কলেজপাড়া যুব
কম্পিউটার প্রশিক্ষণ কেন্দ্র

BOOK

BASIC

CYBER SECURITY

OUR PROFESSIONAL COURSE PARTNER

AN ISO 9001: 2015 CERTIFIED ORGANIZATION
NHIIT
Where passions meet Opportunity

📖 অধ্যায় ১: সাইবার সিকিউরিটি কী ও কেন?

🔐 সাইবার সিকিউরিটি কী?

সাইবার সিকিউরিটি (Cyber Security) হল ডিজিটাল জগতে আমাদের ব্যক্তিগত তথ্য, কম্পিউটার, মোবাইল, নেটওয়ার্ক এবং অন্যান্য ইলেকট্রনিক সিস্টেমকে **অননুমোদিত প্রবেশ, আক্রমণ, ক্ষতি বা চুরির হাত থেকে রক্ষা করার একটি ব্যবস্থা**।

আমরা প্রতিদিন ইন্টারনেট ব্যবহার করি—চ্যাট করি, অনলাইন কেনাকাটা করি, টাকা লেনদেন করি, সামাজিক যোগাযোগ মাধ্যমে সময় কাটাই। এসব কাজের মাধ্যমে আমাদের অনেক ব্যক্তিগত তথ্য (যেমনঃ নাম, ফোন নম্বর, ব্যাঙ্ক অ্যাকাউন্ট, পাসওয়ার্ড) অনলাইনে ছড়িয়ে পড়ে। এগুলো চুরি বা হ্যাক হয়ে গেলে আমাদের জীবনে বড় ধরনের বিপদ ঘটতে পারে।

এমন অবস্থায় সাইবার সিকিউরিটি আমাদের **ডিজিটাল দেহরক্ষী** হিসেবে কাজ করে।

🎯 সাইবার সিকিউরিটি কেন গুরুত্বপূর্ণ?

1. ✅ **ব্যক্তিগত তথ্য রক্ষা:** আধুনিক যুগে ব্যক্তিগত তথ্য সবচেয়ে মূল্যবান সম্পদ।
2. 💰 **আর্থিক নিরাপত্তা:** অনলাইনে লেনদেন নিরাপদ রাখা জরুরি—হ্যাকাররা এটিএম কার্ড, UPI, ব্যাংক অ্যাকাউন্ট হ্যাক করতে পারে।
3. 🏢 **প্রাতিষ্ঠানিক নিরাপত্তা:** ব্যাংক, হাসপাতাল, সরকারী অফিসের তথ্য রক্ষাও সাইবার সিকিউরিটির অন্তর্গত।
4. 🛡️ **জাতীয় নিরাপত্তা:** দেশের প্রতিরক্ষা, প্রশাসনিক যোগাযোগ—সবই এখন ডিজিটাল। একে রক্ষা করাও সাইবার সিকিউরিটির অংশ।

🌍 কিছু বাস্তব উদাহরণ (ভারতের প্রেক্ষাপটে)

- **২০১৬** সালে Indian Army-এর একাধিক অফিসারের ই-মেইল হ্যাক করে পাকিস্তানি হ্যাকার গ্রুপ তথ্য চুরি করেছিল।
- **২০২০** সালে Maharashtra Power Grid-এ সাইবার হামলার কারণে কিছু এলাকা অন্ধকারে ডুবে গিয়েছিল — এটি চীনা হ্যাকারদের কৃতকর্ম বলে ধারণা।

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

📌 এই বইটি থেকে আপনি কী শিখবেন?

এই বইয়ে আপনি শিখবেন—

- ✓ সাধারণ মানুষ কীভাবে সহজ ভাষায় সাইবার ঝুঁকি বুঝতে পারে।
- ✓ কিভাবে প্রতিদিনকার জীবনে নিরাপদ থাকতে হবে (ফিশিং, ভাইরাস, পাসওয়ার্ড ব্যবস্থাপনা ইত্যাদি)।
- ✓ ভারতে বিদ্যমান সাইবার আইন ও সংবিধানিক দৃষ্টিভঙ্গি।
- ✓ বাস্তব সাইবার অপরাধ ও তার প্রতিকার।

📖 অধ্যায় ২: কুকিজ ও ক্যাশে ফাইল — সাইবার নিরাপত্তায় ভূমিকা

◆ কুকিজ (Cookies) কী?

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

কুকিজ হল ছোট ছোট ফাইল যেগুলো আপনি কোনও ওয়েবসাইটে প্রবেশ করলেই আপনার ব্রাউজারে স্বয়ংক্রিয়ভাবে ডাউনলোড হয়ে যায়। এই ফাইলগুলিতে থাকে:

- ❖ আপনার লগইন তথ্য
- ❖ আপনি কী ব্রাউজ করলেন
- ❖ আপনার পছন্দ বা অবস্থান

➡️ কুকিজ ওয়েবসাইটকে সাহায্য করে আপনাকে চিনতে এবং বারবার তথ্য চাওয়ার ঝামেলা কমায়। যেমনঃ Facebook, Amazon এ বারবার লগইন না করেও প্রবেশ করতে পারা।

📌 তবে হ্যাকাররা যদি কুকিজ চুরি করতে পারে, তাহলে আপনার একাউন্টে অনুপ্রবেশ করতে পারে। এটাকে বলা হয় **Session Hijacking**।

◆ ক্যাশে (Cache) ফাইল কী?

ক্যাশে ফাইল হল অস্থায়ী ডেটা যেগুলো আপনার ব্রাউজারে জমা হয় যেন পরবর্তী বার সেই ওয়েবপেজ আরও দ্রুত লোড হয়। যেমনঃ ছবি, HTML, CSS ইত্যাদি।

🧠 যেমন: আপনি যদি YouTube খুলে থাকেন, তার লোগো বা থাম্বনেইল ব্রাউজারে ক্যাশে হয়ে থাকবে, যাতে পরেরবার দ্রুত খোলে।

⚠️ কিন্তু পুরনো ক্যাশে ফাইল আপনার গোপনীয়তা বা নিরাপত্তা বিপন্ন করতে পারে। তাই মাঝে মাঝে ক্যাশে ক্লিয়ার করাও গুরুত্বপূর্ণ।

✅ সাইবার সিকিউরিটিতে এদের ভূমিকা

বিষয়	সুবিধা	ঝুঁকি
Cookies	ওয়েবসাইট ব্যবহারে সুবিধা	একাউন্ট হাইজ্যাক, ট্র্যাকিং
Cache	দ্রুত লোডিং	পুরনো বা সংবেদনশীল ডেটা ফাঁস

সতর্কতা:

- Public Computer-এ Browsing শেষে Cookies ও Cache Clear করুন
- Browser এর "Incognito Mode" ব্যবহার করুন
- Trusted Site ছাড়া Cookies Allow করবেন না

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

📝 অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. _____ are tiny files which get downloaded automatically when we visit a website.	Cookies	Caches	Bots	Crawlers	A
২. _____ gets propagated through networks and replicates itself.	Worms	Antivirus	Malware	Multimedia files	C

📖 অধ্যায় ৩: ম্যালওয়্যার, ভাইরাস ও ওয়ার্ম — কীভাবে ছড়ায় ও কীভাবে রক্ষা করবেন

🔍 ম্যালওয়্যার (Malware) কী?

Malware শব্দটি এসেছে "Malicious Software" থেকে — অর্থাৎ, ক্ষতিকর সফটওয়্যার। এটি তৈরি করা হয় কম্পিউটার বা মোবাইলের ভিতরে অনুপ্রবেশ করে তথ্য চুরি, ক্ষতি বা নিয়ন্ত্রণ নেওয়ার জন্য।

ম্যালওয়্যার বিভিন্ন ধরণের হতে পারে:

- **ভাইরাস (Virus)**
- **ওয়ার্ম (Worm)**
- **ট্রোজান (Trojan)**
- **স্পাইওয়্যার (Spyware)**
- **র‍্যানসমওয়্যার (Ransomware)**

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

🔍 ভাইরাস ও ওয়ার্ম: পার্থক্য কী?

বৈশিষ্ট্য	ভাইরাস	ওয়ার্ম
নিজের কপি তৈরি	বাহ্যিক ফাইলের সাহায্যে ছড়ায়	নিজে নিজেই ছড়াতে পারে
ফাইল সংযুক্তি	হ্যাঁ	না
ছড়ানোর গতি	তুলনামূলক ধীর	খুব দ্রুত

🧠 উদাহরণ:

- **ILOVEYOU Virus** (২০০০ সাল)
- **WannaCry Worm** (২০১৭ সালে বিশ্বব্যাপী হ্যাকিং)

💻 কম্পিউটারে ম্যালওয়্যার কীভাবে প্রবেশ করে?

- সন্দেহজনক ইমেইল লিঙ্কে ক্লিক করলে
- অজানা সফটওয়্যার ইনস্টল করলে
- ফ্রিতে কিছু ডাউনলোড করলে
- পেনড্রাইভ বা এক্সটারনাল ডিভাইস থেকে

🛡 কীভাবে ম্যালওয়্যার থেকে বাঁচবেন?

1. ✅ **নির্ভরযোগ্য অ্যান্টি-ভাইরাস সফটওয়্যার** ব্যবহার করুন
   যেমন: Norton, Windows Defender, Quick Heal
2. 🔄 সফটওয়্যার **নিয়মিত আপডেট** করুন
3. 🚫 সন্দেহজনক লিঙ্ক বা ইমেইলে ক্লিক করবেন না
4. 🔒 শক্তিশালী পাসওয়ার্ড ও ফায়ারওয়াল ব্যবহার করুন
5. 📂 অপ্রয়োজনীয় ফাইল বা অ্যাপ আনইনস্টল করুন

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

📝 অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. নিচের কোনটি একটি অ্যান্টি-ম্যালওয়্যার টুল?	Norton Antivirus	Windows Defender	Anti-malware	Microsoft Security Essentials	B
২. সঠিক না ভুল? কিছু ম্যালওয়্যার আছে যা মোবাইল ও কম্পিউটার দুটোতেই কাজ করে।	True	False	Vulnerability	Threat	A
৩. Worm ও Virus-এর মধ্যে পার্থক্য কী?	ওয়ার্ম কপি তৈরি করে না	ভাইরাস ফাইল ইনফেক্ট করে, ওয়ার্ম খায়	ওয়ার্ম বিশেষ কাজে ব্যবহৃত ভাইরাস	ওয়ার্ম ফাইল ছাড়াই ছড়ায়	D
৪. নিচের কোনগুলো ভাইরাসের ধরন?	Parasitic	Bootstrap sector	Companion	সবগুলো	D

৫. নিচের কোনটি অ্যান্টি-ভাইরাস সফটওয়্যার?	Norton	K7	Quick Heal	সবগুলো	D
৬. নিচের কোনটি খুব পরিচিত অ্যান্টি-ভাইরাস নয়?	AVAST	SMAG	AVG	McAFee	B

📖 অধ্যায় ৪: সফটওয়্যার আপডেট ও সিস্টেম নিরাপত্তা

🔄 সফটওয়্যার আপডেট কী?

সফটওয়্যার আপডেট হল একটি প্রক্রিয়া যার মাধ্যমে একটি সফটওয়্যারের নতুন সংস্করণ ইনস্টল করা হয়। এতে যুক্ত হয়:

- ❖ নতুন বৈশিষ্ট্য (Features)
- ❖ পূর্বের বাগ বা সমস্যা সমাধান (Bug Fixes)
- ❖ **নতুন নিরাপত্তা ব্যবস্থা (Security Patch)**

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

➡️ আপডেট না করলে ডিভাইসটি **হ্যাকারদের আক্রমণের ঝুঁকিতে** পড়ে যেতে পারে।

🤔 আপডেট না করলে কী হতে পারে?

1. 💣 **পুরনো দুর্বলতা (Vulnerabilities)** থেকে হ্যাকার প্রবেশ করতে পারে
2. 🔒 Personal Data চুরি হতে পারে
3. 🐞 সফটওয়্যারে সমস্যা, ফ্রিজ বা হ্যাং হতে পারে
4. 🚫 কিছু অ্যাপ কাজ করা বন্ধ করে দিতে পারে

🔐 সিস্টেম সফটওয়্যার কী?

সিস্টেম সফটওয়্যার হল এমন একটি সফটওয়্যার যেটি কম্পিউটার বা মোবাইলের হার্ডওয়্যার ও ইউজারের মধ্যে সংযোগ ঘটায়। যেমনঃ

- Windows (PC)
- Android (Mobile)
- iOS (Apple Devices)

➡️ সিস্টেম সফটওয়্যার সঠিকভাবে আপডেট না করলে পুরো ডিভাইস বিপন্ন হতে পারে।

🛡️ নিরাপত্তা রক্ষায় করণীয়:

করণীয়	কারণ
✅ নিয়মিত আপডেট	নিরাপত্তা দুর্বলতা দূর করে
🔒 পাসওয়ার্ড পরিবর্তন	অ্যাক্সেস নিরাপদ করে
🔍 সফটওয়্যার রিভিউ দেখে ইনস্টল	ভুয়া অ্যাপ এড়াতে সহায়তা করে
⛔ অজানা ফাইল বা সফটওয়্যার চালানো বন্ধ	ভাইরাস ছড়ানো রোধ করে

📝 অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

কম্পিউটার প্রশিক্ষণ কেন্দ্র

নিচের প্রশ্নগুলো এই অধ্যায়ের জ্ঞান যাচাইয়ের জন্য তৈরি:

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. সফটওয়্যার আপডেটের উদ্দেশ্য কী?	নতুন সফটওয়্যার কিনতে	হার্ডওয়্যার বদলানো	বাগ ফিক্স ও সিকিউরিটি বাড়ানো	ফোন হ্যাং করা	C
২. কোনটি সিস্টেম সফটওয়্যার?	MS Word	Chrome	Windows	Photoshop	C
৩. কোনটি নিয়মিত আপডেট না করলে বিপদ হতে পারে?	Calculator App	System Software	Music Player	Gallery	B
৪. আপডেট ছাড়া কোনটি হতে পারে?	নিরাপত্তা দুর্বলতা	নতুন ফিচার	ডিভাইস দ্রুত চলা	আরও ব্যাটারি ব্যাকআপ	A

📖 অধ্যায় ৫: ফিশিং, স্প্যামিং ,হ্যাকিং— চেনা ও প্রতিরোধের উপায় ও হ্যাকার

🎣 ফিশিং (Phishing) কী?

ফিশিং হল এমন এক ধরণের প্রতারণা যেখানে হ্যাকার আপনাকে ভুয়া ইমেইল বা ওয়েবসাইট পাঠায় এবং আপনি নিজের অজান্তে **ব্যক্তিগত তথ্য (ব্যাংক, পাসওয়ার্ড)** দিয়ে ফেলেন।

🧠 সাধারণ লক্ষণ:

- আপনার ব্যাংক থেকে ইমেইল এসেছে দাবি করা
- ক্লিক করতে বলা হচ্ছে একটি লিঙ্কে
- বলা হচ্ছে আপনার অ্যাকাউন্ট বন্ধ হয়ে যাবে

🧨 এইসব লিঙ্কে ক্লিক করলেই আপনি হ্যাকারদের হাতে তথ্য তুলে দিচ্ছেন।

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

📩 স্প্যাম (Spam) কী?

স্প্যাম হল অবাঞ্ছিত বার্তা বা ইমেইল যেগুলো আপনার অনুমতি ছাড়া পাঠানো হয়।

🔍 সাধারণ স্প্যাম উদাহরণ:

- অজানা অফার বা লটারি জেতার বার্তা
- ক্লিক করে পুরস্কার জেতার প্রলোভন
- অদ্ভুত লিঙ্ক ও অ্যাটাচমেন্ট

➡️ স্প্যামের মাধ্যমে **ম্যালওয়্যার বা ফিশিং আক্রমণ** করা হয়ে থাকে।

🧠 হ্যাকিং কী?

হ্যাকিং হল অন্য কারো কম্পিউটার বা সিস্টেমে বেআইনিভাবে প্রবেশ করে তথ্য চুরি বা ক্ষতি করা।

প্রচলিত হ্যাকিং পদ্ধতি:

- **Phreaking:** মোবাইল বা টেলিফোন হ্যাকিংয়ের প্রাচীনতম পদ্ধতি
- **Pharming:** ভুয়া ওয়েবসাইট তৈরি করে ডাটা চুরি
- **Keylogger:** কী টাইপ করছেন, তা রেকর্ড করা

প্রতিরোধের উপায়

সমস্যা	প্রতিরোধের উপায়
ফিশিং	অজানা ইমেইলের লিঙ্কে ক্লিক করবেন না
স্প্যাম	Spam Filter অন রাখুন, অজানা অ্যাটাচমেন্ট খুলবেন না
হ্যাকিং	শক্তিশালী পাসওয়ার্ড ব্যবহার করুন, ২-FA চালু রাখুন

✅ নিজের ডিভাইসে **Antivirus ও Firewall** আপডেট রাখুন

✅ পাবলিক ওয়াইফাই ব্যবহার করার সময় সতর্ক থাকুন

✅ প্রতিটি অ্যাকাউন্টে আলাদা পাসওয়ার্ড ব্যবহার করুন

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

হ্যাকার কাদের বলে?

হ্যাকার হল সেই ব্যক্তি, যিনি কম্পিউটার সিস্টেম, নেটওয়ার্ক বা সফটওয়্যারের গঠন ও কার্যপ্রণালী সম্পর্কে গভীর জ্ঞান রাখেন এবং এই জ্ঞানের সাহায্যে সিস্টেমে প্রবেশ করতে পারেন — সেটা ভালো বা খারাপ উদ্দেশ্যেই হোক।

✅ হ্যাকাররা যা করতে পারে:

- সিস্টেমের দুর্বলতা খুঁজে বের করা
- তথ্য সংগ্রহ বা পরিবর্তন করা
- নিরাপত্তা জোরদার করা (নৈতিক হ্যাকাররা)
- বেআইনি প্রবেশ করে ক্ষতি করা (অনৈতিক হ্যাকাররা)

🧠 হ্যাকারদের প্রকারভেদ (Types of Hackers)

হ্যাকারদের উদ্দেশ্য, নৈতিকতা ও কাজের পদ্ধতির উপর ভিত্তি করে কয়েকটি প্রধান ভাগে ভাগ করা হয়:

১. সাদা টুপি হ্যাকার (White Hat Hacker)

👉 এরা নৈতিক হ্যাকার।

🎯 কাজ: সিস্টেমের দুর্বলতা খুঁজে বের করে তা ঠিক করা।

🛡️ সাইবার নিরাপত্তা রক্ষা করাই এদের লক্ষ্য।

✅ আইনি অনুমতির সাথে কাজ করে।

📌 যেমন: নিরাপত্তা বিশ্লেষক, ইথিক্যাল হ্যাকার।

২. কালো টুপি হ্যাকার (Black Hat Hacker)

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

👉 এরা অনৈতিক হ্যাকার।

🎯 কাজ: বেআইনি ভাবে সিস্টেমে প্রবেশ করে ক্ষতি করা, তথ্য চুরি, ভাইরাস ছড়ানো ইত্যাদি।

💣 এদের কাজ আইনের পরিপন্থী।

📌 যেমন: সাইবার অপরাধী, তথ্য চোর।

৩. ধূসর টুপি হ্যাকার (Gray Hat Hacker)

👉 এরা সাদা ও কালো টুপির মাঝামাঝি অবস্থানে।

🎯 কাজ: অনুমতি ছাড়া হ্যাক করলেও অনেক সময় ক্ষতি না করে সমস্যা জানিয়ে দেয়।

❗ কিছুটা অনৈতিক হলেও অনেক সময় উপকারী হয়।

৪. লাল টুপি হ্যাকার (Red Hat Hacker)

👉 এরা মূলত সাদা টুপি হ্যাকারদের মতোই কিন্তু আগ্রাসী।

🎯 কাজ: কালো টুপি হ্যাকারদের বিরুদ্ধে লড়াই করা।

🔥 কখনো কখনো কালো হ্যাকারদের সিস্টেমে আক্রমণও করে।

৫. নীল টুপি হ্যাকার (Blue Hat Hacker)

👉 এরা প্রতিশোধপরায়ণ বা অপেশাদার হ্যাকার।

🎯 কাজ: কারো উপর রাগ থেকে বা আনন্দের জন্য হ্যাক করা।

🧪 কখনো কখনো সফটওয়্যার পরীক্ষায় অংশ নেয়।

৬. সবুজ টুপি হ্যাকার (Green Hat Hacker)

👉 এরা নতুন বা শিক্ষানবিস হ্যাকার।

🎯 কাজ: শেখার জন্য হ্যাকিং চর্চা করা।

📚 এদের লক্ষ্য — দক্ষ হ্যাকার হওয়া।

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

৭. হ্যাকার্টিভিস্ট (Hacktivist)

👉 এরা সামাজিক বা রাজনৈতিক বার্তা পৌঁছাতে হ্যাক করে।

🎯 কাজ: কোন আন্দোলন, প্রতিবাদ বা সচেতনতা ছড়ানো।

📌 যেমন: ওয়েবসাইট ডিফেস করা, সরকারবিরোধী বার্তা দেওয়া।

৮. স্ক্রিপ্ট কিডি (Script Kiddie)

👉 এরা পেশাদার নয়, শুধু ইন্টারনেট থেকে ডাউনলোড করা টুল বা স্ক্রিপ্ট ব্যবহার করে।

🎯 কাজ: নিজে না বুঝে হ্যাকিং করা, শো অফ করার মানসিকতা।

⚠️ সাধারণত বিপজ্জনক নয়, কিন্তু ক্ষতি করতে পারে।

উপসংহার

হ্যাকার মানেই খারাপ নয়। কারো উদ্দেশ্য যদি ইতিবাচক হয়, তবে সেই হ্যাকার সাইবার সিকিউরিটির জন্য খুবই গুরুত্বপূর্ণ।
এজন্য হ্যাকারদের সঠিকভাবে চেনা ও বুঝা দরকার।

অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. Identify the oldest phone hacking technique used.	Spamming	Phreaking	Cracking	Phishing	B
২. Try not to keep _____ passwords.	Biometric	PIN-based	Alphanumeric	Short	A
৩. Where might a spammer get your personal information?	Facebook	MySpace	LinkedIn	All of these	D
৪. Which of the following are direct harms caused by spamming?	Loss of productivity	Increased downloading costs	Increased infrastructure costs	All of the above	D
৫. Which of the following is not an appropriate way to hack mobile?	Target mobile hardware vulnerabilities	Target apps' vulnerabilities	Setup Keyloggers and spyware	Snatch the phone	D
৬. Which of the following is not an email-related hacking tool?	Mail Password	Email Finder Pro	Mail PassView	Sendinc	D
৭. Which of the following is the hacking approach used in phishing?	Pharming	Website-Duplication	Mimicking	Spamming	A
৮. Which of the following spam filtering techniques uses rules and keywords?	Community Filtering	Bayesian Filtering	Challenge-Response Filtering	Keyword Filtering	D

📖 অধ্যায় ৬: পাসওয়ার্ড ব্যবস্থাপনা ও দুই ধাপ যাচাইকরণ (2FA)

🔑 পাসওয়ার্ড কী?

পাসওয়ার্ড একটি সিক্রেট কোড যা দিয়ে ব্যবহারকারী নিজের অ্যাকাউন্টে প্রবেশ করতে পারেন। এটি একটি নিরাপত্তা প্রাচীরের মতো কাজ করে।

👀 কিন্তু যদি পাসওয়ার্ড দুর্বল হয়, তাহলে হ্যাকার খুব সহজেই সেটি ভেঙে ফেলতে পারে।

🧪 কীভাবে পাসওয়ার্ড চুরি হয়?

1. **ডিকশনারি অ্যাটাক (Dictionary Attack):**
   - হ্যাকার সাধারণ শব্দ ব্যবহার করে পাসওয়ার্ড অনুমান করার চেষ্টা করে।
2. **ব্রুট ফোর্স অ্যাটাক:**
   - সব ধরণের সম্ভাব্য কম্বিনেশন ট্রাই করা হয়।
3. **ফিশিং / কী-লগার:**
   - আপনি টাইপ করলে সেই পাসওয়ার্ড রেকর্ড হয়ে যায়।
4. **পাসওয়ার্ড ব্রাউজারে সংরক্ষণ:**
   - এটি সুবিধাজনক হলেও, **ব্রাউজার হ্যাক হলে** আপনার সব পাসওয়ার্ড চলে যেতে পারে।

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

✅ শক্তিশালী পাসওয়ার্ড কেমন হওয়া উচিত?

- কমপক্ষে ৮-১২ অক্ষরের
- বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন যুক্ত
- অনুমান করা কঠিন (যেমন: P@55w0rd!23)

✕ দুর্বল পাসওয়ার্ডের উদাহরণ:

- 123456
- password
- abc123
- নিজের নাম + জন্মতারিখ

২-স্তরের যাচাইকরণ (Two Factor Authentication - 2FA)

এই পদ্ধতিতে লগইনের সময় শুধু পাসওয়ার্ড নয়, **অতিরিক্ত একটি ধাপ** প্রয়োজন হয়। যেমন:

- OTP (মোবাইলে আসা কোড)
- অ্যাপ ভিত্তিক কোড (Google Authenticator)
- ফিঙ্গারপ্রিন্ট/ফেস আইডি

➡ এটি আপনার অ্যাকাউন্টকে আরও **নিরাপদ** করে।

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

কিভাবে নিজেকে নিরাপদ রাখবেন?

করণীয়	ব্যাখ্যা
শক্তিশালী পাসওয়ার্ড ব্যবহার	অনুমান করা কঠিন হয়
প্রতিটি অ্যাকাউন্টে আলাদা পাসওয়ার্ড	একটার সমস্যা অন্য অ্যাকাউন্টে ছড়ায় না
নিয়মিত পাসওয়ার্ড পরিবর্তন	ঝুঁকি কমায়
2FA চালু রাখুন	পাসওয়ার্ড চুরি হলেও হ্যাকার ঢুকতে পারবে না
ব্রাউজারে পাসওয়ার্ড সেভ না করা	নিরাপত্তা বাড়ে

অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. A _____ is a process of breaking a password using a list of words.	Dictionary attack	Phishing attack	Social engineering attack	MiTM attack	A
২. Password are used to improve the_____of a Network/Application.	Performance	Reliability	Application Security	All of the above	D
৩. Saving passwords in the browser is a good habit.	True	False			B
৪. Try not to keep _____ passwords, especially on social platforms.	Biometric	PIN-based	Alphanumeric	Short	A

অধ্যায় ৭: ভারতের সাইবার আইন ও সংবিধানে সাইবার নিরাপত্তা

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

সাইবার আইন কী?

সাইবার আইন বা **আইটি আইন (Information Technology Act, 2000)** হল একটি আইন যা ভারতে ইলেকট্রনিক লেনদেন, ডিজিটাল সিগনেচার, এবং সাইবার অপরাধ নিয়ন্ত্রণে সহায়তা করে।

ভারতের আইটি আইন (IT Act 2000)

আইটি অ্যাক্ট, ২০০০ সালের মাধ্যমে সাইবার অপরাধগুলোর বিরুদ্ধে বিচারিক পদক্ষেপ নেওয়া সম্ভব হয়। এতে কয়েকটি গুরুত্বপূর্ণ ধারা আছে:

ধারা	বিবরণ
ধারা 43	বিনা অনুমতিতে অন্যের কম্পিউটারে প্রবেশ বা ক্ষতি করলে জরিমানা হতে পারে
ধারা 66	কম্পিউটার রিসোর্সের অপব্যবহার করলে **তিন বছরের জেল বা জরিমানা** হতে পারে

ধারা 66C	আইডেন্টিটি চুরি সংক্রান্ত অপরাধ (পাসওয়ার্ড, ডিজিটাল সিগনেচার চুরি)
ধারা 66D	ফিশিং ও অনলাইন প্রতারণা
ধারা 67	অশ্লীল কনটেন্ট ছড়ানো (pornographic materials)
ধারা 70	গুরুত্বপূর্ণ তথ্য পরিকাঠামো রক্ষা সংক্রান্ত

ভারতীয় দণ্ডবিধি (IPC) এর প্রাসঙ্গিক ধারা

ধারা	অপরাধ	শাস্তি
ধারা 419	ভুয়া পরিচয় ব্যবহার	জেল ও জরিমানা
ধারা 420	অনলাইন প্রতারণা	৭ বছর পর্যন্ত জেল
ধারা 500	অনলাইন মানহানি	২ বছর জেল বা জরিমানা
ধারা 506	অনলাইনে হুমকি	শাস্তিযোগ্য অপরাধ

ভারতের সংবিধানে প্রাসঙ্গিক ধারা

কম্পিউটার প্রশিক্ষণ কেন্দ্র

ধারা	ব্যাখ্যা
অনুচ্ছেদ 21	প্রত্যেক নাগরিকের জীবনের অধিকার আছে — এর মধ্যে **Privacy** অন্তর্ভুক্ত
অনুচ্ছেদ 19(1)(a)	বাক স্বাধীনতা, কিন্তু এর অপব্যবহার করলে আইনগত ব্যবস্থা নেওয়া যায়
ডিজিটাল ব্যক্তিগত তথ্য সুরক্ষা বিল, 2023 (DPDP Bill)	নাগরিকদের ডিজিটাল তথ্য রক্ষা নিশ্চিত করতে তৈরি

আপনি যদি সাইবার অপরাধের শিকার হন?

➡ এই পদক্ষেপগুলি গ্রহণ করুন:

1. 📲 www.cybercrime.gov.in তে অভিযোগ করুন
2. 🏢 নিকটস্থ সাইবার থানায় অভিযোগ জানান
3. 📞 1930 – সাইবার হেল্পলাইন নম্বর

অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. _____monitors user activity on internet and can steal personal information.	Malware	Spyware	Adware	None of these	B
২. Once activated _____ can enable _____ to misuse your data.	virus, cyber-criminals	malware, penetration testers	trojans, cyber-criminals	virus, penetration testers	C
৩. Which of the following act violates cyber security the most?	Exploit	Attack	security auditors	cyber-criminals	B
৪. Which of the following actions compromise cyber security?	Vulnerability	Attack	Threat	Exploit	C
৫. Which of the following is the most viral section on cybercrime platforms?	Chat Messenger	Social networking sites	Tutorial sites	Chat-rooms	B
৬. Which of the following type of attack can activate cybercriminals?	Both Active and Passive attack	Neither Active nor Passive attack	Active attack	Passive attack	C

কম্পিউটার প্রশিক্ষণ কেন্দ্র

অধ্যায় ৮: ভারতে ঘটে যাওয়া বাস্তব সাইবার আক্রমণ

সাইবার আক্রমণ মানে এমন এক ধরনের অনুপ্রবেশ যা ডিজিটাল পদ্ধতিতে কম্পিউটার সিস্টেম, নেটওয়ার্ক, কিংবা তথ্য চুরি বা ক্ষতি করতে ব্যবহার করা হয়।

ভারতে ঘটে যাওয়া গুরুত্বপূর্ণ সাইবার হামলার ঘটনা

১. Cosmos Bank হ্যাক (২০১৮, পুনে)

- **হ্যাকাররা** ম্যালওয়্যার ব্যবহার করে ব্যাংকের সার্ভারে প্রবেশ করে।
- মাত্র ২ দিনে **৯৪ কোটি টাকার বেশি টাকা চুরি** হয়।
- আক্রমণকারীরা বিশ্বব্যাপী ২৮টি দেশের ATM ব্যবহার করে টাকা তুলে নেয়।

২. Aadhaar Data Leak (২০১৭)

- ১০ কোটিরও বেশি ভারতীয় নাগরিকের ব্যক্তিগত তথ্য ফাঁস হয়ে যায়।
- UIDAI-এর নিরাপত্তায় ফাঁক থাকার কারণে এই ঘটনা ঘটে।

৩. AIIMS Delhi Ransomware Attack (২০২২)

- AIIMS-এর সার্ভার র‍্যানসমওয়্যারে আক্রান্ত হয়, ফলে মেডিক্যাল রেকর্ড অ্যাক্সেস করা বন্ধ হয়ে যায়।
- হ্যাকাররা **cryptocurrency-তে মুক্তিপণ** দাবি করে।

৪. Indian Nuclear Power Plant (Kudankulam Attack, ২০১৯)

- North Korea-এর Lazarus গ্রুপ দ্বারা পরিচালিত সাইবার হামলা।
- লক্ষ্য ছিলো plant-এর administrative network।

কলেজপাড়া যুব

সাধারণ সাইবার আক্রমণের ধরন

আক্রমণের ধরন	ব্যাখ্যা
Phishing	ভুয়া ইমেইল বা লিংকের মাধ্যমে তথ্য চুরি
Malware	ভাইরাস, ট্রোজান, স্পাইওয়্যার দিয়ে ডিভাইস নিয়ন্ত্রণ নেওয়া
DDoS Attack	সার্ভারকে অতিরিক্ত অনুরোধ পাঠিয়ে ডাউন করে ফেলা
Brute Force Attack	পাসওয়ার্ড অনুমানের মাধ্যমে সিস্টেমে প্রবেশ
Trojan Horse	সাধারণ অ্যাপ্লিকেশনের আড়ালে হ্যাকিং টুল

আক্রমণের লক্ষণ

- ডিভাইস হঠাৎ ধীরগতির হয়ে যাওয়া
- অজানা অ্যাপ ইন্সটল হওয়া
- ওয়েবসাইট/অ্যাকাউন্টে অজানা লগইন

- ফাইল হঠাৎ গায়েব হওয়া

কিভাবে সাইবার হামলা রোধ করবেন?

- অজানা ইমেইলে ক্লিক করবেন না
- সবসময় অ্যান্টি-ভাইরাস আপডেট রাখুন
- 2FA চালু রাখুন
- নিয়মিত ব্যাকআপ নিন
- সফটওয়্যার হালনাগাদ রাখুন

অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
১. _____ is an anti-malware tool found on most Windows systems.	Norton Antivirus	Windows Defender	Anti-malware	Microsoft Security Essentials	B
২. Attackers could steal _____ to achieve identity theft.	plug-ins	cache	cookies	history	C
৩. Brute force attack is _____	fast	inefficient	slow	complex to understand	C
৪. Trojan creators do not look for _____	Credit card information	Confidential data	Securing systems	Important documents	C
৫. True or False? Malware exists which affects both software and hardware.	True	False	Vulnerability	Threat	A
৬. What is the difference between a worm and Virus?	Worms don't replicate	Virus infects, worm eats	Worms target specific	Worm doesn't attach like virus	D
৭. What is the top method an attacker might infect a system?	Social engineering	SQL injection	Buffer overflow	Hacking via Internet	A
৮. Which of the following is a type of cyber attack?	Phishing	SQL Injection	Password Attack	All of the above	D

📖 অধ্যায় ৯: ব্যবহারকারীদের জন্য সাইবার নিরাপত্তা পরামর্শ ও নৈতিকতা

🔐 নিরাপদ ডিজিটাল জীবনযাপনের মূলমন্ত্র

আজকের যুগে ইন্টারনেট আমাদের জীবনের অবিচ্ছেদ্য অংশ। তাই প্রয়োজন সচেতনতা ও সতর্কতা। কিছু সহজ অভ্যাস আপনাকে রাখতে পারে সাইবার আক্রমণ থেকে মুক্ত।

✅ ব্যবহারকারীদের জন্য গুরুত্বপূর্ণ সাইবার নিরাপত্তা পরামর্শ

পরামর্শ	ব্যাখ্যা
১. শক্তিশালী পাসওয়ার্ড ব্যবহার করুন	পাসওয়ার্ডে অক্ষর, সংখ্যা ও চিহ্ন ব্যবহার করুন (যেমন: R@ju#98!)
২. 2FA (Two-Factor Authentication) চালু রাখুন	লগইনের সময় দ্বিতীয় স্তরের যাচাইকরণ
৩. VPN ব্যবহার করুন	পাবলিক Wi-Fi ব্যবহারের সময় ব্যক্তিগত তথ্য গোপন রাখে
৪. নিয়মিত সফটওয়্যার আপডেট করুন	পুরোনো সফটওয়্যারে নিরাপত্তা ফাঁক থাকতে পারে
৫. সন্দেহজনক লিংকে ক্লিক করবেন না	ফিশিং এড়াতে লিংকের উৎস যাচাই করুন
৬. গুরুত্বপূর্ণ ডেটা ব্যাকআপ রাখুন	র‍্যানসমওয়্যার আক্রমণে উপকারী
৭. সোশ্যাল মিডিয়ায় সীমিত তথ্য শেয়ার করুন	পরিচয় চুরি ও হুমকির আশঙ্কা কমে
৮. অফিসিয়াল অ্যান্টিভাইরাস ব্যবহার করুন	রিয়েলটাইম সুরক্ষা দেয়
৯. সাইবার অপরাধ হলে রিপোর্ট করুন	www.cybercrime.gov.in বা **1930** নম্বরে জানাতে ভুলবেন না

ডিজিটাল নৈতিকতা (Cyber Ethics)

নিয়ম	ব্যাখ্যা
অনলাইন সম্মান বজায় রাখুন	কাউকে হয়রানি, হুমকি বা অপমান করবেন না
অন্যের তথ্যের গোপনীয়তা বজায় রাখুন	অনুমতি ছাড়া কারো তথ্য শেয়ার নয়
কপিরাইট মানুন	চুরি করা কনটেন্ট ব্যবহার নয়
ফেক নিউজ ছড়াবেন না	যাচাই না করে তথ্য শেয়ার করা অনৈতিক
শিক্ষামূলক উদ্দেশ্যে ইন্টারনেট ব্যবহার করুন	অপব্যবহার থেকে বিরত থাকুন

বাস্তব জীবনের অনুশীলন:

1. আপনি যদি অজানা লিংক পান—কী করবেন?
2. আপনার ফেসবুক একাউন্ট হ্যাক হলে কী করবেন?
3. Wi-Fi পাসওয়ার্ড কীভাবে নিরাপদ রাখবেন?
4. আপনার ছবি যদি অনলাইনে কেউ বিকৃত করে পোস্ট করে, তাহলে কী আইনগত পদক্ষেপ নেওয়া যায়?

কলেজপাড়া যুব কম্পিউটার প্রশিক্ষণ কেন্দ্র

অধ্যায়ের শেষে প্রশ্নোত্তর (MCQ)

প্রশ্ন	অপশন A	অপশন B	অপশন C	অপশন D	সঠিক উত্তর
1. What is the safest practice to prevent online frauds?	Avoiding social media	Strong password + 2FA	Opening all emails	Ignoring antivirus	B
2. What is 2FA used for?	Protecting hardware	Data backup	Authentication	Virus scanning	C
3. Which of the following is a cyber ethics rule?	Spreading hate	Sharing unknown links	Respecting privacy	Ignoring copyright	C
4. What should you do when using public Wi-Fi?	Log in to bank account	Use VPN	Share OTP	Turn off antivirus	B

5. What is cyberbullying?	Theft	Online abuse or harassment	Firewall testing	Antivirus attack	B
6. Where to report a cybercrime in India?	Facebook	cybercrime.gov.in	Twitter	police.net	B

কলেজপাড়া যুব
কম্পিউটার প্রশিক্ষণ কেন্দ্র

Unlock Your Potential with Students' Professional Courses

1. TALLY & GST
2. Advance Excel
3. Web Development
4. Kids Coding
5. Graphic Design

ChatGPT & AI Tools Training