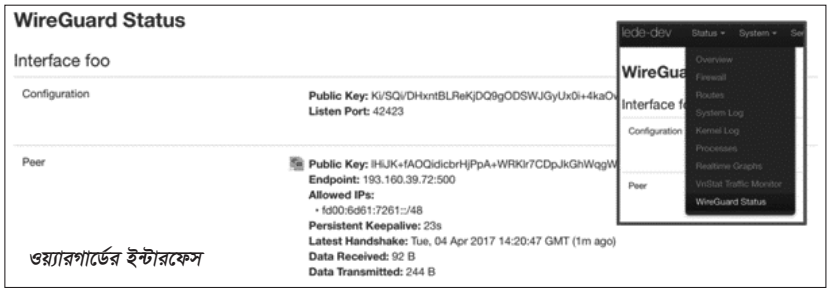
নিরাপদ ও গোপনীয়তার সাথে ওয়েবে ব্রাউজ করা

মইন উদ্দীন মাহ্‌মুদ

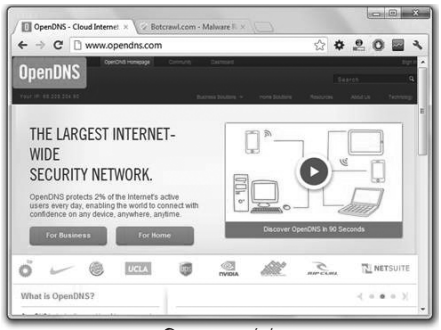
ইন্টারনেট ব্যবহারকারীরা সাধারণত নানা সমস্যার মুখোমুখি হন। সেগুলোর মধ্যে অন্যতম এক সাধারণ সমস্যা হলো ইন্টারনেট থেকে আপনার কাঙ্ক্ষিত তথ্য সরাসরি খুঁজে পাওয়া বেশ কঠিন। এর কারণ হলো, এখানে কোনো সেন্ট্রাল 'main menu' নেই, যেখানে ব্যবহারকারীরা আক্সেস করতে পারবেন ইন্টারনেট জুড়ে নেভিগেট করার জন্য। যদিও এখানে কোনো অফিসিয়াল মেনু থাকার সম্ভাবনা নেই, তবে অনলাইন এবং অফলাইন উভয়ের জন্য রয়েছে বেশ কিছু রিসোর্স, যা নেট সার্ফিংকে সহজতর করেছে। ইন্টারনেট হলো এক ট্রাফিক রিসোর্স। এটি ধারণ করে শত শত ওয়েবসাইট, যা হাজার হাজার টপিকের জন্য ডেডিকেটেড। কিছু কিছু ওয়েবসাইট রয়েছে, যেগুলো ব্যবহার হয় ওয়েবে তথ্য সার্চ করার জন্য। ওয়েবে তথ্য সার্চিংয়ে মুভ করতে হয় পেজ থেকে পেজে, ওয়েবসাইট থেকে ওয়েবসাইটে, যাকে বলা হয় ওয়েব ব্রাউজিং। এখানে একটি প্রধান সফটওয়্যার/অ্যাপ্লিকেশন আছে, যা মূলত ব্যবহার হয় ওয়েব ব্রাউজিংয়ে, যাকে বলা হয় ওয়েব ব্রাউজ করা বা ওয়েব ব্রাউজিং।



ওয়্যারগার্ডের ইন্টারফেস

মূলত ওয়েব ব্রাউজার হলো একটি ইন্টারফেস, যা কমপিউটার ব্যবহারকারীকে সহায়তা করে ইন্টারনেটের এবং কমপিউটারের হার্ডডিস্কের সব কনটেন্টে অ্যাক্সেসের। ওয়েব ব্রাউজারের সহায়তায় ব্যবহারকারী ফাইল, ফোল্ডার এবং ওয়েবসাইট জুড়ে নেভিগেট করতে পারে। যখন ব্রাউজার ব্যবহার হয় ওয়েব পেজ ব্রাউজিংয়ের জন্য, তখন পেজ ধারণ করতে পারে নির্দিষ্ট কিছু লিঙ্ক, যা নতুন ব্রাউজারে ওপেন হতে পারে।

সুতরাং, এখন প্রশ্ন হলো, আপনি কী নিরাপদে এবং গোপনীয়তার সাথে ওয়েব ব্রাউজ করতে চান? কঠিন বাস্তবতা হলো নিরাপদে এবং গোপনীয়তার সাথে ওয়েব ব্রাউজ করা প্রায় অসম্ভব।



ওপেন ডিএনএসের ইন্টারফেস

কোন সাইটে ভিজিট করছেন তা শুধু আপনার ইন্টারনেট সার্ভিস প্রোভাইডার জানে তা কিন্তু নয়, বরং সরকার এবং অন্যান্য সরকারও জানে। এ ছাড়া সোশ্যাল মিডিয়া সাইট, অ্যাড নেটওয়ার্ক অথবা অ্যাপ ওয়েব আপনাকে ট্র্যাক করতে থাকে সুনির্দিষ্ট এবং টার্গেট করা অ্যাড সরবরাহ করার জন্য। আপনার ওয়েব ব্রাউজিং হিস্ট্রি হতে পারে প্রচন্ডভাবে পার্সোনাল। এটি উন্মোচন করতে আপনার স্বাস্থ্য সচেতনতা, আপনার রাজনৈতিক বিশ্বাস এবং এমনকি আপনার পর্ণ অভ্যাসও। আপনি ছাড়া অন্য সবাই কেন এসব তথ্য জানবে?

যখনই আপনি একটি ওয়েবসাইটে ভিজিট করবেন, তখন ডাটার চিহ্ন পেছনে ফেলে রেখে যাবেন। আপনি এসব থামাতে পারবেন না কোনোভাবে। ঠিক যেভাবে ইন্টারনেট কাজ করে, এটা হবে ঠিক সেভাবে। তবে আপনার ফুটপ্রিন্ট কমানোর জন্য রয়েছে প্রচুর পরিমাণের উপকরণ। এ লেখায় কিছু টিপ তুলে ধরা হয়েছে আপনার বেজের বেশিরভাগ কাভার করার জন্য।

একটি ভিপিএন আইডেন্টিটি হাইড করতে সহায়তা করে, কিন্তু আপনাকে আনআইডেন্টিফাইড করে না

আপনি হয়তো শুনে থাকবেন, একটি ভিপিএন তথা ভার্চুয়াল প্রাইভেট নেটওয়ার্ক স্নুফার থেকে আপনার ইন্টারনেট ট্রাফিক নিরাপদ রাখে।

ভিপিএন আপনাকে একটি ডেডিকেটেড টানেল তৈরি করার সুযোগ করে দেবে, যাতে আপনার সব ট্রাফিক এর মধ্য দিয়ে প্রবাহিত হয়। সাধারণত একটি ভিপিএন সার্ভার আপনার ইন্টারনেট ট্রাফিককে ইন্টারনেট সার্ভিস প্রোভাইডারের কাছ থেকে লুকিয়ে রাখার সুযোগ কর দেয়। এটি ভালো হয় যদি আপনি এমন একটি দেশে থাকেন, যেখানে সেন্সরশিপ অথবা সার্ভিলেন্স চালু আছে অথবা লোকেশনভিত্তিক ব্লকিং এড়িয়ে যাওয়ার চেষ্টা করুন। আপনার সব ইন্টারনেট ট্রাফিক একটি ভিপিএন প্রোভাইডারের কাছে সেন্ড করছেন। মূলত আপনার ভিপিএন প্রোভাইডার অথবা আপনার ইন্টারনেট প্রোভাইডার এই দুইয়ের মধ্যে কাকে বেশি বিশ্বাস করেন, তা বেছে নিতে হবে। সমস্যাটি হলো সবচেয়ে ফ্রি ভিপিএন প্রোভাইডার তাদের অর্থ বানাচ্ছে আপনার ডাটা বিক্রি করে অথবা আপনার অ্যাড সার্ভ করার মাধ্যমে। এমনকি আপনি যদি প্রাইভেসির জন্য প্রিমিয়াম ভিপিএন প্রোভাইডার ব্যবহার করেন, তাহলে এগুলো আপনার পেমেন্ট ইনফরমেশন কানেক্ট করতে পারবে আপনার ইন্টারনেট ট্রাফিকে এবং অনেক ভিপিএন প্রোভাইডার আপনার ডাটা এনক্রিপ্ট করার জন্য মাথা ঘামায় না।

সিকিউরিটি প্রফেশনালদের মাধ্যমে পরিচালিত বিভিন্ন পরীক্ষায় দেখা গেছে কিছু কিছু ভিপিএন প্রোভাইডার একে অপরের চেয়ে ভালো। যেমন WireGuard-এর মতো সার্ভিস ব্যাপকভাবে রিকোমেন্ড করা হয়, যা আইফোন এবং আইপ্যাডসহ বিভিন্ন সিস্টেম এবং ডিভাইসে সদ্ব্যবহার করা যায়। সম্প্রতি বিভিন্ন গবেষণা প্রতিষ্ঠানের প্রোফাইলে দেখা গেছে যে, আইফোনের জন্য Guardian Mobile Firewall নামের এক স্মার্ট ফায়ারওয়াল-টাইপ অ্যাপ নিরাপদে টানেল করে যাতে ব্যবহারকারীর ডাটা নামহীনভাবে থাকে এবং অন্য কারো পক্ষে বুঝা সম্ভব নয়। এ অ্যাপ আপনার ফোনের অ্যাপকেও প্রতিহত করে, যাতে আপনি ট্র্যাক করতে না পারেন, যেমন আপনার কন্টাক্ট অথবা আপনার জিওলোকেশন।

যেহেতু TechCrunch-এর Romain Dillet ব্যাখ্যা করে বলেন যে, সেরা ভিপিএন হলো ওইটি যেটিকে আপনি নিজেই নিয়ন্ত্রণ করতে পারবেন। আপনি নিজেই কয়েক মিনিটের মধ্যে তৈরি করে নিতে পারবেন আপনার নিজস্ব ভিপিএন সার্ভার Algo VPN। আপনার নিজস্ব Algo VPN সেটআপ দিয়ে কানেকশন, সার্ভার এবং ডাটা কন্ট্রোল করতে পারবেন।

আপনার দরকার একটি নিরাপদ ডিএনএস

"your internet provider knows what sites you visit," anyway? এর অর্থ কী?

ইন্টারনেটে পর্দার আড়ালে ডিএনএস (Domain Name System) ওয়েব অ্যাড্রেসকে কমপিউটার রিডেবল আইপি অ্যাড্রেসে রূপান্তর করে। বেশিরভাগ ডিভাইস স্বয়ংক্রিয়ভাবে ব্যবহার করে রিসলভার, যা আপনার কানেক্টেড নেটওয়ার্কের সাধারণত ইন্টারনেট প্রোভাইডারের মাধ্যমে সেট করা হয়। এর অর্থ হচ্ছে আপনার ইন্টারনেট প্রোভাইডার জানে আপনি কোন ওয়েবসাইটে ভিজিট করেছেন। সম্প্রতি কংগ্রেস এক আইন পাস করে, যা আপনার ইন্টারনেট প্রোভাইডারকে আপনার ব্রাউজিং হিস্ট্রি ▸

বিজ্ঞাপনদাতাদের কাছে বিক্রি করা অনুমোদন করে।

এজন্য দরকার একটি নিরাপদ এবং প্রাইভেট ডিএনএস প্রোভাইডার। অনেকেই সর্বসাধারণের জন্য উন্মুক্ত সার্ভিস যেমন OpenDNS অথবা গুগলের PublicDNS ব্যবহার করেন। এগুলো সহজে আপনার কমপিউটারে অথবা ডিভাইসে অথবা হোম রাউটারে সেটআপ করা যায়।

একটি রিকোমেন্ডেড অফার হলো Cloudflare-এর সিকিউরিটি ডিএনএস, যাকে 1.1.1.1 বলা হয়। ক্লাউডফ্লায়ার আপনার ট্রাফিক এনক্রিপ্ট করে, অ্যাড সার্ভ করার জন্য আপনার ডাটা ব্যবহার করে না এবং যেকোনো দীর্ঘতর ২৪ ঘণ্টার জন্য আপনার আইপি অ্যাড্রেস স্টোর করে না। আপনি ইচ্ছে করলে অ্যাপলের অ্যাপ স্টোর এবং গুগল প্লে থেকে ক্লাউডফ্লায়ারের 1.1.1.1 অ্যাপ ডাউনলোড করতে পারবেন।

এইচটিটিপিএস

পার্সোনাল ইন্টারনেট সিকিউরিটির জন্য অন্যতম সেরা উপাদান হলো এইচটিটিপিএস (HTTPS)। এইচটিটিপিএস আপনার ফোন অথবা কমপিউটার থেকে শুরু করে ভিজিট করা সাইট পর্যন্ত সব কানেকশন সিকিউর করে। বেশিরভাগ গুরুত্বপূর্ণ ওয়েবসাইট এইচটিটিপিএস-এনাবল এবং আবির্ভূত হয় অ্যাড্রেস বারে গ্রিন প্যাডলক সহকারে। এইচটিটিপিএস কোনো কোনো ব্যক্তির জন্য আপনার ইন্টারনেট ট্রাফিক ইন্টারসেপ্টের ওপর গোয়েন্দাগিরি করা এবং ট্রানজিস্টের সময় ডাটা চুরি করা প্রায় অসম্ভব করে তোলে।

যখনই আপনার ব্রাউজার সবুজ বর্ণে প্রজ্বালিত হবে অথবা একটি প্যাডলক ফ্ল্যাশ করবে, এইচটিটিপিএস আপনার কমপিউটার এবং ওয়েবসাইটের মাঝে কানেকশন এনক্রিপ্ট করবে। এমনকি আপনি যখন একটি পাবলিক ওয়াই-ফাই নেটওয়ার্কে থাকবেন, তখন একটি এইচটিটিপিএস-এনাবলড ওয়েবসাইট আপনাকে একই নেটওয়ার্কের স্নুফ-ার থেকে রক্ষা করবে।

প্রায় প্রতিদিন ওয়েব হয়ে উঠছে অধিকতর নিরাপদ। কিছু ওয়েবসাইট হলো এইচটিটিপিএস রেডি, তবে বাই ডিফল্ট এটি এনাবল করা নয়। এর মানে হচ্ছে আপনি লোড করছেন একটি আনএনক্রিপ্টেড এইচটিটিপিএস পেজ যখন আপনি একটি সম্পূর্ণ এইচটিটিপিএস পেজে অ্যাক্সেস করতে পারবেন।

এক্ষেত্রে একটি ব্রাউজার এক্সটেনশন HTTPS সব জায়গায় কাজ করতে পারে। এই এক্সটেনশন ওয়েবসাইটকে বাধ্য করে বাই ডিফল্ট স্বয়ংক্রিয়ভাবে HTTPS লোড করতে। এটি এত ছোট এবং সহায়ক টুল হলেও ব্যবহারকারী ভুলে যায় এর উপস্থিতি।

পুনর্বিবেচনা করুন আপনার ওয়েব প্লাগ-ইনস

ফ্ল্যাশের কথা মনে আছে কী? জাভা সম্পর্কে কী জানেন? সম্ভবত এগুলোর সম্পর্কে সাম্প্রতিক কোনো তথ্য আপনার জানা নেই, ওইসব সেকেলে বা অপ্রচলিত প্রোগ্রাম রেন্ডার করতে ওয়েব বিবর্ধিত হয়েছে। এক সময়ের জনপ্রিয় দুই ওয়েব প্লাগ-ইন ফ্ল্যাশ এবং জাভা উভয়ই আপনার ওয়েব ব্রাউজারে ইন্টারেক্টিভ কনটেন্ট ভিউ করার সুযোগ করে দেবে। কিন্তু, এখন ওইগুলোর বেশিরভাগই প্রতিস্থাপিত হয়েছে HTML5-এর মাধ্যমে। এটি আপনার ওয়েব ব্রাউজারের একটি সহজাত টেকনোলজি।

ফ্ল্যাশ এবং জাভা দীর্ঘদিন ধরে উপহাসের পাত্র হয়ে আছে তাদের স্থায়ী নিরাপত্তাহীনতার কারণে। এগুলো ছিল বাগ ও ভালনিয়ারিবিলিটি পরিপূর্ণ, যা ইন্টারনেটকে বছরের পর বছর এমনভাবে আচ্ছন্ন করে রেখেছে। ওয়েব ব্রাউজার ২০১৫ সালে জাভার ব্যবহার বন্ধের পরিকল্পনা করেছে, সাথে ফ্ল্যাশ ২০২০ সালের মধ্যে।

যদি আপনি এগুলো ব্যবহার না করেন এবং বেশিরভাগ লোক যদি এগুলো না চান, তাহলে অপসারণ করতে পারেন। শুধু এগুলো ইনস্টল করা হলেও আক্রান্ত হওয়ার ঝুঁকির মধ্যে পড়তে হবে আপনাকে। উইন্ডোজ এবং ম্যাকে ফ্ল্যাশ এবং জাভা আনইনস্টল করতে পারবেন মাত্র কয়েক মিনিটের প্রচেষ্টায়।

ফায়ারফক্স এবং ক্রোমের মতো বেশিরভাগ ব্রাউজার আপনাকে অন্যান্য অ্যাড-অনস অথবা এক্সটেনশন রান করানোর সুযোগ করে দেয় আপনার ওয়েব এক্সপেরিয়েন্স উন্নত করতে। যেমন আপনার ফোনের অ্যাপ। এদের দরকার আপনার ব্রাউজারে অ্যাক্সেস করা, এমনকি আপনার ডাটায় অথবা কমপিউটারে অ্যাক্সেস। যদিও ব্রাউজার এক্সটেনশন ম্যালিশাস ব্যবহার প্রতিরোধে চেক হয়, তারপরও কখনো কখনো খারাপ এক্সটেনশন খুঁজে পাওয়া যায় না। আবার কোনো কোনো এক্সটেনশন স্বয়ংক্রিয়ভাবে আপডেট হয় ম্যালিশাস কোড ধারণ করতে অথবা গোপনে ব্যাকগ্রাউন্ডে ক্রিপ্টোকারেন্সি মাইন।

কোনটি ভালো এক্সটেনশ আর কোনটি নয়, তা নির্ধারণ করার কোনো নির্দিষ্ট নিয়ম নেই। এক্ষেত্রে ব্যবহার করতে হবে নিজস্ব মেধা-মনন। নিশ্চিত করুন, আপনার ইনস্টল করা প্রতিটি এক্সটেনশন আপনার প্রত্যাশার চেয়ে বেশি কিছু আশা করে না। যেসব এক্সটেনশন আপনি কখনো ব্যবহার করেন না, সেগুলো অপসারণ ও আনইনস্টল করার ব্যাপারটি নিশ্চিত করুন।

প্লাগ-ইনস এবং এক্সটেনশন আপনাকে প্রোটেক্ট করতে পারবে

কিছু কিছু এক্সটেনশন আছে, যেগুলো খুব মূল্যবান। এসব এক্সটেনশন আমাদের বিবেচনায় থাকা উচিত-

অ্যাড-ব্লকার : নামেই বুঝা যাচ্ছে অ্যাড ব্লক করার জন্য অ্যাড-ব্লকার (AdBlock) চমৎকারভাবে কাজ করলেও কোড প্রাইভেসি ভেদ করে, যা সাইট জুড়ে ট্র্যাক করতে পারে। uBlock হলো এক কার্যকর জনপ্রিয় ওপেন সোর্স ব্লকার, যা খুব বেশি মেমরি কনজ্যুম করে না যেমনটি অ্যাডব্লক এবং অন্যান্য

অ্যাডব্লকার ইন্টারফেস

টুল করে থাকে। অনেক অ্যাড-ব্লকার বর্তমানে পারমিট তথা অনুমোদন করে "acceptable ads", যা পাবলিশারদেরকে অর্থ আয়ের সুযোগ করে দেয়, তবে প্রচুর পরিমাণে মেমরি ব্যবহার করে না অথবা অনধিকার প্রবেশমূলক নয়। অ্যাড-ব্লকার টুল ওয়েবসাইট লোড করে দ্রুতগতিতে।

ক্রস-সাইট ট্র্যাকার ব্লকার : প্রাইভেসি ব্যাজার (Privacy Badger) হলো এক চমৎকার টুল, যা ব্লক করতে পারে ক্ষুদ্র "pixel" সাইজ ট্র্যাকার, যা ওয়েব পেজে হিডেন থাকে, তবে আপনাকে ট্র্যাক করবে সাইট থেকে সাইটে, আপনাকে অ্যাড সার্ভ করার জন্য আপনার সম্পর্কে আরো বেশি জানবে। Ghostery হলো আরেকটি অ্যাডভ্যান্সড লেভেলের অ্যান্টি ট্র্যাকার, যার লক্ষ্য হলো বাই ডিফল্ট ব্যবহারকারীদেরকে হিডেন ট্র্যাকারদের কাছ থেকে রক্ষা করা।

টর ব্যবহার করা

টর (Tor) গূঢ় রহস্যপূর্ণতা নেটওয়ার্ক হিসেবে পরিচিত। এটি একটি প্রটোকল, যা ব্যবহারকারীর ইন্টারনেট ট্রাফিক বিশ্বজুড়ে এক সিরিজ র‍্যান্ডম রিলে সার্ভারের মাধ্যমে বাউন্স করে এবং কাভার করে আপনার ট্র্যাক। আপনি এটি বেশিরভাগ ডিভাইসে এবং রাউটারে কনফিগার করতে পারবেন। বেশিরভাগ লোক যারা টর ব্যবহার করেন, তারা টর ব্রাউজার ব্যবহার করেন। এটি ফায়ারফক্সের প্রিকনফিগার করা এবং লকড-ডাউন ভার্সন, যা ভালো কাজ করে শুরু থেকে হতে পারে এটি রেগুলার ওয়েবসাইট অথবা একটি অনিয়ন সাইট।

আপনার ওয়েব ট্রাফিকের ওপর নজরদারিকে প্রায় অসম্ভব করে তুলেছে, বিশেষ করে কোন সাইট ভিজিট করছেন তা জানা। অ্যাক্টিভিস্ট এবং সাংবাদিকেরা সচরাচর সেন্সরশিপ এবং নজরদারি এড়ানোর জন্য টর ব্যবহার করেন কজ