কিছু অপরিহার্য ফ্রি সিকিউরিটি চেক

তাসনুভা মাহ্‌মুদ

বর্তমান কমপিউটিংবিশ্ব বিভিন্ন ধরনের হুমকি দিয়ে পরিপূর্ণ। ব্যক্তিগত ডাটা থেকে শুরু করে সব ধরনের ডাটা বা তথ্যের নিরাপত্তার প্রসঙ্গটি ইন্টারনেট সিকিউরিটি প্রোগ্রাম ইনস্টল করার চেয়ে বেশি প্রাধান্য পেয়েছে। অনলাইন বিশ্বে বর্তমানে অসংখ্য এবং বিভিন্ন ধরনের হুমকি দিনকে দিন বেড়ে যাওয়ায় তা প্রতিরোধে বিভিন্ন ধরনের ব্যবস্থা গ্রহণ করার বিষয়টি অপরিহার্য হয়ে পড়েছে।

তথ্যের নিরাপত্তার বিষয়টিকে গুরুত্ব দিয়ে এবং সবার কাছে নিরাপত্তাসংশ্লিষ্ট কাজটিকে সহজতর করার উদ্দেশ্যে কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালায় এবার উপস্থাপন করা হয়েছে কিছু সিকিউরিটি চেক, যা বাস্তবায়ন করা বর্তমানে প্রত্যেক ব্যবহারকারীর উচিত। আপনি উইন্ডোজ পিসি, অ্যাপল ম্যাক বা স্মার্টফোন যে ধরনের ব্যবহারকারী হন না কেনো তথ্যের নিরাপত্তার জন্য এ লেখার উল্লিখিত টিপগুলো প্রয়োগ করে অনলাইন ব্রাউজিংয়েও নিরাপদে থাকতে পারবেন।

স্ট্যান্ডার্ড উইন্ডোজ অ্যাকাউন্ট ব্যবহার করা

উইন্ডোজ এক্সপিতে অ্যাডমিনিস্ট্রেটর অ্যাকাউন্ট ছাড়া অন্য সবকিছু ব্যবহারকে জটিল করেছে মাইক্রোসফট। সে কারণেই অপারেটিং সিস্টেমের লিমিটেড ইউজার অ্যাকাউন্ট টাইপ সীমাবদ্ধ করা হয়েছে। উইন্ডোজ ৭ এবং ভিস্তা স্ট্যান্ডার্ড অ্যাকাউন্ট দিয়ে এসব বিরক্তিকর

চিত্র-১

ফিচার দরুণভাবে মোকাবেলা করা সম্ভব। যথাযথ অ্যাডমিনিস্ট্রেটর পাসওয়ার্ড দেয়ার মাধ্যমে এগুলো ব্যবহারকারীকে সেটিং টোয়েকের সুবিধা দেয়। যেখানে ক্ষতিকর প্রোগ্রাম/সফটওয়্যার এবং সাধারণ ব্যবহারকারীরা থাকবেন সীমতি পরিবর্তনে। আর এ কাজটি করা যাবে অ্যাডমিনিস্ট্রেটর লেভেল অ্যাক্সেস আনচেক করা ছাড়াই।

উইন্ডোজে ন্যূনতম একটি অ্যাডমিনিস্ট্রেটর অ্যাকাউন্ট সেটআপ করা থাকতে হবে। এর অর্থ হচ্ছে সিঙ্গেল ইউজার অ্যাকাউন্টবিশিষ্ট পিসি শুধু অ্যাকাউন্ট টাইপ পরিবর্তন করে না বরং নতুন স্ট্যান্ডার্ড অ্যাকাউন্ট তৈরি ও কনফিগার করে।

উভয় বিষয় হ্যান্ডেল হয় কন্ট্রোল প্যানেলে ইউজার অ্যাকাউন্ট অ্যান্ড ফ্যামিলি সেইফটি ফিচারের মধ্যে। উইন্ডোজ ৭ এবং ভিস্তা ব্যবহারকারীদের অ্যাডমিনিস্ট্রের অ্যাকাউন্ট ব্যবহার করার জন্য তাগাদা দেয়া হয় ইউজার অ্যাকাউন্ট কন্ট্রোল থেকে বাড়তি নিরাপত্তার জন্য। এ সম্পর্কে পরে আরও বিস্তারিত আলোচনা করা হয়েছে।

পাসওয়ার্ড প্রোটেক্ট ইউজার অ্যাকাউন্ট

উইন্ডোজে অনাকাঙ্ক্ষিত অ্যাক্সেসকে প্রতিহত করার সবচেয়ে সহজ এবং দ্রুততম উপায় হলো ইউজার অ্যাকাউন্টে পাসওয়ার্ড প্রোটেকশন যুক্ত করা। এ ধরনের কার্যকলাপ আপনাকে অনেক সময় অবরুদ্ধ করে ফেলতে পারে। তাই এ ক্ষেত্রে সচেতন থাকা উচিত। উইন্ডোজ ৭ এবং ভিস্তার ক্ষেত্রে Control Panel→User Accounts and Family Safety→User Accounts-এ গিয়ে 'Create a Password for your account'-এ ক্লিক করতে হবে। আর এক্সপির ক্ষেত্রে Control Panel ওপেন করে User Accounts-এ ক্লিক করুন এবং পরিবর্তন করার জন্য account আইকনে ক্লিক করে 'create a password' অপশনে ক্লিক করুন।

উইন্ডোজ আপডেট সেটিং চেক করা

উইন্ডোজ আপডেটের জন্য নিয়মিতভাবে প্রম্পট করে থাকে, যা অনেকের কাছে রীতিমতো বিরক্তিকর এক ব্যাপার হয়ে দাঁড়িয়েছে। আপনি ইচ্ছে করলে এ বিরক্তিকর পরিস্থিতিকে সহজেই এড়িয়ে যেতে পারেন, তবে এ ফিচারকে ডিজ্যাবল না করে। কেননা আপডেট ফিচার ডিজ্যাবল করা তেমন কার্যকর কোনো সমাধান নয়। এর বিকল্প হিসেবে উইন্ডোজ ৭ এবং ভিস্তার Control Panel ওপেন করে System and Security-তে ক্লিক করে Windows Update and Change Settings-

চিত্র-২

এ ক্লিক করুন। আর এক্সপিতে Security Center-এ ক্লিক করে Automatic Updates (Manage Security Settings for) ক্লিক করে। স্বয়ংক্রিয় আপডেটের জন্য ইনস্টলেশন ওপেন করলে প্রতিদিনই পাবেন সেরা প্রটেকশন। তবে Download Updates for me, but let me choose when to install them' অপশন উইন্ডোজকে প্রতিহত করবে অনাকাঙ্ক্ষিত প্রম্পট শুরু করা থেকে। তবে ক্ষেত্রবিশেষে ডাউনলোড আপডেটকে ইনস্টল করতে ভুল যাতে না হয় সেদিকে খেয়াল রাখা উচিত।

সিকিউরিটি স্ক্যানকে কার্যকর করা

রিয়েল-টাইম ডিটেকশনে সক্ষম ম্যালিশাস সফটওয়্যার প্রটেকশন টুল সব ধরনের হুমকিকে প্রতিরোধ করতে পারে না। সে ক্ষেত্রে ক্ষতিকর সফটওয়্যার শনাক্ত করার একমাত্র উপায় হলো 'full' স্ক্যান কার্যকর করা। যদি না নিয়মিতভাবে স্বয়ংক্রিয় স্ক্যান প্রতিসপ্তাহে অন্তত একবার কার্যকর করা হয় অথবা অনুরূপ কিছু কার্যকর করা হয়। সুতরাং স্বয়ংক্রিয় স্ক্যান চালু করুন এবং যতক্ষণ পর্যন্ত না শেষ হচ্ছে ততক্ষণ পর্যন্ত অপেক্ষা করুন।

প্রথমে বিল্ট-ইন আপডেট চেক কার্যকর করার বিষয়টি নিশ্চিত করুন। অবশ্য এর প্রক্রিয়া সফটওয়্যারের ওপর ভিত্তি করে ভিন্ন ভিন্ন হতে পারে। সবচেয়ে ভালো অভ্যাস হলো আপডেটকে স্বয়ংক্রিয়ভাবে কার্যকর হতে দেয়া, তবে নিয়মিতভাবে ম্যানুয়াল আপডেট চেক করার অভ্যাসটি সবসময় ভালো অভ্যাস।

ইউজার অ্যাকাউন্ট কন্ট্রোল এনাবল করা

মাইক্রোসফট উইন্ডোজ ভিস্তায় অ্যাডমিনিস্ট্রেটর অ্যাকাউন্টে অনাকাঙ্ক্ষিত ক্ষতিকর কার্যকলাপকে প্রতিহত করার জন্য প্রবর্তন করে ইউজার অ্যাকাউন্ট কন্ট্রোল। তবে ব্যবহারকারীর কনফারমেশনের জন্য অব্যাহত রিকোয়েস্টে বিরক্ত হয়ে অনেকেই এ ফিচারকে ডিজ্যাবল করতে বাধ্য হন। এ ফিচারকে আরও সংস্কার করে উন্নত করা হয় ভিস্তা সার্ভিস প্যাক ১ (SPI)-এ এবং আরও উন্নত করা হয় উইন্ডোজ ৭-এ। সুতরাং এ ফিচার যদি ডিজ্যাবল করা থাকে, তাহলে তা আবার এনাবল করা উচিত। সম্ভবত ভিস্তার সার্ভিস প্যাক-১-এ বা উইন্ডোজ ৭-এ এ ফিচার ব্যবহার হচ্ছে।

উইন্ডোজ ৭ এবং ভিস্তায় এই ফিচার ব্যবহার করতে চাইলে স্টার্ট মেনু থেকে Control Panel ওপেন করে ইউজার অ্যাকাউন্ট পেজে ভিজিট করুন। এজন্য User Accounts-এ গিয়ে User Accounts and Family Safety-এ ক্লিক করুন। এরপর উইন্ডোজ ভিস্তায় Turn User Account Control On or Off অপশনে, আর উইন্ডোজ ৭-এ Change User Account Control Settings অপশনে ক্লিক করুন। উইন্ডোজ ভিস্তায় অপশনের জন্য অফ/অন টোগাল রয়েছে, যেখানে উইন্ডোজ ৭-এ রয়েছে একটি স্লাইডার এবং এর Default পজিশনটি ব্যবহারের জন্য শ্রেষ্ঠ সেটিং।

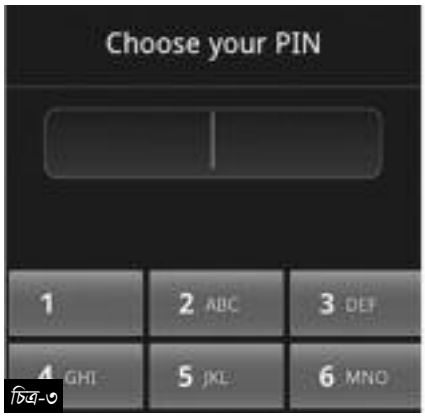
মাইক্রোসফটের অ্যান্টিভাইরাস টুল ব্যবহার করা

অ্যান্টিভাইরাস সফটওয়্যারকে অবশ্যই ইনস্টল করতে হবে এবং তা সবসময় আপডেট রাখতে হবে। তবে অ্যান্টিভাইরাস প্রোগ্রামের পেইড ভার্সনের বিকল্প অপশনও রয়েছে। উইন্ডোজ ডিফেন্ডার হলো একটি সক্ষম বা কার্যকর অ্যান্টিস্পাইওয়্যার টুল, যা উইন্ডোজ ভিস্তা এবং উইন্ডোজ ৭-এ বিল্ট-ইন। এ টুল ব্যবহার করতে চাইলে Start মেনুর সার্চ বক্সে Defender টাইপ করে এন্টার চাপুন। ▶

মাইক্রোসফট এর ব্যবহারকারীদের জন্য আরও অফার করেছে এক ফ্রি এবং অধিকতর কার্যকর টুল, যা উইন্ডোজ সিকিউরিটি অ্যাসেনশিয়ালস অ্যাপ্লিকেশন হিসেবে পরিচিত। এ টুলটি উইন্ডোজ ৭, ভিস্তা এবং এক্সপির জন্য ফ্রি ডাউনলোড করা যাবে।

ফায়ারওয়াল প্রতিরোধ টেস্ট (উইন্ডোজ ৭, ভিস্তা, এক্সপি, ম্যাক ওএস এক্স, আইওএস এবং অ্যান্ড্রয়িড)

একটি সফটওয়্যার ফায়ারওয়াল অথবা রাউটারে একটি বিল্ট-ইন সফটওয়্যার ফায়ারওয়াল গ্রহণ করা বা মেনে নেয়া ঠিক হবে না একটি ডিভাইস বা নেটওয়ার্ক প্রতিরোধের



চিত্র-৩

জন্য। অনলাইন পোর্ট স্ক্যানিং সার্ভিস সাইট 'শিল্ড আপ' Common Port এবং All Service Ports-এর ওপর এক টেস্ট পারফরম করে প্রমাণ করে একটি পিসির ওপেন পোর্টগুলো হতে পারে হ্যাকারদের জন্য সম্ভাব্য এক এন্ট্রি পয়েন্ট। যেসব পোর্ট নাম্বারে সবুজ বর্ণের আইকন সংবলিত 'Stealth' হিসেবে লেবেল করা নয়, সেগুলোকে ফায়ারওয়াল সেটিংয়ের সময় অবশ্যই চেক করে দেখা উচিত। কিছু সুনির্দিষ্ট অ্যাপ্লিকেশনের জন্য পোর্ট ওপেন রাখা হয় এবং সেগুলো চমৎকারভাবে কাজ করে। তবে বিস্তৃত উন্মুক্ত পোর্ট রেঞ্জ অথবা যেগুলো ডিলিট না করে রেখে দেয়া হয়েছে সেগুলোকে বা অ্যাপ্লিকেশনগুলোকে অবশ্য বন্ধ করা উচিত।

ওয়াই-ফাই সেটিং রিভিউ করা (উইন্ডোজ ৭, ভিস্তা, এক্সপি, ম্যাক ওএস এক্স, আইওএস এবং অ্যান্ড্রয়িড)

দীর্ঘদিন ধরে ওয়েপ (WEP) কলঙ্কিত হয়েছিল একটি সিকিউর ওয়্যারলেস এনক্রিপশন প্রক্রিয়া হিসেবে। তবে যেকেউ এখনও পুরনো ব্রডব্যান্ড ওয়াই-ফাই রাউটারে এটি ব্যবহার করতে পারেন। সব ওয়াই-ফাই রাউটার এটি বিভিন্নভাবে ব্যবহার করতে পারে, তবে ওয়াই-ফাই সেটিংয়ের জন্য ওয়্যারলেস সেটিংস বা এনক্রিপশনের জন্য অনুসন্ধান করে সবাই এবং WPA বা WPA2-তে পরিবর্তন করে পাসওয়ার্ডসহ যা হয় বর্ণমালা, সংখ্যা এবং সিম্বলসহ। যদি WPA বা WPA2 এনক্রিপশন না থাকে, তাহলে রাউটার বাতিল হিসেবে গণ্য হবে যেহেতু ওয়্যারলেস ডিভাইস এ এনক্রিপশন স্ট্যান্ডার্ড সাপোর্ট করে না। ব্রাউজারে ১৯২.১৬৮.১. টাইপ করে রাউটারে লগিং করুন এবং ম্যানুয়ালি ডিভাইসকে চেক করে দেখুন।

ওয়াই-ফাই এসএসআইডি পরিবর্তন করা

ব্রডব্যান্ড ওয়্যারলেস রাউটার যেগুলো ব্যবহার করে ডিফল্ট ম্যানুফ্যাকচারার সেট আইডেন্টেটিস অথবা এসএসআইডি, সেগুলো হলো হ্যাকারদের কাছে এক ধরনের নির্দেশক। কেননা এর অন্যান্য ডিফল্ট সেটিংগুলো যথাযথ জায়গায় থাকে। এর ফলে এটি হ্যাকারদের কাছে হয়ে ওঠে সহজ টার্গেটে। এসএসআইডিকে পরিবর্তন করুন অনির্দিষ্ট কোনো কিছুতে, যা কোনো ব্যক্তিগত শনাক্তকরণ তথ্য ব্যবহার করে না এবং রিকনফিগার করুন যেকোনো ওয়্যারলেস ডিভাইসকে, যা রাউটারের সাথে যথাযথভাবে যুক্ত থাকে।

সেট করুন আইওএস পাসকোড

চুরি হওয়া আইফোনে বা আইপ্যাডে গুরুত্বপূর্ণ তথ্য থাকতে পারে চোরদের জন্য। তাই ব্যক্তিগত তথ্যকে একান্তই ব্যক্তিগত রাখার জন্য একটি পাসকোড সেট করুন। Tap Settings-এর পর General সিলেক্ট করে Passcode Lock সিলেক্ট করুন এবং এরপর Turn Passcode On-এ ট্যাপ করুন।

এবার Tap করুন এবং চার ডিজিটের পাসকোড নিশ্চিত করুন। এরপর Require Passcode-এ ট্যাপ করুন এবং সেট করুন কখন এটি সক্রিয় হবে। এ ক্ষেত্রে Immediately হলো সবচেয়ে নিরাপদ অপশন। তবে '5 Minutes'-এ সেট করলে প্রোটেকটেড ডিভাইস ব্যবহারের ক্ষেত্রে কম বিরক্ত সৃষ্টি করবে। সাধারণ পাসকোডকে ডিজ্যাবল করার জন্য একটি অপশনও রয়েছে। ব্যবহারকারীর উচিত দীর্ঘ পাসওয়ার্ড ব্যবহার করা। Erase Data অপশনকে এনাবল রাখা উচিত। এর ফলে আইফোন আইপ্যাড মুছে যাবে যদি দশবার ব্যর্থ পাসকোড প্রচেষ্টা কার্যকর করা হয়।

ডিজ্যাবল করুন স্বয়ংক্রিয় ওয়াই-ফাই সংযোগ

ডিভাইসগুলো স্বয়ংক্রিয়ভাবে ওয়াই-ফাই নেটওয়ার্কে যুক্ত করতে পারে সুবিধার জন্য। তবে এটি নিরাপত্তা ব্যবস্থাকে দুর্বল করে দিতে পারে, হট স্পট হয়ে উঠতে পারে ব্যক্তিগত ডাটার হার্ভেস্ট। এ ফিচারকে ডিজ্যাবল করুন Settings-এর মাধ্যমে। এবার Wi-Fi ট্যাপ করে স্লাইডারকে সরিয়ে Ask to Join Networks Switch-কে off-এ সেট করুন। কাছাকাছি যেকোনো নতুন ওয়াই-ফাই নেটওয়ার্ক এখন সংযোগের জন্য ম্যানুয়ালি সিলেক্ট হবে। ডিভাইসগুলো স্বয়ংক্রিয়ভাবে ওয়াই-ফাই নেটওয়ার্কে যুক্ত হবে, যা ইতোপূর্বে ব্যবহার হতো। সুতরাং যেকোনো সন্দেহজনক জানা নেটওয়ার্ককে ডিলিট করুন নীল বর্ণের ডান পয়েন্টিং অ্যারোর পাশে ট্যাপ করে এবং Forget this Network-এ ট্যাপ করুন।

অ্যান্ড্রয়িড পাসকোড সেট করুন

এনাবল করুন অ্যান্ড্রয়িড পাসকোড প্রটেকশন। এজন্য Security→Settings→Setup Screen Lock-এ নেভিগেট করুন। এজন্য একটি চার ডিজিট পিন কোড বা দীর্ঘতর পাসওয়ার্ড সেট করা যায়, তবে Pattern অপশন এড়িয়ে যান। অবশেষে


চিত্র-৪

স্ক্রিনে সাজোরে আঙ্গুলের চাপ মারলে প্যাটার্ন উন্মোচিত হতে পারে। একইভাবে অ্যান্ড্রয়িড ৪.০-এ (আইসক্রিম স্যান্ডউইচ) ক্যামেরাভিত্তিক 'face unlock' অপশন খুব সহজেই ফটোসহ বাইবাস করে যেতে পারে, যদিও এটি অ্যান্ড্রয়িড ৪.১-এ(জেলি বিনে) সমাধান করা হয়েছে। তাই নিজেকে সিকিউরিটি হুমকি থেকে রক্ষা করা উচিত।

লোকেশন ট্র্যাকিং সেটআপ করা

অ্যাপল ফ্রি অফার করে লোকেশন ট্র্যাকিং আইওএস এবং ওএস ডিভাইসের জন্য আইক্লাউড সার্ভিসের মাধ্যমে। ফ্রি অ্যাকাউন্টের জন্য রেজিস্ট্রেশন করুন এবং সেট করুন একটি পাসকোড বা পাসওয়ার্ড, যাতে এ সার্ভিস ডিজ্যাবল না হয়ে যায়। প্রে প্রজেক্ট (Prey Project) অনুরূপ কিছু অফার করে উইন্ডোজ ওএস এক্স এবং লিনআক্স কমপিউটারের জন্য। এর সাথে আরও আছে আইওএস এবং অ্যান্ড্রয়িড স্মার্টফোন। এটি সর্বোচ্চ তিনটি ডিভাইসের জন্য ফ্রি।

ওএস এক্স হার্ডডিস্ক এনক্রিপ্ট করা

ম্যাক ওএস এক্স অফার করে বিল্ট-ইন ডিস্ক এনক্রিপশন, যাকে বলা হয় File Vault। এটি ইউজার অ্যাকাউন্ট পাসওয়ার্ড ফিচারকে আরও শক্তিশালী করে যথাযথ পাসওয়ার্ড ছাড়াই ডাটাকে আনরিডেবল করার মাধ্যমে। এর ফলে পারফরম্যান্সের ওপর এর কিছু প্রভাব পড়ে। তাই প্রয়োজনে Performance and Security Privacy ফিচারের মাধ্যমে ফাইল ভল্টকে এনাবল করুন। এরপর File Vault ট্যাবে ক্লিক করুন। এবার Turn On File Vault-এ ক্লিক করুন কাজ শুরু করার জন্য। এবার আবির্ভূত হওয়া recovery key-এর নোট তৈরি করুন এবং এনক্রিপশন প্রসেস শেষ হওয়ার জন্য অপেক্ষা করুন।

সর্বাধুনিক ওয়েব ব্রাউজার ব্যবহার করুন (অনলাইন)

উন্নত নিরাপত্তা ব্যবস্থা থেকে সুবিধা পেতে চাইলে ব্যবহারকারীকে সবসময় সর্বাধুনিক ওয়েব ব্রাউজার ব্যবহার করতে হবে।

ভিন্ন পাসওয়ার্ড ব্যবহার করা (অনলাইন)

প্রত্যেক অনলাইন অ্যাকাউন্টের জন্য একই পাসওয়ার্ড ব্যবহার না করে ভিন্ন ভিন্ন পাসওয়ার্ড ব্যবহার করুন। কেননা একটি অ্যাকাউন্ট ভাঙ্গা গেলে অন্যগুলো ভাঙ্গা যাবে কজ

ফিডব্যাক : swapan52002@yahoo.com