ফেসবুক পেজ জনপ্রিয় করার ১০টি টিপস

মাথায় নতুন কোনও আইডিয়া আসলেই সবার আগে চাই একটা ফেসবুক পেজ। পেজ খোলা তো মিনিট দুয়েকের কাজ। এরপর ফেসবুক পেজ জনপ্রিয় করবেন কী করে? হুড়মুড় করে সবাই লাইক বা ফলো করবে না নিশ্চয়ই। পেজে লাইক বাড়াতে থাকা চাই ধৈর্য, জানা চাই বিশেষ কিছু টিপস।

প্রোফাইল গুছিয়ে নিন
ফেসবুক পেজের জন্য অন্যরকম একটা নাম থাকলে নিজেকে আলাদা করতে পারবেন ঠিকই, তবে ব্যবহারকারীরা পেজটাকে সহজে খুঁজে পাবে না। মাথায় রাখতে হবে মানুষের খোঁজার অভ্যাস। অর্থাত্ মানুষ গুগল বা ফেসবুকে কী লিখে সার্চ করছে সেটা মাথায় রেখে পেজের নাম ও ইউআরএল ঠিক করুন। এক্ষেত্রে পরিচিত ব্র্যান্ড হলে সে নামেই পেজ খোলা যায়। আর যদি ব্র্যান্ডের চিন্তা মাথায় না থাকে, তবে পেজের নাম বা ইউআরএল যতটা সম্ভব সাধাসিধে রাখুন।

অনেকে আবার কোনোরকম পেজ খুলেই লাইক বাড়াতে ঝাঁপিয়ে পড়েন। ডেসক্রিপশন, স্লোগান, ঠিকানা, খোলা থাকার সময়, ওয়েবসাইট, ফোন নম্বর, লোকেশন এসব ঠিকঠাক না করলে সেই পেজের প্রচার করবে না ফেসবুক। তাই সময় নিয়ে এসব তথ্য পূরণ করুন। নিজের মতো করে একটি এনিমেটেড বা ভিডিও কাভার যোগ করতে পারলে বেশ ভালো। কোনও ছবি আপলোড করলে সেটার একটা সুন্দর বর্ণনা লিখতে ভুলবেন না। পেজের সবচেয়ে আকর্ষণীয় পোস্টটাকে ‘পিন’ করে রাখুন।

লাইক-কমেন্ট করুন
নিজের পেজে অন্যের লাইক কমেন্টের আশায় হা করে বসে না থেকে পেজের প্রোফাইল থেকে অন্যের পেজের ভালো পোস্টগুলোতে লাইক ও গঠনমূলক কমেন্ট করুন। শুধু শুধু নিজের পেজের নামটা দেখানোর জন্য এক শব্দে বা এলোমেলো কিছু লিখতে যাবেন না। এতে আপনার পেজের প্রতি কারও আগ্রহ থাকবে না। পেজের অর্গানিক গ্রোথ বাড়াতে শুরুতে আপনার পেজটি যেন ‘সবার বন্ধু’ হিসেবেই থাকে।

কল টু অ্যাকশন
বিজনেস সংক্রান্ত পেজ হলে অবশ্যই ওপরের দিকের বারে উপযুক্ত বাটন রাখবেন। কারও ক্ষেত্রে সেটা হতে পারে সেন্ড মেসেজ, কারও বেলায়

সাইন-আপ। আবার পেজের ‘শপ’ সেকশনে যখন যথেষ্ট আইটেম থাকবে তখন ‘শপ নাও’ বাটনও যোগ করতে পারেন। এক্ষেত্রে সেন্ড মেসেজ বা কল বাটনের ব্যবহারই বেশি বলা যায়।

যোগ করুন গ্রুপ
পেজের ফ্যান-ফলোয়ার বাড়তে শুরু করলে তাদের সবাইকে এক ছাদের তলায় নিয়ে আসার চেষ্টা করুন। তাদের মতামত বা পোস্ট শেয়ার করার জন্য আলাদা করে একটা গ্রুপ বানিয়ে নিতে পারেন। ওই গ্রুপের কারণেও বাড়তে পারে অর্গানিক লাইক।

লাইভ
সাধারণ ভিডিও বা পোস্টের চেয়ে ১০ গুণ বেশি রিচ পাওয়া যাচ্ছে ফেসবুক লাইভ ভিডিওতে। তাই পেজের সঙ্গে মানানসই কোনও আইডিয়া পেলে সেটার লাইভ করার চেষ্টা করুন। ফেসবুক এখনও লাইভ ভিডিওগুলোকে তাদের নিউজ ফিডে সবার ওপরে রাখার চেষ্টা করে। এক্ষেত্রে কোনও পণ্য বা সেবার ডেমো কিংবা মজার কোনও টিউটোরিয়াল দেখাতে পারেন।

পোস্টের মাপ
একটি আদর্শ অর্গানিক ফেসবুক পোস্টের দৈর্ঘ্য হলো ৪০-৮০টি অক্ষর (ইংরেজিতে, স্পেসসহ)। অল্প কথায় বেশি তথ্য দিতে পারলেই সেটার ‘রিচ’ বাড়িয়ে দেয় ফেসবুক।

ভুল তথ্য নয়
পেজের এনগেজমেন্ট বাড়াতে উল্টোপাল্টা খবর বা ভুল কিছু পোস্ট করতে যাবেন না। ভুয়া তথ্য নিয়ে ফেসবুক এখন বেশ সরব। ভুল তথ্যের ‘রিপোর্ট’ পেলে দেখা যাবে আপনার পেজটা চলে যাবে লাল তালিকায়।

সময়জ্ঞান
আপনার গ্রাহক বা পেজের অনুসারীদের অভ্যাস বা রুটিন বুঝে নিন। সেই অনুযায়ী বেছে নিতে হবে পোস্ট করার সময়। একেক ধরনের পেজে ব্যবহারকারীদের এংগেজমেন্টের সময়টাও একেক রকম। যেমন খাবার ডেলিভারি সংক্রান্ত পেজ হলে সকাল বা বিকালের সময় পোস্ট করুন, মধ্যরাতে নয়।

ইনস্ট্যান্ট রিপ্লাই
আপনার বিজনেস পেজে ইনবক্স করা মাত্রই যেন ক্রেতারা কোনও না কোনও তথ্য পায়, সে জন্য অটোমেটিক রিপ্লাইয়ের ব্যবস্থা রাখুন। পেজের সেটিংস-এ গিয়ে বামপাশের মেসেজিং অপশনে যান। এরপর রেসপন্স অ্যাসিসট্যান্ট সিলেক্ট করে ‘সেন্ড ইনস্ট্যান্ট রিপ্লাইস’

সিলেক্ট করুন। চেঞ্জ-এ ক্লিক করে নিজের মতো করে বার্তাটি লিখুন। আপনার ক্রেতা বা গ্রাহক যদি শুধু এ দেশীয় হয়, তবে অভ্যর্থনার বার্তা বাংলাতেই লিখুন। সবশেষে ‘সেভ’ করুন।

ফেসবুক পিক্সেল
আপনার যদি আলাদা ওয়েবসাইট থাকে তবে সেই সাইটের ফেসবুক পেজের জন্য ‘ফেসবুক পিক্সেল’ অপশনটি ব্যবহার করুন। এর জন্য কিছুটা আইটি জ্ঞান থাকা চাই। পিক্সেল বলতে এখানে একটি ছোট কোডকে বোঝানো হচ্ছে যা আপনার ওয়েবসাইটে থাকবে। ওই কোডের মাধ্যমে আপনার ওয়েবসাইট ভিজিট করা গ্রাহকদের তথ্য পাবে ফেসবুক। সেই অনুযায়ী ঠিক করতে পারবেন ‘টার্গেট অডিয়েন্স’। অর্থাত্ যারা আপনার ওয়েবসাইটে মাঝে মধ্যে ঢুঁ মারে তারাই আপনার ফেসবুকের পোস্ট যেন বেশি বেশি দেখতে পায়, সেটাই করে ফেসবুক পিক্সেল।

উবারের সিস্টেম হ্যাক করল কিশোর

হ্যাকিংয়ের শিকার হয়েছে জনপ্রিয় রাইড শেয়ারিং প্রতিষ্ঠান উবার। ১৮ বছরের এক কিশোর মার্কিন এ প্রতিষ্ঠানের কম্পিউটার সিস্টেম হ্যাক করেছে। অ্যামাজন ওয়েব সার্ভিসেস এবং গুগল ক্লাউডসহ উবারের বেশকিছু বাণিজ্যিক টুলে প্রবেশ করতে সক্ষম হয়েছে বলে দাবি ওই কিশোর হ্যাকারের। হ্যাকার নিজেই উবারের স্ল্যাক সিস্টেমে এ বিষয়ে পোস্ট করেছেন।

উবারের অভ্যন্তরীণ গোপন নথিপত্রের স্ক্রিনশট শেয়ার করে ওই হ্যাকার বলেন, আমি একজন হ্যাকার এবং ডেটা ফাঁসের শিকার হয়েছে উবার।

প্রযুক্তিবিষয়ক সাইট ভার্জ এ বিষয়ে উবারের কাছে জানতে চাইলে কোনো ধরনের উত্তর দিতে রাজি হয়নি প্রতিষ্ঠানটি। তবে উবার এরইমধ্যে কর্মীদের বেশকিছু সফটওয়্যার ব্যবহার বন্ধ করে দিয়েছে, এমনটাই জানিয়েছে নিউ ইয়র্ক টাইমস।

কোনো খারাপ উদ্দেশ্য নিয়ে উবারের কম্পিউটার সিস্টেমে প্রবেশ করেনি ওই হ্যাকার। মজা করতে গিয়েই এমনটা করেছেন তিনি।
তবে এক টুইট বার্তায় উবারের পক্ষ থেকে বলা হয়েছে, সাইবার নিরাপত্তা বিষয়ক ঘটনার তদন্ত করছি। আইন-শৃঙ্খলা বাহিনীর সঙ্গেও যোগাযোগ রাখছি। উবার নিশ্চিত করছে, কোম্পানির পরিষেবায় কোনো সমস্যা নেই।

ইউগা ল্যাবসের সিনিয়র ইঞ্জিনিয়ার স্যাম বলেন, ওই কিশোর হ্যাকার অভ্যন্তরীণ গোপন নথিপত্রের যে স্ক্রিনশট শেয়ার করেছে তা খুবই বিশ্বাসযোগ্য।

উবারের প্রাক্তন প্রধান নিরাপত্তা কর্মকর্তা জোসেফ সুলিভান ২০১৬ সালে একটি বড়সড় সাইবার হামলা ধামাচাপা দেওয়ার চেষ্টা করেছিলেন। হ্যাকারদের ১০ লাখ মার্কিন ডলার দিতে চেয়েছিলেন তিনি। যার বিচার এখনও চলমান রয়েছে। সে ঘটনায় প্রায় ৫৭ মিলিয়ন গ্রাহক এবং ড্রাইভারের ব্যক্তিগত তথ্য চুরি হয়েছিল।

সাইবার সিকিউরিটির অধ্যাপক অ্যালান উডওয়ার্ড বলেছেন, হ্যাকারের কাছে উবারের হাই অ্যাক্সেস আছে বলে মনে হচ্ছে। প্রতিষ্ঠানটির পক্ষে এটা জানাও কঠিন হবে যে তারা হ্যাকারকে নেটওয়ার্ক থেকে সরিয়ে দিতে পেরেছে কি না।

সামাজিক যোগাযোগ মাধ্যমে নিরাপদ থাকার কৌশল

আমাদের দৈনন্দিন ইন্টারনেট ব্যবহারের বড় একটি অংশজুড়েই সামাজিক যোগাযোগ মাধ্যম। বিশেষত ফেসবুক, মেসেঞ্জার, ইনস্টাগ্রাম ও স্ন্যাপচ্যাটের জনপ্রিয়তা তুঙ্গে। যত দিন যাচ্ছে ইউজার সংখ্যাও বাড়ছে। আর এরইমধ্যে কিছু দুষ্কৃতিকারী নানাভাবে আপনার একাউন্ট নষ্ট করার চক্রান্তে মেতে আছে। মূলত অনলাইনে আপনার তথ্য চুরি কিংবা একাউন্ট চুরি করে নানা অপকর্ম করছে। অনেক সময় অনেকের টাকা- পয়সা হাতিয়ে নেওয়ার মতো ঘটনাও ঘটেছে।

তাই নিরাপত্তার বিষয়ে সচেতনতা বাড়ানো দরকার। অবশ্য আজকাল অনেকেই এসব বিষয়ে সতর্ক হতে শুরু করেছেন। তবু চক্রান্তকারীরা নানা ফাঁদ-কৌশল আবিষ্কারের মাধ্যমে আপনার নিরাপত্তা বিঘ্নিত করছে। অনলাইনে নিজেকে নিরাপদ রাখবেন কিভাবে তবে? প্রতিটি সামাজিক যোগাযোগ মাধ্যমই এখন নিজেদের সেফটি ফিচার চালু করেছে। আবার কিছু কিছু নিরাপত্তা কৌশল আপনাকে নিজের ডিভাইস থেকেই করতে হবে।

আজ মূলত এসব কৌশল নিয়েই আলোচনা করবো। মনোযোগ দিয়ে পড়ুন। আপনার কাজে আসবে।

ফেসবুকে নিরাপত্তা নিশ্চিত করুন

সম্ভবত ফেসবুকেই আমরা নিজেদের অধিকাংশ তথ্য দিয়ে থাকি। পরিচিতরা আপনার ব্যক্তিগত তথ্য জানতেই পারেন। কিন্তু সামাজিক যোগাযোগ মাধ্যমে অপরিচিতরাও আপনার তথ্য জেনে যেতে পারে। দেখা গেছে, এসব তথ্য ব্যবহার করে সাইবার হামলা, কিংবা অন্যের আর্থিক ক্ষতির মতো ভয়ানক কাজেও জড়িয়ে পড়ে কিছু চক্র। ফেসবুকের বিভিন্ন কৌশল ব্যবহার করেই তারা এমনটা করে থাকে। ফেসবুকের নিরাপত্তা বিষয়ে ব্যক্তিগত কিছু ভুলেও এমনটা হয়ে থাকে। সেই বিষয়গুলোই এখানে আপনাদের জানিয়ে দেই।

বন্ধু তালিকা
বন্ধু তালিকায় অপরিচিত কাউকে না রাখাই ভালো। এমনকি নতুন কাউকে ফ্রেন্ডলিস্টে এড করলে তার প্রোফাইল দেখে নিন। আবার সময় অসময়ে একবার ফ্রেন্ডলিস্ট চেক করুন। তাতে বুঝতে পারবেন কোন একাউন্টগুলো ইনেক্টিভ কিংবা বন্ধ। সচরাচর ফ্রেন্ড লিস্টে অপরিচিত, ফেক একাউন্ট রাখবেন না।

ফেসবুকে প্রাইভেসি সেটিংস নির্বাচন
ফেসবুকে আপনার তথ্যগুলো কারা দেখবে, বা আদৌ দেখতে পারবে কিনা তা নির্ধারণ করুন। সেই সুযোগ আপনাকে এখন দেওয়া হয়েছে। আপনি ভালোমতোই জানেন সামাজিক মাধ্যম তথ্যকে গুরুত্ব দেয়। তাই নিজের ব্যক্তিগত তথ্য নিয়ে অবহেলা নয়।

পাসওয়ার্ড সচেতনতা
পাসওয়ার্ড সংরক্ষণে ও নির্ধারণে সতর্ক হন। একেবারে সহজ পাসওয়ার্ড দেওয়া উচিত না। আর সময়ে সময়ে নিজের পাসওয়ার্ড বদল করুন। এক পাসওয়ার্ড দীর্ঘদিন ব্যবহার করবেন না।

টু-স্টেপ অথেনটিকেশন
দুই ধাপ নিশ্চিতকরণের মাধ্যমে একাউন্টের নিরাপত্তা নিশ্চিত হয়। এতে সহজে আপনার একাউন্টে পাসওয়ার্ড জানা সত্ত্বেও প্রবেশ করতে পারবে না।

একই একাউন্ট থেকে পেজ ম্যানেজ করা
আজকাল ফেসবুকে ব্যবসা পরিচালনার জন্যে অনেকে একই একাউন্ট দিয়ে পেজ ম্যানেজ করেন। এতে কিন্তু আপনার নিজের একাউন্ট বিপদে পড়তে পারে। ফেসবুকে আপনাকে পেজে বিভিন্ন পদে যোগ করার সুযোগ আছে। তা ব্যবহার করুন।

গেম বা কুইজ থেকে সতর্ক
ফেসবুকে আজকাল অনেক গেম দেখা যায়। আবার আজকাল কিছু এপ আসে যেগুলোর মাধ্যমে অন্যরা নাম গোপন রেখে আপনায় মেসেজ দিতে পারে। এ ধরণের এপ থেকে সাবধান। এতে গেম খেলার সময় আপনার অনেক তথ্য চুরি হতে পারে। একাউন্টও হারাতে পারেন।

নিয়মিত চেকাপ
facebook.com/privacy/checkup এই লিংকের মাধ্যমে নিজের প্রোফাইলের নিরাপত্তা আপনি দেখতে পারবেন।

ইনস্টাগ্রামে একাউন্টের নিরাপত্তা নিশ্চিত করুন
ফেসবুকে আপনার নিরাপত্তা কিংবা প্রাইভেসি নির্ধারণ অনেক সহজ। কিন্তু ইনস্টাগ্রামে কাজটি এত সহজ নয়। ফেসবুকে প্রতিটি পোস্টে প্রাইভেসি নির্ধারণ করা যায়। ইনস্টাগ্রামে তা নেই। সেক্ষেত্রে আপনার ফলোয়ার এর অবস্থা দেখে নেবেন। অপরিচিতদের যোগ না করাই ভালো। এমনকি আপনার একাউন্ট প্রাইভেট করে রাখুন। এতে যারা আপনার সম্মতিতে যুক্ত আছে তারাই শুধু দেখতে পারবে আপনার দেওয়া ছবি বা ভিডিও।

রিপোর্ট করুন ঝামেলা দেখলে
অনলাইনে নিজের একাউন্ট নিরাপদ রাখাটাই একমাত্র উপায় নয়। আপনাকে অনলাইনের পরিবেশকেও নিরাপদ রাখতেই হবে। কাজটির জন্যে কখনও সামাজিক যোগাযোগ মাধ্যমে বাজে কন্টেন্ট পেলেই রিপোর্ট করুন। আপত্তিকর পোস্ট না সরিয়ে আমরা আজকাল কমেন্টে নানা আজেবাজে তর্কে জড়িয়ে পড়ি। তাতে আপনার নানাবিধ সমস্যা যেমন সাইবার বুলিং এর শিকার হতে হয়। সেজন্যে আপত্তিকর পোস্টে নিজেকে সংযুক্ত না করে রিপোর্ট করুন।

মেসেঞ্জার ব্যবহারে সতর্কতা
ফেসবুক ও ইনস্টাগ্রামের মেসেজ দেখতে মেসেঞ্জার এখন বহুল জনপ্রিয়। মেসেঞ্জারে কিছু বাড়তি নিরাপত্তা গ্রহণ করতে হয়। যেমন মেসেঞ্জারে যেহেতু আপনার পার্সোনাল ইনবক্স থাকে তাই একে এপলক দিয়ে সিকিউর রাখুন। এমনকি মেসেঞ্জারে চাওয়া ক্যামেরা, অডিও পার্মিশন না দেওয়াই ভালো। এতে আপনার ব্যক্তিগত তথ্য নিরাপদ থাকবে।

ই-মেইলের নিরাপত্তা
যেকোনো সামাজিক যোগাযোগ মাধ্যমে ইমেইল ব্যবহার বাধ্যতামূলক। তাই ইমেইল নিরাপদ রাখতে প্রয়োজন বাড়তি সতর্কতা। শুধু আপনার ইমেইল হ্যাক করতে পারলে হারাতে পারে অনেক কিছু। যেকোন ডিভাইসে আপনার ইমেইল দিয়ে লগিন দেবেন না। নিজের রেগুলার ডিভাইসেই মেইল একাউন্ট রাখুন।

লোকেশন সার্ভিস বন্ধ রাখুন
লোকেশন শেয়ার সার্ভিস অপ্রয়োজনে চালু করবেন না। আবার আমরা আজকাল হুটহাট অনেককে গুগল ম্যাপের লোকেশন দিয়ে রাখি। এতে আপনার ফোনের অনেক প্রাইভেট ডাটাও অন্য কেউ চেক করতে পারে। বিশেষ প্রয়োজনে আপনি লোকেশন শেয়ার করতেই পারেন। কিন্তু লোকেশন সার্ভিস চালু রাখবেনই না। একবার ভেবে দেখুন, আপনি কোন এলাকায় আছেন তা সর্বক্ষণ বিভিন্ন সামাজিক যোগাযোগ মাধ্যমেও আপডেট হয়ে থাকবে। এমনভাবে নিজের প্রাইভেসি বিঘ্নিত করা মোটেও সুখবর নয়।

অনলাইনে কেনাকাটার সময় সাবধান
একসময় ফিশিং লিংক দিয়ে অনেকের আইডি হ্যাক করা হতো। আজকাল সেই পদ্ধতিতে বদল এসেছে। মানুষ এখন অধিকাংশ কেনাকাটা অনলাইনেই করে। সামাজিক যোগাযোগ মাধ্যমে বিভিন্ন পেজ বা লিংকের মাধ্যমে অনলাইন শপে কেনাকাটা করে। অনেক সময় কিছু লিংকে প্রবেশ করে পেমেন্ট করে নানা ভোগান্তির শিকার হতে হয়। পেমেন্ট করার সময় আমরা সচরাচর কার্ড ব্যবহার করি। পেমেন্ট করার পর ব্যাংকের সাথে যোগাযোগ করে আপনার কার্ডের নিরাপত্তার বিষয়টি নিশ্চিত হোন। বিশেষত ডেবিট কার্ডে কিছু নিরাপত্তার খুত বের করে হ্যাকাররা টাকা চুরি করে। তাই সাবধান থাকুন।

আর্থিক লেনদেন
ব্যাংকিং ব্যবস্থাও এখন ডিজিটাল হয়ে গেছে। আবার ব্যাংকিং বাদ হয়ে এসেছে এমএফএস। আর্থিক লেনদেনের ক্ষেত্রে সবসময় সবকিছু চেক করে নেবেন। কোথাও টাকা পাঠানোর ক্ষেত্রেও সবকিছু নিশ্চিত হয়ে

দিবেন। আপনার পেমেন্টের প্রতিটি ইনফরমেশন এবং ট্রানজেকশনের মেসেজ সংরক্ষণ করুন। আবার অনেকের আইডি হ্যাক হওয়ার পর হ্যাকাররা পরিচিতদের কাছে টাকা চায়। আপনার সাথে এমন কিছু হলে যে ব্যক্তির আইডি তার সাথে যোগাযোগ করে নিশ্চিত হোন বিষয়টি। লেনদেনের ক্ষেত্রে সবসময় প্রমাণ ও ট্র্যাকিং প্রমাণ রাখবেন।

একাধিক যন্ত্রে লগিন দেবেন না
একাধিক যন্ত্রে লগিন দিয়ে রাখবেন না। আমরা সচরাচর সবকিছু সহজ রাখতে এমনটাই করি। আবার অফিসের ডিভাইসেও এমনটা করে থাকি। এই কাজ করবেন না। অপরিচিত কোনো ব্রাউজারে যদি প্রবেশ করেন তাহলে ব্রাউজারে ইনকগনিটো চালু করে নেবেন। এতে আপনার সব তথ্য আর রেকর্ড হবে না ব্রাউজারে। এতে আপনার ব্রাউজিং নিরাপদ থাকবে। তাই সহজ হবে অনলাইনে আপনার বিচরণ।

এছাড়া আরও কিছু নিরাপত্তা কৌশল আছে। অনেকে ফোনে এন্টিভাইরাস ব্যবহার করেন। এমনটার প্রয়োজন নেই। একথা সত্য আজকাল কিছু স্মার্টফোনের সফটওয়ারে প্রচুর বিজ্ঞাপন দেখায়। তবে সেটা সফটওয়ারের কারণে হয়। ফোন কেনার আগে জেনেবুঝে কিনুন। একথা মনে রাখতে হবে। অনলাইনে তথ্য খুব মূল্যবান। তথ্যের মাধ্যমে অনেক কিছুই করা যায়। তাই সবসময় সতর্ক থাকতে হবে। কাজগুলো কঠিন কিছুই নয়। একটু সবদিক বিবেচনা করতে হবে

বাজারে এলো ৫টি ফিচার ফোন

একটা সময় ছিল, যখন প্রায় সবার হাতেই ঘুরতো নানা ব্র্যান্ড ও মডেলের ফিচার ফোন। বিভিন্ন লুকের এসব ফোন সবার কাছে অত্যন্ত প্রয়োজনীয় ছিল। তবে গত ১০ বছরে সবকিছু বদলে গিয়েছে। এখন সবার হাতে হাতে ঘুরছে সর্বোচ্চ প্রযুক্তির স্মার্টফোন।

তবে এখনো অনেকেই ফিচার ফোন ব্যবহার করেন। প্রায় প্রতিটি মোবাইল ফোন উৎপাদনকারী ব্র্যান্ডেরই রয়েছে বিভিন্ন মডেলের ফিচার ফোন। সাশ্রয়ী দাম ও বেশি সময় চার্জ থাকাই মূলত ফিচার ফোনের জনপ্রিয়তার কারণ। বিক্রয় ডট কম-এর মতো অনলাইন মার্কেটপ্লেসসহ বিভিন্ন শো-রুমে নানা মডেলের এসব ফিচার ফোন

পাওয়া যাচ্ছে। চলুন দেখে নেওয়া যাক এসব ফিচার ফোনগুলো সম্পর্কে বিস্তারিত।

সিম্ফনি এল৩৩
দেশের মোবাইল মার্কেটে সিম্ফনি বেশ জনপ্রিয় একটি ব্র্যান্ড। তাদের মোবাইলগুলো যেমন নির্ভরযোগ্য তেমনি সিম্ফনি ব্যবহারকারীদের জন্য সাধ্যমতো দামে দারুণ সব ফিচার অফার করে।

২০২১ সালের নভেম্বরে তারা বাজারে আনে সিম্ফনি এল৩৩ মোবাইলটি। বর্তমানে এই মডেলের ফিচার ফোনটি আকর্ষণীয় ডিজাইন ও দু’টি ভিন্ন কালার অপশনে পাওয়া যাচ্ছে।

সিম্ফনি এল৩৩ মোবাইলটির বর্তমান দাম বাংলাদেশে ১ হাজার ৩৫০ টাকা।

এনার্জাইজার ই২৮২এসসি
আমাদের মধ্যে অনেকেই এনার্জাইজার ব্র্যান্ডকে তাদের দীর্ঘস্থায়ী ব্যাটারির জন্য চিনে থাকি। কিন্তু ব্যবহারকারীদের অন্যান্য চাহিদার কথা মাথায় রেখে তারা বেশ কিছু মানসম্মত মোবাইল ফোনও মার্কেটে নিয়ে এসেছে। যার মধ্যে ২০২১ সালের ডিসেম্বরে রিলিজ পাওয়া একটি মডেল হচ্ছে এনার্জাইজার ই২৮২এসসি। দুই রঙা এই ফ্লিপ মোবাইলটিতে রয়েছে ৪জি নেটওয়ার্ক সাপোর্ট।

এনার্জাইজার ই২৮২এসসি মোবাইলটির বর্তমান দাম বাংলাদেশে ৮ হাজার টাকা।

ওয়ালটন অলভিও এল২৮এস
দেশের এক অন্যতম সেরা লোকাল ব্র্যান্ড ওয়ালটন। আপনার ঘরকে স্মার্ট হোম বানাতে যতরকম ইলেকট্রনিক্স পণ্যের প্রয়োজন, সব কিছুই পাবেন ওয়ালটন-এর কাছে। সাশ্রয়ী দামের রেঞ্জে তারা দারুণ সব ব্যবহার-উপযোগী ফিচার মোবাইল মার্কেটে লঞ্চ করে থাকে প্রতিনিয়ত। ২০২২ সালের এপ্রিলে আকর্ষণীয় ও উজ্জ্বল বেশ কিছু কালার অপশন নিয়ে ওয়ালটনের অলভিও এল২৮এস মোবাইলটি লঞ্চ করা হয়।

ওয়ালটন অলভিও এল২৮এস মোবাইলটির বর্তমান দাম বাংলাদেশে ১ হাজার ৩০০ টাকা।

আইটেল ম্যাজিক ৩
আইটেল চাইনিজ একটি প্রযুক্তি প্রতিষ্ঠান, যারা মূলত অল্প কিছু

দেশে তাদের মোবাইল ফোনগুলো দারুণ সাশ্রয়ী দামে বিক্রি করে থাকে। তাদের ফোন গুলোর মধ্যে বেশ জনপ্রিয় একটি মডেল হচ্ছে আইটেল ম্যাজিক ৩। আকর্ষণীয় লুকের এই ফিচার মোবাইলটি লঞ্চ করা হয় ২০২২ সালের জানুয়ারি মাসে।

আইটেল ম্যাজিক ৩ মোবাইলটির বর্তমান দাম বাংলাদেশে ২ হাজার ১৯০ টাকা।

নকিয়া ২৭৬০ ফ্লিপ
জনপ্রিয়তা এবং ব্যবহারকারীদের কথা মাথায় রেখে এই বছরেই নকিয়া তাদের ‘নকিয়া ২৭৬০ ফ্লিপ’ মোবাইলটি নতুন রূপে পুনরায় লঞ্চ করতে যাচ্ছে। মোবাইলটিতে আমরা দেখতে পাবো দারুণ একটি আউটলুক এবং আধুনিক বিভিন্ন ফিচার।

নকিয়া ২৭৬০ ফ্লিপ মোবাইলটির নতুন ভার্সন এই বছরের আগস্ট মাসে লঞ্চ হবে আশা করা যাচ্ছে। মোবাইলটির দাম অনুমান করা হচ্ছে বাংলাদেশে ৬ হাজার ২৫০ টাকা মাত্র।

সাইবার হামলায় নাকাল দেশের শীর্ষ ৩ প্রযুক্তি প্রতিষ্ঠান: ঝুঁকিতে টেলিকম

গত কয়েক মাস ধরেই বাংলাদেশের বিভিন্ন প্রতিষ্ঠান র্যানসামওয়্যার আক্রমণের শিকার হচ্ছে। আক্রমণের শিকার হয়েছে বেক্সিমকো, আকিজ এবং ডিজিকন টেকনোলজিস এর মতো বড় বড় বাণিজ্যিক প্রতিষ্ঠান।

প্রতিষ্ঠানগুলোতে হামলার মাধ্যমে হ্যাকাররা হাতিয়ে নিয়েছে স্পর্শকাতর অনেক তথ্য। আক্রমণের ঝুঁকির তালিকায় শীর্ষে রয়েছে বিটিসিএল, গ্রামীণফোন লিমিটেড, আজিয়াটা লিমিটেড, লিংক থ্রি টেকনোলজিস, সিস্টেমস সল্যুশনস অ্যান্ড ডেভেলপমেন্ট টেকনোলজিস লিমিটেড, বন্ধু নেটওয়ার্ক লিমিটেড, আমরা নেটওয়ার্ক লিমিটেড, বাংলালিংক ডিজিটাল কমিউনিকেশনস লিমিটেড এবং টেলিটক বাংলাদেশ

লিমিটেড।

বাংলাদেশের সাইবার পরিস্থিতি ও র্যানসমওয়্যার পরিস্থিতি নিয়ে প্রকাশিত গবেষণা প্রতিবেদন ‘র্যানসমওয়্যার ল্যান্ডস্কেপ বাংলাদেশ ২০২২’ থেকে এসব তথ্য পাওয়া গেছে। প্রতিবেদনটি প্রকাশ করেছে সরকারের সাইবার নিরাপত্তা নিয়ে কাজ করা প্রতিষ্ঠান বিজিডি ই-গভ সার্ট।

সরকারের তথ্য ও যোগাযোগপ্রযুক্তি বিভাগের অধীন সাইবার নিরাপত্তা নিয়ে কাজ করা সংস্থা বিজিডি ই-গভ সার্ট বাংলাদেশের সাইবার পরিস্থিতি ও র্যানসামওয়্যার পরিস্থিতি নিয়ে গবেষণা করেছে। তারা ‘র্যানসামওয়্যার ল্যান্ডস্কেপ বাংলাদেশ ২০২২’ নামে একটি প্রতিবেদন প্রকাশ করেছে। সার্ট ডার্ক ওয়েব মনিটরিং, ওএসআইএনটি (ওপেন-সোর্স থ্রেট ইন্টেলিজেন্স) থেকে বাংলাদেশে র্যানসমওয়্যার আক্রমণ সম্পর্কে প্রাসঙ্গিক তথ্য সংগ্রহ করেছে । তারা ২০২১ সাল থেকে এ পর্যন্ত পাওয়া বিভিন্ন তথ্য পর্যালোচনা করে এ প্রতিবেদনটি তৈরি করেছে।

বাংলাদেশে ২০২১ সাল থেকে এখন পর্যন্ত ৪টি র্যানসামওয়্যার আক্রমণের তথ্য পাওয়া গেছে বলে জানিয়েছে সার্ট। এর মধ্যে তিনটি বেসরকারি প্রতিষ্ঠানের কথা উল্লেখ করেছে তারা। এশিয়া প্যাসিফিক অঞ্চলে সবচেয়ে বেশি র্যানসামওয়্যার আক্রমণের শিকার হয় ভারত। এরপর আছে জাপান, থাইল্যান্ড, চায়না, তাইওয়ান।

ক্যাসপারস্কি সিকিউরিটি বুলেটিন ২০২১ সালের তথ্য দিয়ে সার্ট বলেছে, বাংলাদেশ অন্য যেকোনো দেশের তুলনায় র্যানসমওয়্যার ট্রোজান দ্বারা সবচেয়ে বেশি আক্রমণের শিকার।

বাংলাদেশের অন্যতম শীর্ষ ব্যবসা প্রতিষ্ঠান আকিজ গ্রুপ নাইট স্কাই নামক র্যানসামওয়্যার দ্বারা আক্রমণের শিকার হয়। প্রতিষ্ঠানটির সার্ভারের সমস্ত ফাইল, কর্মীদের জীবনবৃত্তান্ত, মেইল সার্ভার ডেটা, গিটল্যাব কোড বেস, ইআরপি সিস্টেম ডেটাবেস, ব্যাকআপ সহ সমস্ত ওয়েবসাইট সিপ্যানেল ডেটা, ব্যক্তিগত কম্পিউটার ব্যাকআপ ফাইলও ডার্ক ওয়েবে ফাঁস হয়ে যায়।

দেশের আরেক শীর্ষ ব্যবসা প্রতিষ্ঠান বেক্সিমকো গ্রুপ অ্যাল্টডোস নামক র্যানসামওয়্যার আক্রমণের শিকার হয়। তাদের ৩৪টি ওয়েবসাইট থেকে শত শত গিগাবাইট ফাইল, ডেটাবেস, তাদের টেলিকম ভর্তুকি, ৫৬ হাজার পেমেন্ট রেকর্ডসহ বিভিন্ন তথ্য ফাঁস হয়েছে।

তথ্য প্রযুক্তি বিষয়ক প্রতিষ্ঠান ডিজিকন টেকনোলজিস রাশিয়াভিত্তিক কন্টি গ্রুপ যা উইজার্ড স্পাইডার ছদ্মনামে চলে, তাদের দ্বারা আক্রমণের শিকার হয়েছে।

সার্ট সম্ভাব্য র্যানসামওয়্যার আক্রমণের চেইনের সঙ্গে যুক্ত ম্যালওয়্যারের ধরণগুলোও তুলে ধরেছে। ২০২১ সাল থেকে বাংলাদেশ থেকে ১৪ হাজার ৬২৭টি আইপি ঠিকানা ম্যালওয়্যার দ্বারা সংক্রমিত বলে তথ্য পাওয়া গেছে। যার দ্বারা সম্ভাব্য র্যানসামওয়্যারের আক্রমণের ঝুঁকি ছিল।

অটোনোমাস সিস্টেম নম্বর (এএসএন) এর মধ্যে এক বা একাধিক নেটওয়ার্ক অপারেটর পরিচালিত হয়। সার্ট এর প্রতিবেদন অনুযায়ী, বাংলাদেশে প্রায় ৬১২ জন এএসএনধারী সম্ভাব্য র্যানসমওয়্যার আক্রমণের ঝুঁকিতে আছে। যাদের সংক্রমণের এক হাজারের বেশি রেকর্ড রয়েছে তাদের নাম উল্লেখ করেছে সার্ট। শীর্ষ ১০ সম্ভাব্য ঝুঁকিতে থাকা এএসএনধারী হচ্ছে, বাংলাদেশ টেলিগ্রাফ ও টেলিফোন বোর্ড যা এখন বিটিসিএল নামে পরিচিত, গ্রামীণফোন লিমিটেড, আজিয়াটা লিমিটেড, লিংকথ্রি টেকনোলজিস, সিস্টেমস সল্যুশনস অ্যান্ড ডেভেলপমেন্ট টেকনোলজিস লিমিটেড, বন্ধু নেটওয়ার্ক লিমিটেড, আমরা নেটওয়ার্ক লিমিটেড, বাংলালিংক ডিজিটাল কমিউনিকেশনস লিমিটেড এবং টেলিটক বাংলাদেশ লিমিটেড।

বেক্সিমকো-আকিজের তথ্য নিয়ে গেছে হ্যাকাররা

বেক্সিমকো, আকিজ এবং ডিজিকন টেকনোলজিসের এর মতো বড় বড় প্রতিষ্ঠানে সাইবার হামলার মাধ্যমে হ্যাকাররা এসব প্রতিষ্ঠান থেকে অনেক তথ্য হাতিয়ে নিয়েছে। বাংলাদেশের সাইবার পরিস্থিতি ও র্যানসমওয়্যার পরিস্থিতি নিয়ে প্রকাশিত গবেষণা প্রতিবেদন ‘র্যানসমওয়্যার ল্যান্ডস্কেপ বাংলাদেশ ২০২২’ থেকে এসব তথ্য পাওয়া গেছে।

প্রতিবেদনটি প্রকাশ করেছে সরকারের সাইবার নিরাপত্তা নিয়ে কাজ করা

গুগল ক্রোমে হ্যাকার থেকে সাবধান

গুগল ক্রোম বর্তমান বিশ্বের সবচেয়ে জনপ্রিয় ওয়েব ব্রাউজার। মোবাইল কিংবা কম্পিউটার সব ধরনের ডিভাইসেই এই ব্রাউজার ব্যবহৃত হয়। গুগল ক্রোম দিয়ে অন্যান্য অনেক প্লাগিন বা সুবিধা ব্যবহার করা যায়। সম্প্রতি এইসব জটিলতার মধ্যে সাইবার অপরাধীদের তৎপরতা বাড়তে শুরু করেছে। ব্যবহারকারীদের তথ্য চুরির ঘটনা অহরহই ঘটছে।

ক্রোমের সুরক্ষা নিয়েও বেশকিছু গাফলতির তথ্য সম্প্রতি সামনে এসেছে। যখন থেকেই ওয়েব ব্রাউজার ব্যবহারে সতর্কতার বিষয়ে সতর্কবার্তা জারি করেছেন বিশেষজ্ঞরা। যেহেতু গুগল ক্রোম এখনো বেটা ভার্সনে আছে তাই ব্যবহারকারীদের অপেক্ষা করতে হয় আপডেটের জন্য।

ক্রোম
ই-মেইলে আসা অপরিচিত কারো লিংকে নিশ্চিত না হয়ে প্রবেশ করবেন না তাই বলে কি হ্যাকার থেকে বাঁচার উপায় নেই? আছে তো অবশ্যই। নিজের নিরাপত্তা নিশ্চিতে যা করতে পারেন:

ব্রাউজার নিয়মিত রিফ্রেশ করবেন। এছাড়াও ব্রাউজারের কুকি কিছুক্ষণ পরপর পরিষ্কার করুন।
ক্রোম ব্রাউজার নিয়মিত আপডেট দিন। এতে পূর্ববর্তী ভার্সনের বাগগুলো ঠিক হয়ে যাবে।
গুগল ক্রোমে পাসওয়ার্ড সংরক্ষণের সুযোগ থাকলেও করবেন না। ক্রোম ব্রাউজারের সার্চ বক্সে যেকোনো লিংকে ঢুকবেন না। হ্যাকারদের পাতা ফাঁদ হতে পারে।
পাবলিক ওয়াইফাই ব্যবহার করবেন না। অনিরাপদ নেটওয়ার্কের জন্যেও ডিভাইস হ্যাক হতে পারে।
কম্পিউটারে এন্টিভাইরাস ইন্সটল করুন।
ই-মেইলে আসা অপরিচিত কারো লিংকে নিশ্চিত না হয়ে প্রবেশ করবেন না।

এআর-ভিআর প্রযুক্তির মিশেলে হেডসেট তৈরি করছে অ্যাপল

ভিআর (ভার্চ্যুয়াল রিয়েলিটি) এবং এআর (অগমেন্টেড রিয়েলিটি) প্রযুক্তির সংমিশ্রণে হেডসেট তৈরি করছে অ্যাপল। তা–ও আবার একটি নয়, তিনটি মডেলের হেডসেট বাজারের আনতে কাজ করছে প্রতিষ্ঠানটি। তবে হেডসেটগুলোর মডেল এবং কার্যকারিতা সম্পর্কে আনুষ্ঠানিক কোনো মন্তব্য করেনি অ্যাপল।

ব্লুমবার্গের এক প্রতিবেদনে বলা হয়েছে, অ্যাপলের হেডসেট তৈরির কার্যক্রম এখনো প্রাথমিক পর্যায়ে রয়েছে। এন ৩০১, এন ৬০২ এবং এন ৪২১ কোড নামের হেডসেটগুলোতে একই সঙ্গে ভার্চ্যুয়াল রিয়েলিটি এবং অগমেন্টেড রিয়েলিটির ছবি দেখা যাবে। শুরুতে এন ৩০১ কোড নামের হেডসেটটি উন্মুক্ত করা হতে পারে।

‘অ্যাপল রিয়েলিটি প্রো’ নামে বাজারে আসতে যাওয়া হেডসেটটি ফেসবুকের ‘কুইস্ট প্রো’ হেডসেটের সঙ্গে প্রতিদ্বন্দ্বিতা করতে সক্ষম হবে বলে ধারণা করা হচ্ছে। আগামী বছরের জানুয়ারি মাসে নিজেদের তৈরি প্রথম হেডসেট বাজারে আনতে পারে অ্যাপল। দুটি ফোরকে প্রযুক্তির মাইক্রো ওএলইডি ডিসপ্লে সুবিধার হেডসেটটি ব্যবহারকারীর চোখের নড়াচড়া শনাক্ত করে ভিডিও প্রদর্শন করতে পারবে।

সূত্র: টাইমস অব ইন্ডিয়া

হ্যাক হওয়ার দাবি অস্বীকার করল টিকটক

সপ্তাহখানেক আগেই টিকটকের অ্যান্ড্রয়েড অ্যাপে ভয়ংকর নিরাপত্তা ত্রুটির সন্ধান পেয়েছিলেন মাইক্রোসফটের একদল গবেষক। এ ত্রুটি কাজে লাগিয়ে হ্যাকাররা খুব সহজেই ব্যবহারকারীদের অ্যাকাউন্ট

নিজেদের দখলে নিতে পারতেন।

বিষয়টি টিকটক কর্তৃপক্ষকে জানানোর পর তারা দ্রুত নিরাপত্তা ত্রুটির সমাধান করে। ফলে লাখ লাখ টিকটক ব্যবহারকারী সাইবার হামলা থেকে রক্ষা পায়। এবার ‘অ্যাগেইন্সটদ্যওয়েস্ট’ নামেরএকদল হ্যাকার দাবি করেছেন, তাঁরা টিকটক হ্যাক করে ব্যবহারকারীদের তথ্য এবং অ্যাপের সোর্স কোড সংগ্রহ করেছেন। কিন্তু হ্যাকারদের এ দাবি অস্বীকার করেছে টিকটক কর্তৃপক্ষ।

প্রযুক্তিবিষয়ক ওয়েবসাইট ব্লিপিং কম্পিউটারের তথ্যমতে, সম্প্রতি একদল হ্যাকার সাইবার হামলা চালিয়ে টিকটকের তথ্যভান্ডারে থাকা তথ্য সংগ্রহ করার পাশাপাশি সেগুলোর ছবি হ্যাকারদের ফোরামে প্রদর্শন করেছেন। হ্যাকারদের দাবি, তাঁরা টিকটকের ৭৯০ গিগাবাইট তথ্য চুরি করেছে যার মধ্যে ব্যবহারকারী ও কোডসহ বিভিন্ন গুরুত্বপূর্ণ তথ্য রয়েছে। হ্যাক হওয়ার ঘটনা অস্বীকার করে টিকটকের এক মুখপাত্র জানিয়েছেন, টিকটকে নিরাপত্তা ত্রুটির কোনো প্রমাণ পাওয়া যায়নি।

যেসব তথ্য পোস্ট করা হয়েছে, সেগুলো ব্যবহারকারীদের সাধারণ তথ্য, যা সবাই দেখতে পারেন। আমরা নিশ্চিত হয়েছি টিকটকের সিস্টেম, নেটওয়ার্ক বা তথ্যভান্ডারে সাইবার হামলা চালিয়ে তথ্যগুলো সংগ্রহ করা হয়নি। আর তাই ব্যবহারকারীদের নিরাপত্তা বৃদ্ধির জন্য কোনো উদ্যোগ নিতে হবে না। ছোট আকারের ভিডিও সহজে তৈরি ও বিনিময়ের সুযোগ থাকায় তরুণ-তরুণীদের কাছে বর্তমানে খুবই জনপ্রিয় টিকটক। এই অ্যাপের জন্য মজার ভিডিও তৈরি করে তারকাও বনে গেছেন অনেকে। এরই মধ্যে গুগল প্লে স্টোর থেকে ১০০ কোটিরও বেশিবার নামানো হয়েছে টিকটক অ্যাপ।

স্মার্টফোন ফাস্ট করবেন যেভাবে

স্মার্টফোনের বাজারে এখন যে উত্তাপ ছড়াচ্ছে, সে সময় অনেকেই আর নতুন ফোন কেনার ব্যাপারে আগ্রহী হতে পারছেন না। প্রতি বছরই নতুন

মডেলের, আরও উন্নত প্রসেসর নিয়ে বাজারে আসছে স্মার্টফোন। এমনকি ফোনের পেছনে বিনিয়োগের পরিমাণটাও এখন কম নয়।

স্মার্টফোনের পেছনে টাকা খরচ করার পর অনেকেই আশা করেন ফোন দীর্ঘস্থায়ী হবে। দামি ফোনগুলোতে সচরাচর বড় সমস্যা দেখা যায় না। কোম্পানিগুলো সচরাচর ফ্ল্যাগশিপ ফোন বানানোর সময় সফটওয়ার ও হার্ডওয়ারে যথেষ্ট গুরুত্ব দিয়ে থাকে। তাদের ওতটা সমস্যা হয় না। কিন্তু যারা কম দামে কিংবা মিডরেঞ্জে ফোন কেনেন, তাদেরই যত অসুবিধে। অনেকে তো পুরনো স্মার্টফোনও কিনে নেন। অনেক সময় অনেক ছোট ছোট কারণে এসব ফোন ধীরগতির হয়ে যায়।

ইউটিউবে ‘মিস্টার হুজ দ্য বস’ নামে ইউটিউব চ্যানেলের উপস্থাপক অরুন কদিন আগেই তার একটি ভিডিওতে জানান, ফ্ল্যাগশিপ বানানোর সময় কোম্পানিগুলো মিডরেঞ্জে কিছু সমস্যা দিয়েই রাখে। এতে ফ্ল্যাগশিপ ফোন বিক্রি করতে পারে তারা। তবে আপনার জন্যে ফ্ল্যাগশিপ মডেল অনেক ভালো হলেও টাকার অভাবে তা সম্ভব নয়। সেজন্যে আপনার জন্যে রইলো কিছু টিপস, যা দিয়ে সহজেই ফোনকে কিছুটা ইন্টার্যাক্টিভ করা সহজ হবে:
সিস্টেম আপডেট করুন
আজকাল প্রতিটি ফোন কোম্পানিই নিজস্ব ইন্টারফেস ব্যবহার করে। সময়ে সময়ে তারা সিস্টেম আপডেট দেয়, নতুন ফিচার যেন ইউজাররা উপভোগ করতে পারেন। তাই ফোন স্লো হয়ে গেলে সিস্টেম আপডেট দিয়ে দেখুন। অবশ্য বেশ কদিন ধরে কিছু কোম্পানির ফোনে সিস্টেম আপডেট দেওয়ার পর নানা সমস্যা পাওয়া গেছে। তাই আগে ফোরামগুলোতে গিয়ে আপডেটটির রিভিউ জেনে নিন। তাতে নিরাপদেই আপডেট দিতে পারবেন। যদি রিভিউতে বাগের তথ্য পান, তাহলে দেওয়ার প্রয়োজন নেই।

ব্যাটারির যত্নে মনোযোগ দিন
মোবাইল চালানোর সময় সফটওয়ার যতটা জরুরি ব্যাটারিও ততটাই জরুরি। বিশেষত মোবাইল চার্জ দেওয়ার সময় ফোন চালাবেন না। এমনকি ফোন সব সময় ফুল চার্জ করা অথবা একেবারে চার্জ শেষ করা ঠিক না। ব্যাটারি উৎপাদনের সময় ঠিক কতবার ফুল চার্জ হওয়ার সক্ষমতা রাখে তা নির্ধারিত থাকে। ঘন ঘন ফুল চার্জ দিলে ব্যাটারির ক্ষতি হয়। সারারাত ফোন চার্জে রাখবেন না। সচরাচর চার্জ ৯০ শতাংশ হলেই চার্জ থেকে খুলে নিন ও ২০ শতাংশে কমে এলে চার্জে দিন। বাইরে থাকলে পাওয়ার ব্যাংক রাখুন।

ব্লোটওয়ার সরান

মোবাইল রিসেট দেওয়ার পর কিংবা নতুন কেনার পর সবসময় কিছু অ্যাপ থাকে যা আপনার কাজে আসে না। এদের বলা হয় ব্লোটওয়ার। মূলত স্মার্টফোন কোম্পানিগুলো অতিরিক্ত আয়ের জন্যে কিছু গেমস বা অতিরিক্ত অ্যাপ দিয়ে থাকে। কিছু কিছু অ্যাপ আন-ইনস্টল করা যায় আবার কিছু কিছু অ্যাপ আন-ইনস্টল করাই যায় না। যেগুলো আন-ইনস্টল করা যায়, সেগুলো দ্রুত সরিয়ে ফেলুন। এমনকি মোবাইলে অপ্রয়োজনীয় অ্যাপ রাখবেনই না।

সিস্টেম স্টোরেজ ফুল করবেন না
আজকাল মোবাইলের সিস্টেম স্টোরেজ ব্যবহার করেন অনেকে। কারণ ফোনের সিস্টেম স্টোরেজের জায়গাও নেহাৎ কম থাকে না। তবে স্টোরেজ বেশি হলেও আজকাল ফাইলও বেশ বড় হয়। দেখা যায় দ্রুত সিস্টেম স্টোরেজ ভরাট হয়ে যাচ্ছে। এমন অবস্থায় সিস্টেম স্টোরেজ কখনই ৯০ শতাংশের বেশি ভরবেন না। বাজারে এসডি কার্ড পাওয়া যায় তা ব্যবহার করতে পারেন। তবে এসডি কার্ডের ক্ষেত্রে ক্লাস টেন কি না, তা দেখে নিন। নকল বা সাধারণ এসডি কার্ড ফোন আরও স্লো করে দেয়।

অ্যাপ্লিকেশন ক্যাশ সাফ করুন
আপনার ফোনে ক্যাশ ফাইল জমে খেয়াল করবেন হয়তো। অনেকে নামটিই শুনলেও কোথায় আছে জানেন না। মূলত ক্যাশ ফাইল হলো ইন্টারনেট ব্যবহারের সময় ফোনে ব্রাউজার থেকে জমা হওয়া কিছু ফাইল। শুধু ডেভেলপাররাই এই ফাইলগুলোর সঠিক ব্যবহার করতে পারে। আপনার তেমন কাজে আসে না। প্রায় প্রতিটি অ্যাপ বিশেষত গুগলের ইউটিউব, জিমেইল, ফেসবুক ও ভারি গেমের অ্যাপ ক্যাশ জমা করে। এসব অ্যাপ্লিকেশন ক্যাশ ফাইল আপনার ফোনকে স্লো বানিয়ে দেয়। সিস্টেম স্টোরেজে গেলে সহজেই এই ক্যাশ ফাইল দূর করতে পারবেন। অনেকে অবশ্য অ্যাপের মাধ্যমেই এই কাজ করেন। তবে আমাদের অভিজ্ঞতা বলে, সিস্টেম অ্যাপ ব্যবহারেই ক্যাশ সরানো উচিত।

এপ্লিকেশনকে যত্রযত্র পারমিশন দেবেন না
ফোনে নতুন অ্যাপ ইনস্টল করার পরই নানা পারমিশন চেয়ে বসে। এতে আপনার প্রাইভেসি যেমন ঝুঁকির মধ্যে থাকে, তেমনই ব্যাটারির চার্জও কমে যায়। এছাড়া ফোন হয়ে যায় স্লো। কারণ সিস্টেম ডাটা এই পারমিশনগুলো সবসময় দেয় বলে অ্যাপগুলো ব্যাকগ্রাউন্ডে চালু থাকে। সৌভাগ্যের কথা হলো এন্ড্রয়েডের নতুন সংস্করণে আপনি যখন অ্যাপ ব্যবহার করবেন, তখনই পারমিশন কার্যকর হবে, এমন সেটিং চালু আছে। অ্যাপ ইনস্টল করে তাই ভেবেচিন্তে পার্মিশন দিন।

সবসময় ডাটা ও ওয়াই ফাই চালু রাখবেন না
ফোনে সবসময় ডাটা বা ওয়াইফাই চালু রাখবেন না। যখন প্রয়োজন হবে তখনই এদের ব্যবহার করুন। এছাড়াও ব্যাকগ্রাউন্ড ডাটা নিষ্ক্রিয় রাখুন। তাতে ফোন স্লো হবে না।

বিজ্ঞাপন দেয় এমন অ্যাপ রাখবেন না
আজকাল কমদামি ফোন কিংবা মিডরেঞ্জ অনেক কোম্পানির ফোনে বিজ্ঞাপনে অতিষ্ঠ হওয়ার জো। রুচি ও মানের দিক থেকে যেমন এই বিজ্ঞাপনগুলো নিম্নমানের তেমনি ফোন স্লো করার পেছনেও এদের হাত আছে। অবশ্য স্মার্টফোন কোম্পানির দেওয়া রমে বিজ্ঞাপন পুরোপুরি থামানো সম্ভব না হলেও অ্যাপের কিছু পার্মিশন বন্ধ করে বিজ্ঞাপন থেকে কিছুটা রেহাই মিলবে। এছাড়াও এমন অ্যাপ ব্যবহার করবেন না যেগুলো প্রচুর বিজ্ঞাপন দেখায়। যদি ফোনের রমে সমস্যা থেকেই থাকে, তাহলে কাস্টম রম বা স্টক এন্ড্রয়েড ব্যবহার করুন।

ফ্যাক্টরি ডাটা রিসেট
ফোনের অবস্থা যদি একদমই বাজে হয়, তাহলে ফ্যাক্টরি ডাটা রিসেট ছাড়া উপায় নেই। এতে ফোন আবার প্রাথমিক অবস্থায় যেমন ছিল তেমন হয়ে যাবে। ফ্যাক্টরি রিসেট দেওয়ার পর আমাদের দেওয়া টিপসগুলো মেনে চললে আপনার ফোন নিয়ে বড় সমস্যায় পড়বেন না। স্মার্টফোন স্লো হওয়ার জন্যে অনেকাংশে কোম্পানির সফটওয়ার দায়ী হলেও আপনাকে কিছুটা সচেতন হয়েই চালাতে হবে।