স্মার্টফোনের নিরাপত্তা ও আমাদের করণীয়

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

আমাদের দেশে স্মার্টফোনের ব্যবহার দিন দিন বেড়েই চলেছে। স্মার্টফোনের ব্যবহার বাড়ার সাথে সাথে এর নিরাপত্তার বিষয়টিও এখন গুরুত্বপূর্ণ হয়ে উঠেছে। ডেস্কটপ কিংবা ল্যাপটপের ইন্টারনেটভিত্তিক অনেক কাজই এখন মানুষ স্মার্টফোনে সেরে ফেলেন। ফলে ইন্টারনেটভিত্তিক বিভিন্ন ভাইরাস স্মার্টফোনে ঢুকে যাওয়ার ঝুঁকিও মারাত্মকভাবে বেড়ে যাওয়ার আশঙ্কা রয়েছে। সতর্ক না থাকলে সাইবার অপরাধীরা খুব সহজেই তাদের উদ্দেশ্য পূরণ করতে পারে। ম্যালওয়্যার ভাইরাস খুব সহজেই ব্যক্তিগত কমপিউটারের মতো মোবাইল ডিভাইসগুলোতেও একই ধরনের আক্রমণ করছে। মেইলের অ্যাটাচমেন্ট দেখা, ওয়েবসাইটে ক্লিক করা অথবা একটি ফাইল বা অ্যাপ ডাউনলোড করার মধ্য দিয়েও ভাইরাস তার ক্ষতিকর কার্যক্রম পরিচালনা করতে পারে। সাইবার ক্রিমিনালেরা সেল্যুলার নেটওয়ার্কে DDoS (Distributed Denial of Service) আক্রমণ করার জন্য এসব মোবাইল ডিভাইসগুলো ব্যবহার করে। এরা এদের টার্গেটেড ওয়েবসাইটকে ট্র্যাফিক ওভারলোড করে ক্র্যাশ করাতে পারে। ভাইরাস আক্রমণ কমিউনিকেশন নেটওয়ার্কের মাধ্যমে আক্রমণ করে জিএসএম, ওয়াইফাই, ব্লুটুথ ইত্যাদিতে।

ক্রমাগত সাইবার ক্রিমিনালদের দৌরাত্ম্যই মোবাইল ম্যানুফ্যাকচারারদের মোবাইল সিকিউরিটি সফটওয়্যার নিয়ে ভাবতে বাধ্য করছে। গত বছরের হিসাব অনুযায়ী, আমাদের দেশের ৯৫ শতাংশ ইন্টারনেট ব্যবহারকারী হলেন মোবাইল ব্যবহারকারী এবং এর একমাত্র কারণ মোবাইলে কাজ করা অন্যান্য ডিভাইসের চেয়ে খুবই সহজ ও সবার কাছেই আছে, সব সময়ই চালু থাকে, একটি মাত্র ডিভাইস, যা একাই অনেকগুলো ডিভাইসের কাজ করে এবং সবসময় হাতে থাকে। তাই মোবাইল কোম্পানিগুলোও মোবাইল সিকিউরিটির ব্যাপারে সচেতন হচ্ছে। স্মার্টফোন ব্যবহারে নিরাপত্তা ঝুঁকি থাকলেও তা যেহেতু আমাদের উৎপাদনশীলতা বাড়িয়ে দেয়, তাই আমাদের স্মার্টফোন ব্যবহারের বিকল্প নেই। নিরাপত্তা ঝুঁকি কমাতে মোবাইল ডিভাইসের নিরাপত্তাবিষয়ক টিপগুলো মনে রাখলে আপনার স্মার্টফোনকে নিরাপদ রাখতে পারবেন।

টিপস-১ : ডিভাইসে শক্তিশালী পাসওয়ার্ড সেট করা। পাসওয়ার্ড নির্ধারণের ক্ষেত্রে আপনার ফোন নম্বর, জন্মদিনের তারিখ কিংবা আপনার বহুল ব্যবহৃত কোনো নাম্বার ব্যবহার করবেন না। পাসওয়ার্ডটিতে অবশ্যই সংখ্যা ছোট হাতের এবং বড় হাতের অক্ষরের মিশেল রাখবেন। এছাড়া প্যাটার্ন লক ব্যবহার করে দেখতে পারেন।

টিপস-২ : অ্যান্টি-থেফট সলিউশন ব্যবহার করুন। ল্যাপটপ কিংবা ডেস্কটপের তুলনায় স্মার্টফোন হরহামেশাই হারায় কিংবা চুরি হয়ে থাকে। তাই স্মার্টফোনে অ্যান্টি-থেফট সলিউশনের ব্যবহার খুবই গুরুত্বপূর্ণ। কিছু মোবাইলে এই সলিউশনটি ইনস্টল করাই থাকে। যেমন আইফোনে আছে 'ফাইন্ড মাই আইফোন'। তবে যাদের ফোনে এই ধরনের সলিউশন থাকে না, তারা অ্যাভিরা ফ্রি মোবাইল সিকিউরিটির মতো বিশ্বস্ত কোনো মোবাইল সিকিউরিটি ব্যবহার করতে পারেন।

টিপস-৩ : অপারেটিং সিস্টেমের হালনাগাদ সংস্করণ ইনস্টল করুন। কিছু কিছু অপারেটিং সিস্টেম নিজ থেকেই হালনাগাদ হয়ে থাকে। তবে আপনার স্মার্টফোনে সাপোর্ট করে এমন সর্বশেষ হালনাগাদ ভার্সনের অপারেটিং সিস্টেমটি ব্যবহারের চেষ্টা করুন। এতে শুধু অপারেটিং সিস্টেমে নতুন ফিচারই যোগ হবে না, ফোনের নিরাপত্তা ব্যবস্থাও হালনাগাদ থাকে। ফলে ভাইরাসে আক্রান্ত হওয়ার সম্ভাবনা কম থাকে।

টিপস-৪ : অ্যাপ হালনাগাদকরণ। অপারেটিং সিস্টেমের মতো অ্যাপসগুলোও সবসময় হালনাগাদ রাখতে হবে। অ্যাপসগুলো হালনাগাদ রাখার মাধ্যমেও স্মার্টফোনকে অনেকখানি নিরাপদ রাখা যায়।

টিপস-৫ : একটি সিকিউরিটি সলিউশন ইনস্টল রাখা। বেশিরভাগ ক্ষেত্রেই দেখা যায়, বিভিন্ন মোবাইল অ্যাপসগুলো দেখতে যেমন মনে হয়। সত্যিকার অর্থে সেগুলো সেরকম নয়। অনেক ক্ষেত্রে দেখা যায়, অ্যাপসগুলোতে যেসব ফিচারের কথা বলা থাকে, সেগুলো বাস্তবে সেসব কাজ করে না। তাই একটি ভালোমানের সিকিউরিটি সলিউশন ব্যবহারের মাধ্যমে অপরিচিত ম্যালওয়্যারের আশঙ্কা থেকে নিরাপদ থাকা যায়।

টিপস-৬ : আন-অফিসিয়াল অ্যাপস্টোর থেকে ডাউনলোড না করা। মোবাইল মানে নিত্যনতুন অ্যাপস ডাউনলোড করা আর মজা নেয়া। কিন্তু আপনি একটুও ভেবে দেখেছেন আপনার অ্যাপসটি ভাইরাসমুক্ত কি না। হ্যাঁ, অবশ্যই আপনার মোবাইল অ্যাপসটি পরীক্ষা করবেন। এই তো কিছুদিন আগে গুগলে ৫০ হাজার অ্যাপস রিমুভ করেছে। কারণ গুগলে এর অ্যাপস সবসময় ভাইরাসমুক্ত থাকে। তাই তারা কোনো সমস্যা হওয়ার আগে এসব অ্যাপস রিমুভ করে থাকে। দেখা গেছে, ২০১২ সালে ৩২ মিলিয়ন অ্যান্ড্রয়িড ডিভাইস অ্যাপসের ভাইরাসে আক্রান্ত হয়েছে। এগুলো অ্যাপলে ৯৫ শতাংশ আক্রান্ত হয়েছে। আপনি যদি অ্যাপল পছন্দ না করেন, কিন্তু যদি এটা আপনার সখের মোবাইলের সাথে হয়, তবে কেমন হবে। তাই অবশ্যই অ্যাপস বা সফটওয়্যার ডাউনলোড করার সময় সতর্ক থাকবেন।

টিপস-৭ : স্মার্টফোনের সব পার্টস না খোলা। অনেককে অতি আগ্রহী হয়ে স্মার্টফোনের বিভিন্ন পার্টস খুলে নড়াচড়া করতে দেখা যায়। এটা করলে ডিভাইসের ওয়্যারেন্টিজনিত সমস্যার পাশাপাশি নিরাপত্তা সমস্যার দুয়ারও খুলে যেতে পারে।

টিপস-৮ : অনিরাপদ ওয়াই-ফাইয়ে সংযুক্ত হওয়া থেকে বিরত থাকুন। বর্তমানে বিভিন্ন প্রতিষ্ঠানে কিংবা স্থানে ওয়াই-ফাই উন্মুক্ত থাকে। আপনি যখনই অনিরাপদ ওয়াই-ফাই নেটওয়ার্কে সংযুক্ত হবেন, তখনই আপনার স্মার্টফোনে সংরক্ষিত বিভিন্ন পাসওয়ার্ডসহ গুরুত্বপূর্ণ তথ্য প্লেন ডাটা হিসেবে সেই নেটওয়ার্কে চলে যেতে পারে।

টিপস-৯ : নিরাপত্তার বিষয়টি সবসময় মাথায় রাখা। নন-উইন্ডোজ অপারেটিং সিস্টেম ব্যবহারের ফলে অনেকেই ভাইরাস আক্রান্ত হওয়ার বিষয়টি ভুলে যান, যা কোনোভাবেই কাম্য নয়। আপনি যেকোনো সন্দেহজনক ওয়েবসাইট ব্রাউজিং, ই-মেইল অ্যাটাচমেন্ট খোলা কিংবা অ্যাপস ব্যবহারের সময় অজান্তেই ভাইরাসে আক্রান্ত হতে পারেন কিংবা আপনার গোপন তথ্য অন্যের হাতে চলে যেতে পারে।

টিপস-১০ : অ্যান্ড্রয়িড মোবাইলের দ্বিতীয় সিকিউরিটি যে বিষয়টি আছে তা হয়তো অনেকে জানেন না বা বুঝতে পারেন না। যেকেউ আপনার আই ক্লাউড বা আপনার জি-মেইল অ্যাকাউন্টে গিয়ে আপনার কত বড় ক্ষতি করতে পারে। যখন আপনি স্মার্টফোনে অনেক কষ্ট করে কিছু তৈরি করলেন এবং কেউ আপনার মোবাইলে আই ক্লাউড বা জি-মেইল ব্যবহার করে আপনার সব তথ্য চুরি করে নিল। আপনি এজন্য মোবাইলের জি-মেইল অ্যাকাউন্টে ২ স্টেপ অ্যাকটিভ করে নিতে পারেন। এই কাজটি করলে কেউ যদি আপনার জি-মেইল পাসওয়ার্ড জেনেও যায়, তাহলে ভয়ের কিছু নেই। কারণ আপনার মোবাইলের ২ স্টেপ অ্যাকটিভ করা আছে। তাই কেউ যদি আপনার জি-মেইলে লগইন করে তাহলে মোবাইলে যে কোডটি আসবে সেটা ছাড়া কেউ অ্যাকাউন্টে প্রবেশ করতে পারবে না।

টিপস-১১ : যদি আপনার মোবাইলে কোনো ব্যাংকের কাজ করে থাকেন, তাহলে অবশ্যই আপনার স্মার্টফোনে একটি মাত্র ব্রাউজার ব্যবহার করতে হবে। এসব কাজ করতে অবশ্যই অফিশিয়াল অ্যাপস ব্যবহার করতে হবে। উদাহরণস্বরূপ ব্যাংক অব আমেরিকা, ভানগার্ড, মিন্ট ইত্যাদি কোম্পানির নিজস্ব ব্রাউজার থাকে।

টিপস-১২ : বর্তমানে হ্যাকারেরা ম্যাসেজের মাধ্যমে কিছু লোভনীয় অফার দিয়ে থাকে এবং তার ভেতর ট্রোজান, স্পাইওয়্যার প্রভৃতি দিয়ে দেয়। এই ধরনের অফার থেকে দূরে থাকুন।

স্মার্টফোন ব্যবহারকারীরা উপরে উল্লিখিত বিষয়গুলো মেনে চললে নিজেকে অনেক বেশি নিরাপদ রাখতে পারবেন কজ

ফিডব্যাক : jabedmorshed@yahoo.com