অফলাইন প্রোটেকশন
লোকাল ডাটা রক্ষার উপায়

তাসনুভা মাহমুদ

প্রযুক্তিক বিশ্বে কমবেশি প্রায় সবাই এখন আতঙ্কিত তাদের ডাটা সুরক্ষার ব্যাপারে। তবে এ কথা সত্য, পাশ্চাত্য বিশ্বের তুলনায় তৃতীয় বিশ্বের লোকেরা বিশেষ করে বাংলাদেশের মতো স্ট্যাটাসের দেশের মানুষ ডাটার সুরক্ষার ব্যাপারে তেমন সচেতন নন। কেননা, এসব দেশের লোকেরা অনলাইনে যত না কাজ করেন তার চেয়ে অনেক গুণ বেশি কাজ করেন অফলাইনে। অফলাইনে থেকে দৈনন্দিন কমপিউটিং কাজ সম্পাদন করা হয় বলেই যে ডাটা শতভাগ সুরক্ষিত থাকবে তেমন নয়। অফলাইনে কাজ করলেও ডাটা হারানোর বা ক্ষতিগ্রস্ত হওয়ার ভয় থেকেই যায় বিভিন্ন কারণে। আর এই উপলব্ধিতে এবার কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালায় উপস্থাপন করা হয়েছে অফলাইনে তথা লোকাল ডাটা সুরক্ষাসংশ্লিষ্ট বিভিন্ন বিষয়।

লাখ লাখ বাগ, ওয়ার্ম, ভাইরাস এবং ম্যালওয়্যার ইন্টারনেটে বিচরণ করছে এবং আক্রান্ত করছে পিসিকে। বেশিরভাগ ব্যবহারকারীই তাদের পিসিতে অ্যান্টিভাইরাস প্রোগ্রাম ইনস্টল করেন, তারপরও ব্যবহারকারীকে ডাটার পরিপূর্ণ সুরক্ষা নিশ্চিত করার জন্য কিছু পদক্ষেপ নিতে হয়। কেননা প্রতিনিয়ত পিসির ভাইরাসের স্বভাব ও গতি-প্রকৃতি পরিবর্তন হচ্ছে। যার কারণে বিশ্বস্ত অ্যান্টিভাইরাস প্রোগ্রামও অনেক সময় ভাইরাস সংক্রমণকে শনাক্ত করতে পারে না। এমনকি কোনো কোনো ক্ষেত্রে ভাইরাস নিজেই স্টার্ট হতে পারে ম্যালিশাস অ্যান্টিভাইরাস ইনস্টলেশন থেকে। ম্যালওয়্যার বা ভাইরাস থেকে ডাটা রক্ষা করা ছাড়াও ব্যবহারকারীকে কিছু পদক্ষেপ নিতে হয়, যাতে ফাইল এবং হার্ডওয়্যার করাপ্ট অথবা ফিজিক্যাল সমস্যার কারণে ডাটা হারানো রোধ করা যায়। বেশিরভাগ ক্ষেত্রে এ ধরনের ঘটনা ঘটে থাকে দুর্ঘটনাক্রমে। এক্ষেত্রে ফাইল হ্যান্ডলিংয়ে নিয়মিত কিছু প্র্যাকটিসই আপনাকে দিতে পারে পরিপূর্ণ নিশ্চয়তা। ফলে আপনি কখনই অস্থির হবেন না গুরুত্বপূর্ণ কোনো ফাইল দুর্ঘটনাক্রমে ডিলিট হয়ে গেলে বা ডাটা করাপ্ট বা চুরি হয়ে গেলে।

হুমকি কী

আমাদের লোকাল ড্রাইভ গুরুত্বপূর্ণ সব ফাইলের লাইব্রেরির মতো। যদি আপনি খুবই প্রযুক্তিমনস্ক ব্যক্তি হয়ে থাকেন, তাহলে আপনার কাছে থাকতে পারে বছরব্যাপী গুরুত্বপূর্ণ ঘটনার ফটো ও ভিডিও, বিপুল পরিমাণে মুভি ও মিউজিকের সংগ্রহসহ গুরুত্বপূর্ণ ফাইল। এগুলোসহ পেনড্রাইভ ও এক্সটারনাল হার্ডড্রাইভ থাকার সম্ভাবনা রয়েছে যেখানে স্টোর করা থাকে গুরুত্বপূর্ণ ফাইল। খুব সঙ্গত কারণে আপনি চাইবেন না, এসব ফাইল অন্যের নাগালে চলে যাক। ভাইরাস ও ম্যালওয়্যার এসব ড্রাইভ করাপ্ট তথা নষ্ট করে দিতে পারে এবং সব ডাটাকে ব্যবহার অযোগ্য বা অর্থহীন করে ফেলতে পারে। পরিচয়বিহীন পিসি থেকে আপনার ডাটা চুরি হয়ে যেতে পারে বা চুরি হতে পারে এক্সটারনাল স্টোরেজ ডিভাইস থেকেও। সুতরাং ডাটাকে এমনভাবে স্টোর করতে হবে যাতে সবার নাগালের বাইরে থাকে, এমনকি স্টোরেজ ডিভাইসগুলো যদি অনাকাঙ্ক্ষিত ব্যক্তির নাগালে চলে যায় তাতেও যেনো ডাটা সুরক্ষিত থাকে তা নিশ্চিত করতে হবে।

যেভাবে করবেন

যদি অফলাইন মোডে কাজ করেন, তাহলে আপনার ডাটা তুলনামূলকভাবে বেশি নিরাপদ থাকবে। এক্ষেত্রে মূল হুমকি আসবে এক্সটারনাল স্টোরেজ ডিভাইস থেকে, যা ধারণ করতে পারে সংক্রমিত ফাইল। এক্সটারনাল ডিভাইসের মাধ্যমে বন্ধুবান্ধব বা সহকর্মীদের সাথে ডাটা বিনিময় করার সময় আপনার পিসি সংক্রমিত হতে পারে। আপনার পিসি প্রোটেকটেড থাকলেও অন্যের পিসি যদি প্রোটেকটেড না থাকে তাহলে এক্সটারনাল ডিভাইসের মাধ্যমে ডাটা বিনিময় করার সময় আপনার পিসি সংক্রমিত হতে পারে। এর ফলে ফাইল করাপ্ট করতে পারে যদিও তা সচরাচর দেখা যায় না। ফাইল করাপ্টশন হয় যদি ডকুমেন্ট যথাযথভাবে সেভ করা না হয় অথবা ফাইলে কাজ করার সময় প্রোগ্রাম ক্র্যাশ করলে। আপনি ফাইলকে ড্যামেজ করে ফেলতে পারেন যদি হঠাৎ করে পিসির পাওয়ার অফ করেন অথবা পিসি হ্যাং করার কারণে ম্যানুয়ালি পিসি রিস্টার্ট করলে।

ফাইল চুরি হতে পারে পাবলিক অ্যাক্সেস মেশিন থেকে অথবা আপনার নিজস্ব লোকাল মেশিন থেকে অনাকাঙ্ক্ষিত ব্যবহারকারীর মাধ্যমে। উইন্ডোজ এক্সপ্লোরার থেকে ফাইল ডিলিট করলে তা থেকেই যায় রিসাইকেল বিনে। আবার কিছু কিছু সফটওয়্যার তৈরি করে ফাইলের নিয়মিত ব্যাকআপ যেগুলো ব্যবহার হতে থাকে। অনাকাঙ্ক্ষিত ব্যবহারকারীদের যদি ডাটা চুরি করার উদ্দেশ্য থাকে, তাহলে রিসাইকেল বিন থেকে ফাইল রিস্টোর করতে পারে বা সার্চ করতে পারে ব্যাকআপ ফাইল বা টেম্পোরারি স্টোর করা ফাইল।

যেভাবে প্রতিরোধ করবেন

কমপিউটার ব্যবহারকারীর সচেতনতাই ডাটা সুরক্ষার নিয়মরীতি নিশ্চিত করতে পারে। যদি পিসি অরক্ষিত অবস্থায় ফেলে রাখেন বা আনলক অবস্থায় রাখেন তাহলে অনাকাঙ্ক্ষিত ব্যবহারকারীরা সহজেই আপনার পিসিতে অ্যাক্সেস পাবে। তাই আপনাকে সবসময় নিশ্চিত করতে হবে, আপনি ডাটাকে যথাযথভাবে সেভ করেছেন এবং বিভিন্ন ডিভাইস বা ড্রাইভে ওই ফাইলের মাল্টিপল কপি তৈরি করেছেন। কেননা কোনো সোর্সের ফাইল করাপ্ট করলেও অন্য সোর্সের ডাটা থাকবে সুরক্ষিত, যা দিয়ে চালিয়ে নিতে পারবেন কাজ।

পাসওয়ার্ড প্রোটেক্ট

অনাকাঙ্ক্ষিত ব্যবহারকারীদের প্রতিহত করার অর্থ হচ্ছে সবকিছুর জন্য পাসওয়ার্ড তৈরি করা। আপনি পাসওয়ার্ড লক তৈরি করতে পারেন বায়োস পাসওয়ার্ড সেটিংয়ের মাধ্যমে, যার ফলে পিসি স্টার্টআপের সময় পাসওয়ার্ড দিয়ে অ্যাক্সেস করতে হয়। পরবর্তী ধাপটি হলো অপারেটিং সিস্টেমের জন্য। আপনি বিভিন্ন ইউজার অ্যাকাউন্ট তৈরি করতে পারবেন, যার প্রতিটির জন্য রয়েছে নিজস্ব পাসওয়ার্ড। আপনি ইচ্ছে করলে নির্দিষ্ট ফোল্ডার ও ফাইলকে লুকিয়ে রাখতে পারবেন, যাতে সেগুলো পাসওয়ার্ড ছাড়া রান, কপি বা ট্রান্সফার করা না যায়।

বায়োসে পাসওয়ার্ড তৈরি করতে চাইলে আপনাকে অবশ্যই অপারেটিং সিস্টেম লোড হওয়ার আগে বায়োস সেটআপে এন্টার করতে হবে। পিসি বুট হওয়ার স্ক্রিনে প্রদর্শিত হবে এক সিরিজ ডায়াগনস্টিক টুল যেখানে বায়োস সেটআপ করার নির্দেশাবলী রয়েছে। বায়োসে সাধারণত অ্যাক্সেস করা হয় Del বা F2 ফাংশন কি চেপে। বায়োস সেটআপে রয়েছে সিকিউরিটি ট্যাব, যার মাধ্যমে পাবেন ইউজার পাসওয়ার্ড সেট করার অপশন। এখানে সেট করতে পারবেন ইউজার পাসওয়ার্ড যাতে আপনার সিস্টেম অপারেটিং সিস্টেম লোড করার আগে পাসওয়ার্ড অথেনটিকেশনের জন্য রিকোয়েস্ট করে। পাসওয়ার্ড সেট করার পর বায়োস সেটিং পরিবর্তনের কথা মনে রাখতে হবে যাতে প্রতিবার মেশিন চালু করলে পাসওয়ার্ডের জন্য প্রম্পট করে। এই অপশনটি পাবেন বায়োস ফিচার সেটআপ মেনুতে।

ইচ্ছে করলে ব্যবহার করতে পারেন সিকিউরিটি সফটওয়্যার, যা আপনাকে এনাবল করবে সুনির্দিষ্ট ফাইল এবং ফোল্ডারকে লক করার জন্য। টপ ল্যাং সফটওয়্যার নামের এক প্রতিষ্ঠান (Top Lang Software) তৈরি করেছে ফাইল লক ৬.১ (File Lock 6.1) নামের এক সফটওয়্যার যা আপনাকে ফাইল, ফোল্ডার বা সম্পূর্ণ ড্রাইভ লক করার সক্ষমতা দান করবে। আপনি ইচ্ছে করলে এক্সপ্লোরার থেকে ফাইল এবং ফোল্ডার লুকিয়ে রাখতে পারবেন। শুধু তাই নয়, সিডি/ডিভিডি ড্রাইভও লক করতে পারবেন। এ ধরনের টুল ব্যবহার করে অন্যদেরকে প্রতিরোধ করতে পারবেন যারা আপনার অজান্তে ফাইল বা ফোল্ডার কপি করার চেষ্টা করবে।

ব্যাকআপ তৈরি করা

কেউ বলতে পারবে না কখন, কিভাবে আপনার ফাইল করাপ্ট করবে। তবে মনে রাখা দরকার, সফটওয়্যার ম্যালফাংশন বা হার্ডওয়্যারের ড্যামেজের কারণে ফাইল করাপ্ট করতে পারে। তাই ডাটার নিরাপত্তার কথা বিবেচনায় রেখে ডাটার ব্যাকআপ তৈরি করা উচিত। ডাটা ব্যাকআপ করার জন্য ক্লাউড সার্ভার অপশন যেমন বেছে নিতে পারেন, তেমনি ভাবতে পারেন বিভিন্ন ড্রাইভে ফাইলের মাল্টিপল কপি সেভ করার কথা। বিপুল আকারের ডাটা ব্যাকআপের জন্য দরকার হতে পারে কিছু বিশেষ ধরনের সফটওয়্যার। সুপ্রতিষ্ঠিত ম্যানুফ্যাকচারার যেমন এইচপি, ডেল, লেনোভো প্রভৃতি কোম্পানি তাদের পণ্যের সাথে সিকিউরিটি স্যুট দিয়ে থাকে যেখানে সম্পৃক্ত থাকে ব্যাকআপ ফিচারও। যদি এ ধরনের কোনো স্যুট না থাকে তাহলে ব্যবহার করতে পারেন EaseUS Todo Backup বা Cobian Backup ধরনের সফটওয়্যার। এসব সফটওয়্যারের সাথে নির্দিষ্ট ফোল্ডার বা পুরো ড্রাইভের ব্যাকআপ তৈরির অপশন সমন্বিত রয়েছে। কিছু ব্যাকআপ সফটওয়্যার অফার করে ডাটা এনক্রিপ্ট অপশন এবং ব্যাকআপ ড্রাইভ বা ফোল্ডারের সাইজ কমানোর জন্য কম্প্রেস ফাইলও অফার করে।

ভালো সিকিউরিটি স্যুট

ভাইরাস বা ম্যালওয়্যার থেকে রক্ষা পাওয়ার সবচেয়ে ভালো ও বিশ্বস্ত উপায় হলো ভালো ও কার্যকর অ্যান্টিভাইরাস ব্যবহার করা। ইদানীং বেশিরভাগ সিকিউরিটি স্যুটের সাথে থাকে বান্ডেল আকারে বিভিন্ন ধরনের সার্ভিস, যেমন অ্যান্টিভাইরাস প্রোটেকশন থেকে শুরু করে স্প্যাম ব্লকার। মনে রাখা দরকার, একটি ভালো সিকিউরিটি সফটওয়্যার আপনাকে বিভিন্ন উপায়ে সুরক্ষিত করবে। যদি আপনার প্রতিষ্ঠানটি বেশ বড় ধরনের হয় যেখানে ডাটার নিরাপত্তার বিষয়টি খুবই গুরুত্বপূর্ণ সেখানে ফ্রি ভার্সনের সিকিউরিটি টুল ব্যবহার করার পরিবর্তে পেইড ভার্সনের টুল ব্যবহার করা উচিত। কেননা ফ্রি ভার্সনের টুলগুলো কিছু দিনের জন্য ফ্রি থাকে, যা ট্রায়াল ভার্সন হিসেবে পরিচিত। এসব ফ্রি ভার্সনে আবার কিছু কিছু ফিচার ব্লক করা থাকে। এ ছাড়া আরেকটি গুরুত্বপূর্ণ বিষয় হলো আপনার ব্যবহারের সফটওয়্যারগুলো যেনো সবসময় আপডেটেড হয় সে ব্যাপারে নিশ্চিত থাকতে হবে। ভালো মানের অ্যান্টিভাইরাস প্রোগ্রামগুলো নিয়মিতভাবে আপডেট করা হয় সর্বশেষ ভাইরাস ডাটাবেজ এবং লুপহোলের জন্য ফিক্স দিয়ে। সুতরাং নিয়মিত আপডেট দিয়ে পিসি কনফিগার করা খুবই গুরুত্বপূর্ণ কাজ।

ডাটা এনক্রিপ্ট করা

যদি আপনার ডাটা খুবই গুরুত্বপূর্ণ ও সংবেদনশীল হয়ে থাকে তাহলে এসব মূল্যবান ডাটা ইন্টারনেট বা এক্সটারনাল স্টোরেজ মিডিয়ার মাধ্যমে ট্রান্সফার করার সময় আপনাকে নিশ্চিত করতে হবে যে এসব ডাটায় থার্ড পার্টি ব্যবহারকারীরা যাতে অ্যাক্সেস না পায়। কোনো কোনো ক্ষেত্রে ডাটার সুরক্ষার জন্য ব্যবহার করা উচিত এনক্রিপশন সফটওয়্যার।

মাইক্রোসফট উইন্ডোজ ৭-এর কোনো কোনো ভার্সনে বিটলকার (BitLocker) টুলকে বান্ডেল আকারে দিয়েছে ব্যবহারকারীদেরকে। এই টুল ব্যবহার করে ব্যবহারকারীরা তাদের পিসি ও রিমুভাল ড্রাইভের ডাটাকে এনক্রিপ্ট করতে পারবে। এই সফটওয়্যারটি উইন্ডোজ ৭ আল্টিমেট বা এন্টারপ্রাইজ ভার্সনেই পাওয়া যাবে। তবে এনক্রিপ্টেড ফাইল ভিস্তা এবং এক্সপি অপারেটিং সিস্টেমেও পড়া যাবে।

ইচ্ছে করলে আপনি ট্রুক্রিপট (TrucCrypt) নামের ফ্রি টুল ব্যবহার করতে পারবেন। এই টুলটি মাল্টিপ্লাটফরম ওপেন সোর্স এনক্রিপশন প্রোগ্রাম ট্রুক্রিপট টুল দিয়ে ফাইল এনক্রিপ্ট করা যায় ড্রাইভে ফোল্ডার তৈরি করার মাধ্যমে এবং গুরুত্বপূর্ণ ও সংবেদনশীল ডকুমেন্টকে এনক্রিপ্টেড ফোল্ডারের মধ্যে রেখে অথবা সম্পূর্ণ পার্টিশন বা স্টোরেজ ডিভাইস যেমন ইউএসবি ফ্ল্যাশড্রাইভ বা পোর্টেবল হার্ডডিস্ককে এনক্রিপ্ট করতে পারবেন। ট্রুক্রিপট প্রোগ্রাম ব্যবহার করে মাল্টিপল এনক্রিপশন অ্যালগরিদম এবং স্টোর করে এনক্রিপশন ফাইলকে স্টোরেজ ডিভাইসের ট্রুক্রিপট এনক্রিপ্টেড ভলিউমে যা সাধারণ ফোল্ডারের মতো এবং এনক্রিপ্টেড ফাইল শনাক্ত করাকে প্রায় অসম্ভব করে ফেলেছে।

হার্ডওয়্যার নিরাপদ রাখা

ডাটা সুরক্ষার ব্যাপারে নিশ্চিত থাকতে চাইলে স্টোরেজ হার্ডওয়্যারকে অবশ্যই নিরাপদ রাখতে হবে। হার্ডওয়্যারের ফিজিক্যাল ড্যামেজ খুব সহজেই হতে পারে। তাই এক্সটারনাল স্টোরেজ ডিভাইসকে নিরাপদ জায়গায় যেমন রাখতে হবে তেমনি নিশ্চিত করতে হবে শক প্রুফকে। তাছাড়া ভোল্টেজ স্ট্যাবিলাইজার এবং ইউপিএস ব্যবহার করা উচিত বাধ্যতামূলকভাবে। কেননা আমাদের দেশে বিদ্যুতের বেহাল দশার কারণ ভোল্টেজের ওঠানামা যেমন হয় খুব বেশি তেমনি হয় বিদ্যুৎ যখন-তখন আসা-যাওয়া। এ দুটো বিষয়ই মূলত আমাদের দেশে হার্ডড্রাইভ ড্যামেজের প্রধান কারণ, যার কারণে লোকাল ডাটা তথা অফলাইন ডাটা হারানোর ঘটনা বেশি ঘটে থাকে।

ফিডব্যাক : swapan52002@yahoo.com

প্রোগ্রামিং সি/সি++

(৮৫ পৃষ্ঠার পর)

দেখলে বোঝা যাবে, লুপটি একটি অসীম লুপ। কারণ, এই লুপের এক্সপ্রেশন হিসেবে সরাসরি একটি নন-জিরো মান দেয়া হয়েছে এবং এই মানটির পরিবর্তনের কোনো ইনস্ট্রাকশন দেয়া নেই। অর্থাৎ যতবার এই এক্সপ্রেশনের মান চেক করা হবে ততবার একটি নন-জিরো মান পাওয়া যাবে অর্থাৎ লুপের কন্ডিশন সত্য বলে বিবেচিত হবে। প্রথমবার প্রোগ্রাম যখন লুপটিতে আসবে, তখন দেখবে যে কন্ডিশন সত্য, সুতরাং প্রোগ্রাম লুপে প্রবেশ করবে। এরপরে i-এর মান (১) প্রিন্ট করবে। এরপর i-এর মান ১ বাড়বে। তারপর চেক করবে i-এর মান ১০০ কি না। যদি ১০০ হয়, তাহলে লুপটি ব্রেক করবে অর্থাৎ প্রোগ্রাম লুপ থেকে বের হবে। আর যদি ১০০ না হয়, তাহলে প্রোগ্রাম আবার লুপের কন্ডিশনে ফিরে যাবে এবং দেখবে যে কন্ডিশন কি সত্য না মিথ্যা। এবারেও কন্ডিশন সত্য হবে, কারণ এক্সপ্রেশন হিসেবে সরাসরি একটি নন-জিরো মান দেয়ায় লুপটি অসীম হয়ে গেছে। দ্বিতীয়বার প্রোগ্রাম লুপটিতে প্রবেশ করার পর আবার i-এর মান প্রিন্ট করবে। এবার কিন্তু i-এর মান হিসেবে ২ প্রিন্ট করবে, কারণ পূর্বের লুপে i-এর মান ১ ইনক্রিমেন্ট অর্থাৎ বাড়ানো হয়েছে। এভাবে লুপটি চলতে থাকবে। অর্থাৎ এই প্রোগ্রামটি চালালে ১ থেকে ১০০ পর্যন্ত প্রিন্ট করা হবে। ১০০ প্রিন্ট করার পর যখন i-এর মান ১০১ হয়ে যাবে তখন প্রোগ্রাম Bd স্টেটমেন্টে প্রবেশ করবে এবং তখন if-এর কন্ডিশন সত্য হওয়ার জন্য প্রোগ্রাম লুপটি ব্রেক করবে। উল্লেখ্য, প্রোগ্রাম যখন একবার কোনো লুপ বা কেস ব্রেক করে তখন তাকে নির্দেশ না দেয়া পর্যন্ত নিজে থেকে কখনও ওই লুপ/কেসে প্রবেশ করে না।

কয়েক ধরনের এমন লুপ আছে সি ল্যাঙ্গুয়েজে। এদের একেকটির কাজ একেক রকম। তবে একটির কাজ অন্যটি দিয়ে করা সম্ভব। কেস এবং লুপ সম্পর্কে আরও ভালোভাবে জানার জন্য ইন্টারনেট ব্যবহার করা প্রয়োজন। ইন্টারনেট থেকে বিভিন্ন টিউটোরিয়াল দেখলে লুপ/কেস সম্পর্কে ধারণা আরও স্পষ্ট হবে।

ফিডব্যাক : wahid_cseaust@yahoo.com

www.comjagat.com

'কমজগৎ ডট কম' বাংলা ভাষায় সবচেয়ে বড় ও তথ্যসমৃদ্ধ ওয়েব পোর্টাল। এতে মাসিক কমপিউটার জগৎ-এ প্রকাশিত সব তথ্য অন্তর্ভুক্ত করা হয়েছে। এটি বাংলাদেশে তথ্যপ্রযুক্তিভিত্তিক প্রথম ও বহুল প্রচারিত মাসিক পত্রিকা, যা ১৯৯১ সালের মে মাস থেকে নিয়মিতভাবে প্রকাশিত হয়ে আসছে।