সচেতনতা

CYBER SECURITY

SAFETY FIRST

ISLAMIC CYBER SECURITY

ICS

WE PROTECT ISLAM

সাইফুল ইসলাম

সাইবার সিকিউরিটি

সাইফুল ইসলাম

“

নিশ্চয়ই আমার সালাত, আমার কুরবানি, আমার জীবন এবং আমার মরণ সবকিছু কেবল বিশ্বজগতের প্রতিপালক আল্লাহ তায়ালার জন্য।

“

সূচি

সাইবার সিকিউরিটি কী? ১০

ভয় নেই। এটা আপনার সহযোগী ১৭

সতর্কতা ১৮

পাসওয়ার্ড ভুলে গেছেন। তারপর.. ২১

ফিশিং; সতর্ক হোন ২৪

কপিরাইট; অজান্তে গায়েব হবে আপনার আইডি ২৫

ফেইসবুক Suspected একাউন্ট ২৮

ইমো কনভার্সেশন ৩১

ভিন্ন কিছু ৩৩

ফেইসবুক একাউন্ট ডিজেবল কতভাবে ৩৫

অডিও রেকর্ড এড়ানোর পাঁচটি উপায় ৩৯

ICS কে নিয়ে এক ভাইয়ের অভিযোগ, আমার জবাব ৪৩

আনলক হতে পারে আপনার একাউন্ট ৫৪

যেভাবে কাজ করে আপনার ফেসবুক নিউজফিড ৫৭

Two Factor Authentication সমস্যা,

একটি পরামর্শ ৬১

Facebook-এ "GG" এর মানে কি? ৬২

হ্যাকারদের হাত থেকে কিভাবে আপনার ফেসবুক অ্যাকাউন্ট রক্ষা করবেন ৬৫

আইডির রিচ; কিছু কথা ৭১

আইডি সেফটি ৭৬

ফেসবুকের সার্ভার ডাউন থাকলে বুঝবেন কীভাবে? ৭৭

পাসওয়ার্ড ভুলে না যাওয়ার সহজ সমাধান ৮১

ইন্টারনেটের ব্যান্ডউইথ চুরি হয় যেভাবে ৮৪

ফেসবুকের সাহায্যেই 'ফেসবুক ব্যবহার নিয়ন্ত্রণ' করবেন যেভাবে ৮৭

ফেইসবুক হ্যাক, কার্যকর পদ্ধতি ৯১

ফেইসবুক মেসেঞ্জার ব্যাবহার করছেন? ৯৯

হ্যাকিং রোধে ফেসবুকের নতুন ফিচার। ১০৩

লিংকে ক্লিক বা কল রিসিভ না করলেও ফোনে পেগাসাস ঢোকে কীভাবে? ১০৬

Zero-Click Hacks: কীভাবে হ্যাক করে এই স্পাইওয়্যার ? এটা কতটা ভয়ঙ্কর ? ১১৩

স্পাইওয়্যার থেকে ফোনের সুরক্ষা ১১৯

বিশ্বের ভয়ঙ্কর ৫ হ্যাকার ১২৬

হ্যাক হয়েছে কিনা কীভাবে বুঝবেন? হ্যাক হলে কী করণীয় জানুন। ১৩৪

জিমেইলের ব্যাপারে সাবধান ১৪১

সাইবার বুলিং ও আমাদের করণীয় ১৪২

ফেসবুকে যেসব কাজ করতে মানা। ১৪৭

স্মার্টফোন হ্যাক হওয়ার লক্ষণ ও করণীয় ১৫৬

স্মার্টফোন হ্যাক হলে কী করবেন? ১৬২

ফেসবুক স্ট্যাটাস: পিকচার বা স্টিকার কমেন্ট আইডি বাঁচাতে পারে? ১৬৭

২০ সেকেন্ড - ১৭৩

-প্রথম কথা

আধুনিক তথ্য প্রযুক্তির যুগে পুরো দমে মজে আছে আমাদের মন মস্তিষ্ক অনলাইনে। সেখানে আমাদের বেশিরভাগ সময় ব্যয় হচ্ছে ফেইসবুকে। ফেইসবুক এখন আমাদের মূল্যবান জীবনের একটি অংশ। ফেসবুক ব্যবহারকারীর সংখ্যা ২৫০ কোটি ছাড়িয়েছে। ২০১৯ সালের শেষ প্রান্তিকে ফেসবুক ব্যবহারকারীর সংখ্যা ২৪৫ থেকে বেড়ে ২৫০ কোটিতে পৌঁছায়। ২০১৯ সালের জানুয়ারিতে বাংলাদেশে ৩১৩১৩০০০ ফেসবুক ব্যবহারকারী ছিলেন, যা এর সমগ্র জনসংখ্যার ১৯.৯% ছিল। ২১ সালের নভেম্বরে এসে দাঁড়িয়েছে প্রায় ৫ কোটি ২০ লাখ।

আমরা কমবেশি ফেইসবুকে ব্যাক্তিগত তথ্য শেয়ার করে থাকি। দুঃখজনক হলো ফেইসবুক থেকেও তথ্য চুরি হচ্ছে। ২০১১ সালে ফেসবুক নিজেই তথ্য বিক্রি করেছে বলে দাবি উঠেছিল। মার্কিনরা এই অভিযোগ করলে ফেসবুক বাধ্য হয়ে জরিমানা দেয়। তারপর ২০১৯ সালের আগের ঘটনা। তথ্য বিশ্লেষণকারীরা জানাচ্ছেন, এই ডেটাবেজ-এ ১০৬টি দেশের ৫৩ কোটি মানুষের তথ্য রয়েছে। এর মধ্যে এক

কোটি ১০ লক্ষ ফেসবুক ব্যবহারকারীর তথ্য ব্রিটেন থেকে, যুক্তরাষ্ট্র থেকে তিন কোটি এবং অস্ট্রেলিয়া থেকে ৭০ লক্ষ মানুষের তথ্য ফাঁস করে দেয়া হয়েছে। ফেসবুক বলছে, বছর দেড়েক আগেই নিরাপত্তার ফাঁকফোকরগুলো বন্ধ করা হয়েছে। কিন্তু বর্তমানেও ফাঁকফোকর রয়ে গেছে।

জনাথন জোসেফ জেমস। একজন বিশ্বখ্যাত আমেরিকান হ্যাকার এবং সবচেয়ে কমবয়সী কিশোর যিনি ১৬ বছর বয়সেই সাইবার অপরাধের সাথে লিপ্ত হয়ে জেলে গিয়েছিলেন। তিনি ১৯৯৯ সালের দিকে তখন মাত্র ১৫ বছর বয়সে বেল-সাউথ, মিয়ামি ডেড, আমেরিকার প্রতিরক্ষা বিভাগ এবং নাসার ওয়েব সাইট হ্যাক করেন। এছাড়াও তিনি ব্যাকডোর কম্পিউটিং এর মাধ্যমে ডালাস এবং ভিরজিনার সার্ভারে একটি স্নিফার ইন্সটল করেন। যার মাধ্যমে তিনি ওই সব স্থানের প্রায় তিন হাজার তথ্য চুরি করেন। যার মধ্যে ছিল ওই এলাকা গুলোর সকল চাকুরীজিবিদের তথ্য, এমন কি কমপক্ষে ১০ টি অফিশিয়াল মিলিটারী কম্পিউটারের তথ্য। তথ্য চুরির ধারাবাহিকতা এখনো চলমান। প্রযুক্তি উন্নতির সাথে বাড়ছে ফাঁদে ফেলার চতুরতাও।

অ্যানোনিমাস। আরেকটি দল তারা। তাদের টার্গেট ছিল সরকারি এবং সরকারের সাথে সম্পর্কিত বিভিন্ন ওয়েবসাইটে হামলা দিত। সেখান থেকে তথ্য নিয়ে ছড়িয়ে দিত বা মোটা অংকে বিক্রি করে দিত। ২০১১ সালের মে মাসে অ্যানোনিমাসের একটি ছোট দল "এইসবিগ্যারে" হ্যাক করে। এই দলের সদস্য "টিফ্লু", "টপিয়ারি", "সাবু" ও "ক্যালা" মিলে পরবর্তীতে লালজ সিকিউরিটি নামে একটি হ্যাকার দল গঠন করেন। যা সংক্ষিপ্তভাবে লালজসেক নামে পরিচিত। এই দলের প্রথম সাইবার হামলা ছিল ফক্স.কমের বিরুদ্ধে। তারা ফক্সের সাইট হ্যাক করে কিছু পাসওয়ার্ড, লিংকডইন প্রোফাইল এবং এক্স ফ্যাক্টরের ৭৩ হাজার প্রতিযোগীর তথ্য ফাঁস করে দেয়। ২০১১ সালের মে মাসে তারা আমেরিকান পাবলিক ব্রডকাস্টিং সার্ভিস (পিবিএস) হ্যাক করে পরিচিতি লাভ করে। ২০১২ সালের জুনে লালজসেক সনি পিকচার্স হ্যাকের কথা জানায় এবং তারা সেখান থেকে হাজার হাজার গ্রাহকের নাম, ইউজারনেইম, পাসওয়ার্ড, ইমেইল ঠিকানা, বাড়ির ঠিকানা ও জন্মদিনের তথ্য ইত্যাদি প্রকাশ করে দেয়। জুনের প্রথম দিকে তারা পর্নোগ্রাফি.কম ওয়েবসাইট হ্যাক করে সেখান থেকেও ২৬,০০০ ইমেইল ঠিকানা ও পাসওয়ার্ড চুরি করে প্রকাশ

করে দেয়। ১৪ জুলাই, ২০১২ সালে তারা তাদের এক ভক্তের অনুরোধে মাইনক্রেফট, লিগ অফ লেজেন্ড, দ্য এসকেপিস্ট ও আইটি নিরাপত্তা কোম্পানি ফিনফিশারের ওয়েব সাইট হ্যাক করে বন্ধ করে দেয়।

আমি এই বইয়ে চেষ্টা করেছি অনলাইন জগতে সচেতনতা বাড়ানোর। পাশাপাশি ফেসবুক সংক্রান্ত কিছু বিষয়ে ধারণা দেওয়ার। বইয়ের বেশিভাগ লেখাই ফেইসবুকে সময়ে সময়ে লিখেছিলাম।

সাইফুল ইসলাম

শুরুর আগে...

একে কোনো পুস্তিকা বলবো না। নির্দিষ্ট একটি বিষয় নিয়ে লেখাও না। তবে সাইবার সম্পর্কিত কিছু তথ্য একসাথ করেছি। অগোছালো ভাবে বহু তথ্য তুলে ধরার চেষ্টা করেছি। পাঠকের বোধগম্যের প্রতি বিশেষ লক্ষ্য রাখার আপ্রাণ চেষ্টা করেছি। পাঠক মুগ্ধ হবে এমন কিছু না থাকলেও আশাহত হবে না বলে আমার দৃঢ় বিশ্বাস।

মূলত এই ছোট্ট পুস্তিকাটি কিছু অতীতে আপলোড করা পোস্ট। সময়ে সময়ে ফিলহাল পক্ষে বিপক্ষে সাইবার সম্পর্কিত লেখাগুলো সন্নিবেশনে জন্ম এই "সাইবার সিকিউরিটি" এর।

পাঠকের দুয়ারে একটি বিনীত নিবেদন থাকবে, কথায় অসঙ্গতি বা দৃষ্টিকটু বা অন্য কিছু দৃষ্টিগোচরে আসলে ধরিয়ে দেবার অনুরোধ। এখানে যা ভালো কিছু আছে তা আল্লাহর পক্ষ থেকে। আর ভুল ও খারাপ কিছু আমার পক্ষ থেকে।

—ঠিকানা

covidvirus500@gmail.com

সাইবার সিকিউরিটি কী? সাইবার সিকিউরিটি পরিচিতি। কিভাবে ইন্টারনেটে নিজেকে সুরক্ষিত রাখবেন?

ইন্টারনেটের ব্যবহার দিনের পর দিন বেড়েই চলেছে তার সাথে বাড়ছে ইন্টারনেটে সিকিউরিটির গুরুত্ব। কারন আপনি সাইবার সিকিউরিটি ছাড়া ইন্টারনেট জগতে টিকে থাকতে পারবেন না। অনেকেই ইন্টারনেট ব্যবহার করেন কিন্তু ইন্টারনেটে যে সব সময় সিকিউর রাখতে হবে নিজেকে সে বেপারে তারা অজ্ঞ। তাই ইন্টারনেট ব্যবহার যেন আমাদের ক্ষতির কারণ না হয়ে যায় তাই আমাদের সবসময় সতর্ক থাকতে হবে। এই জন্য সাইবার সিকিউরিটি অনেক গুরুত্বপূর্ণ।

ইন্টারনেট দিয়ে যেমনভাবে অনেকের ভাল করা সম্ভব তেমনিভাবে অনেকের নানাভাবে ক্ষতিও করা সম্ভব। তাই সবাই সাইবার সিকিউরিটি সম্পর্কে অনেক বিস্তারিত জানতে হবে। আধুনিক সব ধরনের ডিজিটাল ডিভাইস হ্যাকিং এর

শিকার হতে পারে। তাই যদি সবসময় সাবধান থাকা উচিৎ যদি সব সময় সাবধান না থাকেন, তাহলে আপনিও ক্ষতির সম্মুখীন হতে পারেন। সাইবার আক্রমণগুলি প্রতিষ্ঠান, কর্মচারী এবং ভোক্তাদের জন্য একটি বিপন্ন বিপদ।

সাইবার সিকিউরিটি কী? সাইবার সিকিউরিটি পরিচিতিঃ

সাইবার সিকিউরিটি হচ্ছে কোনও সাইবার অ্যাটাক থেকে নেটওয়ার্ক, ডিভাইস এবং প্রোগ্রাম গুলি সুরক্ষিত ও পুনরুদ্ধারের প্রক্রিয়া। ইন্টারনেটের জগতে হ্যাকিং বা ম্যালওয়ার অ্যাটাক থেকে বাঁচার জন্য যেসব ব্যাবস্থা গ্রহণ করা হয় সেই বিষয় গুলি সাইবার সিকিউরিটির মধ্যে পরে। ওয়েবসাইট অবৈধ প্রবেশ বন্ধ করতে সাইবার সিকিউরিটি সম্পর্কে জানা প্রয়োজন। যখন কেউ আপনার কম্পিউটার বা স্মার্টফোনকে অসৎ ভাবে অ্যাক্সেস নেয়ার চেষ্টা করে তখন তা হ্যাকিং এর আওতায় পরে। বা আপনার কম্পিউটার বা স্মার্টফোন কেও হ্যাক করার চেষ্টা করছে।

আর এ ধরনের খারাপ অভিজ্ঞতা থেকে বাঁচার জন্য আপনাকে অবশ্যয় সাইবার সিকিউরিটি সম্পর্কে বিস্তারিত জানতে হবে।

সাইবার হুমকি ধরনঃ

কি কি ধরনের সাইবার হুমকি আপনি পেতে পারেন সেসব সম্পর্কে জানাটা আগে জরুরী। যদি আপনি সাইবার হুমকি সম্পর্কে না জানেন তাহলে সাইবার সিকিউরিটি সম্পর্কে বিশেষ ভাবে বুঝতে পারবেন না। তো চলুন কি কি ধরনের সাইবার হুমকি আপনি পেতে পারেন সেসব সম্পর্কে কিছু আলোচনা করা যাক।

অনেক ধরণের সাইবার হুমকি রয়েছে যা আপনার ডিভাইস এবং নেটওয়ার্কগুলিতে আক্রমণ করতে পারে, কিন্তু সাইবার হুমকি সাধারণত তিনটি ভাগে বিভক্ত সেগুলো হল Confidentiality, Integrity, and Availability.

Attacks on Confidentiality : এটি দ্বারা সাধারণভাবে

বুঝায় আপনার ব্যক্তিগত তথ্য চুরি এবং আপনার ব্যাংক অ্যাকাউন্ট বা ক্রেডিট কার্ড তথ্য চুরি করা। অনেক আক্রমণকারীরা আপনার এসব তথ্য সংগ্রহ করবে এবং অন্যদের ব্যবহার করার জন্য এটি ডার্ক ওয়েবে বিক্রি করবে।

Attacks on integrity : এই আক্রমণ দ্বারা সাধারণভাবে বুঝায় ব্যক্তিগত বা এন্টারপ্রাইজ sabotage তথ্য চুরি করা, এবং প্রায়ই লিক বলা হয়। এটি একটি সাইবারক্রিমিনাল অ্যাক্সেস এবং প্রকাশ্যে তথ্য প্রকাশ করবে এবং যেই সংস্থার তথ্য চুরি করবে সেই সংস্থার উপর বিশ্বাস হারানোর জন্য জনগণকে প্রভাবিত করবে। সহজ কথায় বলা যায় আপনার ব্যাবসা নষ্ট করার জন্য এসব হাকিং করা হয়ে থাকে।

Attacks on availability : এই ধরণের সাইবার আট্যাকের লক্ষ্য ব্যবহারকারীদের তাদের নিজস্ব ডেটা অ্যাক্সেস চুরি করবে এবং একটি নিদিষ্ট পরিমাণ ফি বা মুক্তিপণ না দেওয়া পর্যন্ত আপনার তথগুলো অবরুদ্ধ করে

রাখবে। সাধারণত, এই সাইবার ক্রিমিনাল আপনার নেটওয়ার্ককে অনুপ্রবেশ করবে এবং গুরুত্বপূর্ণ ডেটা অ্যাক্সেস থেকে আপনাকে অবরুদ্ধ করবে। আপনি আপনার ডাটা গুলোর অ্যাক্সেস পাবেন না।

নিচে কয়েকটি সাইবার হুমকির উদাহরণ দেওয়া হয়েছে যা উপরে তালিকাভুক্ত তিনটি বিভাগে পড়ে:

১। Social engineering / সামাজিক প্রকৌশলী

২। APTs (Advanced Persistent Threats)

৩। Malware /

৪। ভালনারবিলিটি

৫। ব্যাকডোর

৬। ডিরেক্ট অ্যাক্সেস অ্যাটাক

৭। ফিশিং

সাইবার নিরাপত্তা জন্য নিচের পদক্ষেপ গুলো অনুসরণ করুনঃ

১। আপনার ব্যক্তিগত তথ্য প্রদান করার সময় শুধুমাত্র বিশ্বস্ত সাইট ব্যবহার করুন। যদি সাইটে "https://," থাকে তাহলে সেই সাইটকে বিশ্বাস করা যেতে পারে, আর যদি "http://," মানে s মিসিং থাকে তাহলে সেই সাইটকে বিশ্বাস করা যায় না।

২। অজানা কোন লিঙ্ক থেকে ইমেইল ওপেন করবেন না বা আপনার কোন Password দিবেন না।

৩। সর্বদা আপনার ডিভাইস আপডেট রাখা।

৪। সাইবার আক্রমণ প্রতিরোধে করতে নিয়মিত আপনার ফাইলগুলি ব্যাকআপ করুন।

৫। Password দেওয়ার সময় উপরের কিঙ্ক দেখে নিবেন সব সময়। যাতে কেউ আপনার Password ফিসিং করতে না পারে।

-ভয় নেই। এটা আপনার সহযোগী

ফেইসবুক কর্তৃপক্ষ অনেক ইউজারকে একটি মেসেজ দিচ্ছে। যেটা দেখে সাধারণ কিছু মানুষ হয়রান হয়ে ছুটে বেড়াচ্ছে বিভিন্ন স্পাই দরবারে। [মেসেজটি ফটো আকারে নিচে দেওয়া আছে।]

মেসেজটি যারা পেয়েছেন তাদের ভয় পাওয়ার কোনো কারণ নেই। বরং উল্টো খুশি হওয়া দরকার। কারণ..

কারণ আপনার মোবাইল ছাড়া অন্য যেই মোবাইল বা কম্পিউটারে অথবা আপনার মোবাইলের অন্য যেই ব্রাউজারে আপনার এই আইডিটি লগইন আছে ফেইসবুক অটোমেটিক লগআউট করে দিয়েছে আপনার সুরক্ষার জন্য।

ফেইসবুক ধীরে ধীরে সুরক্ষা বাড়াচ্ছে। ইউজার সুরিক্ষিত থাকবে থাকতে পারবে সেটাও ফেইসবুকের আনন্দ। তাই তারা বিভিন্ন সময় বিভিন্নভাবে আপনাকে সিকিউরিটি দিয়ে যাচ্ছে।

-সতর্কতা

বিষয়টি পুরাতন হলেও সবার কাছে নতুন। ইতিমধ্যে অনেকের কাছ থেকেই প্রশ্নটি পেয়েছি। ফেইসবুক থেকে সরাসরি আইডিতে যুক্ত থাকা মোবাইল নম্বরে "কর্তৃপক্ষ আইডি ডিসেবল করে দিবে" এমন warning দেওয়া হচ্ছে। এসএমএসে কিছু লেখা থাকে তারপর শেষে একটা লিঙ্ক যুক্ত করে দেওয়া হয়।

এসএমএস টি এরকম হয়-

SMS alerts about unrecognized logins into your Facebook account will be disabled in 7 days. If you want to keep receiving these warnings via email you need to enable that in settings:

https://m.facebook.com/login alerts/settings/

❐ সমাধান :

Get alerts about unrecognized logins অপশনে গিয়ে সবগুলো অপশন অন করে দিলে ঝামেলা শেষ।

কাজটি করবেন যেভাবে –

পদ্ধতি–১.

মেসেজে দেওয়া লিংকে প্রবেশ করে সবগুলো অপশন On করে সহজে কাজটি করতে পারবেন।

পদ্ধতি—২.

Settings > security and login > Get alerts about unrecognized logins তারপর সব On করে দিবেন।

পদ্ধতি—২ এ যেভাবে দেখানো হয়েছে সেভাবে সবাই করে রাখবেন। ৩ টা অপশনই On করে রাখবেন।

——একটি প্রশ্ন —ইমেইল বা নোটিফিকেশনে Warning মেসেজটা না এসে, নম্বরে কেন আসলো?

——উত্তর হলো, ১. Alerts অপশনটা শুধুমাত্র নম্বরেই On করা ছিল। ২. Alerts অপশনটা জিমেইলে On করা ছিল না।

-পাসওয়ার্ড ভুলে গেছেন। তারপর..

পাসওয়ার্ড ভুলে গেছি। ফরগেট করতে গেলে নম্বর শো করে না। শুধু জিমেইল একাউন্ট শো করে। জিমেইলটা অনেক আগের। পাসওয়ার্ড মনে নেই। মোবাইলে লগইন ও নেই। কোনো দয়াবান ব্যক্তি কি আইডিটা ব্যাক করে দিতে পারবেন? অথবা নম্বর শো করিয়ে দিতে পারবেন??

উত্তর :

আমরা একটা ভুল করি যে, নম্বরটা পুরোপুরি অ্যাড করা হয় না বলে ফরগেট করতে গেলে নম্বরটা শো করে না। আমরা ভাবি নম্বর তো অ্যাড ছিল। আমি নিজেই অ্যাড করেছি। কিন্তু নম্বরটা অ্যাড হয়নি।

আমাদের যে ভুলটা হয়ে থাকে যে, আইডিতে নম্বর অ্যাড করতে গেলে নম্বরে একটা কোড যায়। সেই কোডটা দিয়ে নম্বরটা কনফ্রম করতে হয়। কিন্তু অনেকে একাজটা করে না।

—আরেকটা প্রশ্ন এখানে এমনি চলে আসে। সেটা হলো আমি তো আইডি খোলার সময় নম্বর দিয়েই খুলেছি। তাহলে নম্বর আইডিতে পরিপুর্ণ অ্যাড হলো না কিভাবে?

উত্তর :

আমরা যারা ফেইসবুক সম্পর্কে অজ্ঞ তারা এই কাজটা করে থাকি যে, একটা নম্বর দিয়েই কয়েকটা আইডি খুলে থাকি। একটা আইডি খুলেছি তারপর পাসওয়ার্ড ভুলে যাওয়াতে আরেকটা আইডি খুলি। যার কারণে নম্বর এক আইডি থেকে অটোমেটিক ডিলেট হয়ে যায়।

আরেকটা প্রশ্ন। সেটা হলো- যেই আইডির ফরগেট মারলে নম্বর অ্যাড থাকা সত্ত্বেও নম্বর শো করে না, সেই নম্বর কি শো করানো সম্ভব?

উত্তর : সম্ভব নয়। আইডি থেকে যেই নম্বর ডিলেট হয়ে গেছে বা ডিলেট করে দিয়েছেন সেটা পূনরায় আইডিতে ফিরিয়ে আনা সম্ভব নয়।

——অনেক সময় নম্বর এবং জিমেইল অ্যাড থাকা সত্ত্বেও নম্বর/জিমেইল একটাই শো করে। জিমেইল এবং নম্বর উভয়টা শো করে না।

এর সমাধান এভাবে হতে পারে। অন্য আরেকটা মোবাইল দিয়ে ফরগেট মারতে পারেন। এভাবে কয়েকটা মোবাইল দিয়ে ট্রাই করতে পারেন। অথবা এক মোবাইলেই ব্রাউজার চেঞ্জ করে ট্রাই করতে পারেন।

❒ আমাদের করণীয় :

একটা নম্বর দিয়ে একটাই আইডি খুলুন। নম্বর অ্যাড রাখার পাশাপাশি জিমেইল অ্যাড রাখুন। জিমেইল এর অ্যাকসেস রাখুন। সম্ভব চেষ্টা করবেন ফেইসবুক আইডির পাসওয়ার্ড এবং জিমেইল এর পাসওয়ার্ড যেন ভিন্ন হয়। নম্বর অ্যাড আছে কিনা সেটা চেক করে রাখুন। অন্য কোনো আইডিতে আপনার নম্বর অ্যাড আছে কিনা খোঁজে ডিলেট করুন।

-ফিশিংঃ সতর্ক হোন

50GB Free Internet #NewYearOffer 😋

প্রতিবছরই স্কেমাররা এমন ফিশিং লিংক ভাইরাল করে।।

এই লিংকে রয়েছে Powerfull Trojan Virus যা আপনি ক্লিক করলে অজান্তেই ডাউনলোড হয়ে যেতে পারে আপনার ফোনে এই ভাইরাস।

ভাইরাসটি আপনার ফোনে জায়গা করে নেওয়ার সাথেই সাথেই আপনার ডিভাইস অটোমেটিক Factory Data Reset হয়ে যাবে। অতঃপর সব হারালেন!🙂

তাই সাবধান এসব লিংক ক্লিক করবেন না।। আপনাকে কোনো কোম্পানি অফার দিলে তাদের অফিসিয়াল ওয়েব, ফোন নাম্বার বা বিজ্ঞাপনের মাধ্যমে জানিয়ে দেবে।। #staysafe

-কপিরাইট: অজান্তে গায়েব হবে আপনার আইডি

ধরেন NTV নিউজ চ্যানেল থেকে খুবই গুরুত্বপূর্ণ একটা নিউজ আপলোড দেওয়া হলো যা দেখে আপনার শেয়ার করতে মন চাইলো কিন্তু আপনি শেয়ারটা দিছেন নরমাল শেয়ার নয় না বুঝে আপনি তাদের ভিডিও তাদের লিংক থেকেই ডাউনলোড দিয়ে নিজের প্রফাইলে আপলোড দিছেন।।

তো এইখানে কয়েকটা জিনিস বুঝতে হবে কপিরাইট ইস্যু নিয়ে।। এই ভিডিওটিতে প্রতিটি কন্টেন্ট বলি বা অবজেক্ট সবই তাদের নিজের কপিরাইট মালিকানাধীন বা তাদের নিজের লাইসেন্স করা যা ফেসবুক থেকে কপিরাইট লাইসেন্স নেওয়া তাদের। যেহেতু তারা ভেরিফাই নিউজ পেইজ।।

তো আপনি আপলোড দেওয়ার সাথে সাথেই তাদের পেইজ থেকে আপনার ভিডিওতে অটোমেটিক কপিরাইট স্ট্রাইক

চলে আসবে এবং আপনার আইডি শেষ 🙂 Your account has been desabled.

শুধু তাই নয় এই ডিজেবল এতোটাই মারাত্মক যে আপনার ডিভাইসে যতোটি একাউন্ট অপেন করা সব একাউন্ট ডিজেবল হয়ে যাবে একই আইপি এর যতোগুলা আইডি আছে শুধু তাই নয় নতুন একাউন্ট খুলতে গেলেও এই সমস্যায় পড়বেন।।।

যাকে বলে Copyright infringement desabled সর্বমোট ৬ টি উপায় এই আইডি ফিরিয়ে আনা যায় তাও খুব কম সাক্সেস হওয়ার সম্ভাবনা।

ভিডিওটিতে থাকা লগো ভোকাল সব কিছুই কপিরাইট এর ইস্যুতে পড়ে আপনি চাইলে দেখেন T series এর কোনো কন্টেন্ট আপলোড দিয়ে বা তাদের কোনো মিউজিক আপনার ভিডিওতে এড দিয়ে তাদের লিগ্যাল পারমিশন ছাড়া দেখবেন আইডি ডিজেবল না হলেও অডিও মিউট হয়ে যায় অডিও বন্ধ হয়ে যায়।।

যতোদিন যাচ্ছে যুগের সাথে ফেসবুক ব্যাবহারকারিদের সিকিউরিটি এর সার্থে তাদের সবকিছু আপডেট দিচ্ছে।

নিজের ভুলের কারনে না বুঝেই নিজের অতি প্রয়োজনীয় আইডি হারাতে বসছেন তাই সতর্ক থাকুন।।

মনে রাখবেন লাইসেন্স ছাড়াও আপনি যে পোস্ট করছেন ধরেন আমি এই যে পোস্ট লিখলাম কেউ যদি আমার ক্রেডিট ছাড়া নিজের টাইমলাইনে পোস্ট কপি করে আমি চাইলেই তার পোস্টে কপিরাইট রিপোর্ট দিতে পারি সাথে সাথেই তার আইডি ডিজেবল হয়ে যাবে। কারন ১ নেনো সেকেন্ড আগেও পোস্ট করলেও এইটা মালিকানা আমার। এবং ফেসবুক তাই বলে।।

সতর্ক থাকুন হুজুগে যা ইচ্ছে তাই কারো কন্টেন্ট আপলোড দেওয়ার আগে ভাবুন প্রয়োজনে লোগো ব্লার করে বা মুছে দিন বা অডিও চ্যাঞ্জ করোন একটা অবজেক্টও যদি ধরা খান

সাথে সাথেই ফেসবুক শেষ আর এই ডিজেবল আইডি ফিরিয়ে আনা বলতে গেলে অসম্ভব অনেক পরিশ্রম আর মেধা খরচ করতে হয়।।

-ফেইসবুক Suspected একাউন্ট

ইদানিং যতোটি #Facebook #Suspended Account এর ভিকটিম আসছে আমাদের কাছে তাদের মধ্যে ৭০%ই তাদের ইনবক্সে ম্যাসেঞ্জারে পর্নোগ্রাফি কন্টেট শেয়ার করায় এই অবস্থা হয়েছে।। হয়তোবা কেউ কারো বন্ধুদের সাথে বা গার্লফ্রেন্ড এর সাথে (এটা যার যার ব্যাক্তিগত ব্যাপার) কিন্তু ইউজাররা জানেন না এইটা ফেসবুক Community Guidelines Follow না করায় হয় সেক্সোয়াল কন্টেন্ট আপলোড বা শেয়ার করা বা ম্যাসেঞ্জারে শেয়ার করা এইসবই Facebook Community Standards এর বাহিরে। যার কারনে অনেকেই হঠাৎ ঘুম থেকে উঠে দেখেন " We suspended your account "

Recently একজন ভিক্টিম তার ২বছরের বাচ্চা বাগিনা এর উলংগ ভিডিও এক সহপাঠীকে মেসেঞ্জারে শেয়ার করে যেখানে বাচ্চাটির গোপনাংগ দেখা যাচ্ছে স্পষ্ট শেয়ার করার

কিছুক্ষন পরই ফেসবুক উনার একাউন্ট সাস্পেন্ড করে দেয় তাহলে বুঝে নেন যারা অতি উতসাহে ফেসবুকের নিয়মকানুন না বুঝেই যা ইচ্ছা তা শেয়ার করছেন হউক তা ব্যাক্তিগত কিন্তু ফেসবুক তো নিয়ম ভাংগতে পারেনা! সাথে সাথেই নিজেই অতি প্রয়োজনীয় একাউন্টটি হারাতে বসছেন।

যার কারনে আমরা অভিজ্ঞরা অনেকবার ফেসবুকে আপিল করার পরও অনেকের আইডি ফিরিয়ে আনতে পারছিনা।।

তাছাড়া আপনারা যারা রিলেশনের নামে মেসেঞ্জারে একজন আরেকজনের Nude শেয়ার করছেন তারাও কিন্তু এই তালিকায় (এটা আপনাদের ব্যাক্তিগত ব্যাপার)

তাই সাবধনতার সাথে ফেসবুক এর কমিউনিটি গাইডলাইন ফলো করে ব্যাবহার করaccount....auses of Facebook Account Suspension

Facebook suspension is directed by the rules

that you have violated whether major or minor. Some of the common causes for which you can face a suspended FB account have been listed below for reference:

* Using Fake Identity- Not using your real name

* Unidentified Location- Logging into your account from a new location.

* Reported Account- If someone reported your account to Facebook.

* Illegal Login Attempt- Suspicious login attempt to your account

* Posting Offensive Content- posting something odious or unlawful

There can be several other reasons for which you may face suspension by Facebook.

-ইমো কনভার্সেশন

মেয়ে- হ্যালো। আপনি কি মামুন বলছেন?

মামুন- জ্বী বলছি

.

.

.

মেয়ে- তোমাকে অনেক ভালবাসি। একান্ত করে দেখতে ইচ্ছে করে

মামুন- আমারও

.

.

.

মেয়ে- তোমাকে কিছু ভিডিও পাঠিয়েছি দেখ। আগামী ৬ ঘন্টার ভেতরে ১ লাখ টাকা না পাঠালে এগুলো তোমাএ এলাকায় ছড়িয়ে যাবে।

এভাবে করেই প্রেমের ফাদে ফেলে ব্লাকমেইল করা হচ্ছে মামুনদের। আমাদের ধারনা ছিল বেশিরভাগ সময়ে মেয়েরাই এধরনের সাইবার আক্রমনের স্বীকার হয় তবে উলটো ঘটনাও ঘটছে অহরহ। বেশিরভাগ ক্ষেত্রেই টাকার বিনিময়ে হয় রফা আর এ কারনে এ অপরাধীদের মূল টার্গেট হয় বিদেশে অবস্থানরত প্রবাসীগন।

অনেকক্ষেত্রে নানা বাহানায় হাতিয়ে নেয়া হয় ইমোর OTP এবং হ্যাক করা সেই ইমো একাউন্ট থেকে শুরু হয় পরবর্তি অপরাধ কার্যক্রম।

সাইবার পুলিশ সেন্টার এমনই এক অপরাধী গ্রুপকে সনাক্ত এবং গ্রেফতার করতে সক্ষম হয়েছে। সবচেয়ে অবাক করা বিষয় হচ্ছে গ্রেফতারকৃতদের বেশিরভাগের বয়সই ১৬-২৪ এর ভেতরে।

অনলাইনে কারো সাথে সম্পর্কে জড়াবার আগে ভালভাবে তার ব্যাপারে না জেনে পার্সোনাল কন্টেন্ট শেয়ার করবেন না। পরবর্তিতে এটিই আপনার বিপদের কারন হতে পারে।

ভিন্ন কিছু

আপনার অজান্তেই আপনার পুরো বা অধিকাংশ সময়ই চলে যাচ্ছে মোবাইলে। আপনার দোষেই। বরবাদ হচ্ছে আপনার সফলতা আকাঙ্ক্ষিত জীবন। নষ্ট হচ্ছে আল্লাহর দেওয়া বড় নিয়ামত প্রতিভা। হয়তো আল্লাহ্ আপনাকে এমন কোনো প্রতিভা দান করেছেন যা হাতে গুনে কয়েকজনের ভেতরেও পাওয়া যায় না। কিন্তু আপনি; দিন যত যাচ্ছে অকৃতজ্ঞ হচ্ছেন। হেয়ালি করে নষ্ট করছেন জীবন প্রতিভাকে।

.

আমরা ফেইসবুকে কত সময়ই না ব্যয় করি। অযথা কতই মোবাইল চাপি। লাইক কমেন্ট আর চ্যাটিং ছাড়া ফেইসবুকে আমাদের আর যেন কর্মই নেই। আল্লাহর এই নিয়ামতি জীবনের সময় কত সহজেই শেষ করছি।

.

ফেইসবুক আমাদের জীবনের অবিচ্ছেদ্য অধ্যায় এসে দাড়িয়েছে। জীবন থেকে সব ডিলেট করে দিতে পারলেও ফেইসবুক স্ক্রোল যেন ডিলেট করতে পারবো না। না খেয়ে

কাটিয়ে দিতে পারবো ১২ ঘন্টার লম্বা দিনটা, কিন্তু ফেইসবুক না চালিয়ে এক মুহুর্তও যেন কাটানো ইম্পসিবল।

.

ফেইসবুকে সময় দেওয়াটা সমস্যা না। সময় দেওয়াকে আমি অভিযুক্ত করছি না। তবে এতো সময় দেওয়া বোকামি যেটা আপনার নেশায় পরিণত হয়। বরবাদ করে আপনার জীবন প্রতিভা। নষ্ট করে আপনাকে, আপনার জীবনের প্রতিটি ক্ষণকে। আমি অভিযুক্ত করছি সেই ফেইসবুক আর মোবাইল চালানোকে; যেটা চালাতে গিয়ে আপনি আল্লাহকে ভুলে যান। আখিরাতকে ভুলে আপনি দুনিয়াসক্ত হয়ে পরেন।

.

সময় এমন এক চিজ। যা একবার চলে গেলে আর ফিরে আসে না। যাঁরাই চলে যাওয়া সময়ের মূল্যায়ন করেন তারাই মূল্যায়িত হয়। যারা অবমূল্যায়ন করে তারাই অবমূল্যায়িত হয়।

-ফেইসবুক একাউন্ট ডিজেবল কতভাবে

একটা একাউন্ট কত ভাবে #Disabled হইতে পারে? আর কেনই বা ডিজেবল হয়? অনেকেই জানে আবার অনেকেই জানেনা ।

একটা #Account ৭ ভাবে ডিজেবল হতে পারে। তা হলো: ✅

1. Pretending_disabled
2. Violence_disabled
3. Facelock_disabled
4. disabled_ineligible
5. Child_disabled
6. Copyright_infringement_disabled
7. Remembering_removed

এই ৭ ভাবে একটা আইডি #ডিজেবল হইতে পারে । এর বাহিরে আরেকটা ডিজেবল আছে । সেখানে লেখা থাকবে Your account have been disabled permanently আর তার নিচে সোজা লেখা থাকবে Log out🐸

সেই পারমানেন্ট ডিজেবল নিয়ে বলার কিছু নাই, ঐ আইডি রিকভার করার আপাতত কোনো উপায় নাই । বাঁকি ৭ প্রকারগুলোর সংক্ষেপে বিবরণ দেই ।

- Pretending:

এ নিয়ে কিছু বলার নাই । ২টা আইডি ৭০% মিলে গেলে ফেসবুক সেটাকে #প্রিটেনডিং ধরে নেয় । প্রিটেনডিং এর আরেক নাম #Impersonating_disabled. এখন যেহেতু #impostor_report অফ আছে তাই তা নিয়ে কিছু বলবনা ।

- #Violence:

ফেসবুকের কিছু Terms বা নীতিমালা আছে । এগুলোর কোনো একটা না মানলে #ভায়োলেন্স ডিজেবল হতে পারে আইডি ।

- #Facelock:

ফেসলক থেকে ডিজেবল হয় উপযুক্ত ফটো সাবমিট না করার জন্য । এটা তিন ভাবে হতে পারে । রিকভারির পদ্ধতিও ৩ রকম ।

- #Ineligible:

এই ডিজেবল টা হাফ পারমানেন্ট বলা চলে । এক সাথে অনেকগুলো Terms ব্রেক করলে কোনো রিপোর্ট ছাড়াই এমন ডিজেবল হতে পারে । রিকভার করা অনেক কঠিন ।

- #Child:

চাইল ডিজেবল হয় #Underage_report করলে । ১৩ বছর বয়সের নিচে বা বয়স আর প্রোফাইল পিক ম্যাচ না করলে আর কেউ রিপোর্ট করলেই ডিজেবল হতে পারে। সহজেই রিকভার হয় ।

- #Copyright_infringement:

এই ডিজেবল টা এতোটাই মারাত্মক, ডিজেবল আইডিটা যে যে ফোনে লগিন করা আছে সব ফোনের সব আইডি ডিজেবল হবে অটোমেটিক । তবে রিকভার করতে ডকুমেন্ট লাগেনা । বিজনেস একাউন্ট আর রেগুলার একাউন্ট ২ রকম একাউন্টের জন্য রিকভারির মোট ৬টা স্টেপ আছে ।

- #Remembering:

রিমেম্বারিং রিপোর্ট করার সময় ২টা অপসন আছে । একটা হলো #Memorialize আরেকটা #Account_remove. যদি মেমোরিলাইজ করা হয় তাহলে সেটা ডিজেবল না বরং মমি(মৃত একাউন্ট) হয়ে যায় । আর যদি #remove

রিকোয়েস্ট করা হয় তাহলে ডিজেবল হয়ে যায় । রিকভারিও করা যায় ।

এই ৭ ভাবে একটা #Facebook_Account ডিজেবল হতে পারে । আশা করি ডিজেবল & রিকভারি নিয়ে স্বচ্ছ ধারণা এসে গেছে।

-অডিও রেকর্ড এড়ানোর পাঁচটি উপায়

'দেয়ালেরও কান আছে'—প্রচলিত এ প্রবাদ মানুষ এখন হাড়ে হাড়ে টের পাচ্ছে। ডিজিটাল এ সময়ে আড়ি পাতা হচ্ছে ফোনকলে। তাই অডিও রেকর্ডারই এখন এক অদৃশ্য কান। রেকর্ডিংয়ের ভয়ে এখন মন খুলে দু-চারটি কথাও বলা যায় না। বেফাঁস কিছু বলে ফেলবেন আর সঙ্গে সঙ্গেই সেটা হয়ে যাবে 'ভাইরাল'। তারপর মানসম্মান, পদ এবং 'চাকরি' হারানোর আশঙ্কা তো আছেই। কিছু উপায়ও অবশ্য আছে, যা অনুসরণ করে কথা বললে ফোনকলের অডিও রেকর্ড এড়িয়ে মন খুলে যা খুশি তা–ই বলতে পারবেন...

—

১. ওল্ড ইজ গোল্ড

চিঠি লেখার দিনে ফিরে যান। মনের ভাব প্রকাশের জন্য এটাই সবচেয়ে নিরাপদ উপায়। যা খুশি তা-ই লিখে ফেলতে পারবেন। প্রাপক আর প্রেরকের মধ্যে সব তথ্য গোপন থাকবে। তবে চিঠি পাঠানোর ক্ষেত্রে যদি ডাকপিয়নকে অবিশ্বাস করেন, তাহলে কবুতরের পায়ে চিঠি বেঁধে পাঠিয়ে দিন। কেউ আর লুকিয়ে আপনার চিঠি পড়ে ফেলতে পারবে না।

—

২. ভিডিও কল, তবে...

মুখে কোনো আওয়াজ না করে ভিডিও কলে কথা বলতে পারেন। এ ক্ষেত্রে আপনাকে কিছুটা কৌশলী আর সৃজনশীল হতে হবে। এ জন্য ইশারাভাষা শিখুন। এরপর অপর প্রান্তের ব্যক্তিকে ভিডিও কল দিয়ে ইশারাভাষায় মন খুলে কথা বলুন। আপনি যদি সৃজনশীল হয়ে থাকেন, তাহলে

মূকাভিনয় রপ্ত করতে পারেন। আপনার মনের ভেতরে থাকা যাবতীয় কথাবার্তা মূকাভিনয়ের মাধ্যমে প্রকাশ করতে পারবেন। গোপনে কথা বলা ছাড়াও মূকাভিনয়ের এ দক্ষতা দিয়ে আপনি কিন্তু রাতারাতি তারকাও বনে যেতে পারেন।

—

৩. টেলিপ্যাথি

আগেই বলে নেওয়া ভালো, বিজ্ঞানের ওপর অগাধ বিশ্বাস থাকলে এ পথ আপনার জন্য নয়। তবে যাঁরা খানিকটা কল্পনাপ্রবণ কিংবা বিজ্ঞানের বাইরেও চিন্তা করতে আগ্রহী, তাঁরা চেষ্টা করে দেখতে পারেন। এ ক্ষেত্রে পরামর্শ হলো টেলিপ্যাথি। হ্যাঁ, টেলিপ্যাথির মাধ্যমে মনের ভাব আদান–প্রদান করুন। টেলিপ্যাথিতে মুখ দিয়ে কথা বলা তো দূরের কথা, হাত–পা নাড়িয়ে ইশারাও করতে হবে না। আপনার চিন্তা আরেকজনের মস্তিষ্কে ধরা পড়বে। অডিও–ভিডিও এমনকি অলিম্পিকে রেকর্ড হওয়ারও কোনো আশঙ্কা নেই।

—

৪. সহকারীকে ব্যবহার করুন

নতুন কিছু শেখা যদি আপনার কাছে ঝক্কি মনে হয়, তাহলে একজন সহকারী নিয়োগ দিন। আপনার কথাগুলো সহকারীর মুখ দিয়ে বলান। যদি অডিও রেকর্ড ফাঁস হয়ে যায়, তাহলে ধরা পড়বে আপনার সহকারীর কাছে। আর ধরা পড়ার পর যদি সহকারী আপনাকে ফাঁসিয়ে দেয়, সেখানেও বাঁচার উপায় আছে। এ রকম বিপদে ওই সহকারীকে আপনার আশপাশে থাকা একজন 'অনুপ্রবেশকারী' হিসেবে পরিচয় করিয়ে দিন।

—

৫. তুরুপের তাস

ধরুন, ওপরের কোনো পদ্ধতিই অনুসরণ করলেন না। মুঠোফোনে মুখ ফসকে বেফাঁস কিছু বলেই ফেলেছেন। তখন কৌশলে দায় স্বীকার করে নিন। তখন সব দোষ হতভাগা মুখের। এ রকম অবস্থায় আপনার মন্তব্য হবে, 'আমার মুখ এসব বলেছে। মুখের ব্যক্তিগত কর্মকাণ্ডের দায় পুরো ব্যক্তি হিসেবে আমি নেব না।'

-ICS কে নিয়ে এক ভাইয়ের অভিযোগ, আমার জবাব

মদিনা শরিফের খুতবা || যাদের মাধ্যমে আল্লাহ ইসলামের হেফাজত করেন।

~ শায়খ ড. আবদুল মুহসিন বিন মুহাম্মাদ আল-কাসেম

আল্লাহ নিজের বান্দাদের জন্য একটি দ্বীন বাছাই করেছেন। এর মাধ্যমে তারা প্রতিপালকের ইবাদত করে। দ্বীন তাদের কাছে প্রচার করতে তিনি বিভিন্ন রাসুল পাঠিয়েছেন। ওলামায়ে কেরাম এ কথায় একমত পোষণ করেন যে, দ্বীনের হেফাজত করা পাঁচটি মৌলিক প্রয়োজনের মধ্যে প্রধান প্রয়োজন। তাই দ্বীন রক্ষা করার বিষয়টি প্রাণ, বুদ্ধি, ইজ্জত ও সম্পদ রক্ষার ওপর অগ্রাধিকার পাবে। পূর্ববর্তী জাতিদের মধ্যে দ্বীন হেফাজতের দায়িত্ব ন্যস্ত ছিল নবী-রাসুল ও তাদের অনুসারীদের ওপর। আল্লাহ বলেন, 'নিশ্চয় আমি তাওরাত অবতীর্ণ করেছি। তাতে আছে দিশা ও আলো। নবীরা, যারা আল্লাহর অনুগত ছিলেন, তারা ইহুদিদের

তদনুসারে বিধান দিতেন, রবের প্রকৃত সাধক ও বিদ্বান লোকেরাও বিধান দিত। কেননা, তাদের আল্লাহর কিতাবের রক্ষক করা হয়েছিল এবং তারা ছিল এর সাক্ষী।' (সুরা মায়েদা : ৪৪)।

তাদের মৃত্যুর পর তাদের দ্বীনে বিকৃতি ও গরমিল চলে আসে। তবে এ উম্মতের দ্বীনের হেফাজতের দায়িত্ব যিনি নিয়েছেন তিনি হলেন স্বয়ং আল্লাহ। তিনি বলেন, 'নিশ্চয় আমি কোরআন নাজিল করেছি এবং আমিই সেটার সংরক্ষক।' (সূরা হিজর : ৯)। আল্লাহর এ প্রতিশ্রুতি কেয়ামতের দিন পর্যন্ত মহান কোরআনের শব্দাবলি ও তার মর্মের সংরক্ষণ এবং কোরআনের ব্যাখ্যাকারী রাসুলের হাদিস ও সুন্নাহর সংরক্ষণের বিষয়টিকে ধারণ করে থাকবে। এ কাজের জন্য আল্লাহ তাঁর সৃষ্টির শ্রেষ্ঠতম অংশকে প্রতিনিধিত্ব দিয়েছেন। এর দ্বারা তিনি তাদের সম্মানিত করেছেন। তাঁর দ্বীনের হেফাজতের কাজকে তিনি তাদের সবচেয়ে বড় মর্যাদা ও তাদের একান্ত বিশেষ কীর্তি বানিয়েছেন। দ্বীনের প্রচারের ক্ষেত্রে তিনি নিজের ও তাঁর রাসুলদের মধ্যে জিবরাইল (আ.) কে মাধ্যম হিসেবে নির্বাচন করেছেন। তিনি নিজের রব যে কালাম তাঁর প্রতি

ওহি হিসেবে দিয়েছেন, তা হেফাজত করেছেন। তা নিয়ে আমাদের নবী মুহাম্মাদ (সা.) এর কাছে এসেছেন। প্রতি বছর তিনি একবার করে নবীজির সঙ্গে কোরআনের পাঠ-পর্যালোচনা করতেন। নবীর মৃত্যুর বছরে তিনি দুবার তাঁর কাছে কোরআন উপস্থাপন করেছেন। এ দায়িত্ব তিনি পূর্ণাঙ্গরূপে ও সুচারুভাবে পালন করেছেন। আল্লাহ বলেন, 'নিশ্চয় এটি রাব্বুল আলামিনের অবতীর্ণ কিতাব। বিশ্বস্ত আত্মা জিবরাইল তা আপনার হৃদয়ে নিয়ে এসেছে, যাতে করে আপনি সতর্ককারীদের অন্তর্ভুক্ত হন।' (সুরা শুআরা : ১৯২-১৯৪)।

দ্বীন হেফাজতের ক্ষেত্রে অন্য ফেরেশতাদেরও প্রচুর অংশগ্রহণ রয়েছে। তাদের কেউ আসমানে নিয়োজিত আছে শয়তানদের চৌর্যবৃত্তি থেকে ওহিকে হেফাজত করার জন্য। তাদের কেউ আসমান থেকে বড় বড় নিদর্শন নিয়ে আসে। কেউ কেউ রাসুলের পক্ষে তাঁর সঙ্গে দ্বীন রক্ষার জন্য ও মুসলমানদের সাহায্য করতে যুদ্ধ করে।

আল্লাহ যেভাবে আদেশ করেছেন নবীরা সেভাবে দ্বীনের

হেফাজত করেছেন। এ পথে তাঁরা এমন কষ্ট সহ্য করেছেন, যা অন্যরা সইতে পারবে না। তাদের কাউকে নির্যাতন করা হয়েছে। কাউকে নিজ দেশ থেকে বিতাড়িত করা হয়েছে। কারও দাওয়াতে কেউ সাড়া দেয়নি। কাউকে হত্যা করা হয়েছে। আল্লাহ বলেন, 'আপনি ধৈর্য ধরুন যেমন ধৈর্য ধরেছিল দৃঢ় মনোবলসম্পন্ন রাসুলরা।' (সুরা আহকাফ : ৩৫)। নিজের রবের পক্ষ থেকে অবতীর্ণ দ্বীনের হেফাজতে আমাদের নবী মুহাম্মাদ (সা.) সবচেয়ে বেশি সচেষ্ট ও তৎপর ছিলেন। জিবরাইল (আ.) যখন তাঁর কাছে কোরআন পাঠ করতেন, তখন তিনি ভুলে যাওয়ার আশঙ্কায় তা আগে আগেই পড়ে ফেলতেন। তখন তাঁর রব নিশ্চয়তা দিলেন, তিনি তাঁর জন্য সেটার সংরক্ষণ সহজ করে দেবেন।

দ্বীনের হেফাজত ও উম্মতের কাছে তা প্রচারের পথে নবীজি ভীষণ নির্যাতন ভোগ করেছেন। তাঁকে মিথ্যা ও গণকবৃত্তির অপবাদ দেওয়া হয়েছে। তাঁর বুদ্ধি ও সম্মান নিয়ে আঘাত করা হয়েছে। তাঁকে দেশ থেকে বের করে দেওয়া হয়েছে। তাঁকে জাদু করা হয়েছে। শত্রুরা তাঁর ওপর ঝাঁপিয়ে পড়েছে। তাঁর সম্প্রদায় তাঁর বিরুদ্ধে যুদ্ধ করেছে। তাঁর মাথায় আঘাত করে তাঁর দাঁত ভেঙে ফেলা হয়েছে। তাঁর

সামনে নিজের সঙ্গীদের হত্যা করা হয়েছে। তিনি তাঁর সাহাবাদের কোরআন সংরক্ষণের আদেশ দিতেন। কোরআন ও তাঁর সুন্নাহ লিখে রাখার নির্দেশ দিতেন। পরবর্তী সময়ের কাছে সেগুলো প্রচারের আদেশ করতেন। তিনি বলেছেন, 'তোমরা আমার পক্ষ থেকে একটি আয়াত হলেও প্রচার করে দাও।' (বোখারি)।

তাই সাহাবায়ে কেরাম দ্বীনের হেফাজতে প্রবলভাবে আগ্রহী হয়েছেন। তারা এ বিষয়ে এত বেশি গুরুত্ব প্রদান করেছেন, যা পরবর্তী সময়ে কেউ দিতে পারবে না। তারা চামড়ায়, হাড্ডিতে ও পাথরে পবিত্র কোরআন লিখে রেখেছেন। নিজেদের বক্ষে তা মুখস্থ করে রেখেছেন। পরবর্তী সময়ের কাছে তা সতেজ ও তাজা অবস্থায় পৌঁছে দিয়েছেন। নবীজির কথা ও কর্ম তাদের কাছে বহন করেছেন। শায়খুল ইসলাম ইবনে তাইমিয়া (রহ.) বলেন, 'বর্তমান থেকে কেয়ামত পর্যন্ত মুসলমানদের মধ্যে ঈমান, ইসলাম, কোরআন, ইলম, জ্ঞানবিজ্ঞান, ইবাদতবন্দেগি, জান্নাতে প্রবেশ ও জাহান্নাম থেকে মুক্তিসহ প্রত্যেক কল্যাণকর যতকিছুই আছে সেগুলো সাহাবায়ে কেরামের সম্পাদিত কাজের বরকতেই হয়েছে, যারা দ্বীন পৌঁছে দিয়েছেন।'

তাদের পরে আল্লাহ্ ওলামায়ে কেরাম তৈরি করে দিয়েছেন। দ্বীন শিক্ষাদানের ক্ষেত্রে সততা ও একনিষ্ঠতা তাদের সমবেত করেছে। তারা নির্দিষ্ট কোনো দেশ, জাতি, শ্রেণি বা বর্ণের সঙ্গে সীমাবদ্ধ নন, বরং তাদের মধ্যে আছে ছোটবড়, ধনী-গরিব। আছে দাস ও স্বাধীন মানুষ। উচ্চপদস্থ ও নিম্নশ্রেণি। আছে সুস্থসবল ও অন্ধ, বধির ও কানা লোকও। তারা দারিদ্র্য, ক্ষুধা, ভয় ও নির্যাতন সত্ত্বেও লিখেছেন, মুখস্থ করে সংরক্ষণ করেছেন ও ধৈর্য ধরেছেন। নিজেদের জানমাল ও সময় ব্যয় করেছেন, যা তাদের আল্লাহর দ্বীন হেফাজতের প্রতিশ্রুতি বাস্তবায়নের জীবন্ত প্রমাণে পরিণত করেছে।

ওলামায়ে কেরাম প্রত্যেক বিদ্যাতেই পা-িত্য অর্জন করেন। তাদের অধিকাংশই ছিলেন বিভিন্ন ধরনের বিদ্যায় সব্যসাচী। পাশাপাশি পার্থিব বিদ্যায়ও তারা ছিলেন পারদর্শী, যা মানুষের উপকারে এসেছে। কোরআন ও তাফসিরের আলেমরা কোরআনের শব্দ ও অক্ষরের সংরক্ষণ ও পরিসংখ্যান করেছেন। প্রত্যেক শব্দের মর্ম বর্ণনা করেছেন, তা একক শব্দ হোক বা যুক্তশব্দ হোক। তারা

কোরআন পাঠের বিধিমালা ঠিক করে দিয়েছেন। হরফের বিশুদ্ধ উচ্চারণের পন্থা সুন্দর করে বর্ণনা করেছেন। দুর্লভ শব্দের ব্যাখ্যা করেছেন। কোরআনের বিধান গবেষণা করে বের করেছেন। প্রত্যেক আয়াত নাজিলের সময় ও স্থান লিখে দিয়েছেন।

হাদিসের সনদ ও বর্ণনাবিষয়ক আলেমরা ও তাত্ত্বিকরা আবির্ভূত হয়েছেন। তারা বিভিন্ন দেশ সফর করেন। প্রবাসের তিক্ততায় ও পরিস্থিতির নাজুকতায় ধৈর্য ধরেন। তাদের মধ্যে ইমাম আহমাদ (রা.) সারা দুনিয়া দুইবার ভ্রমণ করেছেন, ফলে তিনি মুসনাদে আহমাদ সংকলন করতে পেরেছেন। তারা নবীজির কথা, কাজ ও স্বীকৃতিগুলো মুখস্থ করেন। তার শব্দসম্ভার, বিবরণ, বর্ণনাকারীদের মতভেদ ও ঐকমত্য সবকিছু সঠিকভাবে সংকলন করেছেন। ইমাম বোখারি (রা.) বলেন, 'আমি ১৬ বছরে বোখারি রচনা করেছি। সাত লাখ হাদিস থেকে তা চয়ন করেছি। এটাকে আমার মধ্যে ও আল্লাহর মধ্যে একটা প্রমাণ বানিয়েছি।'

আকিদাবিষয়ক আলেমরা ঈমান-আকিদার মাসআলা বর্ণনা

করেন। সেগুলো নির্ধারণ করেন। এর প্রমাণাদি একত্র করেন। মানুষের জন্য তা সহজবোধ্য করেন। আল্লাহর রুবুবিয়্যত ও তাঁর নামগুলোর তাৎপর্য স্পষ্ট করে বর্ণনা করেন। ভ্রান্ত লোকদের সন্দেহাদি নাকচ প্রমাণিত করেন।

ভাষা জ্ঞান ও শিক্ষার মাধ্যম। ভাষার দ্বারাই তা বোধগম্য হয়, উপলব্ধ হয়। তার প্রচার, প্রসার ও ভাষান্তর করা হয়। ভাষার প-িতরা ওহিকে ভাষার প্রথম উৎস হিসেবে ধরেন। তারপর তারা আরবদের মুখ থেকে ভাষার শব্দাবলি সন্ধান করেন। সেগুলো সংকলন করেন, বিন্যাস করেন। সেগুলোর অর্থ লিপিবদ্ধ করেন ও পরিচিত করেন। ভুল-শুদ্ধ আলাদা করেন। ভাষার নীতিমালা প্রণয়ন করেন, যা শব্দের অবস্থানগত অর্থ ও বিভক্তিচিহ্ন নিয়ন্ত্রণ করে, ভাষাকে বিশুদ্ধ করে। বাগ্মিতা রক্ষা করে। তার দ্বারা ভাষালঙ্কার অনুধাবন করা যায়, তার বিশুদ্ধতা পরিমাপ করা হয়।

ইতিহাস হলো সৃষ্টির তথ্যবিবরণী। আল্লাহর সৃষ্টির বিষয়ে আল্লাহর বিধিমালার পথনির্দেশক। তার মধ্যে সর্বশ্রেষ্ঠ হলো আমাদের নবী মুহাম্মাদ (সা.) এর জীবনচরিত বা সিরাত।

সিরাতবিষয়ক প-িতরা নবীর জীবন, স্বভাব, বৈশিষ্ট্য, চরিত্র, গুণাবলি ও তাঁর অবয়বের বিবরণ, তাঁর জীবনের ছোটবড় প্রত্যেক অনুষঙ্গ, তাঁর নাম, বংশ, বয়স, জন্ম-মৃত্যু সবকিছুই গ্রন্থন করে রেখেছেন। রাসুলুল্লাহ (সা.) এর নবুয়ত, যা নিয়ে তিনি প্রেরিত হয়েছেন, তাঁর হিজরত, তাঁর স্ত্রী, ছেলেমেয়ে, সাথিসঙ্গী ও প্রিয়জন, তাঁর দৈহিক বৈশিষ্ট্য ও অবয়বের বর্ণনা, চরিত্রের আলোচনা উল্লেখ করেছেন। তাঁর যুদ্ধবিগ্রহ, অভিযান, তৈজসপত্র, তরবারি, তির-বর্ষা, চতুষ্পদ বাহন, তাঁর বস্ত্রের রং, জুতার বিবরণ, সুগন্ধির প্রকার যা তিনি ব্যবহার করতেন, তাঁর নিদ্রার বিবরণ, তিনি পানি পান করতেন কতটি নিঃশ্বাসে, তাঁর আহারের বর্ণনা, কোন খাবার তিনি পছন্দ করতেন, তাঁর হাঁটার ধরন, হাসিকান্না ও তাঁর দাড়ি ও মাথার সাদা চুলের সংখ্যার কথা পর্যন্ত ইতিহাসবেত্তারা লিখে রেখেছেন।

শতাব্দীর পর শতাব্দী আলেমরা দ্বীনের হেফাজত করে যাচ্ছেন। পরবর্তীদের জন্য তা বহন করে নিয়ে আসছেন। তারা ইলম ও ইবাদতের সমন্বয় সাধন করেন। নানা গ্রন্থ রচনা করেন। শিক্ষাদান করেন। এতে তাদের সময় খরচ করেন। তারা বিপদ ও কঠিন পরিস্থিতিতে ধৈর্য ধরেন।

তাদের প্রচেষ্টার ফলে কোরআনের একটি হরফও বাদ যায়নি। হাদিসের কোনো কিছুই নষ্ট হয়নি। যুদ্ধবিগ্রহ, দারিদ্র্য, হাজার বিরোধ, মতপার্থক্য, শত্রুদের চক্রান্ত ও উপহাস সত্ত্বেও দ্বীনের কোনো অংশই ধ্বংস হয়নি। বান্দার কর্তব্য হলো, তারা আল্লাহর শোকর আদায় করবে, কারণ তিনি তাদের জন্য ইসলামকে হেফাজত করেছেন। তাদের ইসলামের অনুসরণের সুযোগ দান করেছেন। ওলামায়ে কেরামের প্রতি শ্রদ্ধা প্রদর্শন করা আল্লাহর দ্বীন ও আল্লাহর প্রতি শ্রদ্ধা প্রদর্শনের অন্তর্ভুক্ত। তারাই তো নবুয়তের উত্তরাধিকার বহন করেন। আল্লাহ তাদের মর্দাদা উন্নত করেছেন। তিনি বলেন, 'তোমাদের মধ্য থেকে যারা ঈমান এনেছে এবং যাদের ইলম দান করা হয়েছে, আল্লাহ তাদের মর্দাদা সমুন্নত করেন।' (সুরা মুজাদালাহ : ১১)।

৫ রবিউস সানি ১৪৪২ হিজরি মসজিদে নববির জুমার খুতবার সংক্ষিপ্ত ভাষান্তর করেছেন

✓ মাহমুদুল হাসান জুনাইদ

কমেন্টের স্ক্রিনশট নিচে||

[redacted]

সবকিছুই ঠিক আছে ভাই,
কিন্তু আপনাদের পেইজ এর ট্যাগলাইন বা স্লোগান সম্পর্কে আমাকে একটু ভাবায়।

আপনারা যে বলছেন "we protect Islam" এই কথার মাহাত্ম্য কি বোঝায় বলেন তো?

আপনারা ইসলাম কে রক্ষা করেন?? ভাই আমরা খুব ই নগণ্য এবং পাপী বান্দা, আমাদের মুখে এই কথা মানায় না।

আপনি বলতে পারেন আপনি অশ্লীলতা কে দূর করতে পারেন কিন্তু ইসলাম কে রক্ষা করার ব্যাপকতা অনেক।

সম্ভবত ইসলাম কে রক্ষা করার দায়িত্ব মহান আল্লাহর নিজের ই।।এবং তিনিবতা ভালভাবেই পারেন।
আর সেই অর্থে ভাবলে আপনারা কিন্তু নিজেদেরকে আল্লাহর সমতুল্য ভাবছেন এই কথার মাধ্যমে,

আমি কোন মুহাদ্দিস বা মুফতী নই,
আপনাদের কাছে বিষয়টি আরো একবার ভেবে দেখবার অনিরোধ রইলো।

আমার ছোট্ট জ্ঞানে যেটুকু মনে হয়েছে তাই বলেছি

27 mins   Like   Reply   1

-আনলক হতে পারে আপনার একাউন্ট

Two step authentication থাকলেও

ফেসবুকে Two Step authentication on থাকলেও হ্যাকাররা আনলক করতে পারবে আপনার একাউন্ট।।

অবাক হচ্ছেন?

ফেসবুকের প্রধান কোম্পানির নাম পরিবর্তন করতে গিয়ে ফেসবুকে নতুন কিছু আপডেট নিয়ে আসছে meta authority...

সেক্ষেত্রে এই সিস্টেমটায়েও দুর্বলতা ধরা পড়েছে।।

এক ভিক্টিমের অভিযোগে আমরা তাকে হ্যাল্প করতে গিয়ে এই ত্রুটির সন্ধান পেয়েছি।।

যেখানে ভিক্টিমের ফোন হারিয়ে যায়।। ফোনে যে নাম্বার

সিম ছিলো সেটা উনার ব্যাক্তিগত একাউন্টে Two step verification এর জন্য অন করে রেখেছিলেন।। তো উনি ফোনও হারিয়েছেন আর ব্যাক্তিগত সমস্যার কারনে সিমটাও উঠাতে পারছেন না। কারন সেই নাম্বারেও ভেরিফিকেশন কোড গেলেই উনি উনার আইডিতে লগইন করতে পারবেন।।

তাই উনি আমাদের কাছে আসেন আমরা উনাকে সাহায্য করি।। সাহায্য করতে গিয়ে দেখলাম উনার ফেসবুকের সাথে জাতীয় পরিচয়পত্রের তথ্যের মিল নাই।। তাই আমরা উনাকে নকল ভার্চুয়াল এন আইডি তৈরি করে দেই তবে তার আগে থানায় জিডি করতে বলি উনি আমাদের কাছে দেওয়ার পর আমরা কাজ শুরু করি।।

Tow Step verification Unlocked করতে গেলে ফেসবুক কর্তৃপক্ষের কাছে একটা ফর্ম সাবমিট করতে হয়।। আমরা সেটাই করলাম যেখানে উনি উনার নকল এন আইডি লাইভ হাতে নিয়ে কর্তৃপক্ষের কাছে জমা দিলেন।। আশ্চর্য বিষয় এটাই ২৪ ঘন্টার ভেতর উনার ফেসবুক আইডি

এক্সেস নেওয়ার জন্য উনাকে কর্তৃপক্ষ মেইলে অভিনন্দন জানায়।।

Moral of the Investigation এ যা বুঝা যায় ফেসবুকের কাছে আপনার নির্বাচন কমিশনের কোনো তথ্য নেই সেক্ষেত্রে আপনি তাদের নকল না আসল আইডি কার্ড সাবমিট করছেন সেটা তারা ভেরিফাই করতে পারেনা তাই যে কেউই চাইলে আপনার পাসওয়ার্ড জেনে গেলে Two Step Verification locked কে Unlocked করেই আপনার ফেসবুকের এক্সেস নিতে পারে।।

তো কথা হলো Two step verification এর মতো সেকিউর সিস্টেম থেকেও যদি আমরা নিরাপদ না হই তাহলে উপায় কি??

উপায় আছে ঃ

১) আপনার প্রফাইলে দেওয়া জন্ম তারিখ হাইড রাখুন

যেনো পাবলিক না দেখে।।

২) আপনার ফেসবুকের যাবতীয় তথ্য এন আইডি এর সাথে মিলে রেখে ভেরিফাই করে নিন সেক্ষেত্রে আমরা সাহায্য করতে পারি।।

৩) আপনার পাসওয়ার্ড শক্তিশালী করোন।।

৪) ফেসবুকে ট্রাস্টেড কন্টাক যুক্ত করোন।।

-যেভাবে কাজ করে আপনার ফেসবুক নিউজফিড

ফেসবুক হোমপেজে আমরা বন্ধুবান্ধব, পেইজ, গ্রুপ এবং অন্যান্য পার্টির যেসব স্পন্সরড কনটেন্ট দেখতে পাই সেটিই হচ্ছে “নিউজফিড”; সোশ্যাল নেটওয়ার্কিং এই কোম্পানিটির মতে নিউজফিড মূলত ব্যবহারকারীর জন্য একটি

“কাস্টমাইজড নিউজপেপার”; কিন্তু কখনো ভেবেছেন, এটি কীভাবে কাজ করে? গড়ে প্রত্যেক ফেসবুক ব্যবহারকারীর নিউজফিডে দিনে প্রায় ১৫০০ সম্ভাব্য পোস্ট ফিল্টার হয়ে থাকে। কিন্তু আমরা এগুলোর মাত্র ২০% দেখতে পাই!

কেউ কেউ হয়ত ভাবতে পারেন ফেসবুকে সময়ের ক্রমানুসারে পোস্ট র‍্যাংক করা হয়। অর্থাৎ যত আগের পোস্ট তত নিচে থাকবে, এভাবে সর্বশেষ কনটেন্ট সবার উপরে দেখা যাবে।

কিন্তু এত ব্যাপারটি আসলে এত সহজ না। এভাবে চিন্তা করলে ফেসবুক কর্তৃপক্ষ বিশ্বজুড়ে এতগুলো মানুষেরর আবেগ-অনুভুতি নিয়ে ব্যবসা করতে পারত না। আসলে নিউজফিডে স্টোরিগুলো স্কোরের ভিত্তিতে সাজানো থাকে। এখন কথা হচ্ছে, এই স্কোরিং কে করে? কীভাবে করে?

আচ্ছা প্রথম প্রশ্নের উত্তর চোখ বন্ধ করে বলে দেয়া যায়। পোস্টের স্কোরিং বা র‍্যাংকিং করে ফেসবুকের সেন্ট্রাল সার্ভার সিস্টেম। কিন্তু এর পদ্ধতিটি অত্যন্ত জটিল এবং

নিয়ত পরিবর্তনশীল।

স্টোরি র‍্যাংকিংয়েরজন্য স্কোর নির্ধারণ করতে অনেকগুলো ফ্যাক্টর বিবেচনা করা হয়, যার সবগুলো ফেসবুক জনসম্মুখে প্রকাশ করেনা। এদের মধ্যে যে কয়েকটি বিষয় জানা গেছে তা হল, ব্যাবহারকারীদের সাথে আপনার সম্পর্ক, যোগাযোগ, কমেন্ট-শেয়ার-লাইক সংখ্যা ইত্যাদি। এছাড়া একজন ব্যবহারকারীর সর্বশেষ ৫০টি ক্রিয়া-প্রতিক্রিয়াও র‍্যাংকিংয়ে প্রভাব ফেলে। এক্ষেত্রে আপনি কোন বন্ধুর পোস্টে লাইক করেছেন, কার সাথে কতটা মেসেজ বিনিময় করেছেন, কার টাইমলাইনে নিয়মিত ভিজিট করেন, একসাথে কাজ করেন প্রভৃতি উল্লেখযোগ্য।

যেমনটি আগেই বলেছি, নিউজফিড এলগোরিদম সবসময় ধ্রুব থাকেনা- এতে নিয়মিত বিরতিতে পরিবর্তন আসে। এই যেমন কিছুদিন আগেও হোমপেজ রিফ্রেশ করলে নতুন কনটেন্টগুলো একটু কম স্কোরড হলেও তা সবার উপরে চলে আসত। কিন্তু অতি সম্প্রতি স্কোরিং সিস্টেমে পরিবর্তন আসায় দিনের শুরুতে পোস্টকৃত স্টোরিগুলোও সন্ধ্যায় একদম উপরের দিকে দেখতে পারেন। এবং ফেসবুক সিস্টেম যতক্ষণ পর্যন্ত মনে করবে আপনি

দরকারী/সম্পর্কিত পোস্টগুলো এখনো দেখেননি ততক্ষণ তা চোখের সামনে রাখবে, এজন্য কখনো কখনো একই পোস্ট একাধিকবারও নিউজফিডে উপস্থিত হতে পারে।

ফেসবুকের এই কৌশল পরিবর্তন আপাতত সাইটটির ডেস্কটপ ভার্সনে প্রয়োগ করা হয়েছে। কোম্পানিটি বলছে ইতোমধ্যেই এটা ইউজার এঙ্গেজমেন্ট বৃদ্ধি করেছে। সুতরাং দরকারী পোস্টগুলো সত্যি সত্যিই এখন আপনার নিউজফিডের প্রধান প্রধান অবস্থানে চলে আসছে। ফেসবুকের মতে, সাইটটিতে এখন আগের চেয়ে ১৩% বেশি পোস্ট দেখা হচ্ছে এবং ৫% বেশি প্রতিক্রিয়া (লাইক, কমেন্ট, শেয়ার) পাওয়া যাচ্ছে। একইভাবে নিউজফিড কিংবা সাইডবারে প্রদর্শিত বিজ্ঞাপনগুলোও আলাদা যুক্তি ব্যবহার করে ইউজারদের ওয়েব ব্রাউজিং অভ্যাস অনুযায়ী উপস্থিত। হয়ে আসছে। উদাহরণস্বরূপ, আপনি কোন ওয়েবসাইট ভিজিট করছেন, কী তথ্য সার্চ করছেন পিসি থেকে এসব তথ্য নিয়েই ফেসবুক আপনাকে বিজ্ঞাপন দেখাচ্ছে।

আশা করি ফেসবুক নিউজফিডের জটিল কার্যপদ্ধতির কিছুটা হলেও সহজ ধারণা উপস্থাপন করতে পেরেছি।

Two Factor Authentication সমস্যা

-একটি পরামর্শ

Two factor authentication কোড না আসার সমস্যাটা আজকের নতুন না। তবে আগের তুলনায় এখন আরো বেড়েছে এই সমস্যা। তবে এখন আরো বড় সমস্যা হচ্ছে Two factor authentication সিকিউরিটি ভায়পাস হচ্ছে না। কার্ড সাবমিট দিলেও আশায় বসে থাকতে হয়।

ফেইসবুক নতুন একটি সিস্টেম এনেছে "প্রোটেক্ট"। এই অপশন টা অন করতে হলে Two factor authentication অন করতে হবে আপনাকে।

একদিকে যারা "প্রোটেক্ট" অন করার জন্য নোটিফিকশান পেয়েছে তারা অন না করলে আইডি ইউজ করতে পারছে না। আবার প্রোটেক্ট বা Two factor authentication অন করলে অনেকসময় কোড আসে না। ২ দিক থেকেই ইউজাররা বিপাকে।

পরামর্শ :

যারা protect বা Two factor authentication নতুন করে চালু করতে চাচ্ছেন তারা Two factor authentication এর recover code সংরক্ষণে রাখবেন। হয় note এর মধ্যে অথবা স্ক্রীনশট নিয়ে drive এ আপলোড দিয়ে রাখবেন বা google photos এপে ব্যাকাপ দিয়ে রাখেন। অর্থাৎ যেভাবে সহজ হয় আপনি কোডগুলো সংরক্ষণে রাখবেন।

পরবর্তীতে কোড না আসলেও আপনি "রিকভারি কোড" দিয়ে সহজেই লগইন করতে পারবেন। যেমনটা আমি করি।

-Facebook-এ "GG" এর মানে কি?

GG এর অর্থ হল "Good Games" এবং এটি আক্ষরিক কয়েক দশক ধরে গেমারদের মধ্যে একটি জনপ্রিয় বাক্যাংশ। ফেসবুক এই GG শব্দটি প্রবর্তন করেছে এর কোনো পরিচয় না দিয়েই। তাই, ফেসবুক 'GG'-এর মতো

কিছু এলোমেলো অক্ষর দিয়ে এক ধরনের মিনি অ্যানিমেশন মজা দেওয়ার চেষ্টা করছে। শুধু GG নয়, ব্যবহারকারীরা তাদের স্ক্রিনে 'ggg' লিখে অ্যানিমেশনের অভিজ্ঞতাও পাচ্ছেন। বড় বা ছোট আকারে দুইবার বা তিনবার 'G' টাইপ করুন, এটি Facebook স্ক্রিনে অ্যানিমেশন ট্রিগার করে।

অনলাইন গেমস - বিশেষ করে স্টারক্রাফট - 90 এর দশকে জনপ্রিয়তা পেতে শুরু করলে, খেলোয়াড়দের মধ্যে যথাযথ অনুভূতি প্রতিষ্ঠিত হয়। অনলাইন গেমারদের জন্য একটি অলিখিত নিয়ম ছিল যে ম্যাচের শেষে, আপনার প্রতিপক্ষ ভালো খেলেছে তা বোঝাতে আপনার চ্যাটে "GG" টাইপ করা উচিত। প্রকৃতপক্ষে, "GGWP" (ভাল খেলা, ভাল খেলা) একটি জনপ্রিয় শর্টহ্যান্ড হয়ে উঠেছে।

লোকেরা আজও প্রচুর গেমে "GG" ব্যবহার করে এবং এটি অ-গেমার কথাবার্তায়ও থ্রেশহোল্ড অতিক্রম করেছে।

কিন্তু কিছুদিন যাবত একটি কথা বেশ ছড়িয়ে পড়েছে।

কমেন্টে GG লিখলে যদি কালো থাকে তাহলে বুঝতে হবে আইডি অনিরাপদ। আর যদি গোলাপী হয় তাহলে আইডি নিরাপদ। এটা ভুয়া।

আরেকটি কথা প্রচলিত আছে, কমেন্টে GG লিখলে যদি কালো থাকে তাহলে বুঝতে হবে আইডির ইউজার গেমার না বা গেইম লাইক করে না। আর যদি গোলাপী হয় তাহলে আইডি আইডির ইউজার গেমার বা গেইম লাইক করে। এটাও ভুয়া তথ্য।

How to Protect Your Facebook Account from Hackers [-হ্যাকারদের হাত থেকে কিভাবে আপনার ফেসবুক অ্যাকাউন্ট রক্ষা করবেন]

আমাদের অনেকের কাছে ফেসবুক দৈনন্দিন জীবনের অংশ। এখানে আমরা বন্ধু এবং সহকর্মীদের সাথে যোগাযোগ করি, আমাদের প্রিয় সেলিব্রেটিদের অনুসরণ করি এবং সর্বশেষ খবরের শীর্ষে থাকি। আমরা অনেকেই ফেসবুককে নিজেদের এক্সটেনশন হিসেবে দেখি, যে কারণে আপনার ফেসবুক অ্যাকাউন্ট হ্যাক হওয়া অপমানজনকই হতে পারে। একটি হ্যাক হওয়া Facebook অ্যাকাউন্ট আপনার খ্যাতি নষ্ট করতে পারে, ব্যক্তিগত তথ্য প্রকাশ করতে পারে বা এমনকি আপনার অর্থ ব্যয় করতে পারে। আপনার যদি সন্দেহ হয় যে আপনার Facebook অ্যাকাউন্ট হ্যাক হয়েছে, তাহলে প্রথমেই আপনার পাসওয়ার্ড পরিবর্তন করতে হবে।

√ Protecting Your Password (আপনার পাসওয়ার্ড রক্ষা)

০১. একটি শক্তিশালী, সুরক্ষিত পাসওয়ার্ড তৈরি করুন। আপনার ফেসবুক পাসওয়ার্ড অনুমান করা কঠিন হওয়া উচিত, তবে আপনার মনে রাখা সহজ। আপনার পাসওয়ার্ডে আপনার নাম, জন্মতারিখ, পোষা প্রাণী বা সাধারণ শব্দ অন্তর্ভুক্ত করা এড়িয়ে চলুন।

পাসওয়ার্ড যত দীর্ঘ হবে, অন্যদের জন্য ট্রাক করা তত কঠিন হবে। একটি শক্তিশালী পাসওয়ার্ড তৈরি করার একটি উপায় হল একটি দীর্ঘ বাক্যাংশ বা শব্দের সিরিজ যা আপনি মনে রাখতে পারেন, কিন্তু কেউ কখনও অনুমান করতে পারবে না।

আপনার পাসওয়ার্ডে সর্বদা সংখ্যা, বড় এবং ছোট হাতের অক্ষরের মিশ্রণ এবং প্রতীক অন্তর্ভুক্ত করুন। কমপক্ষে 10 টি অক্ষরের লক্ষ্য রাখুন।

একটি স্মরণীয় বাক্য বা গানের লিরিক্সের সংক্ষিপ্তসার তৈরি করার চেষ্টা করুন। উদাহরণস্বরূপ, "I'm gonna take my horse to the old town road"------ iG@Mht#th7tR9 হতে পারে! এটা কে অনুমান করবে?

০২. অন্য কোন ওয়েবসাইট বা অ্যাপে আপনার ফেসবুক পাসওয়ার্ড ব্যবহার করবেন না। আপনার ব্যবহার করা প্রতিটি পরিষেবার জন্য আপনার আলাদা পাসওয়ার্ড থাকা উচিত। উদাহরণস্বরূপ, ধরা যাক আপনি ফেসবুকের জন্য একই পাসওয়ার্ড ব্যবহার করেন যেমনটি আপনি Gmail-এর জন্য করেন। যদি আপনার Gmail হ্যাক হয়ে থাকে, হ্যাকার আপনার Facebook অ্যাকাউন্টেও অ্যাক্সেস পেতে পারে। একারনে প্রতিটা পরিষেবায় আলাদা আলাদা পাসওয়ার্ড ইউজ করুন।

০৩. একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করুন। আপনি যখন আরও শক্তিশালী এবং অনন্য পাসওয়ার্ড তৈরি করবেন, সেগুলি সব মনে রাখা কঠিন হবে। অনেক ভাল পাসওয়ার্ড ম্যানেজার পাওয়া যায় যা আপনার পাসওয়ার্ড

এনক্রিপ্ট এবং নিরাপদে সংরক্ষণ করবে যাতে আপনাকে শুধুমাত্র একটি মাস্টার পাসওয়ার্ড মনে রাখতে হবে। কিছু জনপ্রিয় বিকল্প হল LastPass, Dashlane, এবং 1password।

এমনকি আপনার অপারেটিং সিস্টেমে একটি পাসওয়ার্ড ম্যানেজারও থাকতে পারে। উদাহরণস্বরূপ, আপনার যদি ম্যাক, আইফোন বা আইপ্যাড থাকে তবে আপনি বিনামূল্যে আইক্লাউড কীচেন ব্যবহার করতে পারেন।

আপনি যদি এমন একটি ব্রাউজার ব্যবহার করেন যা আপনার পাসওয়ার্ড সংরক্ষণ করে, যেমন গুগল ক্রোম, তাহলে আপনাকে সাধারণ লেখায় দেখতে একটি মাস্টার পাসওয়ার্ড দিতে হবে। ক্রোমের ক্ষেত্রে, আপনাকে আপনার Google পাসওয়ার্ড লিখতে হবে। যদি এটি Microsoft Edge হয় এবং আপনি Windows 10 ব্যবহার করেন, তাহলে আপনাকে আপনার ডিফল্ট সাইন-ইন পাসওয়ার্ড বা PIN নিশ্চিত করতে হবে। তবে এটা অনেক সময় সমস্যা করে।

০৪. প্রতি দুই মাসে একবার আপনার পাসওয়ার্ড পরিবর্তন করুন। এটি শুধুমাত্র Facebook নয়, আপনার সমস্ত পাসওয়ার্ডের জন্য যায়। মনে রাখা কঠিন হলে সংরক্ষণে রাখার মতন একটি উপায় বের করুন।

০৫. আপনার ফেসবুক পাসওয়ার্ড কারো সাথে শেয়ার করবেন না। Facebook বা অন্য কোনো পরিষেবা থেকে কেউ কখনও কেউ পাসওয়ার্ড চাইবে না।

০৬. শুধুমাত্র বিশ্বস্ত কম্পিউটারে লগ ইন করুন। আপনি যদি এমন একটি কম্পিউটার ব্যবহার করেন যা আপনি জানেন না বা বিশ্বাস করেন না, তাহলে এমন কিছু করা এড়িয়ে চলুন যাতে আপনার পাসওয়ার্ড লিখতে হয়।

হ্যাকাররা সাধারণত কম্পিউটার সিস্টেমে কী লগার ব্যবহার করে যা পাসওয়ার্ড সহ আপনার টাইপ করা সবকিছু রেকর্ড করে।

আপনি যদি বিশ্বাস করেন না এমন একটি কম্পিউটারে লগ

ইন করতে হয়, আপনি কিছু অঞ্চলে Facebook থেকে এককালীন পাসওয়ার্ডের জন্য অনুরোধ করতে পারেন। এটি করার জন্য, 32665 নম্বরে একটি পাঠ্য বার্তা পাঠান (যদি আপনি মার্কিন যুক্তরাষ্ট্রে না থাকেন তবে আপনার নম্বরের জন্য এই তালিকাটি দেখুন) যাতে otp অক্ষর রয়েছে। যতক্ষণ না আপনার মোবাইল ফোন Facebook-এর সাথে লিঙ্ক থাকে, ততক্ষণ আপনি একটি 6-সংখ্যার অস্থায়ী পাসকোড পাবেন যা আপনি সাইন ইন করতে "পাসওয়ার্ড" ফাঁকা ব্যবহার করতে পারেন।

যদি আপনার পক্ষে এককালীন পাসওয়ার্ড ব্যবহার করা সম্ভব না হয় এবং আপনাকে অবশ্যই সাইন ইন করতে হবে, আপনার নিজের কম্পিউটার, ফোন বা ট্যাবলেটে ফিরে আসার সাথে সাথে আপনার ফেসবুক পাসওয়ার্ড পরিবর্তন করুন।

আপনার নিজের ব্যতীত অন্য কম্পিউটারে "remember password" বৈশিষ্ট্যটি ব্যবহার করা এড়িয়ে চলুন। আপনি যদি একটি পাবলিক কম্পিউটারে (বা এমনকি

একটি বন্ধুর বাড়িতেও) Facebook-এ সাইন ইন করেন, তাহলে আপনি একটি "remember password" প্রম্পট দেখতে পাবেন যা জিজ্ঞাসা করে আপনি পাসওয়ার্ডটি সংরক্ষণ করতে চান কিনা। Not Now বা অনুরূপ বিকল্পটি চয়ন করুন, অন্যথায় সেই কম্পিউটারের অন্যান্য ব্যবহারকারীরা আপনার অ্যাকাউন্টে অ্যাক্সেস পেতে পারে।

-আইডির রিচঃ কিছু কথা

আইডির রিচ কি?

আইডির রিচ বলতে আমরা যা বুঝি, নিজেকে সবার সামনে প্রদর্শন। প্রদর্শন যত বেশি রিচ তত ভালো। প্রদর্শন যত কম রিচ তত কম।

√ এক্টিভ ফ্রেন্ড; ফ্রেন্ড লিস্টে add করে নেওয়া। (অনেকেই এটা বলেন) আমি পুরোপুরি একমত নই। কারণ

অ্যাক্টিভ হলেই সে আপনার পোস্ট পাবে না।

পোস্ট কার কাছে পৌঁছবে?

• যিনি আপনার প্রতি আগ্রহী। যে আগ্রহী হবে সে অবশ্যই আপনার পোস্ট পেতে উৎসুকী থাকবে। তখন সে আপনার পোস্ট না পেলে আপনাকে সার্চ করে খোঁজে বের করবে। আপনার টাইমলাইন ঘুরে বেড়াবে। আপনার পোস্টে লাইক কমেন্ট করবে।

উপরোল্লিখিত কথা থেকে কয়েকটা বিষয় চলে আসছে যে, কার কাছে আপনার পোস্ট যেতে পারে। তবে একটু বাড়িয়ে বলবো..

১. আপনাকে যে সার্চ করে বের করবে।

২. আপনার টাইমলাইনে যে ঘুরে বেড়াবে। সার্চ করে হোক

বা সার্চ না করে হোক।

৩. যে আপনাকে লাইক কমেন্ট করবে।

৪. যার মিচুয়াল ফ্রেন্ড আপনার পোস্টে কমেন্ট করবে। তার কাছে আপনার পোস্ট যাবে।

৫. রুচির একটা ব্যাপার আছে। যে যে ধরনের পোস্ট পড়তে আগ্রহী তার কাছে ঐ ধরনের পোস্টটি পৌঁছাবে। এখন আপনার পোস্ট যদি তার আগ্রহের সাথে মিলে সে আপনার পোস্ট পাবে। নচেত না।

৬. Area. আপনি যে area তে আছেন সেই area এর ফ্রেন্ডের পোস্ট আপনি বেশি পাবেন। সে আপনার area এর হলে পাবে।

৭. ফেসবুকের কামিনিটি সিস্টেম ফলো করলে আইডির রিচ

ঠিক থাকবে। নচেৎ থাকবে না।

৮. কারো নিউ ফ্রেন্ড হলে। অর্থাৎ আপনি যখন কারো ফ্রেন্ড লিস্টে নতুন হবেন তখন নতুন নতুন আপনার পোস্ট তার কাছে পৌঁছবে।

৯. আপনাকে unfollow না করতে হবে।

১০. ফেইসবুক যে পোস্টটা জরুরী মনে করে। এবং যার জন্য জরুরি মনে করে। তার কাছে যাবে।

১১. যদি পোস্ট প্রমোট করেন। তাহলে ফ্রেন্ড না তাদের কাছেও পৌঁছবে।

১২. আপনার ফ্যান ফলোয়ার যদি বেশি হয়। এবং ফেসবুক আপনাকে কিছু ভাবে যদি।

.

উপরোল্লিখিত বিষয় কিছু এমন আছে যেগুলা সময়িক সময় পরে আবার অফ হয়ে যাবে। অর্থাৎ পোস্ট আর পৌঁছবে না। তখন আপনার ফ্রেন্ড যদি আবার ঐ সমস্ত কাজ করে তাহলে আবার পোস্ট পৌঁছতে শুরু করবে।

তবে অবশ্যই আপনাকে ফেইসবুকে একটা অবস্থান তৈরি করে নিতে হবে। যদ্দরুন মানুষ আপনাকে, আপনার লেখা কথাগুলোকে পড়বে, মানবে। এবং অপেক্ষায় থাকবে কখন আপনি পোস্ট করবেন আর তারা পড়বে।

-আইডি সেফটি

যাদের chack your important settings বা "প্রোটেক্ট" অনশনটা আসতেছে না বা নাই, তারা নিরাপত্তার জন্য নিচের 3 টি কাজ করে রাখতে পারেন।

1. একটি স্ট্রং পাসওয়ার্ড ইউজ করবেন। পাসওয়ার্ডের ধরন : nG#89f@d!f3

2. Get alert about unrecognizable logins (login alert) এ গিয়ে সবক'টা অপশন অন করে দিবেন।

3. Two factor authentication চালু করে দিবেন।

-ফেসবুকের সার্ভার ডাউন থাকলে বুঝবেন কীভাবে?

শুরুতেই ফেসবুকের প্ল্যাটফর্ম স্ট্যাটাস ওয়েবপেজ দেখুন। সেখানে কোনো সেবায় বিঘ্ন থাকলে দেখাবে। তবে পেজটি ফেসবুকের সার্ভারেই থাকে। সমস্যার ধরন বুঝে কখনো কখনো তথ্যগুলো হালনাগাদ না-ও থাকতে পারে।

টুইটারে #facebookdown হ্যাশট্যাগ খুঁজে দেখুন। অন্য ব্যবহারকারীদের টুইটে সময় দেখে বোঝার চেষ্টা করুন, একই সময় আর কেউ ফেসবুকে সমস্যার মুখে পড়েছেন কি না।

টুইটারে যখন ঢুকেছেনই, সেখানে ফেসবুকের পেজ থেকে দেখে আসতে পারেন প্রতিষ্ঠানটির পক্ষ থেকে কোনো আপডেট দেওয়া হয়েছে কি না। তবে আপনি যদি টুইটার, ইউটিউবসহ অন্যান্য জনপ্রিয় ওয়েবসাইট দেখতে না পারেন, তবে সমস্যা আপনার ডিভাইসে কিংবা ইন্টারনেট সেবাদাতা প্রতিষ্ঠানেও (আইএসপি) হতে পারে।

জনপ্রিয় ডিজিটাল প্ল্যাটফর্মগুলো বন্ধ থাকলে ব্যবহারকারীরা সচরাচর ডাউনডিটেকটর ডটকমে জানিয়ে থাকেন। এমন আরও কিছু সেবার ফেসবুক অংশ থেকে বোঝার চেষ্টা করতে পারেন, যেমন ডাউন ফর এভরিওয়ান অর জাস্ট মি, ইজ ইট ডাউন রাইট নাউ কিংবা আউটেজ ডট রিপোর্ট।

সংবাদমাধ্যমে চোখ রাখুন। ঘটনা বড় হলে দ্রুততম সময়ে খবর চলে আসার কথা।

আর কেউ যদি সমস্যার কথা না জানিয়ে থাকেন, তবে ধরে নিতে হবে সেটা আপনার প্রান্তে।

ফেসবুকে ঢুকতে না পারলে কী করবেন?

ফেসবুকের ওয়েব ঠিকানা ঠিক লিখেছেন কি না, তা দেখতে পারেন। আইওএস বা অ্যান্ড্রয়েড অ্যাপ হলে সেটি ফেসবুকের অফিশিয়াল অ্যাপ কি না, তা-ও দেখে নিতে

পারেন।

ওয়েব ব্রাউজার থেকে ফেসবুক দেখতে না পারলে অ্যাপ থেকে দেখার চেষ্টা করুন। অ্যাপে সমস্যা পেলে স্মার্টফোন বা ট্যাবের ব্রাউজারে দেখতে পারেন।

ব্রাউজারের ক্যাশ ও কুকিজ পরিষ্কার করে দেখতে পারেন। সেটিংসে অপশনগুলো পাবেন।

অ্যান্টিভাইরাস সফটওয়্যার দিয়ে ডিভাইসের ম্যালওয়্যার স্ক্যান করতে পারেন।

ডিভাইস বন্ধ করে চালু (রিস্টার্ট) করে দেখতে পারেন।

অনেক সময় স্থানীয়ভাবে ফেসবুক বন্ধ রাখা হয়। সেটা বুঝতে চাইলে ভিপিএন ব্যবহার করে পরীক্ষা করা একটি উপায়।

কোনো কিছুতেই কিছু না হলে ধরে নিতে হবে আপনার ইন্টারনেটে সমস্যা। হয় সংযোগ বন্ধ আছে, নয়তো গতি কম। আবার একসঙ্গে অনেক মানুষ এক নেটওয়ার্কে যুক্ত হলেও সমস্যা দেখা দিতে পারে।

আবার অনেক সময় ফেসবুকের পক্ষ থেকেই সেবা বিঘ্নের খবর জানিয়ে দেওয়া হয়। তেমন কোনো বার্তা পেলে পড়ে বোঝার চেষ্টা করতে পারেন। তা ছাড়া সার্ভার ডাউন থাকলে ইনস্টাগ্রাম ব্যবহারকারীদের তা জানিয়ে দেওয়ার একটি সুবিধা নিয়েও পরীক্ষা–নিরীক্ষা চলছে।

ফেসবুক নিয়ে এত মাথা ঘামিয়ে কীই–বা হবে বলুন! ফেস বাদ দিয়ে শুধু বুক (বই) নিয়ে পড়ুন। নয়তো নাক ডেকে ঘুমান।

-পাসওয়ার্ড ভুলে না যাওয়ার সহজ সমাধান

পাসওয়ার্ড মনে রাখা অধিকাংশ মানুষের জন্যই কঠিন কাজ। অথচ ডিজিটাল প্ল্যাটফর্মে আমাদের কর্মকাণ্ড যত বাড়ছে, তত বেশি পাসওয়ার্ড মনে রাখতে আমরা বাধ্য হচ্ছি। এতো পাসওয়ার্ডের ভিড়ে অনেকেই প্রায়ই জরুরি পাসওয়ার্ডটি ভুলে যান। সে কারণে প্রায় সব ওয়েবসাইটে পাসওয়ার্ড পুনরুদ্ধারের সুবিধা থাকে।

অনলাইন দুনিয়ায় গুরুত্বপূর্ণ সফটওয়্যার ও ওয়েবসাইটগুলির সুরক্ষায় পাসওয়ার্ড ব্যবহার করা হয়। ভিন্ন ভিন্ন সাইটের জন্য আলাদা পাসওয়ার্ড মনে রাখা কষ্টকর বিধায় অনেকে একটি পাসওয়ার্ড একাধিক সফটওয়্যার ও ওয়েবসাইটগুলি জন্য ব্যবহার করেন। কিন্তু মনে রাখা জরুরি, একটি পাসওয়ার্ড অনেকগুলো সাইট বা সফটওয়্যারের জন্য ব্যবহার করা হলে সবগুলো সাইট নিরাপত্তা হুমকিতে পড়ে। কারণ সেই পাসওয়ার্ড হ্যাক হলে সেটি দিয়ে বাকি সবগুলো সাইটে প্রবেশ করা যায়।

আবার নোটবুকে পাসওয়ার্ড লিখে রাখা খুবই অনিরাপদ। তাহলে কি করবেন? পাসওয়ার্ড ম্যানেজার আপনার এই

সমস্যার সমাধান দিতে পারে।

পাসওয়ার্ড ম্যানেজার আপনার অ্যাকাউন্টগুলির জন্য শক্তিশালী পাসওয়ার্ড তৈরি করে এগুলি এনক্রিপ্ট করে ভল্টে সংরক্ষণ করে এবং স্বয়ংক্রিয়ভাবে আপনার জন্য ওয়েবসাইট ও সফটওয়্যার লগইন ফর্মগুলি পূরণ করে। আলাদাভাবে পাসওয়ার্ড লগইন বক্সে লেখার প্রয়োজন হয় না।

যথেষ্ট নিরাপত্তা ব্যবস্থা মেনেই পাসওয়ার্ড ম্যানেজার সফটওয়্যারগুলো তৈরি করা হয়, নিয়মিত নিরাপত্তা হালনাগাদের ব্যবস্থাও আছে। তবু জনপ্রিয়গুলোর বাইরে কোনো পাসওয়ার্ড ম্যানেজার ব্যবহার করা মোটেই উচিত হবে না। প্রায় সব পাসওয়ার্ড ম্যানেজার অর্থ পরিশোধ করে ব্যবহার করতে হয়।

তবে ফ্রি সংস্করণ পাওয়া যায়, এমন সেবাগুলোর উল্লেখ করা হলো এখানে।

👇

লাস্টপাস

ওয়েবসাইট: www.lastpass.com

লগ মি ওয়ান্স

ওয়েবসাইট: www.logmeonce.com

বিটওয়ারডেন

ওয়েবসাইট: bitwarden.com

এবার যে সেবা ব্যবহার করতে চান সেটির ওয়েবসাইটে গিয়ে প্রয়োজন বুঝে কম্পিউটার বা স্মার্টফোনের জন্য অ্যাপ নামিয়ে নিন।

তবে পাসওয়ার্ড ম্যানেজার ব্যবহার নিরাপদ কিনা এ প্রশ্নের সদুত্তর আজো কেউ দিতে পারেননি।

-ইন্টারনেটের ব্যান্ডউইথ চুরি হয় যেভাবে

চুরি হয়ে যাচ্ছে আপনার ইন্টারনেট ব্যান্ডউইথ । অথচ বুঝতেই পারছেন না কিভাবে শেষ হল। দিনের পর দিন নিজের টাকা খরচের খাতায় যাচ্ছে। কিন্তু বিষয়টা আসলে কী?

এতদিন পর্যন্ত জালিয়াতরা বিভিন্ন তথ্য চুরির জন্য অন্যের ডিভাইসে হানা দিত। এখনও করে। কারও ডিভাইস থেকে ব্যক্তিগত তথ্য চুরি, কারও কাছ থেকে ক্রিপ্টোকারেন্সি সংক্রান্ত গোপন তথ্য হাতিয়ে নেওয়াসহ আরও বিভিন্ন ক্ষেত্রে জাল বিছিয়ে রেখেছে জালিয়াতরা। কিন্তু এবার বিভিন্ন ডিভাইসে হানা দিচ্ছে শুধুমাত্র ব্যান্ডউইথ চুরি করতে। সেই ব্যান্ডউইথ চুরি করে তা থেকে মোটা অঙ্কের টাকা রোজগার করছে জালিয়াতরা । কীভাবে এই কাজটা সম্পন্ন হচ্ছে?

পুরো কাজটির জন্য একটি প্রক্সিওয়্যার ব্যবহার করছে জালিয়াত চক্রের পাণ্ডারা। সিসকো ট্যালোস ইতিমধ্যে ওই

বিশেষ প্রক্সিওয়্যারের সন্ধান পেয়েছে। ওই ওয়্যারের মাধ্যমে বিভিন্ন ডিভাইসকে টার্গেট করা হয়। তবে এক্ষেত্রে সব ডিভাইসকে টার্গেট করতে পারে না প্রক্সিওয়্যার। মূলত যে সব সিস্টেমে বা ডিভাইসে আগে থেকেই ম্যালওয়্যার ঢুকে রয়েছে, বেছে বেছে সেই সিস্টেমগুলিতেই হামলা চালায় জালিয়াতরা।

'জেডডিনেট' নামে একটি সংস্থা জানিয়েছে, প্রক্সিওয়্যার কোনো অবৈধ কিছু নয়। বিভিন্ন গুরুত্বপূর্ণ কাজে প্রক্সিওয়্যার ব্যবহার করা হয়। কিন্তু জালিয়াতরা ওই প্রক্সিওয়্যার ব্যবহার করে খারাপ উদ্দেশ্যে। এই প্রক্সিওয়্যার টুলটিকেই অস্ত্র হিসেবে ব্যবহার করছে হ্যাকাররা। ব্যবহারকারীর অজান্তেই তাদের কোনও ডিভাইসে প্রক্সিওয়্যার সফটওয়্যারটিকে ইনস্টল করে দেওয়া হচ্ছে। এর পরেই সেই ডিভাইসের ব্যান্ডউইথ চুরি হয়ে যাচ্ছে এবং তা চলে যাচ্ছে হ্যাকারদের দখলে। এমনকী দীর্ঘদিন কেটে গেলেও ব্যবহারকারীরা বুঝতে পারে না তাদের ডিভাইসে এই ধরনের কোনও অ্যাপ রয়েছে।

কীভাবে প্রক্সিওয়্যার ইনস্টল করে দেওয়া হচ্ছে?

মূলত কোনও পাইরেটেড অ্যাপের মাধ্যমে বা কোনও সফটওয়্যারের মাধ্যমে ওই প্রক্সিওয়্যার ইনস্টল করে দেওয়া হচ্ছে।

কীভাবে বোঝা সম্ভব কোনও ডিভাইসে প্রক্সিওয়্যার রয়েছে কি না?

১) প্রতিনিয়ত ফোন বা ল্যাপটপে থাকা অ্যাপ বা সফটওয়্যারের উপর নজর রাখতে হবে। যদি দেখা যায় কোনও অ্যাপ নিজে থেকে ডাউনলোড করা হয়নি অথচ মোবাইলে দেখতে পাচ্ছেন, তাহলে তা দ্রুত ডিলিট করে দিতে হবে।

২) কোনো অ্যাপ ডাউনলোড করার আগে তার সোর্স যাচাই করতে হবে। গুগল প্লে স্টোর এবং অ্যাপল অ্যাপ স্টোর থেকে ডাউনলোড করাই ভালো।

৩) ফোনে বিল্ট ইন সিকিউরিটি স্ক্যানার থাকলে তা অ্যাকটিভ রাখতে হবে।

৪) অপরিচিত কেউ কোনও লিঙ্ক পাঠালে তাতে ক্লিক করা উচিত নয়।

৫) পাইরেটেড অ্যাপ বা সফটওয়্যার কোনও ডিভাইসে ইনস্টল করা সঠিক সিদ্ধান্ত নয়।

-ফেসবুকের সাহায্যেই 'ফেসবুক ব্যবহার নিয়ন্ত্রণ' করবেন যেভাবে

'কাঁটা দিয়ে কাঁটা তোলা'—প্রবাদটি শোনেননি এমন মানুষ খুঁজে পাওয়া মুশকিল হবে। সামাজিক যোগাযোগ মাধ্যম ফেসবুক ব্যবহারের ক্ষেত্রেও এই প্রবাদটি কাজে লাগালে সুফল মিলতে পারে। এ সুযোগ অবশ্য ফেসবুক কর্তৃপক্ষই

করে দিয়েছে।

অনেক ব্যবহারকারীর ফেসবুকে প্রবেশের পর বের হওয়ার কথা মনে থাকে না। কখন যে ঘণ্টার পর ঘণ্টা চলে যায় বুঝতেই পারেন না তারা। এভাবে ফেসবুক ব্যবহার করলে শরীরের যেমন ক্ষতি হয় তেমনি জীবন থেকে চলে যায় গুরুত্বপূর্ণ অনেক সময়।

ব্যবহারকারীদের গুরুত্বপূর্ণ সময় যেন নষ্ট না হয় সেজন্য ফেসবুক কর্তৃপক্ষ চালু রেখেছে একটি ফিচার। 'ডিজিটাল ওয়েলবিং' নামের এই ফিচার ফেসবুকে সময় ব্যয় করার পরিমাণ কমিয়ে আনতে সাহায্য করবে। আপনিও চাইলে ডিজিটাল ওয়েলবিং ফিচারের মাধ্যমে প্রতিদিন ফেসবুকের জন্য একটি নির্দিষ্ট সময় বরাদ্দ রাখতে পারবেন।

গেজেটস নাউ এক প্রতিবেদনে জানায়, ব্যবহারকারীরা যেন ফেসবুকে আসক্ত না হয়ে পড়ে সেজন্য 'ডিজিটাল ওয়েলবিং' ফিচার চালু করেছে কর্তৃপক্ষ। ফিচারটির সাহায্যে ফেসবুক ব্যবহার সীমিত করা যাবে। সামাজিক যোগাযোগ

মাধ্যমটিতে আপনি কত সময় ব্যয় করছেন তা জানা যাবে এই ফিচারের মাধ্যমে। এমনকি প্রতিদিন কী পরিমাণ সময় ফেসবুকে দিতে চান তাও নির্ধারণ করে দিতে পারবেন ব্যবহারকারীরা।

ফেসবুকের ডিজিটাল ওয়েলবিং ফিচার যেভাবে ব্যবহার করবেন—

১. স্মার্টফোনে ফেসবুক অ্যাপ ওপেন করুন।

২. ডানদিকে ওপরের কোণায় থাকা তিনটি লাইনে ক্লিক করতে হবে। এরপর 'সেটিংস অ্যান্ড প্রাইভেসি' অপশনে ক্লিক করে নিচের দিকে গেলে 'ইওর টাইম অন ফেসবুক' নামের অপশন পাবেন। এখানেই পাওয়া যাবে ডিজিটাল ওয়েলবিংয়ের সুবিধাগুলো।

৩. ম্যানেজ ইওর টাইমের নিচে 'সি টুলস' অপশনে ক্লিক করতে হবে।

৪. এখানে ‘কোয়ায়েট মোড’ এর অধীনে দুটি অপশন পাওয়া যাবে। একটি সরাসরি ‘কোয়ায়েট মোড’ এবং অন্যটি ‘শিডিউল কোয়ায়েট মোড’। কোয়ায়েট মোড চালু করলে ওই অপশনে দেওয়া নির্দিষ্ট সময়ের পর ফেসবুক স্বয়ংক্রিয়ভাবে বন্ধ হয়ে যাবে। আর শিডিউল কোয়ায়েট মোডে গিয়ে প্রতিদিন কয়টা থেকে কয়টা পর্যন্ত ফেসবুক ব্যবহার করতে চান তা নির্ধারণ করতে পারবেন।

৫. এই দুটি অপশন ছাড়াও নিচে ‘ডেইলি টাইম রিমাইন্ডার’ নামে আরও একটি অপশন আছে। এখানে গিয়ে প্রতিদিন ফেসবুক ব্যবহারের জন্য একটি সময় বরাদ্দ রাখতে পারবেন। বরাদ্দকৃত ওই সময় পার হয়ে যাওয়া মাত্রই ফেসবুক আপনাকে নোটিফিকেশনের মাধ্যমে জানিয়ে দেবে।

যেমন ধরুন, প্রতিদিন আপনি ১ ঘণ্টা ৩০ মিনিট ফেসবুক ব্যবহার করতে চান। এজন্য ডেইলি টাইম রিমাইন্ডারে গিয়ে এই সময় বেঁধে দিলেন। প্রতিদিন যখনই আপনি দেড় ঘণ্টা ফেসবুকে কাটাবেন তখনই সামাজিক যোগাযোগ

মাধ্যমটি আপনাকে জানিয়ে দেবে—আজ ফেসবুকের জন্য বরাদ্দকৃত দেড় ঘণ্টা শেষ হয়ে গেছে।

-ফেইসবুক হ্যাক, কার্যকর পদ্ধতি

ফেসবুক অ্যাকাউন্ট হ্যাকের সবচেয়ে কার্যকর ৩টি পদ্ধতি! জেনে নিন কীভাবে এই হ্যাকিং থেকে বেঁচে থাকবেন?

আপনি কি জানেন? ফেসবুক এর অ্যাক্টিভ মেম্বার কতজন? বেশি না মাত্র ১.৯৪ বিলিয়ন বা ১৯৪ কো পৃথিবীর জনসংখ্যা ৭.৫ বিলিয়ন বা ৭৫০ কোটি। তার মানে প্রতি ৭.৫ জন মানুষের মধ্যে ২ জন ফেসবুক চালায়। এই পরিসংখ্যানটি সারা পৃথিবীতে হলেও আমাদের দেশে ফেসবুকের ব্যবহারকারী গড়ে অনেক বেশি। ফেসবুক কে আমরা নানা কাজে ব্যবহার করি। আমাদের জীবনের গুরুত্বপূর্ণ মুহূর্তগুলো আমরা ফেসবুক এর মাধ্যমে শেয়ার করি। আমরা কোন সময় কোথায় আছি, কি করছি তার প্রায় সবই আমরা ফেসবুক দিয়ে আমরা শেয়ার করছি।

এমনকি কারো ফেসবুক প্রোফাইল ঘুরলে সেই ব্যক্তি সম্পর্কে অনেক কিছুই বলে দেয়া সম্ভব। কারণ আমরা ফেসবুক এর মাধ্যমেই আমাদের চিন্তাভাবনা অন্যদের জানিয়ে দিই। তাই কেউ যদি আমাদের ফেসবুক প্রোফাইল ভালভাবে একটু ঘাটাঘাটি করে তাহলে সে আপনার অনেক কিছুই বলে দিতে পারবে। এখন হয়ত আপনি বলবেন আমি সব কিছু হাইড করে রাখি। কিন্তু আপনি যতই হাইড করে রাখুন মনে রাখবেন ইন্টারনেটে কোন কিছুই সেইফ না।

আপনি যেমন অনেকের উপর নজর রাখেন তেমনি আপনার উপরও নজর রাখা হতে পারে। আমরা ফেসবুককে প্রধানত ব্যবহার করি অন্যদের সাথে যোগাযোগ করার জন্য। কিন্তু কেউ কেউ ফেসবুককে ক্ষতিকর কারণে ব্যবহার করতে পারে। আপনি যদি কোথাও গিয়ে আপনার লোকেশান সম্পর্কে টিউন দেন তাহলে আপনার ফ্রেন্ডরা জেনে যাবে আপনি বাসায় আছেন কিনা। তাই আপনার বাসা ফাঁকা পেলে অনেকেই আপনার ক্ষতি করতে পারে।

এবং এগুলো সবই করা সম্ভব আপনার ফেসবুক আইডি

হ্যাক না করেই। তাই কেউ যদি কোনভাবে আপনার ফেসবুক আইডি এর অ্যাক্সেস পেয়ে যায় তাহলে সে কি করতে পারে কখন ভেবে দেখেছেন কি?

তাই আমি আজকে দেখাবো কোন ৩ পদ্ধতিতে আপনার ফেসবুক অ্যাকাউন্ট হ্যাক হতে পারে। এবং কিভাবে আপনি সেগুলো থেকে সাবধান থাকবেন।

১. কীলগার

কীলগার হল এমন এক ধরনের সফটওয়্যার যেটি আপনার কীবোর্ড এর প্রেস করা প্রতিটি বাটন রেকর্ড করতে পারে। আপনার কম্পিউটারে কীলগার ইনস্টল করা থাকলে আপনি বুঝতেই পারবেন না। এবং কার ফেসবুক আইডি হ্যাক করতে কীলগার সবচেয়ে ভাল কাজ করে। কারণ এই পদ্ধতি সবসময় কাজ করে। তবে কীলগার এর সমস্যা হল এই সফটওয়্যারটি ভিক্টিম এর কম্পিউটারে ডাউনলোড করে একবার রান করতেই হবে। নাহলে হবে না।

তাই কীলগার সাধারণত যেসব কম্পিউটারে হ্যাকারের অ্যাক্সেস আছে সেখানে হ্যাকাররা ব্যবহার করে। এবং

আপনার কম্পিউটারে যদি কীলগার ইনস্টল করা থাকে তাহলে কম্পিউটার ওপেন করার সাথে সাথেই এই সফটওয়্যার চালু হয়ে যাবে এবং এর কাজ অর্থাৎ কীবোর্ড এর কি-প্রেস ক্যাপচার করা শুরু করে দিবে। তাই অজানা কোন লিঙ্ক থেকে কিছু নামাবেন না। কার দেয়া কোন সফটওয়্যার বা ফাইল ওপেন করার পূর্বে স্ক্যান করে নিবেন।

হার্ডওয়্যার কিলগার

এর আগে আমি সফটওয়্যার কীলগার এর কথা বলছি। কিন্তু সফটওয়্যার ব্যবহার না করেও কীবোর্ড এর বাটন প্রেস সম্পর্কে জানা যায়। এর জন্য ব্যবহার করা হয় হার্ডওয়্যার কীলগার। এই ধরনের কীলগার পেনড্রাইভ এর সাইজ এর হয় এবং সামনে ইউএসবি মেল এবং পিছনে ইউএসবি ফিমেল পোর্ট থাকে। এই কীলগার কে কীবোর্ড আর কম্পিউটার এর মাঝখানে ব্যবহার করা হয়। কীবোর্ডটিতে এর কীলগার এর সাথে কানেক্ট করে কীলগার কে কম্পিউটারের সাথে কানেক্ট করা হয়।

এর পর কীলগার তার কাজ শুরু করে দেয়। এবং পরে এই হার্ডওয়্যার কীলগার কে যেকোনো কম্পিউটারে লাগিয়ে তিনটি গোপন বাটন একসাথে চাপলেই কীলগার এর ফাইল পাওয়া যায়। এবং সেখান থেকে ভিক্টিম কি কি টাইপ করেছে তা পাওয়া যায়। এখন অনেক হার্ডওয়্যার কীলগারে ওয়াইফাই থাকে। তাই দূরে বসেই ইউজার এর ডাটা পাওয়া সম্ভব।

কিভাবে কীলগার থেকে বেঁচে থাকবেন?

তাই এই ধরনের কীলগার থেকে বাচতে ভাল মানের অ্যান্টিভাইরাস ব্যবহার করুন। ভাল দেখে একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করুন। কারণ আপনি যদি পাসওয়ার্ড টাইপ না করেন তাহলে কীলগার তা ক্যাপচার করতে পারবে না। এবং নিয়মিত পাসওয়ার্ড চেঞ্জ করুন।

২. ফিসিং

ফেসবুক আইডি হ্যাকিং এর এই পদ্ধতি সম্পর্কে এখন প্রায়

সবাই জানে। তারপরেও অনেক সময় এই পদ্ধতি ব্যবহার করে অনেক অভিজ্ঞ ব্যক্তিকেও ধোকা দেয়াও সম্ভব। বড়শি দিয়ে যেভাবে মাছ ধরে "ফিশিং" সেভাবেই কাজ করে। এর পদ্ধতি আপনি যেই ওয়েবসাইট বেশি চালান, ধরলাম ফেসবুক, সেই ওয়েবসাইট এর হুবুহু নকল একটি ওয়েবসাইট তৈরি করে। এবং যেকোনো ফ্রি হোস্টিংএ আপলোড করে দেয়। তারপরে কোন মাধ্যমে আপনাকে সেই লিঙ্ক দেয়া হয়। বেশিরভাগ সময় ফেসবুক ম্যাসেজ এর মাধ্যমে এসব লিঙ্ক ছড়িয়ে দেয়া হয়।

এবং আপনি যদি আগে থেকে না জানেন তাহলে লিঙ্ক এ ধুকে দেখবেন আপনি ফেসবুকে আছেন। আসলে আপনি হ্যাকার এর তৈরি ফেক ওয়েবসাইটে আছেন। এবার ঐ ওয়েবসাইটে আপনার ফেসবুক আইডি এর পাসওয়ার্ড চাওয়া হবে। আপনি দিয়ে দিলেই আপনার আইডির পাসওয়ার্ড হ্যাকার এর কাছে চলে যাবে।

ফিশিং থেকে কিভাবে বেঁচে থাকবেন?

তাই সাবধান। অপরিচিত কারো লিঙ্ক ব্যবহার করবেন না।

এবং যেকোনো লিঙ্ক এ ঢোকার আহে চেক করে ঢুকবেন। ইমেইল এর মাধ্যমে পাওয়া লিঙ্ক দেখলেই ঢুকবেন না। কোথা থেকে ইমেইল আসলো তা দেখে নিবেন। আর ফেসবুক বা গুরুত্বপূর্ণ ওয়েবসাইট এ ঢোকার সময় ওয়েবসাইট এর ইউ.আর.এল দেখে ঢুকবেন। কারণ ফিশিং ওয়েবসাইট এর ইন্টারফেস দেখতে একি হলেই ওয়েবসাইট আলাদা। যেহেতু ফ্রি ওয়েব হোস্টিং ব্যবহার করে এসব সাইট তৈরি করা হয় তাই ফিশিং এর ওয়েবসাইট এর লিঙ্কগুলো বিদঘুটে হয়।

৩. ম্যান ইন দা মিডেল অ্যাটাক

যদি ভিক্টিম এর খুব কাছে থাকা যায় তাহলে খুব সহজেই তার ফেসবুক বা যেকোনো আইডি হ্যাক করা সম্ভব। এবং ভিক্টিম যেই নেটওয়ার্ক এ আছে সেই একি নেটওয়ার্ক এ কানেক্ট হওয়া যায় তাহলে ভিক্টিম এর ফেসবুক আইডি হ্যাক করা সম্ভব। রাস্পবেরি পাই এবং একটি ওয়াইফাই কার্ড ব্যবহার করেই এই হ্যাকিং করা সম্ভব। রাস্পবেরি পাই দিয়ে প্রথমে ভিক্টিম এর ওয়াইফাই তে কানেক্ট হতে হয়। অনেক সময় এর জন্য ওয়াইফাই হ্যাক করা হয়। তারপরে রাস্পবেরি দিয়ে হ্যাকার রাউটার এবং ভিক্টিম এর ডিভাইস

কে বলদ বানায়।

হ্যাকার তার ডিভাইস দুয়ে রাউটারকে বলে আমি তোমার ইউজার(ভিক্টিম) এবং ভিক্টিম এর ডিভাইসকে বলে আমি রাউটার। তাই ভিক্টিমে র ডিভাইস তার সব ডাটা হ্যাকার এর কম্পিউটারের ভিতরে দিয়ে পাস করে। এবং হ্যাকার গুরুত্বপূর্ণ ডাটা পেয়ে যায়। এই পদ্ধতি সহজ মনে হলেও অনেক কঠিন।

ম্যান ইন দা মিডেল অ্যাটাক থেকে কিভাবে বেঁচে থাকবেন?

হ্যাকার যদি অনেক অভিজ্ঞ হয় তাহলে আপনি বুঝতেই পারবেন না আপনার আইডি হ্যাক হয়ে গেছে। তবে এই ধরনের হ্যাকিং থেকে বাচতে সবসময় “https” কানেকশন ব্যবহার করুন। এবং পাবলিক ওয়াইফাই ব্যবহার থেক দূরে থাকুন। আপনার বাসার ওয়াইফাই কে শক্তিশালী করুন। কঠিন পাসওয়ার্ড ব্যবহার করুন। এবং সুরক্ষিত থাকতে চাইলে ভিপিএন ব্যবহার করতে পারেন।

-ফেইসবুক মেসেঞ্জার ব্যাবহার করছেন?

আপনি যদি ফেসবুক মেসেঞ্জারের এক দশমিক তিন বিলিয়ন ব্যবহারকারীর একজন হন, তাহলে এই প্ল্যাটফর্ম থেকে আপনার সরে যাওয়ার গুরুত্বপূর্ণ কারণ রয়েছে। যদিও সাম্প্রতিক খবরে বলা হচ্ছে- এই প্ল্যাটফর্মটি নতুন করে সুরক্ষার বিষয় যোগ করছে।

তবে সেখানে একেবারে বাজে বিষয় লুকায়িত আছে। কল্পনার চেয়েও বেশি ঝুঁকিপূর্ণ করে তুলছে এই প্ল্যাটফর্ম। ফলে ফেসবুক এবং এর নিরাপত্তা বিষয়ক সিস্টেমগুলো সম্পর্কে নতুন করে প্রশ্ন উঠছে।

অ্যাপলের বিতর্কিত সিএসএএম আপডেটের বিষয়টি শিরোনামে উঠে এসেছে। তবে, ফেসবুক চুপিসারে মেসেঞ্জারে একটি বিশাল পরিবর্তন করে ফেলেছে; অ্যাপল যা করেছে তার তুলনায় এটি আপনার নিরাপত্তা এবং গোপনীয়তার ক্ষেত্রে আরো গুরুতর প্রভাব ফেলছে।

এক প্রতিবেদনে বলা হয়েছে, মেসেঞ্জারের সবচেয়ে বড় সমস্যা হলো- সবসময় ডিফল্ট এন্ড-টু-এন্ড এনক্রিপশনের অভাব। কয়েক বছর বিলম্ব করে এবং হতাশা দেখে ফেসবুক এখন বলছে যে, তারা দীর্ঘ প্রতীক্ষিত বিষয়টির কার্যকারিতা পরীক্ষা করছে। কিন্তু সেখানে দুটি বিশাল সমস্যা গোপন রয়েছে; যার উভয়টিই আপনাকে জানতে হবে, যদি আপনি অ্যাপটি ব্যবহার করা অব্যাহত রাখতে চান।

ফেসবুক তথ্য সংগ্রহের ব্যবসা করে- আমরা সবাই এটা জানি। ব্যবহারকারী সংগ্রহের ব্যবসাও আছে ফেসবুকের। শুধু সংখ্যার দিকে তাকান। ফেসবুকের চারটি অ্যাপ রয়েছে; যা তিন বিলিয়নের বেশি ইন্সটল করেছে। সেটা হলো- ফেসবুক নিজেই, মেসেঞ্জার, হোয়াটসঅ্যাপ এবং ইনস্টাগ্রাম। এর বাইরে কেবল টিকটক এই সংখ্যা ছুঁয়েছে।

কিন্তু এইসব প্ল্যাটফর্মের ব্যবহারকারী কিন্তু এক রকম নয়। সেখানে হোয়াটসঅ্যাপ একেবারেই আলাদা। আপনাকে এই প্ল্যাটফর্মে টেনে নিয়ে আসার জন্য কোনো অ্যালগরিদমিক বিষয়বস্তু নেই। এখানে স্ক্রল করার সময়সীমা নেই, শুধু

কারো সাথে কিংবা গ্রুপে চ্যাট করা যায়; যেখানে ব্যবহারকারীরা একে অপরকে গোপনীয়ভাবে বার্তা পাঠায়। ফেসবুক বিজ্ঞাপন দেখায় এবং ব্যবসায়িক পরিষেবাগুলোকে প্রমোট করে। কিন্তু হোয়াটসঅ্যাপ আলাদা।

বহু নামকরা নিরাপত্তা বিশেষজ্ঞ বলছেন, এন্ড-টু-এন্ড এনক্রিপশন সবখানে হওয়া উচিত। ইন্টারনেট সিকিউরিটি কম্পানি ইএসইটি'র জ্যাক মোরে বলেছেন, মেসেঞ্জার সব ধরনের যোগাযোগের ক্ষেত্রে এন্ড-টু-এন্ড এনক্রিপশনের গুরুত্বকে ডিফল্ট করার সঠিক সিদ্ধান্ত নিয়েছে। নিঃসন্দেহে এটি এমন একটি প্ল্যাটফর্মের প্রতি আস্থা বাড়াবে, যা সাম্প্রতিক বছরগুলোতে বন্ধ হয়ে গেছে।

ফেসবুক বলেছে, মেসেঞ্জার এনক্রিপশন এই প্ল্যাটফর্মে শিশু নির্যাতনের বিষয়টি চিহ্নিত করার ক্ষমতা কমিয়ে ফেলবে না। এ বছরের শুরুর দিকে, ফেসবুকের গ্লোবাল পলিসি ম্যানেজমেন্টের প্রধানের কাছে জানতে চাওয়া হয়েছিল- শিশু নির্যাতনের রিপোর্ট করা ঘটনাগুলো এনক্রিপশনসহ 'অদৃশ্য' বা মুছে ফেলা হবে কি না।

সেই প্রশ্নের জবাবে তিনি বলেছেন, আমি আশা করি এই সংখ্যা কমে যাবে। যদি কন্টেন্ট শেয়ার করা হয় এবং সেই কন্টেন্টে যদি আমাদের প্রবেশাধিকার না থাকে, তাহলে আমরা তা দেখতেও পারবো না এবং রিপোর্টও করতে পারবো না।

এরই অংশ হিসেবে, ফেসবুক এখন বলছে যে, তারা ব্যবহারকারীদের কিছু অধিকার দেবে; যা দ্বারা ব্যবহারকারী ঠিক করবে কে তার ইনবক্সে পৌঁছাতে পারে, তার রিক্যুয়েস্ট ফোল্ডারে কে যাবে এবং কে তাকে মোটেও বার্তা দিতে পারবে না- এসব নির্ধারণ করার সক্ষমতা দেবে। ফলে ব্যবহারকারীরা অবাঞ্ছিত মিথস্ক্রিয়া থামাতে পারবে।

- সূত্র: ফোর্বস।

-হ্যাকিং রোধে ফেসবুকের নতুন ফিচার।

ফেসবুকে কে কত জনপ্রিয় সেটা বোঝা যায় তাদের পোস্টের লাইক, রিয়েক্ট ও কমেন্ট দেখে। কিন্তু এখানে থেকে যাচ্ছে কিছু সিকিউরিটি ও প্রাইভেসি ইস্যু। এ সিকিউরিটি ও প্রাইভেসির ব্যাপারে চিন্তা করে অনেকেই চান না নিজেদের পোস্টের লাইক ও রিয়েক্ট অন্য কেউ বা অপরিচিত কেউ দেখুক। ফেসবুক এ ইউজার প্রাইভেসির কথা মাথায় নিয়ে এসেছে নতুন একটি ফিচার, যার নাম-রিয়েকশন প্রেফারেন্সেস।

ইউজার প্রাইভেসি নিয়ে জেআর টেকনোলজির ডিরেক্টর জেনিফার আলম যুগান্তরকে জানান, ফেসবুকের এ অপশনটি অনেক গুরুত্বপূর্ণ; বিশেষ করে মেয়েদের জন্য। সাধারণত ইউজারদের খুব কাছের মানুষই তাদের প্রায় পোস্টে লাভ ও বিভিন্ন পোস্ট অনুযায়ী রিয়েকশন দিয়ে থাকে। সুতরাং সে ক্ষেত্রে কিন্তু কোনো হ্যাকার বা কোনো দুষ্কৃতিকারী যদি তাদের ফলো করে তারা খুব সহজেই বুঝে

যাবে, তার ভিকটিমের কাছের লোক কারা, ভিকটিম কাদের সঙ্গে সবচেয়ে বেশি মেলামেশা করে। এ ফিচারটির মাধ্যমে ভিকটিম অনেকাংশেই ফিশিং ও আইডি হ্যাক থেকে কিছুটা হলেও নিরাপদ থাকতে পারবে। তাই ফেসবুকের এমন নতুনত্বকে সাধুবাদ জানানো যায় এবং যারা প্রাইভেসি মেইনটেইন করে থাকতে চান, তাদের উৎসাহিত করবে ফেসবুকের এ ফিচারটি ব্যবহার করতে।

যারা এ ফিচারটি ব্যবহার করতে চান তারা মোবাইল থেকে ফেসবুক অ্যাপটি ওপেন করে সরাসরি সেটিংস অপশনে চলে যাবেন, তারপর স্ক্রল করে সেটিংস অপশনের একদম নিচেই দেখতে পাবেন 'Reaction Preferences' নামে একটি অপশন আছে; সেখানে ক্লিক করলেই আপনার পোস্টে কে কে লাইক রিয়েক্ট দিয়েছে তা হাইড করতে পারবেন। আর যারা ফেসবুকের ওয়েবসাইট থেকে যারা করতে চান তারা প্রথমে 'Settings and Privacy'তে যাবেন এরপর 'News Feed Preferences' এ গিয়ে 'Reaction preferences' আপনি আপনার পছন্দমতো অপশন সিলেক্ট করতে পারবেন।

এ বিষয়ে আইটি ও সিকিউরিটি অ্যানালিস্ট রাইয়ান মালিক বলেন, যারা প্রাইভেসির কথা মাথায় রেখে ফেসবুক ইউজ করছে, তাদের জন্য এ সেটিংস খুবই গুরুত্বপূর্ণ। টার্গেটেড আইডি হ্যাক করার জন্য ও ফেসবুক অ্যাকাউন্টের কিছু সিকিউরিটি সার্ভিস ভাঙতে তাদের প্রয়োজন হয় ভিকটিমের কাছের মানুষের আইডি খুঁজে বের করা। পাশাপাশি যদি ফিশিং অ্যাটাকের কথা বলি, তাহলে সেখানেও হ্যাকাররা আপনার আইডি বা ফোন হ্যাক করার জন্য আপনার কাছের বা পরিচিত মানুষের আইডি হ্যাক করে বা ক্লোন আপনাকে ম্যালিসিয়াস লিংক পাঠাতে পারে। কারণ অনেক সময় হ্যাকারদের অপরিচিত অ্যাকাউন্ট থেকে পাঠানো লিংকে ভিকটিম ক্লিক করে না। এক্ষেত্রে ভিকটিমের লাইক-রিয়েকশন অফ করা থাকলে ভিকটিমের পরিচিত আইডি খুঁজে বের করা কিছুটা কষ্টসাধ্য। প্রাইভেসি ও সিকিউরিটির কথা চিন্তা করলে বলাই যায়, এ সার্ভিসটি নিয়ে আসা ফেসবুকের খুব ভালো একটি উদ্যোগ।

Written Habib Sarker

-লিংকে ক্লিক বা কল রিসিভ না করলেও ফোনে পেগাসাস ঢোকে কীভাবে?

অন্য স্পাইওয়্যারের সঙ্গে পেগাসাসের পার্থক্য হলো, কোনো লিংকে ক্লিক বা কল রিসিভ না করলেও এটি স্মার্টফোনে প্রবেশ করতে পারে। এরপর তথ্য সংগ্রহ করে পাচার করতে পারে, ভিডিও ধারণ করতে পারে, এমনকি স্ক্রিনশটও নিতে পারে।

প্রশ্ন হলো, ক্লিক ছাড়াই, কল রিসিভ করা ছাড়াই কীভাবে সেটি ফোনে প্রবেশ করে? 'বিবিসি সায়েন্স ফোকাস' সাময়িকীকে সেসব প্রশ্নের উত্তর দিয়েছেন কিংস কলেজ লন্ডনের সাইবার সিকিউরিটি রিসার্চ গ্রুপের প্রধান টিম স্টিভেন্স।

পেগাসাসকে এখন পর্যন্ত তৈরি সবচেয়ে শক্তিশালী স্পাইওয়্যার বলা হচ্ছে। সেটা কি ঠিক?

এটা বলা মুশকিল। হয়তো আরও শক্তিশালী কোনো

স্পাইওয়্যার থাকতে পারে, যা আমাদের গোচরে আসেনি। তবে আমরা যে স্পাইওয়্যারগুলো সম্পর্কে জানি, পেগাসাসের তথ্য হাতিয়ে নেওয়ার ক্ষমতা সেসব থেকে আলাদা।

এটি কেন আলাদা?

অতীতে আপনাকে হয়তো কেউ ই-মেইল করে বা সামাজিক যোগাযোগমাধ্যমে বার্তা পাঠিয়ে লিংকে ক্লিক করতে বলত। এরপর আপনি ওই লিংকে ক্লিক করলে খুদে একটি ক্ষতিকর সফটওয়্যার আপনার ডিভাইসে প্রবেশ করে কাজ শুরু করত।

তবে পেগাসাস কোনো কিছুতে ক্লিক করা ছাড়াই আপনার সিস্টেমে প্রবেশ করতে পারে। এটাকে বলা হয় ‘জিরো-ক্লিক’ ম্যালওয়্যার। কেউ আপনার ডিভাইসে একটি বার্তা পাঠালেই হলো। সেটা খোলারও প্রয়োজন নেই। ওই ডিভাইসের অপারেটিং সিস্টেমের ত্রুটির সুযোগ কাজে লাগায় পেগাসাস।

এটাকে বলা হয় 'জিরো-ডে ভালনারেবিলিটিস'। কারণ, সেটা ডিভাইস নির্মাতা প্রতিষ্ঠানগুলো বা গবেষকেরা খুঁজে পাননি। যখন সেটি সবার নজরে এল, তখন ক্রুটি সারানোর জন্য 'জিরো' সময় পাওয়া যায়। যে কাজের জন্য সেটি তৈরি করা হয়েছিল, ততক্ষণে তা করা হয়ে গেছে।

অ্যাপলের আইওএস বা গুগলের অ্যান্ড্রয়েডের মতো বড় অপারেটিং সিস্টেম বা অন্য সফটওয়্যারগুলোতে ত্রুটি থাকে। এটা জানা ঘটনা। কোনোটাই নিখুঁত নয়। গবেষকেরা এই ত্রুটিগুলো খুঁজে বের করে প্রতিষ্ঠানগুলোকে সারানোর জন্য বলেন। আবার প্রতিষ্ঠানগুলোও নিজ উদ্যোগে তা করে থাকে। পেগাসাসের মতো স্পাইওয়্যার এই ত্রুটিগুলো ব্যবহার করে ডিভাইসে ঢোকার সুযোগ পেয়ে থাকে।

এটা অনেকটা বাড়ির মূল দরজা-জানালা বন্ধ করে রান্নাঘরের জানালা রাতভর খোলা রাখার মতো। চোর পুরো বাড়িতে ঠিকঠাক খুঁজলে খোলা জানালার খোঁজ পেয়ে যাবেই, সে বাড়ি যত বড়ই হোক। সফটওয়্যারের ক্ষেত্রেও

সেটাই হচ্ছে।

সাংবাদিক, বিরোধী দলীয় নেতা এবং মানবাধিকার কর্মীদের ওপর পেগাসসের মাধ্যমে নজরদারী করায় হাঙ্গেরির সরকারের বিরুদ্ধে বুদাপেস্টে প্রতিবাদে অংশ নেন মানুষ
সাংবাদিক, বিরোধী দলীয় নেতা এবং মানবাধিকার কর্মীদের ওপর পেগাসসের মাধ্যমে নজরদারী করায় হাঙ্গেরির সরকারের বিরুদ্ধে বুদাপেস্টে প্রতিবাদে অংশ নেন মানুষ
রয়টার্স অর্থাৎ প্রবেশের অনেক পথ আছে পেগাসাসের। কোনো কোনো ক্ষেত্রে সেটা কেবল একটি বার্তা বা ফোন কলের মতোই সাধারণ?

আপনি যদি প্রযুক্তি সম্পর্কে ধারণা রাখেন, তবে কোনো অ্যাপ আপনার ই-মেইল বা ফোন নম্বরের তালিকায় প্রবেশের অনুমতি চাইলে আপনি সতর্ক হয়ে যাবেন। অনুমতি না দিলে সে দরজা আপনি খুললেন না। পেগাসাসের বেলায়, আপনি জানেনেই না সেখানে একটি দরজা ছিল।

পেগাসাস আপনার ফোনের জেইলব্রেক (নির্মাতা প্রতিষ্ঠানের নিরাপত্তাসুবিধা নষ্ট করে দেওয়া) করে। এরপর ফোনে প্রবেশ করে লুকিয়ে থাকে এবং ফোনে কী কী করা হচ্ছে, তা জানার সব সুযোগ পেয়ে যায়। এটা বেশ নতুন ও চমৎকার কারিগরি অর্জন।

পেগাসাসের কাজ করার জন্য ফোন কল গ্রহণ করা জরুরি?

না, আপনি যখন কাউকে কল করেন, তখন ডিজিটাল 'করমর্দন' হয়। আমার ডিভাইসটিকে কোনোভাবে আপনার ডিভাইসের সঙ্গে যোগাযোগ করতে হয়। যখন সেই যোগাযোগ স্থাপন হয়, ফোন কল রিসিভ করা হোক বা না হোক, ডেটার আদান–প্রদানের একটা পথ তৈরি হয়। আর সেই পথের সুযোগ নিয়ে থাকে জিরো-ক্লিক ম্যালওয়্যারগুলো।

পেগাসাসের নির্মাতা প্রতিষ্ঠান ইসরায়েলের এনএসও গ্রুপের বিরুদ্ধে ইসরায়েলেই প্রতিবাদে অংশ নেন মানুষ

পেগাসাসের নির্মাতা প্রতিষ্ঠান ইসরায়েলের এনএসও গ্রুপের বিরুদ্ধে ইসরায়েলেই প্রতিবাদে অংশ নেন

মানুষরয়টার্স পেগাসাস কি বৈধ?

এটা একটি জটিল প্রশ্ন। আপনি কোন দেশে আছেন, তার ওপর নির্ভর করে এর শত শত উত্তর থাকতে পারে। এখন বেশির ভাগ দেশের আইন বলে, আপনি কম্পিউটার সিস্টেমে অননুমোদিত প্রবেশাধিকার পেতে পারেন না। অর্থাৎ সিস্টেম হ্যাক করার অধিকার আপনার নেই। তবে কোনো আইনে কিন্তু বিদেশে সে কাজ করতে নিষেধ করা হয়নি। আর দুটি দেশের মধ্যে পারস্পরিক সহযোগিতা থাকলে ব্যাপারটি আরও জটিল হয়ে যায়। গোয়েন্দা তৎপরতার মতো এই বিষয়গুলোও কোনো আন্তর্জাতিক আইনে পরিষ্কারভাবে অবৈধ করা হয়নি।

এর ব্যাপারে কী করা যেতে পারে?

প্রথমে আমাদের নিশ্চিত করতে হবে, কাকে লক্ষ্য করে পেগাসাস স্পাইওয়্যার প্রয়োগ করা হয়েছে। এরপর ফোনের ডেটা ঘেঁটে বুঝতে হবে, তাতে পেগাসাস আছে কি না। এটা যদিও শনাক্ত করা কঠিন, তবে কিছু ডিজিটাল পদচিহ্ন থেকেই যায়।

এরপর আসে রাজনৈতিক বা অর্থনৈতিক সিদ্ধান্তের প্রশ্ন। পেগাসাসের নির্মাতা ইসরায়েলি প্রতিষ্ঠান এনএসও গ্রুপের গ্রাহকেরা বেশির ভাগই কোনো দেশের সরকার। সরকার কি স্বীকার করবে, তারা কী করেছে? তারা কি বলবে যে এনএসও গ্রুপের সঙ্গে চুক্তিবদ্ধ হয়েছে? যদি স্বীকার করেও থাকে, তবে বলতে পারে, কাজটি আইন প্রয়োগ বা সন্ত্রাস দমনের জন্য করা হয়েছে। গণমাধ্যম ও নাগরিক সমাজের কাছ থেকে পর্যাপ্ত চাপ না এলে এমন সত্য সামনে আসবে বলে আমার মনে হয় না।

Zero-Click Hacks:

-কীভাবে হ্যাক করে এই স্পাইওয়্যার ? এটা কতটা ভয়ঙ্কর ?

এটি এমন একটি পদ্ধতি যার লক্ষণগুলি সাধারণভাবে বোঝা সম্ভব নয়, কিন্তু এর ফল পুরো জীবন পরিবর্তন করে দিতে পারে।

Zero-Click Hacks: গোটা বিশ্ব, দেশ এবং রাজ্য-রাজনীতিতে এখন একটাই চর্চা- পেগাসাস স্পাইওয়্যার (Pegasus Spyware)। ইতিমধ্যেই খবর হয়েছে, পেগাসাস স্পাইওয়্যারের হ্যাকিং প্রসেস জিরো ক্লিক হ্যাকসকে (Zero-Click Hacks) অনুসরণ করে। এটি একটি এমন গোপন পদ্ধতি যার সঠিক ঠিকানা এখনও অবধি বুঝে উঠতে পারেনি কোনও আইটি সংস্থা। সাইবার নিরাপত্তার মাধ্যমগুলি এখন দিনরাত এক করে দিয়েছে নিরাপত্তা সংক্রান্ত দিকগুলি আরও উন্নত করার লক্ষ্যে।

তেমনই দুরন্ত গতিতে বাড়ছে জিরো ক্লিক হ্যাকের গতি। এই সাইবার হানা অত্যাধুনিক কৌশল সম্পন্ন। যার পরিণতি অত্যন্ত ভয়ানক। এটি এমন একটি পদ্ধতি যার লক্ষণগুলি সাধারণভাবে বোঝা সম্ভব নয়, কিন্তু এর ফল পুরো জীবন পরিবর্তন করে দিতে পারে।

-জিরো-ক্লিক হ্যাক আসলে কী?

এই পদ্ধতি নিয়ে বিশেষজ্ঞরা যা বলেছেন তা হল প্রাথমিক ভাবে সাইবার অ্যাটাকের ক্ষেত্রে যে কোনও কারও ফোনে ২৪ ঘণ্টা গোপন নজরদারি চালানো যায়। তার জন্য প্রথমে ফিশিং নেটওয়ার্ক বা মেসেজের মাধ্যমে একটি হ্যাকিং ইউআরএল (URL) পাঠানো হয়। সেই বিশেষ ইউআরএলটিতে ক্লিক করা মাত্রই হ্যাকারদের আওতায় চলে যায় ফোনে থাকা সব গুরুত্বপূর্ণ তথ্য সহ ব্যবহারকারীর ব্যক্তিগত জীবন। তবে জিরো ক্লিক হ্যাক পদ্ধতি এই সবের উর্ধে। এটি এতটাই শক্তিশালী হয়ে উঠেছে যে এখন আর টার্গেটকে কোনও লিঙ্কও পাঠানো হয় না, কিন্তু নির্দিষ্ট ব্যক্তি হ্যাকারদের নজরে চলে আসেন। এই পদ্ধতিকেই

জিরো-ক্লিক হ্যাক নাম দেওয়া হয়েছে।

জিরো-ক্লিক হ্যাকস সাইবার অ্যাটাক যে কোনও ভাবে হতে পারে। তাতে ব্যবহারকারী যেই ডিভাইজ-ই ব্যবহার করুক, সেটা iOS হোক বা Android, Windows বা macOS, আক্রমণ হতে পারে সিস্টেমের যে কোনও ডেটা ভেরিফিকেশনের ফাঁকফোকর দিয়ে। বিশ্বের তাবড় সফওয়্যার প্রতিষ্ঠানগুলি যারা ডেটা ভেরিফিকেশন উন্নতির কাজ করে, তারাও এখনও জিরো-ক্লিক হ্যাকস নিয়ে চিন্তিত। এই সংক্রান্ত কোনও সঠিক বার্তা দিতে পারেনি তারা এবং জিরো-ক্লিক হ্যাকের মতো অত্যাধুনিক পদ্ধতির উৎসই বা কোথা থেকে তারও কোনও হদিশ এখনও খুঁজে পাওয়া যায়নি।

-জিরো-ক্লিক হ্যাকস কী ভাবে কাজ করে?

২০১৯ সালে জনপ্রিয় মেসেজিং অ্যাপ Whatsapp প্রথম উত্থাপন করেছিল এই সংক্রান্ত হ্যাকিংয়ের কথা। Whatsapp-এ মিসড কলের মাধ্যমে টার্গেটকে আয়ত্তে আনা হত। জানা গিয়েছে, সেই সময় Whatsapp-এর

ফ্রেমওয়ার্কের ত্রুটি কাজে লাগিয়ে জিরো-ক্লিক হ্যাক করা সম্ভব হয়েছিল। এই পদ্ধতিটি ঠিক এইরকম যখন টার্গেটকে মিসড কল করা হচ্ছে সেই সময় দু'টি ডিভাইজের মধ্যে একটি ডেটা বিনিময়ের ক্ষেত্র তৈরি হয়। সেই সময়ই স্পাইওয়্যারের মতো হ্যাকিং পদ্ধতিতে অনুমতি পাওয়া যায়। আর একবার যদি এই পদ্ধতিতে সফল হওয়া যায় তাহলে হ্যাকারদের সব মুশকিল আসান হয়ে যায়। টার্গেটের ডিভাইজে সফটওয়্যার ফ্রেমওয়ার্কের গভীরে এমবেড হয়ে যায় হ্যাকাররা।

জিরো-ক্লিক হ্যাকের একটি মূল বৈশিষ্ট্য হল এরা কাজ করবার পর তার পিছনে কোনও চিহ্ন ফেলে যায় না। যার ফলে সাইবার নিরাপত্তা সংস্থাগুলি তার কোনও ট্রেস করতে পারে না। দ্য সিটিজেন ল্যাবের (The Citizen Lab) সিকিউরিটি রিসার্চার (Security Researcher) বিল মার্কজ্যাক (Bill Marczak) জিরো-ক্লিক নিয়ে বলেছেন, “জিরো ক্লিক একটি অত্যাধুনিক অ্যান্টি ফরেন্সিক ক্ষমতাসম্পন্ন প্রক্রিয়া। যা এতটাই বৃহৎ যা সহজে চিহ্নিত করা যাচ্ছে না। এর ফলে তা প্রযুক্তিগত চ্যালেঞ্জগুলি বাড়িয়ে তুলছে”।

-এই হ্যাক প্রতিরোধ করার কোনও উপায় আছে?

দ্য সিটিজেন ল্যাবের সিকিউরিটি রিসার্চার, বিল মার্কজ্যাক বলেছেন, “এই সংক্রান্ত হ্যাক সনাক্ত করা গেলেও, বর্তমান প্রযুক্তিতে নিরামূলের এখনও কোনও উপায় নেই। প্রযুক্তির আপডেটের প্রয়োজন আছে, যেহেতু দিনে দিনে জিরো-ক্লিক হ্যাকস নিজের কৌশল বৃদ্ধি করছে, যার ফলে স্পাইওয়্যার ডেভেলপাররা বিশ্বব্যাপী বাধাহীন ভাবে কাজ করে উঠতে সক্ষম হয়ে উঠছে”।

Google Project Zero-র সাইবার সিকিউরিটি এক্সপার্ট, ইয়ান বিয়ার (Ian Beer) বলেছেন, “জিরো-ক্লিক হ্যাকসের বিরুদ্ধে প্রতিরক্ষা গড়ে তোলার জন্য একটি বৃহত্তম সংগঠন তৈরি করতে হবে। যারা এক ফোরামের অন্তর্গত হয়ে কাজ করবে”।

দ্য সিটিজেন ল্যাবের সিকিউরিটি রিসার্চার, বিল মার্কজ্যাক

মনে করছেন “প্রথমেই জিরো-ক্লিক হ্যাকসকে সনাক্ত করার ক্ষমতা রাখতে হবে। তার পরে এর ওপর কাজ শুরু করতে হবে। সন্দেহজনক কোনও লক্ষণ না থাকলেও সব সময় খেয়াল রাখতে হবে ফোনের মধ্যে কোনও প্রকার অদ্ভূত কিছু দেখা যাচ্ছে কি না। এইসব ঘটনাগুলি ক্ষণস্থায়ী হতে পারে, শুধুমাত্র একবারও হতে পারে।”

শেষে একটাই কথা বলা যায়, সর্তকতা হল জীবনের সবথেকে বড় হাতিয়ার। একটু দেরিতে হলেও সব কিছু নির্মূলের উপায়ও বের হবে। ইতিমধ্যে, বিশ্বের বড় আইটি সংস্থারা নতুন হ্যাকিং পদ্ধতি নিয়ে গবেষণা চালিয়ে যাচ্ছে। আশা করা হচ্ছে খুব তাড়াতাড়ি সমাধান সূত্র বের হবে।

-স্পাইওয়্যার থেকে ফোনের সুরক্ষা

'পেগাসাস' নামের ভয়ংকর স্পাইওয়্যার তথা নজরদারি সফটওয়্যারে আতঙ্কিত স্মার্টফোন ব্যবহারকারীরা। পেগাসাসের মতো এতটা শক্তিশালী না হলেও সাইবার দুনিয়ায় রয়েছে অসংখ্য স্পাইওয়্যার। এসব স্পাইওয়্যার থেকে সুরক্ষিত থাকার কৌশল নিয়ে আজকে আপনাদের সামনে উপস্থিত আমি সাইফ।

প্রাত্যহিক ব্যস্ত জীবনের অন্যতম সঙ্গী স্মার্টফোন। স্মার্টফোনে যেন পুরো বিশ্বই আজ মুঠোবন্দি। কথা বলা, মেসেজিং কিংবা ছবি ও ভিডিও করা ছাড়াও ইন্টারনেট নির্ভর যাবতীয় কার্যক্রম চলছে স্মার্টফোনে। ফলে ব্যবহারকারীর দিনযাপন থেকে শুরু করে ব্যক্তিগত ও আর্থিক তথ্যের নিয়ন্ত্রণ নিতে এখন স্মার্টফোন হ্যাকারদের অন্যতম টার্গেটে পরিণত হয়েছে। হ্যাকারদের দৌরাত্ম্যে ব্যবহারকারীর অজান্তেই ফোনের ব্যক্তিগত তথ্য-উপাত্ত অন্যের হাতে চলে যাচ্ছে। প্রতিরোধ ব্যবস্থা যতই শক্তিশালী হচ্ছে, হ্যাকারও তত নিত্যনতুন কৌশলে অবলম্বন করে হাতিয়ে নিচ্ছে গুরুত্বপূর্ণ গোপন তথ্য। চোখের পলকে

সাইবার আক্রমণের শিকার হচ্ছেন বিশ্বজুড়ে অগণিত স্মার্টফোনসহ নানা ডিভাইস ব্যবহারকারী।

স্মার্টফোন হ্যাকিং নতুন কোনো ঘটনা নয়, তবে সম্প্রতি ইসরায়েলি প্রতিষ্ঠান 'এনএসও'র তৈরি হ্যাকিং সফটওয়্যার 'পেগাসাস' বিশ্বব্যাপী আতঙ্ক তৈরি করেছে। বিশ্বের ১৭টি গণমাধ্যমে ১৮ জুলাই একযোগে এই হ্যাকিংয়ের ঘটনা ফাঁসের পর এটি সাইবার বিশ্বের আলোচনার কেন্দ্রবিন্দুতে পরিণত হয়েছে।

গুরুত্বপূর্ণ ব্যক্তিদের স্মার্টফোনে আড়ি পাতার খবর প্রথম আসে প্যারিসভিত্তিক সংস্থা ফরবিডেন স্টোরিজ ও অ্যামনেস্টি ইন্টারন্যাশনালের কাছে। পরে দ্য গার্ডিয়ান, দ্য ওয়্যারসহ অন্য গণমাধ্যমগুলোকে জানায় তারা। 'পেগাসাস প্রজেক্ট' নামে একটি অনুসন্ধান পরিচালনা করে ৫০টি দেশে হ্যাকিংয়ের শিকার হাজারো নম্বরের সন্ধান পায় তারা। এতে জানা যায়, ইসরায়েলি প্রতিষ্ঠান এনএসও গ্রুপ পেগাসাস নামে এই ম্যালওয়্যার তৈরি করেছে, যা মোবাইল ফোনে ঢুকে ব্যবহারকারীর ছবি, মেসেজ, ই-মেইল পাচার করতে

সক্ষম এবং কল রেকর্ডসহ গোপনে মাইক্রোফোন চালু রাখতে পারে। মানবাধিকার কর্মী, সাংবাদিক থেকে শুরু করে ব্যবসায়ী, রাজনীতিবিদ, আইনজীবীর ফোন এই স্পাইওয়্যারের মাধ্যমে নজরদারিতে রাখা হয়েছিল।

সাইবার বিশ্বে অসংখ্য স্পাইওয়্যার রয়েছে যা পেগাসাসের মতো শক্তিশালী না হলেও আপনার জন্য মাথাব্যথার কারণ হতে পারে। কেননা ব্যক্তিগত ফোনে নজরদারির এই ঘটনা ছাড়াও যে কোনো সময় হ্যাকিংয়ের শিকার হতে পারে আপনার স্মার্টফোন। তবে অ্যান্ড্রয়েড অপারেটিং সিস্টেমের স্মার্টফোনের পাশাপাশি ম্যালওয়্যার প্রতিরোধী বা অ্যান্ড্রয়েড থেকে নিরাপদ বিবেচিত আইফোনের মাধ্যমে পেগাসাস ছড়িয়ে পড়ার খবর বেশ আলোড়ন তুলেছে। এখন দেখা যাচ্ছে কোনো ডিভাইসই আসলে শতভাগ নিরাপদ নয়। তবে প্রশ্ন হলো- কীভাবে এই ম্যালওয়্যারের আক্রমণ থেকে ব্যবহারকারীরা তাদের ফোন নিরাপদ রাখবেন। পেগাসাস ম্যালওয়্যার ব্যাপকভাবে ছড়িয়ে দেওয়া না হলেও অনেক ধরনের ম্যালওয়্যার তৈরির উদ্দেশ্যই থাকে অধিকসংখ্যক স্মার্টফোনে ছড়িয়ে দেওয়া। আর সব ক্ষেত্রেই নিরাপদ থাকার প্রক্রিয়া সিংহভাগ হলো স্মার্টফোন

ব্যবহারের ক্ষেত্রে সচেতনতা অবলম্বন।

-হ্যাকিং কী

হ্যাকিং এমন একটি প্রক্রিয়া যেখানে অবৈধভাবে জোরপূর্বক কোনো ডিভাইস বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে তথ্য-উপাত্ত হাতিয়ে নেওয়া হয়। মোবাইল ফোন, ল্যান্ডফোন, গাড়ি ট্র্যাকিং, ইলেকট্রনিক ডিভাইস ও যন্ত্রপাতি অবৈধভাবে ব্যবহারও হ্যাকিংয়ের আওতায় পড়ে। উন্নত নিরাপত্তা বলয়ের ইন্টারনেট কানেকশন থেকে দুর্বল ইন্টারনেট কানেকশনেও হ্যাকাররা হানা দিতে সক্ষম। অ্যান্ড্রয়েড ফোন, আইফোনসহ সব ধরনের ফোনেই হ্যাকিংয়ের ঘটনা ঘটতে পারে।

-ফোনের সুরক্ষা যেভাবে

হ্যাকিং থেকে নিরাপদ থাকার অন্যতম উপায় যে কোনো ডিভাইস ব্যবহারের ক্ষেত্রে সচেতনতা অবলম্বন। তাই বিশ্বজুড়ে ছড়িয়ে পড়া হ্যাকিং থেকে বাঁচতে বিশেষজ্ঞরা কিছু পরামর্শের পাশাপাশি ব্যক্তিগত ফোন ব্যবহারে সতর্কতার

প্রতি গুরুত্বারোপ করেন। স্মার্টফোন আমাদের নিত্যদিনের সঙ্গী, শত কাজের তথ্য-উপাত্ত আদান-প্রদানের মাধ্যম। তাই এই জরুরি ও গুরুত্বপূর্ণ ডিভাইসটি ব্যবহারে ক্ষেত্রে সব সময় কিছু বিষয়ের দিকে লক্ষ্য রাখুন-

- স্মার্টফোনে যে কোনো বার্তার লিঙ্ক এলে দুটি বিষয়ের দিকে খেয়াল রাখতে হবে- প্রেরক ও ওয়েবসাইট। যিনি বার্তাটি পাঠিয়েছেন, তিনি আপনার পরিচিত কিনা বা আপনার বিশ্বাসযোগ্য কিনা এবং যে লিঙ্কটি পাঠানো হয়েছে সেটি নির্ভরযোগ্য কোনো ওয়েবসাইটের কিনা। অধিকাংশ ক্ষেত্রেই দেখা যাচ্ছে সাইবার অপরাধীরা এ মাধ্যম দুটি ব্যবহারের চেষ্টা করছেন।

- অপরিচিত ও অনুমোদিত অ্যাপ ডাউনলোড ও ইনস্টল থেকে বিরত থাকুন। স্বীকৃত ও অনুমোদিত অ্যাপ ব্যবহার করুন। রিভিউ ও পর্যালোচনার ভিত্তিতে গ্রহণযোগ্য মনে হলে নতুন অ্যাপ ইনস্টল করুন।

- আপনার ফোনের ব্যক্তিগত এবং স্পর্শকাতর তথ্য যেন

বেহাত হয়ে না যায় সে কারণে গুগল, ফেসবুকসহ অন্য সামাজিক যোগাযোগ মাধ্যমে টু-ফ্যাক্টর অথেনটিকেশন সচল রাখুন। এটি দ্বিতীয় পর্যায়ের ভেরিফিকেশন মেথড। এতে হ্যাকাররা আপনার তথ্য নিতে বাধার সম্মুখীন হবে।

- আপনার স্মার্টফোনের অপারেটিং সিস্টেম থেকে শুরু করে সব অ্যাপ সর্বশেষ আসা সংস্করণে হালনাগাদ করে নিন। নতুন সংস্করণ এলে আপনার ডিভাইসে তা প্রদর্শিত হয়। অনেকে অবহেলায় শেষ সংস্করণ থেকে বিরত থাকেন। তবে সফটওয়্যারের সর্বশেষ হালনাগাদে নিরাপত্তার সর্বশেষ কৌশল অন্তর্ভুক্ত থাকে।

- ম্যালওয়্যার তৈরিতে সময়, শ্রম ও অর্থের খরচ কম হয় না। এরপর সেটি ব্যবহারকারীর স্মার্টফোনে ছড়িয়ে দিতে পারলে তবেই নজর রাখার সুযোগ পায় হ্যাকার। এটা তো গেল ভার্চুয়াল দিক। 'ফিজিক্যাল' দিকটাও মাথায় রাখুন। যে কেউ যেন আপনার ফোন ব্যবহার করতে না পারে সে জন্য পিন কোড, ফিঙ্গারপ্রিন্ট বা ফেস লকের মতো অপশন সচল রাখতে ভুলবেন না।

- ফ্রি পাবলিক ওয়াইফাই ব্যবহার না করাই ভালো। বিশেষ করে যখন গোপনীয় তথ্য ব্যবহার করছেন। আর ব্যবহার যদি করতেই হয়, তবে ভিপিএন একটি ভালো সমাধান হতে পারে।

- সম্ভব হলে ফোনে থাকা সংবেদনশীল তথ্য এনক্রিপ্ট করে রাখুন। আর যেসব ক্ষেত্রে দূর থেকে তথ্য মুছে ফেলার সুবিধা রিমোট ওয়াইপ আছে, সেসব ক্ষেত্রে সেটি সচল রাখুন। এতে আপনার ফোনটি হারিয়ে গেলে বা চুরি হলে অন্তত হাতে একটা অপশন থাকবে।

লোকেশন ও ডিভাইস ট্র্যাকিং পরিষেবা চালু রাখুন। ডিভাইস হারিয়ে গেলে লোকেশন ট্র্যাকিং করতে এবং ফোনের তথ্য-উপাত্ত মুছে ফেলতে পারবেন।

পাসকোড লক ও জটিল পাসওয়ার্ড ব্যবহার করুন। সংখ্যা, বর্ণ ও চিহ্নের ব্যবহারে শক্তিশালী পাসওয়ার্ড তৈরি করুন। এই পাসওয়ার্ড একাধিক স্থানে ব্যবহার থেকে বিরত থাকুন।

-আনঅফিসিয়াল অ্যাপস্টোর থেকে অ্যাপের ব্যবহার না করা, নিয়মিত ইন্টারনেট হিস্ট্রি মুছে ফেলা, ই-মেইল ও টেক্সট পাঠানোর ক্ষেত্রে সতর্ক থাকা. ভিপিএন ব্যতীত পাবলিক ওয়াইফাই ব্যবহার না করার মাধ্যমেও আমরা ফোন হ্যাকিং থেকে নিজেদের তথ্য-উপাত্ত সুরক্ষিত রাখতে পারি।

আসুন পরিচিত হই

-বিশ্বের ভয়ঙ্কর ৫ হ্যাকার

হ্যাকারদের তৎপরতা সবচেয়ে বেশি বাড়ে ইন্টারনেট আবিষ্কার এবং সম্প্রসারণের পর থেকে। ইন্টারনেটকে সকলের জন্য উন্মুক্ত রাখার উদ্যোগ হিসেবেই প্রথমযুগের হ্যাকাররা তৎপর ছিলেন।

ডিজিটাল তথ্যপ্রযুক্তি নির্ভর সংযুক্ত বিশ্বে হ্যাকিং এক বড়

হুমকির নাম। প্রতিবছর বিশ্বের বাণিজ্যিক প্রতিষ্ঠানগুলো হ্যাকিংয়ের শিকার হয়ে লাখ লাখ ডলার লোকসান দেয়। আবার হ্যাকার ঠেকাতে সাইবার নিরাপত্তার পিছনেও ব্যয় করতে হয় প্রচুর অর্থ।

হ্যাকারদের তৎপরতা সবচেয়ে বেশি বাড়ে ইন্টারনেট আবিষ্কার এবং সম্প্রসারণের পর থেকে। অনলাইনে এখন নবীন হ্যাকাররা কার্যকর হ্যাকিং টুল প্রায়ই বিনামূল্যে ডাউনলোড করার সুযোগ পাচ্ছেন।

হ্যাকিংয়ের এই প্রবণতা অবশ্য একদিনে তৈরি হয়নি। অধুনা অপেশাদার হ্যাকারদের একটি বড় অংশ তথ্য ফাঁস করে দেওয়ার সঙ্গে লিপ্ত। এরা মূলত সবার জন্য উন্মুক্ত এক ইন্টারনেট বিশ্ব ব্যবস্থায় বিশ্বাস রাখেন। তবে ইন্টারনেটকে সকলের জন্য উন্মুক্ত রাখার চেষ্টা কিন্তু প্রথমযুগের হ্যাকাররাই করেছিলেন।

আজকের দুনিয়ায় খুবই বিখ্যাত এসব হ্যাকার ইন্টারনেট সংযোগ ব্যবস্থার গুরুত্বপূর্ণ কিছু ত্রুটি আবিষ্কার করেন।

তাদের মাঝে শীর্ষ পাঁচজনের নাম প্রকাশ করেছে বিখ্যাত অ্যান্টি-ভাইরাস ও ইন্টারনেট সিকিউরিটি সফটওয়্যার সেবাদাতা ক্যাসপারেস্কি ল্যাব।

১. কেভিন মিটনিক

মার্কিন হ্যাকারদের মাঝে সবচেয়ে খ্যাতনামা কেভিন মিটনিক কিশোর বয়স থেকেই হ্যাকিংয়ে হাতযশ তৈরি করেছিলেন। ১৯৮১ সালে তিনি প্রথম প্যাসিফিক বেল নামক একটি টেলিফোন কোম্পানির কম্পিউটার ম্যানুয়াল চুরি করেন। তার পরের বছর ঘটান আরও দুঃসাহসী এক কাণ্ড।

১৯৮২ সালে তিনি হ্যাক করেন যুক্তরাষ্ট্রের অত্যাধুনিক বিমান ও ক্ষেপণাস্ত্র প্রতিরক্ষা ব্যবস্থা নোরাডের নেটওয়ার্ক। উল্লেখ্য, স্নায়ুযুদ্ধের সেই উত্তাল সময়ে সোভিয়েত পরমাণু হুমকি থেকে সতর্ক থাকতেই নোরাড তাদের সংযোগ নেটওয়ার্ক গড়ে তোলে। মিটনিকের এই হ্যাকিংয়ের ঘটনা থেকে অনুপ্রেরণা নিয়েই পরবর্তী সময়ে ১৯৮৩ সালে মুক্তি

পায় ‘ওয়ার গেমস’ নামক এক চলচ্চিত্র।

সর্বশেষ পাওয়া খবর অনুসারে মিটনিক বর্তমানে সফটওয়্যারের দুর্বলতাকে কাজে লাগাতে সক্ষম বিশেষ প্যাচ অনলাইন নিলামে বিক্রি করছেন।

২. অ্যানোনিমাস

‘অ্যানোনিমাস’ শব্দের অর্থ অজ্ঞাতনামা। আর এই নামেই ২০০৩ সাল থেকে কাজ করছে হ্যাকারদের ছোট্ট এক গ্রুপ। হ্যাকার গোষ্ঠীটি সামাজিক বিচার প্রতিষ্ঠায় বিশ্বাসী। এই লক্ষ্য থেকেই তারা ২০০৮ সালে চার্চ অব সাইন্টোলজি নামে অভিজাত কর্পোরেট ব্যবসায়ীদের এক ধর্মীয় গ্রুপের নেটওয়ার্ক হ্যাক করে।

অ্যানোনিমাস হ্যাকাররা ধর্মীয় গোষ্ঠীটির ওয়েবসাইটগুলো বন্ধ করে দেয়। ফলে গুগল সার্চ র‍্যাংকিংয়েকমে যায় এসব ওয়েবসাইটের র‍্যাংকিং। এখানেই শেষ নয়, ওই বছরের

মার্চে এখন প্রায় সকলের পরিচিত গাই ফক্স মুখোশ পরে পুরো বিশ্বব্যাপী সাইন্টোলজির কেন্দ্রগুলো ভ্রমণ করে একদল 'অ্যানো'।

নিউ ইয়র্কার ম্যাগাজিন জানায়, এফবিআই এবং অন্যান্য আইনশৃঙ্খলা রক্ষাকারী বাহিনী অ্যানোনিমাস দলের কয়েকজন সদস্যকে চিহ্নিত করতে পেরেছেন। তবে এরপরেও নেতৃত্ব কাঠামোয় সমতা থাকায় অ্যানোনিমাস'কে মুছে ফেলা প্রায় অসম্ভব।

৩. অ্যাড্রিয়ান লামো

২০ বছর বয়সী এই হ্যাকারের সবচেয়ে বড় অঘটন ঘটান ২০০১ সালে । ওই বছর ইয়াহু'র একটি কন্টেন্ট ম্যানেজমেন্ট টুল ব্যবহার করে তিনি বার্তা সংস্থা রয়টার্সের এক সংবাদে সম্পাদনা করেন। সংবাদে জুড়ে দেন, তৎকালীন মার্কিন অ্যাটর্নি জেনারেল জন অ্যাশক্রফটের এক কাল্পনিক বিবৃতি।

প্রত্যেক হ্যাকারের একটি স্বতন্ত্র বৈশিষ্ট্য থাকে। লামোর বৈশিষ্ট্য ছিল তিনি হ্যাকিংয়ের পরেই তার ভিকটিম এবং গণমাধ্যম উভয়ের কাছেই তা প্রকাশ করে দিতেন।

দ্য ওয়্যারড জানায়, ২০০2 সালে লামো একটু বেশি সাহসী হয়ে ওঠেন। এসময় তিনি নিউইয়র্ক টাইমসের দাপ্তরিক নেটওয়ার্কে অনুপ্রবেশ করে, সেখানে নিজেকে একজন বিশেষজ্ঞ পরামর্শদাতা হিসেবে অন্তর্ভুক্ত করেন। টাইমসের ডাটাবেজ ব্যবহার করে কিছু বিখ্যাত ব্যক্তিত্বের ওপর অনুসন্ধান শুরু করেন।

ব্যক্তি জীবনে আড্রিয়ান লামো যাযাবর প্রকৃতির। তার পুরো সংসার এক ব্যাকপ্যাকেই সীমাবদ্ধ। একারণেই গণমাধ্যমের কাছে দ্য হোমলেস হ্যাকার নামেই পরিচিত লামো। ২০১৮ সালে লামো মাত্র ৩৭ বছর বয়েসে মারা যান। তার আকস্মিক মৃত্যুর কোনো যথার্থ কারণ আজও উদঘাটণ করা সম্ভব হয়নি।

৪.অ্যালবার্ট গঞ্জালেজ

নিউইয়র্ক ডেইলির এক সংবাদে গঞ্জালেজের নাম দেওয়া হয়েছিলে ‘সুপানাজি’। সেদিন থেকে ওই নামেই তাকে চেনে হ্যাকিং দুনিয়ার অধিকাংশ মানুষ। মিয়ামির একটি হাইস্কুলে পড়ার সময়েই কম্পিউটার পোগ্রামিং আসক্ত কিশোরদের নিয়ে এক দল গড়ে তুলেছিনে গঞ্জালেজ। সেখান থেকেই তার পদস্খলন হয় একজন কুখ্যাত সাইবার অপরাধী হিসেবে।

সাইবার অপরাধীদের বাণিজ্যিক সাইট শ্যাডোক্রু ডটকমের একজন রীতিমতো সক্রিয় হয়ে ওঠেন গঞ্জালেজ। ওই সময়ে তাকে বাণিজ্যিক ওয়েবসাইট হ্যাকিংয়ে পৃথিবী সেরা হ্যাকার বলে গণ্য করা হতো। ২২ বছর বয়সে গঞ্জালেজকে প্রায় ১০ লাখ ক্রেডিট কার্ডের তথ্য চুরির দায়ে নিউইয়র্কে গ্রেফতার করা হয়। এরপর কারাদণ্ড এড়াতে তিনি মার্কিন সরকারের শীর্ষ গোয়েন্দা সংস্থা সিক্রেট সার্ভিসের জন্য একজন তথ্যদাতা হিসেবে কাজ করতে থাকেন।

তবে সাইবার অপরাধীদের লাগাম দেওয়া মুশকিল। সিক্রেট সার্ভিসের বেতনভোগী ইনফরমার হিসেবে কাজ করার সময়ে গঞ্জালেজ এবং তার সহযোগীরা মোট ১৮ কোটি ক্রেডিট কার্ড অ্যাকাউন্টের তথ্য চুরি করে। এসময় টিজিএক্স নামক একটি ক্রেডিট কার্ড কোম্পানি থেকে মোট ২৫ কোটি ৬০ লাখ ডলার চুরি করা হয়। ২০১৫ সালে এসব অপরাধে নেতৃত্ব দেওয়ার দায়ে যুক্তরাষ্ট্রের একটি ফেডারেল কোর্ট তাকে কারাদণ্ড দেয়।

৫. ম্যাথিউ বেভান ও রিচার্ড প্রাইস

১৯৯৬ সালে এই দুই ব্রিটিশ হ্যাক করেন বিশ্বের সুরক্ষিত কিছু সামরিক নেটওয়ার্ক। যেসব স্থাপনার নেটওয়ার্কে তারা অনুপ্রবেশ করতে সক্ষম হন এর মাঝে ছিল গ্রিফিজ বিমানঘাঁটি, ডিফেন্স ইনফরমেশন সিস্টেম এজেন্সি এবং কোরিয়ান অ্যাটমিক রিসার্চ ইনস্টিটিউড (কারি)।

ডাটা স্ট্রিম কাউবয় খ্যাত এই দুই হ্যাকার তাদের নিজেদের কর্মকাণ্ডে বিশ্বকে প্রায় তৃতীয় বিশ্বযুদ্ধের হুমকির মুখে ঠেলে

দিয়েছিলেন। উত্তর কোরিয়ার পারমাণবিক অস্ত্র গবেষণা তথ্য তারা মার্কিন সামরিক নেটওয়ার্কে ডাম্প করলে, এই হুমকি তৈরি হয়।

-হ্যাক হয়েছে কিনা কীভাবে বুঝবেন? হ্যাক হলে কী করণীয় জানুন।

বিভিন্ন কোম্পানি থেকে শুরু করে সাধারণ মানুষ, হ্যাকারদের টার্গেটে আজ সবাই। দেশ যত ডিজিটাল হচ্ছে ততই হ্যাকাররা নিজেদের পরিসরকে বিস্তার করছে। ফলে স্মার্টফোন বা প্রোফাইল হ্যাক হওয়ার ঘটনা এখন হামেশাই খবরের হেডলাইন হচ্ছে। কিন্তু বেশিরভাগ সময়েই দেখা যাচ্ছে যে, ইউজাররা তাদের ডিভাইস থেকে তথ্য চুরি যাওয়ার এই ঘটনাকে সনাক্ত করে উঠতে পারছেন না। সেহেতু বড়োসড়ো আর্থিক ক্ষতির সম্মুখীন হতে হচ্ছে তাদের। এমনকি হ্যাকাররা তাদের এই কাজে এতটাই দক্ষ হয়ে উঠেছে যে, মোবাইলের ক্যামেরাকেও তারা দূর থেকে নিয়ন্ত্রণ করার ক্ষমতা রাখে। যা ব্যক্তিগত জীবনে হস্তক্ষেপ

করার জন্য যথেষ্ট! তাই আজ আমরা এমন কয়েকটি উপায় আপনাদের জানাবো, যেগুলির মাধ্যমে আপনি বুঝতে পারবেন যে আপনার ডিভাইসকে হ্যাক করা হয়েছে কিনা। তাহলে আসুন এই উপায়গুলি জেনে নেওয়া যাক।

এই ৫টি লক্ষণ জানিয়ে দেবে আপনার মোবাইল হ্যাক হয়েছে কিনা

১. অত্যাধিক পরিমানে ব্যাটারি ড্রেন হবে

টেক জ্ঞান :Samsung, Xiaomi কে টেক্কা দিতে iPhone 13 সিরিজ আসছে অলওয়েজ অন ডিসপ্লে ফিচার সহRealme Pad আসছে বিশাল বড় ডিসপ্লে ও ৭,১০০ mAh ব্যাটারির সাথে, ফাঁস হল রেন্ডারএক্সচেঞ্জ অফারে ৬৫০ টাকার কমে কিনে নিন Poco M3, রয়েছে আকর্ষণীয় ব্যাঙ্ক অফারইলেকট্রিক স্কুটার কিনতে চান? TVS iQube শীঘ্রই দেশজুড়ে এক হাজার ডিলারশিপে উপলব্ধ হবেফাঁস হয়ে যাচ্ছে Telegram ব্যবহারকারীদের চ্যাট, সমাধান জেনে নিনআন্ডার ডিসপ্লে ক্যামেরার দ্বিতীয় ফোন, ZTE

Axon 30 5G লঞ্চ হচ্ছে ২৭ জুলাই

স্মার্টফোনের ব্যাটারি ক্যাপাসিটি সময়ের সাথে সাথে হ্রাস পায় ঠিকই, তবে এই প্রক্রিয়াটি সাধারণত সময়বহুল অর্থাৎ ধীরে ধীরে হয়। তাই আপনার ডিভাইসের ব্যাটারি লাইফ যদি হঠাৎ করে অত্যাধিক পরিমানে ড্রেন হতে থাকে, তাহলে ফোন হ্যাক হতে পারে। দ্রুত ব্যাটারি ড্রেন হওয়ার এই লক্ষণটির কারণ হলো, হ্যাকার দ্বারা প্রেরিত কোনো ম্যালিসিয়াস সফটওয়্যার যদি ডিভাইসের ব্যাকগ্রাউন্ডে সর্বদা সক্রিয় থাকে তবেই এরূপ ঘটনা ঘটে থাকে।

২. ডিভাইস পারফরম্যান্সে প্রভাব ফেলবে

সম্প্রতি যদি আপনার মোবাইলে ওয়েব পেজ ঠিক মতো লোড না হয় অথবা হ্যান্ডসেটটি ধীর গতিতে কাজ করে তাহলে বুঝতে হবে যে আপনার ডিভাইসের পারফরম্যান্সে কোনো কারণে প্রভাব পড়ছে। সেক্ষেত্রে, হতেই পারে যে আপনার ডিভাইসটি হ্যাক করা হয়েছে এবং সেটির ব্যাকগ্রাউন্ডে একটি ম্যালিসিয়াস সফটওয়্যার সর্বদা চলমান অবস্থায় আছে। এই ধরণের সফটওয়্যার আপনার অগোচরে

মোবাইলে থাকা ডেটা, ফাইল এমনকি ছবি পর্যন্ত চুরি করে নেবে, তাও আপনারই মোবাইলের সিস্টেম রিসোর্সেকে কাজে লাগিয়ে।

৩. অজ্ঞাত এবং সন্দেহজনক পপ-আপ বা অ্যাড দেখা যাবে

আপনি কি সম্প্রতি গুগল, টুইটার বা ফেসবুক ব্যবহার করার সময়ে কোনো প্রকারের অজ্ঞাত এবং সন্দেহজনক পপ-আপ বা অ্যাড দেখতে পেয়েছেন? যদি দেখতে পান তাহলে সতর্ক হয়ে যান। কারণ প্লে স্টোর সার্টিফাইড অ্যাপগুলি কখনোই আপনাকে অ্যান্টি-ভাইরাস বা কোনো টুল ইনস্টল করার জন্য পপ-আপ নোটিফিকেশন পাঠাবে না। তাই আপনার গোচরে যদি এই ধরণের ম্যালিসিয়াস পপ-আপ বা অ্যাড আসে তাহলে বুঝতে হবে আপনার মোবাইলটি অ্যাডওয়্যার দ্বারা সংক্রামিত বা সোজা কথায় হ্যাক হয়েছে।

৪. মোবাইলে অ্যাপগুলি সঠিকভাবে কাজ করবে না অথবা অপরিচিত অ্যাপ দেখা যাবে

হোয়াটসঅ্যাপ বা ইনস্টাগ্রামের মতো অ্যাপ যেগুলিকে আপনি নিয়মিত ব্যবহার করেন, সেগুলি যদি ফ্রীজ (আটকে) হয়ে যায়, অথবা বিনাকারণে কাজ করা বন্ধ করে দেয় তাহলে কিন্তু চিন্তার বিষয়। সম্ভবত আপনার ডিভাইসে এমন কোনো ক্ষতিকারক সফটওয়্যার ঘাপটি দিয়ে আছে, যা মোবাইলের সিস্টেম রিসোর্সকে ব্যবহার করে মেমোরিকে নিঃশেষ করে দিচ্ছে। আর ডিভাইস মেমোরি কমে গেলে স্বাভাবিক ভাবেই অ্যাপগুলি কাজ করা বন্ধ করে দেবে।

৫. ইন্টারনেট ডেটার ব্যবহার মাত্রাতিরিক্ত বেড়ে যাবে

অ্যাডওয়্যার দ্বারা সংক্রামিত একটি ডিভাইস প্রতি মুহূর্তে নিজেকে আপডেট রাখার জন্য, ম্যালিসিয়াস সার্ভারের ব্যবহার করে ম্যালওয়্যার ডাউনলোড করতে থাকে। আবার হ্যাকারের কাছে মোবাইল ইউজারের কন্টাক্ট, ছবি এবং ফাইলের মতো ব্যক্তিগত ডেটাগুলিকে পাঠানোর কাজটিও এই ম্যালওয়্যার সফটওয়্যারটি করে থাকে। আর এই পুরো কর্মকান্ড সম্পন্ন করার জন্য এটি আপনারই মোবাইল ডেটা বা ওয়াই-ফাই ব্যবহার করে। ফলে মাত্রাতিরিক্ত ডেটা খরচ

হওয়া স্বাভাবিক। তাই আপনার ডিভাইসে যদি আকস্মিক ডেটা খরচ বেড়ে যায় তাহলে বুঝতে হবে যে আড়াল থেকে অন্য কেউ আপনার মোবাইলকে চালনা করছে।

হ্যাকারের হাত থেকে ডিভাইসকে সুরক্ষিত রাখতে কী কী করা উচিত?

আপনার ব্যক্তিগত তথ্যাদি যাতে অচেনা কোনো ব্যক্তির হাতে না পরে তার জন্য কয়েকটি বিষয়ে খেয়াল রাখতে হবে। যেমন, গুগল প্লে স্টোর বা অ্যাপেলের অ্যাপ স্টোর ছাড়া অন্য কোনো রিসোর্স থেকে কিছু ডাউনলোড করবেন না। অনলাইন অ্যাড দেখে কোনো অ্যাপ ইনস্টল করবেন না। বিশেষ করে, APK ফাইল একদমই ডাউনলোড করবেন না। কারণ এগুলির মাধ্যমেই ম্যালিসিয়াস সফটওয়্যার আপনার ডিভাইসে প্রবেশ করতে পারে। সর্বোপরি, পাবলিক নেটওয়ার্ক ব্যবহারের সময়ে অধিক সাবধানতা অবলম্বন করুন।

হ্যাক হওয়া ডিভাইসকে কীভাবে রিস্টোর করবেন ?

যাদের ফোন হ্যাক গিয়েছে তারা, Sophos, Malwarebytes, AVG অথবা Kaspersky কোম্পানির অ্যান্টি-ম্যালওয়্যার অ্যাপ ইন্সটল করতে পারেন। এই অ্যাপগুলির মাধ্যমে আপনারা মোবাইল স্ক্যান করে অজ্ঞাত তথা সন্দেহজনক অ্যাপকে চিহ্নিত করতে এবং সেগুলিকে আনইনস্টল করতে পারবেন। এছাড়া, আপনারা নিজেদের ব্যক্তিগত ডেটা ও ফাইলের একটি ব্যাকআপ রাখতে পারেন। সাথে অবশ্যই ডিভাইসটির ফ্যাক্টরি সেটিংসকে রিসেট করতে ভুলবেন না। এগুলি করলে মোবাইলে থাকা ম্যালওয়্যার ডিভাইস থেকে অপসারিত হয়ে যাবে।

সুতরাং, এই কয়েকটি বিষয়ে আপনি নিজে যদি সতর্ক থাকেন, তবে আপনার ডিভাইসও হ্যাকারদের হাত থেকে সুরক্ষিত থাকবে।

-জিমেইলের ব্যাপারে সাবধান

আপনার Mobile Device এ লগইন করা আছে এমন যে কোন Google Gmail যদি ভিকটিম তার মোবাইলে লগইন করতে পারে তখন ভিকটিম চাইলে আপনার Mobile টা Reset করে দিতে পারবে ..!

কোনো ধরনের Fake Account থেকে আপনাকে বলবে তাকে একটা Gmail Creat করে দেওয়ার জন্য কিংবা তার Gmail Problem হচ্ছে একটু ঠিক করে দেওয়ার জন্য ..!!

কোনভাবে অপরিচিত কারো থেকে এমন মেসেজের ফাঁদে পা দিবেন না। আপনার Mobile এ Login Kora Gmail যদি তার Mobile এ লগইন করতে পারে কিংবা তার মোবাইলে লগইন থাকা Gmail আপনার Mobile এ Login করাতে পারে তাহলে ভিকটিম আপনার Mobile Reset করতে পারবে।

আপনার মোবাইল reset করে দেওয়া মানেই New Mobile এর মত হয়ে যাবে আপনার Mobile টি.! ..!

আপনার Download করা কোন Apps থাকবে না আপনার গ্যালারির কোন কিছু থাকবে না .! এতে করে আপনি হারাতে পারেন আপনার প্রয়োজনীয় অনেক তথ্য। সুতরাং এমন চক্র থেকে সবাই সাবধান থাকবেন।

-সাইবার বুলিং ও আমাদের করণীয়

সাইবার বুলিং কি?

সাইবার বুলিং, যাকে সাইবার বুলিং বা ভার্চুয়াল বুলিং বলা হয়, হ'ল হুমকি, হয়রানি, অবমাননা বা যেকোন ব্যক্তিগত আঘাতের মাধ্যমে কোনও ব্যক্তি বা একদল লোককে তাড়না ও হয়রানি করার জন্য ডিজিটাল মিডিয়া ব্যবহার করা is টেলিফোনি, ইন্টারনেট, অনলাইন ভিডিও গেমস,

সোশ্যাল নেটওয়ার্ক ইত্যাদির মতো টেলিমেটিক যোগাযোগ প্রযুক্তির মাধ্যমের মাধ্যমে অন্তরঙ্গ তথ্যের প্রকাশের অন্য ধরণের । এটি কোনও ফৌজদারি অপরাধ হতে পারে। সাইবার বুলিংয়ে বৈদ্যুতিন মাধ্যমে প্রক্রিয়া করা ঘন ঘন, পুনরাবৃত্তিক ক্ষতিতে জড়িত। বর্বরতা আক্রান্তদের আবেগজনিত উদ্বেগ, অস্থিরতা ও উদ্দীপনা জাগিয়ে তোলে এবং ইচ্ছাকৃতভাবে যোগাযোগের জন্য কোনও আসল উদ্দেশ্য নেই।

.

সামাজিক যোগাযোগের মাধ্যমগুলোতে এখন নানা ধরনের বিড়ম্বনার শিকার হচ্ছেন নেটিজেনরা। ফেসবুক, ম্যাসেঞ্জার, টুইটার, ভাইবার, হোয়াটসঅ্যাপ ইত্যাদির মাধ্যমে তারা সাইবার অপরাধীদের শিকারে পরিণত হচ্ছেন। এর মধ্যে অন্যতম হচ্ছে সাইবার বুলিং। নারীরা ও শিশুরা এর প্রধান শিকার।

ভার্চুয়াল প্ল্যাটফরমে কারো ব্যক্তিগত দুর্বলতাকে কাজে লাগিয়ে হেয় প্রতিপন্ন করা, ভয় দেখানো বা মানসিক

নির্যাতন বা অন্যায় কোনো কিছুতে প্রলুব্ধ করা ইত্যাদি হলো সাইবার বুলিং। কিশোর-কিশোরীরাই প্রথম দিকে এ ধরনের হয়রানির শিকার হচ্ছিল। এখন মধ্যবয়সীরাও এ ফাঁদে পা দিচ্ছেন।

বাংলাদেশে স্কুল, কলেজ ও বিশ্ববিদ্যালয়ের ছাত্রীসহ ফেসবুক ব্যবহারকারীদের একটি বড় অংশ সাইবার বুলিংয়ের শিকার। তথ্য বলছে দেশের ৪৯ শতাংশ স্কুলপড়ুয়া শিক্ষার্থী সাইবার বুলিংয়ের নিয়মিত শিকার। ডাক ও টেলিযোগাযোগ মন্ত্রণালয়ের হিসাব মতে, দেশের তিন-চতুর্থাংশ নারীই সাইবার বুলিংয়ের শিকার।

তবে এ বিষয়টি অপ্রকাশিতই থেকে যায়। মাত্র ২৬ শতাংশ অনলাইনে নির্যাতনের বিষয়টি প্রকাশ করে অভিযোগ দায়ের করেন। বাকিরা ভয়ে থাকেন অভিযোগ করলেই তাদের সামাজিকভাবে হেয়প্রতিপন্ন হতে হবে।

সাইবার বুলিং ছাড়াও মোবাইল ফোন বা ই-মেইলেও এ ধরনের নির্যাতনের ঘটনা অহরহ ঘটছে। এসবে ফলে

নারীদের মধ্যে প্রচণ্ড হতাশা, পড়াশোনায় অমনোযোগিতা, অনিদ্রা ইত্যাদি নানা সমস্যার সৃষ্টি হয়। এমনকি আত্মহননের ঘটনাও ঘটতে পারে।

সতর্ক থাকবেন যেভাবে

সাইবার বুলিংয়ে চুপ থাকার নীতিই বড় ক্ষতির অন্যতম কারণ। পরিবারের কথা ভেবে কিংবা সম্মান হারোনোর ভয়ে অনেকেই সব 'চুপচাপ' সয়ে যান কিংবা চেপে যান।অপরাধীরা এর ফলে আরো বেশি সুযোগ নেয়। তারা আর্থিক সুবিধা আদায় করতে করতে একসময় ভিকটিমকে যৌন নির্যাতনের ফাঁদেও ফেলে।

বাবা-মা যদি সহজেই সন্তানের বন্ধু হতে পারেন তাহলে এ সংকট নস্যি। সাইবার বুলিং কী, ভার্চুয়াল জগতের পরিচিতরা কেন অনিরাপদ এবং একান্ত ব্যক্তিগত তথ্য কেন সবার সঙ্গে শেয়ার করা যাবে না- এগুলো সন্তানদের বুঝিয়ে বলতে হবে। ভার্চুয়াল জগতে সন্তান কোন মাঠে খেলছে সেদিকে নজর দিতে হবে তারই সঙ্গী হয়ে। এর জন্য

গণসচেতনতা তৈরিরও বিকল্প নেই।

আইনি সহায়তা

যদি বিষয়টি পারিবারিক গণ্ডির বাইরে চলে যায়। তবে আইনের আশ্রয় নিতেই হবে। এক্ষেত্রে 'পুলিশি ঝামেলা' এড়িয়ে চললেই বরং বিপদ। আর তা আপনাকে বিপথেই পরিচালিত করবে। কিছু ধাপ অনুসরণ করলে এই কঠিন কাজই খুব সহজ হয়ে যায়।

এর মধ্যে প্রথম কাজ হচ্ছে থানায় সাধারণ ডায়েরি (জিডি) করা। তবে পরিবারের সদস্যদের সহযোগিতায় না নিয়ে একা একা থানায় যাওয়াটাও বোকামি। সঙ্গে রাখতে হবে হয়রানির প্রমাণও। স্ক্রিন শট কিংবা মেসেজ।

হয়রানির শিকার যে কেউ এখন ৯৯৯ অথবা পুলিশের ফেসবুকে পেজে নক করলেও সহায়তা পাবেন। এ ছাড়া মহিলা ও শিশুবিষয়ক মন্ত্রণালয়ের হটলাইন ১০৯২১ নম্বরে গোপনীয়তা রক্ষা করে এ ধরনের সমস্যার সমাধান করা

হয়। সরাসরি বিটিআরসি'র ফোনে ও ই-মেইলেও অভিযোগ করা যায়। বিড়ম্বনার শিকার যে অনলাইন জগতে সেই জগতেই এর সুরাহা সন্ধানেরও পথের দিশা পাওয়া যাবে।

-ফেসবুকে যেসব কাজ করতে মানা।

হঠাৎ করেই ফেসবুকে প্রবেশ করা যাচ্ছে না। কোনো কোনো পোস্ট রিমুভ হচ্ছে যাচ্ছে। মাঝে মাঝে নিজের বা নিজের ওয়ালে শেয়ার করা অন্যের পোস্টও ফ্লাগশিপ (ঢেকে) করে দিচ্ছে ফেসবুক। অনেক সময় ফ্রেন্ড রিকুয়েস্ট পাঠানো যায় না। কখনো দেখা যায় পোস্ট, কমেন্ট বা শেয়ার বন্ধ হয়ে গেছে। বহু ফেসবুক ব্যবহারকারীকে এসব সমস্যায় পড়তে হয়। সমস্যায় পড়ার পর অন্যের সাহায্য চাওয়া হয়। কিন্তু ফেসবুকের একেবারে সাধারণ নিয়মনীতি মেনে চললে এসব সমস্যা হয় না। ব্যবহারকারীদের জন্য ফেসবুকের এই নির্দিষ্ট নীতিমালাকে বলা হয় 'কমিউনিটি

স্ট্যান্ডার্ড’।

বর্তমান দুনিয়ার সবচেয়ে বড় সামাজিকমাধ্যম ফেসবুক। বিশ্বে বর্তমান এর ব্যবহারকারীর সংখ্যা প্রায় ২ দশমিক ৭ বিলিয়ন। বাংলাদেশে ফেসবুক ব্যবহারকারী সংখ্যা প্রায় ৪ কোটি ৩০ লাখ। ফেসবুকে সাধারণ ব্যবহারকারীদের পাশাপাশি রয়েছে ব্যবসায়িক কার্যক্রম। এ ছাড়া ফেসবুকের অন্য তিনটি প্লাটফর্ম রয়েছে। যেগুলো হলো; ম্যাসেঞ্জার, হোয়াটসঅ্যাপ ও ইনস্টাগ্রাম। চারটি প্লাটফর্ম কোনো না কোনোভাবে একে অন্যের সঙ্গে যুক্ত। চার প্লাটফর্মের কমিউনিটি গাইডলাইন মোটামুটি প্রায় একই রকম।

সাধারণ আমরা কোনো পণ্য বা সেবা নিলে সেখানে একটি নির্দেশিকা থাকে। তেমনি ফেসবুকের কমিউনিটি গাইডলাইন হলো এই প্লাটফর্ম ব্যবসারকারী কমিউনিটিতে যারা রয়েছেন তাদের জন্য একটি নির্দেশিকা। এখানে কী করা যাবে, কী করা যাবে না এসব বিষয়ে নির্দেশনা দেওয়া রয়েছে। ফেসবুক নিয়মিত এই নির্দেশিকা আপডেট বা হালনাগাদ করে থাকে। সর্বশেষ গত মে মাসে তাদের কমিউনিটি গাইডলাইন হালনাগাদ করা হয়েছে। এখানে মূলত দুই ধরনের নির্দেশিকা রয়েছে। একটি সাধারণ

ব্যবহারকারীদের জন্য। অন্যটি বিজ্ঞাপন দাতাদের জন্য।

সাধারণ ব্যবহারকারীদের জন্য ফেসবুকের কমিউনিটি গাইডলাইন ৬টি ভাগে বিভক্ত।

এক. সহিংসতা ও অপরাধমূলক কার্যকলাপ। দুই. নিরাপত্তা। তিন. আপত্তিজনক কনটেন্ট। চার. সত্যতা ও বিশ্বাসযোগ্যতা। পাঁচ. মেধাস্বত্ব (ইন্টেলেকচুয়াল প্রাপার্টি)। এবং ছয়. অনুরোধ ও সমাধান।

সহিংসতা ও অপরাধমূলক কার্যকলাপ:

যে কোনো ধরনের সহিংসতা এবং উসকানিমূলক পোস্ট করা যাবে না। এমনকি হিংস্র বিষয়কে আরও বেশি প্রচারের জন্য বা বিষয়টি নিয়ে মজা করার জন্য তৈরি কোনো গ্রাফিকস পোস্টও করা যাবে না। এর মধ্যে উল্লেখ্যযোগ্য হলো'

১. সহিংসতা এবং উসকানিমূলক পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

২. বিপজ্জনক ব্যক্তি এবং সংস্থার নেতিবাচক কার্যকলাপ

পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৩. সন্ত্রাসবাদী কার্যকলাপ পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৪. সংঘবদ্ধ সহিংসতা বা অপরাধমূলক কার্যক্রম পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৫. গণহত্যা (চেষ্টাসহ) বা একাধিক হত্যা ছবি বা ভিডিও পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৬. মানব পাচারকে উৎসাহিত করে এমন পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৭. কোনো অপরাধে সহায়তা বা অপরাধ প্রচার করে পোস্ট করা বা পোস্ট শেয়ার করা যাবে না।

৮. বিধিবব্ধ যার আইনগত বাধ্যবাধকতা রয়েছে এমন পোস্ট করা বা পোস্ট শেয়ার করা যাবে না। যেমন: অ্যালকোহল ও অস্ত্র।

৯. জালিয়াতি এবং প্রতারণামূরক পোস্ট।

নিরাপত্তা:

কোনো মানুষের জন্য কোনোভাবে নিরাপত্তা বিঘ্নিত হয় এমন পোস্ট করা বা অন্যের করা পোস্ট শেয়ার করা যাবে না। এর মধ্যে উল্লেখ্যযোগ্য বিষয়গুলো হলো;

১. শরীরের নিজের তৈরি আঘাতের চিহ্ন অথবা আত্মহত্যা করার চেষ্টার ছবি পোস্ট করা যাবে না। তবে আত্মহত্যা সম্পর্কিত যে কোনো সংবাদ (বিশ্বাসযোগ্য উৎস থেকে প্রাপ্ত) শেয়ার করা যাবে।

২. শিশু যৌন নির্যাতনের কোনো ধরনের লেখা, ছবি বা ভিডিও ফেসবুকে শেয়ার দেওয়া যাবে না। অন্যের পোস্ট করা কনটেন্টও শেয়ার করা যাবে না।

৩. প্রাপ্তবয়স্কদেরও কোনো নগ্নতাপূর্ণ লেখা, ছবি বা ভিডিও পোস্ট বা শেয়ার করা যাবে না।

৪. ফেসবুক ব্যবহার করে কাউকে কোন ধরনের হুমকি এবং হয়রানি করা যাবে না।

৫. যে কোনো ধরনের মানব শোষণের ভিডিও কিংবা ছবি ফেসবুক গ্রহণ করে না। যেমন: মানবপাচার, ইচ্ছার বিরুদ্ধে বাণিজ্যিক শ্রম বা অন্যান্য ক্রিয়াকলাপ।

৬. কারো ব্যক্তিগত গোপনীয়তা ফেসবুকে ফাঁস করা যাবে না। একান্ত মুহূর্তের ছবি অনুমতি ছাড়া শেয়ার করা যাবে না।

আপত্তিজনক কন্টেন্ট:

১. হিংসাত্মক বক্তৃতা লিখিত বা ভিজ্যুয়াল আকারে ফেসবুকে পোস্ট দেওয়া যাবে না। কোনো জাতি অথবা মানুষের ধর্ম, বর্ণ, লিঙ্গ কিংবা শারীরিক অক্ষমতা নিয়ে সরাসরি আক্রমণ করা যাবে না।

২.ধর্ষণ, মৃতদেহ ও দুর্ঘটনাসহ নিম্নে উল্লেখিত বিষয়াবলির ছবি অথবা ভিডিও পোস্ট করা যাবে না। যেমন; ধর্ষণের ছবি ও ভিডিও, মৃতদেহের ছবি ও ভিডিও, দৃশ্যমান অভ্যন্তরীণ অঙ্গ (খালি শরীরের ছবি), আংশিক পচে যাওয়া শরীর, কোনও ব্যক্তির মৃত্যুদণ্ডের সরাসরি সম্প্রচার, দুর্ঘটনায় রক্তপাত, মারামারি, মাথা থেকে শরীর বিচ্ছিন্ন, আগুন সরাসরি সম্প্রচার, শ্মশানে মৃতদেহ পোড়ানো, যে কোন ধরনের নির্যাতন- শিশু যৌন নির্যাতন, নারী যৌন নির্যাতন , অপ্রাপ্ত বয়স্ক নির্যাতন, প্রাণী শিকার, প্রাণী হত্যা, প্রাণী জবাই, প্রাণীর ক্ষত বা কাটা দৃশ্যমান, গর্ভপাত,

পরিত্যক্ত নবজাতক শিশু ইত্যাদি।

৩. প্রাপ্তবয়স্কদের নগ্নতা এবং যৌন কার্যকলাপ কোনো ছবি দেওয়া যাবে না। যৌনতা কার্যকলাপ নিয়ে খোলামেলা আলোচনা, যৌন আবেদন, যৌনাঙ্গের উন্মুক্ত ছবি, যৌনতা সংক্রান্ত 'ডিজিটালাইজড' ছবি ফেসবুকে দেয়া নিষিদ্ধ। নগ্নতাপূর্ণ এবং অশালীন পোস্ট দেওয়া যাবে না।

সত্যতা ও বিশ্বাসযোগ্যতা:

ফেসবুক ভুয়া আইডি, স্প্যাম, ভুয়া নিউজ সরানোসহ চিরুনি অভিযান পরিচালনা করে থাকে। সাধারণত যেসব আইডি বা কনটেন্ট ফেসবুক সরিয়ে ফেলে বা সাময়ীকভাবে ব্লক কিংসা ফ্লাগশিপ করে সেগুলো হলো;

১. কোনো কারণে কোনো আইডি ভুয়া সন্দেহ হলে।

২. স্প্যামিং করলে। যেমন, একই কমেন্ট বা পোস্ট অব্যহতভাবে বিভিন্ন গ্রুপে, পেজে বা কমেন্টে করলে।

৩. সাইবার নিরাপত্তা বিঘ্নিতমূলক পোস্ট করলে।

৪. অবিশ্বাসযোগ্য তথ্য প্রচার বা পোস্ট করলে।

৫. ভুয়া খবর পোস্ট বা শেয়ার করলে।

মেধাস্বত্ব (ইন্টেলেকচুয়াল প্রপার্টি):

ফেসবুক ইন্টেলেকচুয়াল প্রপার্টি রক্ষা করার জন্য ব্যবহারকারী এবং প্রতিষ্ঠানের নিকট প্রতিশ্রুতিবদ্ধ। ফেসবুক অন্য কারও ইন্টেলেকচুয়াল প্রপার্টি, কপিরাইট এবং ট্রেডমার্ক পোস্ট গ্রহণ করে না। এর মধ্যে মূলিত দুটি বিষয়কে গুরুত্ব দেওয়া হয়। এক. কপিরাইট। দুই. ট্রেডমার্ক।

অনুরোধ ও সমাধান:

যদি কোন ব্যবহারকারী তার নিজস্ব ফেসবুক অ্যাকাউন্ট সরাতে অনুরোধ করে তাহলে ফেসবুক তা করে থাকে। একজন নিহত ব্যবহারকারীর অ্যাকাউন্ট সরানোর অনুরোধ ফেসবুক পেলে সেটিও যাচাই-বাছাই করে ফেসবুক সরিয়ে দেয়। সাধারণত কোনো আইডি বা কনটেন্ট যদি ফেসবুকের গাইডলাইন অমান্য করে বা কারো নিরাপত্তা ক্ষুণ্ণ করে তাহলে সেই কনটেন্ট বা আইডি রিমুভ করার জন্য ফেসবুক কর্তৃপক্ষের কাছে যে কেউ অনুরোধ করতে পারেন। অভিযোগের বিষয় পর্যালোচনা করে ফেসবুক কর্তৃপক্ষ সিদ্ধান্ত দিয়ে থাকেন। এ ছাড়া অপ্রাপ্তবয়স্কদের অতিরিক্ত

সুরক্ষার জন্য ফেসবুক কর্তৃপক্ষ নিজে থেকেই এমন অনেক পদক্ষেপ নিয়ে থাকেন। ফেসবুক কর্তৃপক্ষের নিজস্ব তদারকি টিমও রয়েছে এসব বিষয় দেখভাল করতে।

উপরের কমিউনিটি স্ট্যান্ডার্ড অমান্য করলে ফেসবুক সয়ংক্রিয়ভাবে অনেকে আইডি লিমিট (রেস্ট্রিকটেড) করে দেয়। কখনো সাত দিন বা এক মাসের জন্য পোস্ট করা বন্ধ, কখনো কমেন্ট ও শেয়ার করা বন্ধ হয়। তবে এই সমস্যাগুলো একটি নির্দিষ্ট সময় পর ঠিক হয়ে যায়। এর মধ্যে যদি কারো আইডি ভুয়া মনে হয় তাহলে তার আইডি নিষ্ক্রিয় (ইনঅ্যাক্টিভ) করে দেয়া হয়। তবে ওই আইডি যদি সঠিক হয় তাহলে প্রমাণসহ (জাতীয় পরিচয়পত্রের কপি/পাসপোর্টের কপি বা অনুরূপ) অনুরোধ করলে সেই তথ্য যাচাই করে আইডি সক্রিয় করে দেয়।

-স্মার্টফোন হ্যাক হওয়ার লক্ষণ ও করণীয়

মোবাইল বা স্মার্টফোন আমাদের জীবনে জড়িয়ে আছে ওতপ্রোতভাবে। মোবাইল ফোনের আবিষ্কারের প্রধান কারণ ছিল যোগাযোগের মাধ্যমকে সহজ থেকে সহজতর করা। কিন্তু আজ একবিংশ শতাব্দীতে মোবাইল ফোন শুধুই যোগাযোগের জন্য ব্যবহার হচ্ছে না; মোবাইল ফোন এখন আমাদের দৈনন্দিন জীবনের একটি খুবই গুরুত্বপূর্ণ অংশ হয়ে গিয়েছে।

আজ আমরা মোবাইল ফোনের মাধ্যমে কেনাকাটা থেকে শুরু করে মোবাইল ফোনকে আমাদের নিজের পার্সোনাল অ্যাসিস্ট্যান্ট-এর জায়গায় ব্যবহার করছি। এই মোবাইল আমরা দেশ-বিদেশের বন্ধু, আত্মীয় সবার সাথে যোগাযোগ করতে পারছি সরাসরি ভিডিও কলের মাধ্যমে। এই মোবাইল ফোনের মাধ্যমে আমরা টাকা-পয়সা লেনদেন করছি, নিজের ব্যক্তিগত অনেক কিছুই জমা করছি এই মোবাইল ফোনের মধ্যেই।

কিন্তু কী হবে যদি কখনো আপনি জানতে পারেন আপনি এতো আপন করে স্বাদরে যে মোবাইল ফোনটি ব্যবহার করছিলেন সেটি অনেক আগে থেকেই হ্যাকারদের নিয়ন্ত্রণে ছিল? যদি জানতে পারেন কখনো আপনি আপনার যে মোবাইল ফোনটিকে এতো আপন ভেবে নিজের ব্যক্তিগত সব ডেটা জমা করছিলেন সেই মোবাইলে? এমনকি আপনার ব্যাংকার সব তথ্য চলে গিয়েছে হ্যাকারদের কাছে। আপনি মোবাইলে যেসব সোশ্যাল মিডিয়া একাউন্টগুলো ব্যবহার করছেন যদি জানতে পারেন সেগুলো সব হ্যাকারদের হাতে আছে, তারা আপনার পাসওয়ার্ড নিয়ে লগইন করছে আপনার একাউন্ট!

সাইবার জগতে এমন ভয়ঙ্কর পরিস্থিতি থেকে নিরাপদে থাকা নিয়ে বলতে চাই অনলাইন জগতে সতর্ক থাকাটা এখন নেটিজেনদের জন্য বাধ্যতামূলক। আমরা অনলাইন জগতে যত বেশি সতর্ক থাকতে পারবো ততই আমরা নিরাপদে থাকতে পারবো। মূলত আমরা অনেক সময় নিজের ব্যক্তিগত তথ্য শেয়ার করে থাকি এগুলো করা যাবে না, স্মার্টফোনে অ্যাপ ইন্সটল করার ক্ষেত্রে বেশি সতর্ক থাকতে হবে। একটি অ্যাপ ইন্সটল করিয়ে হ্যাকার

ভিকটিমের পুরো ডিভাইসের নিয়ন্ত্রণ নিয়ে নিতে পারে। সুতরাং এ ক্ষেত্রে আমাদের বেশি সতর্ক থাকতে হবে। কেউ যদি এমন কোন কিছুর শিকার হয় তাদের সেই অবস্থায় আইনশৃঙ্খলা বাহিনীর কাছে যেতে হবে।

আরেকটু বলি সাধারণত আমরা জানি যেসব জিনিস মানুষের মাঝে বেশি জনপ্রিয়, সেসব জিনিসের দিকে অসাধু ব্যক্তি বা দলের নজরও থাকে অনেক বেশি। তেমনি স্মার্টফোনেও রয়েছে সেই তালিকায়। বিভিন্ন জায়গায় বিভিন্ন ধরনের ফাঁদ পাতা থেকে শুরু করে হ্যাক করা বা ইউজারের ডেটা নিয়ে সেটি বিক্রয় করা কোন কিছুই বাদ রাখেনি তারা। তাদের ফাঁদ হিসাবে অনেক কিছু ব্যবহার করলেও যে কৌশলটি ব্যবহার করে তারা সবচেয়ে বেশি উপকৃত হয় বা ইউজারদের সবচেয়ে বেশি ক্ষতি করতে পারে তা হচ্ছে "স্মার্টফোনের অ্যাপ বা অ্যাপ্লিকেশন"।

স্মার্টফোনের নিরাপত্তার ব্যাপারে বলা হয় আমাদের দেশের প্রেক্ষিতে নেটিজেনদের প্রায় সবাই স্মার্টফোনে ইউজার কিন্তু সেই তুলনায় সাইবার স্পেসে সচেতন নাগরিক খুবই কম,

যার সুযোগ নিচ্ছে হ্যাকাররা। বেশিরভাগ ব্যক্তি পর্যায়ের আক্রমণে হ্যাকাররা প্রধানত অস্ত্র সোশ্যাল ইঞ্জিনিয়ারিং; তারা কিছু লোভনীয় ফাঁদ তৈরি করে রাখে যেমন, লটারি, লোভনীয় বিজ্ঞাপন অথবা বলে থাকে আপনার কিছু খারাপ ছবি এখানে ভাইরাল হয়েছে এই লিংকে ক্লিক করে দেখুন, এমন অনেক ফাঁদ তাদের করা থাকে।

স্মার্টফোনে অ্যাপ্লিকেশন ইন্সটল করার সময় আমাদের অনেক বেশি সতর্ক থাকতে হবে, যে অ্যাপ্লিকেশনটি ইন্সটল করবো সেটি কী ধরণের পারমিশন চাচ্ছে তার দিকে লক্ষ্য রাখতে হবে এবং অহেতুক কোন পারমিশন চাচ্ছে কি না সেটি লক্ষ্য রাখতে হবে। সন্দেহ হলে পারমিশন বন্ধ করে দিতে হবে। লিংক ও অহেতুক বিজ্ঞাপনে ক্লিক না করাই ভালো। ভালো একটি এন্টিভাইরাস ব্যবহার করুন।

আসুন জেনে নেই স্মার্টফোন হ্যাক হওয়ার লক্ষণ-

১। রেগুলার ব্যবহার করা অ্যাপসগুলো চালাতে চালাতে হটাৎ হটাৎ বন্ধ হয়ে যায় অথবা বন্ধ থেকে ওপেন হয়ে যায়

২। খুব তাড়াতাড়ি মোবাইলের চার্জ শেষ হয়ে যাওয়া

৩। ব্যাকগ্রাউন্ডে এমন কিছু অচেনা প্রসেস চলবে যা আপনি বা আপনার ব্যবহার করা কোন আপ্লিকেশনের সাথে যায় না

৪। ফোন আগের থেকে স্লো হয়ে যাবে ও অপারেশন স্পিড কমে যাবে

৫। ডেটা ট্রান্সফার (আপলোড) বেশি হয়ে যাবে

৬। ফোন স্বাভাবিক সময়ের থেকে বেশি গরম হবে

৭। ফোন অটোমেটিক রি-বুট/রিস্টার্ট হবে

৮। অটোমেটিক নাম্বার ডায়েল হবে

৯। অটোমেটিক অ্যাপস অন হবে

১০। অচেনা নাম্বার রিসেন্ট কলে খুঁজে পাওয়া ও এটার জন্যে টাকা কাটা

১১। ফোনে অনুভূত টেক্সট মেসেজ খুঁজে পাওয়া যা আপনি সেন্ড বা রিসিভ করেননি

১২। মাঝে মাঝে ফোন সুইচ অফ করতে চাইলেও অফ না হওয়া

১৩। ফোন কল চলাকালীন অদ্ভুত নয়েজ ও ইকো হওয়া

১৪। অদ্ভুত ওয়েবসাইট খুঁজে পাওয়া ব্রাউজার হিস্টোরিতে

১৫। স্মার্টফোনে রেগুলারের তুলনায় বেশি ডেটা ইউজ হওয়া

১৬। নতুন নতুন পোপ-আপ শো হওয়া

১৭। ইনফেক্টেড মোবাইলে যুক্ত মেইল থেকে মেইল যাওয়া ও স্প্যাম মেইল হিসাবে ডিটেক্ট হওয়া

১৮। হটাৎ হটাৎ কল ড্রপ হওয়া (মাঝে মাঝে নেটওয়ার্কের জন্যেও হয়)।

সতর্কতাই আমাদেরকে পারে প্রাথমিকভাবে নিরাপদ রাখতে।

-স্মার্টফোন হ্যাক হলে কী করবেন?

স্মার্টফোন ছাড়া একদিনও চলে না এখন। আপনার প্রয়োজনীয় এই ফোনটি তাই সব সময় নিরাপদে নিজের কাছেই রাখতে হয়। স্মার্টফোনটি দিয়েই আমরা কত রকমের কাজ করি। এটিই আমাদের ফেসবুক, টুইটার, হোয়াটসঅ্যাপ ইত্যাদি বিভিন্ন সোশ্যাল নেটওয়ার্কিং অ্যাপগুলোর মাধ্যমে বন্ধুদের সঙ্গে যুক্ত করে। শুধু তা-ই নয়, স্মার্টফোনে মোবাইল ব্যাংকিংয়ের মাধ্যমে টাকা-পয়সা লেনদেনও করা যায়।

স্মার্টফোন যদি কখনো হ্যাক হয় তবে আপনাকে পড়তে হয় বড় বিপাকে।হ্যাক হয়ে যেতে পারে আপনার বিভিন্ন সোশ্যাল নেটওয়ার্কিং অ্যাকাউন্টগুলো! চুরি হয়ে যেতে পারে আপনার ফোনের ছবি, ভিডিও কিংবা মোবাইল ব্যাংক অ্যাকাউন্টের তথ্য। এসব হ্যাকিংয়ের অন্যতম প্রধান শিকার হচ্ছে নারীরা। হ্যাকাররা হ্যাক করছে তাদের স্মার্টফোন। এরপর তাদের ফোনের তথ্য বা ব্যক্তিগত ছবি চুরি করে

ব্লাকমেল করছে, দাবি করছে মোটা অঙ্কের টাকা।

তাই স্মার্টফোন নিরাপদে রাখতে আপনাকে যেসব বিষয় জানা প্রয়োজন। আসুন জেনে নেই স্মার্টফোন হ্যাক হলে কী করবেন।

স্মার্টফোন হ্যাকিং কী?

স্মার্টফোন হ্যাকিং হলো অবৈধভাবে কারো স্মার্টফোনে অনুপ্রবেশ করে সেই ফোনের নিয়ন্ত্রণ নিয়ে নেয়া। এক্ষেত্রে একজন হ্যাকার ভিকটিমের ফোনটি বিভিন্ন উপায়ে নিজের নিয়ন্ত্রণে নিয়ে আসে এবং এরপর ফোনটি থেকে তার নিজের উদ্দেশ্য হাসিল করে। স্মার্টফোনটি হ্যাক হয়ে যাওয়ার পর হ্যাকার ফোনটি দিয়ে যা খুশি তা-ই করতে পারে। কোনো ফাইল, ছবি, অডিও, ভয়েসকল, টেক্সট মেসেজ সবকিছুই হ্যাকার চুরি করে নিতে পারে ভিকটিমের ফোন থেকে।

ফোন লক করে রাখুন

ফোনটি অন্যের হাত থেকে সুরক্ষিত রাখতে প্যাটার্ন কিংবা পাসকোড দিয়ে লক করে রাখুন। কোনোভাবেই অপরিচিত বা সন্দেহজনক কোনো সোর্স থেকে কোনো অ্যাপ ফোনে ইনস্টল করা যাবে না। কোনো অ্যাপ ইনস্টল করতে এন্ড্রয়েড ফোনের জন্য গুগল প্লে স্টোর আর আইফোনের জন্য অ্যাপস্টোর ব্যবহার করুন। আর যদি ফোনে

অ্যাপ ডাউনলোড করুন

প্লে স্টোর না থাকে সেক্ষেত্রে apkmirror, apk-dl এর মতো নির্ভরযোগ্য ওয়েবসাইট থেকে অ্যাপ ডাউনলোড করুন।

ওয়াইফাই ও ব্লুটুথ

ফোনের ওয়াইফাই ও ব্লুটুথ কখনোই অপ্রয়োজনে চালু রাখবেন না। আমরা প্রায় সবাই এক ফোন থেকে অন্য ফোনে কোনো কিছু আদান-প্রদান করতে ‘শেয়ারইট’

অ্যাপটি ব্যবহার করে থাকি। কিন্তু অনেক ফোনে এই অ্যাপটি ব্যবহার শেষ হওয়ার পরও ওয়াইফাই কিংবা হটস্পট চালু থাকে। তাই এই অ্যাপ ব্যবহার শেষে ওয়াইফাই চালু থাকলে অফ করে নিন।

অপরিচিত লিংক

ফেসবুক, হোয়াটসঅ্যাপ প্রভৃতি সোশ্যাল নেটওয়ার্কিং সাইটে প্রাপ্ত কোনো অপরিচিত লিংক থেকে কিছু ডাউনলোড করবেন না।

ইন্টারনেট চালু

হ্যাকিংয়ের প্রক্রিয়াটি ঘটার জন্য ভিকটিমের ফোনে ইন্টারনেট সংযোগ চালু থাকা প্রয়োজন। তাই প্রয়োজন ছাড়া ইন্টারনেট চালু না রাখলে এড়াতে পারবেন ফোন হ্যাক হওয়ার সম্ভাবনা।

ফিঙ্গারপ্রিন্ট

ফোনটি প্যাটার্ন কিংবা পাসকোড দিয়ে লক রাখুন। হ্যাকিং এড়াতে ফিঙ্গারপ্রিন্ট লক কিংবা ফেসলক পদ্ধতিগুলো খুব একটা কাজের না। কারণ জরুরি প্রয়োজনে হ্যাকার খুব সহজেই আপনার ব্যবহৃত জিনিস থেকে আপনার ফিঙ্গারপ্রিন্ট নকল করে ফিঙ্গারপ্রিন্ট লক এবং আপনার যেকোনো ছবি দিয়ে ফেস লক খুলতে পারবে।

ফ্রি ওয়াইফাই

অপরিচিত ফ্রি পাবলিক ওপেন ওয়াইফাই হটস্পটগুলোতে ফোন কানেক্ট করবেন না। কারণ ওয়াইফাই হটস্পটে কানেক্টেড ফোনগুলো হ্যাকার 'ম্যান ইন দি মিডল' পদ্ধতিতে হ্যাক করতে পারে।

ব্যক্তিগত তথ্য

ফোনে এমন কোনো স্পর্শকাতর কিংবা ব্যক্তিগত তথ্য বা ছবি রাখবেন না যেগুলো অন্যের হাতে পড়লে আপনার ক্ষতি হতে পারে।

-ফেসবুক স্ট্যাটাসঃ পিকচার বা স্টিকার কমেন্ট আইডি বাঁচাতে পারে?

ফেসবুক আইডি বাঁচাতে অনেকে দেয়া স্ট্যাটাসে বন্ধুরা মন্তব্য করেছেন, কিন্তু তা কি সত্যিই আইডি বাঁচাতে পারে?

'আমার ফেসবুক আইডি রিপোর্ট হচ্ছে, কমেন্টে রেসপন্স করুন প্লিজ' বা 'আইডি ঝুঁকির মধ্যে আছে, স্টিকার কমেন্ট প্লিজ'- এ ধরণের অনেক স্ট্যাটাস ফেসবুকে প্রায়ই হয়তো চোখে পড়েছে।

যারা সেই স্ট্যাটাস দিয়েছেন, তাদের তালিকায় থাকা বন্ধুরা অসংখ্য মন্তব্য করে, স্ট্যাটাস দিয়ে সেই ফেসবুক আইডি রক্ষার চেষ্টাও করেছেন।

কিন্তু বাস্তবে এরকম মন্তব্য কতটা কাজে আসে? সত্যিই কি এসব স্টিকারের মাধ্যমে করা মন্তব্য ফেসবুক আইডি বাঁচাতে পারে?

বিবিসি বাংলার এ বিষয়ে জাহিদুল ইসলামকে জিজ্ঞাসা করা হলে তিনি লিখেছেন , আজকে আইডিতে রিপোর্ট পড়ছে ৫৬টা:/ প্লিজ ১০০০ কমেন্ট দরকার :/ :(। তার এই স্ট্যাটাসে কমেন্ট পড়েছে এগারোশোর বেশি।

তিনি বলছেন, "এখনকার একটি ট্রেন্ড হচ্ছে, যারা একটি চেতনা বা ভাবনাচিন্তার পক্ষের লোক, তার অন্য পক্ষকে টার্গেট করে ফেসবুকে রিপোর্ট করে। অনেক সময় স্বার্থ জড়িত কারণেও এটা ঘটে। তখন ফেসবুক থেকে নোটিশ

আসে, লগইন করা সম্ভব হয়না। কিন্তু এভাবে কমেন্টের মাধ্যমে যদি অনেক মানুষের সঙ্গে সংযোগ হয়, তখন হয়তো সেটি আইডির পরিচিতির জন্য ভালো হয়।"

তিনি বলছেন, এই চিন্তা করেই তিনি ওই স্ট্যাটাসটি দিয়েছিলেন। একহাজার মন্তব্য চেয়েছিলেন, কিন্তু ভাবতে পারেনি যে সেটি বারোশো ছাড়িয়ে যাবে।

ফেসবুক ঘেঁটে এরকম আরো অনেকের স্ট্যাটাস দেখা গেছে। সেসব স্ট্যাটাসে যেমন কেউ নানা ধরণের মন্তব্য লিখেছেন, আবার কেউ শুধুমাত্র ইমোজি পোস্ট করেছেন।

আরেকজন ফেসবুক ব্যবহারকারী রায়ান কামাল নিজের ছবির সঙ্গে লিখেছেন, 'আইডিতে রিপোর্ট হচ্ছে, কমেন্টে রেস্পন্স' করুন। সঙ্গে চিন্তার ইমোজি।

বরগুনার একজন তরুণী তার স্ট্যাটাসে লিখেছেন, 'আইডি ঝুঁকির মধ্যে রয়েছে, স্টিকার কমেন্ট প্লিজ'। সেখানে

স্টিকার দিয়ে তার অসংখ্য বন্ধু-স্বজন কমেন্ট করেছেন, যার সংখ্যা কয়েকশো ছাড়িয়ে গেছে।

একহাজার মন্তব্য চেয়ে করা ফেসবুক স্ট্যাটাসে বারোশোর বেশি মন্তব্য পেয়েছেন জাহিদুল ইসলাম

নাম প্রকাশে অনাগ্রহী এই তরুণী বলছেন, কিছুদিন আগে তিনি ফেসবুক থেকে নোটিশ পান যে, তার আইডিতে কেউ প্রবেশ করার চেষ্টা করেছে। এরপর তার একজন বন্ধুর পরামর্শে তিনি ফেসবুকে এই স্ট্যাটাসটি লেখেন, যাতে কোন কারণে আইডি হারিয়ে গেলেও সেটি পুনরুদ্ধার করা যাবে বলে তার আশা।

কিন্তু এরকম মন্তব্যে আদৌ কি কোন কাজ হয়?

এ ধরণের মন্তব্যের মাধ্যমে ফেসবুকে সংযোগ বাড়তে পারে, তবে আইডি রক্ষা বা নিরাপত্তার সঙ্গে এর কোন সম্পর্কে নেই বলে বলছেন বিশেষজ্ঞরা।

বাংলাদেশে ফেসবুক নিয়ে কাজ করে ইউল্যাবের একটি টিম 'ফ্যাক্ট ওয়াচ'। এর উপদেষ্টা অধ্যাপক সুমন রহমান বলছেন, "আমরাও খেয়াল করেছি যে, কিছুদিন পরে পরে এরকম স্ট্যাটাস দেয়ার ঘটনা ঘটছে। যারা এসব লিখছেন, তারা খুব ফেসবুক সেলিব্রেটিও নন। কিন্তু আইডি হ্যাকিং থেকে বাঁচাতে বা আইডির ঝুঁকি বাঁচাতে যেসব লেখা হচ্ছে, তার সঙ্গে ফেসবুকের কাজের আসলে কোন সম্পর্ক নেই। কারণ ফেসবুক এভাবে কাজ করে না।"

তিনি ব্যাখ্যা করে বলেন, " কেউ যদি কারো ফেসবুক আইডি হ্যাক করতে চায়, তাহলে সেটার সঙ্গে এভাবে স্ট্যাটাসে মন্তব্য করা না করার সঙ্গে সম্পর্ক নেই। তিনি নানা কৌশলে সেই চেষ্টা করবে। আবার ফেসবুকে রিপোর্ট করার কারণে কারো আইডি যদি ফেসবুক ব্লক করে দিতে চায়, সেজন্য নিয়ম অনুযায়ী নোটিশ পাঠাবে, তারপর ব্যবস্থা নেবে। সেটা ফিরিয়ে আনারও নানা পদ্ধতি আছে। সুতরাং কমেন্ট করে সেক্ষেত্রে প্রভাবিত করার কোন ব্যাপার নেই। "

ফেসবুকে নিজের ছবির সঙ্গে মন্তব্য চেয়ে স্ট্যাটাস দিয়েছেন

রায়ান কামাল

সহজে জনপ্রিয়তা অর্জন বা নিজের প্রোফাইলে লাইক/কমেন্ট বাড়াতে অনেকে এ ধরণের কাজ করতে পারে বলে তিনি মন্তব্য করেন। কারণ যারা এ ধরণের স্ট্যাটাস দিয়েছেন, তারা কেউই ফেসবুকে খুব পরিচিত নন।

ফেসবুক কি বলছে?

এ বিষয়টি জানতে ফেসবুকের সঙ্গে যোগাযোগ করা হলেও, এই লেখা পর্যন্ত সংস্থাটি এ বিষয়ে কিছু জানায়নি।

ফেসবুক আইডি নিরাপদ রাখতে ফেসবুকের পাতায় বেশ কিছু পরামর্শ রয়েছে। তার মধ্যে টু-ফ্যাক্টর অথেনটিকেশন চালু করতে বলা হয়। এর মাধ্যমে ফেসবুকে প্রবেশ করতে হলে দুইটি মাধ্যম ব্যবহার করতে হবে। এর মধ্যে যেমন প্রচলিত পাসওয়ার্ড দিতে হবে, তেমনি মোবাইলের মেসেজে আসা কোড বা অথেনটিকেটর থেকে পাওয়া কোড প্রবেশ

করিয়ে নিশ্চিত করতে হবে। এর মাধ্যমে ফেসবুক আইডির নিরাপত্তা নিশ্চিত করা সম্ভব বলে জানিয়েছে ফেসবুক।

-২০ সেকেন্ড

Indian একজন hacker এক Tv show তে এসে মাত্র ২০ সেকেন্ডের মধ্যে দর্শকদের মধ্যে একজনের মোবাইল হ্যাক করেছিল।

এটা এমন কোন বড় কথা ছিল না। কেন? কারন ঐ hacker ঐ দর্শকের কাছ থেকে ২০ সেকেন্ডের জন্য তাদের মোবাইল নিয়েছিল আর তার একটি app install করে দিয়েছিল যাতে payload install করা ছিল, যা metasploit এর মাধ্যমে easily বানানো যায়।

সাবধান থাকার উপায়ঃ

১> তাই সবাই সাবধান থাকবেন যেন আপনারা কাওকে

মোবাইল দেয়ার আগে ভাব্বেন।

২> Most of the case app এর নাম MainActivity.apk তাই সবাই সাবধান থাকবেন।

৩> অন্য কোন app এর মধ্যে ও এই payload install করে থাকা থাকতে পারে। তাই কারো মোবাইল থেকেও কোন app নেয়ার আগে ভাব্বেন।

ISLAMIC CYBER SECURITY