ল্যাপটপ নিরাপত্তার কয়েক ধাপ

তাসনীম মাহ্মুদ

কমপিউটার জগৎ-এর নিয়মিত বিভাগ ব্যবহারকারীর পাতার আগস্ট ২০১৫ সংখ্যায় ল্যাপটপ পরিচর্যার গাইডলাইন তুলে ধরা হয়। এরই ধারাবাহিকতায় এবারের সংখ্যায় ব্যবহারকারীর পাতায় উপস্থাপন করা হয়েছে ল্যাপটপ নিরাপত্তা বিধানের কয়েকটি ধাপ।

ধরুন, আগামীকাল সকালে ল্যাপটপ চালু করে দেখলেন আপনার কমপিউটারটি ভাইরাস আক্রান্ত হয়েছে এবং সব ফাইল গায়েব হয়ে গেছে। যেখানে রয়েছে আপনার পারিবারিক ছবিসহ অন্যান্য ছবি, অনলাইনের পাসওয়ার্ডের স্প্রেডশিট প্রভৃতি– তাহলে কেমন হবে? তাছাড়া ব্যবসায়িক কাজে যারা ল্যাপটপ নিয়ে চলাফেরা করেন, তারা সব সময় মারাত্মক নিরাপত্তা ঝুঁকির মধ্যে থাকেন। কেননা, অসাবধানবশত ল্যাপটপটি হারিয়ে যেতে পারে বা চুরি হয়ে যেতে পারে। এর ফলে আপনি যে শুধু আর্থিকভাবে ক্ষতিগ্রস্ত হবেন তা নয়, ব্যাংক অ্যাকাউন্ট নম্বর, ক্রেডিট কার্ড নম্বরসহ গোপনীয় ও গুরুত্বপূর্ণ তথ্য হারিয়ে যেতে পাওে, যা আপনার জন্য মারাত্মক ক্ষতির কারণ হয়ে দাঁড়াতে পারে। আপনার গুরুত্বপূর্ণ ও গোপনীয় সব তথ্য চলে যেতে পারে হ্যাকার বা অপরাধীদের নাগালে, যদি না ল্যাপটপটি কঠিন পাসওয়ার্ড দিয়ে সুরক্ষার ব্যবস্থা করা হয়। কেননা, কঠিন পাসওয়ার্ড বা সুদৃঢ় প্রতিরোধমূলক ব্যবস্থা না থাকায় হ্যাকারেরা খুব সহজে আপনার কমপিউটারে অ্যাক্সেস করে পুরো সিস্টেমের নিয়ন্ত্রণ নিতে যেমন পারবে, তেমনি হাতিয়ে নিতে পারবে আপনার গুরুত্বপূর্ণ তথ্য। সুতরাং এমন অনাকাঙ্ক্ষিত অবস্থা তথা হুমকি থেকে নিজেকে এবং নিজের প্রতিষ্ঠানকে সুরক্ষিত করতে নিচে বর্ণিত কৌশলগুলো অবলম্বন করতে হবে।

পাসওয়ার্ড প্রটেকশন

আপনার কমপিউটারে যাতে কেউ অনাকাঙ্ক্ষিতভাবে অ্যাক্সেস করতে না পারে, সেজন্য প্রথম ও প্রধান কাজ হলো প্রতিরক্ষামূলক ব্যবস্থা নেয়া। সুতরাং প্রথম প্রশ্ন হলো কী করে শক্তিশালী পাসওয়ার্ড দেয়া যায়? এ ক্ষেত্রে প্রথম লক্ষণীয় বিষয় হলো পাসওয়ার্ডের লেংথ, যা কোনো অবস্থাতেই ৮ ক্যারেক্টারের কম হওয়া উচিত নয় এবং যেখানে থাকবে বিভিন্ন ধরনের লেটার, নাম্বার, স্পেশাল ক্যারেক্টার ও সিম্বল। পাসওয়ার্ডে s বোঝাতে $ চিহ্ন এবং ! বোঝাতে i ব্যবহার করা থেকে বিরত থাকা উচিত। কেননা, হ্যাকারেরা এখন কোনো পাসওয়ার্ড ক্র্যাক করতে এসব চিহ্নকে যথেষ্ট গুরুত্বসহকারে নিয়ে থাকে।

পাসওয়ার্ড হিসেবে কখনই নিজের নাম, নিজের প্রতিষ্ঠানের নাম, ইউজার নেম, জন্মদিন ইত্যাদি ব্যবহার করা উচিত নয়। কেননা এগুলো ব্যাপকভাবে ব্যবহার হয়ে থাকে এবং খুব সহজেই অনুমেয়। আপনার প্রিয় গানের বা মুভির ছদ্মনাম ব্যবহার করতে পারেন।

ফায়ারওয়াল

ফায়াওয়াল দুই ধরনের। হার্ডওয়্যার ফায়ারওয়াল ও সফটওয়্যার ফায়ারওয়াল। রাউটার কাজ করে হার্ডওয়্যার ফায়ারওয়াল হিসেবে, পক্ষান্তরে উইন্ডোজ সম্পৃক্ত করেছে একটি সফটওয়্যার ফায়ারওয়াল। এছাড়া কিছু থার্ড পার্টি ফায়ারওয়াল আছে, যেগুলো কমপিউটারে ইনস্টল করে নিতে পারেন। ফায়ারওয়াল আপনার কমপিউটারে হ্যাকার,

ভাইরাস, ওয়ার্মসহ অবৈধ অনুপ্রবেশকারীর বিরুদ্ধে প্রতিরোধ গড়ে তোলে, যাতে অনাকাঙ্ক্ষিতভাবে কেউ সিস্টেমে অ্যাক্সেস করতে না পারে। রাউটারে ফায়ারওয়াল বিল্টইন হলেও নেটওয়ার্ক থ্রেডের বিরুদ্ধে নিরাপত্তা বিধানের জন্য আপনাকে নিশ্চিত করতে হবে কমপিউটারের ফায়ারওয়াল যেন সক্রিয় থাকে।

ইনস্টল করুন অ্যান্টিভাইরাস

অ্যান্টিভাইরাস, অ্যান্টিম্যালওয়্যার, অ্যান্টিস্পাইওয়্যার ও অ্যাড-ব্লকিং সফটওয়্যার ইত্যাদি আপনার কমপিউটারকে সাইবার সিকিউরিটি থ্রেড যেমন ম্যালওয়্যার, ওয়ার্ম, ট্রোজান হর্স ও হ্যাকার থেকে রক্ষা পাওয়ার জন্য সহায়তা করবে। বেশ কিছু অ্যান্টিভাইরাস

প্যাকেজে সম্পৃক্ত রয়েছে ম্যালওয়্যার ও স্পাইওয়্যার প্রটেকশন, তবে অ্যাড-ব্লকার বৈশিষ্ট্যসূচকভাবে আলাদাভাবে ডাউনলোড হয়। অ্যাড-ব্লকার সফটওয়্যার গুরুত্বপূর্ণ, কেননা এটি ম্যালওয়্যারের বিরুদ্ধে প্রতিরোধ গড়ে তোলে (ভুয়া ম্যালওয়্যার অনলাইন অ্যাডভারটাইজমেন্ট), যা আপনার কমপিউটারকেও আক্রান্ত করতে পারে।

নিয়মিত আপডেট করা

কমপিউটারে ভাইরাস প্রটেকশন সফটওয়্যার ইনস্টল করার পর আপনার প্রধান কাজ হবে কমপিউটারের অন্যান্য উপাদানের মতো অ্যান্টিভাইরাস সফটওয়্যারের পরিচর্যা করা, তথা নিয়মিতভাবে আপডেট রাখা। এজন্য মাঝে-মধ্যে আপডেটের জন্য চেক করা উচিত। তবে বেশিরভাগ সিস্টেম আপনাকে সতর্ক করে দেবে, যখনই কোনো আপডেট অ্যাভেইলেবেল হবে। সব ধরনের সফটওয়্যার বা অ্যাপ্লিকেশনের জন্য আপডেট খুবই গুরুত্বপূর্ণ। কেননা, কিছু কিছু আপডেট আগের অজানা সাইবার সিকিউরিটি থ্রেডের প্রতিকার হিসেবে কাজ করে। তবে অনেক ব্যবহারকারী আছেন, যারা নিয়মিতভাবে সফটওয়্যার বা অ্যাপ্লিকেশন আপডেট করাকে বিরক্তিকর কাজ মনে করেন এবং আপডেট করা থেকে বিরত থাকেন। এর ফলে তাদের সিস্টেমটি সবসময় ম্যালওয়্যার, ভাইরাস ও হ্যাকারের টার্গেটে পরিণত হয়। সুতরাং সিস্টেমকে সবসময় নিয়মিতভাবে আপডেট রাখা উচিত।

পাবলিক ওয়াইফাই এড়িয়ে চলা

ল্যাপটপ সিকিউরিটি থ্রেডের মধ্যে অন্যতম হলো পাবলিক ওয়াইফাই। অনিরাপদ পাবলিক ওয়াইফাই হটস্পট হ্যাকারদের সুযোগ করে দেয় আপনার কার্যকলাপের ওপর গোয়েন্দাগিরি করার। হ্যাকারদেরকে সুযোগ করে দেয় আপনার তথ্যে অ্যাক্সেসের। শুধু তাই নয়, আপনার তথ্যকে মডিফাই বা ডিলিটও করে ফেলতে পারে। এ বিষয়টি তাদের জন্য বিশেষভাবে সম্পর্কযুক্ত, যারা পাবলিক ওয়াইফাই হটস্পট থেকে পার্সোনাল অ্যাকাউন্টে অ্যাক্সেস করেন বা অনলাইন ব্যাংক ব্যবহার করেন। সুতরাং পাবলিক ওয়াইফাইয়ে কখনই যুক্ত হওয়া উচিত নয়। আপনার হোম ও বিজনেস ইন্টারনেট কানেকশন যাতে সব সময় পাসওয়ার্ড প্রোটেক্টেড থাকে তা নিশ্চিত করুন।

ব্যাকআপ রাখা

উপরে উল্লিখিত প্রতিটি কৌশলই আপনার ল্যাপটপের তথ্য নিরাপদ রাখতে সহায়ক ভূমিকা পালন করবে। বাস্তবে কোনো কিছুই আপনাকে পুরোপুরি নিরাপত্তা দিতে পারবে না। তাই গুরুত্বপূর্ণ ও সংবেদনশীল ডকুমেন্টগুলোর ব্যাকআপ একটি ইউএসবি এক্সটারনাল হার্ডড্রাইভে নেয়া উচিত। কেননা, দৈব কোনো দুর্ঘটনায় আপনার ডাটা হারিয়ে গেলে এই ব্যাকআপই হবে রক্ষাকবচ।

সিডি বা ইউএসবি থেকে বুট ডিজ্যাবল করা

ফ্রি রিসেটিং প্রোগ্রাম যেমন Pogostick বা Ophcrack ব্যবহার করে সহজে একটি অ্যাকাউন্ট পাসওয়ার্ড পরিবর্তন বা অপসারণ করতে পারবেন। তবে এসব প্রোগ্রাম রান করতে চাইলে কমপিউটারকে বুট করাতে হবে সিডি বা ইউএসবি স্টিক থেকে। আপনি খুব সহজেই ল্যাপটপের সিকিউরিটি বাড়াতে পারবেন সিডি বা ইউএসবি স্টিক প্রভৃতি ডিভাইস থেকে ল্যাপটপ বুটিং সুবিধাকে ডিজ্যাবল করার মাধ্যমে। এ কাজটি করতে পারবেন আপনার ল্যাপটপের বেসিক ইনপুট/আউটপুট সিস্টেমের (BIOS) সেটিং পরিবর্তন করে। বায়োস হলো মেশিনকে কন্ট্রোল করার জন্য জেনেরিক কোড সংবলিত বিল্টইন সফটওয়্যার, যেখানে সহজে অ্যাক্সেস করা যায় কমপিউটারের সুইচ অন করার সাথে F1, F4, F10 বা Del কী চেপে।

এ সেটিং কেউ ওভাররাইট করবে না তা নিশ্চিত করুন। বায়োসকে পাসওয়ার্ড প্রোটেক্ট করুন যাতে পাসওয়ার্ড এন্টার করা ছাড়া কোনো পরিবর্তন করা সম্ভব না হয়। এটিও বায়োস সেটিংয়ে কনফিগার করা যায়।

হার্ডড্রাইভ এনক্রিপ্ট করা

আপনার ল্যাপটপটি চুরি হয়ে গেলে বা হারিয়ে গেলে আপনার জন্য করার কিছুই থাকে না, যা প্রয়োগ করে চোরকে নিবৃত করতে পারবেন, যাতে সে আপনার হার্ডড্রাইভ থেকে কোনো তথ্য অপসারণ করতে পারবে না এবং এটিকে অন্য আরেকটি কমপিউটারের সাথে যুক্ত করতে পারবে না। এ কাজ করে যেকোনো অ্যাকাউন্ট পাসওয়ার্ড প্রটেকশন বাইপাস করুন এবং আপনার ডাটায় সহজে অ্যাক্সেস করার জন্য অনুমোদন দিন।

এ ক্ষেত্রে এটিকে প্রতিহত করার সেরা উপায় হলো আপনার ল্যাপটপের হার্ডড্রাইভকে এনক্রিপ্ট করা। এনক্রিপ্ট করা হার্ডড্রাইভে শুধু তখনই অ্যাক্সেস করা যাবে যখন আপনাকে এনক্রিপ্টশন কী দেয়া হবে। সাধারণত এটি হয় একটি পিন (PIN) ফরমে পাসওয়ার্ড অথবা কী সংবলিত ইউএসবি স্টিক ঢুকিয়ে।

আপনি ইচ্ছে করলে সম্পূর্ণ ড্রাইভকে এনক্রিপ্ট করতে পারবেন বিটলকার নামে একটি এনক্রিপ্টশন ইউটিলিটি ব্যবহার করে। এই টুলটি উইন্ডোজের কয়েকটি ভার্সনের যেমন উইন্ডোজ ভিস্তা, উইন্ডোজ ৭ ও উইন্ডোজ ৮ উপযোগী। এছাড়া বিকল্প হিসেবে ট্রুক্রিপ্ট নামে ওপেনসোর্সভিত্তিক আরেকটি এনক্রিপশন টুল রয়েছে, যা উইন্ডোজ এক্সপি, লিনআক্স এবং ওএসএক্সে কাজ করবে।

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার করা

বিমানবন্দর, সম্মেলন কক্ষ, হোটেল রুম ইত্যাদিতে অফার করা অ্যাক্সেসযোগ্য নেটওয়ার্ক ল্যাপটপ ব্যবহারকারীদের জন্য বিশেষভাবে নিরাপত্তা ঝুঁকিতে থাকে। কেননা, হ্যাকারেরা সাধারণত ফ্রি প্রোগ্রামকে পুঁজি করে একই নেটওয়ার্কে যুক্ত হয়। যেমন কেইন অ্যান্ড অ্যাবেল (Cain and Abel), ওয়্যারহার্ক (Wireshark) বা ইটারক্যাপ (Ettercap) এবং গোপনে ই-মেইলে উঁকিঝুঁকি মারে অথবা পাসওয়ার্ড কপি করে যেহেতু ডাটা নেটওয়ার্ক অতিক্রম করে যায়।

আপনার কমপিউটার ও অফিস নেটওয়ার্কের মধ্য দিয়ে ডাটা ট্রানজিট করার সময় অন্য নেটওয়ার্ক ব্যবহারকারীদের ইন্টারসেপশন থেকে ডাটার সুরক্ষার সেরা উপায় হলো কোম্পানির ভার্চুয়াল প্রাইভেট নেটওয়ার্ক তথা ভিপিএন ব্যবহার করে এনক্রিপ্ট করা।

যদি কোম্পানির ভিপিএনে অ্যাক্সেসের সুবিধা না থাকে তাহলে সার্ভিস প্রোভাইডারেরা এটি ব্যবহার করতে পারেন। যেমন স্ট্রিমভায়া (StreamVia) বা স্ট্রংভিপিএন (StrongVPN)। এটি নিশ্চিত করে আপনার ডাটা এনক্রিপটেড ও পাবলিক লোকাল নেটওয়ার্কের অন্য ব্যবহারকারীদের কাছ থেকে নিরাপদ।

সিকিউর ই-মেইল ব্যবহার করা

ভিপিএন সংযোগ কাজ করছে তা প্রমাণ করা কখনও কখনও কঠিন হয়ে পড়ে। সুতরাং কনফিগার করা যেকোনো ই-মেইল প্রোগ্রাম, ওয়েবমেইল সিস্টেম বা ক্লাউডভিত্তিক ই-মেইল সার্ভিস যাতে সিকিউর সকেট লেয়ার (SSL) বা ট্রান্সপোর্ট লেয়ার সিকিউরিটি (TLS) ব্যবহার করে তা নিশ্চিত করা বিচক্ষণতার পরিচায়ক। এটি নিশ্চিত করে আপনার ইউজার নেম ও পাসওয়ার্ড এবং ই-মেইল কনটেন্ট উভয়ই এনক্রিপটেড থাকে, যেহেতু এগুলো ইন্টারনেট জুড়ে ঘুরে বেড়ায়।

ওয়েবমেইল সার্ভিস যেমন জি-মেইল ও ক্লাউডভিত্তিক সার্ভিস যেমন মাইক্রোসফটের অফিস ৩৬৫ (Office 365) বাইডিফল্ট এভাবেই কনফিগার করা থাকে। তবে বিভিন্ন ইন্টারনেট সার্ভিস প্রোভাইডারের মাধ্যমে অফার করা মেইল নয়।

অন্যান্য ব্যবহারকারীর কাছ থেকে নিজেকে রক্ষা করা

একই বিজনেস সেন্টার বা হোটেল নেটওয়ার্কের সাথে সংযুক্ত অন্যান্য ম্যালিশাস ব্যবহারকারীর বিরুদ্ধে বাড়তি প্রটেকশনের জন্য আপনার ল্যাপটপকে ট্রাবল রাউটারের মাধ্যমে যুক্ত করুন, যা ইথারনেট জ্যাকে প্লাগ করা হয়।

ট্রাবল রাউটার যেমন TP-Link TL-WR702N কাজ করে খুবই কার্যকর হার্ডওয়্যার ফায়ারওয়াল হিসেবে, যা আপনার কমপিউটারকে নেটওয়ার্কের অন্যান্য ব্যবহারকারীর কাছ থেকে আলাদা করে রাখতে সহায়তা করে। লক্ষণীয়, বেশিরভাগ কমপিউটারে ইনস্টল করা থাকে সফটওয়্যার ফায়ারওয়াল প্রোগ্রাম। তবে এই সফটওয়্যার ফায়ারওয়াল ভাইরাস ও অন্যান্য ম্যালিশাস সফটওয়্যারের মাধ্যমে ডিজ্যাবল হতে পারে।

ভলনিয়ারেবিলিটি চেক করা

ভ্রমণের সময় যখন আপনার ল্যাপটপকে ইন্টারনেটের সাথে যুক্ত করা হবে, তখন আপনি সম্ভবত কোনো সিকিউরিটি সিস্টেমের মাধ্যমে সুরক্ষিত থাকবেন না, যা আপনার কোম্পানি ক্ষতিকর ই-মেইল বা ক্ষতিকর ওয়েবসাইট ফিল্টারের জন্য ব্যবহার করে থাকে। এর ফলে হ্যাকারেরা কমপিউটারের ভলনিয়ারেবিলিটিকে কাজে লাগিয়ে আপনার সিস্টেমকে ম্যালওয়্যারে আক্রান্ত করে। এভাবে আক্রান্ত হওয়ার সম্ভাবনাকে কমানোর জন্য আপনার কমপিউটারের অপারেটিং এবং অন্যান্য সফটওয়্যার সবশেষ সিকিউরিটি প্যাচ দিয়ে আপডেটেড কি না তা চেক করে দেখা উচিত।

সিকিউরিটি কোম্পানি কোয়ালিস (Qualys) ব্রাউজারচেক (BrowserCheck) নামে এক ফ্রি সার্ভিস অফার করে, যা আপনার কমপিউটারকে স্ক্যান ও যেকোনো সফটওয়্যারের আপডেট লিঙ্ক দেয়, যা এটি জানা সিকিউরিটি ভলনিয়ারেবিলিটির সাথে খুঁজে পায়।

লক করা

সম্ভবত সবচেয়ে গুরুত্বপূর্ণ উপদেশগুলোর মধ্যে অন্যতম প্রধান যেটি সুযোগ সন্ধানী চোরের ল্যাপটপের সাথে তথ্য হাতিয়ে নেয়ার কাজকে কঠিন করে তোলে, তা আমরা সাধারণত সচরাচর এরিয়ে যাই।

এ কাজ করার সহজ উপায় হলো Kensington lock ব্যবহার করা। এটি একটি ধাতব ক্যাবল, যা কোনো অবজেক্টের ফাঁস হিসেবে কাজ করে। এটি যেকোনো ল্যাপটপের সাথে যুক্ত থাকে, যেখানে কেনসিংটোন স্লট সজ্জিত থাকে।

অবশ্য কেনসিংটোন লক নিশ্চিতভাবে সম্পূর্ণরূপে ল্যাপটপের নিরাপত্তা দিতে পারে না। কেননা, ক্যাবল হিসেবে এটি খুব সহজেই কেটে ফেলা যায় বা ল্যাপটপ থেকে বিচ্ছিন্ন করা যায় কজ

ফিডব্যাক : mahmood_sw@yahoo.com