অধ্যায়-১ সাইবার নিরাপত্তা এবং ঝুঁকি নিয়ন্ত্রণ

SOS অতি সংক্ষিপ্ত প্রশ্নোত্তর ঃ

***** ১। সাইবার নিরাপত্তা (Cyber Security) বলতে কী বুঝায়?**

বাকাশিবো- ২০১৯, ২১, ২৪'পরি

উত্তর ঃ সাইবার নিরাপত্তা (Cyber Security) হলো এমন একটি প্রক্রিয়া, যার মাধ্যমে কম্পিউটার, সার্ভার, মোবাইল ডিভাইস, ইলেকট্রনিক সিস্টেম, নেটওয়ার্ক এবং ডাটাকে ডিজিটাল আক্রমণ বা হ্যাকিং থেকে রক্ষা করা হয়।

*** ২। সাইবার নিরাপত্তা কয় প্রকার ও কী কী?** বাকাশিবো- ২০২২

উত্তর ঃ সাইবার নিরাপত্তাকে কাজের ক্ষেত্র এবং সুরক্ষার ধরন অনুযায়ী সাধারণত ৫টি প্রধান ভাগে ভাগ করা যায়। যথাঃ

i) নেটওয়ার্ক নিরাপত্তা (Network Security)
ii) অ্যাপ্লিকেশন নিরাপত্তা (Application Security)
iii) তথ্য বা ডাটা নিরাপত্তা (Information Security - InfoSec)
iv) ক্লাউড নিরাপত্তা (Cloud Security)
v) এন্ডপয়েন্ট নিরাপত্তা (Endpoint Security)

***** ৩। সাইবার অপরাধ (Cyber Crime) বলতে কী বুঝ?**

বাকাশিবো- ২০১৯, ২১, ২২

উত্তর ঃ ডিজিটাল প্রযুক্তি বা ইন্টারনেট ব্যবহার করে কোনো ব্যক্তি, প্রতিষ্ঠান বা রাষ্ট্রের ক্ষতি করা, তথ্য চুরি করা, অর্থ আত্মসাৎ করা বা হয়রানি করাই হলো সাইবার অপরাধ।

*** ৪। ভাইরাস (Virus)বলতে কী বুঝ?**

উত্তর ঃ ভাইরাস (Virus) হলো এক ধরনের ম্যালওয়্যার (Malware) বা ক্ষতিকারক সফটওয়্যার, যা কোনো বৈধ প্রোগ্রাম বা ফাইলের সাথে নিজেকে যুক্ত করে এবং ব্যবহারকারীর অজান্তেই কম্পিউটারের ক্ষতি সাধন করে।

***** ৫। ট্রোজান হর্স (Trojan Horse) কী?** বাকাশিবো- ২০২০, ২১

উত্তর ঃ ট্রোজান হর্স (Trojan Horse) বা সংক্ষেপে ট্রোজান হলো এক ধরনের ম্যালওয়্যার, যা নিজেকে বৈধ বা উপকারী সফটওয়্যার হিসেবে পরিচয় দিয়ে ব্যবহারকারীকে বিভ্রান্ত করে।

নোটঃ নামকরণ করা হয়েছে গ্রিক পুরাণের বিখ্যাত "ট্রয়ের কাঠের ঘোড়া" (Wooden Horse of Troy) এর গল্প থেকে। গল্পে যেমন গ্রিক সৈন্যরা বিশাল কাঠের ঘোড়ার ভেতরে লুকিয়ে ট্রয় নগরীতে প্রবেশ করেছিল, তেমনি এই ম্যালওয়্যারটিও ভালো সফটওয়্যারের আড়ালে লুকিয়ে কম্পিউটারে প্রবেশ করে।

৬। ব্যাকডোর (Backdoor) কী?

উত্তর ঃ ব্যাকডোর হলো এমন একটি গোপন পথ বা পদ্ধতি, যার মাধ্যমে স্বাভাবিক নিরাপত্তা ব্যবস্থা (যেমনঃ ইউজারনেম, পাসওয়ার্ড বা এনক্রিপশন) এড়িয়ে কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা সফটওয়্যারে প্রবেশ করা যায়।

***** ৭। হ্যাকিং (Hacking) কী?** বাকাশিবো- ২০২৪'পরি

উত্তর ঃ হ্যাকিং হলো এমন একটি প্রক্রিয়া, যার মাধ্যমে কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা ডিজিটাল ডিভাইসের নিরাপত্তা ব্যবস্থার দুর্বলতা খুঁজে বের করা হয় এবং সেই দুর্বলতাকে কাজে লাগিয়ে অনুমতি ছাড়াই সেই সিস্টেমে প্রবেশ বা নিয়ন্ত্রণ নেওয়া হয়।

***** ৮। ইথিক্যাল হ্যাকিং (Ethical Hacking) বলতে কী বুঝ?**

বাকাশিবো- ২০২৪'পরি

উত্তর ঃ ইথিক্যাল হ্যাকিং হলো এমন একটি বৈধ ও পেশাদার প্রক্রিয়া, যার মাধ্যমে কোনো ব্যক্তি বা প্রতিষ্ঠানের অনুমতি নিয়ে তাদের কম্পিউটার সিস্টেম, নেটওয়ার্ক বা অ্যাপ্লিকেশনের নিরাপত্তার দুর্বলতা খুঁজে বের করা হয়।

৯। দূর্বলতা (Vurnerability) বলতে কী বুঝায়?

উত্তর ঃ সাইবার নিরাপত্তার পরিভাষায় দুর্বলতা হলো কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক, সফটওয়্যার বা হার্ডওয়্যারের এমন কোনো ত্রুটি বা

সীমাবদ্ধতা, যা ব্যবহার করে হ্যাকাররা সিস্টেমের নিরাপত্তা ভেঙে ফেলতে পারে।

**** ১০। সম্পূর্ণতা (Integrity) বলতে কী বুঝ?** বাকাশিবো- ২০২৫

উত্তর ঃ Integrity বা অখণ্ডতা বলতে বোঝায়–কোনো তথ্য বা ডেটা ঠিক যেভাবে তৈরি বা পাঠানো হয়েছে, তা অবিকল সেই অবস্থায় রাখা। অনুমোদিত ব্যক্তি ছাড়া অন্য কেউ যেন সেই তথ্য পরিবর্তন, পরিবর্ধন বা নষ্ট করতে না পারে, তা নিশ্চিত করাই হলো ইন্টিগ্রিটি।

SOS সংক্ষিপ্ত প্রশ্নোত্তর ঃ

**** ১। সাইবার নিরাপত্তার মূল লক্ষ্যগুলো লেখ।**

উত্তর ঃ সাইবার নিরাপত্তার প্রধান বা মূল লক্ষ্যগুলোকে সংক্ষেপে CIA Triad বলা হয়। এই তিনটি মূল স্তম্ভের ওপর ভিত্তি করেই পুরো নিরাপত্তা ব্যবস্থা গড়ে ওঠে। নিচে সাইবার নিরাপত্তার ৩টি মূল লক্ষ্য বিস্তারিত আলোচনা করা হলো ঃ

i) গোপনীয়তা (Confidentiality) ঃ এর মূল লক্ষ্য হলো, তথ্য যেন শুধুমাত্র অনুমোদিত ব্যক্তিরাই দেখতে বা ব্যবহার করতে পারে। অননুমোদিত কোনো ব্যক্তি, প্রোগ্রাম বা সিস্টেম যেন তথ্যের নাগাল না পায়।

উদাহরণ ঃ আপনার ফেসবুকের মেসেজ যেন আপনি এবং যার সাথে চ্যাট করছেন, তারা ছাড়া অন্য কেউ পড়তে না পারে। পাসওয়ার্ড এবং এনক্রিপশন (Encryption) ব্যবহার করে এটি নিশ্চিত করা হয়।

ii) অখণ্ডতা (Integrity) ঃ তথ্যের সঠিকতা বজায় রাখা এবং কেউ যেন অনুমতি ছাড়া তথ্য পরিবর্তন, পরিবর্ধন বা নষ্ট করতে না পারে, তা নিশ্চিত করা। তথ্যটি উৎস থেকে গন্তব্যে পৌঁছানো পর্যন্ত অবিকল একই থাকবে।

উদাহরণ ঃ আপনি পরীক্ষার রেজাল্ট শিটে যা পেয়েছেন, হ্যাকার যেন তা পরিবর্তন করে নম্বর বাড়িয়ে বা কমিয়ে দিতে না পারে।

iii) প্রাপ্যতা (Availability) ঃ এর অর্থ হলো, যখন তথ্যের প্রয়োজন হবে, তখন যেন অনুমোদিত ব্যবহারকারী তা সহজেই পায়। সার্ভার বা সিস্টেম সবসময় সচল রাখা এর লক্ষ্য।

উদাহরণ ঃ আপনি যখনই মোবাইল ব্যাংকিং অ্যাপে ঢুকবেন, তখনই যেন ব্যালেন্স চেক করতে পারেন। হ্যাকাররা অনেক সময় সার্ভার জ্যাম করে (DDoS Attack) এই প্রাপ্যতা নষ্ট করার চেষ্টা করে।

***** ২। ইথিক্যাল হ্যাকিং কেন প্রয়োজন?** বাকাশিবো-২০২৪'পরি

অথবা, ইথিক্যাল হ্যাকিং এর উদ্দেশ্যাবলি লেখ।

উত্তর ঃ নিচে ইথিক্যাল হ্যাকিং কেন প্রয়োজন, তার প্রধান কারণগুলো আলোচনা করা হলোঃ

i) দুর্বলতা খুঁজে বের করা ও সমাধান ঃ ব্ল্যাক হ্যাট হ্যাকাররা আক্রমণ করার আগেই সিস্টেমের নিরাপত্তা ত্রুটি বা দুর্বলতাগুলো খুঁজে বের করা এবং তা

সমাধান (Patch) করা ইথিক্যাল হ্যাকিংয়ের প্রধান কাজ। এতে সিস্টেম হ্যাক হওয়ার ঝুঁকি কমে যায়।

ii) তথ্য চুরি রোধ ঃ প্রতিষ্ঠান বা গ্রাহকদের সংবেদনশীল তথ্য (যেমনঃ পাসওয়ার্ড, ক্রেডিট কার্ড নম্বর, ব্যক্তিগত ছবি) হ্যাকারদের হাত থেকে রক্ষা করার জন্য ইথিক্যাল হ্যাকিং প্রয়োজন। এটি তথ্যের গোপনীয়তা (Confidentiality) নিশ্চিত করে।

iii) আর্থিক ক্ষতি থেকে রক্ষা ঃ একটি বড় সাইবার আক্রমণ বা র‍্যানসামওয়্যার অ্যাটাক কোনো কোম্পানিকে আর্থিকভাবে দেউলিয়া করে দিতে পারে। ইথিক্যাল হ্যাকাররা আগে থেকেই নিরাপত্তা নিশ্চিত করে এই বিশাল আর্থিক ক্ষতি থেকে প্রতিষ্ঠানকে বাঁচায়।

iv) জাতীয় নিরাপত্তা রক্ষা ঃ দেশের প্রতিরক্ষা ব্যবস্থা, বিদ্যুৎ কেন্দ্র, ব্যাংকিং সেক্টর এবং সরকারি নথিপত্র এখন ডিজিটাল নেটওয়ার্কের ওপর নির্ভরশীল। বিদেশি হ্যাকার বা সাইবার সন্ত্রাসীদের হাত থেকে দেশের এই গুরুত্বপূর্ণ অবকাঠামো রক্ষা করতে ইথিক্যাল হ্যাকাররা "সাইবার আর্মি" হিসেবে কাজ করে।

v) গ্রাহকের আস্থা অর্জন ঃ যে কোম্পানির নিরাপত্তা ব্যবস্থা যত শক্তিশালী, গ্রাহকরা সেই কোম্পানিকে তত বেশি বিশ্বাস করে। ইথিক্যাল হ্যাকিং নিশ্চিত করে যে ওই প্রতিষ্ঠানের সেবা ব্যবহার করা নিরাপদ।

vi) আইনি সুরক্ষা ঃ অনেক দেশে গ্রাহকের ডেটা সুরক্ষা দেওয়া আইনের বাধ্যতামূলক। ইথিক্যাল হ্যাকিংয়ের মাধ্যমে কোম্পানিগুলো নিশ্চিত হয় যে

তারা সব ধরনের সাইবার আইন মেনে চলছে, ফলে আইনি ঝামেলা এড়ানো যায়।

***** ৩। ইথিক্যাল হ্যাকিং এর প্রকারভেদ বর্ণনা কর।** বাকাশিবো-২০২৫

উত্তর ঃ একজন ইথিক্যাল হ্যাকারকে সিস্টেম সম্পর্কে কতটুকু তথ্য দেওয়া হয়েছে, তার ওপর ভিত্তি করে হ্যাকিংকে ৩টি বক্সে ভাগ করা হয়ঃ

i) ব্ল্যাক বক্স টেস্টিং (Black Box Testing) ঃ এখানে ইথিক্যাল হ্যাকারকে টার্গেট সিস্টেম সম্পর্কে কোনো তথ্যই দেওয়া হয় না। তাকে একজন অপরিচিত বা বাইরের হ্যাকারের (Attacker) মতো শূন্য থেকে দুর্বলতা খুঁজে বের করতে হয়। এটিই আসল হ্যাকিংয়ের সবচেয়ে কাছাকাছি পদ্ধতি।

ii) হোয়াইট বক্স টেস্টিং (White Box Testing) ঃ এখানে হ্যাকারকে সিস্টেমের সব তথ্য (সোর্স কোড, নেটওয়ার্ক ম্যাপ, পাসওয়ার্ড) আগেই দিয়ে দেওয়া হয়। হ্যাকারের কাজ হলো কোডের ভেতর লুকিয়ে থাকা গভীর কোনো ত্রুটি খুঁজে বের করা। এটি সাধারণত ডেভেলপার বা কোম্পানির নিজস্ব লোকরা করে থাকে।

iii) গ্রে বক্স টেস্টিং (Grey Box Testing) ঃ এটি ব্ল্যাক এবং হোয়াইট বক্সের মিশ্রণ। এখানে হ্যাকারকে আংশিক তথ্য (যেমনঃ শুধু সাধারণ ইউজার আইডি বা নেটওয়ার্কের কিছু অংশ) জানানো হয়। বাইরের একজন সাধারণ ইউজার সিস্টেমে ঢুকে কতটা ক্ষতি করতে পারে, তা দেখার জন্য এটি করা হয়।

**** ৪। ইথিক্যাল হ্যাকিং এর ধাপগুলো লেখ।**

উত্তর ঃ ইথিক্যাল হ্যাকিং একটি সুশৃঙ্খল প্রক্রিয়া। একজন ইথিক্যাল হ্যাকার সাধারণত 5টি (রিপোর্টিং সহ 6টি) ধাপে এই কাজটি সম্পন্ন করেন। এই ধাপগুলোকে "Phases of Hacking" বলা হয়।

নিচে ধাপগুলো বিস্তারিত আলোচনা করা হলো ঃ

১. তথ্য সংগ্রহ ঃ এটি হ্যাকিংয়ের প্রথম এবং সবচেয়ে গুরুত্বপূর্ণ ধাপ। এখানে হ্যাকার টার্গেট সিস্টেম বা কোম্পানি সম্পর্কে যথাসম্ভব বেশি তথ্য সংগ্রহ করার চেষ্টা করেন।

২. স্ক্যানিং ঃ প্রথম ধাপে পাওয়া তথ্যের ওপর ভিত্তি করে হ্যাকার বিভিন্ন টুলস ব্যবহার করে সিস্টেমের নির্দিষ্ট দুর্বলতা বা খোলা পথ (Open Ports) খোঁজার চেষ্টা করেন।

৩. সিস্টেমে প্রবেশ ঃ এটিই মূল হ্যাকিং ধাপ। স্ক্যানিংয়ের মাধ্যমে পাওয়া দুর্বলতাকে কাজে লাগিয়ে হ্যাকার সিস্টেমে প্রবেশ করেন বা নিয়ন্ত্রণ নেন।

৪. এক্সেস ধরে রাখা ঃ একবার সিস্টেমে ঢোকার পর, হ্যাকার চেষ্টা করেন ভবিষ্যতে যেন আবার সহজে ঢোকা যায়। কারণ সিস্টেম অ্যাডমিন মূল দুর্বলতাটি ঠিক করে ফেললে হ্যাকার আর ঢুকতে পারবেন না। তাই তিনি বিকল্প পথ তৈরি করেন।

৫. প্রমাণ বা চিহ্ন মুছে ফেলা ঃ সিস্টেমে ঢোকার পর যেন কেউ তাকে ট্রেস বা শনাক্ত করতে না পারে, সেজন্য হ্যাকার তার উপস্থিতির সব প্রমাণ মুছে ফেলেন।

৬. রিপোর্টিং ঃ এটিই ইথিক্যাল হ্যাকিং এবং সাধারণ হ্যাকিংয়ের প্রধান পার্থক্য। ওপরের ৫টি ধাপ শেষ করার পর ইথিক্যাল হ্যাকার একটি বিস্তারিত রিপোর্ট তৈরি করেন।

SOS রচনামূলক প্রশ্নোত্তর ঃ

**** ১। ব্যবসা প্রতিষ্ঠান ও সমাজে সাইবার নিরাপত্তার গুরুত্ব আলোচনা কর।** বাকাশিবো-২০২২

উত্তর ঃ বর্তমান ডিজিটাল যুগে ব্যবসা প্রতিষ্ঠান এবং সমাজের প্রতিটি স্তরে সাইবার নিরাপত্তা বা সাইবার সিকিউরিটির গুরুত্ব অপরিসীম। প্রযুক্তি যেমন আমাদের জীবন সহজ করেছে, তেমনি সাইবার অপরাধের ঝুঁকিও বাড়িয়েছে।

নিচে ব্যবসা প্রতিষ্ঠান ও সমাজে সাইবার নিরাপত্তার গুরুত্ব আলাদাভাবে আলোচনা করা হলোঃ

ক. ব্যবসা প্রতিষ্ঠানে সাইবার নিরাপত্তার গুরুত্ব

১. গ্রাহকের তথ্যের সুরক্ষা ঃ ব্যাংক, ই-কমার্স বা যেকোনো সেবামূলক প্রতিষ্ঠানে গ্রাহকদের ব্যক্তিগত তথ্য (নাম, ঠিকানা, ক্রেডিট কার্ড নম্বর) জমা থাকে। সাইবার নিরাপত্তা নিশ্চিত না করলে হ্যাকাররা এই তথ্য চুরি করতে পারে, যা গ্রাহক এবং প্রতিষ্ঠান উভয়ের জন্যই বিপজ্জনক।

২. আর্থিক ক্ষতি রোধ ঃ র‍্যানসামওয়্যার (Ransomware) আক্রমণ বা আর্থিক জালিয়াতির মাধ্যমে হ্যাকাররা প্রতিষ্ঠানের কোটি কোটি টাকা হাতিয়ে নিতে পারে। সাইবার নিরাপত্তা ব্যবস্থা শক্তিশালী হলে এই বিপুল আর্থিক ক্ষতি থেকে বাঁচা সম্ভব।

৩. সুনাম ও আস্থা রক্ষা ঃ কোনো কোম্পানি হ্যাকিংয়ের শিকার হলে গ্রাহকদের কাছে তাদের বিশ্বাসযোগ্যতা নষ্ট হয়ে যায়। গ্রাহকরা মনে করেন তাদের তথ্য সেখানে নিরাপদ নয়। ব্যবসার সুনাম ধরে রাখতে সাইবার নিরাপত্তা অপরিহার্য।

৪. ব্যবসায়িক গোপনীয়তা রক্ষা ঃ প্রতিটি কোম্পানির নিজস্ব কিছু গোপন কৌশল, ভবিষ্যৎ পরিকল্পনা বা পণ্যের ডিজাইন থাকে (Intellectual Property)। হ্যাকাররা বা প্রতিদ্বন্দ্বী কোম্পানিরা যেন এই তথ্য চুরি করতে না পারে, তার জন্য কঠোর নিরাপত্তা প্রয়োজন।

৫. নিরবচ্ছিন্ন সেবা নিশ্চিত করা ঃ সাইবার আক্রমণ (যেমনঃ DDoS Attack) হলে প্রতিষ্ঠানের ওয়েবসাইট বা সার্ভার ডাউন হয়ে যেতে পারে, ফলে কাজকর্ম বন্ধ হয়ে যায়। সাইবার নিরাপত্তা নিশ্চিত করে যে ব্যবসা সবসময় সচল থাকবে।

খ. সমাজে সাইবার নিরাপত্তার গুরুত্ব ঃ

১. ব্যক্তিগত গোপনীয়তা রক্ষা ঃ সমাজের প্রতিটি মানুষ এখন স্মার্টফোন ও সোশ্যাল মিডিয়া ব্যবহার করে। সাইবার নিরাপত্তা না থাকলে মানুষের ব্যক্তিগত ছবি, চ্যাট বা লোকেশন হ্যাক হতে পারে, যা ব্ল্যাকমেইলিং বা সামাজিক হয়রানির কারণ হতে পারে।

২. অর্থনৈতিক নিরাপত্তা ঃ সাধারণ মানুষ এখন মোবাইল ব্যাংকিং (বিকাশ, নগদ) ও এটিএম ব্যবহার করে। সাইবার নিরাপত্তা ব্যবস্থা শক্তিশালী বলেই মানুষ নিশ্চিন্তে ডিজিটাল লেনদেন করতে পারছে। এর অভাবে মানুষের কষ্টার্জিত টাকা চুরি হওয়ার ঝুঁকি থাকে।

৩. সাইবার বুলিং ও হয়রানি রোধ ঃ সমাজে নারী ও শিশুরা প্রায়ই সাইবার বুলিং বা অনলাইন হয়রানির শিকার হয়। সাইবার নিরাপত্তা আইন এবং সচেতনতা তাদের এই মানসিক নির্যাতন থেকে রক্ষা করতে সাহায্য করে।

৪. জাতীয় ও জরুরি পরিষেবা রক্ষা ঃ বিদ্যুৎ কেন্দ্র, পানি সরবরাহ ব্যবস্থা, ট্রাফিক কন্ট্রোল এবং হাসপাতালের মতো জরুরি সেবাগুলো এখন নেটওয়ার্কের মাধ্যমে নিয়ন্ত্রিত হয়। সাইবার হামলা হলে পুরো সমাজ ব্যবস্থায় বিপর্যয় নেমে আসতে পারে। (যেমনঃ বিদ্যুৎ গ্রিড হ্যাক হলে পুরো দেশ অন্ধকারে ডুবে যাবে)।

৫. গুজব ও ভুয়া তথ্য প্রতিরোধ ঃ সামাজিক যোগাযোগ মাধ্যমে ভুয়া তথ্য ছড়িয়ে দাঙ্গা বা অস্থিরতা সৃষ্টি করা এখন সহজ। সাইবার নিরাপত্তা ব্যবস্থা এবং মনিটরিং-এর মাধ্যমে এই গুজব বা প্রোপাগান্ডা রোধ করে সামাজিক শান্তি বজায় রাখা সম্ভব।

***** ২। সাইবার নিরাপত্তার হুমকিসমূহ বর্ণনা কর।** বাকাশিবো- ২০১৯, ২০

উত্তর ঃ সাইবার নিরাপত্তার হুমকিসমূহকে (Cyber Security Threats) প্রধানত কয়েকটি ভাগে ভাগ করা যায়। হ্যাকাররা বা সাইবার অপরাধীরা বিভিন্ন কৌশলে সিস্টেমের ক্ষতি করার চেষ্টা করে।

নিচে প্রধান সাইবার হুমকিসমূহ আলোচনা করা হলো ঃ

১. ম্যালওয়্যার (Malware) ঃ ম্যালওয়্যার হলো "Malicious Software"-এর সংক্ষিপ্ত রূপ। এটি এমন সব সফটওয়্যার বা প্রোগ্রাম যা কম্পিউটারের ক্ষতি করে। এর মধ্যে রয়েছে ঃ

i) ভাইরাস (Virus) ঃ যা অন্য ফাইলের সাথে যুক্ত হয়ে ছড়ায়।

ii) ওয়ার্ম (Worm) ঃ এটি ভাইরাসের মতোই, তবে ছড়ানোর জন্য কোনো হোস্ট ফাইলের দরকার হয় না; এটি নেটওয়ার্কের মাধ্যমে একা একাই ছড়িয়ে পড়ে।

iii) ট্রোজান হর্স (Trojan Horse) ঃ ভালো সফটওয়্যারের ছদ্মবেশে থাকা ক্ষতিকারক প্রোগ্রাম।

iv) র‍্যানসামওয়্যার (Ransomware) ঃ এটি কম্পিউটারের ফাইল এনক্রিপ্ট বা লক করে দেয় এবং আনলক করার জন্য মুক্তিপণ (টাকা) দাবি করে।

v) স্পাইওয়্যার (Spyware) ঃ এটি গোপনে ব্যবহারকারীর ওপর নজরদারি করে এবং তথ্য চুরি করে।

২. সোশ্যাল ইঞ্জিনিয়ারিং (Social Engineering) ঃ এটি প্রযুক্তির চেয়ে মানুষের মনস্তাত্ত্বিক দুর্বলতাকে কাজে লাগিয়ে করা হয়।

i) ফিশিং (Phishing) ঃ বিশ্বাসযোগ্য প্রতিষ্ঠান (যেমন ব্যাংক বা গুগল)-এর নাম করে ভুয়া ইমেইল বা মেসেজ পাঠিয়ে পাসওয়ার্ড চুরি করা।

**** ৩। সাইবার নিরাপত্তার আইন ও বিধির গুরুত্ব আলোচনা কর।**

বাকাশিবো- ২০২৫

উত্তর ঃ আধুনিক বিশ্বে ইন্টারনেটের প্রসার যেমন বেড়েছে, তেমনি সাইবার অপরাধও পাল্লা দিয়ে বেড়েছে। এই অপরাধ নিয়ন্ত্রণ এবং ডিজিটাল জগতকে নিরাপদ রাখার জন্য সাইবার নিরাপত্তা আইন ও বিধি (Cyber Security Laws and Regulations) অত্যন্ত গুরুত্বপূর্ণ।

নিচে সাইবার আইনের গুরুত্ব আলোচনা করা হলো ঃ

১. অপরাধ দমন ও নিয়ন্ত্রণ ঃ বাস্তব জীবনে চুরি বা ডাকাতি করলে যেমন শাস্তির বিধান আছে, ডিজিটাল জগতেও অপরাধের জন্য শাস্তির ব্যবস্থা থাকা জরুরি। সাইবার আইন অপরাধীদের মনে ভীতি সৃষ্টি করে। যখন হ্যাকাররা জানে যে হ্যাকিং বা তথ্য চুরির জন্য জেল বা বড় অঙ্কের জরিমানা হতে পারে, তখন অপরাধের প্রবণতা কমে আসে।

২. ব্যক্তিগত তথ্যের সুরক্ষা ঃ মানুষের ব্যক্তিগত তথ্য, ছবি বা চ্যাট যেন কেউ অপব্যবহার করতে না পারে, তা নিশ্চিত করা আইনের কাজ। ফেসবুক, গুগল বা ব্যাংকের মতো প্রতিষ্ঠানগুলো কীভাবে আমাদের তথ্য ব্যবহার করবে, তার একটি আইনি সীমারেখা বা গাইডলাইন এই আইনের মাধ্যমে ঠিক করে দেওয়া হয়।

৩. ভুক্তভোগীর আইনি প্রতিকার ঃ কেউ যদি সাইবার বুলিং, হ্যাকিং বা অনলাইন প্রতারণার শিকার হয়, তবে সে কার কাছে বিচার চাইবে? সাইবার আইন ভুক্তভোগীকে পুলিশ বা আদালতের মাধ্যমে বিচার পাওয়ার অধিকার ও পথ দেখায়।

৪. ডিজিটাল অর্থনীতি ও ই-কমার্সের বিকাশ ঃ অনলাইন কেনাকাটা বা মোবাইল ব্যাংকিংয়ের ক্ষেত্রে গ্রাহকের আস্থা বা বিশ্বাস সবচেয়ে জরুরি। যদি কোনো আইনি কাঠামো না থাকে, তবে মানুষ অনলাইনে টাকা লেনদেন করতে ভয় পাবে। সাইবার আইন ডিজিটাল লেনদেনের নিরাপত্তা নিশ্চিত করে দেশের অর্থনীতিকে সচল রাখে।

৫. জাতীয় নিরাপত্তা রক্ষা ঃ সাইবার সন্ত্রাসীরা দেশের বিদ্যুৎ কেন্দ্র, ব্যাংক বা সরকারি সার্ভারে হামলা চালিয়ে অচল করে দিতে পারে। রাষ্ট্রবিরোধী

গুজব বা প্রোপাগান্ডা ছড়াতে পারে। এসব কর্মকাণ্ডকে দেশদ্রোহী অপরাধ হিসেবে গণ্য করে কঠোর ব্যবস্থা নেওয়ার জন্য সাইবার আইন অপরিহার্য।

৬. মেধা সম্পত্তির অধিকার রক্ষা ঃ কারো তৈরি করা সফটওয়্যার, গান, সিনেমা বা বই অনুমতি ছাড়া ইন্টারনেটে ছড়িয়ে দেওয়া (পাইরেসি) রোধ করতে এই আইন গুরুত্বপূর্ণ ভূমিকা পালন করে।

বাংলাদেশের প্রেক্ষাপট ঃ

বাংলাদেশে বর্তমানে 'সাইবার নিরাপত্তা আইন, 2023' (Cyber Security Act, 2023) বলবৎ রয়েছে (যা আগে ডিজিটাল নিরাপত্তা আইন ছিল)। এই আইনের আওতায় হ্যাকিং, ভুয়া তথ্য ছড়ানো, এবং অনলাইন প্রতারণার জন্য বিভিন্ন মেয়াদে কারাদণ্ড ও অর্থদণ্ডের বিধান রয়েছে।

***** ৪। সাইবার নিরাপত্তা ও তথ্য নিরাপত্তার মধ্যে পার্থক্য লেখ।**

বাকাশিবো- ২০২১, ২২

উত্তর ঃ সাইবার নিরাপত্তা (Cyber Security) এবং তথ্য নিরাপত্তা (Information Security বা InfoSec) শব্দ দুটি অনেক সময় একই অর্থে ব্যবহৃত হলেও এদের মধ্যে সূক্ষ্ম ও মৌলিক কিছু পার্থক্য রয়েছে।

বিষয়	সাইবার নিরাপত্তা	তথ্য নিরাপত্তা
১.মূল লক্ষ্য	মূলত অনলাইন বা ডিজিটাল মাধ্যমে থাকা ডেটাকে বাহ্যিক আক্রমণ (যেমন: হ্যাকিং) থেকে রক্ষা করা।	যেকোনো ধরনের তথ্য যেন ভুল হাতে না পড়ে বা নষ্ট না হয় তা নিশ্চিত করা।

২.পরিধি	এটি শুধুমাত্র ডিজিটাল বা সাইবার জগতের মধ্যে সীমাবদ্ধ।	এর পরিধি অনেক বড়; ডিজিটাল ডেটার পাশাপাশি কাগজের ফাইল বা হার্ডকপিও এর অন্তর্ভুক্ত।
৩. সুরক্ষার ধরন	নেটওয়ার্ক, ডিভাইস এবং সফটওয়্যারকে সাইবার ক্রাইম থেকে রক্ষা করে।	তথ্যের গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা নিশ্চিত করে।
৪.উদাহরণ	ফায়ারওয়াল ব্যবহার, ম্যালওয়্যার প্রতিরোধ বা ফিশিং লিংকে ক্লিক করা থেকে বিরত থাকা।	আলমারিতে গুরুত্বপূর্ণ ফাইল তালাবদ্ধ করে রাখা, পাসওয়ার্ড নীতি মেনে চলা বা ডেটা এনক্রিপশন।