ওয়েব ব্রাউজার নিরাপদ রাখুন

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

বাসাবাড়িতে যারা কমপিউটার ব্যবহার করছেন, যারা ছাত্র, যারা ছোট ছোট ব্যবসায় পরিচালনা করছেন, বা যারা এ ধরনের সীমিত আকারে ইন্টারনেট ব্যবহার করে থাকেন, তাদের জন্য নিরাপদে ইন্টারনেট ব্রাউজ করা জানা দরকার। যদিও এ লেখাটি প্রাতিষ্ঠানিক বিষয়ে বা কোনো পলিসি তৈরি করার ক্ষেত্রেও যথেষ্ট সহায়ক হবে।

ব্রাউজার নিরাপদ রাখা কেনো জরুরি

বর্তমানে ইন্টারনেট এক্সপ্লোরার, মজিলা ফায়ারফক্স, সাফারি ইত্যাদি ওয়েব ব্রাউজার ব্যাপকভাবে ব্যবহার হচ্ছে। যেহেতু ওয়েব ব্রাউজার প্রায়ই ব্যবহার করতে হয়, তাই এটি নিরাপদে কনফিগার করার বিষয়টি খুবই জরুরি। অপারেটিং সিস্টেমের সাথে যে ব্রাউজার আসে, সেখানে প্রায়ই নিরাপত্তার বিষয়টি যথেষ্ট গুরুত্ব দিয়ে ডিফল্ট হিসেবে ইনস্টল করা থাকে না। ফলে আপনার অজান্তেই কমপিউটারে স্পাইওয়্যার ইনস্টল হয়ে যাচ্ছে, অর্থাৎ আপনার কমপিউটারের নিয়ন্ত্রণ হ্যাকারদের হাতে চলে যেতে পারে।

প্রকৃতপক্ষে একজন ব্যবহারকারী যেসব সফটওয়্যার ব্যবহার করছেন, সেগুলো কমপিউটারের জন্য কতটা নিরাপদ, ব্যবহারের আগে সে বিষয়টি অবশ্যই পরীক্ষা-নিরীক্ষা করে নিতে হবে। সাধারণত বিক্রেতারা কমপিউটারে সফটওয়্যার লোডেড অবস্থায়ই বিক্রি করে থাকেন। আপনার কমপিউটার সরবরাহকারী যেই হোক না কেন, প্রথমেই দেখে নিতে হবে সিস্টেমে ইনস্টল করা সফটওয়্যারগুলো একটি অপরটির সাথে যথার্থভাবে খাপ খাচ্ছে কি না। বাস্তবতা হলো, একজন সাধারণ ব্যবহারকারীর পক্ষে এটি যাচাই করা প্রায় অসম্ভব।

লক্ষ করা যাচ্ছে, ঝুঁকিপূর্ণ ওয়েব ব্রাউজারের কারণে সফটওয়্যার হামলা উত্তরোত্তর বাড়ছে। অসতর্কভাবে ম্যালিসাস ওয়েব সাইটসগুলো ব্রাউজ করার কারণে সফটওয়্যার হামলার ঝুঁকি বাড়ছে। বিভিন্ন কারণে সমস্যাটি গভীর হচ্ছে, তার মধ্যে উলেখযোগ্য হলো :

- অনেক ব্যবহারকারী নিরাপত্তা ঝুঁকির বিষয়টি না ভেবেই কৌতূহলী হয়ে যেকোনো লিঙ্কে ক্লিক করেন।
- ওয়েবসাইট ঠিকানাটি আপনাকে অনাকাঙ্ক্ষিত কোনো সাইটে নিয়ে যেতে পারে।
- অনেক ওয়েব ব্রাউজার বিশেষ কার্যক্রমের সুবিধার বিনিময়ে নিরাপত্তা ব্যবস্থা শিথিল করে থাকে।
- অনেক সময় দেখা যায়, সফটওয়্যারটি কনফিগার করার পর নতুন করে বিভিন্ন ধরনের নিরাপত্তা হুমকির উদ্ভব হয়েছে, যা আগে ছিল না।
- কমপিউটার সিস্টেম এবং সফটওয়্যার প্যাকেজটির সাথে হয়তো নতুন কোনো অতিরিক্ত সফটওয়্যার যুক্ত করা হয়, যা নিরাপত্তা হুমকিযুক্ত।
- থার্ডপার্টি সফটওয়্যারে হয়তো নিরাপত্তার বিষয়ে আপডেটের কোনো ব্যবস্থা থাকে না।
- অনেক নতুন সফটওয়্যার ইনস্টল করার সময় অতিরিক্ত কিছু ফিচার বা সফটওয়্যার ইনস্টল করতে বলে, যা কমপিউটারের নিরাপত্তা ঝুঁকি আরও বাড়িয়ে দেয়।
- অনেক ব্যবহারকারী জানেনই না কীভাবে নিরাপদে ব্রাউজার ইনস্টল করতে হয়।
- অনেক ব্যবহারকারী অতিরিক্ত ফিচারের সুবিধার লোভে ইচ্ছাকৃতভাবে নিরাপত্তা বাড়ানোর জন্য দরকারী ফিচারগুলো এনাবল বা ডিজ্যাবল করেন না।

উপরোল্লিখিত কারণে হ্যাকারেরা ওয়েব ব্রাউজারের মাধ্যমে আক্রমণ করে কমপিউটারকে নিরাপত্তাহীন করতে উৎসাহিত হয়ে উঠেছে।

ওয়েব ব্রাউজারের ফিচার এবং ঝুঁকি

আপনি যে ব্রাউজার ব্যবহার করছেন, তার ফিচার এবং ঝুঁকিগুলো কী কী তা ভালোভাবে জেনে নেয়া খুবই জরুরি। কিছু কিছু ওয়েব ফিচার এনাবল করা হলে কমপিউটারের ঝুঁকি বেড়ে যেতে পারে। প্রায়ই দেখা যায়, কমপিউটার বিক্রেতারা বেশি কমপিউটিং সুবিধা প্রদর্শনের জন্য ডিফল্ট হিসেবে কিছু কিছু ওয়েব ফিচার এনাবল করে থাকেন। এ এনাবল করা ওয়েব ফিচারই কমপিউটারকে ঝুঁকির মধ্যে ফেলে দেয়।

সাধারণত হামলাকারীরা কমপিউটার সিস্টেমে দুর্বলতাগুলো ব্যবহার করে কমপিউটারের নিয়ন্ত্রণ নিয়ে নেয়, তথ্য চুরি করে, ফাইল সিস্টেম ধ্বংস করে এবং আপনার কমপিউটার ব্যবহার করে অন্যের কমপিউটারে হামলা করে।

হামলাকারীরা বিভিন্ন ধরনের ম্যালিসাস ওয়েবসাইট তৈরি করে কমপিউটারে ট্রোজান সফটওয়্যার বা স্পাইওয়্যার ইনস্টল করে। আর এর মাধ্যমে কমপিউটারের যাবতীয় তথ্য চুরি করে নেয়। শুধু যে কোনো কমপিউটার সিস্টেমকে সুনির্দিষ্ট করে হামলা করে তাই নয়, কোনো ম্যালিসাস ওয়েবসাইট ভিজিট করলেও কমপিউটারে ট্রোজান সফটওয়্যার বা স্পাইওয়্যার ইনস্টল হতে পারে।

অনেক সময় ভিকটিমের মেইলেও ম্যালিসাস ওয়েবসাইট ই-মেইলে পাঠানো হতে পারে, যা ক্লিক করার সাথে সাথে কমপিউটারে ট্রোজান সফটওয়্যার বা স্পাইওয়্যার ইনস্টল হতে পারে।

এখানে নির্দিষ্ট কিছু ওয়েব ব্রাউজার ফিচার এবং তাদের সংশ্লিষ্ট ঝুঁকি নিয়ে আলোচনা করা হলো, যার মাধ্যমে বোঝা যাবে কোন কোন ওয়েব ফিচার কীভাবে কমপিউটার সিস্টেমকে নিরাপত্তা হুমকির মুখে ফেলে দিতে পারে।

উইন্ডোজ সিস্টেম এর ইন্টারনেট এক্সপ্লোরার ব্রাউজারে অ্যাকটিভ-এক্স নামে টেকনোলজি ব্যবহার করে। ওয়েব ব্রাউজারে কিছু অ্যাপ্লিকেশন বা কোনো অ্যাপ্লিকেশনের অংশবিশেষ ব্যবহার করার জন্য অনুমোদন করে এ অ্যাকটিভ-এক্স। একটি ওয়েবসাইট অ্যাকটিভ-এক্স কম্পোনেন্ট ব্যবহার করতে পারে, যা ইতোমধ্যে উইন্ডোজ সিস্টেমে আছে বা একটি সাইট ডাউনলোডযোগ্য অবজেক্ট হিসেবে তা সরবরাহ করতে পারে। গতানুগতিক ওয়েব ব্রাউজিংয়ের চেয়ে কিছু বাড়তি সুবিধা দিলেও কমপিউটার সিস্টেমকে অধিকতর ঝুঁকিপূর্ণ করে, যদি না সঠিকভাবে তা বাস্তবায়ন করা হয়।

জাভা একটি অবজেক্ট-ওরিয়েন্টেড প্রোগ্রামিং ল্যাঙ্গুয়েজ, যা ওয়েবসাইটের অ্যাকটিভ কনটেন্ট ডেভেলপ করার জন্য ব্যবহার করা হয়। জাভা ভার্চুয়াল মেশিন বা জেভিএম, জাভা কোড সম্পাদন করার জন্য ব্যবহার করা হয় বা অ্যাপলেট, যা ওয়েবসাইট সরবরাহ করে। কিছু অপারেটিং সিস্টেম জেভিএমসহ আসে। আবার কিছু সিস্টেমে জাভা ব্যবহার করার আগে জেভিএম ইনস্টল করতে হয়। জাভা অ্যাপলেটগুলো অপারেটিং সিস্টেমের ওপর নির্ভর করে না। জাভা অ্যাপলেটস সাধারণত স্যান্ডবক্সে সম্পাদন করা হয়, যেখানে সিস্টেমের অন্য অংশের সাথে ইন্টারঅ্যাকশন খুবই সীমিত। যাই হোক, জেভিএমের এ বিভিন্ন প্রয়োগ ঝুঁকিগুলো বহন করে, যা অ্যাপলেটকে বাধাগুলো এড়িয়ে যাওয়ার অনুমোদন দেয়। অনুমোদিত জাভা অ্যাপলেটসও স্যান্ডবক্স বাধাগুলো এড়িয়ে যেতে পারে, তবে তারা কাজ সম্পাদনের আগেই ব্যবহারকারীকে সক্রিয় করে।

প্লাগ-ইনস হলো আরেক ধরনের অ্যাপ্লিকেশন, যা ওয়েব ব্রাউজারে ব্যবহার করা হয়। প্লাগ-ইনস ডেভেলপ করার জন্য নেটসক্যাপ, এনপিএপিআই স্টান্ডার্ড তৈরি করেছে, কিন্তু মজিলা ফায়ারফক্স, সাফারিসহ অনেক ব্রাউজার এটি ব্যবহার করছে। প্লাগ-ইনস মোটামুটি অ্যাকটিভ-এক্স কন্ট্রোলের মতোই, কিন্তু ওয়েবসাইট ব্রাউজারের বাইরে তা ব্যবহার করা যায় না। অ্যাডোবি ফ্লাস এ ধরনের একটি ▸

অ্যাপ্লিকেশন, যা প্লাগ-ইনস হিসেবে পাওয়া যায়।

কোকিস হলো আরেক ধরনের ফাইল, যা কোনো নির্দিষ্ট ওয়েবসাইটে ডাটা জমা রাখার জন্য ব্যবহার হয়। একটি কোকিস যেকোনো ধরনের তথ্য বহন করতে পারে, যা একটি ওয়েবসাইট ডিজাইনে দেয়ার জন্য জমা রাখা হয়। কোকিস আপনার ভিজিট করা ওয়েবসাইটস সম্পর্কিত তথ্য রাখতে পারে বা ওয়েবসাইটটির ভিজিট করার অনুমোদন সংক্রান্ত তথ্য জমা রাখতে পারে। যে ওয়েবসাইট কোকিস তৈরি করেছে শুধু তার জন্যই পাঠযোগ্য, অন্য কেউ তা পাঠ করতে পারে না। সেশন কোকিসগুলো ব্রাউজার বন্ধ করার সাথে সাথে চলে যায়, আর পারসিস্টেন্ট কোকিসগুলো একটি নির্দিষ্ট মেয়াদোত্তীর্ণ সময় পর্যন্ত কমপিউটারে থেকে যায়।

কোকিসগুলো ভিজিটরকে সুনির্দিষ্টভাবে চিহ্নিত করার ক্ষেত্রে ব্যবহার করা যায়, যদিও কেউ কেউ এটিকে গোপনীয়তার লঙ্ঘন বলে মনে করে। কোনো ওয়েবসাইট যদি অথেনটিকেশনের জন্য কোকিস ব্যবহার করে, তবে আক্রমণকারী ওই কোকিস অর্জন করে ওয়েবসাইটটিতে অবৈধভাবে অনুপ্রবেশ করতে পারে। পারসিস্টেন্ট কোকিসগুলো যেহেতু সেশন কোকিসগুলোর চেয়ে বেশিদিন কমপিউটারে থাকে, তাই তাদের ঝুঁকিও অনেক বেশি।

জাভাস্ক্রিপ্ট, যাকে ইসিএমএ স্ক্রিপ্টও বলা হয়। এটি একটি স্ক্রিপ্টিং ল্যাঙ্গুয়েজ, যা ওয়েবসাইটকে আরও ইন্টারঅ্যাক্টিভ করার জন্য ব্যবহার হয়। জাভাস্ক্রিপ্ট স্টান্ডার্ডে আলাদা স্পেসিফিকেশন আছে, যা নির্দিষ্ট কিছু ফিচারকে বাধা দেয়। যেমন লোকাল ফাইল।

ভিবিস্ক্রিপ্টস আরও একটি স্ক্রিপ্টিং ল্যাঙ্গুয়েজ, যা শুধু মাইক্রোসফট উইন্ডোজ ইন্টারনেট এক্সপ্লোরারেই ব্যবহার হয়। ভিবিস্ক্রিপ্টস, জাভাস্ক্রিপ্টের মতো হলেও অন্য ব্রাউজারে কমপ্যাটিবিলিটির ক্ষেত্রে সীমাবদ্ধতা আছে বলে ব্যাপকভাবে ব্যবহার হয় না।

ওয়েবপেজে পর্যাপ্ত পরিমাণ ফিচার এবং ইন্টারঅ্যাক্টিভিটি সংযুক্ত করার ক্ষমতা নির্ভর করে স্ক্রিটিং ল্যাঙ্গুয়েজটি চালানোর সক্ষমতার ওপর। এ সক্ষমতাই হ্যাকারেরা ব্যবহার করতে পারে কমপিউটারের সিস্টেমে হামলার জন্য। কমপিউটারে সাধারণত ডিফল্ট হিসেবে স্ক্রিপ্টিং সাপোর্ট এনাবল করা থাকে, ফলে সিস্টেমটি অনায়াসেই নিচের ঝুঁকিগুলোর কবলে পড়ে।

ক্রস সাইট স্ক্রিপ্টিং

ক্রস সাইট স্ক্রিপ্টিংকে প্রায়ই এক্সএসএস হিসেবে চিহ্নিত করা হয়। এ ধরনের ঝুঁকিগুলোর ক্ষেত্রে কোনো ওয়েবসাইটের সাথে আপনার যে বিশ্বস্ততার সম্পর্কটা রয়েছে, হামলাকারীরা এর কন্ট্রোল নিয়ে নেয়। উল্লেখ্য, সাধারণত ক্রস সাইট স্ক্রিপ্টিং কোনো ওয়েব ব্রাউজারের ব্যর্থতার কারণে হয় না।

ক্রস জোন ও ক্রস ডোমেইন

কোনো ওয়েবসাইটে স্ক্রিপ্ট যাতে অন্য ডোমেইন থেকে ডাটা অ্যাক্সেস করতে না পারে, সেজন্য বেশিরভাগ ওয়েব ব্রাউজার সিকিউরিটি মডেল ব্যবহার করে। এ নিরাপত্তা মডেল প্রাথমিকভাবে নেটসক্যাপ সেম অরিজিন পলিসির ওপর ভিত্তি করে গড়ে উঠেছে। নিরাপত্তা জোন আলাদা রাখার জন্য ইন্টারনেট এক্সপ্লোরারেরও আলাদা নীতি রয়েছে।

যেসব ঝুঁকি এ সিকিউরিটি মডেলসমূহ লঙ্ঘন করে, অন্য কোনো কাজ সম্পাদন করার জন্যও তা ব্যবহার করা যায়, যা সাধারণভাবে কোনো সাইটে কার্যকর থাকে না। এর প্রতিক্রিয়া প্রায় ক্রস সাইট স্ক্রিপ্টিংয়ের ঝুঁকিগুলোর মতোই, যদি কোনো ঝুঁকি আক্রমণকারীকে কোনো লোকাল মেশিন জোন বা অন্য কোনো সংরক্ষিত এলাকায় অনুপ্রবেশ করার সুযোগ দেয় তাহলে আক্রমণকারী ঝুঁকিপূর্ণ সিস্টেমে যেকোনো বিধিবহির্ভূত নির্দেশনা নিষ্পন্ন করতে পারে।

অবৈধ অনুপ্রবেশকারী শনাক্ত করা

অ্যান্টিভাইরাস ইন্ট্রুশন ডিটেকশন সিস্টেম (আইডিএস) এবং ইন্ট্রুশন প্রিভেনশন সিস্টেম (আইপিএস) সাধারণত কনটেন্টে বিশেষ প্যাটার্ন দেখে কাজ করে। যদি জ্ঞাত কোনো খারাপ প্যাটার্ন ডিটেক্ট হয়, তবে ব্যবহারকারীকে রক্ষার জন্য প্রয়োজনীয় ব্যবস্থা নিতে পারে। কিন্তু প্রোগ্রামিং ল্যাঙ্গুয়েজের ধরনের বিভিন্নতার কারণে ওয়েবপেজের স্ক্রিপ্টিং ব্যবহার করে এ ধরনের সুরক্ষিত সিস্টেমকে এড়িয়ে চলা যায়।

কীভাবে ওয়েব ব্রাউজারকে নিরাপদ রাখা যায়

ওয়েব ব্রাউজারকে বিশেষ ফিচার দানকারী সফটওয়্যার যেমন অ্যাকটিভ-এক্স, জাভা স্ক্রিপ্টিং (ভিবিস্ক্রিপ্টস, জাভাস্ক্রিপ্ট) ইত্যাদি কমপিউটার সিস্টেমে ঝুঁকিগুলো যোগ করতে পারে। এটি দুর্বল বাস্তবায়ন, দুর্বল ডিজাইন বা অনিরাপদ কনফিগারেশনের কারণেও সিস্টেমে অনুপ্রবেশ করতে পারে। এ কারণে আমাদেরকে জানতে হবে কোন ব্রাউজারে কোন কোন ফিচার সাপোর্ট করে এবং সিস্টেমকে কোন ধরনের ঝুঁকির মধ্যে ফেলতে পারে। কিছু ব্রাউজারে এ ধরনের প্রযুক্তি পুরোপুরি ডিজ্যাবল করা থাকে, আবার কিছু ব্রাউজারে সাইট টু সাইট ভিত্তিতে ফিচারগুলো এনাবল করার সুযোগ থাকে।

এ বিভাগে কিছু জনপ্রিয় ব্রাউজারের নিরাপদে কনফিগার করার এবং কিভাবে ঝুঁকিপূর্ণ ফিচারগুলো ডিজ্যাবল করা যায় সে পদ্ধতি বর্ণনা

(বাকি অংশ ৭২ পৃষ্ঠায়)

মাইক্রোসফট ইন্টারনেট এক্সপ্লোরার

মাইক্রোসফট ইন্টারনেট এক্সপ্লোরার উইন্ডোজ অপারেটিং সিস্টেমের সাথেই সংযুক্ত থাকে। এটিকে সিস্টেম থেকে বাদ দেয়া বাস্তবসম্মত নয়।

জাভাস্ক্রিপ্টসহ অন্যান্য সক্রিয় কনটেন্ট ছাড়া এতে অ্যাকটিভ-এক্স প্রযুক্তির ব্যবহার করা হয়। যখন কোনো ব্রাউজারের বিশেষ কিছু অ্যাপ্লিকেশনের উপস্থিতির কারণে সিস্টেমটি মারাত্মক আক্রমণের ঝুঁকিতে থাকে, তখন অ্যাকটিভ-এক্স প্রযুক্তিমুক্ত কোনো ওয়েব ব্রাউজার ব্যবহার করলে ঝুঁকিগুলো অনেকাংশে কমে যায়। অন্যদিকে বিকল্প ওয়েব ব্রাউজার ব্যবহার করলে এর কার্যকারিতার ওপর প্রভাব ফেলতে পারে, যাতে অ্যাকটিভ-এক্স প্রযুক্তি দরকার হয়। বিকল্প ওয়েব ব্রাইজার ব্যবহার করলে আইই বা উইন্ডোজের অন্য কোনো কম্পোনেন্ট বাদ যায় না। অন্যান্য সফটওয়্যার, যেমন ই-মেইল ক্লায়েন্ট আইই, ওয়েব ব্রাউজার অ্যাকটিভ-এক্স কন্ট্রোল বা আইই এইচটিএমএল রেন্ডারিং ইঞ্জিন ইত্যাদি ব্যবহার করতে পারে।

নিচে ইন্টারনেট এক্সপ্লোরার ৭-এর বিভিন্ন ফিচার ডিজ্যাবল করার ধাপ দেখানো হলো। মনে রাখতে হবে, আইই-এর ভার্সনের ওপর মেনু অপশন নির্ভর করে। কাজেই আপনাকে ধাপগুলো যথাযথভাবে অনুধাবন করতে হবে।

ধাপ-১ : টুলস সিলেক্ট করুন, পরে ইন্টারনেট অপশনে যেতে হবে।

ধাপ-২ : সিকিউরিটি ট্যাব সিলেক্ট করুন। এ ট্যাবের সবচেয়ে ওপরে ইন্টারনেট এক্সপ্লোরারে ব্যবহার হয় এ ধরনের বিভিন্ন সিকিউরিটি জোনের একটি তালিকা পাওয়া যাবে। সেটিংআপ সিকিউরিটি জোন নামে মাইক্রোসফট ডকুমেন্টে এ সংক্রান্ত বিস্তারিত তথ্য পাওয়া যাবে। এখানে প্রত্যেকটি সিকিউরিটি জোনের জন্য একটি কাস্টম প্রটেকশন লেভেল সিলেক্ট করা যাবে। এ কাস্টম প্রটেকশন লেভেল বাটন ক্লিক করলে একটি দ্বিতীয় উইন্ডোজ দেখতে পাবেন, যা আপনাকে ওই জোনের জন্য বিভিন্ন সিকিউরিটি সেটিংয়ের অনুমতি দেবে। শুরুতে এ ইন্টারনেট জোন থেকেই সাইটগুলোর চলা শুরু হয়। এ জোনের সিকিউরিটি সেটিংগুলো সব ওয়েবসাইটের জন্য প্রযোজ্য হবে, যা অন্য কোনো সিকিউরিটি জোনের তালিকার ভেতরে নেই। এ জোনের জন্য 'হাই' সিকিউরিটি সেটিং সিলেক্ট করা উচিত। হাই সিকিউরিটি সেটিং সিলেক্ট করার ফলে অ্যাকটিভ-এক্স, অ্যাকটিভ-স্ক্রিপ্টিং, জাভাস্ক্রিপ্টসহ বেশ কিছু সক্রিয় কনটেন্ট ডিজ্যাবল হয়ে যাবে। এ ফিচারগুলো ডিজ্যাবল করার ফলে ব্রাউজারটি অনেক নিরাপদ হবে। ডিফল্ট লেভেল বাটনটি ক্লিক করুন এবং স্লাইডার কন্ট্রোল চেপে ধরে ওপরে 'হাই' পর্যন্ত নিয়ে যেতে হবে।

ফিচারগুলোর ওপর আরও বেশি সূক্ষ্ম নিয়ন্ত্রণ আরোপ করার জন্য কাস্টম লেভেল বাটনটি ক্লিক করতে হবে। এখানে এ জোনের জন্য ব্যবহার হওয়া সুনির্দিষ্ট সিকিউরিটি অপশনগুলো নিয়ন্ত্রণ করা যায়। উদাহরণস্বরূপ, রান অ্যাকটিভ-এক্স এবং প্লাগ-ইনসের ডিজ্যাবল বাটন ক্লিক করে অ্যাকটিভ-এক্স ডিজ্যাবল করা যায়। হাই বাটন পছন্দের পর রিসেট বাটন ক্লিক করে হাই সিকিউরিটি ডিফল্ট ভ্যালু সেট করা যায়।

ওয়েব ব্রাউজার নিরাপদ রাখুন

(৭৭ পৃষ্ঠার পর)

করা হয়েছে। ব্রাউজার সম্পর্কে বিস্তারিত জানার জন্য তাদের ওয়েবসাইট ভিজিট করতে পারেন। যদি ওয়েবসাইটে ব্রাউজারের নিরাপদ ফিচারগুলো বা নিরাপদে কনফিগার করার জন্য পর্যাপ্ত তথ্য না থাকে, তাহলে তাদের সাথে সরাসরি যোগাযোগ করা যেতে পারে।

আপনার কমপিউটারে একাধিক ব্রাউজার ইনস্টল করা থাকতে পারে। ই-মেইল বা ডকুমেন্ট দেখার জন্য একটি ব্রাউজার, আবার ওয়েবসাইট ব্রাউজ করার জন্য আরেকটি ব্রাউজার ব্যবহার হতে পারে। আবার কিছু ফাইল খোলার জন্য অন্য কিছু ফাইল টাইপ কনফিগার করা হয়ে থাকতে পারে। কোনো ওয়েবসাইটের জন্য ম্যানুয়ালি কনফিগার করা ও কোনো ওয়েব ব্রাউজার ব্যবহার করা মানে এই নয় অন্য ওয়েবসাইটগুলোও এ একই ব্রাউজার ব্যবহার করবে। এ কারণে কোনো কমপিউটার সিস্টেমে ব্যবহার হওয়া প্রত্যেকটি ওয়েব ব্রাউজারকে নিরাপদে আলাদাভাবে কনফিগার করতে হবে। একই সিস্টেমে একাধিক ওয়েব ব্রাউজার ব্যবহার করার সুবিধা হলো একটিকে ব্যাংকিং, ই-কমার্স ইত্যাদি অতিগুরুত্বপূর্ণ স্পর্শকাতর কাজের ক্ষেত্রে এবং অন্যটিকে সাধারণ ওয়েব ব্রাউজিংয়ের জন্য ব্যবহার করা যেতে পারে। এভাবে ওয়েব ব্রাউজারের ঝুঁকিগুলো কমিয়ে আনা যায়। এসব স্পর্শকাতর তথ্যের ক্ষেত্রে আলাদা ওয়েবসাইট সংশ্লিষ্ট সফটওয়্যার ব্যবহার করা যায়।

ওয়েব ব্রাউজারগুলো প্রায়ই আপডেট হয়, যা পুরনো কোনো ফিচার মুছে ফেলে আবার নতুন নতুন ফিচার সংযুক্তও করে। *(আগামী সংখ্যায় সমাপ্ত)*

ফিডব্যাক : jabedmorshed@yahoo.com