অনলাইনে অধিকতর নিরাপদ থাকার জন্য করণীয়

মইন উদ্দীন মাহ্‌মুদ

ই-মেইল হ্যাকার, আইডেন্টিটি চোর এবং অনলাইন ক্রেডিট কার্ড প্রতারক লুট করে নিতে পারে আপনার অর্থ, গুরুত্বপূর্ণ গোপন তথ্য ইত্যাদি। যদি আপনি কখনই ডাটা ব্যত্যয়ের শিকার না হন, তাহলে নিজেকে ভাগ্যবান হিসেবে গণ্য করতে পারেন। তবে ভাগ্য সুপ্রসন্ন হওয়ায় আত্মতৃপ্তিতে গা ভাসিয়ে চলা ঠিক হবে না, কেননা অনলাইনে আপনার চারপাশে রয়েছে অসংখ্য ই-মেইল হ্যাক, আইডেন্টিটি চোর এবং অনলাইন ক্রেডিট কার্ড প্রতারকেরা যারা সুযোগ পেলেই আপনার চরম সর্বনাশ করতে পারে। তাই আপনার উচিত অনলাইন আইডেন্টিটি এবং অ্যাক্টিভিটিকে প্রকৃত অর্থে নিরাপদ করার জন্য কার্যকর ব্যবস্থা নেয়া যায়, যা খুব একটা সময় সাপেক্ষ ব্যাপার নয়। অনলাইনে অধিকতর নিরাপদ থাকার জন্য ব্যবহারকারীকে নিচে বর্ণিত টিপগুলো অনুসরণ করতে হবে।

প্রতিটি লগইনের জন্য ইউনিক পাসওয়ার্ড ব্যবহার

হ্যাকারদের জন্য ব্যবহারকারীর গুরুত্বপূর্ণ তথ্য চুরি করা তথা হাতিয়ে নেয়ার অন্যতম এক সহজ উপায় হলো কোনো এক সোর্স থেকে হ্যাকারেরা ব্যবহারকারীর ইউজারনেম এবং পাসওয়ার্ড কম্বিনেশনে তথ্য পেয়ে যায় এবং ওই ধরনের একই কম্বিনেশন অন্যান্য ক্ষেত্রে ব্যবহার করে অ্যাক্সেস করার চেষ্টা করে। ধরুন Store A হ্যাক হয়েছে এবং হ্যাকারেরা আপনার ইউজারনেম ও পাসওয়ার্ড পেয়ে গেল। এরপর হ্যাকার হয়তো ওই একই ইউজারনেম ও পাসওয়ার্ড কম্বিনেশন ব্যবহার করে চেষ্টা করতে পারে আপনার ব্যাংকিং সাইটে অথবা গুরুত্বপূর্ণ ই-মেইল সার্ভিসে লগইন করতে। ডমিনো ইফেক্ট থেকে ডাটা ব্যত্যয় প্রতিরোধে একক সেরা উপায় হলো আপনার প্রতিটি সিঙ্গেল অনলাইন অ্যাকাউন্টের জন্য একটি ইউনিক পাসওয়ার্ড ব্যবহার করা।

সুতরাং, এ জন্য একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করুন। প্রতিটি অ্যাকাউন্টের জন্য একটি ইউনিক ও শক্তিশালী পাসওয়ার্ড তৈরি করা তেমন কোনো কঠিন কাজ নয়, যেকোনো ব্যবহারকারী এটি অনায়াসে করতে পারবেন। তবে, ঠিক কোন ধরনের কাজ করার জন্য আপনার পাসওয়ার্ড ম্যানেজারকে ডিজাইন করা হয়েছে তা জেনে নেয়া উচিত। কয়েকটি খুব ভালো পাসওয়ার্ড ম্যানেজার আছে, যেগুলো ফ্রি হলেও চমৎকার কাজ করে। এগুলো চালু হতে কিছু সময় নেয়।

যখন একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করবেন, তখন শুধু পাসওয়ার্ড মনে রাখতে হবে, যা নিজেই পাসওয়ার্ড ম্যানেজার লক করবে। পাসওয়ার্ড ম্যানেজার টিপিক্যালি অনলাইন অ্যাকাউন্টে স্বয়ংক্রিয়ভাবে আপনাকে লগ করে (অবশ্যই পাসওযার্ড ম্যানেজার আনলক করার পর)। এর অর্থ হচ্ছে শুধু আপনাকে নিরাপদ রাখাই নয়, বরং সম্প্রসারিত করে আপনার দক্ষতা ও উৎপাদনশীলতা। কেননা, আপনার লগইন আর টাইপ করতে হবে না।

ভিপিএন ব্যবহার

একটি ওয়াইফাই নেটওয়ার্ক ব্যবহার করে আপনি যেকোনো সময় ইন্টারনেটে যুক্ত হতে পারবেন, যা হয়তো আপনি জানেন না। আপনার জন্য উচিত হবে একটি ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) ব্যবহার করা।

ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ইন্টারনেটের মাধ্যমে ইউজার এবং ডাটা অথবা ওয়েবসাইটের মাঝে একটি নিরাপদ কানেকশন প্রদান করে, যেখানে তারা যুক্ত থাকে এবং ওই কানেকশন জুড়ে ডাটা এক্সচেঞ্জ এনক্রিপ্ট করে। এটি হচ্ছে ভিপিএনের সবচেয়ে সংক্ষিপ্ত ব্যাখ্যা।

ধরুন, আপনি একটি কফি শপে গেলেন এবং যুক্ত হলেন একটি ফ্রি ওয়াইফাই নেটওয়ার্কের সাথে। আপনি এ কানেকশনের সিকিউরিটি সম্পর্কে কিছুই জানে না। এখানে নেটওয়ার্কে অন্য কেউ থাকতে পারে আপনার অজান্তে, যারা আপনার ওপর নজর রাখতে পারে, ফাইল চুরি করতে পারে এবং আপনার ল্যাপটপ বা মোবাইল ডিভাইস থেকে ডাটা সেন্ড করতে পারে। বেশ কিছু চমৎকার ফ্রি ভিপিএন সার্ভিস আছে, যেগুলোর মধ্য থেকে একটি ব্যবহার করতে পারেন।

টু-ফ্যাক্টর অথেনটিকেশন সক্রিয় করা

টু-ফ্যাক্টর অথেনটিকেশন অনেকটাই খুব বিরক্তি কর হলেও এটি আপনার অ্যাকাউন্টকে অবশ্যই অধিকতর নিরাপদ রাখবে। টু-ফ্যাক্টর অথেনটিকেশনের অর্থ হচ্ছে ইউজার অ্যাকাউন্টে ঢোকার জন্য ইউজার নেম ও পাসওয়ার্ড ছাড়া নিরাপত্তার আরেকটি লেয়ার অতিক্রম করতে হয়। যদি একটি অ্যাকাউন্টে ডাটা অথবা পার্সোনাল ইনফরমেশন সংবেদনশীল অথবা মূল্যবান হয় এবং অ্যাকাউন্ট অফার করে টু-ফ্যাক্টর অথেনটিকেশন, তাহলে এটি এনাবল করতে পারেন। জি-মেইল, এভারনোট ও ড্রপবক্স হলো অনলাইন সার্ভিসের কয়েকটি উদাহরণ, যা অফার করে টু-ফ্যাক্টর অথেনটিকেশন।

আরেকটি ফ্যাক্টরের মাধ্যমে টু-ফ্যাক্টর অথেনটিকেশন আপনার আইডেন্টিটি ভেরিফাই করে, যা টিপিক্যালি নিচের তিনটি জিনিসের মধ্যে একটি something you are, something you own অথবা something you know। something you 'are' অপশনটি সম্পন্ন করা যায় আঙুলের ছাপ অথবা আইরিস স্ক্যানের ম্যাধ্যম। something you own অপশনটি হতে পারে আপনার মোবাইল ফোন ও ফোন নম্বর। এ ক্ষেত্রে ফোনে এন্টার করার জন্য বিশেষ কোডসহ একটি টেক্সট মেসেজ পাবেন। Something you know অপশনটি হতে পারে আরেকটি পাসওয়ার্ড।

যদি আপনার অ্যাকাউন্টে কেউ লগ করার চেষ্টা করে, তাহলে টেক্সট মেসেজ এনাবল করার মাধ্যমে পাবেন টু-ফ্যাক্টর অথেনটিকেশন। যখনই কেউ আপনার অ্যাকাউন্টে লগইন করার চেষ্টা করে, তখনই একটি টেক্সট মেসেজ পাবেন।

পাসকোড ব্যবহার করা

পাসকোড লক অ্যাপ্লাই করুন যেখানেই অফার করে, এমনকি যদি এটি অপশনাল হয়। সিকিউরিটি বিশেষজ্ঞদের মতে, এ বিষয়টি স্মার্টফোন ও ট্যাবলেটের জন্য খুবই গুরুত্বপূর্ণ।

পাসকোড এন্টার করা

বিশেষজ্ঞদের মতে, ব্যবহারকারীর উচিত চার ডিজিট পিনের পরিবর্তে পাসকোড ব্যবহার করা। ব্যবহার করুন একটি ফিঙ্গারপ্রিন্ট আইডি অথবা আরেকটি বায়োমেট্রিক লক যদি সম্ভব হয়। লক্ষণীয়, যখন আপনি Touch ID ব্যবহার করবেন, তখন পাসকোডে লগইন করার জন্য ব্যাকআপ অপশন পাবেন। এটিকে শক্তিশালী করুন, যেহেতু সচরাচর আপনাকে তা ব্যবহার করতে হবে। তবে যাই হোক, চার ডিজিট পিন এড়িয়ে চলুন। আইওএস (iOS) ডিভাইসের ক্ষেত্রে নেভিগেট করুন Settings → Passcode এবং Simple Passcode সুইচ অফ করুন।

ডিসপোজ্যাবল ক্রেডিট কার্ড নাম্বার

ক্রেডিট কার্ড সিস্টেম ব্যবহার এখন সেকেলের হয়ে গেছে এবং যা ব্যবহার করা মোটেও নিরাপদ নয়। এটি আপনার ভুল না হলেও এখানে কিছু করার আছে আপনার জন্য। এজন্য ব্যবহার করুন ডিসপোজ্যাবল ক্রেডিট কার্ড নাম্বার। আরেকভাবে বলা যায়, আপনার থাকবে রেগুলার ক্রেডিট কার্ড অ্যাকাউন্ট। তবে যেকোনো সময় একটি নতুন ১৬ ডিজিট ক্রেডিট কার্ড নাম্বার ব্যবহার করতে হতে পারে।

সিকিউরিটি টেক জার্নালিস্ট এবং অন্যান্য বিশেষজ্ঞের মতে, কিছু কিছু ব্যাংক যেমন– সিটি মাস্টারকার্ড অফার করে ওয়ানটাইম ইউজ ক্রেডিট কার্ড। ব্যাংক অব আমেরিকার রয়েছে ShopSafe নামে একই ধরনের এক প্রোগ্রাম, যা একইভাবে কাজ করে। এ ক্ষেত্রে আপনার অ্যাকাউন্টে লগ করলে যেমন জেনারেট করবে একটি ১৬ ডিজিট নাম্বার, তেমনই জেনারেট করবে একটি সিকিউরিটি কোড এবং 'on-card' এক্সপায়ইরি ডেট। এরপর কখন সব ডিজিট এক্সপায়ার করবে তার সময় সেট করতে পারেন। যখন অনলাইনে কেনাকাটা করবেন, তখন আপনার প্রকৃত ক্রেডিট কার্ডের জায়গায় ব্যবহার করুন এক নতুন অস্থায়ী নাম্বার। এরপর চার্জ চলে যাবে আপনার রেগুলার অ্যাকাউন্টে। অস্থায়ী কার্ড নাম্বার আর কাজ করবে না ডেট এক্সপায়ার হওয়ার পর।

সুতরাং পরবর্তী সময়ে আপনার ক্রেডিট কার্ড কোম্পানি অথবা ব্যাংক আপনাকে ডাকবে আপগ্রেড ক্রেডিট কার্ড বিক্রি করার জন্য চেষ্টা করতে। এ অবস্থায় তাদের কাছে দাবি করেন, ওয়ান টাইম ইউজ কার্ড এবং অন্যান্য একই ধরনের সার্ভিস। যদি আপনার এ লেভেলের প্রোটেকশন অফার না করে, তাহলে অন্য কোথাও থেকে সেগুলো পেতে পারেন।

বিভিন্ন অ্যাকাউন্টে ভিন্ন ই-মেইল অ্যাড্রেস ব্যবহার

এমন অনেক ব্যবহারকারী আছেন, যারা খুবই অর্গানাইজড এবং মেথোডিক্যাল, তারা তাদের তথ্যের নিরাপত্তার ব্যাপারে প্রচণ্ড সচেতন এবং বিভিন্ন উদ্দেশ্যে ব্যবহার করে থাকেন বিভিন্ন ই-মেইল অ্যাড্রেস। যারা অভিজ্ঞ এবং সিকিউরিটির ব্যাপারে সচেতন, তারা তাদের বিভিন্ন ধরনের অনলাইন অ্যাক্টিভিটির জন্য বিভিন্ন ধরনের অ্যাড্রেস ব্যবহার করে থাকেন। এর মূল কারণ সংশ্লিষ্ট অনলাইন আইডেন্টিটিগুলো আলাদা করে রাখা।

ব্রাউজিং ডাটা পরিষ্কার করা

পাসওয়ার্ড ম্যানেজার অপশন

ক্যাশ ক্লিয়ার করা

ব্রাউজারের ক্যাশ আপনার সম্পর্কে কতটুকু জানে, সে ব্যাপারে কখনও তুচ্ছ করা উচিত নয়। সেভ করা কুকিজ, সেভ করা সার্চসমূহ ও ওয়েব হিস্ট্রি পয়েন্ট করতে পারে হোম অ্যাড্রেস, পারিবারিক তথ্য এবং অন্যান্য পার্সোনাল ডাটাকে।

এসব তথ্যকে ভালোভাবে প্রোটেক্ট করার জন্য যা আপনার ওয়েব হিস্ট্রিতে ওঁৎ পেতে থাকে। ব্রাউজার কুকিজ ডিলিট করেছেন কিনা তা নিশ্চিত করুন ও নিয়মিতভাবে ব্রাউজার হিস্ট্রি ক্লিয়ার করুন। কিছু কিছু টিউনআপ ইউটিলিটির সেটিং থাকে এমনভাবে, যা স্বয়ংক্রিয়ভাবে সেভ করা ব্রাউজার ডাটা পরিষ্কার করে ও আপনি সচরাচর তা পছন্দ করেন।

এসব তথ্য হয়তো ভালোভাবে সুরক্ষার জন্য ব্যবহারকারীর ওয়েব হিস্ট্রিতে লুকিয়ে থাকতে পারে। সুতরাং ব্রাউজার কুকিজ ডিলিট করা ও নিয়মিতভাবে ব্রাউজার হিস্ট্রি ক্লিয়ার করার ব্যাপারে নিশ্চিত থাকুন। তবে বাস্তবতা হলো, বেশিরভাগ ব্যবহারকারী এ কাজটি নিয়মিতভাবে করেন না। কিছু টিউনআপ ইউটিলিটি আছে, যেগুলো স্বয়ংক্রিয়ভাবে ব্রাউজার ডাটা ক্লিয়ার করার জন্য সেট করা থাকে, যা আপনি পছন্দ করতে পারেন।

ব্রাউজারের 'সেভ পাসওয়ার্ড' ফিচার বন্ধ রাখা

বলা হয়, ব্রাউজার আপনার অনলাইন অ্যাক্টিভিটি সম্পর্কে তথ্য ধারণ করে, অর্থাৎ আপনার সম্পর্কে জানে। তাই অনেক ব্রাউজার দেয় পাওয়ার্ড ম্যানেজমেন্ট সলিউশন। তবে বিশেষজ্ঞদের পরামর্শ, এগুলো ব্যবহার না করাই ভালো। সবচেয়ে ভালো হয় অভিজ্ঞদের ওপর পাসওয়ার্ড প্রোটেকশনের দায়িত্ব অর্পণ করা, যে পাসওয়ার্ড ম্যানেজার তৈরি করেন।

বিস্ময়কর হলো, ব্রাউজার বাইডিফল্ট এখনও আপনার ওয়েব পাসওয়ার্ড সেভ করার জন্য প্রম্পট করবে। এটি বন্ধ রাখুন। যদি পাসওয়ার্ড ম্যানেজার ব্যবহার করে থাকেন, তাহলে এটি আপনার জন্য দরকার হবে না। ব্রাউজারে আপনার পাসওয়ার্ড সেভ না করাটা হবে অধিকতর নিরাপদ। বিশেষজ্ঞদের অভিমত, যখন পাসওয়ার্ড ম্যানেজার ইনস্টল করা হয়, তখন এটি টিপিক্যালি অফার করে পাসওয়ার্ড ইম্পোর্ট করার জন্য, যা অনিরাপদভাবে স্টোর হয় ব্রাউজারে। যদি পাসওয়ার্ড ম্যানেজার এটি করতে পারে, তাহলে নিশ্চিত থাকতে পারেন যে, কিছু ম্যালওয়্যার সফটওয়্যার ওই একই কাজ করতে পারবে।

ফাঁদে পা না দেয়া

বর্তমান তথ্যপ্রযুক্তির অবস্থার পরিপ্রেক্ষিতে বিশেষজ্ঞেরা মনে করেন, আপনি যা-ই ক্লিক করুন না কেন, এখন অনলাইনে নিরাপদ থাকা জীবনেরই একটি অংশ হয়ে উঠেছে। এটি অন্তর্ভুক্ত করতে পারে ই-মেইলের লিঙ্ক, ম্যাসেজিং অ্যাপস ও ফেসবুক। ফিশিং লিঙ্কস স্বয়ংক্রিয়ভাবে আপনার ডিভাইস ম্যালওয়্যার ডাউনলোড ও সংক্রমণের কারণ হয়ে দাঁড়াতে পারে।

সুতরাং, কোনো ব্যবহারকারীরই উচিত হবে না অপরিচিত বা অজানা কোনো লিঙ্কে বা টেক্সট ম্যাসেজে ক্লিক করা। সোশ্যাল মিডিয়া সাইটের ক্ষেত্রেও একই ধরনের ব্যাপার ঘটতে পারে।

আপনার ইনস্টল করা সিকিউরিটি টুলস এক্সপ্লোর করা

বেশ কিছু চমৎকার অ্যাপস ও সেটিং আছে, যেগুলো সহায়তা করে আপনার ডিভাইস ও আইডেন্টিটি রক্ষা করতে। তবে এগুলো তখনই খুব মূল্যবান হয়ে উঠবে, যখন যথাযথভাবে ব্যবহার করতে পারবেন। বিশেষজ্ঞদের অভিমত, বিপুলসংখ্যক ব্যবহারকারী সুইচ করেন Find My iPhone অথবা ইনস্টল করেন সিকিউরিটি সফটওয়্যার এবং এরপর কখনই সেটিংস এক্সপ্লোর করেন না অথবা সার্ভিস কেমন করে কাজ করছে, তা পরীক্ষা করে দেখেন না কজ

ফিডব্যাক : mahmood_sw@yahoo.com