ওয়াই-ফাই জোন ব্যবহারে সতর্কতা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

প্রযুক্তির অগ্রগতির সাথে সাথে বাড়ছে ওয়াই-ফাইয়ের ব্যবহার। একই সাথে বাড়ছে হ্যাকার তথা সাইবার অপরাধীদের দৌরাত্ম্য। ম্যালওয়্যার বা ভাইরাসের মাধ্যমে সাধারণ ব্যবহারকারীদের ডিভাইসের দখল নিতে অথবা ব্যক্তিগত তথ্য চুরি করতে হ্যাকারেরা অহরহ ব্যবহার করছে ওয়াই-ফাই সংযোগ। এ অবস্থায় ওয়াই-ফাই নেটওয়ার্কে নিজের ডিভাইস আর ব্যক্তিগত তথ্যের নিরাপত্তা নিশ্চিত করতে নিচে বর্ণিত অভ্যাসগুলো গড়ে তুলুন।

বিরত থাকুন শেয়ারিং থেকে

মিউজিক লাইব্রেরি, প্রিন্টার্স, ফাইলস ইত্যাদি সাধারণ ব্যবহারকারীদের ওয়াই-ফাই জোনে শেয়ার না করাই ভালো। উইন্ডোজ পিসির ক্ষেত্রে অ্যাডভান্সড শেয়ারিং সেটিংস থেকে ওয়াই-ফাই শেয়ারিং বন্ধ করা যায়। ম্যাক পিসির ক্ষেত্রে সিস্টেম প্রেফারেন্স থেকে শেয়ারিং বন্ধ করা যায়। শেয়ারিং চালু করার জন্য উইন্ডোজ পিসিতে অ্যাডভান্সড শেয়ারিং সেটিংস থেকে কন্ট্রোল প্যানেলের নেটওয়ার্ক ও ইন্টারনেট সেটিংসের হোমগ্রুপ ওপেন করতে হবে, যার ফলে কমপিউটারের ফাইল ও প্রিন্টার শেয়ারিং একই নেটওয়ার্ক ব্যবহারীর কাছে দৃশ্যমান হবে। ম্যাক পিসির ক্ষেত্রে সিস্টেম প্রেফারেন্স থেকে শেয়ারিং সিলেক্ট করতে হবে।

বন্ধ রাখুন স্বয়ংক্রিয় ওয়াই-ফাই সংযোগ

স্মার্টফোন বা ট্যাবলেট কমপিউটারে স্বয়ংক্রিয় ওয়াই-ফাই সংযোগ চালু থাকলে ব্যবহারকারীদের অজান্তেই ডিভাইসটি সংযোগ পেয়ে যেতে পারে বিভিন্ন ব্যবহারকারীর ওয়াই-ফাই সিস্টেমে। এতে ম্যালওয়্যার বা ভাইরাস সংক্রমণের আশঙ্কা বেড়ে যায় অনেক। এমনকি ব্যবহারকারীর অজান্তেই সম্পূর্ণ ডিভাইসের দখল নিয়ে নিতে পারে হ্যাকারেরা। এ ক্ষেত্রে নিজের ডিভাইস আর ব্যক্তিগত তথ্যের নিরাপত্তা নিশ্চিত করতে স্মার্টফোন, ট্যাবলেট ইত্যাদিতে স্বয়ংক্রিয় ওয়াই-ফাই সংযোগ বন্ধ রাখাই নিরাপদ।

বেশিরভাগ আধুনিক স্মার্টফোনে এ অপশনটি বন্ধ থাকে। যেসব ওয়াই-ফাই ডিভাইসে এটি থাকে না, সেসব ডিভাইসের ওয়াই-ফাই সেটিং থেকে অটো কানেক্টিং বন্ধ করা যায়। যদি সেটিং অ্যাপে ওয়াই-ফাই বন্ধ করার কোনো অপশন না থাকে, তবে এর মানে হচ্ছে আগে থেকেই বন্ধ রয়েছে ওয়াই-ফাই স্বয়ংক্রিয় সংযোগ।

এইচটিটিপিএস ব্যবহার করুন

বেশিরভাগ ওয়েবসাইট ডাটা ট্রান্সফার করে একেবারেই সোজা টেক্সট হিসেবে। এর ফলে কেউ যদি ব্যবহারকারীর নেটওয়ার্ক সংযোগটি হ্যাক করতে সমর্থ হয়, তবে ওয়েবসাইটের টেক্সট ব্যবহার করেই তথ্য চুরি করতে এবং ডিভাইসটির ক্ষতি করতে পারবে হ্যাকারেরা। কিছু ওয়েবসাইট ডাটা নিরাপত্তা নিশ্চিত করতে এইচটিটিপিএস (https://) এক্সটেনশন ব্যবহার করে ডাটা এনক্রিপ্ট করে ট্রান্সফারের মাধ্যমে। এইচটিটিপিএস প্লাগ-ইন ব্যবহার করে এ কাজটি ব্যবহারকারী নিজেও করতে পারেন। এইচটিটিপিএস এক্সটেনশন ব্যবহার করলে ইন্টারনেট সংযোগ হ্যাক হলেও নিরাপদ থাকবে ব্যক্তিগত ডাটা।

দ্বৈত অথেনটিকেশন

টু ফ্যাক্টর অথেনটিকেশন বা দ্বৈত পরিচয় নিশ্চিত করার অর্থ যেকোনো অ্যাকাউন্টে ঢুকতে দুটি ভিন্ন উপায় ব্যবহার করা। উদাহরণস্বরূপ, এর একটি হতে পারে যা ব্যবহারকারীর কাছে থাকা পাসওয়ার্ড। আর দ্বিতীয়টি হতে পারে এসএমএসের মাধ্যমে সেলফোনে পাঠানো একটি গোপন কোড।

এ ব্যবস্থার সুবিধাটি হলো, হ্যাকার ওয়াই-ফাই

সংযোগ করে আপনার পাসওয়ার্ড চুরি করলেও মোবাইল কোডটির কারণে অনুপ্রবেশ করতে পারবে না অ্যাকাউন্টে। জি-মেইলে দুই ধাপের অথেনটিকেশন সুবিধা পেতে জি-মেইল অ্যাকাউন্টে লগ-ইন করে যেতে হবে সেটিংস অপশনে। সেখান থেকে আদার গুগল অ্যাকাউন্ট সেটিংস থেকে চালু করা যাবে টু ফ্যাক্টর অথেনটিকেশন সুবিধা।

নিজের ফোন নাম্বারটি দিতে হবে গুগলকে, আর ঠিক করতে হবে লগ-ইন করার সময় আপনি গুগলের কাছ থেকে টেক্সট মেসেজ চান নাকি ফোন কল। এরপর গুগল আপনার মোবাইলে পাঠিয়ে দেবে ৬ ডিজিটের একটি কোড। কোডটি চাপলেই চালু হয়ে যাবে আপনার অ্যাকাউন্টের টু ফ্যাক্টর অথেনটিকেশন। এরপর প্রতিবার নতুন কোনো কমপিউটার থেকে গুগল অ্যাকাউন্টে ঢুকতে গেলেই পাসওয়ার্ড এবং গোপন কোড দুটি ব্যবহার করে নিশ্চিত করতে হবে আপনার পরিচয়।

এড়িয়ে চলুন অপরিচিত ওয়াই-ফাই নেটওয়ার্ক

অপরিচিত কোনো ওয়াই-ফাই সংযোগ ব্যবহারের আগে নিশ্চিত হোন ওয়াই-ফাই সংযোগটি নিরাপদ কি না। হ্যাকারেরা ব্যবহারকারীদের ডিভাইস দখলের উদ্দেশ্যে সহজেই চালু করতে পারে ভুয়া নামের ওয়াই-ফাই নেটওয়ার্ক। এসব ক্ষেত্রে অপরিচিত নামের ওয়াই-ফাই সংযোগ এড়িয়ে চলাই নিরাপদ। অপরিচিত কোনো ওয়াই-ফাই জোনে থাকলে ব্যবহারের আগে দায়িত্ববান কাউকে জিজ্ঞেস করে নিন সংযোগটির ব্যাপারে।

ব্যবহার করুন পাসওয়ার্ড ম্যানেজার

একই পাসওয়ার্ড একাধিক অ্যাকাউন্টে ব্যবহার করলে পাসওয়ার্ড ফাঁস হয়ে বেহাত হতে পারে সব অ্যাকাউন্ট। এজন্য আলাদা অ্যাকাউন্টের জন্য ব্যবহার করুন আলাদা পাসওয়ার্ড। একাধিক পাসওয়ার্ড মনে রাখা একটু ঝামেলার। এজন্য ব্যবহার করা যেতে পারে কিপাস বা লাস্টপাসের মতো বিনামূল্যের পাসওয়ার্ড ম্যানেজার। কিপাস ব্যবহারকারীর কমপিউটারে একটি এনক্রিপ্টেড ডাটাবেজ ফাইল রাখে, আর লাস্টপাস তথ্য জমা করে ক্লাউড স্টোরেজে। দুটি ম্যানেজার ব্যবহারেরই ইতিবাচক ও নেতিবাচক দিক আছে। তবে দুটি সেবাই নিরাপদ।

চালু রাখুন ফায়ারওয়াল

বেশিরভাগ অপারেটিং সিস্টেমেই ইনকামিং ও আউটগোয়িং সংযোগে নজর রাখে ফায়ারওয়াল। ফায়ারওয়াল সম্পূর্ণ নিরাপত্তা দিতে না পারলেও এটি সবসময় চালু রাখা প্রয়োজন।

উইন্ডোজ ডিভাইসের ক্ষেত্রে ফায়ারওয়াল সেটিংগুলো থাকে কন্ট্রোল প্যানেলের সিস্টেম অ্যান্ড সিকিউরিটি অপশনে। সেখানে উইন্ডোজ ফায়ারওয়ালে ক্লিক করে চালু করে দিন উইন্ডোজ ফায়ারওয়াল।

ব্যবহার করুন অ্যান্টিভাইরাস

সবসময় ব্যবহার করুন অ্যান্টিভাইরাস সফটওয়্যার। এটি নিয়মিত আপডেট করতেও ভুলবেন না। আপনার নেটওয়ার্ক সিস্টেম অথবা ডিভাইসে কোনো ক্ষতিকর কনটেন্ট, ম্যালওয়্যার বা ভাইরাস অনুপ্রবেশ করলে তা অ্যান্টিভাইরাস সফটওয়্যার দিয়ে সারিয়ে নিন।

ব্যবহার করুন ভিপিএন

পাবলিক হট স্পট থেকে কোনো সেনসেটিভ নেটওয়ার্ক যেমন নিজের অফিস বা হোম নেটওয়ার্ক অ্যাক্সেস করার সময় ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ব্যবহার করুন। এতে আপনার সব কমিউনিশেন এনক্রিপটেডভাবে আদান-প্রদান হবে। ফলে কেউ আপনার ডাটা ইন্টারসেপ্ট করতে পারলেও তার মর্ম উদ্ধার করতে পারবে না।

পাসওয়ার্ড রিসেট করুন

কোনো কারণে যদি পাবলিক নেটওয়ার্ক ব্যবহার করতে হয়, তবে যত দ্রুত সম্ভব সিকিউরড নেটওয়ার্ক থেকে আপনার পাসওয়ার্ডটি রিসেট করে নিন।

এখন জেনে নেয়া যাক যদি নতুন কোনো ওয়াই-ফাই নেটওয়ার্ক কনফিগার করেন, তবে কী কী নিরাপত্তা ব্যবস্থা নেয়া প্রয়োজন।

নতুন নেটওয়ার্ক কনফিগারেশন

- ডিফল্ট নেটওয়ার্ক নেম (SSID) পরিবর্তন করুন।
- কন্ট্রোল প্যানেলের ডিফল্ট ইউজার নেম ও পাসওয়ার্ড পরিবর্তন করুন।
- WPA2-Personal (aka WPA2-PSK) with AES encryption এনাবল করুন।
- ক্লায়েন্ট মেশিনে WPA2 security features এনাবল করুন।
- Network passphrase এমনভাবে তৈরি করুন যাতে তা রেকমেন্ডেড গাইডলাইন মেনে চলে। সহজ ভাষায় কঠিন পাসফেস ব্যবহার করুন কজ

ফিডব্যাক : jabedmorshed@yahoo.com