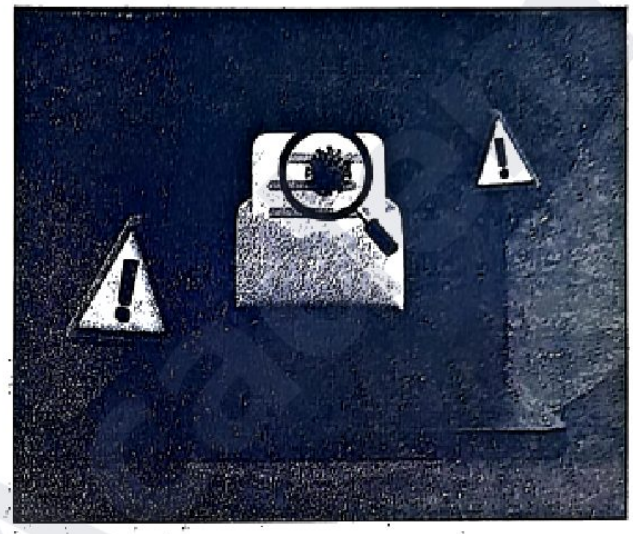
Visit Our Website: all.talukdaracademy.com.bd

ইউনিট-৬

প্রাইভেসি অ্যান্ড সিকিউরিটি

Privacy and Security





Specific Objectives	Content	Teaching and Learning Approach
The student will be able to: • Understand the basics of digital security • Use some security tools. • Understanding digital ethics.	• Introduction to Information Security, cybercrime, DoS and DDoS Attack, Key Management, Digital • Signature and • Certifications, privacy, • Data Security, • Vulnerability, Threat and Risk, Malware, Social Engineering, Hacking, Plagiarism, Fishing, Software Piracy, Worms and Viruses, Spam, Adware, Malware, Spyware, Antivirus • Software • Ethics in the digital world	Classroom Lectures, Lab and Hands-on Practice

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১ তথ্য নিরাপত্তার পরিচিতি (Introduction to Information Security)

তথ্য নিরাপত্তা হলো এমন একটি প্রক্রিয়া বা ব্যবস্থা যার মাধ্যমে তথ্যকে সংরক্ষণ, প্রক্রিয়াকরণ বা আদান-প্রদানের সময় অননুমোদিত প্রবেশ, ব্যবহার, প্রকাশ, পরিবর্তন বা ধ্বংস থেকে রক্ষা করা হয়। এর মূল উদ্দেশ্য হলো তথ্যের গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা নিশ্চিত করা।

৬.১.১ তথ্য নিরাপত্তার মূল লক্ষ্য (CIA ট্রায়াড)

গোপনীয়তা (Confidentiality) – শুধুমাত্র অনুমোদিত ব্যক্তিরা যেন তথ্য ব্যবহার বা দেখতে পারে তা নিশ্চিত করা।

অখণ্ডতা (Integrity) – তথ্য সঠিক, সম্পূর্ণ ও বিশ্বাসযোগ্য রাখা।

প্রাপ্যতা (Availability) – অনুমোদিত ব্যবহারকারীরা প্রয়োজনের সময় যেন তথ্য ও সিস্টেমে প্রবেশ করতে পারে তা নিশ্চিত করা।

৬.১.২ তথ্য নিরাপত্তার গুরুত্ব

তথ্য নিরাপত্তা ব্যক্তি, প্রতিষ্ঠান এবং দেশের জন্য অত্যন্ত গুরুত্বপূর্ণ। এর মাধ্যমে তথ্য চুরি, অপব্যবহার বা ধ্বংস থেকে সুরক্ষিত রাখা হয়। বর্তমান ডিজিটাল যুগে প্রতিদিন অসংখ্য তথ্য তৈরি, সংরক্ষণ ও আদান-প্রদান হচ্ছে, যা সঠিকভাবে সুরক্ষিত না থাকলে বড় ধরনের ক্ষতি হতে পারে।

১. ব্যক্তিগত তথ্য সুরক্ষা
ব্যবহারকারীর নাম, পাসওয়ার্ড, ঠিকানা, জাতীয় পরিচয়পত্র নম্বর, ব্যাংক তথ্য ইত্যাদি সাইবার অপরাধীদের হাত থেকে রক্ষা করে। ব্যক্তিগত গোপনীয়তা (Privacy) বজায় রাখে।

২. আর্থিক ক্ষতি প্রতিরোধ
তথ্য চুরি বা হ্যাকিংয়ের মাধ্যমে ব্যাংক অ্যাকাউন্ট খালি হয়ে যাওয়া, ক্রেডিট কার্ড তথ্য ফাঁস হওয়া ইত্যাদি প্রতিরোধ করে। প্রতিষ্ঠানকে ব্যবসায়িক ক্ষতির হাত থেকে রক্ষা করে।

৩. প্রতিষ্ঠানের সুনাম রক্ষা
ডেটা ফাঁস হলে গ্রাহক ও অংশীদারের আস্থা নষ্ট হয়।
সঠিক তথ্য নিরাপত্তা ব্যবস্থা থাকলে প্রতিষ্ঠানের বিশ্বাসযোগ্যতা বাড়ে।

৪. আইন ও নীতিমালা মেনে চলা
অনেক দেশেই ডেটা সুরক্ষা আইন আছে, যেমন– GDPR, যা তথ্য সুরক্ষাকে বাধ্যতামূলক করেছে।
আইন ভঙ্গ করলে জরিমানা বা শাস্তি হতে পারে।

৫. জাতীয় নিরাপত্তা নিশ্চিত করা
সরকারি গোপন নথি, সামরিক পরিকল্পনা বা গুরুত্বপূর্ণ অবকাঠামোর তথ্য সুরক্ষিত রাখা।
সাইবার হামলা থেকে দেশকে রক্ষা করা।

৬.১.৩ তথ্য নিরাপত্তার সাধারণ হুমকি

তথ্য নিরাপত্তা নানান ধরনের ঝুঁকির সম্মুখীন হয়, যা ব্যক্তিগত, প্রাতিষ্ঠানিক এবং জাতীয় পর্যায়ে ক্ষতির কারণ হতে পারে। এ হুমকিগুলো মূলত সাইবার আক্রমণ, প্রযুক্তিগত সমস্যা এবং মানবিক ত্রুটি থেকে আসে।

১. ম্যালওয়্যার (Malware)
ক্ষতিকর সফটওয়্যার যা কম্পিউটার বা নেটওয়ার্কে ঢুকে তথ্য নষ্ট, চুরি বা লক করে দেয়।
উদাহরণ: ভাইরাস, ওয়ার্ম, ট্রোজান, র‍্যানসমওয়্যার ইত্যাদি।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

২. ফিশিং (Phishing) আক্রমণ
প্রতারণামূলক ইমেইল, মেসেজ বা ওয়েবসাইট ব্যবহার করে ব্যবহারকারীর ব্যক্তিগত তথ্য হাতিয়ে নেয়া।
যেমন: ভুয়া ব্যাংক লগইন পেজে পাসওয়ার্ড প্রবেশ করানো।

৩. অননুমোদিত প্রবেশ (Unauthorized Access)
হ্যাকার বা ভেতরের কর্মচারীর অনুমতি ছাড়া সিস্টেমে প্রবেশ করে তথ্য দেখা বা পরিবর্তন করা।

৪. সোশ্যাল ইঞ্জিনিয়ারিং (Social Engineering)
মানুষের মনস্তাত্ত্বিক দুর্বলতা কাজে লাগিয়ে তথ্য বের করে নেয়া।
উদাহরণ: কাস্টমার কেয়ার সেজে পাসওয়ার্ড চাওয়া।

৫. ডেটা লস (Data Loss)
দুর্ঘটনাজনিত মুছে ফেলা, হার্ডড্রাইভ নষ্ট হওয়া বা প্রাকৃতিক দুর্যোগে ডেটা হারিয়ে যাওয়া।

৬. ডিনায়েল অব সার্ভিস (DoS/DDoS) আক্রমণ
সার্ভারে অতিরিক্ত ট্রাফিক পাঠিয়ে সেটিকে অকেজো করে দেয়া, ফলে বৈধ ব্যবহারকারীরা সেবা পায় না।

৭. ম্যান-ইন-দ্য-মিডল (MITM) আক্রমণ
দুই পক্ষের মধ্যে যোগাযোগে হস্তক্ষেপ করে ডেটা চুরি বা পরিবর্তন করা।

৬.১.৪ তথ্য নিরাপত্তা নিশ্চিত করার উপায়

তথ্যকে অননুমোদিত প্রবেশ, চুরি, বা ধ্বংস থেকে সুরক্ষিত রাখতে কিছু প্রযুক্তিগত, প্রশাসনিক এবং সচেতনতামূলক পদক্ষেপ নেয়া জরুরি।

১. শক্তিশালী পাসওয়ার্ড ও প্রমাণীকরণ (Authentication) ব্যবহার
বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন মিলিয়ে পাসওয়ার্ড তৈরি করা।
দুই ধাপের প্রমাণীকরণ (Two-Factor Authentication) সক্রিয় করা।

২. তথ্য এনক্রিপশন (Encryption)
ডেটা সংরক্ষণ ও আদান-প্রদানের সময় এনক্রিপ্ট করে রাখা, যাতে হ্যাকার পেলেও তা পড়তে না পারে।

৩. নিয়মিত সফটওয়্যার আপডেট
অপারেটিং সিস্টেম, অ্যাপ ও অ্যান্টিভাইরাস নিয়মিত আপডেট করা, যাতে নতুন নিরাপত্তা প্যাঁচ যুক্ত হয়।

৪. নেটওয়ার্ক নিরাপত্তা ব্যবস্থা
ফায়ারওয়াল (Firewall) ব্যবহার করে অননুমোদিত প্রবেশ ঠেকানো।
ইনট্রুশন ডিটেকশন সিস্টেম (IDS) দিয়ে সন্দেহজনক কার্যকলাপ নজরে রাখা।

৫. ব্যাকআপ রাখা
গুরুত্বপূর্ণ তথ্যের নিয়মিত ব্যাকআপ রাখা এবং নিরাপদ স্থানে সংরক্ষণ করা।
ক্লাউড ব্যাকআপ বা অফলাইন স্টোরেজ ব্যবহার করা।

৬. কর্মীদের সাইবার সচেতনতা প্রশিক্ষণ
ফিশিং ইমেইল চেনা, সন্দেহজনক লিঙ্কে ক্লিক না করা এবং নিরাপত্তা নীতি মেনে চলা শেখানো।

৭. অ্যাক্সেস কন্ট্রোল (Access Control)
প্রয়োজন অনুযায়ী অনুমতি দেয়া এবং অপ্রয়োজনীয় অ্যাক্সেস বন্ধ করা।

৮. সিকিউর ওয়েব ব্রাউজিং
নিরাপদ (HTTPS) ওয়েবসাইট ব্যবহার করা।
পাবলিক ওয়াইফাইতে ভিপিএন (VPN) ব্যবহার করা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.২ সাইবার অপরাধ (Cybercrime)

সাইবার অপরাধ হলো এমন অপরাধ যা কম্পিউটার, ইন্টারনেট, নেটওয়ার্ক বা ডিজিটাল ডিভাইস ব্যবহার করে সংঘটিত হয়। এর মাধ্যমে ব্যক্তিগত, প্রাতিষ্ঠানিক বা সরকারি তথ্য চুরি, ধ্বংস বা অপব্যবহার করা হয়।
সাইবার অপরাধ প্রযুক্তি-নির্ভর অপরাধ হওয়ায় এটি খুব দ্রুত ছড়িয়ে পড়তে পারে এবং অপরাধীকে শনাক্ত করা অনেক সময় কঠিন হয়ে যায়।

৬.২.১ সাইবার অপরাধের ধরন

১. **হ্যাকিং (Hacking)**
অনুমতি ছাড়া কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা ডেটায় প্রবেশ করা।
উদ্দেশ্য হতে পারে তথ্য চুরি, পরিবর্তন বা ধ্বংস করা।

২. **ফিশিং (Phishing)**
ভুয়া ইমেইল, মেসেজ বা ওয়েবসাইট ব্যবহার করে ব্যবহারকারীর পাসওয়ার্ড, ব্যাংক তথ্য ইত্যাদি হাতিয়ে নেয়া।

৩. **ম্যালওয়্যার আক্রমণ (Malware Attack)**
ভাইরাস, ওয়ার্ম, ট্রোজান, র‍্যানসমওয়্যার ইত্যাদি ক্ষতিকর সফটওয়্যার ইনস্টল করে তথ্য নষ্ট বা চুরি করা।

৪. **আইডেন্টিটি থেফট (Identity Theft)**
কারও ব্যক্তিগত তথ্য (নাম, জন্মতারিখ, জাতীয় পরিচয়পত্র নম্বর, ব্যাংক তথ্য) চুরি করে প্রতারণা করা।

৫. **ডিনায়েল অব সার্ভিস আক্রমণ (DoS/DDoS)**
সার্ভার বা ওয়েবসাইটে এত বেশি অনুরোধ পাঠানো হয় যে সেটি স্বাভাবিকভাবে কাজ করতে পারে না।

৬. **সাইবার বুলিং (Cyberbullying)**
অনলাইনে হুমকি দেয়া, গুজব ছড়ানো, অপমান করা বা হয়রানি করা।

৭. **অনলাইন প্রতারণা (Online Fraud)**
ভুয়া ই-কমার্স ওয়েবসাইট, লটারি প্রতারণা, বিনিয়োগে প্রলুব্ধ করা ইত্যাদি।

৮. **ম্যান-ইন-দ্য-মিডল আক্রমণ (Man-in-the-Middle Attack)**
দুই পক্ষের মধ্যে যোগাযোগে হস্তক্ষেপ করে তথ্য চুরি বা পরিবর্তন করা।

৯. **স্পুফিং (Spoofing)**
ভুয়া ইমেইল ঠিকানা, ওয়েবসাইট বা আইপি অ্যাড্রেস ব্যবহার করে প্রতারণা করা।

৬.২.২ সাইবার অপরাধের প্রভাব

সাইবার অপরাধ ব্যক্তি, প্রতিষ্ঠান এমনকি একটি দেশের জন্যও মারাত্মক ক্ষতির কারণ হতে পারে। এর প্রভাব শুধু আর্থিক ক্ষতিতে সীমাবদ্ধ নয়, বরং সামাজিক, মানসিক এবং জাতীয় নিরাপত্তার ক্ষেত্রেও বড় ধরনের হুমকি তৈরি করে।

১. **ব্যক্তিগত প্রভাব**
- ব্যক্তিগত তথ্য (পাসওয়ার্ড, ব্যাংক তথ্য, জাতীয় পরিচয়পত্র নম্বর) ফাঁস হয়ে যাওয়া।
- সামাজিক যোগাযোগ মাধ্যমে মানহানি, হয়রানি বা সাইবার বুলিংয়ের শিকার হওয়া।
- মানসিক চাপ ও নিরাপত্তাহীনতা বৃদ্ধি।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

২. আর্থিক প্রভাব

- ব্যাংক অ্যাকাউন্ট বা ক্রেডিট কার্ড থেকে টাকা চুরি।
- ব্যবসা প্রতিষ্ঠান থেকে গোপন তথ্য চুরি করে প্রতিযোগী প্রতিষ্ঠানের কাছে বিক্রি।
- অনলাইন প্রতারণায় অর্থ হারানো।

৩. প্রাতিষ্ঠানিক প্রভাব

- প্রতিষ্ঠানের গুরুত্বপূর্ণ ডেটা চুরি বা ধ্বংস হয়ে যাওয়া।
- গ্রাহকের আস্থা ও প্রতিষ্ঠানের সুনাম ক্ষতিগ্রস্ত হওয়া।
- আইনি জরিমানা ও ক্ষতিপূরণ দিতে বাধ্য হওয়া।

৪. জাতীয় প্রভাব

- সরকারি গোপন নথি বা সামরিক পরিকল্পনা ফাঁস হয়ে যাওয়া।
- গুরুত্বপূর্ণ অবকাঠামো (বিদ্যুৎ, পানি সরবরাহ, পরিবহন) সাইবার আক্রমণে অচল হয়ে যাওয়া।
- জাতীয় নিরাপত্তা হুমকির মুখে পড়া।

৬.২.৩ সাইবার অপরাধ প্রতিরোধের উপায়

সাইবার অপরাধ রোধে প্রযুক্তিগত নিরাপত্তা, সচেতনতা এবং আইনগত পদক্ষেপ একসাথে কার্যকর ভূমিকা রাখতে পারে।

১. শক্তিশালী পাসওয়ার্ড ব্যবহার
বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন মিশিয়ে জটিল পাসওয়ার্ড তৈরি করো।
নিয়মিত পাসওয়ার্ড পরিবর্তন করো।

২. দুই ধাপের প্রমাণীকরণ (Two-Factor Authentication) সক্রিয় করা
লগইনের সময় পাসওয়ার্ডের পাশাপাশি একবার ব্যবহারযোগ্য কোড বা বায়োমেট্রিক যাচাই ব্যবহার করতে হবে।

৩. অ্যান্টিভাইরাস ও ফায়ারওয়াল ব্যবহার
ক্ষতিকারক সফটওয়্যার শনাক্ত ও প্রতিরোধের জন্য আপডেটেড অ্যান্টিভাইরাস ব্যবহার করতে হবে।
ফায়ারওয়াল দিয়ে অননুমোদিত নেটওয়ার্ক অ্যাক্সেস বন্ধ করতে হবে।

৪. সন্দেহজনক ইমেইল ও লিঙ্ক এড়িয়ে চলা
অপরিচিত বা সন্দেহজনক উৎস থেকে আসা ইমেইল, লিঙ্ক বা অ্যাটাচমেন্ট কখনও খোলা যাবে না।

৫. নিয়মিত সফটওয়্যার আপডেট করা
অপারেটিং সিস্টেম, ব্রাউজার ও অ্যাপগুলোর নিরাপত্তা প্যাচ আপডেট করতে হবে।

৬. ডেটার ব্যাকআপ রাখা
গুরুত্বপূর্ণ তথ্যের নিয়মিত ব্যাকআপ নিন এবং নিরাপদ স্থানে সংরক্ষণ করতে হবে।

৭. সাইবার সচেতনতা বৃদ্ধি
কর্মী ও ব্যবহারকারীদের সাইবার নিরাপত্তা প্রশিক্ষণ দিতে হবে।
শিশু ও কিশোরদের নিরাপদ ইন্টারনেট ব্যবহারের অভ্যাস শেখাতে হবে।

৮. আইনগত পদক্ষেপ
সাইবার অপরাধ ঘটলে দ্রুত আইন প্রয়োগকারী সংস্থায় অভিযোগ জানাতে হবে।
জাতীয় সাইবার হেল্পলাইন ও সরকারি সাইবার নিরাপত্তা সেবা ব্যবহার করতে হবে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৩ DoS এবং DDoS Attack
(ডিনায়াল অফ সার্ভিস এবং ডিস্ট্রিবিউটেড ডিনায়াল অফ সার্ভিস আক্রমণ)

DoS এবং DDoS Attack (ডিনায়াল অফ সার্ভিস এবং ডিস্ট্রিবিউটেড ডিনায়াল অফ সার্ভিস আক্রমণ) হলো এক ধরনের সাইবার আক্রমণ যেখানে কোনো সার্ভার, নেটওয়ার্ক বা ওয়েবসাইটকে অপ্রাপ্য বা ধীর করে দেয়া হয়।

১. **DoS Attack (Denial of Service Attack)**
কী: একক কম্পিউটার বা নেটওয়ার্ক ব্যবহার করে লক্ষ্যবস্তু সার্ভার বা সিস্টেমকে অতিরিক্ত অনুরোধ পাঠিয়ে অকার্যকর করা।
উদাহরণ: একটি ওয়েবসাইটে অনেকবার একসাথে রিকোয়েস্ট পাঠানো যাতে সার্ভার ক্র্যাশ বা ধীর হয়ে যায়।

২. **DDoS Attack (Distributed Denial of Service Attack)**
কী: একাধিক কম্পিউটার বা নেটওয়ার্ক (বটনেট ব্যবহার করে) ব্যবহার করে একই সময়ে লক্ষ্যবস্তু সার্ভার বা সিস্টেমে আক্রমণ করা।
উদাহরণ: হাজার হাজার কম্পিউটার থেকে একই ওয়েবসাইটে অনুরোধ পাঠানো, ফলে সার্ভার সম্পূর্ণভাবে অপ্রাপ্য হয়ে যায়।

৬.৩.১ DoS ও DDoS Attack-এর বৈশিষ্ট্য

১. **লক্ষ্যবস্তু অকার্যকর করা (Target Disruption)**
সার্ভার, নেটওয়ার্ক বা ওয়েবসাইটকে ব্যবহারকারীর জন্য অপ্রাপ্য বা ধীর করে দেয়।

২. **উচ্চ ট্রাফিক (High Traffic Volume)**
প্রচুর অনুরোধ বা ডেটা পাঠিয়ে সার্ভারের ক্ষমতা অতিক্রম করা।

৩. **ব্যবহারকারীরা সার্ভিস ব্যবহার করতে অক্ষম (Service Unavailability)**
ব্যবহারকারীরা লক্ষ্যবস্তু সার্ভিসে প্রবেশ করতে বা ব্যবহার করতে পারে না।

৪. **সিস্টেম ক্র্যাশ বা ধীরগতি (System Crash or Slowdown)**
বড় আক্রমণে সার্ভার ক্র্যাশ হতে পারে বা অতি ধীর হয়ে যায়।

৫. **আক্রমণকারীর পরিচয় গোপন থাকে (Attacker Concealment)**
বিশেষ করে DDoS-এ, হাজার হাজার কম্পিউটারের মাধ্যমে আক্রমণ হওয়ায় মূল উৎস শনাক্ত করা কঠিন।

৬. **নিয়ন্ত্রণ ও প্রতিরোধ কঠিন (Difficult to Control & Mitigate)**
একাধিক উৎস থেকে একসাথে আক্রমণ হওয়ায় প্রতিরোধে জটিলতা সৃষ্টি হয়।

৬.৩.২ DoS ও DDoS Attack প্রতিরোধের উপায়

DoS ও DDoS Attack প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে সার্ভার, নেটওয়ার্ক বা ওয়েবসাইটকে এ ধরনের আক্রমণ থেকে সুরক্ষিত রাখা যায়।

১. **ফায়ারওয়াল ও ইন্ট্রুশন প্রিভেনশন সিস্টেম (IPS) ব্যবহার**
অস্বাভাবিক বা অননুমোদিত ট্রাফিক ব্লক করে।

২. **নেটওয়ার্ক ট্রাফিক মনিটরিং**
- নিয়মিত ট্রাফিক পর্যবেক্ষণ করে অস্বাভাবিক প্যাটার্ন শনাক্ত করা।
- প্রাথমিক সতর্কতা বা অ্যালার্ম সিস্টেম ব্যবহার করা।

৩. **ব্যান্ডউইথ বৃদ্ধি ও লোড ব্যালান্সার ব্যবহার**
- অতিরিক্ত ট্রাফিক সামলাতে পর্যাপ্ত ব্যান্ডউইথ রাখা।
- লোড ব্যালান্সার ব্যবহার করে সার্ভারগুলোতে ট্রাফিক সমানভাবে বিতরণ করা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৪. DDoS প্রোটেকশন সার্ভিস ব্যবহার

- ক্লাউডভিত্তিক সেবা যেমন Cloudflare, Akamai ইত্যাদি ব্যবহার।
- বড় আক্রমণও পরিচালনা করতে সক্ষম।

৫. ব্যাকআপ ও রিকভারি পরিকল্পনা

- নিয়মিত ডেটার ব্যাকআপ রাখা।
- আক্রমণের পর দ্রুত সার্ভিস পুনরুদ্ধারের ব্যবস্থা।

৬. নিয়মিত সিস্টেম আপডেট ও প্যাচিং

নিরাপত্তার দুর্বলতা দূর করতে অপারেটিং সিস্টেম, সফটওয়্যার ও নেটওয়ার্ক ডিভাইস আপডেট রাখা।

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. নিচের কোনটি তথ্য নিরাপত্তার অংশ নয়?

ক. গোপনীয়তা　　খ. অখণ্ডতা
গ. ডিজাইন　　ঘ. প্রাপ্যতা

২. ডেটা সুরক্ষা আইন উদাহরণ হিসেবে নিচের কোনটি প্রযোজ্য?

ক. HTML　　খ. EU GDPR
গ. HTTP　　ঘ. SQL

৩. নিচের কোনটি একটি ম্যালওয়্যারের উদাহরণ?

ক. ফায়ারওয়াল　　খ. ট্রোজান
গ. ব্রাউজার　　ঘ. সার্ভার

৪. ফিশিং আক্রমণের মাধ্যমে সাধারণত কী চুরি হয়?

ক. সফটওয়্যার　　খ. হার্ডওয়্যার
গ. ব্যক্তিগত তথ্য　　ঘ. প্রিন্টার

৫. ডেটা লসের একটি কারণ কী হতে পারে?

ক. দ্রুত ইন্টারনেট　　খ. ব্যাকআপ রাখা
গ. প্রাকৃতিক দুর্যোগ　　ঘ. নতুন সফটওয়্যার

৬. এনক্রিপশন কেন ব্যবহার করা হয়?

ক. ছবি সাজানোর জন্য　　খ. হ্যাকার যেন তথ্য না পড়তে পারে
গ. ডেটা দ্রুত পাঠানোর জন্য　　ঘ. ফন্ট পরিবর্তনের জন্য

৭. কোনটি একটি সাইবার অপরাধ?

ক. টাইপিং　　খ. ফাইল কপি
গ. হ্যাকিং　　ঘ. পাসওয়ার্ড লেখা

৮. সাইবার অপরাধ রোধে শিশুদের কী শেখানো উচিত?

ক. নতুন অ্যাপ ডাউনলোড　　খ. খেলাধুলা
গ. নিরাপদ ইন্টারনেট ব্যবহার　　ঘ. ফাইল ডিলিট

উত্তরমালা : ১. গ; ২. খ; ৩. খ; ৪. গ; ৫. গ; ৬. খ; ৭. গ; ৮. গ।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. তথ্য নিরাপত্তার মূল উদ্দেশ্য হলো তথ্যের ....., অখণ্ডতা এবং প্রাপ্যতা নিশ্চিত করা।
উত্তর : গোপনীয়তা

২. ম্যালওয়্যার হলো এমন ক্ষতিকর ..... যা কম্পিউটার বা নেটওয়ার্কে ঢুকে তথ্য নষ্ট বা চুরি করে।
উত্তর : সফটওয়্যার

৩. অনুমোদিত ব্যবহারকারীরা প্রয়োজনের সময় যেন তথ্য ও সিস্টেমে প্রবেশ করতে পারে, এটিই তথ্য নিরাপত্তার ..... দিক। **উত্তর :** প্রাপ্যতা

৪. ফিশিং আক্রমণে প্রতারণামূলক ....., মেসেজ বা ওয়েবসাইট ব্যবহার করা হয়।
উত্তর : ইমেইল

৫. শক্তিশালী পাসওয়ার্ড তৈরি করতে বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও ..... চিহ্ন ব্যবহার করতে হয়। **উত্তর :** বিশেষ

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. শক্তিশালী পাসওয়ার্ড	ক. ডেটা এনক্রিপ্ট করে রাখা
২. এনক্রিপশন	খ. বড়/ ছোট হাতের অক্ষর, সংখ্যা, চিহ্ন ব্যবহার
৩. সফটওয়্যার আপডেট	গ. কর্মীদের ফিশিং চেনা শেখানো
৪. ব্যাকআপ	ঘ. গুরুত্বপূর্ণ তথ্যের কপি রাখা
৫. সচেতনতা প্রশিক্ষণ	ঙ. নতুন নিরাপত্তা প্যাচ যুক্ত করা

উত্তরমালা : ১→ক, ২→ক, ৩→ঙ, ৪→ঘ, ৫→গ

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. সাইবার অপরাধ কী
২. তথ্য নিরাপত্তা কী?
৩. ম্যালওয়্যার কী?
৪. হ্যাকিং কী?
৫. ফিশিং কী?
৬. সাইবার বুলিং কী?
৭. স্পুফিং কী?

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. তথ্য নিরাপত্তার তিনটি মূল লক্ষ্য কী?
২. গোপনীয়তা (Confidentiality) এর অর্থ কী?
৩. অখণ্ডতা (Integrity) এর অর্থ কী?
৪. প্রাপ্যতা (Availability) এর অর্থ কী?

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৫. ম্যালওয়্যার কী এবং এর উদাহরণ দাও।
৬. ফিশিং আক্রমণ কীভাবে কাজ করে?
৭. অননুমোদিত প্রবেশ (Unauthorized Access) কী?
৮. সোশ্যাল ইঞ্জিনিয়ারিং কী?
৯. DoS ও DDoS আক্রমণের মধ্যে পার্থক্য কী?
১০. শক্তিশালী পাসওয়ার্ডের বৈশিষ্ট্য কী কী?
১১. সাইবার অপরাধের কয়েকটি উদাহরণ লেখো।

চ. দৃশ্যকল্প-ভিত্তিক প্রশ্ন :

১. রুবি একটি অনলাইন শপ থেকে কেনাকাটা করলো। কয়েকদিন পর সে দেখে তার ব্যাংক অ্যাকাউন্ট থেকে টাকা কেটে গেছে। পরে জানা গেলো, ফিশিং ওয়েবসাইটে তার কার্ড তথ্য চুরি হয়েছে।

প্রশ্ন: এখানে কোন ধরনের সাইবার অপরাধ ঘটেছে? তথ্য নিরাপত্তার কোন লক্ষ্য (Confidentiality, Integrity, Availability) লঙ্ঘিত হয়েছে এবং কেন?

২. একটি বিশ্ববিদ্যালয়ের সার্ভারে হঠাৎ প্রচুর অনুরোধ আসতে থাকে। ফলে ওয়েবসাইটটি ধীর হয়ে যায় এবং শিক্ষার্থীরা ফলাফল দেখতে পারছে না। আইটি বিভাগ তদন্ত করে দেখে এটি DDoS আক্রমণ।

প্রশ্ন: এখানে কোন ধরনের আক্রমণ ঘটেছে? এ ধরনের আক্রমণ প্রতিরোধে কী কী ব্যবস্থা নেওয়া যেতে পারে?

৩. রাহিম একটি কোম্পানিতে কাজ করে। একদিন সে একটি ইমেইল পেল যেখানে লেখা ছিল, "আপনার অ্যাকাউন্ট বন্ধ হয়ে যাবে, লগইন করতে এখানে ক্লিক করুন।" রাহিম বুঝতে পারলো এটি ভুয়া ইমেইল এবং ক্লিক করেনি।

প্রশ্ন: রাহিম কোন ধরনের আক্রমণ থেকে নিজেকে রক্ষা করলো? সাইবার অপরাধ প্রতিরোধে সচেতনতার ভূমিকা এখানে কীভাবে কার্যকর হলো?

ছ. বর্ণনামূলক প্রশ্ন :

১. তথ্য নিরাপত্তার গুরুত্ব এবং তথ্য নিরাপত্তার সাধারণ হুমকি ব্যাখ্যা করো।
২. তথ্য নিরাপত্তা নিশ্চিত করার প্রযুক্তিগত ও প্রশাসনিক উপায়গুলো ব্যাখ্যা করো।
৩. ব্যক্তিগত তথ্য সুরক্ষার জন্য কি কি ব্যবস্থা গ্রহণ করা যায়?
৪. সাইবার অপরাধ কী এবং এর প্রভাব ব্যাখ্যা করো।
৫. হ্যাকিং এবং ফিশিং আক্রমণের মধ্যে পার্থক্য ব্যাখ্যা করো।
৬. ম্যালওয়্যার আক্রমণের প্রকারভেদ ও প্রতিরোধ ব্যাখ্যা করো।
৭. DoS ও DDoS আক্রমণের বৈশিষ্ট্য ও উদাহরণ ব্যাখ্যা করো।
৮. DoS ও DDoS আক্রমণ প্রতিরোধের জন্য কী কী ব্যবস্থা গ্রহণ করা যায়?
৯. সাইবার সচেতনতা বৃদ্ধির মাধ্যমে তথ্য নিরাপত্তা ও সাইবার অপরাধ প্রতিরোধে কিভাবে সাহায্য করা যায়?

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৪ Key Management (কী ম্যানেজমেন্ট)

Key Management (কী ম্যানেজমেন্ট) হলো একটি প্রক্রিয়া যা ক্রিপ্টোগ্রাফিতে ব্যবহৃত এনক্রিপশন এবং ডিক্রিপশন কীগুলো সুরক্ষিতভাবে তৈরি, বিতরণ, সংরক্ষণ, ব্যবহার এবং অবসান করার নিয়মাবলি নির্ধারণ করে। এটি তথ্য নিরাপত্তার জন্য অত্যন্ত গুরুত্বপূর্ণ।

৬.৪.১ Key Management (কী ম্যানেজমেন্ট)-এর বৈশিষ্ট্য

Key Management (কী ম্যানেজমেন্ট)-এর বৈশিষ্ট্য নিচে দেওয়া হলো–

১. **কী জেনারেশন (Key Generation)**
শক্তিশালী ও নিরাপদ ক্রিপ্টোগ্রাফিক কী তৈরি করা।

২. **কী বিতরণ (Key Distribution)**
বিশ্বাসযোগ্য ব্যবহারকারীর মধ্যে কী নিরাপদভাবে বিতরণ করা।

৩. **কী সংরক্ষণ (Key Storage)**
কী নিরাপদভাবে স্টোর করা, যাতে হ্যাকার বা অননুমোদিত ব্যবহারকারী অ্যাক্সেস করতে না পারে।

৪. **কী ব্যবহার (Key Usage)**
নির্ধারিত প্রোটোকল অনুযায়ী কী ব্যবহার করা।

৫. **কী অবসান ও পুনঃজেনারেশন (Key Expiry & Renewal)**
নির্দিষ্ট সময়ের পর কী অবসান করা এবং প্রয়োজনে নতুন কী তৈরি করা।

৬. **অ্যাকসেস নিয়ন্ত্রণ (Access Control)**
কে কী ব্যবহার করতে পারবে তা নিয়ন্ত্রণ করা।

৬.৪.২ Key Management (কী ম্যানেজমেন্ট)-এর গুরুত্ব

Key Management (কী ম্যানেজমেন্ট)-এর গুরুত্ব হলো ক্রিপ্টোগ্রাফি ব্যবহারের মাধ্যমে তথ্যের সুরক্ষা নিশ্চিত করা। এর মূল গুরুত্বগুলো নিচে দেয়া হলো–

১. **তথ্য নিরাপত্তা নিশ্চিত করা (Ensures Data Security)**
এনক্রিপ্ট করা ডেটা নিরাপদ থাকে এবং অননুমোদিত অ্যাক্সেস থেকে রক্ষা পায়।

২. **গোপনীয়তা বজায় রাখা (Maintains Data Privacy)**
শুধুমাত্র অনুমোদিত ব্যবহারকারী ডেটা অ্যাক্সেস বা ডিক্রিপ্ট করতে পারে।

৩. **সিস্টেমের বিশ্বাসযোগ্যতা বৃদ্ধি (Enhances System Trustworthiness)**
নিরাপদ কী ব্যবস্থাপনা ব্যবহারকারীর ভরসা তৈরি করে।

৪. **আইনি ও নীতি সম্মতি (Compliance with Laws & Policies)**
তথ্য নিরাপত্তা আইন এবং নীতি অনুযায়ী কার্যকর থাকে।

৫. **ডেটা অখণ্ডতা রক্ষা (Protects Data Integrity)**
ডেটা পরিবর্তন বা চুরি রোধে সহায়ক।

৬. **সিস্টেম আক্রমণ প্রতিরোধ (Prevents Unauthorized Access & Attacks)**
হ্যাকার বা ম্যালওয়্যার দ্বারা কী চুরি বা অবৈধ ব্যবহার কমায়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৫ ডিজিটাল স্বাক্ষর (Digital Signature)

ডিজিটাল স্বাক্ষর হলো একটি ইলেকট্রনিক বা ডিজিটাল কোড যা একটি ডিজিটাল ডকুমেন্ট বা বার্তার সত্যতা ও প্রেরকের পরিচয় নিশ্চিত করে। এটি মূলত তথ্যের অখণ্ডতা (Integrity) এবং প্রমাণীকরণ (Authentication) নিশ্চিত করার জন্য ব্যবহৃত হয়।

এটি সাধারণত পাবলিক কি ইনফ্রাস্ট্রাকচার (PKI) প্রযুক্তি ব্যবহার করে তৈরি হয় এবং এতে প্রাইভেট কী ও পাবলিক কী উভয়ের ভূমিকা থাকে।

৬.৫.১ ডিজিটাল স্বাক্ষরের উদ্দেশ্য

প্রমাণীকরণ (Authentication) - বার্তা বা ডকুমেন্ট যে প্রেরক পাঠিয়েছেন তা নিশ্চিত করা।
অখণ্ডতা (Integrity) - বার্তা বা ডকুমেন্ট মাঝপথে পরিবর্তিত হয়নি তা যাচাই করা।
অস্বীকার অযোগ্যতা (Non-repudiation) - প্রেরক পরে বার্তা পাঠানোর বিষয়টি অস্বীকার করতে না পারা।



৬.৫.২ ডিজিটাল স্বাক্ষর কাজ করার পদ্ধতি (সহজ ধাপে)

বার্তা তৈরি – প্রেরক একটি ডকুমেন্ট বা বার্তা প্রস্তুত করেন।
হ্যাশ তৈরি – বার্তার উপর একটি হ্যাশ ফাংশন প্রয়োগ করে একটি নির্দিষ্ট দৈর্ঘ্যের কোড (Message Digest) তৈরি করা হয়।
প্রাইভেট কী দিয়ে এনক্রিপশন – প্রেরক তার প্রাইভেট কী দিয়ে হ্যাশ কোড এনক্রিপ্ট করেন; এটিই ডিজিটাল স্বাক্ষর।
প্রেরণ – ডকুমেন্ট ও ডিজিটাল স্বাক্ষর একসাথে প্রাপককে পাঠানো হয়।
যাচাই – প্রাপক প্রেরকের পাবলিক কী ব্যবহার করে স্বাক্ষর ডিক্রিপ্ট করেন এবং পুনরায় ডকুমেন্ট থেকে হ্যাশ তৈরি করে মিলিয়ে দেখেন। যদি মিলে যায়, তবে স্বাক্ষর বৈধ।

৬.৫.৩ ডিজিটাল স্বাক্ষরের সুবিধা (Advantages of Digital Signature)

১. প্রমাণীকরণ (Authentication)
- নিশ্চিত করে যে বার্তা বা ডকুমেন্ট প্রেরকই পাঠিয়েছেন।
- অননুমোদিত ব্যক্তি বা হ্যাকার বার্তা পাঠাতে পারে না।

২. তথ্যের অখণ্ডতা (Integrity)
- বার্তা বা ডকুমেন্টের মধ্যে কোনো পরিবর্তন হলে তা সহজেই শনাক্ত করা যায়।
- মাঝপথে তথ্য পরিবর্তিত হলে স্বাক্ষর অকার্যকর হয়ে যায়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৩. অস্বীকার অযোগ্যতা (Non-repudiation)
- প্রেরক পরে বার্তা পাঠানোর বিষয়টি অস্বীকার করতে পারে না।
- আইনগতভাবে স্বীকৃত ও প্রমাণযোগ্য হয়।

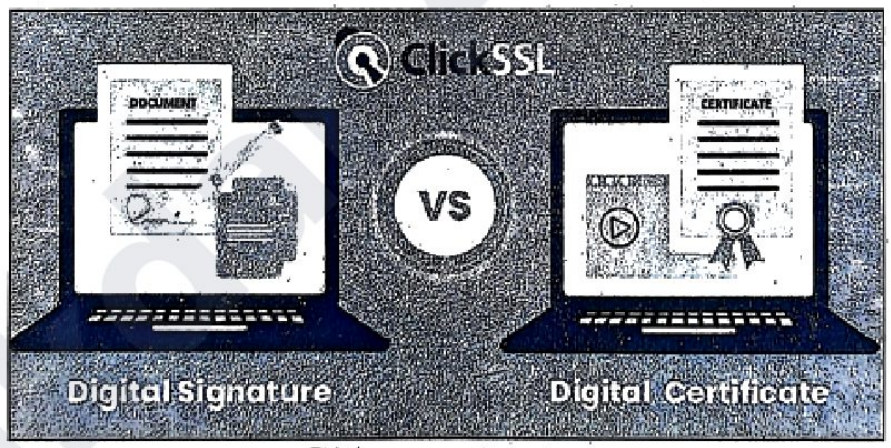
৪. নিরাপত্তা (Security)
- এনক্রিপশন প্রযুক্তি ব্যবহার করে তথ্যকে নিরাপদ রাখা হয়।
- সাইবার হামলা বা জালিয়াতি প্রতিরোধে সহায়ক।

৫. সময় ও খরচ সাশ্রয় (Time and Cost Saving)
- কাগজপত্র ও ফিজিক্যাল স্বাক্ষর ব্যবহারের প্রয়োজন কমে যায়।
- দ্রুত অনলাইন লেনদেন, চুক্তি ও ডকুমেন্ট প্রক্রিয়াকরণ সম্ভব।

৬. আইনি স্বীকৃতি (Legal Recognition)
অনেক দেশে ডিজিটাল স্বাক্ষরকে কাগজের স্বাক্ষরের সমতুল্য আইনগত স্বীকৃতি দেয়া হয়েছে।

৬.৬ ডিজিটাল সার্টিফিকেট (Digital Certificate)

ডিজিটাল সার্টিফিকেট হলো একটি ইলেকট্রনিক ডকুমেন্ট যা কোনো ব্যক্তি, প্রতিষ্ঠান বা ওয়েবসাইটের পরিচয় প্রমাণ করে এবং পাবলিক কী (Public Key) কে বৈধভাবে যাচাই করে। এটি মূলত ডিজিটাল নিরাপত্তা নিশ্চিত করার জন্য ব্যবহৃত হয়।



ছবি উৎস: www.clickssl.net

ডিজিটাল সার্টিফিকেট সাধারণত পাবলিক কী ইনফ্রাস্ট্রাকচার (PKI) সিস্টেমের অংশ হিসেবে জারি করা হয় এবং এটি একটি বিশ্বাসযোগ্য কর্তৃপক্ষ (Certificate Authority - CA) দ্বারা যাচাই করা হয়।

৬.৬.১ ডিজিটাল সার্টিফিকেটের উপাদান

সার্টিফিকেটধারীর নাম – ব্যক্তি বা প্রতিষ্ঠানের পরিচয়।
সার্টিফিকেটধারীর পাবলিক কী – এনক্রিপশন এবং যাচাইয়ের জন্য।
সার্টিফিকেট প্রদানকারী (CA) এর তথ্য – যিনি সার্টিফিকেট ইস্যু করেছেন।
মেয়াদ (Validity Period) – সার্টিফিকেটের বৈধ সময়কাল।
সার্টিফিকেট সিকিউরিটি তথ্য – ডিজিটাল স্বাক্ষর ইত্যাদি।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৬.২ ডিজিটাল সার্টিফিকেটের ধরন (Types of Digital Certificate)

ডিজিটাল সার্টিফিকেট বিভিন্ন প্রয়োজনে ব্যবহৃত হয়। প্রধান ধরনগুলো হলো-

১. ইউজার সার্টিফিকেট (Personal/Client Certificate)
ব্যক্তিগত ব্যবহারকারীর জন্য ব্যবহৃত হয়।
উদ্দেশ্য: ইমেইল এনক্রিপশন, লগইন প্রমাণীকরণ, ব্যক্তিগত ডিজিটাল স্বাক্ষর।

২. সার্ভার সার্টিফিকেট (Server Certificate)
ওয়েবসাইটের নিরাপত্তা নিশ্চিত করতে ব্যবহৃত হয়।
উদাহরণ: HTTPS ওয়েবসাইটে ব্রাউজার ও সার্ভারের নিরাপদ সংযোগ।

৩. কোড সাইনিং সার্টিফিকেট (Code Signing Certificate)
সফটওয়্যারের উৎস ও অখণ্ডতা যাচাই করতে ব্যবহৃত হয়।
উদ্দেশ্য: সফটওয়্যার বা অ্যাপ্লিকেশন ব্যবহারকারীর কাছে নিরাপদভাবে পৌঁছানো।

৪. ডিভাইস সার্টিফিকেট (Device Certificate)
IoT ডিভাইস বা নেটওয়ার্ক ডিভাইসের নিরাপত্তা নিশ্চিত করতে ব্যবহৃত হয়।
উদাহরণ: রাউটার, প্রিন্টার বা সেন্সর ডিভাইসে নিরাপদ লগইন।

৫. রুট সার্টিফিকেট (Root Certificate)
- সিআরএ (CA) কর্তৃক ইস্যু করা প্রধান সার্টিফিকেট।
- অন্যান্য ডিজিটাল সার্টিফিকেটের বিশ্বাসযোগ্যতা যাচাই করতে ব্যবহার হয়।

৬.৬.৩ ডিজিটাল সার্টিফিকেটের সুবিধা (Advantages of Digital Certificate)

১. পরিচয় যাচাই (Authentication)
- নিশ্চিত করে যে সার্টিফিকেটধারী ব্যক্তি, প্রতিষ্ঠান বা ওয়েবসাইটই সত্যিই যিনি দাবি করছেন।
- অননুমোদিত বা ভুয়া ব্যবহারকারীর প্রবেশ রোধ করে।

২. তথ্য নিরাপত্তা (Data Security)
- পাবলিক কী ব্যবহার করে তথ্য এনক্রিপশন নিশ্চিত করে।
- বার্তা বা ডেটা চুরি বা হ্যাকিং থেকে সুরক্ষিত থাকে।

৩. ডিজিটাল স্বাক্ষর যাচাই (Digital Signature Verification)
- ডিজিটাল স্বাক্ষরের সত্যতা যাচাই করা সম্ভব।
- বার্তা বা ডকুমেন্টের অখণ্ডতা নিশ্চিত হয়।

৪. অনলাইন লেনদেন ও যোগাযোগ নিরাপদ করা
- ই-কমার্স, ব্যাংকিং এবং সরকারি ওয়েবসাইটে নিরাপদ লগইন ও লেনদেন নিশ্চিত করে।
- HTTPS ওয়েবসাইটে ট্রাস্ট ও নিরাপত্তা বৃদ্ধি করে।

৫. বিশ্বাসযোগ্যতা বৃদ্ধি (Trustworthiness)
- সার্টিফিকেটধারী ব্যক্তির বা প্রতিষ্ঠানের প্রতি ব্যবহারকারীর আস্থা বৃদ্ধি করে।
- অনলাইন ব্যবসা ও যোগাযোগে বিশ্বাসযোগ্য পরিবেশ তৈরি করে।

৬. আইনি স্বীকৃতি (Legal Recognition)
অনেক দেশে ডিজিটাল সার্টিফিকেট ও এর মাধ্যমে করা লেনদেনকে আইনি স্বীকৃতি দেয়া হয়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৭ প্রাইভেসি (Privacy)

প্রাইভেসি হলো কোনো ব্যক্তি বা প্রতিষ্ঠানের ব্যক্তিগত তথ্য, কার্যকলাপ বা যোগাযোগকে অন্যের অননুমোদিত প্রবেশ, ব্যবহার বা প্রকাশ থেকে রক্ষা করার অধিকার। এটি মূলত গোপনীয়তা ও নিয়ন্ত্রণ নিশ্চিত করে যে কে কোন তথ্য দেখতে বা ব্যবহার করতে পারবে।

৬.৭.১ প্রাইভেসির মূল উপাদান (Key Elements of Privacy)

১. তথ্যের গোপনীয়তা (Confidentiality of Information)

- ব্যক্তিগত বা সংবেদনশীল তথ্য যেমন নাম, ঠিকানা, ফোন নম্বর, ব্যাংক তথ্য বা চিকিৎসা তথ্য অন্যের অননুমোদিত প্রবেশ থেকে রক্ষা করা।
  উদ্দেশ্য: তথ্য ফাঁস বা অপব্যবহার প্রতিরোধ করা।

২. ব্যক্তিগত স্বাধীনতা (Personal Autonomy)

- ব্যক্তি তার ব্যক্তিগত সিদ্ধান্ত, কার্যকলাপ বা জীবনধারায় স্বাধীন থাকে।
- অন্য কেউ ব্যক্তির ওপর নজরদারি বা হস্তক্ষেপ করতে পারে না।

৩. তথ্যের নিয়ন্ত্রণ (Control over Data)

- ব্যক্তি নিজেই নির্ধারণ করে কোন তথ্য কার কাছে, কখন ও কীভাবে শেয়ার করা হবে।
- যেমন: সোশ্যাল মিডিয়ায় প্রাইভেসি সেটিংস ব্যবহার করে তথ্য সীমাবদ্ধ করা।



ছবি উৎস: www.divinalaw.com

৪. পরিচয় সুরক্ষা (Identity Protection)

- ব্যক্তির আসল পরিচয়, যেমন জাতীয় পরিচয়পত্র নম্বর, পাসপোর্ট বা অনলাইন অ্যাকাউন্টের তথ্য নিরাপদ রাখা।
- চুরি বা জালিয়াতি প্রতিরোধে সহায়ক।

৫. যোগাযোগের গোপনীয়তা (Communication Privacy)

- ইমেইল, মেসেজ বা ফোন কলের বিষয়বস্তু অন্যের অজান্তে রক্ষা করা।
- এনক্রিপশন ব্যবহার করে অননুমোদিত অ্যাক্সেস থেকে সুরক্ষা নিশ্চিত করা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৭.২ প্রাইভেসির গুরুত্ব

প্রাইভেসি বা গোপনীয়তা ব্যক্তিগত, সামাজিক, আর্থিক ও ডিজিটাল জীবনের জন্য অত্যন্ত গুরুত্বপূর্ণ। এটি ব্যক্তি ও প্রতিষ্ঠানের তথ্যকে সুরক্ষিত রাখে এবং নিরাপদ পরিবেশ নিশ্চিত করে।

১. ব্যক্তিগত নিরাপত্তা

ব্যক্তিগত তথ্য যেমন নাম, ঠিকানা, ফোন নম্বর, ব্যাংক তথ্য বা চিকিৎসা তথ্য অন্যের হাত থেকে রক্ষা করে।
সাইবার হ্যাকিং ও পরিচয় চুরি প্রতিরোধে সহায়ক।

২. সামাজিক নিরাপত্তা

সামাজিক যোগাযোগ মাধ্যম ও অনলাইন প্ল্যাটফর্মে ব্যক্তিগত কার্যকলাপ গোপন রাখা সম্ভব।
ব্যক্তির সামাজিক মর্যাদা ও সম্মান রক্ষা হয়।

৩. আর্থিক নিরাপত্তা

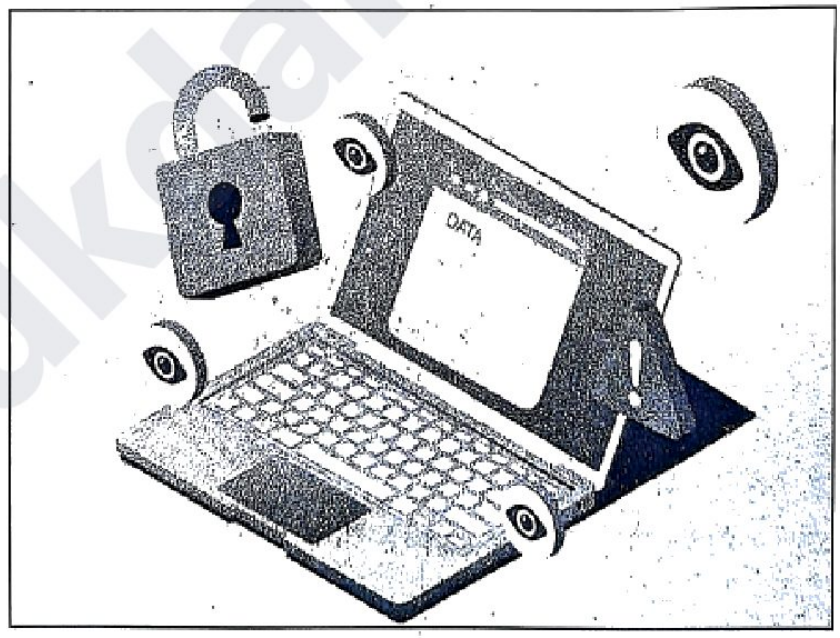
ব্যাংক অ্যাকাউন্ট, ক্রেডিট কার্ড ও অনলাইন লেনদেন নিরাপদ থাকে।
অর্থনৈতিক ক্ষতি এবং অনলাইন প্রতারণা প্রতিরোধ হয়।

৪. স্বাধীনতা ও স্ব-নিয়ন্ত্রণ

ব্যক্তি নিজেই নির্ধারণ করতে পারে কোন তথ্য কার কাছে শেয়ার করা হবে।
অননুমোদিত নজরদারি ও হস্তক্ষেপ থেকে মুক্তি পাওয়া যায়।

৫. আস্থা ও বিশ্বাস বৃদ্ধি

সংস্থা বা প্রতিষ্ঠানের সঙ্গে ব্যবহারকারীর আস্থা বৃদ্ধি পায়।
নিরাপদ অনলাইন লেনদেন ও যোগাযোগে বিশ্বাসযোগ্যতা বজায় থাকে।



৬. আইন ও নীতি মেনে চলা

অনেক দেশে প্রাইভেসি সংরক্ষণ আইন দ্বারা বাধ্যতামূলক।
আইন মেনে চললে আইনি ঝুঁকি ও জরিমানা এড়িয়ে যাওয়া যায়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৭.৩ প্রাইভেসি রক্ষা করার উপায়

প্রাইভেসি বা ব্যক্তিগত তথ্য সুরক্ষিত রাখার জন্য কিছু প্রযুক্তিগত, সচেতনতামূলক এবং আইনগত পদক্ষেপ নেয়া প্রয়োজন।

১. শক্তিশালী পাসওয়ার্ড ব্যবহার

- বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন মিশিয়ে জটিল পাসওয়ার্ড তৈরি করতে হবে।
- একই পাসওয়ার্ড একাধিক অ্যাকাউন্টে ব্যবহার করা যাবে না।

২. দুই ধাপের প্রমাণীকরণ (Two-Factor Authentication)

- লগইনের সময় পাসওয়ার্ডের পাশাপাশি একবার ব্যবহারযোগ্য কোড বা বায়োমেট্রিক যাচাই ব্যবহার করতে হবে।

৩. তথ্য সীমিতভাবে শেয়ার করা

- সোশ্যাল মিডিয়া, ওয়েবসাইট বা অ্যাপসে ব্যক্তিগত তথ্য সীমিতভাবে শেয়ার করতে হবে।
- প্রাইভেসি সেটিংস ব্যবহার করে তথ্যকে কেবল নির্দিষ্ট মানুষ বা গোষ্ঠীর জন্য দৃশ্যমান রাখতে হবে।

৪. এনক্রিপশন ব্যবহার

- ইমেইল, মেসেজ বা সংবেদনশীল তথ্য এনক্রিপ্ট করে পাঠাতে হবে।
- পোর্টেবল ডিভাইসের তথ্য এনক্রিপ্ট করতে হবে।

৫. সন্দেহজনক লিঙ্ক বা ওয়েবসাইট এড়িয়ে চলা

- অপরিচিত ইমেইল, মেসেজ বা লিঙ্কে ক্লিক করা যাবে না।
- নিরাপদ (HTTPS) ওয়েবসাইট ব্যবহার করতে হবে।

৬. সফটওয়্যার ও ডিভাইস আপডেট রাখা

- অপারেটিং সিস্টেম, ব্রাউজার ও অ্যাপ নিয়মিত আপডেট করতে হবে।
- নিরাপত্তা প্যাঁচ ইনস্টল করা নিশ্চিত করতে হবে।

৭. ব্যাকআপ রাখা

- গুরুত্বপূর্ণ তথ্যের নিয়মিত ব্যাকআপ নিতে হবে।
- নিরাপদ স্থানে সংরক্ষণ করতে হবে।

৮. সচেতনতা বৃদ্ধি

- সাইবার নিরাপত্তা ও প্রাইভেসি বিষয়ক সচেতনতা বাড়ানো।
- শিশু ও কিশোরদের অনলাইন নিরাপদ ব্যবহার শেখানো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. প্রাইভেসি রক্ষা করতে কী গুরুত্বপূর্ণ?
ক. সহজ পাসওয়াড খ. দুটি অ্যাকাউন্ট একসাথে গ. শক্তিশালী পাসওয়ার্ড ঘ. সব তথ্য প্রকাশ

২. রুট সার্টিফিকেট মূলত কী?
ক. সাইট ঠিকানা খ. নেটওয়ার্ক সেটিং গ. প্রধান সার্টিফিকেট ঘ. ব্যাকআপ ডেটা

৩. প্রাইভেসি রক্ষা করতে কোনটি ব্যবহার করা উচিত?
ক. গোপন লিঙ্ক খ. এনক্রিপশন গ. টরেন্ট সাইট ঘ. পাবলিক ওয়াইফাই

৪. তথ্যের অখণ্ডতা বলতে কী বোঝায়?
ক. তথ্য পরিবর্তিত হয় খ. তথ্য হারায় গ. তথ্য অপরিবর্তিত থাকে ঘ. তথ্য সবার জন্য খোলা

৫. ডিজিটাল সার্টিফিকেট জারি করে কে?
ক. ব্যাংক খ. সার্ভার গ. ব্যবহারকারী ঘ. সার্টিফিকেট অথরিটি (CA)

উত্তরমালা: ১. গ; ২. গ; ৩. খ; ৪. গ; ৫. ঘ।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. কী ম্যানেজমেন্ট হলো একটি প্রক্রিয়া যেখানে এনক্রিপশন ও ..... কীগুলো সুরক্ষিতভাবে তৈরি, বিতরণ, সংরক্ষণ ও ব্যবহার করা হয়। **উত্তর :** ডিক্রিপশন

২. ডিজিটাল স্বাক্ষর তৈরি করতে বার্তার উপর একটি ..... ফাংশন প্রয়োগ করে নির্দিষ্ট দৈর্ঘ্যের কোড তৈরি করা হয়। **উত্তর :** হ্যাশ

৩. ডিজিটাল সার্টিফিকেট সাধারণত একটি বিশ্বাসযোগ্য কর্তৃপক্ষ দ্বারা জারি করা হয়, যাকে বলা হয় .....। **উত্তর :** সার্টিফিকেট অথরিটি (CA)

৪. প্রাইভেসির মূল উপাদানগুলির মধ্যে একটি হলো ..... সুরক্ষা, যা জাতীয় পরিচয়পত্র নম্বর, পাসপোর্ট বা অনলাইন অ্যাকাউন্টকে সুরক্ষিত রাখে। **উত্তর :** পরিচয়

৫. প্রাইভেসি রক্ষা করার উপায়গুলির মধ্যে একটি হলো শক্তিশালী ..... ব্যবহার করা, যাতে বড় ও ছোট হাতের অক্ষর, সংখ্যা এবং বিশেষ চিহ্ন থাকে। **উত্তর :** পাসওয়ার্ড

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. ইউজার সার্টিফিকেট	ক. সিআরএ কর্তৃক ইস্যুকৃত প্রধান সার্টিফিকেট
২. সার্ভার সার্টিফিকেট	খ. রাউটার, প্রিন্টার ইত্যাদিতে নিরাপত্তা দেওয়া
৩. কোড সাইনিং সার্টিফিকেট	গ. সফটওয়্যারের উৎস ও অখণ্ডতা যাচাই করা।
৪. ডিভাইস সার্টিফিকেট	ঘ. ওয়েবসাইট নিরাপত্তা (HTTPS) নিশ্চিত করা
৫. রুট সার্টিফিকেট	ঙ. ইমেইল এনক্রিপশন, ব্যক্তিগত স্বাক্ষরের জন্য

উত্তরমালা : ১→ঙ, ২→ঘ, ৩→গ, ৪→খ, ৫→ক

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. Key ম্যানেজমেন্ট কী?
২. ডিজিটাল সার্টিফিকেট কী?
৩. কী (Key) ম্যানেজমেন্ট-এর দুটি বৈশিষ্ট্য লেখো।
৪. কী (Key) ম্যানেজমেন্ট-এর দুটি গুরুত্ব লেখো।
৫. PKI পূর্ণরূপ লেখো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬. অথোরাইজেশন কী?
৭. ইনটিগ্রিটি কী?
৮. ডিজিটাল স্বাক্ষর কী?
৯. CA এর পূর্ণরূপ লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. কী ম্যানেজমেন্ট-এর প্রধান বৈশিষ্ট্যগুলো লেখো।
২. কী ম্যানেজমেন্ট-এর গুরুত্ব কী?
৩. ডিজিটাল স্বাক্ষর কী এবং এর মূল উদ্দেশ্য কী?
৪. ডিজিটাল স্বাক্ষর প্রমাণীকরণ কীভাবে নিশ্চিত করে?
৫. ডিজিটাল স্বাক্ষর ব্যবহার করার সুবিধা লেখো।
৬. ডিজিটাল সার্টিফিকেটের প্রধান উপাদানগুলো কী কী?
৭. ডিজিটাল সার্টিফিকেটের প্রধান ধরনের নাম লেখো।
৮. প্রাইভেসি কী বোঝায়?
৯. প্রাইভেসির মূল উপাদানগুলো কী কী?
১০. প্রাইভেসি রক্ষা করার প্রধান উপায়গুলো উল্লেখ করো।

চ. দৃশ্যকল্প-ভিত্তিক প্রশ্ন :

১. একটি এনজিও দাতা-তথ্য AES দিয়ে এনক্রিপ্ট করে, কিন্তু কী ই-মেইলে প্লেইন টেক্সটে পাঠানো, শেয়ার্ড ফোল্ডারে সংরক্ষণ, আর গত ১৮ মাসে একবারও কী রোটেট করা হয়নি–সম্প্রতি কিছু ফাইল ডিক্রিপ্ট হয়ে লিক হয়েছে।

প্রশ্ন: এখানে কী ম্যানেজমেন্টের কোন ধাপগুলো (কী জেনারেশন/বিতরণ/সংরক্ষণ/অ্যাক্সেস কন্ট্রোল/রোটেশন-অবসান) লঙ্ঘিত হয়েছে এবং ঝুঁকি কমাতে তাৎক্ষণিকভাবে কী কী ঠিক করতে হবে?

২. জেলা প্রকৌশল দপ্তরে একটি ই-টেন্ডার পিডিএফ প্রস্তাবনা জমা পড়েছে যা ঠিকাদারের প্রাইভেট কী দিয়ে সাইন করা; যাচাইকারী কর্মকর্তা পোর্টালে আপলোড করে তার পাবলিক কী/সার্টিফিকেট দিয়ে সিগনেচার ভেরিফাই করেন এবং ডকুমেন্টের নতুন করে হ্যাশ বের করে মিলিয়ে দেখেন–দেখা গেল মিলছে না।

প্রশ্ন: এই পরিস্থিতিতে কোন নিরাপত্তা লক্ষ্য (Authentication, Integrity, Non-repudiation) ব্যর্থ হলো, সম্ভাব্য কারণ কী হতে পারে (যেমন ফাইল টেম্পার, ভুল সার্টিফিকেট, এক্সপায়ার্ড সার্টিফিকেট), এবং করণীয় কী?

৩. রিবা একটি ই-কমার্স সাইটে পেমেন্ট দিতে গেলে ব্রাউজার "HTTPS certificate expired/issuer not trusted" সতর্কতা দেখায়; সাইটটি কনট্যাক্টস/লোকেশন অ্যাক্সেসও চাইছে।

প্রশ্ন: এখানে কোন ধরনের সার্টিফিকেট প্রত্যাশিত (সার্ভার সার্টিফিকেট/CA চেইন/ভ্যালিডিটি), সার্টিফিকেটের কোন উপাদান দেখে সিদ্ধান্ত নিতে হবে, এবং প্রাইভেসি রক্ষায় এখন রিবার কী পদক্ষেপ নেওয়া উচিত (তথ্য সীমিতভাবে শেয়ার, 2FA, নিরাপদ নেটওয়ার্ক/VPN, সফটওয়্যার আপডেট/প্যাচ, বিকল্প ভেরিফায়েড সাইট ব্যবহার)?

ছ. ধাপ/প্রক্রিয়ামূলক প্রশ্ন :

১. কী ম্যানেজমেন্ট প্রক্রিয়ার ধাপগুলো বিশদভাবে ব্যাখ্যা করো।
২. ডিজিটাল স্বাক্ষর কাজ করার পদ্ধতি ধাপে ধাপে ব্যাখ্যা করো।

জ. বর্ণনামূলক প্রশ্ন :

১. কী ম্যানেজমেন্ট কীভাবে তথ্য নিরাপত্তা নিশ্চিত করে তা আলোচনা করো।
২. ডিজিটাল স্বাক্ষরের ব্যবহারকারীদের জন্য সুবিধাগুলো বিশ্লেষণ করো।
৩. ডিজিটাল সার্টিফিকেটের কার্যকারিতা এবং গুরুত্ব ব্যাখ্যা করো।
৪. বিভিন্ন ধরনের ডিজিটাল সার্টিফিকেট ও তাদের ব্যবহার ব্যাখ্যা করো।
৫. প্রাইভেসির গুরুত্ব ব্যক্তি, সামাজিক ও আর্থিক নিরাপত্তার দিক থেকে আলোচনা করো।
৬. প্রাইভেসি রক্ষা করার জন্য প্রযুক্তিগত ও সচেতনতামূলক উপায়গুলো বিশদভাবে ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৮ ডেটা সিকিউরিটি (Data Security)

ডেটা সিকিউরিটি হলো তথ্য বা ডেটাকে অননুমোদিত প্রবেশ, ব্যবহার, পরিবর্তন বা ধ্বংস থেকে রক্ষা করার প্রক্রিয়া। এটি ব্যক্তি, প্রতিষ্ঠান ও দেশের জন্য গুরুত্বপূর্ণ কারণ ডেটা হারানো বা চুরি হলে বড় ধরনের আর্থিক, সামাজিক ও আইনগত ক্ষতি হতে পারে।

ডেটা সিকিউরিটি নিশ্চিত করতে প্রযুক্তিগত, প্রশাসনিক ও নীতিমূলক পদক্ষেপ নেয়া হয়।

৬.৮.১ ডেটা সিকিউরিটির উদ্দেশ্য

গোপনীয়তা (Confidentiality) – ডেটা কেবল অনুমোদিত ব্যবহারকারীর কাছে দৃশ্যমান থাকে।
অখণ্ডতা (Integrity) – ডেটা মাঝপথে পরিবর্তিত বা ক্ষতিগ্রস্ত হয় না।
উপলব্ধিতা (Availability) – অনুমোদিত ব্যবহারকারী যেকোনো সময় ডেটা অ্যাক্সেস করতে পারে।

৬.৮.২ ডেটা সিকিউরিটির প্রধান ঝুঁকি

- হ্যাকিং (Hacking) – অনুমতি ছাড়া সিস্টেমে প্রবেশ।
- ম্যালওয়্যার আক্রমণ (Malware Attack) – ভাইরাস, ট্রোজান, র‍্যানসমওয়্যার।
- ফিশিং (Phishing) – প্রতারণামূলক ইমেইল বা ওয়েবসাইটের মাধ্যমে তথ্য চুরি।
- ডেটা লস (Data Loss) – হার্ডওয়্যার ক্ষতি বা প্রাকৃতিক দুর্যোগে ডেটা নষ্ট।
- অনুমোদিত অ্যাক্সেস (Unauthorized Access) - ভেতরের বা বাহ্যিক ব্যবহারকারীর অননুমোদিত প্রবেশ।

৬.৮.৩ ডেটা সিকিউরিটি নিশ্চিত করার উপায়

- শক্তিশালী পাসওয়ার্ড ও দুই ধাপের প্রমাণীকরণ ব্যবহার।
- ডেটা এনক্রিপশন করা।
- ফায়ারওয়াল ও অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার।
- নিয়মিত ব্যাকআপ নেয়া।
- সফটওয়্যার, ব্রাউজার ও সিস্টেম আপডেট রাখা।
- কর্মীদের সাইবার নিরাপত্তা সচেতনতা বৃদ্ধি করা।

৬.৯ ভালনারেবিলিটি (Vulnerability)

ভালনারেবিলিটি হলো কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা সফটওয়্যারে থাকা সেই দুর্বলতা বা ফাঁক, যা অননুমোদিত ব্যবহারকারী বা হ্যাকার দ্বারা শোষণ (exploit) করা যেতে পারে।
এটি তথ্য নিরাপত্তার একটি প্রধান ঝুঁকি, কারণ এর মাধ্যমে সিস্টেমে প্রবেশ, ডেটা চুরি বা ধ্বংস এবং সেবা ব্যাহত করা সম্ভব।

৬.৯.১ ভালনারেবিলিটির ধরন

১. সফটওয়্যার দুর্বলতা (Software Vulnerability)
কোনো প্রোগ্রাম বা অ্যাপ্লিকেশনে থাকা ত্রুটি বা বাগ যা হ্যাকারদের সিস্টেমে প্রবেশের সুযোগ দেয়।
উদাহরণ: অপারেটিং সিস্টেম, ওয়েব অ্যাপ্লিকেশন বা মোবাইল অ্যাপের নিরাপত্তা ফাঁক।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

২. হার্ডওয়্যার দুর্বলতা (Hardware Vulnerability)
কম্পিউটার বা ডিভাইসের ফিজিক্যাল সীমাবদ্ধতা বা ত্রুটি যা নিরাপত্তা হুমকি সৃষ্টি করে।
উদাহরণ: পুরোনো প্রসেসর, নেটওয়ার্ক ডিভাইসের নিরাপত্তা ফাঁক।

৩. নেটওয়ার্ক দুর্বলতা (Network Vulnerability)
নেটওয়ার্কে থাকা ফাঁক যা হ্যাকারদের ডেটা চুরি, হাইজ্যাক বা সেবা ব্যাহত করতে সাহায্য করে।
উদাহরণ: খোলা ওয়াইফাই, দুর্বল এনক্রিপশন, অপ্রত্যাশিত পোর্ট।

৪. মানবীয় দুর্বলতা (Human Vulnerability)
ব্যবহারকারীর ভুল, সচেতনতার অভাব বা অনভিজ্ঞতার কারণে সিস্টেমে নিরাপত্তার ঝুঁকি তৈরি হয়।
উদাহরণ: সহজ পাসওয়ার্ড ব্যবহার, ফিশিং ইমেইলে ক্লিক করা।

৫. প্রক্রিয়া বা নীতি দুর্বলতা (Process/Policy Vulnerability)
প্রতিষ্ঠানের নিরাপত্তা নীতি বা প্রক্রিয়ায় ফাঁক।
উদাহরণ: অননুমোদিত তথ্য শেয়ারিং, নিরাপত্তা নীতির অভাব।

৬.৯.২ ভালনারেবিলিটি চিহ্নিত করার উপায়

ভালনারেবিলিটি চিহ্নিত করা নিরাপত্তা নিশ্চিত করার প্রথম ধাপ। এটি করলে সিস্টেমের দুর্বলতা আগে থেকেই শনাক্ত করে প্রতিরোধ করা সম্ভব।

১. নিরাপত্তা অডিট (Security Audit)
প্রতিষ্ঠানের সিস্টেম, নেটওয়ার্ক ও সফটওয়্যার নিয়মিত পর্যালোচনা করা।
নিরাপত্তা নীতি এবং কার্যপ্রণালি যাচাই করা।

২. পেনেট্রেশন টেস্টিং (Penetration Testing)
হ্যাকারদের মতো সিমুলেটেড আক্রমণ করে সিস্টেমের দুর্বলতা পরীক্ষা করা।
উদ্দেশ্য: কোন অংশে প্রবেশ করা সম্ভব তা খুঁজে বের করা।

৩. লগ ও মনিটরিং বিশ্লেষণ (Log & Monitoring Analysis)
সিস্টেম ও নেটওয়ার্ক লগ পর্যবেক্ষণ করে অস্বাভাবিক কার্যকলাপ শনাক্ত করা।
ব্যবহারকারীর আচরণ, অননুমোদিত প্রবেশ বা আক্রমণ চিহ্নিত করা।

৪. সোর্স কোড বিশ্লেষণ (Source Code Analysis)
সফটওয়্যারের কোড পরীক্ষা করে বাগ বা নিরাপত্তার ফাঁক শনাক্ত করা।
স্বয়ংক্রিয় টুল বা ম্যানুয়াল রিভিউ ব্যবহার করা যেতে পারে।

৫. সুরক্ষা টুল ও স্ক্যানার ব্যবহার (Security Tools & Scanners)
অটোমেটেড ভ্যালনারেবিলিটি স্ক্যানার ব্যবহার করা।
উদাহরণ: Nessus, OpenVAS, Qualys ইত্যাদি।

৬. ব্যবহারকারীর প্রতিক্রিয়া ও রিপোর্ট (User Feedback & Reports)
ব্যবহারকারীরা যেসব সমস্যার সম্মুখীন হয় তা রিপোর্ট করে দুর্বলতা চিহ্নিত করতে সাহায্য করতে পারে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.৯.৩ ভালনারেবিলিটি প্রতিরোধের উপায়

ভালনারেবিলিটি প্রতিরোধ করা তথ্য নিরাপত্তার একটি গুরুত্বপূর্ণ অংশ। এটি করলে সিস্টেম, নেটওয়ার্ক ও ডেটা নিরাপদ থাকে।

১. **সফটওয়্যার ও সিস্টেম আপডেট রাখা**
অপারেটিং সিস্টেম, অ্যাপ্লিকেশন ও সফটওয়্যার নিয়মিত আপডেট করা।
নিরাপত্তা প্যাঁচ ইনস্টল করা যাতে বাগ বা ফাঁক বন্ধ করা যায়।

২. **শক্তিশালী পাসওয়ার্ড ব্যবহার**
বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন মিশিয়ে জটিল পাসওয়ার্ড তৈরি।
একই পাসওয়ার্ড একাধিক অ্যাকাউন্টে ব্যবহার এড়িয়ে চলা।

৩. **দুই ধাপের প্রমাণীকরণ (Two-Factor Authentication)**
লগইনের সময় পাসওয়ার্ডের পাশাপাশি একবার ব্যবহারযোগ্য কোড বা বায়োমেট্রিক যাচাই ব্যবহার।

৪. **ফায়ারওয়াল, অ্যান্টিভাইরাস ও এনক্রিপশন ব্যবহার**
সিস্টেম ও নেটওয়ার্কে অননুমোদিত প্রবেশ রোধ করতে।
ডেটা এনক্রিপশন করে তথ্য চুরি বা পরিবর্তন প্রতিরোধ।

৫. **নিরাপত্তা নীতি ও প্রক্রিয়া অনুসরণ**
প্রতিষ্ঠানের নিরাপত্তা নীতি মানা ও নিয়মিত প্রশিক্ষণ।
ব্যবহারকারীদের সচেতন করা, যেমন সন্দেহজনক লিঙ্কে ক্লিক করা যাবে না।

৬. **নিয়মিত ব্যাকআপ রাখা**
গুরুত্বপূর্ণ তথ্যের ব্যাকআপ নিতে হবে এবং নিরাপদ স্থানে সংরক্ষণ করতে হবে।
তথ্য হারানো বা ক্ষতি হলে দ্রুত পুনরুদ্ধার সম্ভব।

৭. **নিরাপত্তা মনিটরিং ও অডিট**
সিস্টেম ও নেটওয়ার্ক মনিটরিং করা।
নিয়মিত নিরাপত্তা অডিট ও পেনেট্রেশন টেস্ট করা।

৬.১০.১ থ্রেট (Threat)

থ্রেট হলো কোনো সিস্টেম, নেটওয়ার্ক বা ডেটার নিরাপত্তার জন্য সম্ভাব্য হুমকি বা আক্রমণের উৎস। এটি হতে পারে যেকোনো পরিস্থিতি বা ব্যক্তিগত কার্যকলাপ যা তথ্য চুরি, পরিবর্তন বা ধ্বংসের কারণ হতে পারে।

৬.১০.১.১ থ্রেটের ধরন (Types of Threats)

১. **প্রাকৃতিক থ্রেট (Natural Threat)**
প্রাকৃতিক দুর্যোগ বা পরিবেশগত ঘটনার কারণে সিস্টেম ও ডেটার ক্ষতি।
উদাহরণ: বজ্রপাত, ভূমিকম্প, বন্যা, অগ্নিকাণ্ড।

২. **মানবসৃষ্ট থ্রেট (Human Threat)**
মানুষের দ্বারা সৃষ্ট হুমকি যা সিস্টেম বা ডেটার নিরাপত্তাকে প্রভাবিত করে।
উদাহরণ:
হ্যাকার বা সাইবার ক্রিমিনালদের আক্রমণ।
অভ্যন্তরীণ কর্মচারীর ভুল বা অননুমোদিত কার্যকলাপ।
সামাজিক ইঞ্জিনিয়ারিং (Social Engineering)।

Visit Our Website: all.talukdaracademy.com.bd

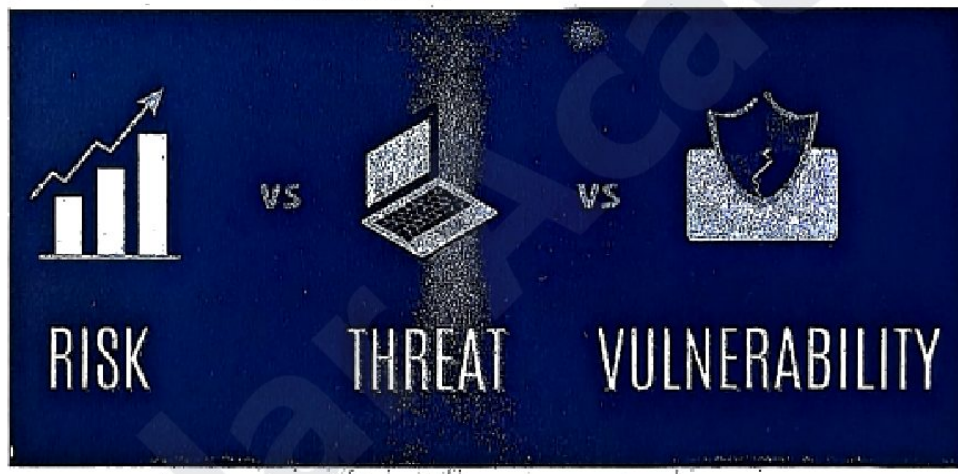
Visit Our Website: all.talukdaracademy.com.bd

৩. প্রযুক্তিগত থ্রেট (Technological Threat)
প্রযুক্তি বা ডিভাইসের সীমাবদ্ধতা ও ত্রুটির কারণে সৃষ্ট হুমকি।
উদাহরণ:
সফটওয়্যারের বাগ বা নিরাপত্তা ফাঁক।
হার্ডওয়্যার ব্যর্থতা বা নেটওয়ার্ক দুর্বলতা।

৪. আইনি বা নীতি সংক্রান্ত থ্রেট (Legal/Policy Threat)
সংস্থা বা প্রতিষ্ঠানের নীতি, নিয়ম বা আইন না মানার কারণে সৃষ্ট ঝুঁকি।
উদাহরণ: ডেটা প্রাইভেসি নীতি লঙ্ঘন, অননুমোদিত তথ্য শেয়ারিং।

৬.১০.২ রিস্ক (Risk)

রিস্ক হলো থ্রেটের কারণে সিস্টেম বা ডেটা ক্ষতির সম্ভাবনা এবং তার প্রভাব। এটি মূলত হুমকি এবং ভ্যালনারেবিলিটির সংমিশ্রণ।
রিস্ক = থ্রেট × ভ্যালনারেবিলিটি × প্রভাব (Impact)



ছবি উৎস : AV Cyber Active

৬.১০.২.১ রিস্কের ধরন (Types of Risk)

১. উচ্চ রিস্ক (High Risk)
- সিস্টেম বা ডেটার জন্য মারাত্মক ক্ষতির সম্ভাবনা খুব বেশি।
- দ্রুত প্রতিরোধমূলক ব্যবস্থা নেয়া প্রয়োজন।

উদাহরণ: ব্যাংকিং সিস্টেমে হ্যাকিং, গুরুত্বপূর্ণ সরকারি ডেটা চুরি।

২. মধ্যম রিস্ক (Medium Risk)
- সিস্টেম বা ডেটার জন্য সীমিত বা আংশিক ক্ষতির সম্ভাবনা।
- নিয়মিত নজরদারি ও আংশিক প্রতিরোধ প্রয়োজন।

উদাহরণ: অফিসের সাধারণ ডকুমেন্ট লস, অল্প গুরুত্বপূর্ণ ওয়েবসাইটে হ্যাক।

৩. নিম্ন রিস্ক (Low Risk)
- ক্ষতির সম্ভাবনা কম এবং প্রভাব সীমিত।
- পর্যবেক্ষণ চালিয়ে রাখতে হবে, কিন্তু তৎক্ষণাৎ বড় ব্যবস্থা নেয়ার প্রয়োজন নেই।

উদাহরণ: ব্যক্তিগত ব্লগ বা সাধারণ তথ্য ডেটার ক্ষতি।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৪. ক্রস ফাংশনাল রিস্ক (Cross-Functional Risk)

- একাধিক সিস্টেম বা বিভাগের মধ্যে সৃষ্ট ঝুঁকি।
- এক সিস্টেমে সমস্যা অন্য সিস্টেমকে প্রভাবিত করতে পারে।

উদাহরণ: নেটওয়ার্ক ব্রেকডাউন যা সমস্ত ডিপার্টমেন্টকে প্রভাবিত করে।

৫. অপারেশনাল রিস্ক (Operational Risk)

দৈনন্দিন কার্যক্রমের কারণে সৃষ্ট ঝুঁকি।

উদাহরণ: সিস্টেম ফেইলিওর, কর্মচারীর ভুল, প্রক্রিয়ার ত্রুটি।

৬.১০.২.২ থ্রেট ও রিস্ক ব্যবস্থাপনার উপায়

১. থ্রেট চিহ্নিতকরণ (Threat Identification)

সম্ভাব্য হুমকি বা থ্রেট সনাক্ত করা।

প্রাকৃতিক, মানবসৃষ্ট, প্রযুক্তিগত বা নীতি সংক্রান্ত থ্রেট আলাদা করা।

২. ভ্যালনারেবিলিটি মূল্যায়ন (Vulnerability Assessment)

সিস্টেম, নেটওয়ার্ক বা ডেটার দুর্বলতা চিহ্নিত করা।

কোন অংশে হুমকি কার্যকর হতে পারে তা জানা।

৩. রিস্ক বিশ্লেষণ (Risk Analysis)

চিহ্নিত থ্রেট এবং ভ্যালনারেবিলিটির প্রভাব অনুযায়ী রিস্ক নির্ধারণ।

রিস্কের মাত্রা (উচ্চ, মধ্যম, নিম্ন) নির্ধারণ করা।

৪. রিস্ক নিয়ন্ত্রণ ও প্রতিরোধ (Risk Mitigation)

প্রতিরোধমূলক ব্যবস্থা গ্রহণ করা।

উদাহরণ:

ফায়ারওয়াল ও অ্যান্টিভাইরাস ব্যবহার।

এনক্রিপশন প্রযুক্তি প্রয়োগ।

শক্তিশালী পাসওয়ার্ড ও দুই ধাপের প্রমাণীকরণ।

নিয়মিত ব্যাকআপ নেয়া।

৫. মনিটরিং ও পুনর্মূল্যায়ন (Monitoring & Review)

সিস্টেম ও নেটওয়ার্ক নিয়মিত পর্যবেক্ষণ।

নতুন হুমকি ও পরিবর্তিত ঝুঁকি মূল্যায়ন।

নিরাপত্তা নীতি ও প্রক্রিয়া আপডেট করা।

৬. সচেতনতা ও প্রশিক্ষণ (Awareness & Training)

ব্যবহারকারী ও কর্মীদের সাইবার নিরাপত্তা ও প্রাইভেসি বিষয়ে সচেতন করা।

সন্দেহজনক ইমেইল বা লিঙ্ক সম্পর্কে জানানো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. কোনটি ডেটা সিকিউরিটির ঝুঁকি?
ক. সফটওয়্যার ডেভেলপমেন্ট খ. হ্যাকিং গ. ব্যাকআপ ঘ. আপডেট

২. ফিশিং কী ধরনের আক্রমণ?
ক. প্রযুক্তিগত খ. সামাজিক প্রকৃতির গ. প্রাকৃতিক দুর্যোগ ঘ. ফিজিক্যাল

৩. নিচের কোনটি মানবীয় দুর্বলতার উদাহরণ?
ক. ফায়ারওয়াল ব্যবহার খ. খোলা ওয়াইফাই গ. ফিশিং ইমেইলে ক্লিক করা ঘ. সফটওয়্যার আপডেট

৪. থ্রেট কী?
ক. ব্যাকআপ পদ্ধতি খ. সম্ভাব্য হুমকি গ. সফটওয়্যার আপডেট ঘ. নিরাপত্তা নীতি

৫. নিচের কোনটি নিরাপত্তা মনিটরিং টুল?
ক. নেসাস খ. টুইটার গ. গুগল ড্রাইভ ঘ. ফেসবুক

উত্তরমালা : ১. খ; ২. খ; ৩. গ; ৪. খ; ৫. ক।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. ডেটা সিকিউরিটির প্রধান উদ্দেশ্য হলো ....., অখণ্ডতা ও উপলব্ধিতা নিশ্চিত করা। **উত্তর :** গোপনীয়তা

২. ..... আক্রমণের মাধ্যমে প্রতারণামূলক ইমেইল বা ওয়েবসাইট ব্যবহার করে তথ্য চুরি করা হয়। **উত্তর :** ফিশিং

৩. ভালনারেবিলিটি হলো কোনো সিস্টেমে থাকা ..... বা ফাঁক, যা হ্যাকাররা শোষণ করতে পারে। **উত্তর :** দুর্বলতা

৪. প্রাকৃতিক থ্রেটের উদাহরণ হলো ....., ভূমিকম্প, বন্যা ইত্যাদি। **উত্তর :** বজ্রপাত

৫. রিস্ক নির্ধারণের সূত্র হলো : রিস্ক = ... × ভালনারেবিলিটি × প্রভাব। **উত্তর :** থ্রেট

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. তথ্য নিরাপত্তা	ক. আইন ও নীতি মেনে কার্যকর থাকে।
২. গোপনীয়তা বজায় রাখা	খ. শুধুমাত্র অনুমোদিত ব্যবহারকারী ডিক্রিপ্ট করতে পারে।
৩. সিস্টেমের বিশ্বাসযোগ্যতা বৃদ্ধি	গ. ডেটা পরিবর্তন বা চুরি রোধ করা হয়।
৪. আইনি ও নীতি সম্মতি	ঘ. ডেটা নিরাপদ থাকে ও অননুমোদিত অ্যাক্সেস রোধ হয়।
৫. ডেটা অখণ্ডতা রক্ষা	ঙ. ব্যবহারকারীর ভরসা তৈরি হয়।

উত্তরমালা : ১→ঘ, ২→খ, ৩→ঙ, ৪→ক, ৫→গ

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. ডেটা সিকিউরিটি কী?
২. থ্রেট কী
৩. ডেটা লস কী?
৪. অননুমোদিত অ্যাক্সেস কী?
৫. ভালনারেবিলিটির দুটি ধরন লেখো।
৬. ডেটা সিকিউরিটি নিশ্চিত করার দুটি উপায় লেখো।
৭. ভালনারেবিলিটি চিহ্নিত করার দুটি উপায় লেখো।
৮. ভালনারেবিলিটি প্রতিরোধের দুটি উপায় লেখো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৯. থ্রেটের দুটি ধরন লেখো।
১০. রিস্ক কী?
১১. রিস্কের দুটি ধরন লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. ডেটা সিকিউরিটির উদ্দেশ্য তিনটি লেখো।
২. ডেটা সিকিউরিটির প্রধান ঝুঁকিগুলো কী কী?
৩. ডেটা সিকিউরিটি নিশ্চিত করার উপায় কী কী?
৪. ভালনারেবিলিটি কী বোঝায়?
৫. ভালনারেবিলিটির প্রধান ধরনগুলো কী কী?
৬. ভালনারেবিলিটি চিহ্নিত করার উপায় লেখো।
৭. ভালনারেবিলিটি প্রতিরোধ করার প্রধান উপায়গুলো কী কী?
৮. থ্রেট কী এবং এর উদাহরণ লেখো।
৯. থ্রেটের ধরনগুলো কী কী?
১০. রিস্ক কী এবং এর সূত্র লেখো।
১১. রিস্ক ব্যবস্থাপনার প্রধান উপায়গুলো কী কী?

চ. দৃশ্যকল্প-ভিত্তিক প্রশ্ন :

১. একটি ব্যাংকের ডাটাবেসে গ্রাহকের ব্যক্তিগত ও আর্থিক তথ্য সংরক্ষিত আছে। হঠাৎ করে র‍্যানসমওয়্যার আক্রমণে সব ডেটা লক হয়ে যায় এবং হ্যাকার টাকা দাবি করে।
প্রশ্ন: এখানে কোন ডেটা সিকিউরিটি ঝুঁকি দেখা দিয়েছে এবং তা প্রতিরোধের জন্য প্রতিষ্ঠানটি আগে থেকেই কী কী ব্যবস্থা নিতে পারতো?

২. একটি সরকারি অফিসে ব্যবহৃত সফটওয়্যারে পুরোনো অপারেটিং সিস্টেমের কারণে বারবার হ্যাকিংয়ের চেষ্টা হচ্ছে। তদন্তে জানা গেল কর্মচারীরা সহজ পাসওয়ার্ড ব্যবহার করছে এবং অনেক সময় সন্দেহজনক ইমেইল লিঙ্কে ক্লিক করছে।
প্রশ্ন: এখানে কোন ধরণের ভালনারেবিলিটি বিদ্যমান এবং তা চিহ্নিত ও প্রতিরোধের উপায় কী হতে পারে?

৩. একটি ই-কমার্স প্রতিষ্ঠানের সার্ভার প্রাকৃতিক দুর্যোগে (বন্যা) ক্ষতিগ্রস্ত হয়েছে। ফলে কাস্টমার ডেটা নষ্ট হওয়ার ঝুঁকি তৈরি হয়েছে।
প্রশ্ন: এখানে কোন ধরণের থ্রেট কাজ করছে? এর ফলে কী ধরনের রিস্ক তৈরি হতে পারে এবং প্রতিষ্ঠানটি কীভাবে রিস্ক ম্যানেজমেন্ট করতে পারে?

ছ. ধাপ/প্রক্রিয়ামূলক প্রশ্ন :

১. রিস্ক বিশ্লেষণ ও নিয়ন্ত্রণ প্রক্রিয়ার ধাপগুলো বিস্তারিতভাবে আলোচনা করো।
২. ভালনারেবিলিটি চিহ্নিত করার পদ্ধতিগুলি ধাপে ধাপে ব্যাখ্যা করো।

জ. বর্ণনামূলক প্রশ্ন :

১. ডেটা সিকিউরিটির উদ্দেশ্য এবং গুরুত্ব বিশদভাবে ব্যাখ্যা করো।
২. হ্যাকিং, ম্যালওয়্যার, ফিশিং ও ডেটা লস-এর মাধ্যমে সৃষ্ট ঝুঁকিগুলো বিশ্লেষণ করো।
৩. ডেটা সিকিউরিটি নিশ্চিত করার জন্য প্রযুক্তিগত ও প্রশাসনিক পদক্ষেপগুলোর ব্যাখ্যা দাও।
৪. ভালনারেবিলিটি কী এবং এটি তথ্য নিরাপত্তার জন্য কেন গুরুত্বপূর্ণ?
৫. সফটওয়্যার, হার্ডওয়্যার, নেটওয়ার্ক, মানবীয় ও নীতি দুর্বলতা বিশ্লেষণ করো।
৬. ভালনারেবিলিটি প্রতিরোধের উপায়গুলো বিশদভাবে ব্যাখ্যা করো।
৭. থ্রেট ও রিস্কের সংজ্ঞা, ধরন ও উদাহরণ ব্যাখ্যা করো।
৮. থ্রেট, রিস্ক ও ভালনারেবিলিটির মধ্যে সম্পর্ক এবং সাইবার নিরাপত্তায় তাদের গুরুত্ব ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১১ ম্যালওয়্যার (Malware)

ম্যালওয়্যার হলো "ম্যালিশাস সফটওয়্যার (Malicious Software)" বা ক্ষতিকর সফটওয়্যার, যা কম্পিউটার, নেটওয়ার্ক বা ডিভাইসকে ক্ষতি করার জন্য ডিজাইন করা হয়।

ম্যালওয়্যার সাধারণত ডেটা চুরি, সিস্টেম ক্ষতি, নেটওয়ার্ক ব্যাহত বা ব্যবহারকারীর গোপন তথ্য চুরির জন্য ব্যবহৃত হয়।

৬.১১.১ ম্যালওয়্যারের ধরন (Types of Malware)

ধরন	সংক্ষিপ্ত বিবরণ	উদাহরণ
ভাইরাস (Virus)	প্রোগ্রামে নিজেকে সংযুক্ত করে এবং সিস্টেমে ছড়িয়ে পড়ে	ফাইল ইনফেকশন, প্রোগ্রাম ধ্বংস
ওয়ার্ম (Worm)	স্বয়ংক্রিয়ভাবে নেটওয়ার্কে ছড়িয়ে পড়ে, (ব্যবহারকারীর হস্তক্ষেপ ছাড়াই)	ইমেইল ও নেটওয়ার্ক ওয়ার্ম
ট্রোজান হর্স (Trojan Horse)	ম্যালিশাস কোড লুকিয়ে রেখে বৈধ সফটওয়্যারের মতো আচরণ করে	ডেটা চুরি, ব্যাকডোর খুলে দেয়া
স্পাইওয়্যার (Spyware)	ব্যবহারকারীর কার্যকলাপ ও তথ্য গোপনে নজরদারি করে	কুকি ট্র্যাকিং, পাসওয়ার্ড চুরি
অ্যাডওয়্যার (Adware)	ব্যবহারকারীর অনুমতি ছাড়া বিজ্ঞাপন দেখানো এবং সিস্টেম ধীর করে	পপ-আপ বিজ্ঞাপন সফটওয়্যার
র‍্যানসমওয়্যার (Ransomware)	ডেটা এনক্রিপ্ট করে মুক্তির জন্য মুক্তিপণ দাবি করে	WannaCry, Petya
রুটকিট (Rootkit)	সিস্টেমে লুকিয়ে থাকে এবং হ্যাকারকে নিয়ন্ত্রণ দেয়	ব্যাকডোর প্রদান, সিস্টেম মনিপুলেশন

৬.১১.২ ম্যালওয়্যার দ্বারা সৃষ্ট সমস্যা

১. **ডেটা ক্ষতি বা চুরি (Data Loss or Theft)**
ম্যালওয়্যার ব্যবহারকারীর গুরুত্বপূর্ণ ফাইল বা ডেটা নষ্ট বা চুরি করতে পারে।
উদাহরণ: ব্যক্তিগত ফাইল, ব্যাংকিং তথ্য, পাসওয়ার্ড চুরি।

২. **সিস্টেম ধীর বা ক্র্যাশ (System Slowdown or Crash)**
ভাইরাস বা ওয়ার্ম সিস্টেমের প্রসেসিং ধীর করে বা হ্যাং/ক্র্যাশ ঘটায়।
কম্পিউটার, সার্ভার বা নেটওয়ার্ক অকার্যকর হয়ে যেতে পারে।

৩. **অননুমোদিত নিয়ন্ত্রণ (Unauthorized Control)**
রুটকিট বা ট্রোজান হ্যাকারকে ব্যবহারকারীর সিস্টেম নিয়ন্ত্রণের সুযোগ দেয়।
উদ্দেশ্য: ডেটা চুরি, স্প্যাম প্রেরণ বা সিস্টেম মনিপুলেশন।

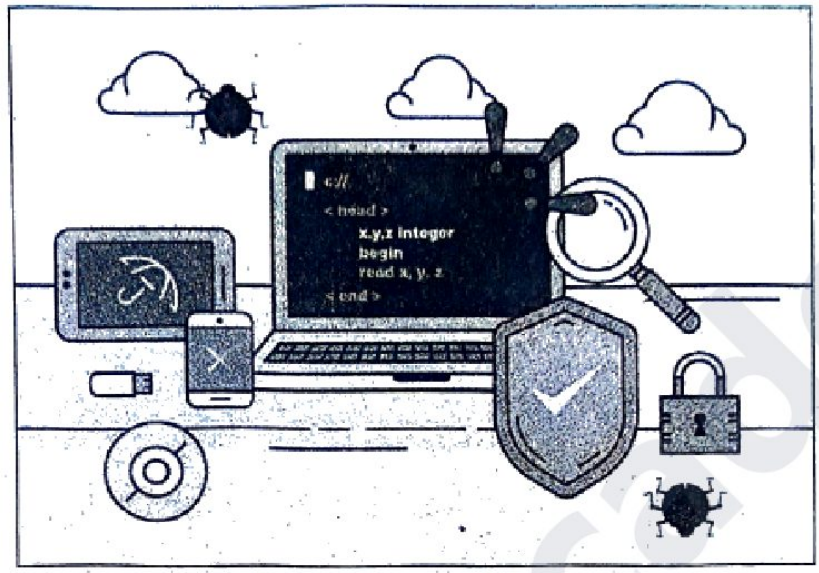
৪. **গোপনীয়তা লঙ্ঘন (Privacy Breach)**
স্পাইওয়্যার বা কুকি ট্র্যাকিং ব্যবহারকারীর কার্যকলাপ ও ব্যক্তিগত তথ্য নজরদারি করে।
ফল: গোপন তথ্য ফাঁস, ব্যক্তিগত আচরণ পর্যবেক্ষণ।

৫. **অর্থনৈতিক ক্ষতি (Financial Loss)**
র‍্যানসমওয়্যার ডেটা এনক্রিপ্ট করে মুক্তিপণ দাবি করে।
ব্যাংকিং বা ই-কমার্সে ফ্রড ও চুরি ঘটতে পারে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬. সাইবার আক্রমণ ও নেটওয়ার্ক ঝুঁকি (Cyber Attack & Network Risk)
ম্যালওয়্যার নেটওয়ার্কে ছড়িয়ে সিস্টেম ব্যাহত করে।
ডিনায়াল-অফ-সার্ভিস (DoS) আক্রমণ, স্প্যাম বা বটনেট তৈরি।



ছবি উৎস : https://www.freepik.com/

৬.১১.৩ ম্যালওয়্যার প্রতিরোধের উপায়

১. অ্যান্টিভাইরাস ও অ্যান্টিম্যালওয়্যার ব্যবহার
কম্পিউটার, মোবাইল ও নেটওয়ার্কে অ্যান্টিভাইরাস সফটওয়্যার ইন্সটল ও সক্রিয় রাখা।
নিয়মিত স্ক্যান করে ম্যালওয়্যার চিহ্নিত ও সরানো।

২. সফটওয়্যার ও সিস্টেম আপডেট রাখা
অপারেটিং সিস্টেম, অ্যাপ্লিকেশন ও ব্রাউজার নিয়মিত আপডেট করা।
নিরাপত্তা প্যাঁচ ইনস্টল করে সফটওয়্যারের দুর্বলতা বন্ধ করা।

৩. সন্দেহজনক ইমেইল ও লিঙ্ক এড়িয়ে চলা
অপরিচিত ইমেইল, ফাইল, লিঙ্ক বা ডাউনলোডে ক্লিক না করা।
ফিশিং বা স্প্যাম থেকে সিস্টেমকে রক্ষা করা।

৪. ফায়ারওয়াল ও নেটওয়ার্ক সিকিউরিটি
ফায়ারওয়াল ব্যবহার করে অননুমোদিত প্রবেশ রোধ করা।
নিরাপদ নেটওয়ার্ক ও এনক্রিপশন ব্যবহার।

৫. নিয়মিত ব্যাকআপ রাখা
গুরুত্বপূর্ণ ডেটার ব্যাকআপ নেয়া এবং নিরাপদ স্থানে সংরক্ষণ করা।
র‍্যানসমওয়্যার বা ডেটা ক্ষতি হলে দ্রুত পুনরুদ্ধার সম্ভব।

৬. ব্যবহারকারী সচেতনতা ও প্রশিক্ষণ
ব্যবহারকারীদের ম্যালওয়্যার সম্পর্কে সচেতন করা।
নিরাপদ অনলাইন ব্যবহার ও সন্দেহজনক ফাইল/লিঙ্ক চিনতে শেখানো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১২ সোশ্যাল ইঞ্জিনিয়ারিং (Social Engineering)

সোশ্যাল ইঞ্জিনিয়ারিং হলো মানুষকে প্রভাবিত বা প্রতারণার মাধ্যমে গুরুত্বপূর্ণ তথ্য, যেমন পাসওয়ার্ড, ব্যাংক অ্যাকাউন্ট, ক্রেডেনশিয়াল বা অন্য সংবেদনশীল তথ্য হাতিয়ে নেয়ার কৌশল। এটি প্রযুক্তিগত হ্যাকিং নয়, বরং মানুষের বিশ্বাস ও মানসিক দুর্বলতার উপর ভিত্তি করে পরিচালিত হয়।

৬.১২.১ সোশ্যাল ইঞ্জিনিয়ারিং-এর ধরন (Types of Social Engineering)

ধরন	সংক্ষিপ্ত বিবরণ	উদাহরণ
ফিশিং (Phishing)	ইমেইল, মেসেজ বা ওয়েবসাইটের মাধ্যমে ব্যবহারকারীকে প্রতারিত করা।	ব্যাংক বা সোশ্যাল মিডিয়া লগইন ফেক লিঙ্ক পাঠানো
স্পিয়ার ফিশিং (Spear Phishing)	নির্দিষ্ট ব্যক্তি বা প্রতিষ্ঠানের উপর লক্ষ্য করে করা ফিশিং।	উচ্চপদস্থ কর্মকর্তা বা নির্দিষ্ট কর্মচারীকে টার্গেট করা
ভয়িং (Vishing)	ফোন কল বা ভয় ব্যবহার করে তথ্য হাতিয়ে নেয়া।	ব্যাংক কলার ছদ্মবেশে পাসওয়ার্ড চাওয়া
স্মার্টফোন বা মেসেজিং (Smishing)	SMS বা মেসেজের মাধ্যমে তথ্য চুরি।	ফেক OTP বা লিঙ্ক পাঠানো
প্রি-টেক্সটিং (Pretexting)	ভুয়া পরিচয় বা গল্পের মাধ্যমে তথ্য নেয়া।	পুলিশের বা ব্যাংকের নাম ব্যবহার করে তথ্য চাওয়া
বাইটিং/ফিজিক্যাল (Baiting/Physical)	মানুষকে লোভ দেখিয়ে বা সরাসরি ফাইল/USB দিয়ে হুমকি সৃষ্টি।	USB দিয়ে ভাইরাস সংক্রমণ

৬.১২.২ সোশ্যাল ইঞ্জিনিয়ারিং-এর ক্ষতি

- ব্যক্তিগত ও সংবেদনশীল তথ্য ফাঁস।
- আর্থিক ক্ষতি ও ফ্রড।
- পরিচয় চুরি ও অননুমোদিত অ্যাক্সেস।
- সিস্টেম ও নেটওয়ার্কে হ্যাকারের নিয়ন্ত্রণ।

৬.১২.৩ সোশ্যাল ইঞ্জিনিয়ারিং প্রতিরোধের উপায়

- সচেতনতা বৃদ্ধি – ব্যবহারকারীকে অনলাইন নিরাপত্তা ও প্রতারণার কৌশল সম্পর্কে শিক্ষা দেওয়া।
- দৃঢ় পাসওয়ার্ড ও দুই ধাপের প্রমাণীকরণ ব্যবহার।
- সন্দেহজনক লিঙ্ক বা মেসেজ এড়িয়ে চলা।
- ব্যাংক, প্রশাসনিক বা সংবেদনশীল তথ্য শেয়ার করার আগে যাচাই।
- নিরাপদ নেটওয়ার্ক ও ফায়ারওয়াল ব্যবহার।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৫. সতর্ক পর্যবেক্ষণ

শিক্ষার্থী বা গবেষকের লেখা নিয়মিত মনিটর করা।
অস্বাভাবিক লেখার ধরণ বা স্টাইলের মিল খুঁজে দেখা।



ছবি উৎস : www.medtextpert.com

৬.১৪.৩ Plagiarism প্রতিরোধের উপায়

Plagiarism প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে অন্যের লেখা বা ধারণা চুরি থেকে রক্ষা পাওয়া যায়। প্রধান পদ্ধতিগুলো হলো:

১. উদ্ধৃতি ও সূত্র ব্যবহার (Proper Citation)
যেকোনো তথ্য বা ধারণা অন্যের হলে উৎস দেখানো বাধ্যতামূলক।
বই, জার্নাল, ওয়েবসাইট বা গবেষণাপত্রের রেফারেন্স সঠিকভাবে ব্যবহার করা।

২. নিজের ভাষায় লেখা (Paraphrasing)
তথ্য বোঝার পর নিজের শব্দে লেখা।
শুধু শব্দ পরিবর্তন নয়, সম্পূর্ণভাবে ধারণা নিজের মতো করে উপস্থাপন করা।

৩. অনলাইন টুল ব্যবহার (Plagiarism Checker)
Turnitin, Grammarly, Plagscan ইত্যাদি ব্যবহার করে লেখা যাচাই।
অনুরূপ অংশ থাকলে তা সংশোধন করা।

৪. নিয়মিত সচেতনতা (Awareness & Training)
শিক্ষার্থী ও গবেষকরা নৈতিকতার প্রতি সচেতন থাকা।
Plagiarism-এর ক্ষতি ও আইনগত পরিণতি বোঝা।

৫. ডকুমেন্টেশন ও ব্যাকআপ (Proper Documentation & Backup)
গবেষণা বা প্রবন্ধের সব নোট, রেফারেন্স ও সূত্র সংরক্ষণ করা।
ভবিষ্যতে যাচাই সহজ হয়।

৬.১৫ Phishing (ফিশিং)

Phishing হলো একধরনের সাইবার আক্রমণ যেখানে হ্যাকার ভুয়া ইমেইল, বার্তা, বা ওয়েবসাইট ব্যবহার করে ব্যবহারকারীর ব্যক্তিগত তথ্য (যেমন পাসওয়ার্ড, ক্রেডিট কার্ড নম্বর, ব্যাংক তথ্য) চুরি করে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৫.১ Phishing-এর ধরন

Phishing-এর সাধারণ ধরন নিচে দেয়া হলো– প্রতিটি ধরন আক্রমণের কৌশল ও মাধ্যম অনুযায়ী আলাদা:

১. **Email Phishing (ইমেইল ফিশিং)**
কী: ভুয়া ইমেইল পাঠিয়ে ব্যবহারকারীর তথ্য চুরি।
উদাহরণ: ব্যাংকের নামে ইমেইল পাঠিয়ে লগইন লিঙ্কে ক্লিক করানো।

২. **Spear Phishing (টার্গেটেড ফিশিং)**
কী: নির্দিষ্ট ব্যক্তি বা প্রতিষ্ঠানের জন্য লক্ষ্যভিত্তিক আক্রমণ।
উদাহরণ: কোম্পানির কোনো কর্মীর তথ্য সংগ্রহ করে সেই অনুযায়ী ভুয়া ইমেইল পাঠানো।

৩. **Smishing (এসএমএস ফিশিং)**
কী: মোবাইল বার্তার মাধ্যমে ফিশিং।
উদাহরণ: পুরস্কার জেতার SMS পাঠিয়ে ভুয়া লিঙ্কে পাঠানো।

৪. **Vishing (ভয়েস ফিশিং)**
কী: ফোন কলের মাধ্যমে ব্যক্তিগত তথ্য নেয়া।
উদাহরণ: নিজেকে ব্যাংক কর্মকর্তা বলে OTP বা PIN চাওয়া।

৫. **Clone Phishing (ক্লোন ফিশিং)**
কী: আগে পাঠানো আসল ইমেইলের কপি বানিয়ে তাতে ক্ষতিকর লিঙ্ক যোগ করা।
উদাহরণ: অফিসের আসল মেইলের মতো একটি মেইল বানিয়ে পাঠানো।

৬.১৫.২ Phishing প্রতিরোধের উপায়

Phishing প্রতিরোধের উপায় মানে হলো সেই পদক্ষেপগুলো যা নিলে ভুয়া ইমেইল, বার্তা বা ওয়েবসাইটের মাধ্যমে তথ্য চুরি রোধ করা যায়।

১. **ইমেইল ও লিঙ্ক যাচাই করা**
সন্দেহজনক বা অচেনা ইমেইল খোলা যাবে না।
লিঙ্কে ক্লিক করার আগে মাউস দিয়ে হোভার করে আসল URL দেখুন।

২. **ওয়েবসাইটের নিরাপত্তা পরীক্ষা**
শুধুমাত্র HTTPS যুক্ত ওয়েবসাইট ব্যবহার করতে হবে।
প্যাডলক আইকন আছে কিনা দেখতে হবে।

৩. **দুই-স্তরের প্রমাণীকরণ (2FA) ব্যবহার**
লগইনের সময় পাসওয়ার্ডের পাশাপাশি OTP ব্যবহার করতে হবে।
পাসওয়ার্ড চুরি হলেও অ্যাকাউন্ট সুরক্ষিত থাকবে।

৪. **সফটওয়্যার ও ব্রাউজার আপডেট রাখা**
নিরাপত্তা দুর্বলতা (security vulnerabilities) বন্ধ করতে আপডেট জরুরি।

৫. **অ্যান্টি-ফিশিং ও অ্যান্টিভাইরাস ব্যবহার**
ইমেইল ও ব্রাউজারে ফিশিং ফিল্টার চালু রাখতে হবে।
অ্যান্টিভাইরাস রিয়েল-টাইম প্রোটেকশন সক্রিয় রাখতে হবে।

৬. **ব্যক্তিগত তথ্য কখনো প্রকাশ না করা**
ফোন, ইমেইল বা SMS-এর মাধ্যমে ব্যাংক বা পাসওয়ার্ড সম্পর্কিত তথ্য দেয়া যাবে না।
বৈধ প্রতিষ্ঠান কখনো এভাবে তথ্য চায় না।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৬ Software Piracy

Software Piracy (সফটওয়্যার পাইরেসি) হলো সফটওয়্যার অবৈধভাবে কপি, বিতরণ বা ব্যবহার করা, যা কপিরাইট আইন লঙ্ঘন করে। এটি একধরনের বৌদ্ধিক সম্পত্তি চুরি এবং অনেক দেশে এটি অপরাধ।

৬.১৬.১ Software Piracy-এর ধরন

Software Piracy-এর ধরন মূলত সফটওয়্যার অবৈধভাবে ব্যবহার, কপি বা বিতরণের পদ্ধতির ওপর ভিত্তি করে ভাগ করা হয়। নিচে প্রধান ধরনগুলো দেয়া হলো–

১. **End-User Piracy (এন্ড-ইউজার পাইরেসি)**
কী: ব্যবহারকারী লাইসেন্স ছাড়া সফটওয়্যার কপি বা ইনস্টল করে ব্যবহার করে।
উদাহরণ: একটি লাইসেন্স দিয়ে একাধিক কম্পিউটারে সফটওয়্যার চালানো।

২. **Counterfeiting (জালিয়াতি)**
কী: সফটওয়্যার, প্যাকেজিং ও লোগো নকল করে আসল হিসেবে বিক্রি করা।
উদাহরণ: নকল MS Office সিডি বিক্রি করা।

৩. **Internet Piracy (ইন্টারনেট পাইরেসি)**
কী: ইন্টারনেটের মাধ্যমে অবৈধভাবে সফটওয়্যার ডাউনলোড, শেয়ার বা বিক্রি করা।
উদাহরণ: টরেন্ট থেকে ক্র্যাক করা সফটওয়্যার ডাউনলোড।

৪. **Client-Server Overuse (ক্লায়েন্ট-সার্ভার ওভারইউজ)**
কী: একটি সার্ভারে সীমিত লাইসেন্স থাকা সত্ত্বেও বেশিসংখ্যক ব্যবহারকারীকে অ্যাক্সেস দেয়া।
উদাহরণ: ৫ জনের লাইসেন্স দিয়ে ২০ জন ব্যবহার করছে।

৫. **Hard-Disk Loading (হার্ড-ডিস্ক লোডিং)**
কী: কম্পিউটার বিক্রেতা নতুন পিসিতে অবৈধ সফটওয়্যার ইনস্টল করে ক্রেতাকে দেওয়া।
উদাহরণ: নতুন ল্যাপটপে ফ্রি ক্র্যাক করা গেমস বা সফটওয়্যার দেওয়া।

৬.১৬.২ Software Piracy চিহ্নিত করার উপায়

Software Piracy চিহ্নিত করার উপায় হলো সেই পদ্ধতিগুলো যা ব্যবহার করে বোঝা যায় কোন সফটওয়্যার আসল (licensed) নাকি অবৈধ (pirated)। নিচে প্রধান উপায়গুলো দেয়া হলো–

১. **লাইসেন্স কী বা অ্যাক্টিভেশন যাচাই করা**
সফটওয়্যার ইনস্টল করার সময় বৈধ লাইসেন্স কী বা অ্যাক্টিভেশন কোড আছে কিনা পরীক্ষা করা।
ক্র্যাক করা বা জেনারেট করা কী থাকলে সেটা অবৈধ হতে পারে।

২. **প্যাকেজিং ও লোগো যাচাই করা**
আসল সফটওয়্যার সাধারণত সঠিক লোগো, হোলোগ্রাম, সিল ও ডকুমেন্টেশনসহ আসে।
নকল সফটওয়্যারের প্যাকেজিং সস্তা বা অস্বাভাবিক মানের হতে পারে।

৩. **মূল্য যাচাই করা**
বাজার মূল্যের তুলনায় অস্বাভাবিকভাবে কম দামে বিক্রি হলে সেটি সন্দেহজনক।

৪. **সোর্স যাচাই করা**
সফটওয়্যার অফিসিয়াল ওয়েবসাইট বা অনুমোদিত বিক্রেতা থেকে কেনা উচিত।
অজানা ওয়েবসাইট বা টরেন্ট থেকে ডাউনলোডকৃত সফটওয়্যার অধিকাংশ সময় পাইরেটেড হয়।

৫. **ফিচার ও আপডেট চেক করা**
পাইরেটেড সফটওয়্যারে প্রায়শই কিছু ফিচার কাজ করে না এবং আপডেট বন্ধ থাকে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. **"Direct Plagiarism" বলতে কী বোঝায়?**
   ক. নিজের কাজ জমা দেয়া খ. সরাসরি কপি করা
   গ. সূত্র উল্লেখ করা ঘ. তথ্য বিশ্লেষণ

২. **ফিশিং আক্রমণের মাধ্যমে কী চুরি হয়?**
   ক. সফটওয়্যার খ. হার্ডওয়্যার
   গ. ব্যক্তিগত তথ্য ঘ. বই

৩. **"Email Phishing" বলতে কী বোঝায়?**
   ক. এসএমএস ফিশিং খ. ভয়েস কল
   গ. ইমেইলের মাধ্যমে তথ্য চুরি ঘ. ওয়েবসাইট ফিশিং

৪. **সফটওয়্যার পাইরেসি কী?**
   ক. সফটওয়্যারকে দ্রুত করা খ. অবৈধভাবে সফটওয়্যার কপি/বিতরণ
   গ. সফটওয়্যারের ব্যাকআপ রাখা ঘ. সফটওয়্যার বিক্রয়

উত্তরমালা : ১. খ; ২. গ; ৩. গ; ৪. খ।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. Plagiarism হলো একধরনের ....., যেখানে অন্যের লেখা, ধারণা বা গবেষণার ফলাফলকে নিজের নামে উপস্থাপন করা হয়।
উত্তর : বৌদ্ধিক চুরি

২. নিজের পুরনো লেখা নতুন কাজ হিসেবে জমা দেওয়াকে ..... Plagiarism বলে।
উত্তর : Self-Plagiarism (নিজের পুনঃপ্রকাশ)

৩. ভুয়া ইমেইল পাঠিয়ে ব্যবহারকারীর ব্যক্তিগত তথ্য চুরি করাকে ..... Phishing বলে।
উত্তর : Email Phishing (ইমেইল ফিশিং)

৪. সফটওয়্যার অবৈধভাবে কপি, বিতরণ বা ব্যবহার করাকে ..... বলা হয়।
উত্তর : সফটওয়্যার পাইরেসি (Software Piracy)

৫. একটি বৈধ লাইসেন্স দিয়ে একাধিক কম্পিউটারে সফটওয়্যার চালানো হলে তা ..... Piracy হিসেবে গণ্য হয়
উত্তর : End-User Piracy (এন্ড-ইউজার পাইরেসি)

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. Direct Plagiarism	ক. Turnitin, Grammarly, Plagscan ইত্যাদি টুল ব্যবহার।
২. Self-Plagiarism	খ. উদ্ধৃতি বা সূত্র উল্লেখ না করা।
৩. Mosaic Plagiarism	গ. কিছু শব্দ পরিবর্তন করে মূল ধারণা চুরি করা।
৪. Accidental Plagiarism	ঘ. নিজের পূর্বের লেখা নতুন কাজ হিসেবে জমা দেওয়া।
৫. অনলাইন প্ল্যাজিয়ার চেকার	ঙ. অন্যের লেখা বা কাজ সম্পূর্ণ বা আংশিক অনুলিপি করা।

উত্তরমালা : ১→ঙ, ২→ঘ, ৩→গ, ৪→খ, ৫→ক

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. Plagiarism কী?
২. Phishing (ফিশিং) কী?
৩. Plagiarism এর দুটি ধরন লেখো।
৪. Plagiarism চিহ্নিত করার দুটি উপায় লেখো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৫. Plagiarism প্রতিরোধের দুটি উপায় লেখো।
৬. Phishing এর দুটি ধরন লেখো।
৭. Phishing প্রতিরোধের দুটি উপায় লেখো।
৮. সফটওয়্যার পাইরেসি কী?
৯. সফটওয়্যার পাইরেসির দুটি ধরন লেখো।
১০. Software Piracy চিহ্নিত করার দুটি উপায় লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. Plagiarism-এর প্রধান ধরনগুলো কী কী?
২. সরাসরি নকল ও নিজের পুনঃপ্রকাশের মধ্যে পার্থক্য লেখো।
৩. মিশ্র/প্যাটার্ন নকল ও অজান্তে নকল কীভাবে চিহ্নিত করা যায়?
৪. Plagiarism চিহ্নিত করার প্রধান পদ্ধতিগুলো কী কী?
৫. Plagiarism প্রতিরোধের উপায়গুলো কী কী?
৬. ফিশিং-এর প্রধান ধরনগুলো কী কী?
৭. ইমেইল ফিশিং ও টার্গেটেড ফিশিং-এর উদাহরণ দাও।
৮. ফিশিং প্রতিরোধের প্রধান উপায়গুলো কী কী?
৯. Software Piracy (সফটওয়্যার পাইরেসি) কী?
১০. সফটওয়্যার পাইরেসি চিহ্নিত করার প্রধান পদ্ধতিগুলো কী কী?

চ. দৃশ্যকল্প-ভিত্তিক প্রশ্ন :

১. রাহিম তার অনার্স ক্লাসে একটি গবেষণাপত্র জমা দিয়েছে। শিক্ষক পরে দেখলেন, পুরো লেখাটিই একটি অনলাইন জার্নাল থেকে কপি করা হয়েছে এবং কোনো উৎস উল্লেখ করা হয়নি।
প্রশ্ন : এখানে কোন ধরনের প্ল্যাজিয়ারিজম ঘটেছে? এর শিক্ষাগত ক্ষতি কী হতে পারে এবং প্রতিরোধে রাহিম কী করতে পারত?

২. একজন ব্যাংক গ্রাহককে একটি ইমেইল পাঠানো হলো, যেখানে লেখা ছিল– "আপনার অ্যাকাউন্ট লক হয়ে গেছে। পুনরায় চালু করতে এখানে ক্লিক করুন।" গ্রাহক ক্লিক করে তার ইউজার আইডি ও পাসওয়ার্ড দিল, কিছুক্ষণ পর তার ব্যাংক অ্যাকাউন্ট থেকে টাকা চুরি হয়ে গেল।
প্রশ্ন : এখানে কোন ধরনের ফিশিং আক্রমণ ঘটেছে? গ্রাহকের কী ক্ষতি হলো এবং ভবিষ্যতে এ ধরনের আক্রমণ থেকে কীভাবে বাঁচা যায়?

৩. একটি কম্পিউটার দোকান নতুন ল্যাপটপ বিক্রির সময় ক্রেতাকে আকৃষ্ট করতে ফ্রি-তে কিছু সফটওয়্যার ইনস্টল করে দেয়। পরে দেখা গেল এগুলো আসলে ক্র্যাক করা পাইরেটেড সফটওয়্যার।
প্রশ্ন : এখানে কোন ধরনের সফটওয়্যার পাইরেসি হয়েছে? এর ফলে ক্রেতা ও প্রতিষ্ঠানের কী ধরনের ঝুঁকি হতে পারে এবং প্রতিরোধের উপায় কী?

ছ. বর্ণনামূলক প্রশ্ন :

১. Plagiarism কী এবং শিক্ষাগত ও পেশাগত ক্ষেত্রে এর ক্ষতি ব্যাখ্যা করো।
২. Plagiarism-এর ধরনগুলো বিস্তারিতভাবে আলোচনা করো।
৩. Plagiarism চিহ্নিত করার জন্য অনলাইন টুল এবং উৎস যাচাইয়ের গুরুত্ব ব্যাখ্যা করো।
৪. Plagiarism প্রতিরোধে উদ্ধৃতি ব্যবহার এবং নিজের ভাষায় লেখা কেন গুরুত্বপূর্ণ তা ব্যাখ্যা করো।
৫. Phishing (ফিশিং) কী এবং এটি ব্যবহারকারীর তথ্য চুরি করতে কীভাবে সাহায্য করে তা ব্যাখ্যা করো।
৬. ফিশিং-এর ধরন (ইমেইল, টার্গেটেড, এসএমএস, ভয়েস, ক্লোন ফিশিং) উদাহরণসহ ব্যাখ্যা করো।
৭. ফিশিং প্রতিরোধে ইমেইল যাচাই, দুই-স্তরের প্রমাণীকরণ এবং সফটওয়্যার আপডেটের ভূমিকা ব্যাখ্যা করো।
৮. Software Piracy কী এবং এটি কম্পিউটার ও নেটওয়ার্কে কীভাবে ক্ষতি করে তা ব্যাখ্যা করো।
৯. সফটওয়্যার পাইরেসি-এর ধরন (এন্ড-ইউজার, জালিয়াতি, ইন্টারনেট পাইরেসি, ক্লায়েন্ট-সার্ভার ওভারইউজ, হার্ড-ডিস্ক লোডিং) উদাহরণসহ ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৭.১ Virus (ভাইরাস)

কম্পিউটার ভাইরাস হলো একধরনের ক্ষতিকর প্রোগ্রাম যা কোনো ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায় এবং সিস্টেমে ক্ষতি করে। এটি সক্রিয় হতে হলে আক্রান্ত ফাইল চালু করতে হয়।

৬.১৭.১.১ কম্পিউটার ভাইরাস এর বৈশিষ্ট্য :

১. **ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়** – ভাইরাস সবসময় কোনো বৈধ ফাইল, প্রোগ্রাম বা ডকুমেন্টের সাথে লুকিয়ে থাকে।
২. **সক্রিয় হতে ইউজারের অ্যাকশন প্রয়োজন** – আক্রান্ত ফাইল চালানো বা খোলার পরই ভাইরাস সক্রিয় হয়।
৩. **নিজে নিজে ছড়াতে পারে না** – এটি শুধু সংক্রমিত ফাইল বা মিডিয়ার মাধ্যমে ছড়ায়।
৪. **ডাটা ও ফাইল ক্ষতি করে** – ফাইল মুছে ফেলা, ডাটা নষ্ট করা বা পরিবর্তন করা।
৫. **সিস্টেমের কর্মক্ষমতা কমায়** – কম্পিউটার ধীর করে দেয়, হ্যাং বা ক্র্যাশ করতে পারে।
৬. **বিভিন্ন মাধ্যম দিয়ে ছড়ায়** – ইমেইল অ্যাটাচমেন্ট, ইউএসবি, CD/DVD, ইন্টারনেট ডাউনলোড ইত্যাদি।
৭. **অ্যান্টিভাইরাস দিয়ে শনাক্ত ও মুছা যায়** - তবে নতুন ভাইরাস শনাক্ত না হলে তা বিপজ্জনক হতে পারে।

৬.১৭.২ Worm (ওয়ার্ম)

ওয়ার্ম হলো স্বয়ংক্রিয়ভাবে নিজেকে নেটওয়ার্কের মাধ্যমে কপি ও ছড়াতে সক্ষম একটি ক্ষতিকারক প্রোগ্রাম। এটি ছড়াতে ইউজারের কোনো অ্যাকশন প্রয়োজন হয় না।

১৭.২.১ ওয়ার্ম এর বৈশিষ্ট্য :

নিজে নিজেই ছড়াতে পারে – কোনো ফাইল বা প্রোগ্রামের সাথে যুক্ত না হয়েও স্বয়ংক্রিয়ভাবে ছড়ায়।
ইউজারের অ্যাকশন প্রয়োজন হয় না – সক্রিয় হতে ফাইল চালানো বা খোলার দরকার নেই।
৩. **নেটওয়ার্কভিত্তিক বিস্তার** – ইন্টারনেট বা লোকাল নেটওয়ার্কের মাধ্যমে দ্রুত ছড়ায়।
৪. **ব্যান্ডউইথ খরচ করে** – অতিরিক্ত নেটওয়ার্ক ট্রাফিক তৈরি করে ইন্টারনেট স্লো করে দেয়।
৫. **সিস্টেম ও নেটওয়ার্ক ক্ষতি করে** – নেটওয়ার্ক ডাউন, সার্ভার ক্র্যাশ এবং অন্যান্য ম্যালওয়্যার ইনস্টল করতে পারে।
৬. **নিজেকে কপি করে** – একাধিক কপি তৈরি করে অন্য সিস্টেমে পাঠায়।
৭. **ফায়ারওয়াল ও সিকিউরিটি দুর্বলতাকে কাজে লাগায়** – সিস্টেমের নিরাপত্তা ফাঁক ব্যবহার করে আক্রমণ করে।

৬.১৭.২.২ Virus ও Worm-এর মধ্যে পার্থক্য

বৈশিষ্ট্য	Virus (ভাইরাস)	Worm (ওয়ার্ম)
বিস্তার পদ্ধতি	ফাইল/প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায়	নিজে নিজেই নেটওয়ার্কে ছড়ায়
সক্রিয় হওয়ার শর্ত	ইউজারের অ্যাকশন (ফাইল চালানো) প্রয়োজন	ইউজারের অ্যাকশন প্রয়োজন নেই
ক্ষতির ধরন	ফাইল নষ্ট, ডেটা চুরি, সিস্টেম ক্র্যাশ	নেটওয়ার্ক স্লো, ব্যান্ডউইথ খরচ
উদাহরণ	ILOVEYOU, Melissa	Conficker, Mydoom

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৭.১ Virus (ভাইরাস)

কম্পিউটার ভাইরাস হলো একধরনের ক্ষতিকর প্রোগ্রাম যা কোনো ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায় এবং সিস্টেমে ক্ষতি করে। এটি সক্রিয় হতে হলে আক্রান্ত ফাইল চালু করতে হয়।

৬.১৭.১.১ কম্পিউটার ভাইরাস এর বৈশিষ্ট্য :

১. **ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়** – ভাইরাস সবসময় কোনো বৈধ ফাইল, প্রোগ্রাম বা ডকুমেন্টের সাথে লুকিয়ে থাকে।
২. **সক্রিয় হতে ইউজারের অ্যাকশন প্রয়োজন** – আক্রান্ত ফাইল চালানো বা খোলার পরই ভাইরাস সক্রিয় হয়।
৩. **নিজে নিজে ছড়াতে পারে না** – এটি শুধু সংক্রমিত ফাইল বা মিডিয়ার মাধ্যমে ছড়ায়।
৪. **ডাটা ও ফাইল ক্ষতি করে** – ফাইল মুছে ফেলা, ডাটা নষ্ট করা বা পরিবর্তন করা।
৫. **সিস্টেমের কর্মক্ষমতা কমায়** – কম্পিউটার ধীর করে দেয়, হ্যাং বা ক্র্যাশ করতে পারে।
৬. **বিভিন্ন মাধ্যম দিয়ে ছড়ায়** – ইমেইল অ্যাটাচমেন্ট, ইউএসবি, CD/DVD, ইন্টারনেট ডাউনলোড ইত্যাদি।
৭. **অ্যান্টিভাইরাস দিয়ে শনাক্ত ও মুছা যায়** - তবে নতুন ভাইরাস শনাক্ত না হলে তা বিপজ্জনক হতে পারে।

৬.১৭.২ Worm (ওয়ার্ম)

ওয়ার্ম হলো স্বয়ংক্রিয়ভাবে নিজেকে নেটওয়ার্কের মাধ্যমে কপি ও ছড়াতে সক্ষম একটি ক্ষতিকারক প্রোগ্রাম। এটি ছড়াতে ইউজারের কোনো অ্যাকশন প্রয়োজন হয় না।

৬.১৭.২.১ ওয়ার্ম এর বৈশিষ্ট্য :

১. **নিজে নিজেই ছড়াতে পারে** – কোনো ফাইল বা প্রোগ্রামের সাথে যুক্ত না হয়েও স্বয়ংক্রিয়ভাবে ছড়ায়।
২. **ইউজারের অ্যাকশন প্রয়োজন হয় না** – সক্রিয় হতে ফাইল চালানো বা খোলার দরকার নেই।
৩. **নেটওয়ার্কভিত্তিক বিস্তার** – ইন্টারনেট বা লোকাল নেটওয়ার্কের মাধ্যমে দ্রুত ছড়ায়।
৪. **ব্যান্ডউইথ খরচ করে** – অতিরিক্ত নেটওয়ার্ক ট্রাফিক তৈরি করে ইন্টারনেট স্লো করে দেয়।
৫. **সিস্টেম ও নেটওয়ার্ক ক্ষতি করে** – নেটওয়ার্ক ডাউন, সার্ভার ক্র্যাশ এবং অন্যান্য ম্যালওয়্যার ইনস্টল করতে পারে।
৬. **নিজেকে কপি করে** – একাধিক কপি তৈরি করে অন্য সিস্টেমে পাঠায়।
৭. **ফায়ারওয়াল ও সিকিউরিটি দুর্বলতাকে কাজে লাগায়** – সিস্টেমের নিরাপত্তা ফাঁক ব্যবহার করে আক্রমণ করে।

৬.১৭.২.২ Virus ও Worm-এর মধ্যে পার্থক্য

বৈশিষ্ট্য	Virus (ভাইরাস)	Worm (ওয়ার্ম)
বিস্তার পদ্ধতি	ফাইল/প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায়	নিজে নিজেই নেটওয়ার্কে ছড়ায়
সক্রিয় হওয়ার শর্ত	ইউজারের অ্যাকশন (ফাইল চালানো) প্রয়োজন	ইউজারের অ্যাকশন প্রয়োজন নেই
ক্ষতির ধরন	ফাইল নষ্ট, ডেটা চুরি, সিস্টেম ক্র্যাশ	নেটওয়ার্ক স্লো, ব্যান্ডউইথ খরচ
উদাহরণ	ILOVEYOU, Melissa	Conficker, Mydoom

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৭.২.৩ Virus এবং Worm-এর প্রতিরোধের উপায়

Virus এবং Worm-এর প্রতিরোধের উপায় হলো সিস্টেম ও নেটওয়ার্ককে সুরক্ষিত রাখা এবং সচেতন ব্যবহার নিশ্চিত করা। নিচে মূল পদ্ধতিগুলো দেয়া হলো–

১. **অ্যান্টিভাইরাস ব্যবহার ও নিয়মিত আপডেট**
সর্বদা আপডেটেড অ্যান্টিভাইরাস ব্যবহার করা।
স্ক্যানিং চালিয়ে ভাইরাস বা ওয়ার্ম শনাক্ত করা।

২. **ফায়ারওয়াল চালু রাখা**
নেটওয়ার্কে অননুমোদিত প্রবেশ বন্ধ করতে ফায়ারওয়াল ব্যবহার।

৩. **অচেনা ইমেইল ও অ্যাটাচমেন্ট না খোলা**
অজানা সোর্সের ইমেইল, লিঙ্ক বা ফাইল ক্লিক না করা।
ভাইরাস/ওয়ার্মের মূল প্রবেশদ্বার প্রতিরোধ।

৪. **সফটওয়্যার ও OS আপডেট রাখা**
নিরাপত্তার দুর্বলতা দূর করতে নিয়মিত আপডেট।

৫. **ব্যাকআপ রাখা**
গুরুত্বপূর্ণ ফাইল নিয়মিত ব্যাকআপে রাখা।
সংক্রমণের ক্ষেত্রে দ্রুত পুনরুদ্ধার সম্ভব।

৬. **নেটওয়ার্ক নিরাপত্তা**
পাবলিক Wi-Fi এ সংবেদনশীল কাজ না করা।
VPN ব্যবহার করে ডেটা এনক্রিপ্ট করা।

৬.১৮ Spam (স্প্যাম)

Spam (স্প্যাম) হলো অনাবশ্যক বা অবাঞ্ছিত ইমেইল, মেসেজ; বা অনলাইন বার্তা যা সাধারণত প্রমোশন, বিজ্ঞাপন, স্ক্যাম বা ম্যালওয়্যার ছড়ানোর উদ্দেশ্যে পাঠানো হয়।

৬.১৮.১ Spam-এর বৈশিষ্ট্য

১. **অবাঞ্ছিত বার্তা (Unsolicited Messages)**
প্রাপক চাইছেন না এমন ইমেইল, SMS বা অনলাইন বার্তা।

২. **বৃহৎ পরিমাণে প্রেরণ (Bulk Sending)**
একই বার্তা অনেক ব্যবহারকারীর কাছে পাঠানো হয়।

৩. **বিজ্ঞাপন বা প্রমোশনমূলক (Promotional Content)**
পণ্য, সার্ভিস বা ওয়েবসাইট প্রচারের উদ্দেশ্য থাকে।

৪. **স্ক্যাম বা ম্যালওয়্যার লিঙ্ক (Malicious Links)**
প্রায়ই ভাইরাস, ওয়ার্ম বা ফিশিং লিঙ্ক সংযুক্ত থাকে।

৫. **নির্দিষ্ট লক্ষ্যহীন (Non-Targeted)**
প্রায়ই যেকোনো ব্যবহারকারীকে পাঠানো হয়, ব্যক্তিগত না।

৬. **বারবার প্রেরণ (Repeated Sending)**
একই বার্তা অনেকবার পাঠানো হতে পারে।

৭. **সন্দেহজনক সোর্স (Suspicious Source)**
প্রেরকের ঠিকানা বা নাম ভুয়া বা অজানা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.১৮.২ Spam-এর ধরন

Spam-এর ধরন মূলত বার্তা প্রেরণের মাধ্যম এবং উদ্দেশ্য অনুযায়ী ভাগ করা যায়। নিচে প্রধান ধরনগুলো দেয়া হলো–

১. **Email Spam (ইমেইল স্প্যাম)**
কী: অজানা ইমেইল ঠিকানায় প্রচুর বিজ্ঞাপন বা স্ক্যাম বার্তা পাঠানো।
উদাহরণ: অফার বা পুরস্কারের নামে ভুয়া ইমেইল।

২. **SMS Spam (এসএমএস স্প্যাম)**
কী: মোবাইলে অপ্রয়োজনীয় বা অবাঞ্ছিত বার্তা পাঠানো।
উদাহরণ: "আপনি জিতেছেন" বা প্রমোশনাল মেসেজ।

৩. **Social Media Spam (সোশ্যাল মিডিয়া স্প্যাম)**
কী: ফেসবুক, ইনস্টাগ্রাম, টুইটার ইত্যাদিতে অবাঞ্ছিত পোস্ট, লিঙ্ক বা বিজ্ঞাপন।
উদাহরণ: ভুয়া প্রতিযোগিতা বা ফ্রি গিফট অফার।

৪. **Comment Spam (কমেন্ট স্প্যাম)**
কী: ব্লগ, ফোরাম বা ওয়েবসাইটে অপ্রয়োজনীয় মন্তব্য বা লিঙ্ক দেয়া।
উদাহরণ: "Click here for free software" বা অপ্রাসঙ্গিক লিঙ্ক।

৬.১৮.৩ Spam প্রতিরোধের উপায়

Spam প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে অপ্রয়োজনীয় বা ক্ষতিকারক বার্তা থেকে রক্ষা পাওয়া যায়।

১. **স্প্যাম ফিল্টার ব্যবহার (Use Spam Filter)**
ইমেইল বা মেসেজের স্প্যাম ফিল্টার চালু রাখা।
Gmail, Yahoo, Outlook-এর স্প্যাম ফিল্টার কার্যকর।

২. **অজানা লিঙ্ক ও অ্যাটাচমেন্ট এড়ানো**
অচেনা ইমেইল, SMS বা সোশ্যাল মিডিয়ার লিঙ্কে ক্লিক না করা।
সন্দেহজনক ফাইল ডাউনলোড না করা।



ছবি উৎস : https://bloomidea.com

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৩. ব্যক্তিগত তথ্য শেয়ার না করা
ফোন নম্বর, ইমেইল বা ব্যাংক তথ্য অজানা সোর্সের কাছে না দেয়া।

৪. অ্যান্টি-স্প্যাম সফটওয়্যার ব্যবহার
কম্পিউটার বা মোবাইলে অ্যান্টি-স্প্যাম প্রোগ্রাম ইনস্টল করা।

৫. অ্যাকাউন্ট নিরাপত্তা বাড়ানো
শক্তিশালী পাসওয়ার্ড এবং দুই-স্তরের প্রমাণীকরণ (2FA) ব্যবহার।

৬. নিয়মিত সচেতনতা
স্প্যাম ও ফিশিং সম্পর্কিত সতর্কতা বজায় রাখা।
নতুন ধরণের স্প্যাম বা স্ক্যাম সম্পর্কে অবহিত থাকা।

৬.১৯ Adware (অ্যাডওয়্যার)

Adware (অ্যাডওয়্যার) হলো একধরনের সফটওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়া বিজ্ঞাপন দেখায় বা পপ-আপ তৈরি করে। এটি প্রায়ই ফ্রি সফটওয়্যারের সাথে যুক্ত থাকে এবং ব্যবহারকারীর ব্রাউজিং অভিজ্ঞতা বা সিস্টেমের কর্মক্ষমতাকে প্রভাবিত করতে পারে।

৬.১৯.১ Adware (অ্যাডওয়্যার)-এর বৈশিষ্ট্য

১. অবাঞ্ছিত বিজ্ঞাপন দেখানো (Displays Unwanted Ads)
পপ-আপ, ব্যানার বা ভিডিও আকারে বারবার বিজ্ঞাপন প্রদর্শন করে।

২. ফ্রি সফটওয়্যারের সঙ্গে আসে (Bundled with Free Software)
সাধারণত বিনামূল্যে সফটওয়্যারের অংশ হিসেবে ইনস্টল হয়।

৩. ব্যবহারকারীর অনুমতি ছাড়া তথ্য সংগ্রহ (Tracks User Behavior)
ব্রাউজিং হিস্ট্রি, সার্চ প্যাটার্ন বা ব্যবহার পছন্দ পর্যবেক্ষণ করে।

৪. সিস্টেম ধীর করে দেয় (Slows Down System)
RAM ও CPU ব্যবহার বাড়িয়ে কম্পিউটার বা ব্রাউজারের কর্মক্ষমতা কমায়।

৫. ফাইল বা ডেটা সরাসরি ক্ষতি করে না (Usually Non-Destructive)
সাধারণত ডেটা ক্ষতি করে না, তবে ম্যালওয়্যারের জন্য পথ খুলতে পারে।

৬. ব্রাউজারের আচরণ পরিবর্তন করে (Alters Browser Behavior)
হোমপেজ, ডিফল্ট সার্চ ইঞ্জিন বা নতুন ট্যাব সেটিং পরিবর্তন করতে পারে।

৬.১৯.২ Adware (অ্যাডওয়্যার)-এর ধরন

Adware-এর ধরন মূলত কাজের ধরন এবং বিজ্ঞাপন প্রদর্শনের পদ্ধতির উপর ভিত্তি করে ভাগ করা হয়।

১. Browser Hijackers (ব্রাউজার হাইজকার)
কী: ব্রাউজারের হোমপেজ, নতুন ট্যাব বা ডিফল্ট সার্চ ইঞ্জিন পরিবর্তন করে।
উদাহরণ: হোমপেজে অবাঞ্ছিত সার্চ বার বা পপ-আপ যোগ করা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

২. **Pop-up Adware (পপ-আপ অ্যাডওয়্যার)**
কী: ব্যবহারকারীর ব্রাউজারে বারবার পপ-আপ বিজ্ঞাপন দেখায়।
উদাহরণ: ভিডিও, ইমেজ বা ব্যানার পপ-আপ।

৩. **Tracking Adware (ট্র্যাকিং অ্যাডওয়্যার)**
কী: ব্যবহারকারীর ব্রাউজিং হিস্ট্রি, সার্চ প্যাটার্ন বা অন্যান্য তথ্য সংগ্রহ করে।
উদাহরণ: অনলাইন বিজ্ঞাপন লক্ষ্যভিত্তিকভাবে দেখানো।

৬.১৯.৩ Adware প্রতিরোধের উপায়

Adware প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে ব্যবহারকারীর কম্পিউটার বা ব্রাউজারে অবাঞ্ছিত বিজ্ঞাপন বা ট্র্যাকিং থেকে রক্ষা পাবে।

১. **সতর্কভাবে সফটওয়্যার ইনস্টল করা**
নতুন সফটওয়্যার ইনস্টল করার সময় "Custom" বা "Advanced" অপশন ব্যবহার করতে হবে।
অনাকাঙ্ক্ষিত প্রোগ্রাম বা অ্যাডওয়্যার ইনস্টল হওয়া থেকে রোধ করা।

২. **অ্যান্টি-অ্যাডওয়্যার সফটওয়্যার ব্যবহার**
Malwarebytes, AdwCleaner ইত্যাদি ব্যবহার করে সিস্টেম স্ক্যান করতে হবে।

৩. **সন্দেহজনক সফটওয়্যার ডাউনলোড এড়ানো**
অজানা ও অনিরাপদ ওয়েবসাইট থেকে সফটওয়্যার ডাউনলোড করা যাবে না।

৪. **ব্রাউজার এক্সটেনশন নিয়মিত পরীক্ষা করা**
অচেনা বা অপ্রয়োজনীয় এক্সটেনশন মুছে দিতে হবে।

৫. **ব্রাউজার ও সফটওয়্যার আপডেট রাখা**
নিরাপত্তা ফাঁক বন্ধ রাখতে সব সফটওয়্যার ও ব্রাউজার আপডেট রাখতে হবে।

৬. **ব্যবহারকারীর তথ্য শেয়ার সীমিত করা**
ব্যক্তিগত তথ্য, ব্রাউজিং হিস্ট্রি বা পছন্দের তথ্য শুধুমাত্র বিশ্বাসযোগ্য সাইটে ব্যবহার করতে হবে।

৬.২০ Malware (ম্যালওয়্যার)

Malware (ম্যালওয়্যার) হলো একধরনের ক্ষতিকারক সফটওয়্যার যা কম্পিউটার, মোবাইল বা নেটওয়ার্কে অননুমানিক ক্ষতি বা অযোগ্য কার্যক্রম ঘটায়। এটি "malicious software" বা দুষ্ট সফটওয়্যারের সংক্ষিপ্ত রূপ।

৬.২০.১ Malware (ম্যালওয়্যার)-এর বৈশিষ্ট্য

১. **ক্ষতিকারক কার্যক্রম (Harmful Behavior)**
কম্পিউটার বা ডিভাইসে ডেটা চুরি, ফাইল ক্ষতি বা সিস্টেম ধীরগতির কারণ হতে পারে।

২. **অপরিচিত বা অননুমানিক ইনস্টলেশন (Stealthy Installation)**
ব্যবহারকারীর অনুমতি বা জ্ঞানের বাইরে ইনস্টল হয়ে যায়।

৩. **স্বয়ংক্রিয় বিস্তার (Self-Propagation)**
ভাইরাস বা ওয়ার্মের মতো ম্যালওয়্যার নিজে নিজে নেটওয়ার্ক বা ফাইলের মাধ্যমে ছড়াতে পারে।

৪. **নিয়ন্ত্রণ হারানো (Unauthorized Control)**
হ্যাকার সফটওয়্যার বা ডিভাইস নিয়ন্ত্রণ নিতে পারে।

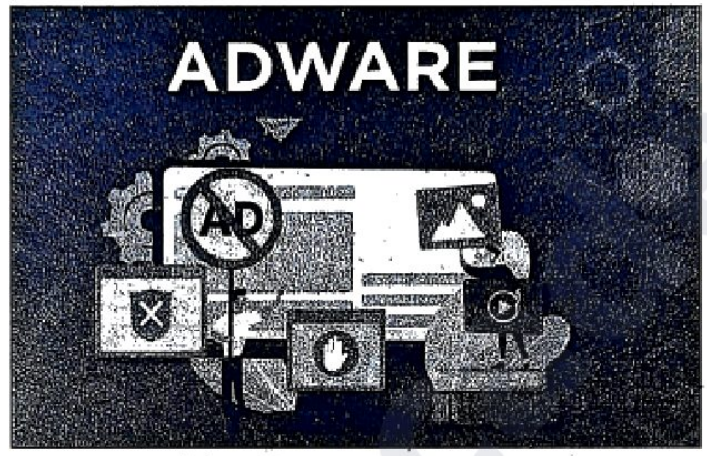
Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৫. **ধরনভিত্তিক আচরণ (Behavior Based on Type)**
ধরন অনুযায়ী ভিন্ন ভিন্ন কাজ করে যেমন: ট্রোজান, র‍্যানসমওয়্যার, স্পাইওয়্যার ইত্যাদি।

৬. **ব্যবহারকারীর তথ্য চুরি (Data Theft)**
লগইন তথ্য, পাসওয়ার্ড, ব্রাউজিং হিস্ট্রি ইত্যাদি সংগ্রহ করতে পারে।

৭. **সিস্টেমের কর্মক্ষমতা কমানো (Reduces System Performance)**
RAM, CPU বা নেটওয়ার্ক ব্যবহার বাড়িয়ে কম্পিউটার ধীর করে দেয়।



ছবি উৎস : www.findmysoft.com

৬.২০.২ Malware (ম্যালওয়্যার)-এর ধরন

Malware (ম্যালওয়্যার)-এর ধরন মূলত তাদের কার্যপ্রণালি ও ক্ষতিকারক বৈশিষ্ট্যের উপর ভিত্তি করে ভাগ করা হয়। নিচে প্রধান ধরনগুলো দেয়া হলো–

১. **Virus (ভাইরাস)**
কী: ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায় এবং ফাইল/ডাটা ক্ষতি করে।
উদাহরণ: ILOVEYOU, Melissa

২. **Worm (ওয়ার্ম)**
কী: নিজে নিজে নেটওয়ার্কে ছড়ায়, ব্যবহারকারীর অ্যাকশন প্রয়োজন হয় না।
উদাহরণ: Conficker, Mydoom

৩. **Trojan Horse (ট্রোজান)**
কী: বিশ্বাসযোগ্য সফটওয়্যারের আড়ালে লুকিয়ে ক্ষতি করে।
উদাহরণ: Zeus, Emotet

৪. **Ransomware (র‍্যানসমওয়্যার)**
কী: ব্যবহারকারীর ডেটাকে এনক্রিপ্ট করে মুক্তিপণ দাবি করে।
উদাহরণ: WannaCry, Petya

৫. **Spyware (স্পাইওয়্যার)**
কী: ব্যবহারকারীর অনুমতি ছাড়া তথ্য সংগ্রহ করে।
উদাহরণ: Keylogger, CoolWebSearch

৬. **Adware (অ্যাডওয়্যার)**
কী: বিজ্ঞাপন দেখায় বা ব্রাউজার ট্র্যাক করে।
উদাহরণ: Fireball, Gator

Visit Our Website: all.talukdaracademy.com.bd

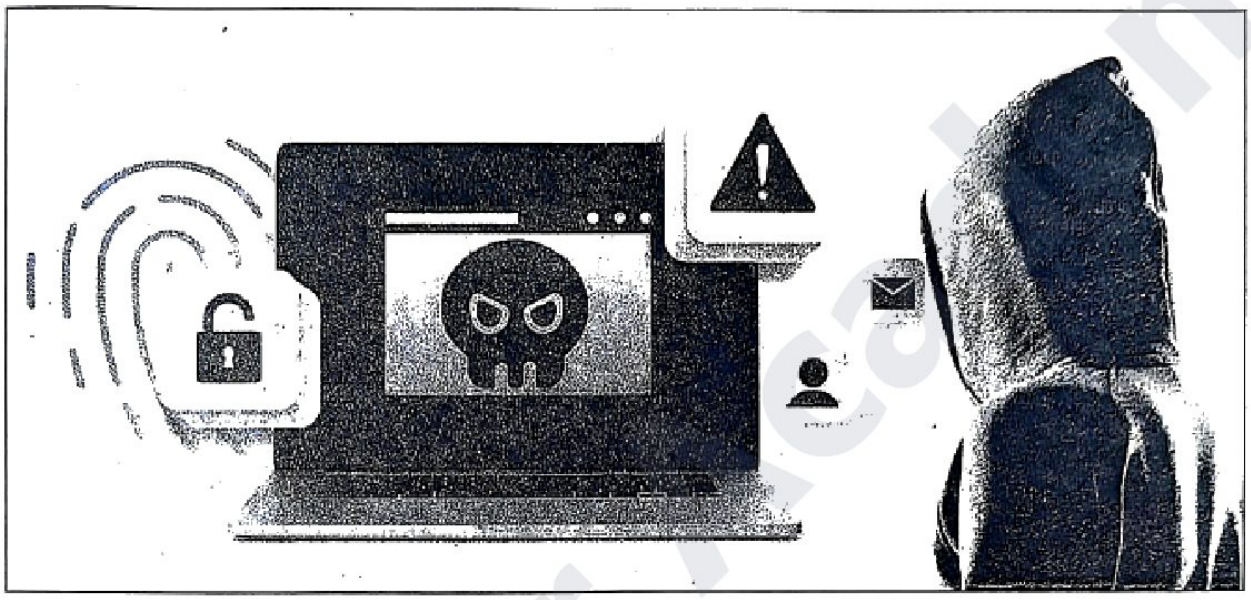
Visit Our Website: all.talukdaracademy.com.bd

৬.২০.৩ Malware (ম্যালওয়্যার) প্রতিরোধের উপায়

Malware (ম্যালওয়্যার) প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে কম্পিউটার, মোবাইল বা নেটওয়ার্ক ম্যালওয়্যারের আক্রমণ থেকে সুরক্ষিত থাকে।

১. আপডেটেড অ্যান্টিভাইরাস ব্যবহার

সব সময় অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল এবং আপডেট রাখতে হবে।
নিয়মিত পুরো সিস্টেম স্ক্যান চালানো।



২. অজানা ইমেইল ও লিঙ্ক এড়ানো

অচেনা ইমেইল, অ্যাটাচমেন্ট বা লিঙ্কে ক্লিক করতে হবে।
ফিশিং ও ভাইরাস প্রবেশের সুযোগ কমানো।

৩. সফটওয়্যার ও অপারেটিং সিস্টেম আপডেট রাখা

নিরাপত্তার দুর্বলতা (vulnerabilities) দূর করতে নিয়মিত আপডেট।

৪. ব্যাকআপ রাখা

গুরুত্বপূর্ণ ফাইল নিয়মিত ব্যাকআপে রাখা।
আক্রান্ত হলে দ্রুত ডেটা পুনরুদ্ধার সম্ভব।

৫. ফায়ারওয়াল ও নেটওয়ার্ক সুরক্ষা

ফায়ারওয়াল সক্রিয় রাখা।
পাবলিক Wi-Fi-এ সংবেদনশীল কাজ এড়ানো।

৬. সচেতন ব্যবহারকারী হওয়া

অজানা সোর্স থেকে সফটওয়্যার ডাউনলোড না করা। ব্রাউজার এক্সটেনশন ও প্লাগইন নিয়মিত পরীক্ষা করা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. ওয়ার্ম কীভাবে ছড়ায়?
ক. মেমোরি কার্ডের মাধ্যমে
খ. ইউজারের ক্লিকের মাধ্যমে
গ. নিজে নিজেই নেটওয়ার্কে
ঘ. সফটওয়্যার আপডেটের মাধ্যমে

২. অ্যাডওয়্যার সাধারণত কোথা থেকে আসে?
ক. পেইড সফটওয়্যার
খ. হার্ডওয়্যার ড্রাইভার
গ. ফ্রি সফটওয়্যারের সাথে
ঘ. BIOS থেকে

৩. নিচের কোনটি অ্যাডওয়্যারের বৈশিষ্ট্য?
ক. ডেটা এনক্রিপ্ট করে
খ. বিজ্ঞাপন দেখায়
গ. ইমেইল স্প্যাম করে
ঘ. ফাইল ছাড়াই কাজ করে

৪. কোন ম্যালওয়্যার ব্যবহারকারীর অনুমতি ছাড়া ইনস্টল হয়?
ক. ট্রোজান
খ. অ্যান্টিভাইরাস
গ. ফায়ারওয়াল
ঘ. এসএমএস

উত্তরমালা : ১. গ; ২. গ; ৩. খ; ৪. ক।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. কম্পিউটার ভাইরাস হলো একধরনের ক্ষতিকারক প্রোগ্রাম যা কোনো ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায় এবং সিস্টেমে ..... করে। **উত্তর : ক্ষতি**

২. ভাইরাস সক্রিয় হতে হলে ..... প্রয়োজন হয়। **উত্তর : আক্রান্ত ফাইল চালানো**

৩. ওয়ার্ম হলো এমন একটি প্রোগ্রাম যা ..... মাধ্যমে স্বয়ংক্রিয়ভাবে নিজেকে কপি ও ছড়াতে পারে। **উত্তর : নেটওয়ার্ক**

৪. স্প্যাম প্রতিরোধের জন্য অজানা লিঙ্ক ও অ্যাটাচমেন্ট ..... করা উচিত। **উত্তর : এড়ানো**

৫. ম্যালওয়্যার থেকে সুরক্ষার জন্য নিয়মিত ব্যাকআপ রাখা দরকার, যাতে সংক্রমণের ক্ষেত্রে ..... সম্ভব হয়। **উত্তর : দ্রুত পুনরুদ্ধার**

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. Virus (ভাইরাস)	ক. অনাবশ্যক ইমেইল বা মেসেজ, বড় পরিমাণে প্রেরণ, বিজ্ঞাপন বা স্ক্যাম সম্পর্কিত।
২. Worm (ওয়ার্ম)	খ. নিজে নিজে নেটওয়ার্কে ছড়ায়, ইউজারের অ্যাকশন প্রয়োজন নেই, ব্যান্ডউইথ খরচ ও নেটওয়ার্ক ক্ষতি করে।
৩. Spam (স্প্যাম)	গ. ফাইল বা প্রোগ্রামের সাথে যুক্ত হয়ে ছড়ায়, ইউজারের অ্যাকশন প্রয়োজন, ফাইল/ডেটা ক্ষতি করে।
৪. Adware (অ্যাডওয়্যার)	ঘ. ক্ষতিকারক সফটওয়্যার, স্বয়ংক্রিয় বিস্তার, ব্যবহারকারীর তথ্য চুরি, সিস্টেম ধীর করে।
৫. Malware (ম্যালওয়্যার)	ঙ. ব্যবহারকারীর অনুমতি ছাড়া বিজ্ঞাপন দেখায়, ব্রাউজার আচরণ পরিবর্তন করে, সিস্টেম ধীর করে।

উত্তরমালা : ১→গ, ২→খ, ৩→ক, ৪→ঙ, ৫→ঘ

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. ভাইরাস কী?
২. Worm (ওয়ার্ম) কী?
৩. Spam (স্প্যাম) কী?
৪. Malware (ম্যালওয়্যার) কী?
৫. ভাইরাসের দুটি ধরন লেখো।
৬. ওয়ার্মের দুটি বৈশিষ্ট্য লেখো।
৭. Virus এবং Worm-এর প্রতিরোধের দুটি উপায় লেখো।
৮. স্প্যামের দুটি বৈশিষ্ট্য লেখো।
৯. স্প্যামের দুটি ধরন লেখো।
১০. স্প্যাম প্রতিরোধের দুটি উপায় লেখো।
১১. অ্যাডওয়্যার কী?
১২. অ্যাডওয়্যারের দুটি বৈশিষ্ট্য লেখো।
১৩. অ্যাডওয়্যার প্রতিরোধের দুটি উপায় লেখো।
১৪. ম্যালওয়্যারের দুটি বৈশিষ্ট্য লেখো।
১৫. ম্যালওয়্যারের দুটি ধরন লেখো।
১৬. ম্যালওয়্যার প্রতিরোধের দুটি উপায় লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. ওয়ার্ম-এর বৈশিষ্ট্যগুলো লেখো।
২. ভাইরাস ও ওয়ার্ম-এর মধ্যে প্রধান পার্থক্য কী?
৩. ভাইরাস ও ওয়ার্ম প্রতিরোধের উপায় কী কী?
৪. স্প্যামের বৈশিষ্ট্যগুলো কী কী?
৫. স্প্যামের ধরনগুলো উদাহরণসহ লেখো।
৬. স্প্যাম প্রতিরোধের উপায়গুলো কী কী?
৭. Adware (অ্যাডওয়্যার) কী এবং এর বৈশিষ্ট্য কী কী?
৮. অ্যাডওয়্যারের ধরনগুলো উদাহরণসহ লেখো।
৯. ম্যালওয়্যার প্রতিরোধের প্রধান উপায়গুলো কী কী?

চ. বর্ণনামূলক প্রশ্ন :

১. ওয়ার্ম কী এবং এটি ভাইরাস থেকে কীভাবে আলাদা তা বিশদভাবে ব্যাখ্যা করো।
২. ওয়ার্ম-এর বৈশিষ্ট্যগুলো ব্যাখ্যা করো এবং নেটওয়ার্কে এর প্রভাব আলোচনা করো।
৩. ভাইরাস এবং ওয়ার্ম প্রতিরোধে অ্যান্টিভাইরাস, ফায়ারওয়াল ও ব্যাকআপের ভূমিকা ব্যাখ্যা করো।
৪. স্প্যাম কী এবং এটি ব্যবহারকারীর জন্য কীভাবে ক্ষতিকারক হতে পারে তা ব্যাখ্যা করো।
৫. ইমেইল স্প্যাম, এসএমএস স্প্যাম, সোশ্যাল মিডিয়া স্প্যাম ও কমেন্ট স্প্যাম উদাহরণসহ ব্যাখ্যা করো।
৬. স্প্যাম প্রতিরোধের জন্য স্প্যাম ফিল্টার, অ্যান্টি-স্প্যাম সফটওয়্যার ও সচেতন ব্যবহার কেন গুরুত্বপূর্ণ তা ব্যাখ্যা করো।
৭. অ্যাডওয়্যার কী এবং এটি ব্যবহারকারীর ব্রাউজিং অভিজ্ঞতা বা সিস্টেমকে কীভাবে প্রভাবিত করে তা ব্যাখ্যা করো।
৮. ব্রাউজার হাইজকার, পপ-আপ অ্যাডওয়্যার এবং ট্র্যাকিং অ্যাডওয়্যার উদাহরণসহ ব্যাখ্যা করো।
৯. ম্যালওয়্যার কী এবং এর প্রধান ধরনগুলো (ভাইরাস, ওয়ার্ম, ট্রোজান, র‍্যানসমওয়্যার, স্পাইওয়্যার, অ্যাডওয়্যার) উদাহরণসহ ব্যাখ্যা করো।
১০. ম্যালওয়্যার প্রতিরোধে নিরাপদ সফটওয়্যার ব্যবহার, নিয়মিত আপডেট, ব্যাকআপ এবং সচেতন ব্যবহারকারীর ভূমিকা ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.২১ Spyware (স্পাইওয়্যার)

Spyware (স্পাইওয়্যার) হলো এক ধরনের ক্ষতিকর সফটওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়া তাদের কম্পিউটার বা মোবাইল থেকে ব্যক্তিগত তথ্য সংগ্রহ করে। এটি সাধারণত ব্যবহারকারীর কার্যক্রম পর্যবেক্ষণ করে এবং তথ্য হ্যাকার বা তৃতীয় পক্ষের কাছে প্রেরণ করে।

৬.২১.১ Spyware (স্পাইওয়্যার)-এর বৈশিষ্ট্য

১. **ব্যবহারকারীর অনুমতি ছাড়া তথ্য সংগ্রহ (Unauthorized Data Collection)**
লগইন তথ্য, পাসওয়ার্ড, ব্রাউজিং হিস্ট্রি এবং অন্যান্য ব্যক্তিগত তথ্য চুরি করে।

২. **সিস্টেম ধীর করে দেয় (Reduces System Performance)**
RAM বা CPU ব্যবহার বাড়িয়ে কম্পিউটার বা মোবাইল ধীর করে।

৩. **অপরিচিত বা গোপন ইনস্টলেশন (Stealthy Installation)**
ব্যবহারকারীর অনুমতি বা জ্ঞান ছাড়া লুকিয়ে ইনস্টল হয়।

৪. **নিয়ন্ত্রণ হারানো (Unauthorized Control)**
হ্যাকার দূরে থেকে ডিভাইস বা সফটওয়্যারের কার্যক্রম নিয়ন্ত্রণ করতে পারে।

৫. **ব্রাউজার আচরণ পরিবর্তন (Alters Browser Behavior)**
হোমপেজ, ডিফল্ট সার্চ ইঞ্জিন বা নতুন ট্যাব সেটিং পরিবর্তন করতে পারে।

৬. **ব্যবহারকারীর গোপনীয়তা লঙ্ঘন (Privacy Violation)**
ব্যক্তিগত তথ্য তৃতীয় পক্ষের কাছে প্রেরণ করা হয়।

৬.২১.২ Spyware (স্পাইওয়্যার)-এর ধরন

Spyware (স্পাইওয়্যার)-এর ধরন মূলত তাদের কার্যপ্রণালী এবং তথ্য চুরির ধরনের উপর ভিত্তি করে ভাগ করা হয়।

১. **Keyloggers (কী-লগার)**
কী: ব্যবহারকারীর টাইপ করা কীস্ট্রোক বা পাসওয়ার্ড রেকর্ড করে।
উদাহরণ: লগইন তথ্য, ব্যাংকিং পাসওয়ার্ড চুরি করা।

২. **Trojan Spyware (ট্রোজান স্পাইওয়্যার)**
কী: ট্রোজানের আড়ালে লুকিয়ে তথ্য চুরি করে বা সিস্টেম নিয়ন্ত্রণ করে।
উদাহরণ: Zeus, Emotet

৩. **Tracking Cookies (ট্র্যাকিং কুকিজ)**
কী: ব্রাউজিং প্যাটার্ন, সার্চ হিস্ট্রি বা ব্যবহারকারীর অভ্যাস ট্র্যাক করে।
উদাহরণ: লক্ষ্যভিত্তিক বিজ্ঞাপন প্রদর্শন।

৪. **System Monitors (সিস্টেম মনিটর)**
কী: পুরো সিস্টেমের কার্যক্রম পর্যবেক্ষণ করে এবং তথ্য সংগ্রহ করে।
উদাহরণ: কোন ফাইল খোলা হয়েছে বা কোন সফটওয়্যার ব্যবহার করা হয়েছে তা নজর রাখা।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.২১.৩ Spyware (স্পাইওয়্যার) প্রতিরোধের উপায়

Spyware (স্পাইওয়্যার) প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে ব্যবহারকারীর ডিভাইস ও তথ্য ম্যালওয়্যারের আক্রমণ থেকে সুরক্ষিত থাকে।

১. আপডেটেড অ্যান্টি-স্পাইওয়্যার ব্যবহার
Malwarebytes, Spybot ইত্যাদি সফটওয়্যার ব্যবহার করতে হবে।
নিয়মিত স্ক্যান চালানো এবং সফটওয়্যার আপডেট রাখতে হবে।

২. অজানা লিঙ্ক, ইমেইল ও সফটওয়্যার এড়ানো
অচেনা ইমেইল বা অ্যাটাচমেন্টে ক্লিক করা যাবে না।
অজানা সোর্স থেকে সফটওয়্যার ডাউনলোড করা যাবে না।

৩. ব্রাউজার এক্সটেনশন ও প্লাগইন নিয়মিত পরীক্ষা
অচেনা বা অপ্রয়োজনীয় এক্সটেনশন মুছে দিতে হবে।

৪. অপারেটিং সিস্টেম ও সফটওয়্যার আপডেট রাখা
নিরাপত্তা দুর্বলতা দূর করতে নিয়মিত আপডেট।

৫. ব্যক্তিগত তথ্য শেয়ার সীমিত করা
ব্যক্তিগত তথ্য, লগইন ডিটেইল বা ব্রাউজিং হিস্ট্রি শুধুমাত্র বিশ্বাসযোগ্য সাইটে ব্যবহার করো।

৬. নিরাপদ নেটওয়ার্ক ব্যবহার
পাবলিক Wi-Fi-এ সংবেদনশীল কাজ এড়ানো।
VPN ব্যবহার করে ডেটা এনক্রিপ্ট করা।

৬.২২ Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার)

Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার) হলো এমন একটি প্রোগ্রাম যা কম্পিউটার, মোবাইল বা নেটওয়ার্ককে ভাইরাস, ম্যালওয়্যার, স্পাইওয়্যার এবং অন্যান্য ক্ষতিকর সফটওয়্যার থেকে সুরক্ষিত রাখে।

৬.২২.১ Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার)-এর বৈশিষ্ট্য

Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার)-এর বৈশিষ্ট্য নিচে দেয়া হলো–

১. ম্যালওয়্যার শনাক্তকরণ (Malware Detection)
ভাইরাস, ওয়ার্ম, ট্রোজান, র‍্যানসমওয়্যার ইত্যাদি চিহ্নিত করতে পারে।

২. রিয়েল-টাইম সুরক্ষা (Real-Time Protection)
ডিভাইস চালু থাকা অবস্থায় সিস্টেমকে স্বয়ংক্রিয়ভাবে সুরক্ষিত রাখে।

৩. স্ক্যানিং ও পরিষ্কার করা (Scanning & Cleaning)
ফাইল, সফটওয়্যার এবং ড্রাইভ স্ক্যান করে ম্যালওয়্যার সরায়।

৪. স্বয়ংক্রিয় আপডেট (Automatic Updates)
নতুন ভাইরাস বা ম্যালওয়্যারের তথ্য নিয়মিত আপডেট করে।

৫. ব্যাকআপ ও পুনরুদ্ধার (Backup & Recovery)
সংক্রমণের পর ডেটা পুনরুদ্ধার করতে সাহায্য করে।

৬. নিরাপদ নেটওয়ার্ক ব্যবহারে সহায়তা (Network Security Assistance)
ফায়ারওয়াল বা নেটওয়ার্ক ট্রাফিক পর্যবেক্ষণ করে সুরক্ষা নিশ্চিত করে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.২২.২ Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার) -এর ধরন

Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার)-এর ধরন মূলত কার্যকারিতা ও ব্যবহারের উপর ভিত্তি করে ভাগ করা হয়।

১. Standalone Antivirus
কী: শুধুমাত্র ভাইরাস শনাক্ত ও সরানোর কাজ করে।
উদাহরণ: ClamAV, Avast Free Antivirus (মূলত ভাইরাস শনাক্তকেন্দ্রিক)।

২. Internet Security Suites
কী: ভাইরাস ছাড়াও ফায়ারওয়াল, স্প্যাম ফিল্টার, ইমেইল সুরক্ষা এবং ওয়েব সিকিউরিটি দেয়।
উদাহরণ: Norton Internet Security, Kaspersky Internet Security।

৩. Cloud-Based Antivirus
কী: ক্লাউড সার্ভারের মাধ্যমে ভাইরাস শনাক্ত এবং অপসারণ করা হয়।
উদাহরণ: Panda Cloud Antivirus, Trend Micro HouseCall।

৪. Hybrid Antivirus
কী: লোকাল + ক্লাউডভিত্তিক প্রযুক্তি ব্যবহার করে সুরক্ষা প্রদান।
উদাহরণ: Bitdefender, ESET Smart Security।

৬.২২.৩ Antivirus Software ব্যবহার ও প্রতিরোধের উপায়

Antivirus Software (অ্যান্টিভাইরাস সফটওয়্যার) ব্যবহার ও প্রতিরোধের উপায় হলো সেই পদক্ষেপগুলো যা গ্রহণ করলে কম্পিউটার বা মোবাইল ডিভাইস ভাইরাস ও ম্যালওয়্যার থেকে সুরক্ষিত থাকে।

১. আপডেটেড অ্যান্টিভাইরাস ব্যবহার
সর্বদা অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করতে হবে।
নিয়মিত আপডেট চালিয়ে নতুন ভাইরাস শনাক্তকরণ সক্ষমতা বজায় রাখতে হবে।

২. নিয়মিত স্ক্যান চালানো
পুরো সিস্টেম, নির্দিষ্ট ফোল্ডার বা ড্রাইভ স্ক্যান করতে হবে।
স্বয়ংক্রিয় স্ক্যান শিডিউল করে রাখলে ভালো।

৩. অজানা বা সন্দেহজনক লিঙ্ক এড়ানো
ইমেইল, মেসেজ বা ওয়েবসাইটের অজানা লিঙ্কে ক্লিক করা যাবে না।
অজানা সফটওয়্যার ডাউনলোড না করা।

৪. ফায়ারওয়াল ব্যবহার
ইন্টারনেট থেকে অননুমোদিত প্রবেশ বন্ধ করতে ফায়ারওয়াল সক্রিয় রাখতে হবে।

৫. ব্যাকআপ রাখা
গুরুত্বপূর্ণ ফাইল নিয়মিত ব্যাকআপে রাখতে হবে।
সংক্রমণের ক্ষেত্রে দ্রুত ডেটা পুনরুদ্ধার সম্ভব।

৬. নিরাপদ নেটওয়ার্ক ব্যবহার
পাবলিক Wi-Fi-এ সংবেদনশীল কাজ এড়ানো।
VPN ব্যবহার করে ডেটা এনক্রিপ্ট করতে হবে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. স্পাইওয়্যার কী কাজ করে?
ক. ফাইল ডিলিট করে খ. মেমোরি বাড়ায়
গ. ব্যক্তিগত তথ্য সংগ্রহ করে ঘ. সফটওয়্যার আপডেট করে

২. ট্র্যাকিং কুকিজ কী করে?
ক. ফাইল ডিলিট করে খ. ব্রাউজিং প্যাটার্ন ট্র্যাক করে
গ. ডেটা ব্যাকআপ করে ঘ. ভাইরাস স্ক্যান করে

৩. ট্রোজান স্পাইওয়্যার কী করে?
ক. গেম খেলে খ. ডিভাইস ফরম্যাট করে
গ. আড়ালে থেকে তথ্য চুরি করে ঘ. ব্যাকআপ তৈরি করে

৪. নিরাপদ নেটওয়ার্ক ব্যবহারে কী ব্যবহার করা উচিত?
ক. ফ্রি Wi-Fi খ. VPN
গ. গেমিং সাইট ঘ. পাবলিক নেটওয়ার্ক

উত্তরমালা : ১. গ; ২. খ; ৩. গ; ৪. খ।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. স্পাইওয়্যার হলো ক্ষতিকর সফটওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়া তাদের কম্পিউটার বা মোবাইল থেকে ..... সংগ্রহ করে। **উত্তর :** ব্যক্তিগত তথ্য

২. স্পাইওয়্যার ডিভাইসকে ধীর করে দেয় কারণ এটি ..... ব্যবহার বাড়িয়ে সিস্টেমকে ব্যস্ত রাখে।
উত্তর : RAM বা CPU

৩. কী-লগার স্পাইওয়্যার ব্যবহারকারীর ..... রেকর্ড করে। উত্তর : কীস্ট্রোক বা পাসওয়ার্ড

৪. অ্যান্টিভাইরাস সফটওয়্যার নতুন ভাইরাস শনাক্ত করার জন্য নিয়মিত ..... চালিয়ে রাখে।
উত্তর : আপডেট

৫. নিরাপদ নেটওয়ার্ক ব্যবহার করার মাধ্যমে স্পাইওয়্যার বা ভাইরাস থেকে সংবেদনশীল তথ্য ..... করা সম্ভব হয়। **উত্তর :** সুরক্ষিত

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. Spyware (স্পাইওয়্যার)	ক. ট্রোজানের আড়ালে লুকিয়ে তথ্য চুরি করে বা সিস্টেম নিয়ন্ত্রণ করে।
২. কী-লগার	খ. ভাইরাস, ম্যালওয়্যার, স্পাইওয়্যার থেকে কম্পিউটার বা মোবাইল সুরক্ষা করে।
৩. ট্রোজান স্পাইওয়্যার	গ. ব্যবহারকারীর অনুমতি ছাড়া তথ্য সংগ্রহ করে।
৪. ট্র্যাকিং কুকিজ	ঘ. ব্রাউজিং প্যাটার্ন, সার্চ হিস্ট্রি বা ব্যবহারকারীর অভ্যাস ট্র্যাক করে।
৫. অ্যান্টিভাইরাস সফটওয়্যার	ঙ. ব্যবহারকারীর টাইপ করা কীস্ট্রোক বা পাসওয়ার্ড রেকর্ড করে।

উত্তরমালা : ১→গ, ২→ঙ, ৩→ক, ৪→ঘ, ৫→খ

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. স্পাইওয়্যার (Spyware) কী?
২. অ্যান্টিভাইরাস সফটওয়্যার কী?
৩. স্পাইওয়্যারের দুটি বৈশিষ্ট্য লেখো।
৪. স্পাইওয়্যারের দুটি ধরন লেখো।
৫. স্পাইওয়্যার প্রতিরোধের দুটি উপায় লেখো।
৬. এন্টিভাইরাস সফটওয়্যারের দুটি বৈশিষ্ট্য লেখো।
৭. এন্টিভাইরাসের সফটওয়্যারের দুটি ধরন লেখো।
৮. এন্টিভাইরাস সফটওয়্যারের দুটি ব্যবহার লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. স্পাইওয়্যার-এর বৈশিষ্ট্যগুলো লেখো।
২. স্পাইওয়্যার কীভাবে ব্যবহারকারীর ডিভাইসকে প্রভাবিত করে?
৩. স্পাইওয়্যার-এর ধরনগুলো উদাহরণসহ লেখো।
৪. কী-লগার কীভাবে তথ্য চুরি করে?
৫. ট্রোজান স্পাইওয়্যার কী এবং এটি কীভাবে কাজ করে?
৬. ট্র্যাকিং কুকিজ কীভাবে ব্যবহারকারীর তথ্য সংগ্রহ করে?
৭. স্পাইওয়্যার প্রতিরোধের উপায়গুলো কী কী?
৮. অ্যান্টিভাইরাস সফটওয়্যারের বৈশিষ্ট্যগুলো লেখো।
৯. অ্যান্টিভাইরাস সফটওয়্যারের ধরনগুলো কী কী?
১০. অ্যান্টিভাইরাস সফটওয়্যার ব্যবহারের নিয়ম ও সতর্কতা কী কী?

চ. বর্ণনামূলক প্রশ্ন :

১. স্পাইওয়্যার কী এবং এটি ব্যবহারকারীর জন্য কীভাবে ক্ষতিকারক হতে পারে তা ব্যাখ্যা করো।
২. স্পাইওয়্যারের বৈশিষ্ট্যগুলো বিশদভাবে ব্যাখ্যা করো।
৩. কী-লগার, ট্রোজান স্পাইওয়্যার, ট্র্যাকিং কুকিজ ও সিস্টেম মনিটরের কাজ ও উদাহরণসহ ব্যাখ্যা করো।
৪. স্পাইওয়্যার প্রতিরোধে অ্যান্টি-স্পাইওয়্যার সফটওয়্যারের ভূমিকা ব্যাখ্যা করো।
৫. অজানা লিঙ্ক, ইমেইল ও সফটওয়্যার এড়ানোর গুরুত্ব ব্যাখ্যা করো।
৬. ব্রাউজার এক্সটেনশন ও প্লাগইন পরীক্ষা করে স্পাইওয়্যার প্রতিরোধ কিভাবে করা যায় তা ব্যাখ্যা করো।
৭. অ্যান্টিভাইরাস সফটওয়্যার কী এবং এটি কীভাবে ম্যালওয়্যার শনাক্ত ও সরায় তা ব্যাখ্যা করো।
৮. অ্যান্টিভাইরাস সফটওয়্যারের বিভিন্ন ধরন (ভাইরাস-কেন্দ্রিক, ওয়েব-সিকিউরিটি সহ, ক্লাউড ভিত্তিক) উদাহরণসহ ব্যাখ্যা করো।
৯. অ্যান্টিভাইরাস সফটওয়্যার ব্যবহারের নিয়মাবলি এবং সতর্কতা বিশদভাবে ব্যাখ্যা করো।
১০. স্পাইওয়্যার ও ম্যালওয়্যার প্রতিরোধে নিরাপদ নেটওয়ার্ক ব্যবহার, ব্যাকআপ ও সচেতন ব্যবহারকারীর ভূমিকা ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৬.২৩ Ethics in the Digital World (ডিজিটাল জগতের নীতি/নৈতিকতা)

Ethics in the Digital World (ডিজিটাল জগতের নীতি/নৈতিকতা) হলো সেই নীতিমালা ও আচরণবিধি যা ডিজিটাল প্রযুক্তি ব্যবহার করার সময় মানুষের দায়িত্বশীলতা, সততা ও সম্মান নিশ্চিত করে। এটি ব্যবহারকারীর অনলাইন আচরণ, তথ্য সুরক্ষা, গোপনীয়তা এবং আইনি সীমার মধ্যে থাকা নিয়ে কাজ করে।

৬.২৩.১ Digital Ethics (ডিজিটাল নীতি/নৈতিকতা)-এর বৈশিষ্ট্য

১. সততা ও সত্যনিষ্ঠা **(Honesty & Integrity)**
ডিজিটাল তথ্য ব্যবহার বা শেয়ার করার সময় সত্যনিষ্ঠ থাকা।

২. গোপনীয়তা রক্ষা **(Privacy Protection)**
ব্যক্তিগত তথ্য, পাসওয়ার্ড বা সংবেদনশীল ডেটা অন্যের কাছে প্রকাশ না করা।

৩. আইনি ও নৈতিক সীমার মধ্যে থাকা **(Lawful & Ethical Behavior)**
অনলাইনে আইন ও নিয়ম মেনে চলা।

৪. দায়িত্বশীলতা ও জবাবদিহিতা **(Responsibility & Accountability)**
অনলাইনে করা কাজের ফলাফলের জন্য দায়িত্ব নেয়া।

৫. সম্মান ও সামাজিক সচেতনতা **(Respect & Social Awareness)**
অনলাইন কমিউনিটিতে অন্যকে সম্মান করা, হিংস্র বা নেতিবাচক আচরণ এড়ানো।

৬. ভরসাযোগ্য অনলাইন ব্যবহার **(Trustworthy Online Behavior)**
তথ্য শেয়ার বা যোগাযোগে বিশ্বাসযোগ্যতা বজায় রাখা।

৬.২৩.২ Digital Ethics (ডিজিটাল নীতি/নৈতিকতা)-এর গুরুত্ব

Digital Ethics (ডিজিটাল নীতি/নৈতিকতা)-এর গুরুত্ব হলো ডিজিটাল প্রযুক্তি ব্যবহারের সময় ব্যবহারকারীর দায়িত্বশীলতা, নিরাপত্তা ও সামাজিক সম্মান নিশ্চিত করা। এর মূল গুরুত্বগুলো নিচে দেয়া হলো–

১. গোপনীয়তা সুরক্ষা **(Protects Privacy)**
ব্যবহারকারীর ব্যক্তিগত তথ্য, পাসওয়ার্ড ও সংবেদনশীল ডেটা চুরি বা অপব্যবহার থেকে রক্ষা করে।

২. আইনি ঝুঁকি কমানো **(Reduces Legal Risks)**
অনলাইনে আইন ও নিয়ম না মেনে চলার কারণে সৃষ্ট সমস্যা বা মামলা থেকে রক্ষা করে।

৩. ভরসাযোগ্য অনলাইন পরিবেশ **(Ensures Trustworthy Online Environment)**
সকল ব্যবহারকারীর জন্য নিরাপদ, বিশ্বাসযোগ্য এবং ইতিবাচক অনলাইন পরিবেশ তৈরি করে।

৪. দায়িত্বশীল ব্যবহার **(Promotes Responsible Usage)**
প্রযুক্তি ব্যবহার করে সমাজে ইতিবাচক অবদান রাখা এবং ক্ষতিকারক কাজ এড়ানো।

৫. সুস্থ সামাজিক আচরণ **(Encourages Respectful Behavior)**
অনলাইন কমিউনিটিতে হিংস্রতা, হয়রানি বা নেতিবাচক আচরণ এড়াতে সাহায্য করে।

৬. সৃজনশীলতা ও শিক্ষাগত উন্নয়ন **(Fosters Creativity & Learning)**
নৈতিকভাবে ডিজিটাল প্রযুক্তি ব্যবহার করে শিক্ষাগত ও পেশাদারী কাজে সৃজনশীলতা বৃদ্ধি পায়।

Security Tools (নিরাপত্তা সরঞ্জাম)

Security Tools (নিরাপত্তা সরঞ্জাম) হলো সফটওয়্যার বা প্রোগ্রাম যা কম্পিউটার, নেটওয়ার্ক ও তথ্যকে সাইবার আক্রমণ, ম্যালওয়্যার, ভাইরাস, হ্যাকিং ও অনাকাঙ্ক্ষিত প্রবেশের ঝুঁকি থেকে রক্ষা করে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

জনপ্রিয় নিরাপত্তা সরঞ্জামসমূহ

সরঞ্জাম (Tool)	উদ্দেশ্য (Purpose)	উদাহরণ (Example)
Antivirus Software	ভাইরাস, ম্যালওয়্যার ও স্পাইওয়্যার শনাক্ত ও সরানো	Avast, Norton, Kaspersky
Firewall	নেটওয়ার্কে অননুমোদিত প্রবেশ রোধ	Windows Firewall, pfSense
Encryption Tools	ডেটা এনক্রিপশন ও ডিক্রিপশন	VeraCrypt, BitLocker
Intrusion Detection System (IDS)	অননুমোদিত প্রবেশ বা আক্রমণ শনাক্ত করা	Snort, Suricata
Intrusion Prevention System (IPS)	আক্রমণ প্রতিরোধ করা	Cisco IPS, McAfee Network Security
Password Manager	শক্তিশালী ও নিরাপদ পাসওয়ার্ড সংরক্ষণ	LastPass, 1Password
VPN (Virtual Private Network)	নিরাপদ ও এনক্রিপ্টেড নেটওয়ার্ক সংযোগ	NordVPN, ExpressVPN
Security Information and Event Management (SIEM)	লগ মনিটরিং ও সিকিউরিটি অ্যানালিসিস	Splunk, IBM QRadar
Penetration Testing Tools	নিরাপত্তা দুর্বলতা পরীক্ষা	Metasploit, Kali Linux Tools
Backup Tools	গুরুত্বপূর্ণ ডেটার ব্যাকআপ ও পুনরুদ্ধার	Acronis, Veeam Backup

ব্যবহার ও প্রতিরোধের উপায়

- সবসময় সফটওয়্যার আপডেট রাখা।
- অ্যান্টিভাইরাস ও ফায়ারওয়াল সক্রিয় রাখা।
- শক্তিশালী পাসওয়ার্ড ব্যবহার ও VPN এর মাধ্যমে সংযোগ সুরক্ষিত রাখা।
- নিয়মিত ব্যাকআপ রাখা এবং নিরাপদ স্থানে সংরক্ষণ।
- সন্দেহজনক লিঙ্ক, ইমেইল বা সফটওয়্যার এড়ানো।

Kaspersky (ক্যাসপারাসকী)

Kaspersky হলো একটি জনপ্রিয় অ্যান্টিভাইরাস এবং ইন্টারনেট সিকিউরিটি সফটওয়্যার যা ব্যবহারকারীর কম্পিউটার, মোবাইল ও নেটওয়ার্ককে ভাইরাস, ম্যালওয়্যার, ট্রোজান, স্পাইওয়্যার এবং অন্যান্য সাইবার হুমকি থেকে সুরক্ষিত রাখে।

Kaspersky-এর বৈশিষ্ট্য

১. **ভাইরাস ও ম্যালওয়্যার সনাক্তকরণ (Virus & Malware Detection)**
রিয়েল-টাইমে ভাইরাস, ওয়ার্ম, ট্রোজান, র‍্যানসমওয়্যার চিহ্নিত করে।

২. **ইন্টারনেট সুরক্ষা (Internet Security)**
ফিশিং, সন্দেহজনক ওয়েবসাইট ও অননুমোদিত প্রবেশ থেকে সুরক্ষা দেয়।

৩. **ফায়ারওয়াল (Firewall)**
নেটওয়ার্ক ট্রাফিক নিয়ন্ত্রণ করে অননুমোদিত অ্যাক্সেস বন্ধ করে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৪. এন্টি-ফিশিং ও এন্টি-স্প্যাম (Anti-Phishing & Anti-Spam)
ক্ষতিকর ইমেইল ও ওয়েবসাইট চিহ্নিত করে ব্যবহারকারীকে সতর্ক করা।

৫. সিস্টেম পারফরম্যান্স রক্ষা (System Performance Protection)
নিরাপত্তা দেয়ার সময় কম্পিউটারের কার্যকারিতা কম প্রভাবিত হয়।

৬. পিতৃত্ব নিয়ন্ত্রণ (Parental Control)
শিশুদের অনলাইনে নিরাপদ ব্যবহার নিশ্চিত করে।

Kaspersky ব্যবহার ও প্রতিরোধ উপায়

- **আপডেটেড সফটওয়্যার ব্যবহার:** সর্বদা Kaspersky আপডেট রাখতে হবে।
- **পূর্ণ স্ক্যান চালানো:** নিয়মিত পুরো সিস্টেম স্ক্যান করতে হবে।
- **সন্দেহজনক ফাইল এড়ানো:** অজানা বা অবিশ্বস্ত লিঙ্ক ও অ্যাটাচমেন্ট ক্লিক করা যাবে না।
- **ফায়ারওয়াল সক্রিয় রাখা:** নেটওয়ার্কে নিরাপত্তা নিশ্চিত করতে ফায়ারওয়াল ব্যবহার করতে হবে।

Norton (নরটন)

Norton একটি জনপ্রিয় সাইবার সিকিউরিটি সফটওয়্যার যা ভাইরাস, ম্যালওয়্যার, স্পাইওয়্যার, ফিশিং, র‍্যানসমওয়্যারসহ বিভিন্ন সাইবার হুমকি থেকে কম্পিউটার, মোবাইল এবং নেটওয়ার্ককে সুরক্ষিত রাখে।

Norton-এর বৈশিষ্ট্য

১. ভাইরাস ও ম্যালওয়্যার সুরক্ষা
রিয়েল-টাইমে ভাইরাস, ট্রোজান, ওয়ার্ম, র‍্যানসমওয়্যার চিহ্নিত ও অপসারণ করে।

২. ইন্টারনেট সিকিউরিটি
ফিশিং ও ভুয়া ওয়েবসাইট থেকে ব্যবহারকারীকে সুরক্ষা দেয়।

৩. স্মার্ট ফায়ারওয়াল
নেটওয়ার্কে আসা-যাওয়া করা ডেটা নিয়ন্ত্রণ করে অননুমোদিত অ্যাক্সেস বন্ধ করে।

৪. পাসওয়ার্ড ম্যানেজার
নিরাপদে পাসওয়ার্ড সংরক্ষণ ও ব্যবস্থাপনার সুবিধা দেয়।

৫. VPN (Virtual Private Network)
ইন্টারনেট ব্রাউজিং এনক্রিপ্ট করে গোপনীয়তা নিশ্চিত করে।

৬. ক্লাউড ব্যাকআপ
গুরুত্বপূর্ণ ফাইলের জন্য অনলাইন ব্যাকআপ সেবা প্রদান করে।

৭. ডার্ক ওয়েব মনিটরিং
আপনার ব্যক্তিগত তথ্য ডার্ক ওয়েবে প্রকাশিত হলে সতর্কবার্তা দেয়।

Norton ব্যবহার ও প্রতিরোধের উপায়

- সফটওয়্যার আপডেট রাখা → সর্বদা Norton-এর সর্বশেষ সংস্করণ ব্যবহার করতে হবে।
- নিয়মিত সিস্টেম স্ক্যান → পুরো ডিভাইস স্ক্যান করে নিরাপত্তা নিশ্চিত করতে হবে।
- পাসওয়ার্ড ম্যানেজার ব্যবহার → শক্তিশালী ও আলাদা পাসওয়ার্ড তৈরি করতে হবে।
- VPN চালু রাখা → পাবলিক Wi-Fi ব্যবহার করার সময় VPN ব্যবহার করতে হবে।
- ফায়ারওয়াল সক্রিয় রাখা → হ্যাকারদের অননুমোদিত প্রবেশ রোধ করতে হবে।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

Avast (অ্যাভাস্ট)

Avast একটি জনপ্রিয় এবং বিনামূল্যে (Free) ব্যবহারযোগ্য সাইবার সিকিউরিটি সফটওয়্যার, যা ভাইরাস, ম্যালওয়্যার, স্পাইওয়্যার, র‍্যানসমওয়্যার, ফিশিং ইত্যাদি থেকে ডিভাইসকে সুরক্ষিত রাখে। এটি Windows, macOS, Android ও iOS প্ল্যাটফর্মে ব্যবহার করা যায়।

Avast-এর বৈশিষ্ট্য

১. **রিয়েল-টাইম ভাইরাস সুরক্ষা**
সিস্টেমে ঢোকার আগেই ভাইরাস, ম্যালওয়্যার এবং ওয়ার্ম শনাক্ত ও ব্লক করে।

২. **স্মার্ট স্ক্যান**
একবারে ম্যালওয়্যার, দুর্বল পাসওয়ার্ড, পুরোনো সফটওয়্যার এবং নেটওয়ার্ক সমস্যা খুঁজে বের করে।

৩. **Web Shield**
বিপজ্জনক ওয়েবসাইট ও ফিশিং লিঙ্ক থেকে সুরক্ষা দেয়।

৪. **Wi-Fi Inspector**
নেটওয়ার্কে কোনো দুর্বলতা বা অননুমোদিত ডিভাইস আছে কিনা তা শনাক্ত করে।

৫. **Sandbox Mode**
সন্দেহজনক ফাইল আলাদা পরিবেশে চালিয়ে নিরাপত্তা পরীক্ষা করে।

৬. **Ransomware Shield**
গুরুত্বপূর্ণ ফাইলকে র‍্যানসমওয়্যার আক্রমণ থেকে রক্ষা করে।

৭. **পাসওয়ার্ড ম্যানেজার**
নিরাপদে পাসওয়ার্ড সংরক্ষণ ও ব্যবহার করার সুবিধা দেয়।

Avast ব্যবহার ও প্রতিরোধের উপায়

- নিয়মিত স্ক্যান চালানো → প্রতিদিন বা সাপ্তাহিক সিস্টেম স্ক্যান করে নিরাপত্তা নিশ্চিত করতে হবে।
- সফটওয়্যার আপডেট রাখতে হবে → সর্বশেষ সিকিউরিটি প্যাচ ব্যবহার করতে হবে।
- Web Shield চালু রাখতে হবে → ইন্টারনেট ব্রাউজিংয়ের সময় অনিরাপদ ওয়েবসাইট থেকে রক্ষা পেতে।
- Sandbox ব্যবহার করো → সন্দেহজনক ফাইল পরীক্ষা করতে।
- Wi-Fi Inspector চালানো → পাবলিক বা হোম নেটওয়ার্কে অননুমোদিত অ্যাক্সেস চেক করতে।

McAfee (ম্যাকঅ্যাফী)

McAfee একটি সুপরিচিত সাইবার সিকিউরিটি সফটওয়্যার, যা ব্যক্তিগত ব্যবহারকারী থেকে শুরু করে বড় প্রতিষ্ঠান পর্যন্ত ভাইরাস, ম্যালওয়্যার, স্পাইওয়্যার, র‍্যানসমওয়্যার এবং অনলাইন হুমকি থেকে সুরক্ষা দেয়। এটি Windows, macOS, Android ও iOS ডিভাইসে কাজ করে।

McAfee-এর বৈশিষ্ট্য

১. **রিয়েল-টাইম থ্রেট প্রোটেকশন**
ভাইরাস, ম্যালওয়্যার, ওয়ার্ম, ট্রোজান ইত্যাদি আক্রমণ রিয়েল-টাইমে শনাক্ত ও প্রতিরোধ করে।

২. **Web Protection (Safe Web Browsing)**
বিপজ্জনক ওয়েবসাইট, ফিশিং লিঙ্ক ও ভুয়া ডাউনলোড থেকে সুরক্ষা দেয়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৩. **Firewall Protection**
অননুমোদিত নেটওয়ার্ক অ্যাক্সেস বন্ধ করে।

৪. **Password Manager**
নিরাপদে পাসওয়ার্ড সংরক্ষণ ও স্বয়ংক্রিয়ভাবে পূরণ করার সুবিধা দেয়।

৫. **Identity Theft Protection**
অনলাইনে ব্যক্তিগত তথ্য চুরি হওয়া প্রতিরোধে সহায়তা করে।

৬. **Multi-Device Support**
এক লাইসেন্সে একাধিক ডিভাইসে সুরক্ষা দেয়।

৭. **PC Optimization Tools**
সিস্টেমের পারফরম্যান্স বাড়ানোর জন্য অপ্রয়োজনীয় ফাইল ও ক্যাশ মুছে দেয়।

McAfee ব্যবহার ও প্রতিরোধের উপায়

- নিয়মিত স্ক্যান চালানো → ভাইরাস ও ম্যালওয়্যার দ্রুত শনাক্ত ও অপসারণের জন্য।
- সফটওয়্যার আপডেট রাখতে হবে → সর্বশেষ সিকিউরিটি ফিচার পেতে।
- Web Advisor চালু রাখতে হবে → ব্রাউজিংয়ের সময় বিপজ্জনক সাইট এড়াতে।
- Firewall সক্রিয় রাখতে হবে → হ্যাকারদের অননুমোদিত অ্যাক্সেস প্রতিরোধে।
- Password Manager ব্যবহার করতে হবে → শক্তিশালী ও অনন্য পাসওয়ার্ড সংরক্ষণে।
- অটো-রিনিউয়াল চালু রাখতে হবে → লাইসেন্স মেয়াদ শেষ হলে সুরক্ষা যেন বন্ধ না হয়।

Firewall (ফায়ারওয়াল)

ফায়ারওয়াল হলো একটি সিকিউরিটি সিস্টেম যা কম্পিউটার বা নেটওয়ার্কে প্রবেশ ও প্রস্থান করা ডেটা ট্র্যাফিক নিয়ন্ত্রণ করে। এটি নির্দিষ্ট নিয়ম অনুযায়ী অনুমোদিত (allowed) ডেটা প্রবেশ করতে দেয় এবং অননুমোদিত (unauthorized) ডেটা ব্লক করে। ফায়ারওয়াল হার্ডওয়্যার বা সফটওয়্যার উভয় রূপেই হতে পারে।

Firewall-এর বৈশিষ্ট্য

১. **ট্র্যাফিক মনিটরিং**
ইনকামিং ও আউটগোয়িং ডেটা প্যাকেট পরীক্ষা করে।

২. **Access Control**
নির্দিষ্ট IP ঠিকানা, পোর্ট, বা অ্যাপ্লিকেশন অনুযায়ী ট্র্যাফিক অনুমোদন বা ব্লক করে।

৩. **Packet Filtering**
প্রতিটি প্যাকেট যাচাই করে নিয়ম অনুযায়ী অনুমতি দেয় বা আটকায়।

৪. **Network Address Translation (NAT)**
নেটওয়ার্কের অভ্যন্তরের IP ঠিকানা বাইরের থেকে লুকিয়ে রাখে।

৫. **Intrusion Prevention**
সন্দেহজনক কার্যকলাপ শনাক্ত করে তাৎক্ষণিকভাবে ব্লক করে।

৬. **Logging and Alerts**
নিরাপত্তা ঘটনার রেকর্ড সংরক্ষণ করে এবং প্রয়োজন হলে সতর্কবার্তা পাঠায়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

Firewall-এর ধরন

১. **Hardware Firewall**
আলাদা ডিভাইস যা নেটওয়ার্ক ট্র্যাফিক নিয়ন্ত্রণ করে। সাধারণত বড় প্রতিষ্ঠানে ব্যবহৃত হয়।

২. **Software Firewall**
কম্পিউটার বা সার্ভারে ইন্সটল করা সফটওয়্যার যা ট্র্যাফিক নিয়ন্ত্রণ করে।

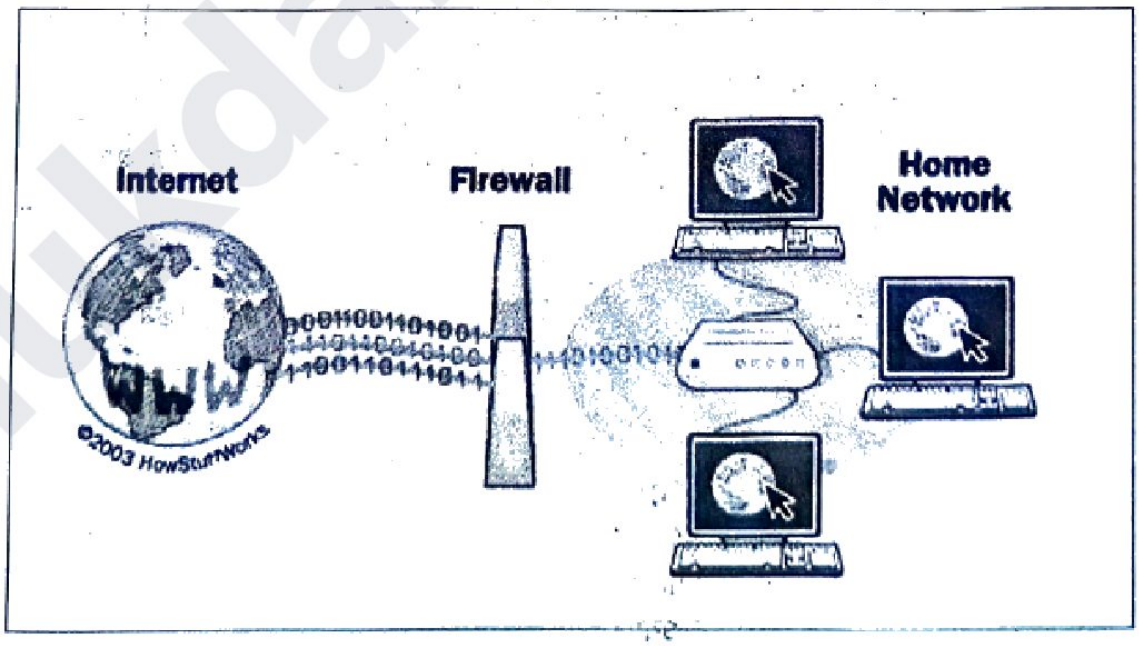
৩. **Network Firewall**
পুরো নেটওয়ার্ক সুরক্ষিত রাখে।

৪. **Host-based Firewall**
নির্দিষ্ট ডিভাইসকে সুরক্ষা দেয়।

৫. **Next-Generation Firewall (NGFW)**
ডিপ প্যাকেট ইন্সপেকশন, অ্যাপ্লিকেশন কন্ট্রোল এবং অ্যাডভান্সড থ্রেট প্রিভেনশন সুবিধা দেয়।

Firewall ব্যবহারের উপায় ও সুরক্ষা কৌশল

- Firewall চালু রাখতে হবে → Windows, macOS, বা রাউটার সেটিংসে ফায়ারওয়াল সক্রিয় রাখতে হবে।
- নিয়ম আপডেট করতে হবে → IP, পোর্ট ও অ্যাপ্লিকেশন অ্যাক্সেস নিয়ম প্রয়োজন অনুযায়ী হালনাগাদ করতে হবে।
- অপ্রয়োজনীয় পোর্ট বন্ধ করতে হবে → হ্যাকারদের প্রবেশ পথ কমাতে।
- Firewall লগ মনিটর করতে হবে → সন্দেহজনক কার্যকলাপ দ্রুত শনাক্ত করতে।
- হার্ডওয়্যার + সফটওয়্যার ফায়ারওয়াল একসাথে ব্যবহার করতে হবে → সর্বোচ্চ সুরক্ষার জন্য।



ছবি উৎস : www.comodo.com

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

Windows Firewall (উইন্ডোজ ফায়ারওয়াল)

Windows Firewall হলো Microsoft Windows অপারেটিং সিস্টেমে বিল্ট-ইন একটি নেটওয়ার্ক সুরক্ষা ব্যবস্থা, যা অননুমোদিত ইনকামিং ও আউটগোয়িং নেটওয়ার্ক ট্র্যাফিক ব্লক করে এবং অনুমোদিত ট্র্যাফিককে অনুমতি দেয়। এটি Windows XP Service Pack 2 থেকে শুরু করে সর্বশেষ Windows সংস্করণগুলোতে অন্তর্ভুক্ত রয়েছে।

Windows Firewall-এর বৈশিষ্ট্য

১. **Built-in Security**
Windows-এর সাথে বিনামূল্যে আসে, অতিরিক্ত ইনস্টলেশন প্রয়োজন হয় না।

২. **Inbound ও Outbound Filtering**
ইনকামিং ও আউটগোয়িং কানেকশন নিয়ন্ত্রণ করে।

৩. **Profile Based Protection**
Domain, Private, ও Public নেটওয়ার্ক প্রোফাইল অনুযায়ী আলাদা সুরক্ষা প্রদান।

৪. **Application Control**
নির্দিষ্ট প্রোগ্রামকে নেটওয়ার্কে প্রবেশ বা বের হওয়া ব্লক বা অনুমোদন করা যায়।

৫. **Logging System**
সন্দেহজনক কার্যকলাপ বা ব্লক হওয়া ট্র্যাফিক রেকর্ড রাখে।

৬. **Integration with Windows Security Center**
সিস্টেমের অন্যান্য সুরক্ষা ফিচারের সাথে সমন্বয় করে কাজ করে।

Windows Firewall ব্যবহারের উপায়

১. **Firewall চালু বা বন্ধ করা**
Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off

২. **Allowed Apps সেট করা**
Allow an app or feature through Windows Defender Firewall এ গিয়ে নির্দিষ্ট অ্যাপ নির্বাচন করতে হবে।

৩. **Advanced Settings ব্যবহার**
Advanced Security থেকে নির্দিষ্ট Inbound ও Outbound Rules তৈরি বা পরিবর্তন করতে হবে।

৪. **Firewall লগ চেক করা**
Advanced Settings → Monitoring → Security Logging।

Windows Firewall ব্যবহারের সুরক্ষা কৌশল

- সবসময় Firewall ON রাখতে হবে।
- পাবলিক Wi-Fi তে থাকলে Public Network Profile ব্যবহার করতে হবে।
- অপ্রয়োজনীয় অ্যাপ্লিকেশনের নেটওয়ার্ক অ্যাক্সেস বন্ধ করতে হবে।
- নিয়মিত Windows Update করো, যাতে Firewall সর্বশেষ সুরক্ষা পায়।

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

অনুশীলনী

ক. সঠিক উত্তরটি খাতায় লেখো :

১. নিচের কোনটি ডিজিটাল নীতির বৈশিষ্ট্য?
ক. গোপনীয়তা রক্ষা
খ. অবৈধ সফটওয়্যার ব্যবহার
গ. ভাইরাস তৈরি
ঘ. ট্রাফিক জ্যাম

২. ডিজিটাল নীতির মাধ্যমে কোনটি নিশ্চিত করা যায়?
ক. মোবাইল খরচ কমানো
খ. তথ্যের গোপনীয়তা
গ. ফাইল হারানো
ঘ. গেম খেলার নিয়ম

৩. কীসের মাধ্যমে নেটওয়ার্কে প্রবেশ নিয়ন্ত্রণ করা হয়?
ক. ফায়ারওয়াল
খ. ক্যালেন্ডার
গ. ওয়ার্ড প্রসেসর
ঘ. ক্যামেরা

৪. নিরাপদ অনলাইন ব্যবহারে কী করণীয়?
ক. ফিশিং ইমেইল খুলা
খ. সন্দেহজনক লিঙ্ক এড়ানো
গ. অজানা সফটওয়্যার ইন্সটল
ঘ. পাবলিক Wi-Fi এ পাসওয়ার্ড শেয়ার

উত্তরমালা : ১. ক; ২. খ; ৩. ক; ৪. খ।

খ. শূন্যস্থান পূরণ (Fill in the blanks) :

১. ডিজিটাল নীতি/ নৈতিকতার একটি গুরুত্বপূর্ণ দিক হলো ব্যক্তিগত তথ্য, পাসওয়ার্ড বা সংবেদনশীল ডেটা ..... রাখা।
উত্তর : গোপনীয়তা রক্ষা

২. অনলাইনে আইন ও নিয়ম মেনে চলা বা অনৈতিক কাজ এড়ানোকে বলা হয় .....।
উত্তর : আইনি ও নৈতিক সীমার মধ্যে থাকা

৩. একজন ব্যবহারকারী তার অনলাইনে করা কাজের ফলাফলের জন্য দায়িত্বশীল এবং ..... থাকে।
উত্তর : জবাবদিহিতা

৪. কম্পিউটার, নেটওয়ার্ক ও তথ্যকে ভাইরাস, ম্যালওয়্যার ও হ্যাকিং থেকে রক্ষা করার জন্য ব্যবহৃত সফটওয়্যারকে বলা হয় .....।
উত্তর : নিরাপত্তা সরঞ্জাম

৫. নিরাপদ নেটওয়ার্ক সংযোগের জন্য যে প্রযুক্তি ব্যবহার করা হয় এবং এটি ট্র্যাফিক নিয়ন্ত্রণ করে, তাকে বলা হয় .....।
উত্তর : ফায়ারওয়াল

Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

গ. Matching (মিলকরণ) :

কলাম-A (পরিভাষা)	কলাম-B (ব্যাখ্যা)
১. সততা ও সত্যনিষ্ঠা	ক. নেটওয়ার্কে প্রবেশ ও প্রস্থান করা ডেটা ট্র্যাফিক নিয়ন্ত্রণ করে, অনুমোদিত ট্রাফিককে দেয় এবং অননুমোদিত ট্রাফিক ব্লক করে।
২. গোপনীয়তা রক্ষা	খ. কম্পিউটার ও নেটওয়ার্ককে ভাইরাস, ম্যালওয়্যার ও অন্যান্য হুমকি থেকে রক্ষা করে।
৩. দায়িত্বশীলতা ও জবাবদিহিতা	গ. অনলাইনে করা কাজের ফলাফলের জন্য দায়িত্ব নেওয়া।
৪. Security Tools (নিরাপত্তা সরঞ্জাম)	ঘ. ব্যক্তিগত তথ্য, পাসওয়ার্ড বা সংবেদনশীল ডেটা অন্যের কাছে প্রকাশ না করা।
৫. ফায়ারওয়াল	ঙ. ডিজিটাল তথ্য ব্যবহার বা শেয়ার করার সময় সত্যনিষ্ঠ থাকা।

উত্তরমালা : ১→ঙ, ২→ঘ, ৩→গ, ৪→খ, ৫→ক

ঘ. অতিসংক্ষিপ্ত প্রশ্ন :

১. ডিজিটাল নীতি/নৈতিকতা কী?
২. ফায়ারওয়াল কী?
৩. Windows Firewall কী?
৪. নিরাপত্তা সরঞ্জাম কী?
৫. দুটি জনপ্রিয় নিরাপত্তা সরঞ্জামের নাম লেখো।
৬. Kaspersky কী?
৭. Kaspersky এর দুটি বৈশিষ্ট্য লেখো।
৮. Norton কী?
৯. Norton এর দুটি বৈশিষ্ট্য লেখো।
১০. অ্যাভাস্ট কী?
১১. অ্যাভাস্ট এর দুটি বৈশিষ্ট্য লেখো।
১২. McAfee কী?
১৩. McAfee এর দুটি বৈশিষ্ট্য লেখো।
১৪. ফায়ারওয়াল কী?
১৫. ফায়ারওয়াল এর দুটি বৈশিষ্ট্য লেখো।
১৬. ফায়ারওয়াল এর দুটি ধরন লেখো।
১৭. Windows Firewall কী?
১৮. Windows Firewall দুটি বৈশিষ্ট্য লেখো।

ঙ. সংক্ষিপ্ত প্রশ্ন :

১. ডিজিটাল নীতির প্রধান বৈশিষ্ট্যগুলো কী কী?
২. অনলাইনে গোপনীয়তা রক্ষার অর্থ কী?
৩. ডিজিটাল নীতি মেনে চলার ফলে কী ধরনের সুবিধা পাওয়া যায়?
৪. ফায়ারওয়াল কী এবং এর উদ্দেশ্য কী?
৫. ফায়ারওয়ালের প্রধান বৈশিষ্ট্যগুলো লেখো।
৬. ফায়ারওয়ালের প্রধান ধরনগুলো কী কী?

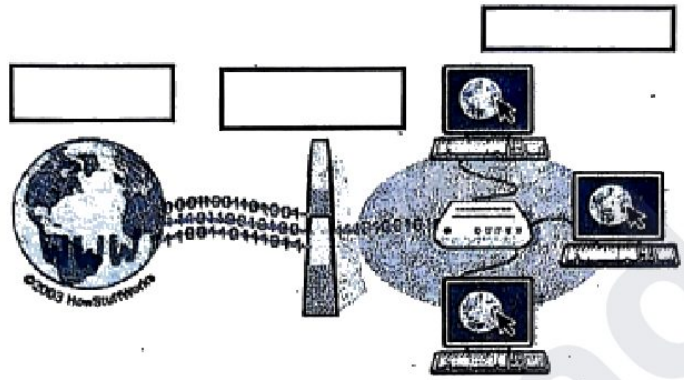
Talukdar Academy
Visit Our Website: all.talukdaracademy.com.bd

Visit Our Website: all.talukdaracademy.com.bd

৭. Windows ফায়ারওয়ালের বৈশিষ্ট্যগুলোর একটি উদাহরণ দাও।
৮. Kaspersky সফটওয়্যারের প্রধান বৈশিষ্ট্য কী কী?
৯. Norton সফটওয়্যারের নিরাপত্তা বৈশিষ্ট্যগুলো কী কী?
১০. অনলাইনে নিরাপদ ব্যবহার নিশ্চিত করতে নীতি ও নিরাপত্তা সরঞ্জাম একসাথে কীভাবে সাহায্য করে?

চ. চিত্রভিত্তিক প্রশ্ন :

১. চিত্রের ফাঁকা বক্সগুলোতে সঠিক নাম লেখ এবং বিশ্লেষণ করো।



ছ. ধাপ/প্রক্রিয়ামূলক প্রশ্ন :

১. Windows ফায়ারওয়াল ব্যবহার ও সেটিং করার পদ্ধতি ব্যাখ্যা করো।
২. Kaspersky সফটওয়্যার ব্যবহার ও প্রতিরোধ কৌশল ব্যাখ্যা করো।

জ. বর্ণনামূলক প্রশ্ন :

১. ডিজিটাল নীতি/নৈতিকতা কেন গুরুত্বপূর্ণ? উদাহরণসহ ব্যাখ্যা করো।
২. সততা, দায়িত্বশীলতা ও সম্মান বজায় রাখার মাধ্যমে অনলাইনে কীভাবে নিরাপদ পরিবেশ তৈরি হয়?
৩. ফায়ারওয়াল কীভাবে অননুমোদিত নেটওয়ার্ক প্রবেশ রোধ করে তা ব্যাখ্যা করো।
৪. Norton সফটওয়্যারের নিরাপত্তা বৈশিষ্ট্য ও ব্যবহারের উপায় বিশদভাবে ব্যাখ্যা করো।
৫. নেটওয়ার্ক সুরক্ষা সরঞ্জাম ও অ্যান্টিভাইরাস সফটওয়্যার একত্রে ব্যবহার করার গুরুত্ব ব্যাখ্যা করো।
৬. ডিজিটাল নীতি মেনে চললে অনলাইনে দায়িত্বশীল ব্যবহার কীভাবে নিশ্চিত হয় তা ব্যাখ্যা করো।
৭. ফায়ারওয়াল এবং অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার করে ব্যক্তিগত তথ্য ও ডিভাইস কীভাবে সুরক্ষিত রাখা যায় তা বিশদভাবে ব্যাখ্যা করো।
৮. ডিজিটাল নীতি ও নিরাপত্তা সরঞ্জামের মাধ্যমে শিক্ষার্থী বা ব্যবহারকারী কিভাবে সৃজনশীলতা ও শিক্ষাগত উন্নয়ন নিশ্চিত করতে পারে তা উদাহরণসহ ব্যাখ্যা করো।

Visit Our Website: all.talukdaracademy.com.bd