ওয়্যারলেস হোম নেটওয়ার্ক নিরাপদ রাখার কৌশল

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

সাইবার হামলা থেকে নেটওয়ার্ককে সুরক্ষিত রাখার বিষয়টি খুবই গুরুত্বপূর্ণ। ওয়্যারলেস হোম নেটওয়ার্ক নিরাপদ রাখতে অবশ্যই কিছু কৌশল প্রয়োগ করতে হবে। এ বিষয়ে ধারণা থাকাও দরকার। কোনো ঘনবসতিপূর্ণ এলাকায় ল্যাপটপ ব্যবহার করলে অনেক সময় আপনি মুক্ত অনিরাপদ ওয়্যারলেস অ্যাক্সেস শনাক্ত করতে পারেন। ফ্রিলোডার, ক্ষতিকর কার্যক্রম যেমন এটি হতে পারে পাসওয়ার্ড স্নিফ করার জন্য খোলা অনিরাপদ। ওয়্যারলেস নেটওয়ার্কগুলো খুবই সংবেদনশীল। ধরুন, বাইরের কেউ একজন অবৈধভাবে কপিরাইট ম্যাটেরিয়াল ডাউনলোড করছিল এবং তদন্তে অবৈধ এই কার্যক্রমের সূত্র খুঁজতে গিয়ে দেখা গেল এই অপরাধ আপনার রাউটার থেকে হয়েছে। ভেবেছেন, এরকম কোনো ঘটনার মুখোমুখি হলে কী ধরনের বিপদের মুখে আপনি পড়তে পারেন? এজন্যই ওয়্যারলেস হোম নেটওয়ার্ক সবসময় নিরাপদ রাখা প্রয়োজন। সর্বোচ্চ গুরুত্বের সাথে আপনার ওয়্যারলেস হোম নেটওয়ার্ককে রক্ষা করতে পদক্ষেপ নেয়া উচিত। সৌভাগ্য, সম্প্রতি সহজলভ্য কনজ্যুমার গ্রেড রাউটারগুলো খুব শক্তিশালী এবং সহজেই দিচ্ছে করছে ওয়্যারলেস নিরাপত্তা সংবলিত নানা ধরনের বৈশিষ্ট্য।

হোম ওয়্যারলেস নেটওয়ার্ক সুরক্ষিত রাখতে বেশ কিছু কৌশল অনুসরণ করতে পারেন, যা আপনার নেটওয়ার্কের নিরাপত্তা নিশ্চিত করতে সাহায্য করবে। আপনার রাউটারের এসএসআইডি (সার্ভিস সেট আইডেন্টি ফায়ার) দুর্বৃত্তদের ল্যাপটপ অথবা ওয়্যারলেস এনাবল ডিভাইসের শনাক্তকরণ সহজেই প্রতিরোধ করতে পারে। সাধারণভাবে একটি নন-ব্রডকাস্টিং ওয়্যারলেস নেটওয়ার্ককে সংযুক্ত করতে এই অপশনটি ওয়্যারলেস ডিভাইসের ওপর চাপ প্রয়োগ করে থাকে। সম্পূর্ণভাবে এসএসআইডি সংযুক্ত করার নিয়ম-কানুন ওয়্যারলেস ডিভাইস ব্যবহারকারীদের জানা উচিত।

এসএসআইডি ব্রডকাস্ট করতে যদি বেশি ভালো মনে করেন, তবে যেকোনোভাবে অস্পষ্ট নাম ব্যবহার করা উচিত, যাতে কেউ আপনাকে চিহ্নিত করতে না পারে।

ম্যাক আড্রেস ফিল্টারিং করতে সক্ষম। একটি ম্যাক অ্যাড্রেস হচ্ছে ইউনিক আইডেন্টিফায়ার, যা বিভিন্ন উৎপাদনকারী প্রতিষ্ঠানের মাধ্যমে নেটওয়ার্ক ডিভাইস সম্পাদন করে। একমাত্র অনুমোদিত ম্যাক অ্যাড্রেস ওয়্যারলেস রাউটার কনফিগার করতে পারে। ওয়্যারলেস নেটওয়ার্ক কার্ডের ডিভাইস প্রোপার্টিজ দেখার মাধ্যমে সহজেই কমপিউটারের ম্যাক অ্যাড্রেস খুঁজে পাওয়া যেতে পারে।

ওয়াই-ফাই প্রোটেক্টেড অ্যাক্সেস (ডব্লিউপিএ) অথবা ডব্লিউপিএ২ (ভার্সন২)-এর সাথে টেম্পোরাল কী ইন্টিগ্রিটি প্রটোকল (টিকেআইপি) অথবা অ্যাডভান্সড এনক্রিপশন স্ট্যান্ডার্ড (এইএস) বান্ডবায়নের মাধ্যমে এনক্রিপশন করা সম্ভব। যদি আপনার ওয়্যারলেস ডিভাইস এটা সাপোর্ট করে, তবে ডব্লিউপিএ২-এর সাথে এইএস হবে অধিকতর শ্রেয় এনক্রিপশন মেথড। আরেকটি অন্যতম সেরা বিকল্প হচ্ছে ডব্লিউপিএ, যা টিকেআইপি'র সমন্বয়, যা বেশ পুরনো দিনের ওয়্যারলেস ডিভাইসের সাথে সঙ্গতিপূর্ণ, যা ডব্লিউপিএ২ এইএস সাপোর্ট নাও করতে পারে। দীর্ঘদিন নির্ভরযোগ্যভাবে নিরাপদ

ওয়্যারলেস হোম নেটওয়ার্ক

বিবেচনা হিসেবে ডব্লিউইপি বর্জন করা ভালো। এনক্রিপশন মেথডের ওপর অবিচল থাকার পর পাশ ফ্রেইজ হচ্ছে সবশেষ পদক্ষেপ। শক্তিশালী পাশ ফ্রেইজের সাথে ছয় অথবা তারচেয়ে বেশি আপার এবং লোয়ারকেস লেটার এবং নম্বরের ন্যূনতম ব্যবহার। যদিও দুর্বল প্রযুক্তিগত সমস্যার জন্য রাউটারের নিরাপত্তা অপশনগুলো সম্পূর্ণভাবে বিধ্বস্ত হতে পারে। বেশিরভাগ রাউটার উৎপাদনকারী প্রতিষ্ঠানগুলো যেকাউকে সহজেই সেটআপ, কনফিগার এবং ওয়্যারলেস অ্যাক্সেসের নিরাপত্তা পরীক্ষা করতে সাহায্য করে থাকে বিস্ময়কর ক্ষমতাসম্পন্ন নিরাপত্তা প্রসেস প্রদান করে। আপনার ওয়্যারলেস হোম নেটওয়ার্ককে রক্ষা করে নিরাপদ রাখার বিষয়টি গুরুত্বের বিবেচনায় উপেক্ষা না করে প্রোঅ্যাকটিভ হবেন।

আপনার পার্সোনাল আইডেনটিটি নিরাপদ রাখার টিপস : অনলাইনে নানা ধরনের অপরাধ বেড়ে যাওয়ার ফলে আপনার পার্সোনাল আইডেনটিটি নিরাপদ রাখার কলাকৌশলগুলো নখদর্পণে থাকা উচিত। বিশ্বে প্রতিনিয়তই সাইবার অপরাধ বাড়ার সাথে সাথে সাইবার নিরাপত্তার বিষয়টি খুবই গুরুত্বের সাথে বিবেচিত হচ্ছে। নিজের প্রয়োজনের তাগিদে অনলাইন নিরাপত্তা সম্পর্কে আপনাকে বেশ সচেতন হতে হবে। কারণ, আপনার আইডেনটিটির সাথে অনেকগুলো গুরুত্বপূর্ণ বিষয় জড়িত। এ বিষয়ে অবহেলা করলে আপনাকে হয়তো বড় ধরনের মাশুল দিতে হতে পারে।

পার্সোনাল আইডেনটিটি চুরির ঘটনা প্রতিদিনই ঘটছে। ২০০৩ সালে এ বিষয়ে দুটি অনুসন্ধান হয়েছিল। যার মধ্যে একটি গার্টনার রিসার্স এবং অন্যটি ছিল হাররিস ইন্টারঅ্যাকটিভ নামে প্রতিষ্ঠানের মাধ্যমে। অনুসন্ধান থেকে জানা যায়, ওই সময় ১২ মাসে ৭ লাখ থেকে ১ কোটি লোক তাদের আইডেনটিটি চুরি হওয়া নিয়ে অভিযোগ করেছিল। তবে এ বিষয়ে একটা ব্যাপার সহজেই অনুমেয় যে, আইডেনটিটি চুরির ঘটনা বেড়েই চলছে। এখন প্রশ্ন হচ্ছে, নিজেকে রক্ষা করতে আপনি কি পদক্ষেপ নেবেন? এই ধরনের অপরাধীরা সাধারণত চুরি করা তথ্য দিয়ে নতুন ক্রেডিট কার্ড অ্যাকাউন্ট খুলে থাকে এবং এরা দ্রুত বড় ধরনের কেনাকাটা করে ফেলে তাদেরকে ধরার আগেই। প্রাথমিকভাবে তাদেরকে খুঁজে পাওয়া কষ্টকর হতে পারে অনেক আইডেনটিটির সাথে। আপনি এই ধরনের ভয়াবহ অপরাধ কমাতে বা আংশিক কমাতে সহায়তা করতে পারেন। কিন্তু প্রশ্ন হতে পারে কীভাবে? উত্তরে হয়তো বলা যেতে পারে বায়োমেট্রিক ফ্ল্যাশড্রাইভের সাহায্যে।

ফ্ল্যাশড্রাইভে ব্যক্তিগত তথ্য স্টোর করতে, এনক্রিপ্ট ফাইল নিরাপদ রাখতে আপনার ফিঙ্গারপ্রিন্ট অ্যাক্সেস দিবে। আপনার সব পার্সোনাল ইনফরমেশন পাসওয়ার্ড, ইউজার নেম, অ্যাকাউন্ট ইনফরমেশন এবং অন্যান্য প্রয়োজনীয় তথ্য একটি নিরাপদ ফ্ল্যাশড্রাইভে রাখতে পারেন। পরবর্তী সময়ে আপনি যখন চাইবেন, তখন এতে প্রবেশ করবেন। এই তথ্যগুলো আপনার হার্ডড্রাইভে ব্যাকআপ সিস্টেমে নিতে পারেন এবং এগুলো আপনার সাথে নিরাপদে রাখতে পারেন। যদি তথ্যগুলো কখনও হারিয়ে যায়, চুরি হয়ে যায় তখন আপনার ফিঙ্গারপ্রিন্ট ডাটাগুলোকে রক্ষা করবে।

বহুমুখী ব্যবহার হিসেবে কমার্শিয়াল সেটিংয়ে এই ফ্ল্যাশড্রাইভ ব্যবহার করতে পারেন। সেখানে কাজ করার জন্য কারও নির্দিষ্ট কোনো কোম্পানির ইনফরমেশন জানার প্রয়োজন নেই। ফ্ল্যাশড্রাইভের সাহায্যে আপনি সর্বোচ্চ দশজন ব্যবহারকারীর প্রবেশে নিয়ন্ত্রণ করতে পারেন, কোনো ক্ষেত্রে তাদের অ্যাক্সেস যদি প্রয়োজন হয়ে থাকে। নিরাপত্তার লেভেল আগের মতো একজন ব্যবসায়ী হিসেবে আপনাকে দিবে। আলাদাভাবে একেকজন কোম্পানির তথ্য সম্পর্কে জানার অনুমতি পাবে এবং এ ক্ষেত্রে তারা নীতিগতভাবে দায়ী থাকবে।

তাদের ফিঙ্গারপ্রিন্ট দিবে তথ্যের নিরাপত্তা রক্ষা, এমনকি যদি তা চুরিও হয়ে থাকে। অনেক কোম্পানিতে চুরির ঘটনায় ফিঙ্গারপ্রিন্ট টেকনোলজি নিরাপত্তা নিশ্চিত করতে বিশেষ ভূমিকা রাখে। যদি মাত্র পাঁচজন চাকরিজীবী কোনো প্রতিষ্ঠানের গোপন তথ্য সম্পর্কে সবকিছু জানে বা জানার অধিকার দেয়া হয়। তবে তারাও তো তথ্য চুরির সুযোগ নিতে পারে। বর্তমানে প্রযুক্তির যুগে আপনার তথ্য কে বা কারা চুরি করেছে, তা বের করা সম্ভব এবং কোথা থেকে কখন তা চুরি হয়েছে তাও বের করা সম্ভব।

ঘটনা ঘটার আগেই প্রতিরোধমূলক ব্যবস্থা নিতে হবে। পাসওয়ার্ড হ্যাকিং প্রতিরোধে পাসওয়ার্ড ম্যানেজার বিশেষ ভূমিকা রাখতে পারে। আপনার পার্সোনাল ইনফরমেশন, ছবি, অন্যান্য তথ্য নিরাপদ রাখতে এটি বেশ কার্যকর। সর্বোপরি বায়োমেট্রিক সিকিউরিটি, ফিঙ্গারপ্রিন্ট ফ্ল্যাশড্রাইভ ইত্যাদি প্রযুক্তি ব্যবহারে অধিকতর নিরাপদভাবে আপনার কার্যক্রম পরিচালনা করতে পারেন কজ

ফিডব্যাক : jabedmorshed@yahoo.com