তাসনুভা মাহ্‌মুদ

যেভাবে কমপিউটারকে ভাইরাস, হ্যাকার ও স্পাইওয়্যার থেকে রক্ষা করবেন

তথ্যপ্রযুক্তি আমাদের প্রাত্যহিক জীবনযাত্রাকে যেমন করেছে সাবলীল, সহজতর ও গতিময়, তেমনই সৃষ্টি করেছে নতুন নতুন উৎকণ্ঠা এবং কমপিউটিং বিশ্বকে করেছে কলুষিত। প্রযুক্তিবিশ্বের যেসব বিষয় কমপিউটিং-বিশ্বকে কলুষিত করেছে এবং ব্যবহারকারীকে প্রতিনিয়তই উৎকণ্ঠার মধ্যে রাখছে, সেগুলোর মধ্যে অন্যতম হলো ভাইরাস, স্পাইওয়্যার এবং হ্যাকার। এগুলোর ব্যাপকতা এতই বেড়েছে যে, ইদানিং বলা হয়ে থাকে প্রযুক্তিবিশ্বে ভাইরাস, স্পাইওয়্যারের হামলার শিকার হননি এমন ব্যবহারকারী বোধহয় খুব একটা খুঁজে পাওয়া যাবে না। নিঃসন্দেহে বলা যায়, এমন অবস্থায় ব্যবহারকারীর জন্য সেরা উপদেশ হলো 'কমপিউটারকে নিরাপদ রাখুন'।

ভাইরাস, স্পাইওয়্যার, হ্যাকার ইত্যাদি এত গুরুত্বপূর্ণ বিষয়ে পরিণত হয়েছে যে, এগুলো সম্পর্কে ব্যবহারকারীদেরকে সচেতন করতে ইতোপূর্বে কমপিউটার জগৎ পত্রিকায় অনেকবার এ বিষয়ে লেখা প্রকাশিত হয়েছে, পরিবর্তিত পরিস্থিতিতে ব্যবহারকারীদেরকে সতর্ক করার তাদিগ দিয়ে। ভাইরাস, স্পাইওয়্যার, হ্যাকার ইত্যাদি থেকে কমপিউটারকে রক্ষা করার বিষয়টি এমনই এক গুরুত্বপূর্ণ বিষয় যে, কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালা বিভাগটি এবার উপস্থাপন করা হয়েছে তারই ভিত্তিতে। এ লেখায় ব্যবহারকারীদের উদ্দেশে উপস্থাপন করা হয়েছে এক গাইডলাইন, যা অফার করা হয় এফবিআইয়ের অফিসিয়াল অনলাইন ওয়েবসাইটে। অবশ্য এ লেখা ব্যবহারকারীদের জন্য সহজবোধ্য করে তুলে ধরার উদ্দেশ্যে কিছুটা মডিফাই করা হয়েছে। এ গাইডলাইনকে সহজবোধ্য করার জন্য কিছু ব্যক্তিগত উপদেশ ও টিপ উপস্থাপন করা হয়েছে। এই গাইডলাইন শুধু কমপিউটারের জন্য নয়, বরং অন্যান্য ডিজিটাল ডিভাইস, যেমন স্মার্টফোনের জন্যও সমভাবে প্রযোজ্য।

যেভাবে ভাইরাস, স্পাইওয়্যার, হ্যাকার থেকে পিসিকে রক্ষা করা যায়, তা নিম্নরূপ।

ফায়ারওয়াল অন রাখা

ফায়ারওয়াল পিসিকে হ্যাকারের হাত থেকে রক্ষা করে, বিশেষ করে যারা সিস্টেম ক্র্যাশ করার জন্য অ্যাক্সেস করতে চেষ্টা করে, গুরুত্বপূর্ণ তথ্য মুছে ফেলে বা পাসওয়ার্ড চুরি করে কিংবা অন্যান্য সংবেদনশীল গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয়, তাদের হাত থেকে রক্ষা করার চেষ্টা করে।

একটি ফায়ারওয়াল হলো ইন্টারনাল সিকিউরিটি সিস্টেম, যা কমপিউটারকে রক্ষা করতে চেষ্টা করে, যাতে কেউ অনাকাঙ্ক্ষিতভাবে অ্যাক্সেস করতে না পারে। মাইক্রোসফট উইন্ডোজ এবং অ্যাপলের ম্যাক অপারেটিং সিস্টেম উভয়ই ফায়ারওয়াল প্রোটেকটেড। যাই হোক, আমাদের মনে রাখা দরকার, ফায়ারওয়াল সাধারণত ইনকর্পোরেট হওয়া সত্ত্বেও সক্রিয় করতে হয়। আর এ অপশনগুলো আপনি তখনই পাবেন, যখন কমপিউটারকে প্রথম সেটআপ করবেন। সিকিউরিটি প্রোটেকশনের ক্ষেত্রে 'Yes' অপশনটিকে নিশ্চিত করুন। ইচ্ছে করলে ফায়ারওয়াল সফটওয়্যার প্রোগ্রাম যেমন Zone Alarm, ক্যাসপারস্কিসহ আরও কিছু সফটওয়্যার আছে, যেগুলোর মধ্য থেকে যেকোনো একটি সফটওয়্যার কিনতে

পারেন।

এই প্রোগ্রামগুলো ফলাফল হিসেবে উদ্ভূত হয় কিংবা উত্তরাধিকার সূত্রে হস্তান্তরিত হয় বছরের পর বছর ধরে। তাই প্রচণ্ডভাবে রেটেড প্রোগ্রাম দিয়ে সিস্টেমের নিরাপত্তা বিধানের চেষ্টা করে দেখতে পারেন।

যদি স্মার্টফোনের সিকিউরিটি প্রসঙ্গে সচেতন হয়ে থাকেন, তাহলে সফোস মোবাইল সিকিউরিটি, এফ-সিকিউর মোবাইল সিকিউরিটি, ক্যাসপারস্কি মোবাইল সিকিউরিটি, ট্রেন্ড মাইক্রো বা নর্টন স্মার্টফোন সিকিউরিটি ইত্যাদির মধ্য থেকে যেকোনো একটি দিয়ে সযত্নে পরীক্ষা-নিরীক্ষা করে দেখতে পারেন। মোবাইল ডিভাইসের জন্য সিকিউরিটি সফটওয়্যারগুলোর মধ্য থেকে এই সফটওয়্যারগুলো বেশি জনপ্রিয়। এই টুলগুলো অ্যান্টিভাইরাস প্রোটেকশনেও কার্যকর ভূমিকা রাখতে পারে।

অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল বা আপডেট করা

অ্যান্টিভাইরাস প্রোগ্রাম ফায়ারওয়ালের চেয়ে ভিন্ন ফাংশনবিশিষ্ট। অ্যান্টিভাইরাস সফটওয়্যারকে ডিজাইন করা হয়েছে এমনভাবে, যাতে ক্ষতিকর সফটওয়্যার আপনার কমপিউটারে অ্যামবেডেট হতে না পারে। অ্যান্টিভাইরাস সফটওয়্যার যদি ক্ষতিকর কোড যেমন ভাইরাস শনাক্ত করতে পারে, তাহলে তা নিষ্ক্রিয় বা অপসারণ করার কাজও করে। লক্ষণীয়, ব্যবহারকারীদের অজ্ঞাতে ভাইরাস কমপিউটারকে আক্রান্ত করে। বেশিরভাগ অ্যান্টিভাইরাসকে সেটআপ করা যায় স্বয়ংক্রিয়ভাবে আপডেট হওয়ার জন্য।

সিমেনটেকের নর্টন অ্যান্টিভাইরাসহ আর কিছু শীর্ষস্থানীয় অ্যান্টিভাইরাস সফটওয়্যার রয়েছে, যেমন– ম্যাকাফি, ক্যাসপারস্কি, ওয়েবরুট ইত্যাদি। পূর্বোল্লিখিত ফায়ারওয়াল সফটওয়্যারগুলোর মতো আপনি চেক করে নিতে পারেন ভালোভাবে রেট করা সফটওয়্যারটি।

ইনস্টল বা আপডেট করুন অ্যান্টিস্পাইওয়্যার টেকনোলজি

স্পাইওয়্যার ঠিক সফটওয়্যারের মতো আচরণ করে, যা কমপিউটারে গোপনে ইনস্টল করে এবং আপনার কমপিউটারের কার্যকলাপকে নিবিড়ভাবে পর্যবেক্ষণ করে। কিছু স্পাইওয়্যার আছে, যেগুলো ব্যবহারকারীর অজান্তে সংগ্রহ করে নেয় গুরুত্বপূর্ণ তথ্য অথবা ব্যবহারকারীর ওয়েবব্রাউজারে প্রডিউস করে অনাকাঙ্ক্ষিত পপ-আপ অ্যাড। 'ওয়েবব্রাউজার' এমন এক টার্ম, যা ব্যবহার হয় প্রোগ্রামের জন্য, যা কমপিউটারকে ইন্টারনেটের সাথে কানেক্ট হওয়াকে অনুমোদন করে, যেমন– উইন্ডোজের জন্য ইন্টারনেট এক্সপ্লোরার, ম্যাকের জন্য সাফারি ইত্যাদি হলো সুপরিচিত ওয়েব ব্রাউজার।

কিছু কিছু অপারেটিং সিস্টেম, যেমন– মাইক্রোসফট উইন্ডোজ এবং অ্যাপলের ম্যাক অপারেটিং সিস্টেম অফার করে ফ্রি স্পাইওয়্যার প্রোটেকশন। ইন্টারনেট থেকে ফ্রি ডাউনলোড করে নিতে পারেন কিংবা কম ব্যয়বহুল সফটওয়্যার স্থানীয় কমপিউটার স্টোর থেকে কিনে নিতে পারেন।

ইন্টারনেট অ্যাড সম্পর্কে সতর্ক থাকা উচিত প্রত্যেক ব্যবহারকারীর। বিশেষ করে যেসব বিজ্ঞাপনে অফার করা হয় ডাউনলোডযোগ্য ▸

অ্যান্টিস্পাইওয়্যার সম্পর্কে। কেননা, কোনো কোনো ক্ষেত্রে এ পণ্যগুলো ভুয়া হতে পারে এবং প্রকৃতপক্ষে ধারণ করতে পারে স্পাইওয়্যার বা অন্যান্য ক্ষতিকর কোড।

অপারেটিং সিস্টেম আপ-টু-ডেট রাখা

কমপিউটার অপারেটিং সিস্টেমকে মাঝেমধ্যে আপ-টু-ডেট করা উচিত, যাতে প্রযুক্তির অগ্রগতি তথা উন্নয়নের সাথে সাথে যথাযথভাবে টিউন থাকে কিংবা সিকিউরিটি হোল ফিক্স করা যায়। সুতরাং অপারেটিং সিস্টেমকে এসব আপডেট ইনস্টল করার ব্যাপারে নিশ্চিত করতে হবে, যাতে আপনার সিস্টেম সুরক্ষিত থাকে সর্বশেষ প্রোটেকশন দিয়ে।

এফবিআইয়ের পক্ষ থেকে বলা হচ্ছে, উইন্ডোজ বা অ্যাপল ম্যাক কমপিউটারের অপারেটিং সিস্টেমের মাধ্যমে সর্বশেষ প্রোটেকশন ব্যবস্থা গড়ে তুলতে হবে। এখানে আরও উল্লেখ করা হয়েছে, 'অটোমেটিক আপডেট' ফিচার চালু রাখুন, যা এ সিস্টেমগুলো প্রদান করছে। এর ফলে আপনাকে আপডেটের ব্যাপারে আর মনোযোগী হতে হবে না।

ডাউনলোড করার ব্যাপারে সতর্ক থাকুন

কী ডাউনলোড করছেন, সে ব্যাপারে নিশ্চিত হয়ে নিন। অসতর্কভাবে ই-মেইল অ্যাটাচমেন্ট ডাউনলোড করার ফলে প্রতারণার শিকার হতে পারেন, এমনকি সবচেয়ে সতর্ক অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল থাকা সত্ত্বেও। সুতরাং কখনই অপরিচিত কোনো ই-মেইল অ্যাটাচমেন্ট ওপেন করা উচিত নয়। শুধু তাই নয়, যাদেরকে চেনেন না, তাদের ফরোয়াড করা অ্যাটাচমেন্ট বিশেষ করে ফাইল, ছবি বা লিঙ্ক সম্পর্কেও সবসময় সতর্ক দৃষ্টি রাখতে হবে। কেননা, এগুলোতে ইচ্ছাকৃত কিংবা অনিচ্ছাকৃতভাবে থাকতে পারে অ্যাডভান্স ম্যালিশাস বা ক্ষতিকর কোড।

গোপনীয়তা রক্ষায় সিস্টেম ও ব্রাউজার ম্যানেজ করা

হ্যাকারেরা সবসময় অপারেটিং সিস্টেমের এবং ব্রাউজারের খুঁত বা হোল খুঁজে বেড়ায়। আপনার কমপিউটার এবং তথ্যকে সুরক্ষিত রাখতে সিস্টেম এবং ব্রাউজারের সিকিউরিটি সেটিংকে মিডিয়াম বা হাই-এ সেট করুন। এবার 'Tool' বা 'Options' মেনু চেক করে দেখুন কীভাবে এ কাজগুলো করা যায়। নিয়মিতভাবে সিস্টেম এবং ব্রাউজার আপডেট করুন। এ ক্ষেত্রে আপডেটের সুবিধা নিতে পারেন। উইন্ডোজ আপডেট হলো একটি সার্ভিস, যা মাইক্রোসফট অফার করে। এটি মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেম, ইন্টারনেট এক্সপ্লোরার, আউটলুক এক্সপ্রেসে ডাউনলোড এবং ইনস্টল করে সফটওয়্যার আপডেট। এটি সিকিউরিটি আপডেটও ডেলিভার করে। অন্যান্য সিস্টেমের জন্য প্যাচ স্বয়ংক্রিয়ভাবেও রান করে, যেমন– ম্যাকিনটোশ অপারেটিং সিস্টেম।

শক্তিশালী পাসওয়ার্ড ব্যবহার করা ও নিজের কাছে রাখা

অবৈধ অনুপ্রবেশকারীর হাত থেকে পিসিকে রক্ষা করা যায় শক্তিশালী পাসওয়ার্ড বেছে নেয়ার মাধ্যমে, যা অনুমান করা কঠিন। শক্তিশালী পাসওয়ার্ড ব্যবহার করা উচিত, যেখানে থাকবে ন্যূনতম ৮ ক্যারেক্টার। এই ৮ ক্যারেক্টারের মধ্যে থাকা উচিত লেটার, সংখ্যা এবং বিশেষ ক্যারেক্টার। পাসওয়ার্ডে কোনো ওয়ার্ড ব্যবহার করা উচিত হবে না, যা অভিধানে পাওয়া যায়। কিছু কিছু হ্যাকার আছে যারা অভিধানের প্রতিটি ওয়ার্ড ব্যবহার করে হ্যাকিংয়ের চেষ্টা করে। ফ্রেজের প্রতিটি ওয়ার্ডের প্রথম লেটার ব্যবহার করে পাসওয়ার্ড সেট করলে মনে রাখা সহজ। উদাহরণস্বরূপ, পাসওয়ার্ড হিসেবে ব্যবহার করতে পারবে HmWc@W2, যা প্রকৃত অর্থে How Much wood Could a woodchuck chuck-এর সংক্ষিপ্ত রূপ। এ ধরনের জটিল পাসওয়ার্ড ব্যবহার করা উচিত, যা আপনার পছন্দের ফ্রেজের প্রথম অক্ষর এবং বিশেষ লেটারের সমন্বয়ে গঠিত।

কমপিউটারকে নিরাপদ রাখার কিছু সাধারণ উপদেশ

মাইক্রোসফট উইন্ডোজ এবং অ্যাপলের ম্যাক অপারেটিং সিস্টেম উভয়ের সাথে প্রি-ইনস্টল করা থাকে ফায়ারওয়াল, অ্যান্টিভাইরাস এবং স্পাইওয়্যার প্রোটেকশন। এগুলো বেশ বিশ্বাসযোগ্য এবং খুব সহায়ক। সুতরাং, বিশেষজ্ঞদের উপদেশ এগুলো 'agree' করুন ব্যবহার করার জন্য। কমপিউটার বা ল্যাপটপ যখন প্রথমবারের মতো সেটআপ করা হয়, তখন কখনও কখনও এসব প্রি-ইনস্টল করা সফটওয়্যার প্রোটেকশন প্রোগ্রাম, বিশেষ করে অ্যান্টিভাইরাস সফটওয়্যার কিছুদিনের জন্য ফ্রি ট্রায়ালের জন্য ব্যবহারের সুযোগ থাকে। তবে ফ্রি ট্রায়াল পিরিয়ডের পর অর্থাৎ এক বছর পর বার্ষিক চাঁদার জন্য তাগাদা দিয়ে থাকে। যদি আপনি দুটি অ্যান্টিভাইরাস বা স্পাইওয়্যার প্রোগ্রামের কথা ভেবে থাকেন ডাবল প্রোটেকশনের জন্য, তাহলে এ বিষয়টিকে নিয়ে আরেকবার ভালোভাবে চিন্তা করুন। কেননা, মাল্টিপল অ্যান্টিভাইরাস এবং স্পাইওয়্যার প্রোগ্রাম অনেক সময় কমপিউটারে কনফ্লিক্টের কারণ হয়ে দাঁড়ায়। সুতরাং, সেরা নিরাপত্তামূলক ব্যবস্থার কথা ভাবুন।

উইন্ডোজ এবং ম্যাক উভয় অপারেটিং সিস্টেমে রয়েছে অটোমেটিক আপডেট ফিচার। যখন অটোমাইজের জন্য প্রম্পট করবে, তখন ব্যবহারকারীর উচিত 'okay/agree'-তে ক্লিক করা, যাতে স্বয়ংক্রিয়ভাবে আপডেট হয়।

ই-মেইল অ্যাটাচমেন্ট ওপেন করার ক্ষেত্রে এফবিআইয়ের জারি করা সতর্কতামূলক ব্যবস্থার প্রতি মনোনিবেশ করা। ধরুন, 'Helen' নামের কোনো এক ব্যক্তির কাছ থেকে একটি ই-মেইল পেলেন, তবে তিনি আপনার পরিচিত ব্যক্তি হেলেন নাও হতে পারেন। এমন ধরনের সন্দেহজনক কোনো ই-মেইল পান, তাহলে তার সাথে সরাসরি যোগাযোগ করুন ই-মেইল অ্যাটাচমেন্টে ক্লিক করার আগে।

ওয়্যারলেস নেটওয়ার্ক নিরাপদ রাখা

যদি বাসায় ওয়্যারলেস নেটওয়ার্ক ব্যবহার করেন, তাহলে তা হ্যাকারের হাত থেকে রক্ষা করার ব্যাপারে সতর্কতামূলক ব্যবস্থা নেবেন। এ ক্ষেত্রে প্রথম পদক্ষেপ হলো ওয়্যারলেস কমিউনিকেশনকে এনক্রিপ্ট করা। এনক্রিপশন ফিচারসহ একটি ওয়্যারলেস রাউটার বেছে নিন এবং তা সক্রিয় রাখুন। WEP-এর চেয়ে WPA এনক্রিপশনকে অধিকতর শক্তিশালী হিসেবে বিবেচনা করা হয়। কমপিউটার রাউটার এবং অন্যান্য ইক্যুইপমেন্টে অবশ্যই একই এনক্রিপশন ব্যবহার করতে হবে। যদি রাউটার আইডেন্টিফায়ার ব্রডকাস্টিংয়ে এনাবল হয়, তাহলে তা ডিজ্যাবল করুন। SSID নেম নোট করে তা রাখুন, যাতে কমপিউটারকে ম্যানুয়ালি নেটওয়ার্কের সাথে যুক্ত করতে পারেন। এই ধরনের ইক্যুইপমেন্টের প্রি-সেট পাসওয়ার্ড হ্যাকারেরা জানে। সুতরাং আপনার রাউটারের ডিফল্ট আইডেন্টিফায়ার এবং প্রি-সেট অ্যাডমিনিস্ট্রেটিভ পাসওয়ার্ড পরিবর্তন করার ব্যাপারে নিশ্চিত হয়ে নিন। যখন কমপিউটার ব্যবহার করবেন না, তখন ওয়্যারলেস নেটওয়ার্ক বন্ধ রাখুন।

লক্ষণীয়, পাবলিক 'হট স্পটস' নিরাপদ নাও হতে পারে, পাবলিক ওয়্যারলেস নেটওয়ার্কের মাধ্যমে গুরুত্বপূর্ণ তথ্যে অ্যাক্সেস করা থেকে বিরত থাকা কিংবা গুরুত্বপূর্ণ সংবেদনশীল তথ্য সেন্ড না করাই ভালো। মোবাইল ব্রডব্যান্ড কার্ড কেনা উচিত, যা আপনাকে ইন্টারনেটের সাথে যুক্ত হওয়ার সুযোগ দেবে ওয়াই-ফাই হটস্পটের ওপর আস্থাশীল না হয়ে। মোবাইল ব্রডব্যান্ড কার্ড এমন এক ডিভাইস, যা কমপিউটারে, ল্যাপটপে, পিডিএ বা সেলফোনে প্লাগ-ইন করা যায় এবং ব্যবহার করে একটি সেফফোন সিগন্যাল, যা হাই-স্পিড ইন্টারনেটে অ্যাক্সেস দেয়।

ফাইল শেয়ারিংয়ে সতর্ক থাকা

অনেক কনজ্যুমার ডিজিটাল ফাইল শেয়ারিং উপভোগ করেন, যেমন– মিউজিক, মুভি, ফটো এবং সফটওয়্যার। ফাইল শেয়ারিং সফটওয়্যার আপনার কমপিউটারকে একটি কমপিউটার নেটওয়ার্কের সাথে যুক্ত করে। এটি সচরাচর ফ্রি পাওয়া যায়। ফাইল শেয়ারিংয়ের কিছু ঝুঁকিও আছে। যখন ফাইল শেয়ারিং নেটওয়ার্কে যুক্ত হবেন, তখন ব্যবহারকারী ফাইলের অন্যান্য কপি অনুমোদন করবেন, যেগুলো আপনি শেয়ার করতে চান না। আপনি ডাউনলোড করতে পারেন ভাইরাস বা কিছু স্পাইওয়্যার, যা কমপিউটারকে ভলনারেবল করবে হ্যাকারদের জন্য। এ ছাড়া কপিরাইট আইনও ভঙ্গ হতে পারে ডাউনলোড করা মেটেরিয়ালের জন্য কজ

ফিডব্যাক : mahmood_sw@yahoo.com