# অনলাইনে অধিকতর সুরক্ষিত থাকার জন্য যেসব কাজ করতে পারেন

তাসনীম মাহ্‌মুদ

**আপনার ডিভাইস, ডাটা, ইন্টারনেট ট্রাফিক এবং পরিচয় সুরক্ষার জন্য নিচে বর্ণিত সহজ কৌশলগুলো অনুসরণ করতে পারেন–**

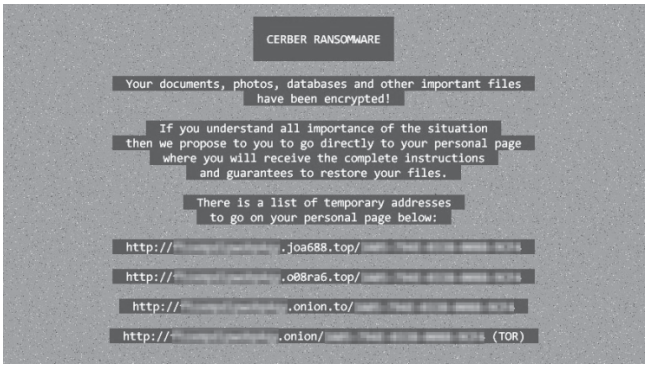
যদি বড় কোনো শপিং অথবা ফিন্যান্সিয়াল সাইট ডাটা লঙ্ঘনের শিকার হয়, তাহলে পাসওয়ার্ড পরিবর্তন করা, একটি নতুন ক্রেডিট কার্ড ব্যবহার করা এবং ক্রেডিট কার্ডের ব্যবহার বন্ধ করা ছাড়া তেমন কিছু করার থাকে না। এ ধরনের আক্রমণ থেকে রক্ষা পাওয়া প্রায় অসম্ভব বলা গেলেও অনেক ধরনের

সিকিউরিটি সমস্যা রয়েছে, যার নিয়ন্ত্রণ আমাদের হাতের নাগালে। মুক্তিপণ প্রদান না করা পর্যন্ত র‍্যানসামওয়্যার কার্যকরভাবে আপনার কমপিউটারকে আটক করতে পারে। ডাটা চুরি করা ট্রোজান আপনার সব সিকিউর লগইন তুলতে পারে। সৌভাগ্যের বিষয়, লোকাল এসব সমস্যার বিরুদ্ধে প্রতিরোধ গড়তে আপনি অনেক কিছু করতে পারেন।

আপনার ডিভাইস, অনলাইন আইডেন্টিটি এবং কার্যকলাপকে অধিকতর সুরক্ষিত করার জন্য খুব বেশি পরিশ্রম করতে হয় না। প্রকৃতপক্ষে, অনলাইনে অধিকতর নিরাপদ থাকার জন্য আপনি যা করতে পারেন, তা হলো সাধারণ জ্ঞান প্রয়োগ করে কার্যকর কিছু পদক্ষেপ গ্রহণ করা, যা হয়তো বেশিরভাগ সময় আমরা এড়িয়ে যাই। এ লেখায় ব্যবহারকারীর অনলাইন জীবনকে অধিকতর সুরক্ষিত করার উদ্দেশ্যে এমনই কিছু সাধারণ জ্ঞানমূলক কৌশল তুলে ধরা হয়েছে।

## ১. একটি অ্যান্টিভাইরাস ইনস্টল এবং সিস্টেমকে আপডেট রাখুন

আমরা যেসব সফটওয়্যারকে অ্যান্টিভাইরাস সফটওয়্যার হিসেবে জানি, সেগুলো আসলে সব ধরনের ম্যালিশাস তথা ক্ষতিকর সফটওয়্যার থেকে আমাদেরকে সুরক্ষিত করে। র‍্যানসামওয়্যার আমাদের ফাইলকে এনক্রিপ্ট করে এবং সেগুলো রিস্টোর করার জন্য মুক্তিপণ দাবি করে। ট্রোজান হর্স প্রোগ্রাম বৈধ প্রোগ্রামের মতো আচরণ করে, কিন্তু পর্দার আড়ালে এগুলো ব্যবহারকারীর ব্যক্তিগত তথ্য হাতিয়ে নেয়। বটস আপনার কমপিউটারকে জম্বি আর্মির এক সৈনিকে রূপান্তর করে ড্যানিয়াল অব সার্ভিস অ্যাটাকে (DoS) অথবা যেকোনো স্প্যাম বা কমান্ডে ব্যস্ত থাকে। একটি ভালো অ্যান্টিভাইরাস প্রোগ্রাম বিভিন্ন ধরনের ম্যালওয়্যার এবং অন্যান্য ক্ষতিকর প্রোগ্রামের বিরুদ্ধে কার্যকরভাবে প্রতিরোধ গড়ে তুলতে পারে। তত্ত্বীয়ভাবে, আপনি অ্যান্টিভাইরাস প্রোটেকশন সেট করতে এবং ভুলে যেতে পারেন যা ব্যাকগ্রাউন্ডে ডাউনলোড, আপডেটসহ আরও কিছু কাজ করে। বেশিরভাগ অ্যান্টিভাইরাস ইউটিলিটি ডিসপ্লে করে এক সবুজ ব্যানার অথবা আইকন যখন কোনো সমস্যা থাকে না এবং সবকিছু ঠিকভাবে কাজ করে। যদি কোনো ইউটিলিটি ওপেন করার পর হলুদ বা লাল বর্ণ দেখতে পাওয়া যায়, তাহলে সবকিছু ট্র্যাকে ফিরিয়ে আনতে নিচে বর্ণিত ধাপগুলো সম্পন্ন করুন।




*চিত্র-২ : সাইবার র‍্যানসামওয়্যারের শিকার*

আপনি হয়তো ভাবতে পারেন, অ্যান্টিভাইরাস উইন্ডোজে বিল্ট-ইন নয়। মাইক্রোসফট উইন্ডোজ ডিফেন্ডার সিকিউরিটি সেন্টার শুধু অপারেটিং সিস্টেমের মধ্যে বেইক করা নয়। এটি যখন অন্য কোনো অ্যান্টিভাইরাস শনাক্ত করে না, তখন স্বয়ংক্রিয়ভাবে সুরক্ষার ভার গ্রহণ করে এবং থার্ড-পার্টি প্রোটেকশন ইনস্টল করার পর স্বয়ংক্রিয়ভাবে আলাদা হয়ে যায়। ব্যাপারটি হলো এই বিল্ট-ইন অ্যান্টিভাইরাসটি সেরা থার্ড-পার্টি সলিউশনের সাথে তুলনা করে না। অনেকের মতে, সেরা ফ্রি অ্যান্টিভাইরাসগুলো উইন্ডোজ ডিফেন্ডারের চেয়ে ভালো কাজ করে।

যদি কোনো সাধারণ অ্যান্টিভাইরাস অথবা একটি পরিপূর্ণ সিকিউরিটি স্যুট বেছে নিয়ে থাকেন, তাহলে আপনাকে প্রতি বছর নতুন করে নবায়ন করে নিতে হবে। আপনার জন্য সবচেয়ে ভালো হবে, স্বয়ংক্রিয়ভাবে নবায়নের জন্য নিবন্ধন করা। অবশ্য কিছু সিকিউরিটি পণ্য ম্যালওয়্যারমুক্ত হিসেবে নিশ্চয়তা প্রদান করে। তবে সিকিউরিটি পণ্যগুলো ভিন্ন অপশনে সুইচ করার জন্য সুযোগ প্রদান করে সবসময়।

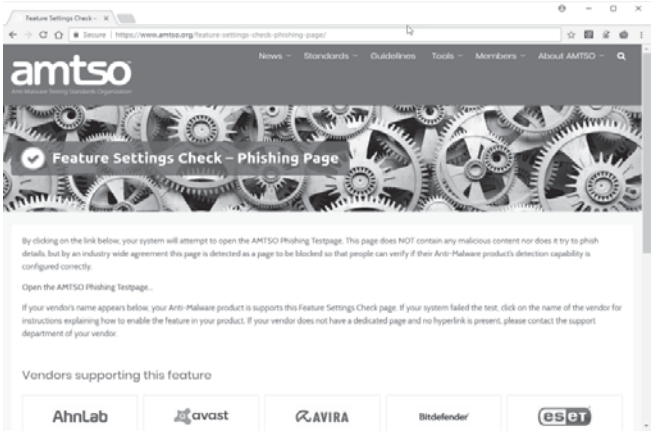
আরেকটি লক্ষণীয় বিষয়, যদি আপনার অ্যান্টিভাইরাস অথবা সিকিউরিটি স্যুটে র‍্যানসামওয়্যার প্রোটেকশন সমন্বিত না হয়, তাহলে প্রটেকশনের আলাদা আরেকটি লেয়ার যুক্ত করার কথা বিবেচনা করতে পারেন। র‍্যানসামওয়্যার-নির্দিষ্ট অনেক ইউটিলিটি আছে, যেগুলো সম্পূর্ণ ফ্রি। কোনো কারণ নেই, এগুলো দিয়ে চেষ্টা না করার। সুতরাং আপনার চাহিদা অনুযায়ী সেরা স্যুট নিন।

## ২. আপনার ইনস্টল করা সিকিউরিটি টুল এক্সপ্লোর করা

অনেক অ্যাপ্লিকেশন এবং সেটিংস আপনার ডিভাইস এবং আইডেন্টিটি রক্ষা করতে সহায়তা করে। তবে এগুলো শুধু তখনই গুরুত্বপূর্ণ ভূমিকা রাখতে পারবে, যখন যথাযথভাবে ব্যবহার করতে পারবেন। উদাহরণস্বরূপ, স্মার্টফোনে এমন এক অপশন যুক্ত করা হয়েছে, যা ফোন হারিয়ে গেলে খুঁজে পেতে সহায়তা করবে। এ ফিচারটি সবসময় সক্রিয় অর্থাৎ অন রাখা উচিত।

আপনার অ্যান্টিভাইরাস টুলটি সম্ভবত পটেনশিয়ালি আনওয়ান্টেড অ্যাপ্লিকেশন (PUAs) প্রতিরোধ করার ক্ষমতা রাখে, ঝামেলাযুক্ত অ্যাপস যা হুবহু ম্যালওয়্যার নয়, তবে উপকারী কিছু করে না। শনাক্তকরণ সেটিংস পরীক্ষা করে দেখুন এবং নিশ্চিত করুন যে এটি বিরক্তিকর বিষয়গুলো ব্লক করার জন্য কনফিগার করা

হয়েছে। তেমনই আপনার সিকিউরিটি স্যুটে এমন কোনো উপাদান থাকতে পারে, যা চালু না করা পর্যন্ত সক্রিয় হয় না। একটি নতুন সিকিউরিটি পণ্য ইনস্টল করার পর মূল উইন্ডোর সব পৃষ্ঠা ফ্লিপ করুন এবং সেটিংসে ন্যূনতম একবার নজর দিন।




*চিত্র-৩ : ফিচার সেটিংস চেক পেজ*

আপনার অ্যান্টিভাইরাসটি কনফিগার করা হয়েছে এবং সঠিকভাবে কাজ করছে তা সম্পূর্ণরূপে নিশ্চিত হওয়ার জন্য আপনি এএমটিএসওর (Anti-Malware Testing Standards Organization) ওয়েবসাইটে সিকিউরিটি ফিচার চেক পেজে ফিরে যেতে পারেন। প্রতিটি ফিচার চেক পেজ অ্যান্টিভাইরাস টুলের লিস্ট করে, যা পাস করা উচিত। যদি আপনার তালিকায় প্রদর্শিত হয় কিন্তু পাস না হয়, তবে টেক সাপোর্টের সাথে যোগাযোগ করে তার কারণ খুঁজে বের করার সময় হয়েছে ধরে নিতে পারেন।

## ৩. প্রতিটি লগইনের জন্য স্বতন্ত্র পাসওয়ার্ড ব্যবহার করা

হ্যাকারদের জন্য তথ্য চুরি করার অন্যতম সহজ উপায় হলো এক উৎস থেকে ব্যবহারকারীর নাম এবং পাওয়ার্ড সংমিশ্রণের একটি ব্যাচ পেয়ে অন্য কোথাও একই সংমিশ্রণ ব্যবহার করার জন্য চেষ্টা করা। উদাহরণস্বরূপ ধরা যাক, হ্যাকারেরা কোনো ই-মেইল প্রোভাইডারকে হ্যাক করে আপনার ইউজার নেম এবং পাসওয়ার্ড পেয়েছে। হ্যাকারেরা একই ইউজার নেম এবং পাসওয়ার্ডের সংমিশ্রণটি ব্যবহার করে ব্যাংকিং সাইট অথবা প্রধান অনলাইন স্টোরগুলোতে লগইন করার জন্য চেষ্টা করবে। সুতরাং একটি ডমিনো ইফেক্ট থেকে ডাটা লঙ্ঘন প্রতিরোধের সবচেয়ে ভালো একক উপায় হলো আপনার প্রত্যেকটি সিঙ্গেল অনলাইন অ্যাকাউন্টের জন্য একটি শক্তিশালী ইউনিক পাসওয়ার্ড ব্যবহার করা।

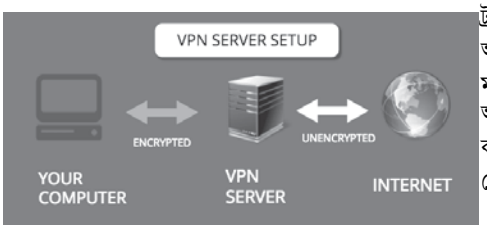
প্রতিটি অ্যাকাউন্টের জন্য একটি ইউনিক এবং শক্তিশালী পাসওয়ার্ড তৈরি করা মানুষের জন্য সম্ভবপর কাজ নয়। আর এ কারণে ব্যবহারকারীরা একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করে। বেশ কয়েকটি ভালো মানের ফ্রি পাসওয়ার্ড ম্যানেজার রয়েছে, যা খুব সহজে ব্যবহার করা যায়। তবে পেইড ভার্সনের পাসওয়ার্ড ম্যানেজার অধিকতর ফিচার সংবলিত, যা সাধারণত বাণিজ্যিক প্রতিষ্ঠানগুলো ব্যবহার করে থাকে।

যখন কোনো পাসওয়ার্ড ম্যানেজার ব্যবহার করবেন, তখন আপনাকে শুধু মাস্টার পাসওয়ার্ডটি মনে রাখতে হবে, যা নিজেই পাসওয়ার্ড ম্যানেজারকে লক করে। যখন আনলক করা হবে, তখন পাসওয়ার্ড ম্যানেজার স্বয়ংক্রিয়ভাবে আপনার অনলাইন অ্যাকাউন্টে লগইন করবে। এটি আপনাকে শুধু নিরাপদ রাখতেই সহায়তা করবে না বরং আপনার দক্ষতা এবং উৎপাদনশীলতা বাড়াতে সহায়তা করে। আপনাকে লগইন টাইপ করতে সময় ব্যয় করতে হবে না অথবা ভুলে যাওয়া পাসওয়ার্ড আবার সেট করার জন্য আপনাকে সময় ব্যয় করতে হবে না।

## ৪. ভিপিএন ব্যবহার করা

ওয়াই-ফাই নেটওয়ার্ক ব্যবহার করে যখনই ইন্টারনেটে যুক্ত হবেন, তখন আপনার জন্য উচিত হবে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক অথবা ভিপিএন ব্যবহার করা। উদাহরণস্বরূপ বলা যায়, কফি শপে গেলেন এবং ফ্রি ওয়াই-ফাই নেটওয়ার্কের সাথে যুক্ত হলেন। আপনি এই সংযোগের নিরাপত্তার ব্যাপরে তেমন কিছুই জানেন না। এটি সম্ভব হতে পারে যে এ নেটওয়ার্কে অন্য কেউ আপনার অজান্তেই আপনার ল্যাপটপ অথবা মোবাইল ডিভাইস থেকে সেন্ড করা ফাইল এবং ডাটা চুরি করে নিতে পারে অথবা আপনার অনলাইন অ্যাক্টিভিটির ওপর তীক্ষ্ণ নজর রাখতে পারে। ভিপিএন ইন্টারনেট ট্রাফিক এনক্রিপ্ট করে, এটিকে ভিপিএন কোম্পানি সার্ভার হিসেবে রুট করে। এর অর্থ হচ্ছে কেউ আপনার ডাটা দেখতে পারবে না, এমনকি ফ্রি ওয়াই-ফাই নেটওয়ার্কের মালিকও।

ভিপিএন ব্যবহার করার সময় আপনার আইপি অ্যাড্রেস হাইড করে রাখে। অ্যাডভার্টাইজার এবং ট্র্যাকার আপনাকে সেই আইপি অ্যাড্রেসের মাধ্যমে শনাক্ত করার অথবা জিওলোকেট করতে চাইবে ভিপিএন কোম্পানির অ্যাড্রেস

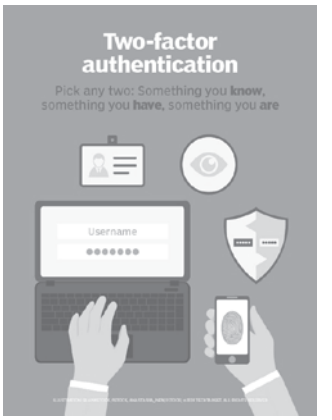



*চিত্র-৪ : ভিপিএন নেটওয়ার্ক*

দেখার পরিবর্তে। অন্য দেশে ভিপিএন সার্ভার ব্যবহার করে আপনার লোকেশন ধাপ্পা দিয়ে হাতিয়ে নিয়ে কনটেন্ট আনলক করার জন্য সার্ভ করতে পারে, যেগুলো আপনার অঞ্চলে পাওয়া যায় না। আরেকটি মারাত্মক বিষয় হলো, সন্ত্রাস দমনকারী দেশগুলোর সাংবাদিক এবং অ্যাক্টিভিস্টরা নিরাপদে যোগাযোগের জন্য দীর্ঘকাল ধরে ভিপিএন প্রযুক্তি ব্যবহার করে আসছে।

সবশেষে বলা যায়, আপনি যদি ওয়াই-ফাইয়ের মাধ্যমে কানেক্ট হন তা ল্যাপটপ, ফোন বা ট্যাবলেট হোক না কেন– প্রকৃত অর্থে আপনার দরকার ভিপিএন।

## ৫. টু-ফ্যাক্টর অথেন্টিকেশন ব্যবহার করা




*চিত্র-৪ : টু-ফ্যাক্টর অথেন্টিকেশন*

অনেকের কাছে টু-ফ্যাক্টর অথেন্টিকেশন যন্ত্রণাদায়ক মনে হতে পারে, তবে এটি নিশ্চিতভাবে ব্যবহারকারীর অ্যাকাউন্টকে অধিকতর সুরক্ষিত করে। টু-ফ্যাক্টর অথেন্টিকেশনের অর্থ হলো আপনার অ্যাকাউন্টে অ্যাক্সে করার জন্য শুধু ইউজারনেম এবং পাসওয়ার্ডই দরকার হয় না বরং আপনাকে অথেন্টিকেশনের আরেকটি লেয়ার অতিক্রম করতে হয়। যদি একটি অ্যাকাউন্টের ডাটা অথবা ব্যক্তিগত তথ্য খুব সংবেদনশীল অথবা মূল্যবান হয় এবং অ্যাকাউন্ট অফার করে টু-ফ্যাক্টর অথেন্টিকেশন, তাহলে আপনার উচিত এটি এনাবল করা। জি-মেইল, এভারনোট এবং ড্রপবক্স হলো কয়েকটি অনলাইন সার্ভিসের উদাহরণ, যা টু-ফ্যাক্টর অথেন্টিকেশন অফার করে।

টু-ফ্যাক্টর অথেন্টিকেশন ন্যূনতম দুটি ভিন্ন ধরনের অথেন্টিকেশন ব্যবহার করে আপনার পরিচয় যাচাই করে। যেমন something you are, something you have, or something you know| সামথিং ইউ নো হলো স্বাভাবিক পাসওয়ার্ড। সামথিং ইউ আর হলো ফিঙ্গারপ্রিন্ট অথবা ফেসিয়াল রিকগনিশন ব্যবহার করে অথেন্টিকেশন। সামথিং ইউ হ্যাভ দিয়ে আপনার মোবাইল ফোন বোঝাতে পারে। আপনাকে হয়তো টেক্সটের মাধ্যমে কোড এন্টার করার জন্য অথবা একটি মোবাইল অ্যাপে কনফারমেশন বাটনে ট্যাব করার জন্য বলতে পারে। সামথিং ইউ হ্যাভ এ ফিজিক্যাল সিকিউরিটি কী বুঝায় গুগল এবং মাইক্রোসফট এ ধরনের অথেন্টিকেশন সমর্থন করে।

যদি অথেন্টিকেশনের জন্য শুধু পাসওয়ার্ড ব্যবহার করেন, তাহলে যারা ওই পাসওয়ার্ডটি জানেন, তারা আপনার অ্যাকাউন্টের মালিক। টু-ফ্যাক্টর অথেন্টিকেশন এনাবল করার সাথে সাথে পাসওয়ার্ড একই অকেজো হয়ে পরে। বেশিরভাগ পাসওয়ার্ড ম্যানেজার টু-ফ্যাক্টর অথেন্টিকেশন সাপোর্ট করে যদিও এটি শুধু তখনই দরকার হয় যখন কোনো নতুন ডিভাইস থেকে একটি সংযোগ শনাক্ত করে। সুতরাং আপনার পাসওয়ার্ড ম্যানেজারের জন্য অবশ্যই টু-ফ্যাক্টর অথেন্টিকেশন এনাবল করা উচিত।

## ৬. ক্যাশ ক্লিয়ার করা

আপনার ব্রাউজার ক্যাশ আপনার সম্পর্কে কতটুকু জানে সে ব্যাপারে কখনো তুচ্ছ-তাচ্ছিল্ল করা উচিত নয়। সেভ করা কুকিজ, সেভ করা সার্চসমূহ এবং ওয়েব হিস্ট্রি আপনার বাড়ির ঠিকানা, পারিবারিক তথ্য এবং অন্যান্য ব্যক্তিগত তথ্য নির্দিষ্ট করতে পারে।

আপনার ওয়েব হিস্ট্রিতে লুকিয়ে থাকা তথ্যটি আরও সুরক্ষিত করতে ব্রাউজার কুকিজ মুছে ফেলার বিষয়ে নিশ্চিত হন এবং নিয়মিতভাবে অ াপনার ব্রাউজার হিস্ট্রি ক্লিয়ার করুন। এ কাজটি খুব সহজে করা যায়। ক্রোম, এজ, ফায়ারফক্স, ইন্টারনেট এক্সপ্লোরার অথবা ওপেরার ক্ষেত্রে Ctrl + Shift + Del চাপলে একটি ডায়ালগ বক্স আবির্ভূত হয়। কোনো ব্রাউজার ডাটা ক্লিয়ার রতে চান তা এই ডায়ালগ বক্স থেকে আপনি বেছে নিতে পারবেন। কুকিজ মুছে ফেলার ফলে কিছু ওয়েবসাইটে সমস্যা সৃষ্টি হতে পারে। বেশিরভাগ ব্রাউজার ফেভারিট ওয়েবসাইটের লিস্ট করে। কজ

ফিডব্যাক : mahmood_sw@yahoo.com