স্মার্টফোনের নিরাপত্তা কি ঝুঁকির মুখে?

মেহেদী হাসান

একটা সময় ছিল যখন মোবাইল ফোন ছিল শুধুই কথা বলার যন্ত্র। অপর প্রান্তের মানুষের সাথে কথা বলা ছাড়া এর আর কোনো উপযোগিতা ছিল না। বর্তমান দশকে মানুষের এই ধারণা আমূল বদলে গেছে। এখন একটি স্মার্টফোন অনেক ক্ষেত্রেই একটি কমপিউটারের চেয়ে বেশি শক্তিশালী। কীভাবে? স্মার্টফোনের আছে হাজারো কাজের লাখো অ্যাপস। যোগাযোগ রক্ষা, পড়াশোনায় সহায়তা, ব্যক্তিগত সহকারীর ভূমিকা, প্রতিদিনের খাদ্যাভ্যাস নিয়ন্ত্রণ, এমনকি স্বাস্থ্য ঠিক রাখতে অনেক ক্ষেত্রেই চিকিৎসা পরামর্শকের কাজ করে এই অ্যাপগুলো। এছাড়া সবসময় সব কাজে হাতের নাগালে স্মার্টফোন পাওয়া সম্ভব, কমপিউটার নয়। ২০০৭ সালে অ্যাপল তাদের প্রথম স্মার্টফোন 'আইফোন' প্রকাশ করেছিল। প্রযুক্তিবিশ্বে সাড়া ফেলে দেয়া সেই স্মার্টফোনটিই বর্তমানের অ্যাপ্লিকেশন স্টোর বা অ্যাপ স্টোরের সূচনা করে (আগেও অ্যাপ্লিকেশন রিপোজিটরি তৈরি হয়েছিল, তবে বর্তমান ধারার অ্যাপ স্টোর প্রথম চালু করে অ্যাপল)। কিন্তু মজার ব্যাপার, প্রথম আইফোন প্রকাশের সময় এর সাথে অ্যাপ স্টোর হিসেবে কিছু ছিল না। কারণ, সে সময়ের অ্যাপল প্রধান স্টিভ জবস ভেবেছিলেন ইন্টারনেটে চালিত ওয়েব অ্যাপ্লিকেশন ব্যবহারকারীদের চাহিদা মেটাবার জন্য যথেষ্ট। কিন্তু কিছুদিন পর দেখা গেল অ্যাপ নির্মাতারা আইফোনের নিরাপত্তা ভেঙে থার্ড-পার্টি অ্যাপ তৈরি করতে শুরু করেছেন। আইফোনের অপারেটিং সিস্টেম আইওএসের দ্বিতীয় সংস্করণে অবশ্য অ্যাপ স্টোর যোগ করতে ভুল করেননি স্টিভ জবসের প্রতিষ্ঠান। এত দ্রুত তা সাড়া ফেলে যেসব স্মার্টফোন নির্মাতা অ্যাপ্লিকেশন স্টোরের গুরুত্ব বুঝতে শুরু করে। এরপর থেকে স্মার্টফোন আর অ্যাপ পাশাপাশি চলে এসেছে। নতুন অ্যাপ ইনস্টলের সুযোগ ছাড়া এখন কেউ আর স্মার্টফোনের কথা কল্পনাও করতে চান না। অপরদিকে হ্যাকারেরা প্রধানত এই অ্যাপগুলোকে তাদের লক্ষ্যবস্তুতে পরিণত করে। স্মার্টফোন আর অ্যাপের এই অবিচ্ছেদ্য সম্পর্ককে কাজে লাগিয়ে নিরাপত্তার বারোটা বাজাতে চায় তারা। সেদিক থেকে বলতে গেলে অপারেটিং সিস্টেম আর অ্যাপস্টোর যেমন একদিকে স্মার্টফোনকে 'স্মার্টার' করে তুলেছে, তেমনি ঠেলে দিয়েছে ঝুঁকির মুখে। তার মানে এই নয় আমরা অ্যাপ কিংবা স্মার্টফোন ব্যবহার করা ছেড়ে দেব। দুয়ারে নতুন প্রযুক্তি রেখে মুখ ফিরিয়ে রাখার কোনো মানে হয় না। দরকার শুধু সচেতনতা।

যে কারণে স্মার্টফোন হ্যাকারদের অন্যতম লক্ষ্য

এটা স্মার্টফোনের যুগ। এক সময় ঘরে ঘরে টেলিভিশন পৌঁছেছে, এখন হাতে হাতে দেখা যাচ্ছে স্মার্টফোন। সর্বোচ্চ সুবিধা পাওয়ার জন্য ব্যবহারকারীরা সাধারণত সব সময় তাদের স্মার্টফোনটিকে ইন্টারনেটে যুক্ত রাখেন, নোটিফিকেশন পাওয়ার জন্য সামাজিক যোগাযোগ রক্ষার অ্যাপগুলোতে লগআউট না করে চালু রাখেন, ইনবক্সে পৌঁছানো ই-মেইল সাথে সাথে পাওয়ার জন্য সবসময় ই-মেইলে লগইন করে থাকেন এবং কোনো কোনো ক্ষেত্রে ব্যাংকের অফিশিয়াল অ্যাপটিতে লগইন কিংবা কমপক্ষে ব্যবহারকারীর আইডি সংরক্ষণ করে রাখেন। এর সবই কিন্তু বাংলাদেশী ব্যবহারকারীদের ক্ষেত্রে সমানভাবে প্রযোজ্য। দেরিতে হলেও আমাদের দেশে অ্যাপের মাধ্যমে ব্যাংকিং সেবা দেয়া শুরু হয়েছে। আর মূলত এসব কারণেই হ্যাকারেরা স্মার্টফোনগুলোকে লক্ষ্যবস্তুতে পরিণত করে। কারণ, আপনি হয়তো আপনার পার্সোনাল কমপিউটারটিতে গোপন তথ্য, নথিপত্র, ব্যাংক অ্যাকাউন্ট কিংবা পাসওয়ার্ড সংরক্ষণ করে রাখেন। তবে স্মার্টফোনের মতো কমপিউটার সারাদিন চালু থাকে না, সব সময় আপনার সাথে থাকে না, কিংবা স্মার্টফোনের মতো অ্যাপ ইনস্টল করেন না।

স্মার্টফোনের নিরাপত্তা নিয়ে যে কারণে ভাবতে হবে

স্মার্টফোনের নিরাপত্তা নিয়ে সারাবিশ্বেই, বিশেষ করে পশ্চিমা দেশগুলোতে তোলপাড় শুরু ▸

হয়ে গেছে। ফোনে আড়ি পাতার ঘটনা এ ক্ষেত্রে আগুনে ঘি ঢালার কাজটা করেছে। কিছুদিন আগে আইওএসের নিরাপত্তা নিয়ে শঙ্কিত হয়ে পড়েন অনেকেই। তাছাড়া প্রায়ই বিভিন্ন অ্যাকাউন্ট হ্যাক করে ব্যবহারকারীর তথ্য চুরির ঘটনা পত্রিকায় ঘন ঘন দেখা গেছে। সব মিলিয়ে স্মার্টফোনের নিরাপত্তা নিয়ে অনেকেই এখন সোচ্চার। দুঃখের বিষয়, এই সাবধানতার বাণী আমাদের দেশীয় স্মার্টফোন ব্যবহারকারীদের কানে এখনও পৌঁছায়নি। তারা এখনও বিশ্বাস করেন কমপিউটার হ্যাক হতে পারে, ওয়েবসাইট হ্যাক হতে পারে, কিন্তু স্মার্টফোন? অসম্ভব! আমাদের জানা থাকা দরকার, হ্যাকারেরা স্মার্টফোনের তথ্য ব্যবহার করে কী করতে পারে এবং কীভাবে করতে পারে। মোটামুটি আঁতকে ওঠার মতো ব্যাপার। প্রথমেই এরা আপনার স্মার্টফোনের ই-মেইলে লগইন করার তথ্যাদি পেয়ে গেলে আপনার সব অ্যাকাউন্টের পাসওয়ার্ড রিসেট করে নিজের ইচ্ছেমতো পাসওয়ার্ড বসিয়ে লগইন করতে পারবে। কারণ সোশ্যাল নেটওয়ার্ক থেকে শুরু করে ব্যাংক অ্যাকাউন্ট পর্যন্ত, সবকিছু এসে যুক্ত হয়েছে আপনার ই-মেইল অ্যাকাউন্টে। ব্যাংক অ্যাকাউন্টের অ্যাক্সেস পেয়ে গেলে কীভাবে অর্থ আত্মসাৎ করতে পারবে তা আপনাদের জানা থাকার কথা। আপনার বাসার ঠিকানা পেয়ে যাবে ম্যাপস থেকে। ফোন নাম্বারের তালিকা থেকে সবার ফোন নাম্বার পেয়ে যাবে। অ্যাপ কিনতে বা অনুরূপ কাজের জন্য ক্রেডিট কার্ডের নাম্বার প্রবেশ করাতে হয়। একটা উদাহরণ দেয়া যাক। মনে করুন, আপনার গুগল অ্যাকাউন্ট দিয়ে গুগল প্লে স্টোর থেকে প্রয়োজনীয় অ্যাপ কেনেন বা কিনেছিলেন। আপনার সেই গুগল অ্যাকাউন্টের সাথে ক্রেডিট কার্ডের নাম্বার যুক্ত আছে। বারবার ক্রেডিট কার্ডের নাম্বার প্রবেশের বিড়ম্বনা থেকে মুক্তি দেয়ার জন্যই গুগল এই ব্যবস্থা চালু করেছে। এখন আপনার ই-মেইলের অ্যাক্সেস পেয়ে যাওয়া মানে সেই গুগল অ্যাকাউন্ট দিয়ে যত অ্যাপ কেনা হবে তার সবকিছু খরচ হবে আপনার পকেট থেকে।

যেভাবে আপনার স্মার্টফোনের তথ্য চুরি যেতে পারে

এ ক্ষেত্রে প্রথমেই আসবে অ্যাপ্লিকেশনের কথা। দুইভাবে অ্যাপ আপনার নিরাপত্তার ক্ষতি করতে পারে। এক. এমন কোনো অ্যাপ ইনস্টল করলেন, যা আপনার ফোনের তথ্য ডেভেলপারদের কাছে পাচার করে দেবে। কিছু কিছু ক্ষেত্রে অবশ্য এই তথ্যগুলো আরও ভালো সেবা দেয়ার জন্য প্রয়োজন হতে পারে। তবে সবক্ষেত্রেই যে সেই তথ্য ডেভেলপাররা ভালো কাজে ব্যবহার করবেন, এমনটা ভাবার কোনো কারণ নেই। এসব ক্ষেত্রে সেই অ্যাপ তৈরি করাই হয় অসৎ উদ্দেশ্যে। আর দ্বিতীয় ক্ষেত্রে হ্যাকারেরা কোনো অ্যাপের নিরাপত্তা পদ্ধতি নষ্ট করে ব্যবহারকারীর তথ্য চুরি করে। হ্যাকারেরা জানে, নতুন অ্যাপের দুর্বল নিরাপত্তা ব্যবস্থা তারা সহজেই ভেঙে দিয়ে ব্যবহারকারীর তথ্য সংগ্রহ করতে পারবে। সুতরাং তারা সেভাবেই কাজে লেগে পড়ে। অবশ্য এর উল্টোটাও দেখা গেছে। স্ন্যাপচ্যাটের মতো জনপ্রিয় অ্যাপের ৪৬ লাখ ব্যবহারকারীর তথ্য চুরি করার পর তা প্রকাশ করা হয়েছিল। টিন্ডার নামের একটি অ্যাপ ব্যবহারকারীর অবস্থান তৃতীয় পক্ষের কাছে ফাঁস করে দিয়েছে। সম্প্রতি অ্যাপলের আইওএসের নিরাপত্তা নিয়ে শঙ্কায় ছিলেন অনেকেই। অপারেটিং সিস্টেম হালনাগাদ না করে থাকলে এখনও হুমকির মাঝে আছেন। সে ক্ষেত্রে ব্যবহারকারীর ফোনের ব্রাউজার অর্থাৎ সাফারি ও ওয়েবসাইটের সার্ভারের মাঝে দেয়া-নেয়া করার তথ্য তৃতীয় পক্ষের হাতিয়ে নেয়ার সুযোগ ছিল। এমন আরও অনেক উদাহরণ আছে। জনপ্রিয় হলেই যে একটি অ্যাপ 'নিরাপদ' হবে, এমনটিও ভাবার কোনো কারণ নেই।

এছাড়া পাবলিক ওয়াইফাই নেটওয়ার্কে হ্যাকার আপনার স্মার্টফোনটি হ্যাক করে সার্ভার ও ফোনের মাঝে দেয়া-নেয়া করার তথ্য হাতিয়ে নিতে পারে। ধরুন, কোনো ওয়েবসাইট থেকে কোনো পণ্য কিনবেন আপনার ক্রেডিট কার্ড ব্যবহার করে। পাবলিক ওয়াইফাই নেটওয়ার্কে হ্যাকার আপনার ক্রেডিট

সাইবার অপরাধীদের হাত থেকে স্মার্টফোন সুরক্ষায় ৮ টিপস

কেনো মোবাইল ফোনের সুরক্ষা দরকার? কারণটা খুব সহজ। আমাদের ভার্চুয়াল আর বাস্তব জীবন, দুই-ই এখন তথ্যপ্রযুক্তির ওপর নির্ভরশীল। আর আপনার ফোনে যে পরিমাণ তথ্য আছে, তা যদি কারও হাতে পড়ে, তাহলে সেই সাইবার অপরাধী আপনার ভার্চুয়াল জীবনটা দখল করে নিতে পারে অনায়াসে। ফেসবুক, জি-মেইল থেকে শুরু করে সবকিছু দখল করে নিয়ে আপনার জীবনের বারোটা নয়, বরং তেরোটা বাজাতেও পারে।

এই ঘোর কলিকালে কীভাবে নিজের ফোন সুরক্ষিত রাখবেন সাইবার অপরাধীদের হাত থেকে? এ বিষয়ে তুলে ধরা হলো ৮ টিপস। আশা করি সবার তা কাজে লাগবে।

০১. পিন লক সেট করুন। সবচেয়ে সহজ পরামর্শ এটিই। ফোনে একটি 'পিন লক' সেট করে রাখুন। কাজটি খুব সহজ, কিন্তু মাত্র ৬০ শতাংশ স্মার্টফোন ব্যবহারকারী এটি করেন। পিন লক সেট করা থাকলে ফোন চুরি হলেও সহজে সেটি আনলক করে তথ্য চুরি করা যাবে না।

০২. পাবলিক ওপেন ওয়াইফাই নেটওয়ার্কে যুক্ত থাকা অবস্থায় ফেসবুক, জি-মেইল বা ব্যাংকিং জাতীয় কাজ না করাই ভালো। এসব নেটওয়ার্কের সিকিউরিটি অত্যন্ত দুর্বল বা আদৌ নেই।

০৩. ফোন করে যদি কেউ এরকম বলেন, 'আমি আপনার ব্যাংক থেকে বলছি, ক্রেডিট কার্ডে সমস্যা আছে, আপনার নম্বরটা বলুন তো', এসব বিশ্বাস করবেন না। এটি খুব সহজ একটি প্রতারণার কৌশল। বরং ফোন কেটে দিয়ে আপনার ব্যাংকের পরিচিত নম্বরে ফোন করুন। এমনকি ইনকামিং ফোনের নম্বর চিনলেও বিশ্বাস করবেন না। ভুয়া ইনকামিং কলার আইডি বানিয়ে ব্যাংকের বা পরিচিত কারও ফোন সেজে অপরাধীরা ফোন করতে পারে।

০৪. স্মার্টফোন, ফেসবুক বা ই-মেইল স্থায়ীভাবে লগইন করে রাখবেন না। কারণ ফোনটা একবার বেহাত হলেই সর্বনাশ! কষ্ট হলেও বারবার লগইন করুন। কাজ শেষে লগআউট করে দিন।

০৫. ফোন স্লো হয়ে গেছে? দ্রুত ব্যাটারি খরচ হয়ে যাচ্ছে? অনেক সময় ফোনে ম্যালওয়্যার/ভাইরাস আক্রমণ করলে ব্যাকগ্রাউন্ডে চলে, ফলে স্লো হয়ে যায় ফোন কিংবা ব্যাটারির চার্জ দ্রুত খেয়ে ফেলে।

০৬. আপনার দরকারি ও গোপনীয় কাগজপত্রের কপি ফোনে না রাখাই ভালো।

০৭. ফোন ট্র্যাকিং সফটওয়্যার ইনস্টল করে রাখুন। এতে করে ফোনটি হারিয়ে গেলেও ট্র্যাক করতে পারবেন। আবার অনেক সফটওয়্যারে রিমোট ওয়াইপিং করা যায়, ফলে ফোন হারালেও ইন্টারনেটের মাধ্যমে গোপন তথ্যগুলো ডিলিট করে দিতে পারবেন।

০৮. অ্যাপ্লিকেশন ইনস্টল করার সময় খেয়াল রাখুন কোথা থেকে ইনস্টল করছেন। সেটি কী আসলেই গুগল বা অ্যাপলের অ্যাপস্টোর নাকি নকল কোনো সাইট, যা অপরাধীরা বানিয়ে টোপ ফেলেছে?

উপরের পরামর্শগুলা আসলে সামান্যই। স্মার্টফোনে সতর্ক থাকতে হলে আরও অনেক কিছুই করা দরকার। তবে আমার বিশ্বাস, ওই আটটি টিপ মেনে চললে দুর্বৃত্তদের আক্রমণ থেকে অন্তত শতকরা ৯০ ভাগ নিজের ফোন ও নিজের তথ্যকে সুরক্ষিত রাখতে পারবেন।

কার্ড সম্পর্কিত তথ্য চুরি করতে পারে। নিদেনপক্ষে আপনার ফোনটি হারিয়ে যেতে পারে। আর হয়তো এমন কারও হাতে পড়ল যে নিমেষেই আপনার সব ব্যক্তিগত তথ্য হাতিয়ে নেবে। চলতি বছরের জানুয়ারিতে অ্যালকাটেল-লুসেন্টের প্রকাশিত এক প্রতিবেদনে দেখা যায়, মোবাইলে ম্যালওয়্যারের

আক্রমণ ২০১৩ সালে প্রায় ২০ শতাংশ বেড়েছে।

অ্যান্ড্রয়িড অ্যাপ বেশি ঝুঁকিপ্রবণ

বাংলাদেশের নতুন স্মার্টফোন ব্যবহারকারীর বেশিরভাগই অ্যান্ড্রয়িডনির্ভর হ্যান্ডসেট কিনছে। কারণ, অ্যান্ড্রয়িড তুলনামূলকভাবে সহজলভ্য। আইফোন, ব্ল্যাকবেরি কিংবা উইন্ডোজ ফোন-নির্ভর ডিভাইসের উচ্চমূল্য এবং মডেলের স্বল্পতা মানুষকে অ্যান্ড্রয়িডে আগ্রহী করে তুলেছে। এটা অবশ্যই ভালো দিক। তবে বিশেষজ্ঞদের মতে, অ্যান্ড্রয়িডনির্ভর স্মার্টফোন অন্যান্য ফোনের তুলনায় বেশি 'ঝুঁকিপ্রবণ'। মোবাইলে নিরাপত্তা ভঙ্গের প্রায় ৬০ শতাংশ ঘটেছে অ্যান্ড্রয়িডে। অ্যাপলের অ্যাপস্টোরে যেকোনো অ্যাপ যোগ করার আগে অ্যাপল কর্তৃপক্ষ তা পরীক্ষা-নিরীক্ষা করে দেখে সন্তুষ্ট হলে তবেই তা অ্যাপস্টোরে যোগ করে। অ্যান্ড্রয়িডের ক্ষেত্রে এমন বাধা নেই। স্মার্টফোনের মার্কেট দখলে নেয়ার জন্য গুগল তাদের অ্যাপ মার্কেট ডেভেলপারদের জন্য উন্মুক্ত করে দিয়েছে। ফলে অনেক ঝুঁকিপূর্ণ অ্যাপ প্লেস্টোরে প্রতিদিন যোগ হচ্ছে, যা ব্যবহারকারীকে ফেলছে ঝুঁকির মুখে। তবে এই ঝুঁকি কিন্তু গুগলের অ্যাপ মার্কেটের সাথে সম্পর্কিত নয়। অ্যান্ড্রয়িড অপারেটিং সিস্টেম ও প্লেস্টোরের নিরাপত্তা নিয়ে গুগল কর্তৃপক্ষ যথেষ্টই হুশিয়ার এবং এরা এদের দায়িত্ব যথাযথভাবে পালন করে যাচ্ছে। ঝুঁকি মূলত থার্ড-পার্টি অ্যাপগুলোর কারণে ঘটছে এবং এ ব্যাপারে ব্যবহারকারীকেই থাকতে হবে সতর্ক। অন্যান্য অপারেটিং সিস্টেমেও নিরাপত্তা ভঙ্গের কথা শোনা যায়, তবে তা সংখ্যায় কম কজ

ফিডব্যাক : m_hasan@ovi.com

স্মার্টফোনের নিরাপত্তার জন্য যা করণীয়

এতক্ষণ অনেক ভীতিমূলক কথাবার্তা চললেও ভয় পাবেন না। কারণ দুটো। প্রথমত, স্মার্টফোন ব্যবহারকারীদের সতর্ক করার জন্যই এই লেখা। এখানে সম্ভাব্য সমস্যার কথা বলা হয়েছে। বাস্তবে সব ক্ষেত্রে সমস্যা এত তীব্রতর হয়তো হবে না। দ্বিতীয়ত, নিরাপত্তা ঝুঁকি রোধে ব্যবহারকারীর করণীয় অনেক কিছু আছে, যা মেনে চললে ঝুঁকির পরিমাণ একদম কমিয়ে ফেলা সম্ভব। সে ধরনের কিছু সাবধানতার কথা এখানে উল্লেখ করা হলো।

০১. স্মার্টফোন তো বটেই, ফিচার ফোনেও স্ক্রিন লক পদ্ধতি আছে। আপনার ফোনের স্ক্রিন লক সচল করে রাখুন এবং একটি নির্দিষ্ট সময় পর্যন্ত স্মার্টফোনটি নিষ্ক্রিয় থাকলে যেনো স্বয়ংক্রিয়ভাবে স্ক্রিন লক হয়ে যায়, সেদিকে খেয়াল রাখুন। এতে স্মার্টফোনটি অন্য কোনো ব্যক্তির হাতে পড়লে কিংবা চুরি হয়ে গেলে সহজে ব্যবহার করতে পারবে না।

০২. প্রয়োজন না থাকলে স্মার্টফোনের ওয়াইফাই এবং বিশেষ করে ব্লুটুথ বন্ধ করে রাখুন। ব্লুটুথের মাধ্যমে সাইবার অ্যাটাকের ঘটনা ঘটে।

০৩. যারা তাদের অ্যান্ড্রয়িড ফোনের সব সুবিধা পেতে চান, তারা সাধারণত স্মার্টফোনটি রুট করেন। কারণ, অনেক অ্যাপের পূর্ণ সুবিধা পেতে হলে ফোন রুট করতেই হয়। এতে প্রস্তুতকারকের ওয়ারেন্টি ভঙ্গ হয় এবং স্মার্টফোনটি ঝুঁকির মুখে পড়ে। অ্যাপলের আইফোন কিংবা আইপ্যাডের ক্ষেত্রে এটি জেইলব্রোকেন নামে পরিচিত। স্মার্টফোনটি জেইলব্রেক কিংবা রুট করার আগে সম্ভাব্য সমস্যার কথা মাথায় রাখুন এবং অ্যাপের রুট পারমিশনের ক্ষেত্রে সতর্ক থাকুন।

০৪. স্মার্টফোনে অ্যাপগুলোর পারমিশন ইনস্টল করার সময় লক্ষ রাখুন। অ্যাপ পারমিশন মানে কোন অ্যাপ আপনার স্মার্টফোনের কী কী ব্যবহার করতে পারবে এবং কোন ধরনের পরিবর্তন আনতে পারবে তার একটি তালিকা। কোনো ফাইল ব্রাউজার অ্যাপের ইন্টারনেট অ্যাক্সেস চাওয়া যেমন অদ্ভুত, তেমনি ওয়েব ব্রাউজারের ক্যামেরা অ্যাক্সেস চাওয়াও অদ্ভুত। এ দিকটা লক্ষ রাখুন।

০৫. আপনার ফোনে ডাটা এনক্রিপশন সুবিধা থাকলে গোপনীয় এবং প্রয়োজনীয় ফাইলগুলো এনক্রিপ্ট করে ড্রপবক্স, ওয়ান ড্রাইভ কিংবা গুগল ড্রাইভের মতো নির্ভরযোগ্য ক্লাউড স্টোরেজে সংরক্ষণ করে রাখুন। এতে একদিকে যেমন ফাইলগুলো সুরক্ষিত থাকবে, অপরদিকে স্মার্টফোন হারিয়ে গেলেও তথ্য হারাবে না। তথ্য সঙ্কুচিত করে রাখার নাম ডাটা এনক্রিপশন। এতে কারও হাতে তথ্য গেলেও সে সেই তথ্য উদ্ধার করতে পারবে না।

০৬. স্মার্টফোনে অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার করুন। একদিকে যেমন তথ্যের নিরাপত্তা নিশ্চিত হবে, অপরদিকে ভবিষ্যৎ নিরাপত্তা ঝুঁকি থেকে স্মার্টফোন থাকবে সুরক্ষিত।

০৭. পাসওয়ার্ড নির্বাচন করার সময় কঠিন পাসওয়ার্ড নির্বাচন করুন, যা আপনার মনে থাকবে, কিন্তু দ্বিতীয় কেউ অনুমান করতে পারবে না।

০৮. রিমোট ওয়াইপের নাম শুনেছেন? স্মার্টফোনের জন্য চমৎকার একটি ব্যবস্থা। আপনার ফোনটি হারিয়ে গেলে কিংবা চুরি হলে ঘরে বসেই আপনি আপনার ফোনের সব তথ্য মুছে ফেলতে পারবেন। ফলে সেই তথ্য অন্য কারও হাতে যাবে না।

০৯. গুগল ম্যাপস কিংবা অনুরূপ অ্যাপ্লিকেশনে নিজের হোম এবং অফিস অ্যাড্রেস দেয়া থেকে বিরত থাকুন। সেই সাথে লোকেশন ট্রেস এবং লগ করার সুবিধা বন্ধ করে রাখুন। এতে আপনার অবস্থান সম্পর্কে অন্য কেউ জানতে পারবে না।

১০. ওয়েব ব্রাউজারে পাসওয়ার্ড সংরক্ষণ করার মতো বোকামি না করাই উচিত। কারণ ওয়েব ব্রাউজারে সংরক্ষিত পাসওয়ার্ড সহজেই দেখা যায়। এর বদলে পাসওয়ার্ড ম্যানেজার অ্যাপ ব্যবহার করুন, যা আপনার সব পাসওয়ার্ড সংরক্ষণ করে রাখবে, আবার তা দেখতে চাইলে মাস্টার পাসওয়ার্ড ব্যবহার করেই দেখতে হবে।

১১. যেসব ক্ষেত্রে নিরাপত্তার প্রশ্ন জড়িত, সেসব ক্ষেত্রে পাসওয়ার্ড সংরক্ষণ না করে বরং প্রতিবার নিজে প্রবেশ করুন। এতে হয়তো বারবার আপনাকে পাসওয়ার্ড দিতে হবে, তবে আপনার ডাটার নিরাপত্তা থাকবে অটুট।

১২. ফোনের অপারেটিং সিস্টেম নিয়মিত হালনাগাদ করুন। এতে আপনার স্মার্টফোন সম্ভাব্য ঝুঁকির হাত থেকে রক্ষা পাবে।

১৩. অ্যান্টি-থেফট সফটওয়্যার চুরির হাত থেকে আপনার ফোনকে রক্ষা করতে সাহায্য করবে। জিপিএসের মাধ্যমে ফোনের অবস্থান আপনাকে জানাবে, যার মাধ্যমে আপনি হারিয়ে যাওয়া স্মার্টফোনটি পুনরুদ্ধার করতে পারবেন।

১৪. অপ্রয়োজনীয় এবং নতুন অ্যাপ ইনস্টল করা থেকে বিরত থাকুন। একান্ত প্রয়োজন হলে অ্যাপ ডেভেলপার সম্পর্কে জেনে নিন।

স্মার্টফোনের নিরাপত্তা নিশ্চিত করার দায়িত্ব প্রধানত তিন পক্ষের ওপর। স্মার্টফোন প্রস্তুতকারকের উচিত অপারেটিং সিস্টেমকে যেকোনো নিরাপত্তা ঝুঁকির উর্ধ্বে রাখা। অ্যাপ নির্মাতাদের উচিত সর্বোচ্চ নিরাপত্তা বিধান করা। আর ব্যবহারকারীকে থাকতে হবে সতর্ক। বাকি দুই পক্ষের কাজ এরা করবে, সেখানে আমাদের করার কিছু নেই। তবে আমার স্মার্টফোনের নিরাপত্তার ব্যাপারে সর্বোচ্চ সাবধানতা অবলম্বন করতে হবে আমাকেই।

নকিয়া অ্যান্ড্রয়িড স্মার্টফোন

নাফিস রহমান

নকিয়া কোম্পানি যে মাইক্রোসফট কিনে নিয়েছে, সে খবর আমরা কম-বেশি সবাই জানি। তবে সবচেয়ে অবাক করা যে বিষয়টি টেক বিশ্বকে মোটামুটি নাড়িয়ে দিয়েছে, সেটি হলো নকিয়া বাজারে নিয়ে আসছে অ্যান্ড্রয়িড স্মার্টফোন।

কিছুটা চমকে গেছেন? আসলে ব্যাপারটি অনেকটা এমনই, কারণ সবাই জানেন মাইক্রোসফটের নিজস্ব মোবাইল ওএস আছে, তা সত্ত্বেও কেনো এই সিদ্ধান্ত? ম্যাশঅ্যাবলের প্রতিবেদন– মাইক্রোসফটের কাছে মালিকানা হস্তান্তরের আগেই অ্যান্ড্রয়িড অপারেটিং সিস্টেমের স্মার্টফোন বাজারে ছাড়তে চেয়েছিল নকিয়া। এজন্য ফক্সকনের কাছ থেকে ১০ হাজার ইউনিটের অর্ডারও দিয়েছে!

তবে মাইক্রোসফটের কাছে বিক্রি হয়ে যাওয়ার ঘটনায় নকিয়ার সে অ্যান্ড্রয়িড প্রজেক্ট আলোর মুখ দেখবে– এমন ধারণা করা হয়েছিল, তবে সব জল্পনা-কল্পনার অবসান ঘটিয়ে গত ২৪ ফেব্রুয়ারি স্পেনের বার্সেলোনায় অনুষ্ঠিত মোবাইল ওয়ার্ল্ড কংগ্রেস উপলক্ষে 'এক্স', 'এক্স প্লাস' ও 'এক্স এল' নামে অ্যান্ড্রয়িডের কাস্টমাইজড সংস্করণের তিনটি ফোন উন্মুক্ত করেছে নকিয়া।

সাশ্রয়ী দাম আর নকিয়ার গুডউইল– এ দুটি ব্যাপার পুঁজি করে পথ চলা শুরু করছে নকিয়ার অ্যান্ড্রয়িড স্মার্টফোন। তবে প্রথমে সবচেয়ে বড় যে প্রতিবন্ধকতার মুখোমুখি হবেন ব্যবহারকারীরা তা হলো গুগল প্লেস্টোরের অনুপস্থিতি। অ্যান্ড্রয়িডনির্ভর হলেও এই ফোনগুলো থেকে গুগল প্লেস্টোরে যাওয়ার সুযোগ থাকবে না। নকিয়া এক্স সিরিজের ডিভাইসে ব্যবহৃত অপারেটিং সিস্টেমকে 'নকিয়া এক্স ওএস' বলে পরিচিত করছে ফিনিশ কোম্পানিটি এবং নকিয়া ও মাইক্রোসফট মিলে তাদের এই অ্যান্ড্রয়িড ডিভাইসের জন্য নিজস্ব অ্যাপস স্টোর বানানোর কথা ভাবছে।

নকিয়া এক্স ফোন রুট করে তাতে 'গুগল অ্যান্ড্রয়িড' ব্যব হারে সফল হয়েছেন স্পেনের ডেভেলপার কাশা মালাগা। কয়েক দিন আগে এক্সডিএ ডেভেলপার ফোরামে পাঁচটি পর্যায়ে এই রুট প্রক্রিয়াটিকে তিনি বর্ণনা করেছেন। এক্সডিএ ডেভলপার ওয়েবসাইটের ভিজিট করে সহজ পাঁচটি ধাপ অনুসরণ করুন। এরপর নকিয়া এক্স স্মার্টফোনেও গুগল প্লেস্টোরসহ গুগলের অন্যান্য অ্যাপ চালাতে পারবেন। তবে রুট করার ফলে ব্যবহারকারীরা প্রস্তুতকারকের দেয়া বিক্রিপরবর্তী সেবা থেকে বঞ্চিত হবেন এবং রুট করার প্রক্রিয়ায় ত্রুটির কারণে ক্ষতিগ্রস্ত হতে পারে আপনার প্রিয় অ্যান্ড্রয়িড ডিভাইসটি।

অ্যান্ড্রয়িডচালিত হলেও উইন্ডোজ ফোনের ইউজার ইন্টারফেসের মতো আবহ পেতে রাখা হয়েছে হোম টাইলস ডেকোরেশন আর নকিয়ার চিরাচরিত গ্লান্স স্ক্রিন। ফোন তিনটির হোম স্ক্রিন উইন্ডোজ ফোনের সাথে সাদৃশ্য রেখে তৈরি হয়েছে এবং আকারে নকিয়ার এক্স এল স্মার্টফোনটির ডিসপ্লে পাঁচ ইঞ্চি এবং এক্স ও এক্স প্লাস মডেল দুটির ডিসপ্লে চার ইঞ্চি। প্রাপ্য কনফিগারেশন থেকে দেখা যাচ্ছে, তিনটি ফোনেই মোটামুটি ডুয়াল সিম, লেটেস্ট ভার্সন কিটক্যাট ৪.৪.২, ৫ মেগা পিক্সেল ক্যামেরা, ১ গিগাহার্টজ ডুয়াল কোর প্রসেসর, ৪ জিবি স্টোরেজ, এডনো ২০৩ জিপিইউ, ৫১২ থেকে ৭৬৮ মেগাবাইট র‍্যাম থাকছে।

স্মার্টফোনটির সাথে স্কাইপ, আউটলুক, হিয়ার ম্যাপস, মিক্সর ্যাডিও প্রভৃতি অ্যাপ বিল্টইন থাকবে। স্ট্যান্ডবাই টাইম হচ্ছে ১৭ দিন এবং মিউজিক প্লেব্যাক পাবেন টানা ২৬ ঘণ্টা পর্যন্ত আর ভিডিও প্লেব্যাক পাবেন ৮.৪ ঘণ্টা। এর বডি উন্নতমানের প্লাস্টিক দিয়ে বানানো। এর পেছনের দিকে রাবারের প্রলেপ থাকায় পেছনের দিকটা দেখতে আকর্ষণীয় ও স্ক্যাচ পড়ার সম্ভাবনাও কম। লাল, সবুজ, হলুদ, কালো ও সাদা পাঁচটি রংয়ে এই ফোন এখন আপনার হাতের কাছেই পাওয়া যাচ্ছে।

মোটামুটি এন্ট্রি লেভেলের এসব স্মার্টফোন বাজারে ফ্ল্যাগশিপ স্ট্যাটাসও নেবে না। বাজারে আসার আগেই এই নকিয়া এক্স সিরিজ হিট করার আভাস দিচ্ছে। চীনে ইতোমধ্যে এই সেটগুলোর ১ মিলিয়ন (১০ লাখ) ইউনিট প্রি অর্ডার প্রদান করেছে।

বাংলাদেশ এক্স প্লাস ও এক্স এল মডেল দুটির দাম হবে যথাক্রমে প্রায় ১০ হাজার ৬০০ ও ১১ হাজার ৭০০ টাকা। আর নকিয়ার এক্স স্মার্টফোনটির দাম হবে ৯ হাজার ৫০০ টাকা।

দেখা যাক নকিয়ার এই পরীক্ষামূলক পদক্ষেপ নকিয়াকে কতটা ব্যবসায় সফল করে। তবে নকিয়ার মতো টেক জায়ান্টের অ্যান্ড্রয়িডপ্রীতি যে গুগলের এই ওস-কে আরও জনপ্রিয় করবে সেটাই সবার কাম্য কজ

ফিডব্যাক :
nafisrahman2012@gmail.com

Nokia Android Phone Spacifications

	Nokia X	Nokia X+	Nokia XL
OS	Android	Android	Android
Screen Size	4-inches	4-inches	5-inches
Resolution	480 x 800	480 x 800	480 x 800
Rear Camera	5MP	5MP	5MP+flash
Front Camera	No	No	2MP
Processor	1GHz dual-core	1GHz dual-core	1GHz dual-core
Storage	4GB	4GB	4GB
Memory	512MB	768MB	768MB
Battery	1500mAh	1500mAh	2000mAh
Height	4.55 in	4.55 in	5.57 in
Width	2.5 in	2.5 in	3.1 in
Thickness	.41 in	.41 in	.43 in