- আপডেটেড ব্রাউজার হ্যাকিং-এর ঝুঁকি কমায়।
- Antivirus real-time protection সক্রিয় রাখুন।

৩.৪ পপ-আপ ও অজানা লিঙ্কে ক্লিক করবেন না

- "You won a prize!" ধরনের লিঙ্ক প্রায়ই ম্যালওয়্যার ছড়ায়।

৩.৫ Public Wi-Fi নিরাপদ নয়

- ব্যাংকিং, লেনদেন বা লগইন Public Wi-Fi-তে করবেন না
- জরুরি প্রয়োজনে VPN ব্যবহার করুন

---

৪. পরিচয় সুরক্ষা (Identity Protection)

ইন্টারনেটে অসতর্ক ব্যবহার আপনাকে **Identity Theft** বা পরিচয় চুরির ঝুঁকিতে ফেলতে পারে।

৪.১ পরিচয় চুরি কী?

যখন কেউ আপনার অনুমতি ছাড়া—

- নাম
- ফোন নম্বর
- পাসওয়ার্ড
- জাতীয় পরিচয়পত্র তথ্য

- ক্রেডিট কার্ড তথ্য
- ছবি
  এসব ব্যবহার করে প্রতারণা করে, তখন তাকে Identity Theft বলে।

৪.২ পরিচয় সুরক্ষার উপায়

✔ব্যক্তিগত তথ্য অতিরিক্ত শেয়ার করবেন না

নিজের ঠিকানা, স্কুল/কলেজ, জন্মতারিখ, ফোন নম্বর সর্বত্র প্রকাশ করা বিপজ্জনক।

✔দুই স্তরের নিরাপত্তা (Two-Factor Authentication – 2FA) ব্যবহার করুন

OTP, Authenticator App, Fingerprint ইত্যাদি।

✔Social Site-এর Privacy Settings সঠিকভাবে সেট করুন

- Public → Friends → Only Me
  মনে রাখুন, সব পোস্ট Public করা উচিত নয়।

✔Password Leak Monitor ব্যবহার করুন

Google Password Manager বা Firefox Monitor ব্যবহার করতে পারেন।

✔Suspicious Apps অনুমতি না দিয়ে Install করবেন না

“Contacts, Camera, Location” অ্যাকসেস চাওয়া অ্যাপ নিরাপত্তা ঝুঁকি তৈরি করতে পারে।

---

৫. সামাজিক যোগাযোগমাধ্যমের নিরাপদ ব্যবহার (Safe Use of Social Networks)

Facebook, Instagram, WhatsApp, X (Twitter), YouTube ইত্যাদি আমাদের ডিজিটাল জীবনকে প্রভাবিত করে।
তাই এগুলো ব্যবহারে সচেতনতা অত্যন্ত গুরুত্বপূর্ণ।

৫.১ আগামী বিপদসমূহ

- Fake profile
- Cyberbullying
- Online fraud (Lottery, job scam)
- Revenge porn/blackmail
- Phishing link
- Impersonation
- Hate speech trap

৫.২ নিরাপদ ব্যবহারের নিয়ম

✔অজানা ব্যক্তির friend request গ্রহণ করবেন না

ফেক অ্যাকাউন্টের প্রধান লক্ষ্য—তথ্য সংগ্রহ।

✔কাউকে ব্যক্তিগত ছবি/ভিডিও পাঠানোর আগে ভাবুন

একবার ইন্টারনেটে আপলোড হলে চিরকালই থেকে যেতে পারে।

✔Location Sharing বন্ধ রাখুন

“Live Location” অপ্রয়োজনীয়ভাবে শেয়ার করা ঝুঁকির।

✔শিশু এবং কিশোরদের জন্য Parental Control সক্রিয় করুন

Cyber grooming-এর আশঙ্কা বেশি।

✔সন্দেহজনক পোস্ট/মন্তব্য রিপোর্ট করুন

সোশ্যাল প্ল্যাটফর্মে Report/Block অত্যন্ত কার্যকর।

---

৬. Cyber Threats – প্রধান ঝুঁকি ও প্রতিরোধ

৬.১ Malware

সমাধান: Antivirus, Firewall, নিরাপদ ডাউনলোড।

৬.২ Phishing Attack

ভুয়া লিঙ্ক/ইমেল ব্যবহার করে তথ্য চুরি।
সমাধান: লিঙ্ক ক্লিকের আগে যাচাই, Sender Authenticity পরীক্ষা।

৬.৩ Ransomware

তথ্য লক করে মুক্তিপণ দাবি।
সমাধান: Backup রাখা, অজানা সফটওয়্যার ইনস্টল না করা।

৬.৪ Social Engineering

মানুষকে প্রতারণা করে তথ্য বের করে নেওয়া।
সমাধান: অচেনা কল/মেসেজে OTP শেয়ার না করা।

---

৭. নৈতিক ব্যবহার (Ethical & Responsible Use of Internet)

✔ভুয়া তথ্য ছড়াবেন না

✔Cyberbullying করবেন না

✔Copyright মেনে চলুন

✔ব্যক্তিগত তথ্য চুরি অপরাধ

✔অন্যের গোপনীয়তা সম্মান করুন

সুস্থ ডিজিটাল সমাজ গড়তে নৈতিকতা অপরিহার্য।

---

৮. উপসংহার

নিরাপদ ব্রাউজিং এবং সামাজিক মাধ্যমের সঠিক ব্যবহার আমাদের ডিজিটাল পরিচয়, তথ্য, আর্থিক নিরাপত্তা এবং ব্যক্তিগত গোপনীয়তা রক্ষা করে।
পরিচয় সুরক্ষা, সতর্কতা, শক্তিশালী পাসওয়ার্ড, প্রাইভেসি কন্ট্রোল, নিরাপদ ও দায়িত্বশীল আচরণ—এগুলো মিলেই একজন সচেতন ডিজিটাল নাগরিক তৈরি করে।
ডিজিটাল যুগে সাইবার নিরাপত্তা শুধু প্রযুক্তিগত নয়—এটি শিক্ষারও গুরুত্বপূর্ণ অংশ।

⭐ MCQ Set – 55 Questions (with Answers)

(Safe Browsing • Cybersecurity • Social Media Safety • Identity Protection)

A. Safe Browsing – Basic Concepts

১. HTTPS-এর ‘S’ কী নির্দেশ করে?

A) Safe
B) Secure
C) System
D) Software
✔উত্তর: B

২. কোনটি নিরাপদ ওয়েবসাইটের চিহ্ন?

A) www দিয়ে শুরু
B) HTTP
C) HTTPS + □ lock icon
D) Flash Player
✔উত্তর: C

৩. ‘Phishing’ কী?

A) ওয়াই-ফাই শেয়ার করা
B) ফেক লিঙ্ক পাঠিয়ে তথ্য চুরি
C) ছবি আপলোড করা

D) ভিডিও রেকর্ড করা
✔উত্তর: B

৪. নিম্নের কোনটি Safe Browsing-এর নিয়ম নয়?

A) শক্তিশালী পাসওয়ার্ড
B) সন্দেহজনক সাইট এড়ানো
C) পাবলিক Wi-Fi-তে ব্যাংকিং লগইন
D) Browser update করা
✔উত্তর: C

৫. Public Wi-Fi ব্যবহার নিরাপদ নয় কেন?

A) নেট স্লো
B) হ্যাকিং সহজ
C) চার্জ নেয়
D) সিগনাল কম
✔উত্তর: B

B. Identity Protection

৬. Identity Theft বলতে বোঝায়—

A) ডিভাইস চুরি
B) ব্যক্তিগত তথ্য চুরি
C) ইমেল পাঠানো
D) ইউজারনেম পরিবর্তন
✔উত্তর: B

৭. Two-Factor Authentication কোথায় ব্যবহৃত হয়?

A) Account security
B) Keyboard typing
C) File printing
D) Computer shutdown
✔উত্তর: A

৮. শক্তিশালী পাসওয়ার্ডের বৈশিষ্ট্য—

A) ছোট ও সহজ
B) জন্মতারিখ
C) নাম + 123
D) অক্ষর + সংখ্যা + প্রতীক
✔উত্তর: D

৯. কোনটি Identity চুরির ঝুঁকি বাড়ায়?

A) Privacy settings বন্ধ রাখা
B) Password Manager
C) HTTPS ব্যবহার
D) ফোনে screen lock
✔উত্তর: A

১০. Dark Web সাধারণত ব্যবহৃত হয়—

A) Social media
B) অবৈধ তথ্য লেনদেন
C) Online teaching
D) Video uploads
✔উত্তর: B

C. Cybersecurity Threats

১১. Malware কী?

A) একটি সফটওয়্যার আপডেট
B) ক্ষতিকারক সফটওয়্যার
C) স্টোরেজ ডিভাইস
D) অ্যাকাউন্ট সেটিং
✔উত্তর: B

১২. Ransomware কী করে?

A) ফোন চার্জ কমায়
B) গেম ইনস্টল করে

C) ডেটা লক করে মুক্তিপণ দাবি করে
D) ভিডিও প্লে করে
✔উত্তর: C

১৩. Virus ছড়ায়—

A) Pen drive
B) ফিশিং ইমেল
C) অজানা সফটওয়্যার
D) সবগুলো
✔উত্তর: D

১৪. Firewall-এর প্রধান কাজ—

A) Screen protect করা
B) Unauthorized access ব্লক করা
C) Keyboard ঠিক করা
D) Printer sync করা
✔উত্তর: B

১৫. Antivirus software ব্যবহৃত হয়—

A) গেম খেলতে
B) ফাইল কমপ্রেস করতে
C) ভাইরাস শনাক্ত ও অপসারণ করতে
D) ছবি সম্পাদনা করতে
✔উত্তর: C

D. Social Media Safety

১৬. সামাজিক মাধ্যমে সবচেয়ে বড় ঝুঁকি—

A) Networking
B) Fake profile
C) Music share
D) Photo editing
✔উত্তর: B

১৭. Cyberbullying কী?

A) গাড়িতে ধাক্কা
B) অনলাইনে অপমান/হয়রানি
C) ভিডিও ডাউনলোড
D) পোস্ট শেয়ার
✔উত্তর: B

১৮. কোনটি সামাজিক মাধ্যমে নিরাপত্তা বাড়ায়?

A) Location always ON
B) সব পোস্ট Public
C) Strong privacy settings
D) অজানা Friend Request গ্রহণ
✔উত্তর: C

১৯. Impersonation বলতে বোঝায়—

A) ভুল লেখা
B) নকল পরিচয় ব্যবহার
C) কম রেজোলিউশন ছবি
D) ভিডিও পোস্ট করা
✔উত্তর: B

২০. Social media-তে কোনটি কখনও শেয়ার করা উচিত নয়?

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

E. Ethical & Responsible Use

২১. Plagiarism হলো—

A) নিজের লেখা
B) কপি করা লেখা নিজের নামে ব্যবহার
C) ভিডিও আপলোড
D) Picture editing
✔উত্তর: B

২২. Cyber ethics শেখায়—

A) দ্রুত ব্রাউজ করা
B) ভদ্র আচরণ ও দায়িত্বশীল ব্যবহার
C) অবৈধ ডাউনলোড
D) Anonymous পোস্ট
✔উত্তর: B

২৩. কোনটা নৈতিক আচরণ?

A) অন্যের ছবি অনুমতি ছাড়া পোস্ট করা
B) ভুয়া খবর ছড়ানো
C) অনলাইনে সম্মান বজায় রাখা
D) Password শেয়ার করা
✔উত্তর: C

F. Safe Use of Web Services

২৪. Cookies ব্যবহৃত হয়—

A) Memory increase
B) User preference সংরক্ষণে
C) Virus ছড়াতে
D) Screen clean করতে
✔উত্তর: B

২৫. Browser cache পরিষ্কার করলে—

A) হ্যাকিং বাড়ে
B) ব্রাউজিং ধীর হয়
C) নিরাপত্তা বাড়ে

D) মেমরি কমে
✔উত্তর: C

২৬. Pop-up blocker ব্যবহৃত হয়—

A) বিজ্ঞাপন আটকাতে
B) ফাইল কম্প্রেস করতে
C) ছবি বড় করতে
D) Printer sync করতে
✔উত্তর: A

৭. Private/Incognito Mode ব্যবহৃত হয়—

A) History save না করার জন্য
B) ভুয়া ইমেল পাঠাতে
C) গেম খেলতে
D) ভিডিও পরিষ্কার করতে
✔উত্তর: A

২৮. কোনটি নিরাপদ লগইন পদ্ধতি?

A) Only password
B) Password + OTP
C) Password বন্ধুদের বলা
D) Public Wi-Fi login
✔উত্তর: B

G. Online Scams & Fraud Prevention

২৯. Lottery scam সাধারণত কোথায় দেখা যায়?

A) Offline poster
B) Social media/Email
C) Restaurant
D) Cinema hall
✔উত্তর: B

৩০. Job scam চিনতে সহায়ক—

A) High salary without interview
B) Official email
C) Verified account
D) Proper documentation
✔উত্তর: A

৩১. OTP কারো সাথে শেয়ার করা—

A) নিরাপদ
B) বিপজ্জনক
C) জরুরি
D) শিক্ষামূলক
✔উত্তর: B

৩২. Fake App শনাক্ত করা যায়—

A) Low downloads
B) Negative reviews
C) Excessive permissions
D) সবগুলো
✔উত্তর: D

H. Children & Youth Online Safety

৩৩. Parental control ব্যবহৃত হয়—

A) শিশুদের জন্য নিরাপদ ব্যবহার নিশ্চিত করতে
B) মিউজিক শোনাতে
C) গেমিং বাড়াতে
D) নেট স্পিড বাড়াতে
✔উত্তর: A

৩৪. Cyber grooming প্রধানত কারা করে?

A) শিক্ষক
B) অপরিচিত প্রাপ্তবয়স্ক ব্যক্তি
C) ডাক্তার

D) বন্ধু
✔উত্তর: B

৩৫. School cyber safety program-এর উদ্দেশ্য—

A) Online gaming
B) Digital citizenship শেখানো
C) Drawing competition
D) Sports
✔উত্তর: B

I. Devices & Security Tools

৩৬. VPN ব্যবহৃত হয়—

A) ইন্টারনেট লুকাতে
B) নিরাপদ নেটওয়ার্ক তৈরি করতে
C) ভিডিও বড় করতে
D) পাসওয়ার্ড মনে রাখতে
✔উত্তর: B

৩৭. কোনটি একটি security tool?

A) Calculator
B) Firewall
C) Paint
D) Media player
✔উত্তর: B

৩৮. Backup রাখা জরুরি কেন?

A) PC সুন্দর লাগে
B) ডেটা হারানো থেকে রক্ষা
C) Anti-virus চলে
D) নেট স্পিড বাড়ে
✔উত্তর: B

৩৯. Encryption ব্যবহৃত হয়—

A) ডেটা সুরক্ষিত রাখতে
B) ছবি এডিট করতে
C) Software install করতে
D) Color পরিবর্তন করতে
✔উত্তর: A

৪০. CAPTCHA ব্যবহৃত হয়—

A) মানুষ–মেশিন আলাদা করতে
B) PC ফরম্যাট করতে
C) ব্যাটারি বাঁচাতে
D) স্ক্রিন পরিষ্কার করতে
✔উত্তর: A

J. Miscellaneous (General Awareness)

৪১. Spam mail সাধারণত—

A) গুরুত্বপূর্ণ
B) অনাকাঙ্ক্ষিত
C) গবেষণামূলক
D) সুরক্ষিত
✔উত্তর: B

৪২. Browser history পরিষ্কার করলে—

A) Privacy বাড়ে
B) গেম চালু হয়
C) RAM বাড়ে
D) Data loss হয়
✔উত্তর: A

৪৩. কোনটি Privacy Issue?

A) Data leak
B) Music download
C) Calculator ব্যবহার

D) Screen brightness
✔উত্তর: A

৪৪. Digital footprint বলতে বোঝায়—

A) বাস্তব পদচিহ্ন
B) অনলাইনে রেখে যাওয়া তথ্য
C) জন্ম সনদ
D) পাসপোর্ট
✔উত্তর: B

৪৫. Cybercrime report করার উপায়—

A) থানায়
B) 1930 হেল্পলাইনে
C) cybercrime.gov.in
D) সবগুলো
✔উত্তর: D

K. Bonus Set — 10 Extra MCQs

৪৬. কোনটি নিরাপত্তার লাল সংকেত?

A) Email from trusted domain
B) Spelling mistakes in email
C) Verified icon
D) Govt website
✔উত্তর: B

৪৭. Strong privacy setting মানে—

A) Public for all
B) Friends only
C) Everyone can see
D) Unlimited share
✔উত্তর: B

৪৮. কোনটি নিরাপদ অভ্যাস নয়?

A) Password notebook-এ লেখা
B) 2FA
C) HTTPS browsing
D) Antivirus enable
✔উত্তর: A

৪৯. সাইবার হুমকির মূল টার্গেট—

A) Data
B) Fan
C) Keyboard
D) Speaker
✔উত্তর: A

৫০. Cyberstalking হলো—

A) Physical fight
B) অনবরত অনলাইন নজরদারি/অনুসরণ
C) গেমিং
D) পোস্ট শেয়ার
✔উত্তর: B

৫১. কোনটি অনলাইন সুরক্ষার মূলনীতি?

A) Think before you click
B) সব লিঙ্কে ক্লিক
C) অজানা ফাইল ডাউনলোড
D) Password share
✔উত্তর: A

৫২. Which one protects your online identity?

A) 2FA
B) Public Wi-Fi
C) Weak password
D) Fake profile
✔উত্তর: A

৫৩. Social media-এর কোন তথ্য Criminals বেশি ব্যবহার করে?

A) Birthday
B) Hobbies
C) Phone number
D) সবগুলো
✔উত্তর: D

৫৪. Anti-phishing toolbar ব্যবহৃত হয়—

A) Fake website শনাক্ত করতে
B) Printer চালাতে
C) গেম খেলতে
D) Browser refresh করতে
✔উত্তর: A

৫৫. Digital citizenship অন্তর্ভুক্ত করে—

A) নিরাপদ ব্যবহার
B) নৈতিক ব্যবহার
C) দায়িত্বশীল ব্যবহার
D) সবগুলো
✔উত্তর: D

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

⋆ *মডেল প্রশ্ন+ সংক্ষিপ্ত উত্তর*

SAQ–1: Safe Browsing বলতে কী বোঝায়?

উত্তর:
Safe Browsing হলো ইন্টারনেট ব্যবহার করার সময় নিজের ব্যক্তিগত তথ্য, লগইন ডেটা, আর্থিক তথ্য ও ডিভাইসকে সাইবার আক্রমণ, ম্যালওয়্যার, ফিশিং ও ডেটা লিক থেকে সুরক্ষিত রাখার প্রক্রিয়া।

SAQ–2: HTTPS ও HTTP-এর মধ্যে পার্থক্য লিখো।

উত্তর:
HTTP অনিরাপদ প্রোটোকল, আর HTTPS (HyperText Transfer Protocol Secure) ডেটা এনক্রিপশন ব্যবহার করে নিরাপদ যোগাযোগ নিশ্চিত করে। HTTPS সাইটের অ্যাড্রেস বারে □ লক চিহ্ন থাকে।

SAQ–3: Phishing কী?

উত্তর:
Phishing হলো ভুয়া ইমেল, বার্তা বা লিঙ্ক ব্যবহার করে ব্যক্তিগত ডেটা (পাসওয়ার্ড, ব্যাংক তথ্য) চুরি করার প্রতারণামূলক কৌশল।

SAQ–4: Identity Theft কী?

উত্তর:
কোনো ব্যক্তি তার অনুমতি ছাড়া তার ব্যক্তিগত তথ্য (নাম, ফোন, ব্যাংক তথ্য, ছবি) ব্যবহার করে অপরাধ করা বা আর্থিক প্রতারণা করাকে Identity Theft বলা হয়।

SAQ–5: Two-Factor Authentication (2FA) কী?

উত্তর:
পাসওয়ার্ডের পাশাপাশি দ্বিতীয় ধাপের নিশ্চয়তা (OTP, Authenticator App, Fingerprint) যুক্ত করে অ্যাকাউন্টের নিরাপত্তা বাড়ানোর পদ্ধতিকে 2FA বলে।

SAQ–6: Strong Password তৈরির নিয়ম কী?

উত্তর:
কমপক্ষে ১২+ অক্ষর, বড় ও ছোট হাতের অক্ষর, সংখ্যা এবং প্রতীক মিলিয়ে ব্যবহার করা; জন্মতারিখ/নাম ব্যবহার না করা।

SAQ–7: Social Engineering কী?

উত্তর:
মানুষকে প্রতারণা করে সংবেদনশীল তথ্য বের করে নেওয়ার কৌশল। যেমন: প্রলোভন, ভয় দেখানো, ভুয়া ফোন বা বার্তা।

SAQ–8: Cyberbullying বলতে কী বোঝায়?

উত্তর:
অনলাইনে কাউকে অপমান, হুমকি, গালি, কটূক্তি বা মানসিক হয়রানি করাকে Cyberbullying বলা হয়।

SAQ–9: Fake Profile কেন বিপজ্জনক?

উত্তর:
Fake Profile ব্যবহার করে তথ্য সংগ্রহ, ব্ল্যাকমেইল, অনলাইন প্রতারণা এবং সাইবারবুলিং করা হয়। এটি পরিচয় চুরির ঝুঁকি বাড়ায়।

SAQ–10: Incognito Mode কী?

উত্তর:
Incognito (Private) Mode ব্রাউজিং হিস্ট্রি, কুকিস ও ফর্ম ডেটা সংরক্ষণ করে না, ফলে অস্থায়ী গোপনীয়তা বাড়ে।

SAQ–11: Ransomware কী?

উত্তর:
একটি ম্যালওয়্যার যা কম্পিউটারের ডেটা এনক্রিপ্ট করে লক করে দেয় এবং পুনরুদ্ধারের জন্য মুক্তিপণ দাবি করে।

SAQ–12: Parental Control Tools-এর ভূমিকা কী?

উত্তর:
শিশুদের অনিরাপদ কন্টেন্ট, গেম বা অচেনা ব্যক্তির যোগাযোগ থেকে সুরক্ষিত রাখতে ব্যবহৃত নিরাপত্তা টুল।

SAQ–13: Digital Footprint বলতে কী বোঝানো হয়?

উত্তর:
ব্যবহারকারীর অনলাইনে রেখে যাওয়া পদচিহ্ন—যেমন সার্চ ইতিহাস, পোস্ট, কমেন্ট, লগইন ডেটা ইত্যাদি।

SAQ–14: CAPTCHA-এর উদ্দেশ্য কী?

উত্তর:
মানুষ এবং বটের মধ্যে পার্থক্য নির্ণয় করে স্বয়ংক্রিয় আক্রমণ প্রতিরোধ করা।

SAQ–15: Public Wi-Fi কেন ঝুঁকিপূর্ণ?

উত্তর:
Public Wi-Fi-তে ডেটা এনক্রিপ্টেড নয়; Man-in-the-Middle Attack, Session Hijacking, Password Theft-এর ঝুঁকি বেশি।

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

⋆ *মডেল প্রশ্ন + বিশদ উত্তর*

LAQ–1: Safe Browsing-এর নীতি ও গুরুত্ব বিস্তারিত ব্যাখ্যা করো।

উত্তর:
Safe Browsing হলো এমন এক নিরাপদ ইন্টারনেট ব্যবহার ব্যবস্থা যেখানে ব্যক্তি তার ডেটা, পরিচয়, পাসওয়ার্ড ও আর্থিক তথ্যকে সাইবার আক্রমণ থেকে রক্ষা করে।
এর গুরুত্ব হলো—

1. **ব্যক্তিগত তথ্য সুরক্ষা**
2. **ব্যাংকিং/লেনদেন নিরাপদ রাখা**
3. **ফিশিং ও ম্যালওয়্যার এড়ানো**
4. **ডিভাইস সুরক্ষা**
5. **অনলাইন প্রতারণা প্রতিরোধ**

Safe Browsing-এর নীতি:

- শুধুমাত্র HTTPS সাইট ব্যবহার
- শক্তিশালী পাসওয়ার্ড
- 2FA ব্যবহার
- সন্দেহজনক লিঙ্কে ক্লিক না করা
- Browser/OS/Antivirus আপডেট
- Pop-up blocker ব্যবহার
- Public Wi-Fi এড়ানো
- VPN ব্যবহার

Safe Browsing সচেতনতা একজন ব্যবহারকারীকে সাইবার অপরাধ থেকে নিরাপদ রাখে।

LAQ–2: Social Media Safety কী? সামাজিক মাধ্যম ব্যবহারের ঝুঁকি ও সুরক্ষা কৌশল ব্যাখ্যা করো।

উত্তর:
Social Media Safety হলো Facebook, Instagram, WhatsApp, X (Twitter) ইত্যাদি প্ল্যাটফর্মে দায়িত্বশীল এবং নিরাপদ ব্যবহারের কৌশল।

সামাজিক মাধ্যমের ঝুঁকি:

- Fake profile
- Identity theft
- Cyberbullying
- Online blackmail
- Revenge porn
- Location tracking risk
- Phishing scams
- Data leak

সুরক্ষা কৌশল:

- Privacy settings সঠিকভাবে সেট করা
- Only Friends mode ব্যবহার
- অজানা request এড়ানো
- Location sharing বন্ধ রাখা
- Strong password ও 2FA
- Report/Block ব্যবহার
- ব্যক্তিগত তথ্য কম শেয়ার করা
- শিশুদের জন্য Parental control

সামাজিক মাধ্যমের নিরাপত্তা নিশ্চিত করতে সচেতনতা অত্যন্ত গুরুত্বপূর্ণ।

LAQ–3: Identity Theft কী? এর ধরন, ঝুঁকি ও প্রতিরোধব্যবস্থা ব্যাখ্যা করো।

উত্তর:

Identity Theft:

ব্যক্তির নাম, ছবি, জন্মতারিখ, ফোন, ব্যাংক তথ্য, জাতীয় পরিচয়পত্র ইত্যাদি চুরি করে প্রতারণা করা।

Identity Theft-এর ধরন:

- Financial identity theft
- Social media identity theft
- Criminal identity theft
- Medical identity theft
- Synthetic identity theft

ঝুঁকি:

- ব্যাংক অ্যাকাউন্ট হ্যাক
- সোশ্যাল মিডিয়া অ্যাকাউন্ট চুরি
- ব্ল্যাকমেইল
- পরিচয় ব্যবহার করে অপরাধ
- ডিজিটাল নিরাপত্তা ক্ষতিগ্রস্ত হওয়া

প্রতিরোধব্যবস্থা:

- শক্তিশালী পাসওয়ার্ড
- দুই স্তরের নিরাপত্তা (2FA)
- সীমিত ব্যক্তিগত তথ্য শেয়ার
- Privacy settings
- Password leak monitor
- অজানা লিঙ্ক/কল এড়ানো
- VPN ব্যবহার

Identity Theft প্রতিরোধে ব্যবহারকারীর সতর্কতা সবচেয়ে বড় অস্ত্র।

LAQ–4: Cyber Threats (Malware, Phishing, Ransomware, Social Engineering) ব্যাখ্যা করো এবং সেগুলো থেকে সুরক্ষার উপায় আলোচনা করো।

উত্তর:

১. Malware:

ক্ষতিকর সফটওয়্যার যা ডিভাইস ক্ষতিগ্রস্ত করে।
সুরক্ষা: Antivirus, firewall, safe download।

২. Phishing:

ভুয়া লিঙ্ক/ইমেল পাঠিয়ে তথ্য চুরি।
সুরক্ষা: Sender যাচাই, suspicious link avoid।

৩. Ransomware:

ডেটা লক করে মুক্তিপণ দাবি।
সুরক্ষা: Backup, antivirus, unknown email avoid।

৪. Social Engineering:

মানুষকে প্রতারণা করে তথ্য সংগ্রহ।
সুরক্ষা: OTP শেয়ার না করা, caller verification, সচেতনতা।

সাইবার হুমকি থেকে রক্ষা পেতে প্রযুক্তিগত নিরাপত্তা + ব্যবহারকারীর সতর্কতা দুইই জরুরি।

LAQ–5: শিশু-কিশোরদের অনলাইন নিরাপত্তার চ্যালেঞ্জ ও সমাধান আলোচনা করো।

উত্তর:

চ্যালেঞ্জ:

- Cyberbullying
- Fake account interaction
- Cyber grooming
- Inappropriate content
- Excess screen time
- Addiction
- Privacy leak

সমাধান:

- Parental control tools
- Screen time limit
- Child-safe browsers
- School cyber safety education
- Family rules for internet use
- Social media age restriction মানা

শিশুদের নিরাপত্তার জন্য প্রযুক্তিগত কন্ট্রোলের পাশাপাশি অভিভাবকের সচেতনতা অত্যন্ত গুরুত্বপূর্ণ।

□ এক পাতার সংক্ষিপ্ত নোট

ইন্টারনেটে নিরাপদ ব্রাউজিং ও সামাজিক যোগাযোগমাধ্যম ব্যবহারের সঠিক পদ্ধতি

---

১. Safe Browsing – কী ও কেন?

Safe Browsing হলো ইন্টারনেট ব্যবহার করার সময় নিজের **ব্যক্তিগত তথ্য, পাসওয়ার্ড, আর্থিক তথ্য, ডিভাইস ও ডেটা**কে সাইবার ঝুঁ