সিকিউরিটি সফটওয়্যার সেটিং ও স্ট্যাটাস চেক করবেন যেভাবে

তাসনীম মাহ্মুদ

কমপিউটিং বিশ্বের ব্যবহারকারীরা সম্প্রতি ভাইরাস, ম্যালওয়্যার, ট্রোজান, ফিশিং, স্ক্যাম প্রভৃতির কারণে বেশ উৎকণ্ঠার মধ্যে কমপিউটিং জীবন অতিবাহিত করছেন। সুতরাং নিশ্চিতভাবে বলা যায়, বেশিরভাগ ব্যবহারকারী তাদের সিস্টেমে, নোটবুকে, ফোনে এবং ট্যাবলেটে একটি অ্যান্টিভাইরাস, একটি ভিপিএন এবং অন্যান্য সিকিউরিটি সফটওয়্যার ইনস্টল করেছেন। কিন্তু সেগুলো কী যথাযথভাবে কাজ করে অথবা আপনি কী ইতোমধ্যে হ্যাকের শিকার হয়েছেন এমনসব প্রশ্নের মুখোমুখি হতে হয় প্রায় সব ব্যবহারকারীকে। এ লেখায় ব্যবহারকারীর উদ্দেশে কিছু টিপ তুলে ধরা হয়েছে, যেগুলো ব্যবহারকারীদেরকে সহায়তা করবে তাদের নিজস্ব সিকিউরিটি চেকআপ পারফরম করাতে।

আপনার অ্যান্টিভাইরাস অথবা সিকিউরিটি স্যুট কতদিন আগে ইনস্টল করেছেন? এরপর থেকে কতবার এ অ্যান্টিভাইরাস অথবা সিকিউরিটি স্যুটের দিকে লক্ষ করেছেন? সাধারণত সিকিউরিটি পণ্য ডিজাইন করা হয় ওইসব ইউজারের প্রতি লক্ষ রেখে, যারা সিকিউরিটি পণ্য সেট করার পরিকল্পনা করে এবং ভুলে যায়। আপনার উচিত তাদেরকে মাঝেমধ্যে মনে করিয়ে দেয়া এবং সেখানে কোনো ত্রুটি নেই তা নিশ্চিত করা।

আপনার সিকিউরিটি সিস্টেম থেকে কতটুকু নিরাপত্তা পেতে পারেন, তা নিশ্চিত করার জন্য নিচে ব্যবহারকারীর উদ্দেশে কয়েকটি সহজ ধাপ তুলে ধরা হয়েছে।

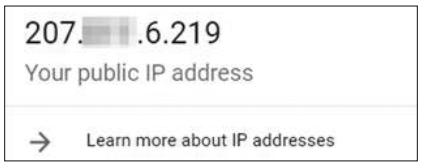
সেরা সিকিউরিটি সফটওয়্যার ব্যবহার করা

আপনার প্রতিটি সিকিউরিটি প্রোডাক্টের বৈশিষ্ট্যের দিকে খেয়াল করুন এবং কীভাবে এটি বেছে নিতে পারেন তা বিবেচনা করুন। টিভিতে কি এ বিষয়ের কোনো বিজ্ঞাপন দেখেছেন? কোনো বন্ধু কি এটি সাজেস্ট করেছেন? এটি কি কমপিউটারের সাথে প্যাকেজ আকারে এসেছে?

আপনি যে সেরা অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার করছেন নিশ্চিত হওয়ার জন্য, বিভিন্ন অ্যান্টিভাইরাসের ওয়েবসাইটে ভিজিট করে জেনে নিন তাদের গুণাগুণ ও বৈশিষ্ট্য। যদি অ্যান্টিভাইরাস প্রোডাক্টের প্রটেকশনে কোনো ত্রুটির কথা জানতে পারেন অথবা ভালো র‍্যাঙ্কের না হয়ে থাকে, তা এড়িয়ে যেতে পারেন। লক্ষণীয়, যদি ফ্রি সিকিউরিটি সফটওয়্যার ব্যবহার করেন, তাহলে মনে রাখবেন লাইসেন্সড সফটওয়্যারের চেয়ে এর ফিচার ও সুবিধা কম থাকবে সঙ্গত কারণে।

ভিপিএন ভেরিফাই করা

একটি ভিপিএনের (VPN) পূর্ণ রূপ হলো ভার্চুয়াল প্রাইভেট নেটওয়ার্ক। ভার্চুয়াল প্রাইভেট নেটওয়ার্ক হলো একটি টেকনোলজি, যা কম নিরাপদ নেটওয়ার্কের মাধ্যমে তৈরি করে এক নিরাপদ এবং এনক্রিপটেড কানেকশন, যেমন ইন্টারনেট। রিমোট ইউজারদের অনুমোদন করার জন্য ভিপিএন টেকনোলজি ডেভেলপ করা হয় একটি উপায় হিসেবে এবং ব্রাঞ্চ অফিস নিরাপদে কর্পোরেট অ্যাপ্লিকেশন এবং অন্যান্য রিসোর্সে অ্যাক্সেস করতে পারে।



আইপি অ্যাড্রেস সম্পর্কে জানা

ভিপিএন ইন্টারনেট ট্যাফিক প্রোটেক্ট করে একটি এনক্রিপ্টেড কানেকশনের মাধ্যমে এটিকে রাউটিং করে। এ সময় কেউ আপনার ডাটা দেখতে পারবে না, এমনকি নেটওয়ার্কের স্বত্বাধিকারীও দেখতে পারবে না এবং যে সাইটের সাথে কানেক্ট হয়েছেন তা ভিপিএন সার্ভারের আইপি অ্যাড্রেস দেখে, শুধু আপনার নিজেরটি নয়। এভাবে আপনার প্রাইভেসি রক্ষিত হবে। কিন্তু কীভাবে বুঝবেন এটি যে কাজ করছে?

আপনার ভিপিএন যদি লিক করে, তাহলে তা বুঝতে পারবেন কিছু সাধারণ কৌশল অবলম্বন করে। ভিপিএন বন্ধ করুন এবং আপনার প্রকৃত আইপি অ্যাড্রেস দেখার জন্য গুগলে "what is my ip" সার্চ করুন। এবার ভিপিএনকে ব্যস্ত রাখুন এবং আবার চেক করুন। আপনার উচিত একটি ভিন্ন আইপি অ্যাড্রেস দেখা। আপনি ইচ্ছে করলে ওই আইপি অ্যাড্রেসের লোকেশন ভেরিফাই করার জন্য একটি জিওলোকেশন ওয়েবসাইট ব্যবহার করতে পারেন, যাতে ভিপিএনের মাধ্যমে এর লোকেশনের অবস্থান নিশ্চিত করা যায়।

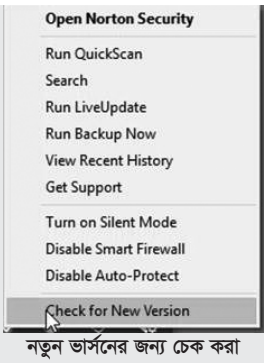
মোবাইল ডিভাইস চেক করা

অ্যাপল আইওএসকে আকর্ষণীয়ভাবে এয়ারটাইট করে তৈরি করেছে। তবে অ্যান্ড্রয়েড ডিভাইস তেমনভাবে নিরাপদ নয়। বর্তমানে প্রযুক্তিবিশ্বে লাখ লাখ ম্যালিশাস প্রোগ্রামের অস্তিত্ব রয়েছে, যাদের উদ্দেশ্য অ্যান্ড্রয়েড ডিভাইসের ব্যাপক ক্ষতিসাধন করা। যদি আপনার অ্যান্ড্রয়েড ডিভাইসে কোনো সিকিউরিটি প্রোগ্রাম না থাকে, তাহলে বলা যায়, আপনি এক মারাত্মক ঝুঁকির মধ্যে আছেন এবং টিপিক্যাল অ্যান্ড্রয়েড সিকিউরিটি টুল ম্যালওয়্যার প্রোটেকশন এবং অ্যান্টিথেফট উভয় ফিচার অফার করে।

ইতোমধ্যেই আপনার কাছে অ্যান্ড্রয়েড প্রোটেকশন ব্যবস্থা থাকতে পারে একটি ▸

অ্যান্টিভাইরাসকে আপ টু ডেট রাখা

আধুনিক অ্যান্টিভাইরাস ইউটিলিটি ব্যবহার করে আচরণভিত্তিক ডিটেকশন সিস্টেম। সুতরাং এগুলো এমনসব ম্যালওয়্যার প্রতিহত করতে পারে, যেগুলো ইতঃপূর্বে কখনোই হতে দেখা যায়নি। যাই হোক, বেশিরভাগ অ্যান্টিভাইরাস ইউটিলিটি এখনো সহজ-সরল পরিচিত হুমকি অপসারণ করার জন্য ব্যবহার করে ম্যালওয়্যার সিগনেচার, যা এক ধরনের ডিজিটাল ফিঙ্গারপ্রিন্ট। আপনার অ্যান্টিভাইরাস ইউটিলিটি ওপেন করুন। ভাইরাস ডাটাবেজ আপডেট করার প্রয়োজনীয়তা সংশ্লিষ্ট কোনো মেসেজ কখনো কী দেখেছেন? এমনকি আপনি যদি কমান্ড খোঁজার জন্য পুঙ্খানুপুঙ্খ অনুসন্ধান নাও করেন, যা আপডেটের জন্য অন-ডিমান্ড চেক রান করে।



নতুন ভার্সনের জন্য চেক করা

আরো চেক করে দেখুন, পণ্যের নিজের জন্য আপডেট অ্যাভেইলেবেল কি না। আসলে আপডেটের জন্য আপনার সব সিকিউরিটি পণ্য চেক করা উচিত। আপডেট চেক করার জন্য আপনি বৈশিষ্ট্যসূচকভাবে File অথবা Help মেনুতে একটি অপশন পাবেন অথবা নোটিফিকেশন এরিয়ায় প্রোডাক্ট আইকনে ডান ক্লিক করলে একটি মেনু আবির্ভূত হবে। এ কাজ করার সময় আবিষ্কার করতে পারবেন যে আপনার সাবস্ক্রিপশন মেয়াদ শেষ হয়েছে।

ডেস্কটপ সিকিউরিটি স্যুটের অংশ হিসেবে। আধুনিক কিছু কিছু সিকিউরিটি স্যুট মাল্টিপল প্লাটফরম জুড়ে কাজ করতে পারে। কোন অ্যান্ড্রয়েড অ্যান্টিভাইরাস টুল কেমন পারফরম করতে পারে, তা জানতে অ্যান্ড্রয়েড প্রোটেকশন ওয়েবসাইটে ভিজিট করুন।

পাসওয়ার্ড অ্যানালাইজ করা

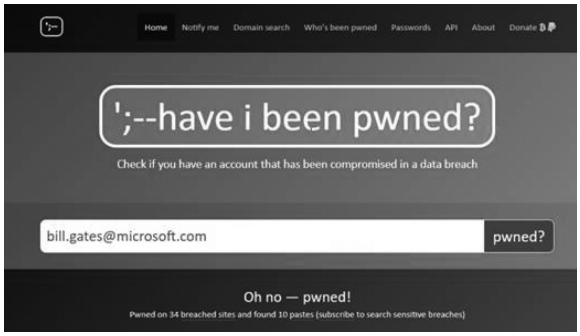
একটি পাসওয়ার্ড ম্যানেজার হলো একটি সফটওয়্যার অ্যাপ্লিকেশন। এটি মূলত ব্যবহার হয় পাসওয়ার্ড স্টোর ও ম্যানেজ করতে, যা এটি ব্যবহারকারীর আছে বিভিন্ন অনলাইন অ্যাকাউন্ট এবং সিকিউরিটি ফিচারের জন্য। একটি পাসওয়ার্ড ম্যানেজার জটিল পাসওয়ার্ড জেনারেট এবং রিট্রাইভ করতে সহায়তা করে।

সুতরাং এখন প্রশ্ন হলো, আপনি কি কোনো পাসওয়ার্ড ম্যানেজার ব্যবহার করেছেন? যদি ব্যবহার করে থাকেন, তাহলে ভালো কথা। কিন্তু এটি কি আপনার জন্য একগুচ্ছ দুর্বল, ডুপ্লিকেট পাসওয়ার্ড সেভ করছে না? আসলে একটি সিস্টেমে আপনার সব পাসওয়ার্ড পাওয়াটাই হলো আসল কথা।

বেশিরভাগ পাসওয়ার্ড ম্যানেজার পাসওয়ার্ড স্ট্রেন্থের ওপর একটি রিপোর্ট সম্পৃক্ত করে। সেরাটি একটি লিস্ট প্রদান করে, যা আপনি শক্তির আলোকে সর্ট তথা ক্রমানুসারে বিন্যাস করতে পারবেন। যদি আপনি একগুচ্ছ দুর্বল এবং ডুপ্লিকেট পাসওয়ার্ড সেভ করেন, তাহলে সেগুলো ফিক্স করার জন্য চেষ্টা করুন। সবচেয়ে খারাপ পাঁচটি ফিক্স করুন অথবা যদি হাতে প্রচুর সময় থাকে. তাহলে সেগুলোও ফিক্স করুন।

Have You Been Pwned?

Have I Been Pwned? (HIBP) হলো একটি ওয়েবসাইট, যা ইন্টারনেট ব্যবহারকারীদেরকে সুযোগ করে দেয় তাদের পার্সোনাল ডাটা চেক করে দেখার জন্য যে ডাটা ব্যত্যয়কারীদের মাধ্যমে তাদের ডাটা কমপ্রোমাইজ হয়েছে কি না। এ সার্ভিসটি জনপ্রিয় এবং এই টুল সাধারণত ব্যবহার হয় আইটি সিকিউরিটিতে।



Have I Been Pwned ওয়েবসাইট

একটি ডাটাবেজ সার্ভিস সংগ্রহ করা হয় পরিচিত লিক সাইট থেকে। বিশেষ কোনো ই-মেইল অ্যাকাউন্ট ডাটা ব্যত্যয়ের মাধ্যমে কম্প্রোমাইজ হয়েছে কি না তা দ্রুতগতিতে চেক করে দেখার জন্য সার্ভিস ব্যবহারকারীদের সুযোগ করে দেয়। বেশ কিছু ক্রল করা ওয়েবসাইট এবং ডাটাবেজ স্তূপ থেকে ডাটাবেজ সংগ্রহ করা হয়।

প্রতি সপ্তাহে ডাটা ব্যত্যয় ঘটে থাকে এবং পার্সোনাল ইনফরমেশন ডার্ক ওয়েবে লিক হয়। এর ফলে আপনি হয়তো এক্সপোজ হতে পারেন, কিন্তু তা জানবেন কীভাবে?

এমন এক অবস্থায় Have I Been Pwned নামে এক ওয়েবসাইট আপনাকে সাহায্য করতে পারে। এক্ষেত্রে একটি পরিচিত ডাটা ব্যত্যয়ে (breach) আপনার তথ্য প্রকাশিত হয়েছে কি না, তা খুঁজে পেতে অথবা Pastebin-এর মতো সাইটে ডাটা ডাম্পে শুধু আপনার ই-মেইল অ্যাড্রেস এন্টার করুন। যদি আপনি 'Oh no' pwned মেসেজ রিসিভ করেন, তাহলে তাৎক্ষণিকভাবে আপনার অ্যাকাউন্ট পাসওয়ার্ড বদলিয়ে ফেলুন।

সোশ্যাল মিডিয়া সিকিউরিটি রিভিউ করা

বিনাবাক্যে বলা যায়, আপনার সোশ্যাল মিডিয়া অ্যাকাউন্ট (টুইটার ছাড়া) প্রাইভেটে সেট করা করা উচিত, যাতে শুধু আপনার বন্ধুরা আপনার পোস্ট দেখতে পারবেন। তবে সেরা নিরাপত্তা ব্যবস্থার জন্য আপনি কনফিগার করেছেন কি না, তা নিশ্চিত হওয়ার জন্য কখনো কি চেক করে দেখেছেন? এবার লগইন করুন, সেটিংয়ে নেভিগেট করুন এবং সিকিউরিটি অথবা প্রাইভেসিসংশ্লিষ্ট যেকোনো জিনিস রিভিউ করুন।

সিকিউরিটি ওয়াচ লোগো

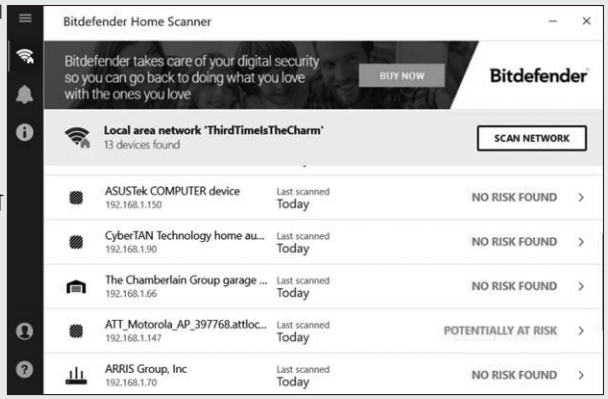
উদাহরণস্বরূপ, আপনি চান ফেসবুকে বন্ধুরা শুধু আপনার পোস্ট দেখতে পারবে এবং শুধু বন্ধুদের বন্ধুরা নতুন ফ্রেন্ড রিকোয়েস্ট পাঠানোর জন্য অনুমোদিত। সার্চ ইঞ্জিন আপনার প্রোফাইলে লিঙ্ক করুক তা আপনি চান না।

ফেসবুক আপনাকে সব ডিভাইস রিভিউ করার সুযোগ করে দেবে যেগুলো আপনার অ্যাকাউন্টে লগ করা আছে। লিস্ট রিভিউ করুন এবং এগুলোর মধ্যে কোনোটি যদি অনিয়মিত বা সন্দেহজনক মনে হয়, তাহলে তাৎক্ষণিকভাবে লগআউট করুন।

আপনি হয়তো এটি বুঝতে নাও পারেন। এমনকি যদি আপনার নিজের সেটিং খুব দৃঢ় হয়, তাহলেও ফ্রেন্ডস এবং অ্যাপস আপনার ডাটা লিক করতে পারবে। ফেসবুকে এপিআই (API) শেয়ারিং ডিজ্যাবল করার মাধ্যমে আপনি ওই লিক বন্ধ করতে পারবেন। ফেসবুক এবং গুগলের মাধ্যমে আপনি ডাউনলোড এবং ভিউ করা ডাটা সেভ করতে পারবেন কজ

ইন্টারনেট অব থিংস স্ক্যান করা

আপনার কমপিউটার এবং মোবাইল ডিভাইসই একমাত্র উপকরণ নয়, যা আপনার হোম নেটওয়ার্কের সাথে কমিউনিকেট করতে পারে। আপনার ওই নেটওয়ার্কে অন্যান্য আরো অনেক ডিভাইস থাকার সম্ভাবনা আছে, যেমন গেম কন্সোল, ভিডিও ডোরবেল, গ্যারেজ-ডোর ওপেনার ইত্যাদি। কিন্তু সমস্যাটা হলো এসব ডিভাইসে সিকিউরিটি সফটওয়্যার ইনস্টল করা যায় না। সুতরাং এসব ডিভাইস যে নিরাপদ সে ব্যাপারে আপনি নিশ্চিত হতে পারবেন না কখনোই।



বিটডিফেন্ডার সিকিউরিটি টুল দিয়ে নেটওয়ার্ক স্ক্যান করা

ইদানীং ফ্রি হোম সিকিউরিটি স্ক্যানারের ক্যাটাগরি ক্রমবর্ধমান হারে বাড়ছে, যেমন অ্যাভাইরা হোম গার্ডের মতো প্রোগ্রাম, যা দুটি প্রয়োজনীয় কাজ সম্পাদন করে। প্রথমত, নেটওয়ার্কে ঠিক কী কী ডিভাইস আছে তা জানার সুযোগ করে দেয়। এ লিস্টের সাইজ দেখে আপনি হয়তো বিস্মিত হতে পারেন। দ্বিতীয়ত, এগুলো ওইসব ডিভাইসের সিকিউরিটি সমস্যা চেক করে দেখবে।

বিটডিফেন্ডার হোম স্ক্যানার সম্ভাব্য ভলনিয়ারিবিলিটির ওপর সাধারণ রিপোর্ট একধাপ ছাড়িয়ে গেছে। যখন একটি নতুন ডিভাইস নেটওয়ার্কে যুক্ত হয়, তখন এটি পপআপ করে একটি নোটিফিকেশন এবং এটি স্ক্যান করার জন্য অফার করে।