অথেনটিকেশন নিরাপত্তা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

সম্প্রতি এক গবেষণায় দেখা গেছে, প্রতিদিন প্রায় ৬ লাখ ফেসবুক অ্যাকাউন্ট হ্যাক হচ্ছে। রিপোর্টটি আরও জানায়, প্রতিদিন প্রায় ১০ কোটি লগইন ফেসবুকে করা হয়, যার মধ্যে ০.০৬ শতাংশ ক্ষেত্রে লগইন কম্প্রোমাইজের ঘটনা ঘটে। জি-মেইল, ইয়াহুসহ সব ওয়েবভিত্তিক ই-মেইল সার্ভিসের ক্ষেত্রেও এই ধরনের প্রচুর হ্যাকিংয়ের বা কম্প্রোমাইজের ঘটনা ঘটে। এ লেখায় আলোচনা করা হয়েছে কীভাবে আমরা আমাদের এসব অ্যাকাউন্টের নিরাপত্তা বলয় আরও শক্তিশালী করতে পারি।

ফেসবুক নিরাপত্তা

যখন আমরা কোনো ওয়েবসাইট ভিজিট করি, তা সাধারণত http প্রটোকলের মাধ্যমে হয়ে থাকে। যাদের কাছে http প্রটোকল শব্দটি অপরিচিত মনে হচ্ছে, তাদের জন্য বলি– http প্রটোকলে আমাদের সব তথ্য নরমাল টেক্সট হিসেবে বিনিময় হয় ইন্টারনেটের মাধ্যমে। ফলে যেকেউ আমাদের তথ্য ইচ্ছে করলে ইন্টারসেপ্ট করে পড়তে পারবে। তাই নিরাপত্তা বিশেষজ্ঞরা, গুরুত্বপূর্ণ ও গোপনীয় তথ্য এনক্রিপটেডভাবে পাঠানোর পরামর্শ দেন। এনক্রিপটেড তথ্য কেউ যদি ইন্টারসেপ্ট করতেও পারে, তবুও সে সেখান থেকে মূল বা আসল তথ্যটি বের করতে পারবে না। সাধারণত ই-কমার্স, অনলাইন ব্যাংকিং ও ইউজার অথেনটিকেশনের জন্য এনক্রিপটেড পদ্ধতি ব্যবহার করা হয়। ওয়েবের তথ্যকে এনক্রিপটেডভাবে পাঠানোর জন্য https প্রটোকল ব্যবহার করা হয়। সুতরাং বোঝা যাচ্ছে, নরমাল http প্রটোকলের মাধ্যমে ফেসবুক ব্যবহার করলে যেকেউ বিভিন্ন হ্যাকিং টুল (বার্প সুইট) বা নেটওয়ার্ক মনিটরিং টুল (ওয়্যার শার্ক) দিয়ে আমাদের ইউজার নেম ও পাসওয়ার্ড হাতিয়ে নিতে পারে।

প্রতিকার : ফেসবুক সিকিউর ব্রাউজিং

এজন্য আমাদের ফেসবুকের https ব্রাউজিং এনাবল করতে হবে। নিচে এর ধাপগুলো আলোচনা করা হলো–

০১. প্রথমে অ্যাকাউন্ট সেটিংসে যেতে হবে।

০২. ডান পাশে সিকিউরিটি অপশনে ক্লিক করতে হবে।

০৩. সিকিউর ব্রাউজিংয়ে 'Browse Facebook on a secure connection (https) when possible' ক্লিক করে সেভ চেঞ্জেসে ক্লিক করতে হবে।

০৪. সিকিউরড ব্রাউজিং এনাবলের আগে।

০৫. সিকিউরড ব্রাউজিং এনাবলের পরে।

মোবাইল সিকিউরিটি কোড

আপনার ফেসবুক অ্যাকাউন্টটি মোবাইল সিকিউরিটি কোডের (লগইন অ্যাপরোভাল) মাধ্যমে আরও নিরাপদ করতে পারেন। এই পদ্ধতিতে যখনই কেউ আপনার অ্যাকাউন্টে অন্য কোনো (আননোন) কমপিউটার থেকে অ্যাকসেস করতে চাইবে, সে আপনার মোবাইলে একটি সিকিউরিটি কোড পাঠাবে এবং ওই কোডটি তাকে লগইনের সময় ব্যবহার করতে হবে। যেহেতু মোবাইল ফোনটি আপনার কাছে থাকবে, তাই সহজে কেউ আপনার কাছ থেকে কোডটি চুরি করতে পারবে না। সুতরাং, আপনার পাসওয়ার্ডটি চুরি হয়ে গেলেও অ্যাকাউন্টটি থাকবে নিরাপদ। এ ক্ষেত্রে বলা যায়, সিকিউরিটি কোডটি তখনই চাইবে, যখন কেউ অন্য কোনো কমপিউটার থেকে ফেসবুকে লগইন করার সময় সঠিক ইউজার নেম ও পাসওয়ার্ড দিতে পারবে। সুতরাং, এখন একজন হ্যাকারকে প্রথমে ব্যবহারকারীর ইউজার নেম ও পাসওয়ার্ড চুরি করতে হবে। তারপর তার ফোনটিও চুরি করতে হবে।

মোবাইল সিকিউরিটি কোড এনাবল করতে

০১. আগের মতোই অ্যাকাউন্ট সেটিংয়ে যেতে হবে। তারপর সিকিউরিটি অপশনে।

০২. এরপর লগইন অ্যাপরোভালসে ক্লিক করতে হবে।

০৩. এরপর সেটআপে ক্লিক করলে স্ক্রিনে আপনার কাছে মোবাইল নম্বর চাইবে। আপনি যে নম্বরটি দেবেন সেই নম্বরে একটি গোপন নিরাপত্তা কোড এসএমএসের মাধ্যমে মোবাইলে চলে যাবে।

০৪. এখন আপনাকে মোবাইলের এসএমএসে আসা নিরাপত্তা কোডটি দিতে হবে।

০৫. পরে যখনই আপনি বা অন্য কেউ নিজের কমপিউটার ছাড়া অন্য কোনো কমপিউটার বা ডিভাইস দিয়ে ফেসবুকে লগইন করতে যাবেন, তখনই আপনার কাছে নিরাপত্তা কোডটি এসএমএসের মাধ্যমে চলে যাবে এবং আপনাকে তা দিয়ে লগইন করতে হবে। বিষয়টি বিরক্তিকর মনে হতে পারে, যদি ব্যবহারকারী একাধিক কমপিউটার বা ডিভাইস ব্যবহার করেন। আপনার ঝামেলা কমাতে পারে রিকগনাইজড ডিভাইস অপশনটি। এর মাধ্যমে আপনি নতুন নতুন ডিভাইসকে ফেসবুকে অ্যাড করে নিতে পারেন। এই অপশনটি প্রথমবার ওই ডিভাইস থেকে ফেসবুকে অ্যাকসেস করার সময়ই পাবেন।

জি-মেইলের নিরাপত্তা

ইদানীং জি-মেইলের পাসওয়ার্ড চুরির ঘটনাও অনেক বেরে গেছে। আপনি মোবাইল ফোনের মাধ্যমে আপনার জি-মেইল অ্যাকাউন্টটির নিরাপত্তা আরও শক্তিশালী করতে পারেন। এজন্য আপনাকে জি-মেইলের টু-ওয়ে ভেরিফিকেশন অপশন ব্যবহার করতে হবে। টু-ওয়ে ভেরিফিকেশন কীভাবে কাজ করে, তা নিচে দেখানো হয়েছে।

যা করতে হবে

০১. প্রোফাইল থেকে অ্যাকাউন্ট সেটিংয়ে যেতে হবে।

০২. ২-স্টেপ ভেরিফিকেশনের এডিট অপশনে ক্লিক করতে হবে।

০৩. আপনার মোবাইলের নম্বর দিতে হবে এবং সেন্ড কোড বাটনে ক্লিক করতে হবে। অবশ্য ভয়েজ কলের মাধ্যমেও কোডটি পেতে পারেন।

০৪. আপনার মোবাইলে পাঠানো সিকিউরিটি কোডটি দিয়ে ভেরিফাই অপশনে ক্লিক করুন। ▶

০৫. এরপর আপনাকে ২-স্টেপ ভেরিফিকেশনটি অন করতে হবে।

এখন কেউ আপনার অ্যাকাউন্টে অবৈধভাবে অ্যাকসেস করতে চাইলে তাকে মোবাইল কোডটি পেতে হবে এবং তা ব্যবহার করতে হবে। যেহেতু কোডটি একবার মাত্র ব্যবহার করা যাবে, সুতরাং কেউ আপনার আগের কোডটি জানতে পারলেও অ্যাকাউন্টটি থাকবে নিরাপদ।

ইয়াহু মেইলের নিরাপত্তা

ই-মেইল অ্যাকাউন্ট নিরাপদ রাখার জন্য ইয়াহু নিয়ে এসেছে ছবি ও টেক্সভিত্তিক ডিভাইস আইডেন্টিফিকেশন। ইয়াহুর এই সার্ভিসটির নাম

Create your sign-in seal। এই সার্ভিসের মাধ্যমে আমরা যে সব কমপিউটার থেকে ইয়াহু অ্যাকাউন্ট অ্যাকসেস করি, সে সব কমপিউটারে নিজেদের সিল তৈরি করতে পারি। ফলে যখনই আমরা ইয়াহুতে লগইন করতে যাব, লগইন পেজে আমাদের ছবি বা নিজের দেয়া টেক্সটি দেখতে পাব। এর মাধ্যমে ইন্টারনেটে পাসওয়ার্ড চুরির অন্যতম পদ্ধতি ফিশিং থেকে নিজেদেরকে নিরাপদ রাখতে পারব।

কীভাবে নিজের সিল তৈরি করবেন

০১. লগইন পেজে Create your sign-in seal লিঙ্কে ক্লিক করুন।

০২. Create a text seal অথবা Upload an image অপশনের মধ্যে যেকোনো একটি বেছে নিন।

০৩. যদি Upload an image অপশনটি বেছে নেন, তাহলে নিজের কমপিউটার থেকে একটি ছবি ব্রাউজ করে নিন।

০৪. এরপর show me preview অপশনে ক্লিক করুন।

০৫. এবার Save This Seal বাটনে ক্লিক করুন।

এখন যখনই কমপিউটার থেকে ইয়াহুতে লগইন পেজে যাবেন, তখন আপনার দেয়া ছবিটি দেখতে পাবেন।

কোনো হ্যাকার যদি আপনার কাছে কোনোভাবে ইয়াহু মেইলের লগইন পেজের মতো একটি নকল পেজ পাঠায়, তাহলে আপনি খুব সহজেই তা ধরে ফেলতে পারবেন। কারণ, তার পাঠানো পেজে সে আপনার সিলটি নকল করতে পারবে না।

উপসংহার

পৃথিবীর কোনো সিস্টেমেই ১০০ শতাংশ নিরাপত্তা দেয়া সম্ভব নয়। এ পদ্ধতিগুলোতে (ফেসবুক ও জি-মেইল) যেহেতু মোবাইল ফোনের ব্যবহার আছে, তাই আমাদের মোবাইল ফোনের নিরাত্তার দিকেও খেয়াল রাখতে হবে। বিশেষ করে মোবাইল হারিয়ে গেলে। তবে মোবাইল হারিয়ে গেলেও আপনি আগের মতোই আপনার অ্যাকাউন্ট অ্যাকসেস করতে পারবেন। তবে সে ক্ষেত্রে নতুন সিম তুলে অথবা নম্বর পরিবর্তন করলে অ্যাকাউন্টে নতুন নম্বরটি সংযোজন করে নিতে হবে।

তবে ওপরের কোনো পদ্ধতিই পাসওয়ার্ডের বিকল্প নয় বরং সহায়ক শক্তি। বলতে পারেন সেকেন্ড লাইন অব ডিফেন্স। শক্ত, অপ্রচলিত এবং অবশ্যই গোপনীয় পাসওয়ার্ডের কোনো বিকল্প নেই কজ

ফিডব্যাক : jabedmorshed@yahoo.com

উইন্ডোজ ১০ নেটওয়ার্কে প্রিন্টার ইনস্টল ও শেয়ার করা

(৬০ পৃষ্ঠার পর)

সিস্টেমে ইনস্টল করা প্রিন্টারের তালিকা এখানে দেখা যাবে

প্রক্রিয়াটি শুরু করার আগে আপনাকে নিশ্চিত করতে হবে নেটওয়ার্কের অন্যান্য কমপিউটারগুলো যেন সৃষ্ট হোমগ্রুপে নিজ নিজ অবস্থান থেকে যুক্ত হয়। এবার ধাপগুলো নিচে দেখানো হলো–

ক. আপনি যখন হোমগ্রুপে যুক্ত হবেন তখন নিশ্চিত হোন Library of folder-এর অধীনে Printers & Devices আইটেমে Permissions অপশনে যেন Shared সিলেক্ট করা থাকে।

খ. এবার পরের স্ক্রিনে হোমগ্রুপ পাসওয়ার্ড এন্ট্রি দিতে হবে।

হোমগ্রুপে অন্যান্য রিসোর্সের মতো প্রিন্টার করা

গ. এখন Windows Explorer-এ গিয়ে Network অপশনে ক্লিক করুন। এখানে আপনি ইনস্টল করা শেয়ারড প্রিন্টারটি দেখতে পাবেন।

শেয়ার করা প্রিন্টারটি নেটওয়ার্কের আওতায় দেখা যাবে

উইন্ডোজ ১০ ভিত্তিক নেটওয়ার্কে একটি প্রিন্টার ইনস্টল ও তা শেয়ার করা সহজ একটি প্রক্রিয়া, যা এখানে বর্ণনা করা হয়েছে। তবে যে বিষয়টি এখানে মনে রাখতে হবে, তাহলো প্রিন্টারের জন্য যথাযথ ড্রাইভার ইনস্টল করা। যদি প্রিন্টারের সাথে ড্রাইভার সিডি আকারে না পেয়ে থাকেন, তাহলে ওই প্রিন্টার নির্মাতার ওয়েবসাইট থেকে সেটি ডাউনলোড করে ইনস্টল করতে হবে কজ

ফিডব্যাক : kazisham@yahoo.com