Explore the world of hacking

SAIFUL ISLAM

ISLAMIC CYBER SECURITY

কী এই হ্যাকিং?

“কেউ একজন আমার ফেসবুক একাউন্ট হ্যাকিং করে নেয়ার চেষ্টা করেছে।”

“আমার একাউন্ট হ্যাক করে কেউ আমার সব টাকা নিয়ে নিয়েছে।”

এই ধরনের হ্যাকিং সংক্রান্ত অভিযোগ আমরা প্রায়ই শুনে থাকি। তথ্যপ্রযুক্তির যত উন্নতি হচ্ছে হ্যাক বা হ্যাকিং সংক্রান্ত বিষয়গুলো আমাদের কাছে আরো বেশি স্পষ্ট হয়ে ধরা দিতে শুরু করেছে। কিন্তু হ্যাকিং কী? কারা হ্যাকার? কীভাবে আসলে তারা হ্যাক করে? এই বিষয়গুলো সম্পর্কে আমরা অনেকেই জানি না। তাই আজকের লিখাতে চেষ্টা করব হ্যাকিং এবং হ্যাকিং সংক্রান্ত যাবতীয় তথ্য তুলে ধরতে। তাহলে দেরি না করে শুরু করা যাক...

হ্যাকিং কী?

কোন ব্যক্তির অনুমতি ছাড়া যদি অন্য কোন ব্যক্তির অ্যাকাউন্টে বা নেটওয়ার্কে বা কম্পিউটারে প্রবেশ করে সেখান থেকে গুরুত্বপূর্ণ তথ্য গ্রহণ করা, মুছে ফেলা বা এমন কোনভাবে পরিবর্তন করা যা ওই

ব্যক্তি বা প্রতিষ্ঠানের জন্য ক্ষতিকারক হয়, তাহলে তাকে হ্যাকিং বলা হয়। হ্যাকিং এর মাধ্যমে অনলাইন জগতে প্রায় সবকিছুই করা সম্ভব। যেমন: অনলাইন অ্যাকাউন্ট থেকে টাকা চুরি করা, কোন ব্যক্তির ব্যক্তিগত তথ্য সংগ্রহ, ভাইরাস বা কোন ক্ষতিকর প্রোগ্রামের মাধ্যমে আক্রমণ এই সব কিছুই হ্যাকিং এর মাধ্যমে করা সম্ভব।

হ্যাকিং অনেক ধরণের হতে পারে। মোবাইল ফোন, ল্যান্ড ফোন, গাড়ি ট্র্যাকিং, বিভিন্ন ইলেক্ট্রনিক্স ও ডিজিটাল যন্ত্র সবকিছুকেই হ্যাকিং এর মাধ্যমে নিয়ন্ত্রণ করা সম্ভব। হ্যাকাররা সাধারণত বিভিন্ন নেটওয়ার্ক, ওয়েবসাইট বা ইলেকট্রনিক্স ডিভাইসের ত্রুটি বের করে সেই ত্রুটির ওপর ভিত্তি করেই হ্যাক করে।

হ্যাকিং এর ইতিহাস

গত শতাব্দীর পঞ্চাশ ও ষাটের দশকে মূলতঃ ম্যাসাচুসেট ইনস্টিটিউড অফ টেকনোলজি (MIT) এর কিছু শিক্ষার্থী তাদের মেধার সর্বোত্তম ব্যবহারের জন্য গঠন করে বিশেষ একটি দল, যারা অন্যান্য শিক্ষার্থীদের তুলনায় চিন্তা ও দক্ষতায় অনেক এগিয়ে। যেকোনো প্রোগ্রামিং সমস্যা সমাধানের জন্য MIT এর এই দলই শেষ ভরসা। এই দলেরই প্রত্যেক সদস্যকে বলা হত হ্যাকার।

সত্তরের দশকে আবির্ভাব ঘটে ফ্রিকদের। এরাও এক ধরণের হ্যাকার কিন্তু তাদের কাজের ধরণ অনুযায়ী এই নামকরণ করা হয়। এরা টেলিফোন সিস্টেমের নেটওয়ার্ক হ্যাক করে বিনা খরচে কথা বলতো টেলিফোনে। ১৯৭০ সালে টেলিফোন সিস্টেমের নেটওয়ার্ক হ্যাক করার জন্য John Thomas Draper নামে একজন ফ্রিকারকে একাধিক-বার গ্রেফতার করা হয়। যিনি Captain Crunch নামেও পরিচিত।

এছাড়া ক্যালিফোর্নিয়ার Homebrew Computer Club এর দু'জন সদস্য "blue boxes" নামে একধরণের ডিভাইস তৈরি করে যা দিয়ে টেলিফোন সিস্টেমের নেটওয়ার্ক হ্যাক করে ফ্রী-তে কথা বলা যেত। এই দুজন পরে "Berkeley Blue" ও "Oak Toebark" নামে পরিচিতি লাভ করে। আর শুনে তাজ্জব হবেন যে এরা দুজন ছিলো "Berkeley Blue" (Steve Jobs) and "Oak Toebark" (Steve Wozniak) যারা পরবর্তীতে Apple Computer প্রতিষ্ঠা করেন।

হ্যাকার

যেই ব্যাক্তি হ্যাকিং করা বা হ্যাকিং এর সাথে জড়িত তাকেই হ্যাকার বলে। হ্যাকার নিরাপত্তা ব্যবস্থার দুর্বল দিক খুঁজে বের করার

কাজে বিশেষভাবে দক্ষ। একই সঙ্গে তিনি অন্য কম্পিউটার বা নেটওয়ার্ক ব্যবস্থায় অবৈধভাবে অনুপ্রবেশ করতে সক্ষম। কোনো কম্পিউটারের সিস্টেম বা নেটওয়ার্কে দুর্বলতা খুঁজে বের করে সেই সিস্টেম বা নেটওয়ার্কের নিরাপত্তা ভাঙ্গাই হ্যাকারদের প্রধান কাজ।

হ্যাকারদের চিহ্নিত করতে Hat বা টুপি এই শব্দটি ব্যবহার করা হয়। এর ভিত্তি করেই হ্যাকারদের ৩টি ভাগে ভাগ করা হয়েছে।

1. White Hat Hacker

2. Grey Hat Hacker

3. Black Hat hacker

হোয়াইট হ্যাট হ্যাকার (White Hat Hacker)

হোয়াইট হ্যাট হ্যাকার বলা হয় তাদের যারা, কোনো সিকিউরিটি সিস্টেমের দুর্বলতা বা ত্রুটি খুঁজে বের করে ঐ সিকিউরিটি সিস্টেমের মালিককে বা সংশ্লিষ্ট প্রতিষ্ঠানকে সেই ত্রুটিগুলো সম্পর্কে অবগত করেন যেন তারা ভবিষ্যতে যেকোন সাইবার হামলা থেকে মুক্ত থাকতে পারেন। এই সিকিউরিটি সিস্টেমটির মধ্যে রয়েছে কোনো কম্পিউটার বা কোনো কম্পিউটার নেটওয়ার্কের ওয়েবসাইট বা কোনো সফটওয়ার। হোয়াইট হ্যাট হ্যাকারদের প্রধান কাজ হল

সাইবার ওয়ার্ল্ডের নিরাপত্তা প্রদান করতে সাহয্য কর। এই ধরনের হ্যাকারদেরকে ইথিক্যাল হ্যাকারও বলা হয়ে থাকে।

গ্রে হ্যাট হ্যাকার (Grey Hat Hacker)

গ্রে হ্যাট হ্যাকাররা হচ্ছে দু'মুখো সাপের মত। কারণ এরা যখন একটি আপারেটিং বা সিকিউরিটি সিস্টেমের ত্রুটিগুলো বের করে তখন সে তার নিজের ইচ্ছা মত কাজ করবে। তার যদি ইচ্ছা হয় ঐ সিকিউরিটি সিস্টেমের মালিকে ত্রুটি জানাতে তাহলে সে জানাবে আবার তার যদি ইচ্ছে হয় ইনফরমেশনগুলো নষ্ট করবে বা চুরি করবে তাহলে সে তাও করতে পারে। আবার সে তার নিজের স্বার্থের জন্যও তথ্যগুলো ব্যবহার করতে পারে। বেশির ভাগ হ্যাকাররাই এ ক্যাটাগরির মধ্যে পড়ে।

ব্ল্যাক হ্যাট হ্যাকার (Black Hat Hacker)

এই ধরনের হ্যাকাররা সাইবার জগতে বিভিন্ন অপরাধের সাথে যুক্ত থাকেন। এরা বিভিন্ন সিস্টেম বা নেটওয়ার্কের দুর্বলতা খুঁজে নিজেদের আর্থিক অথবা ব্যক্তিগত স্বার্থসিদ্ধি করে থাকেন। কোনো সিস্টেমের সিকিউরিটির মধ্যে কোন ত্রুটি খুজে পেলে তারা সেটিকে নিজেদের স্বার্থে ব্যবহার করে। সিস্টেমের ডেটাবেজ নষ্ট করা, ভাইরাস ছড়িয়ে দেয়া, তথ্য চুরি করা সহ বিভিন্ন ধরণের অবৈধ

কাজ করে থাকেন।

এই তিন প্রকারের হ্যাকার বাদেও আরো কিছু হ্যাকার রয়েছে যারা বিভিন্ন ক্ষেত্রে পারদর্শী এবং বিভিন্ন ধরনের হ্যাকিং প্যাটার্ন অনুসরণ করেন। যেমন:

স্ক্রিপ্ট কিডি

এরা প্রোগ্রামিংয়ের বিষয়ে তেমন দক্ষ নয়। নিজেরা কোনো হ্যাকিং টুলস তৈরি করতে পারে না, অন্য হ্যাকারদের বানানো টুলস বা স্ক্রিপ্ট ব্যবহার করে হ্যাকিং করে থাকে। কোনো সিস্টেম হ্যাক করার পর এরা সঠিকভাবে নিজেদের লুকিয়ে রাখতে বা পরিচয় গোপন রাখতে পারে না।

ক্র্যাকার

অনেক সময় ক্ষতিকারক হ্যাকার ব্লাক হ্যাট হ্যাকারদের ক্র্যাকার বলা হয়। এদের শখ বা পেশাই হচ্ছে বিভিন্ন পাসওয়ার্ড ভাঙ্গা, Trojan Horse তৈরি করা এবং অন্যান্য ক্ষতিকারক সফটওয়ার

তৈরি করা। এসব ক্ষতিকারক সফটওয়ারকে তারা নিজেদের কাজে ব্যবহার করে অথবা বিক্রি করে।

এলিট হ্যাকার

এরা হ্যাকারেরা খুবই দক্ষ। কোনো সিস্টেমকে হ্যাক করার পাশাপাশি দক্ষতার সঙ্গে নিজেদের পরিচয় গোপন করতে পারে। এরা নতুন নতুন হ্যাকিং কৌশল আবিষ্কার করে থাকেন। এরা প্রোগ্রামিংয়ে বিশেষ দক্ষ হয়ে থাকেন। বিভিন্ন ধরনের হ্যাকিং টুলস এবং সফটওয়ার এরাই মূলত তৈরি করে থাকেন।

Referance-

http://www.techbengal.com/hacking/1917

https://www.techopedia.com/definition/26361/hacking

https://www.malwarebytes.com/hacker/

https://en.wikipedia.org/wiki/Hacking

https://economictimes.indiatimes.com/definition/hacking

ক্লিক করুন

পড়তে পারেন হ্যাকিং সম্পর্কিত জনপ্রিয় বই সমূহ রকমারি ডট কম এ

কম্পিউটারের বিবর্তন, হ্যাকারদের বিবর্তন: শুরুর কথা

হ্যাকিং নিয়ে আগ্রহ নেই এরকম মানুষ খুব বেশী খুঁজে পাওয়া যাবে না। কম্পিউটার সম্পর্কে যাদের ধারণা নেই, তারাও থাকবেন এই দলে। কম্পিউটার বিজ্ঞানের অন্যতম সৃজনশীল এই বিষয়টিকে সাধারণ মানুষের জন্য বিনোদন হিসেবে উপস্থাপন করার পিছনে হলিউডের অনেক অবদান। হ্যাকার বলতে তাই চোখে ভেসে ওঠে বড় সাইজের টি-শার্ট, মাথায় উস্কোখুস্কো বড় চুল আর চোখে চশমা পড়া কেউ একজন। কী-বোর্ডে দ্রুতগতিতে কিছু টাইপ করে কয়েক সেকেন্ডের মধ্যে সে ধ্বসিয়ে দিয়েছে শত্রুপক্ষের নিরাপত্তা ব্যবস্থা।

যদিও বাস্তবের হ্যাকিং এত সহজে হয় না, এত কম সময়ে হয় না, এত কম চেষ্টাতেও হয় না। আমাদের আলোচনার বিষয়ও রুপালী পর্দার হ্যাকিং নয়, সত্যিকারের হ্যাকিংয়ের ইতিহাস। আমি বলতে চেষ্টা করবো কীভাবে শুরু হয়েছিলো কম্পিউটারের নিরাপত্তা ভেঙে তার ভিতরে ঢুকে পড়ার এই সর্বনাশা খেলা। সময়ের সাথে সাথে কীভাবে পরিবর্তিত হয়েছে কম্পিউটার, কম্পিউটারের নিরাপত্তা ব্যবস্থা এবং হ্যাকিংয়ের কলাকৌশল।

হলিউডের হ্যাকিং আর বাস্তব জগতের হ্যাকিংয়ের একটি তুলনামুলক মজার চিত্র

হ্যাকিং এবং সিস্টেম ক্র্যাকিং শুরু হয়েছিল প্রথম ইলেক্ট্রনিক কম্পিউটার উদ্ভাবনের পর থেকেই। আমরা যাদের কম্পিউটার বলি সেগুলোই শুধু কম্পিউটার নয়। যেগুলো কম্পিউট বা গণনা করতে পারে, সেসব কিছুই আসলে কম্পিউটার। ক্যালকুলেটর, ফোন থেকে শুরু করে গুগলের বিশাল বিশাল সাইজের সার্ভার সবই আসলে কম্পিউটার। সুতরাং হ্যাকিংয়ের শুরু যে আধুনিক কম্পিউটার থেকে হয়নি, হয়েছে তার অনেক আগে থেকে সেটা বোঝাই যায়।

সবচেয়ে পুরাতন কার্যক্ষম ডিজিটাল কম্পিউটার। একে সব ডিজিটাল কম্পিউটারের দাদু ভাই বলা যায়। একটি সংখ্যাকে আরেকটি সংখ্যা দিয়ে ভাগ করার জন্য উনি ১০ সেকেন্ড সময় নিতেন।

হ্যাকিং বলতে যা বোঝায় তার শুরু হয়েছিলো উনবিংশ শতাব্দীর দিকেই। ১৮৭০ সালের দিকেই যুক্তরাষ্ট্রে অল্পবয়সী কিছু ছেলেমেয়ে সেই দেশে সদ্য স্থাপিত ফোন সিস্টেমকে নিজেদের নিয়ন্ত্রণে নেয়ার কৌশল বের করেছিলো। হ্যাকিংয়ের ইতিহাস ঘাটলে আমরা হয়তো এর পিছনে আর যেতে পারবো না।

তখন বেল টেলিফোন কোম্পানীর সুইচবোর্ড অপারেটররা টেলিফোনের কলগুলো নিয়ন্ত্রণ করতেন। অনেক সময় তারা ইচ্ছা করেই কলগুলো কেটে দিতেন বা কলগুলোর গন্তব্য পরিবর্তন করে দিতেন। বলা যায় এখান থেকেই শুরু হয়েছিলো হ্যাকারদের যাত্রা।

এখন যার কথা বলবো তাকেও ধরা হয় একেবারে প্রথম দিককার হ্যাকারদের একজন। তার হ্যাকিংয়ের ঘটনাটি যথেষ্টই চমকপ্রদ। এটিও এক শতকের বেশী আগের ঘটনা।

১৯০৩ সালের জুন মাসের কোনো এক বিকেলে বিখ্যাত পদার্থবিদ জন ফ্লেমিং লন্ডনের রয়্যাল ইনস্টিটিউশনে একটি যুগান্তকারী আবিষ্কার জনসম্মুখে প্রকাশ করার প্রস্তুতি নিচ্ছিলেন। প্রকৃতপক্ষে এই আবিষ্কারটি ছিল তার শিক্ষক আরেক বিখ্যাত বিজ্ঞানী মার্কনীর, যাকে আমরা রেডিওর উদ্ভাবক হিসেবে চিনি।

ওইসময় তিনি বেশি দূরত্বে কোনো রকম তারের সাহায্য ছাড়া কীভাবে মোর্স কোড বার্তা পাঠানো যায় তা নিয়ে কাজ করছিলেন। তিনি ইংল্যান্ডের কর্নওয়ালের ক্লিফটপ স্টেশন থেকে প্রায় ৩০০ মাইল দূরে লন্ডনে ফ্লেমিংয়ের কাছে সংকেত পাঠানোর প্রস্তুতি নিচ্ছিলেন।

ঠিক এই সময়ে লন্ডন থিয়েটারে স্থাপিত প্রাপক যন্ত্রটি কিছু অদ্ভুত বার্তা গ্রহণ করতে লাগলো, যেগুলো আসলে মার্কনী পাঠাননি। প্রথমে বার্তা হিসেবে শুধু একই শব্দ বারবার শোনা যাচ্ছিলো। পরে তা হয় কবিতা, যা আসলে মার্কনীকে সবার সামনে ব্যঙ্গ করার জন্য পাঠানো হয়েছিলো। তখন পরিস্কারভাবেই বোঝা গিয়েছিলো যে তাদের সব আয়োজন মোটামুটি পন্ড হতে চলেছে, কারণ কেউ একজন তাদের সিস্টেম হ্যাক করে সেখানে বার্তা পাঠাচ্ছে।

কিন্তু কে সে? আর কেন এবং কীভাবেই বা এই হ্যকিংয়ের ঘটনা ঘটলো? আবারও মনে করিয়ে দেই এটি এক শতকেরও বেশী আগের ঘটনা। তখন ইন্টারনেটের ধারণাটুকুও তেমন ছিলো না। তাহলে এই মার্কনীর প্রাপক যন্ত্রে এই অনাকাঙ্খিত বার্তাগুলো কোথা থেকে এলো?

কে ছিলেন এই হ্যাকার তা জানার জন্য অবশ্য বেশী সময় অপেক্ষা করতে হয়নি। চার দিন পর The Times of London এর কাছে একটি চিঠি আসে এই হ্যাকিংয়ের ঘটনা স্বীকার করে। প্রেরক ছিলেন নেভিল ম্যাস্কেলাইন নামের ৩৯ বছর বয়সী একজন ব্রিটিশ ম্যাজিশিয়ান, আমাদের কাঙ্খিত হ্যাকার। তবে সাধারণ মানুষের ভালোর জন্যই মার্কনীর যন্ত্রের নিরাপত্তার খুতটুকু প্রকাশ করে দেওয়া প্রয়োজন ছিলো বলে তিনি দাবি করেন।

কিন্তু ঘটনা এখানেই শেষ নয়। ম্যাস্কেলাইন আসলে মোর্স কোড ব্যবহার করতেন ম্যাজিক দেখানোর কাজে। ১৯০০ সালের দিকেই তিনি ভূমি থেকে ১০ মাইল উপরে একটি বেলুনে তারবিহীন বার্তা পাঠানোর প্রক্রিয়া আবিষ্কার করেছিলেন। কিন্তু পরবর্তীতে মার্কনী এই আবিষ্কারের পেটেন্ট করে ফেলায় ম্যাস্কেলাইন হতাশাগ্রস্ত হয়ে পড়েন। তাই মার্কনীর বিরুদ্ধে প্রতিশোধ নেওয়ার এরকম একটি মোক্ষম সুযোগ তিনি হাতছাড়া করেননি।

এই আয়োজনের কয়েক মাস আগে মার্কনী লন্ডনের একটি পত্রিকায় দেয়া সাক্ষাতকারে দাবি করেছিলেন তার সিস্টেম একটি নির্দিষ্ট তরঙ্গদৈর্ঘ্যে গোপন বার্তা প্রেরণ করতে পারবে কোনো রকম নিরাপত্তা ঝুঁকি ছাড়াই। কিন্তু বার্তাটি নির্দিষ্ট গন্তব্যে পৌঁছানোর আগেই ম্যাস্কেলাইন ২৫ ফুট লম্বা একটি এন্টেনা দিয়ে ধরে ফেলেন এবং তার বদলে ভিন্ন একটি বার্তা পাঠাতে সক্ষম হন যার কথা আগেই উল্লেখ করা হয়েছে ।

জনসমক্ষে এই ঘটনা ঘটার কারণে মার্কনীর আবিষ্কারের উপর অনেকেই আস্থা হারিয়ে ফেলেছিলেন। এমনকি তাদের সাথে চুক্তিবদ্ধ কোম্পানীগুলোও অর্থ সাহায্য বন্ধ করে দেয়। বলা যায় এই হ্যাকিংয়ের ঘটনা মার্কনী এবং ফ্লেমিংকে যথেষ্টই বিপদে ফেলে দিয়েছিলো।

এরপরের ঘটনাটি ১৯৩৭ সালের দিকে দ্বিতীয় বিশ্বযুদ্ধের সময়ে। সেই সময়ে গোপন বার্তা পাঠানো হতো সাংকেতিকভাবে। আর এজন্য ব্যবহার করা হতো এনিগমা মেশিন যার কোড কোনো একটি বার্তাকে এনক্রিপ্ট করতো।

কিন্তু এই মেশিনটির কি স্পেস (Key space) অনেক কম থাকায় তিনজন পোলিশ ক্রিপটো-অ্যানালিস্ট মিলে ব্রুট ফোর্স পদ্ধতি ব্যবহার করেই কোড ভেঙে ফেলতে সক্ষম হয়েছিলেন। ব্রুট ফোর্স মানে হলো সবগুলো কম্বিনেশন চেষ্টা করে দেখা। এই পদ্ধতি সঠিক ফলাফল অবশ্যই দিবে, কিন্তু সার্চ স্পেস বড় হলে ব্রুট ফোর্স সম্ভব নয়।

পরবর্তীতে অ্যালান টুরিং আরও কার্যকরী একটি যন্ত্র তৈরী করেন এই কোড ভাঙার জন্য যার নাম Bombe। তার এই যন্ত্রটি দ্বিতীয় বিশ্বযুদ্ধের সময়ে জার্মানদের এনিগমা মেশিন ব্যবহার করে পাঠানো বার্তা উদ্ধারের কাজে ব্যবহার করা হতো। এই ঘটনা নিয়ে হলিউডের একটি বিখ্যাত চলচ্চিত্র আছে যার নাম The Imitation Game। অভিনেতা Benedict Cumberbatch যেখানে অ্যালান টুরিংয়ের চরিত্রে অভিনয় করেন।

অ্যালান টুরিংকে বলা হয় তত্ত্বীয় কম্পিউটার বিজ্ঞান এবং কৃত্রিম বুদ্ধিমত্তার জনক। তিনিই সর্বপ্রথম টুরিং মেশিন নামে একটি আধুনিক কম্পিউটারের ধারণা দেন। তার তৈরি Bombe মেশিনের কারণে তিনি ইতিহাসের সবচেয়ে গুরুত্বপূর্ণ হ্যাকারদের একজন।

অ্যালান টুরিং

সেই সময়ে ডাটা সংরক্ষণ এবং প্রসেস করার জন্য ব্যবহার করা হতো Punch card। এই কার্ডের কোনো একটি নির্দিষ্ট স্থানে হয় একটি ছিদ্র থাকতো, নাহয় থাকতো না। যার মানে হলো শুন্য অথবা এক। বিংশ শতাব্দীর অধিকাংশ সময় জুড়ে ডিজিটাল কম্পিউটারগুলো ডাটা ইনপুট নিতো এবং আউটপুট দিতো এই ধরনের কার্ডের মাধমে।

হিটলারের নাৎসি বাহিনী ইহুদীদের অবস্থান জানার জন্য এক ধরনের Punch card ব্যবহার করতো। আর তা হ্যাক করতে সক্ষম হন ফ্রান্সের একজন কম্পিউটার বিশেষজ্ঞ।

এভাবেই ধীরে ধীরে শুরু হয়েছিলো হ্যাকিং সংস্কৃতির। এর সাথে জড়িয়ে আছে বেশ কিছু বিখ্যাত মানুষের নাম। আমরা শুরুর দিকের এইসব হ্যাকিংয়ের সাথে হয়তো এত পরিচিত নই। এর কারণ

হয়তো কম্পিউটার সম্পর্কে আমাদের চিরাচরিত ধারণা। কিন্তু আমরা ধীরে ধীরে সামনে যত আগাবো তত পরিচিত মনে হবে সবকিছু।

কম্পিউটারের ধারণা বদলে যাওয়ার সাথে সাথে বদলে গেছেন হ্যাকাররাও। অনেক ক্ষেত্রে তারা এগিয়ে ছিলেন সমসাময়িক অনেকদের থেকে, এখনও এগিয়ে আছেন। প্রচন্ড প্রতিভাবান এইসব হ্যাকারদের বাস্তব জগতও যে রুপালী পর্দার হ্যাকারদের মতোই চমকপ্রদ তাও আমরা বুঝতে পারবো সামনের পর্বগুলোতেই।

হ্যাকারদের বিবর্তন:
এমআইটির হ্যাকিং ইতিহাস

১৯৫০ থেকে ১৯৬০ সালের সময়ের এমআইটির একদল ছাত্র-ছাত্রী পুরো পৃথিবীর প্রযুক্তি জগতকেই চিরতরে পাল্টে দিয়েছিল। হ্যাকিং নিয়ে আজকের পৃথিবীতে যে উন্মাদনা, তার শুরুটা হয়েছিলো তাদের হাত ধরেই। নিছক বিনোদন কিংবা বিখ্যাত হওয়ার জন্য তারা যে কাজগুলো করেছিল তাই পরবর্তীতে ইতিহাসে স্থান পেয়েছে। তাদেরকে বলা হয় আধুনিক হ্যাকিংয়ের প্রতিষ্ঠাতা, আধুনিক হ্যাকারদের পূর্বপুরুষ।

‘কম্পিউটারের বিবর্তন, হ্যাকারদের বিবর্তন’ শিরোনামে এটি রোর বাংলায় দ্বিতীয় লেখা। প্রথম লেখাটিতে ১৮৭০ থেকে ১৯৬০ সালের আগের সময় পর্যন্ত কম্পিউটার এবং হ্যাকিংয়ে দুটোর ইতিহাসটুকু সমান্তরালে সংক্ষিপ্তভাবে বলার চেষ্টা করা হয়েছে। পুরো ব্যাপারটি চট করে বুঝে ফেলা হয়তো খুব সহজ নয়। কারণ ওই সময়ের কম্পিউটার এবং হ্যাকিংয়ের ধারনা এখনকার মতো ছিলো না।

ম্যাসাচুসেটস ইনস্টিটিউট অফ টেকনোলজি (Massachusetts

Institute of Technology) বা সংক্ষেপে এমআইটি (MIT) বর্তমানে পৃথিবীর সবচেয়ে বিখ্যাত বিশ্ববিদ্যালয়গুলোর একটি। বলা যায় ১৯৬০ সালে এই বিশ্ববিদ্যালয়েই সর্বপ্রথম হ্যাকার শব্দটির উৎপত্তি হয়। আর সেই সময়ের এমআইটির আর্টিফিশিয়াল ইন্টেলিজেন্স ল্যাবটি (MIT Artificial Intelligence Lab অথবা MIT AI Lab) ছিল এই সমস্ত ঘটনার কেন্দ্রবিন্দু।

এমআইটির বিখ্যাত আর্টিফিশিয়াল ইন্টেলিজেন্স ল্যাব; Image Source: cap.csail.mit.edu

তখন এই ল্যাবে খুবই দক্ষ একদল প্রোগ্রামার ছিল। তারা FORTRAN প্রোগ্রামিং ল্যাংগুয়েজ ব্যবহার করে নানা রকম উচ্চমানের প্রোগ্রাম তৈরি করত। প্রসঙ্গক্রমে বলে রাখি- FORTRAN হলো লো লেভেল থেকে হাই লেভেলের মাঝামাঝি একটি প্রোগ্রামিং ল্যাংগুয়েজ যা বিভিন্ন বৈজ্ঞানিক গণনাকার্যে ব্যবহৃত হতো। FORTRAN-কে আসলে হাই লেভেলের ল্যাংগুয়েজ হিসেবেই ধরা হয়। হাই লেভেলের ল্যাংগুয়েজগুলোর সাহায্যে খুব বড় একটি কাজ অনেক অল্প পরিশ্রমে করে ফেলা যায়। যেমন- Python, Visual Basic, Delphi, Perl, PHP, ECMAScript, Ruby, Lisp এগুলো হলো হাই লেভেল প্রোগ্রামিং ভাষা। আর লো লেভেল ল্যাংগুয়েজগুলোতে খুব অল্প কিছু কাজ করতে অনেক পরিশ্রমের দরকার হয়, অনেক বড়

বড় সাইজের কোড লিখতে হয়। সেই সময়টাতে তারা আরও অনেকগুলো প্রোগ্রামিং ভাষাতে পারদর্শী ছিল, যেগুলো ছিল FORTRAN এর চেয়েও পুরোনো এবং আরও লো লেভেলের দিকের।

এতকিছু বলার কারণ হলো যাতে এমআইটির সেসব হ্যাকারদের প্রোগ্রামিং জ্ঞান নিয়ে কারও কোনো প্রকার সন্দেহ না থাকে। হ্যাকিংয়ের কথা আসলে সেখানে প্রোগ্রামিংও থাকবে। কারণ কোনো কিছু হ্যাক করতে গেলে সেখানে কোড তো লিখতেই হবে। কিন্তু এই ব্যাপারটা তখনকার সময়ে সত্যি ছিল না। তখনকার হ্যাকাররা সফটওয়্যারের চেয়ে হার্ডওয়্যার নিয়েই বেশী ব্যস্ত ছিল।

সেই সময়ে কিন্তু কম্পিউটারের অলিগলি সম্পর্কে মানুষের ধারণা ছিল খুবই কম। এমনকি সেটা এমআইটির মতো বিখ্যাত একটি বিশ্ববিদ্যালয়ের সাধারণ ছাত্র-ছাত্রীদের ক্ষেত্রেও প্রযোজ্য। বাকি সবাই যখন বিকালে মাঠে খেলাধুলা করতে ব্যস্ত ছিল, তখন এই সকল তরুণ-তরুণীরা বিশ্ববিদ্যালয়ের ল্যাবগুলোতে কম্পিউটার নিয়ে পড়ে থাকতো। এই কারণে তাদেরকে Nerds অথবা Geeks বলে ঠাট্টা করতো সবাই। কিন্তু ল্যাবের ডিরেক্টর মারভিন মিনস্কি ঠিকই বুঝতে পারতেন তাদের প্রতিভা। তাই ল্যাবের সকল প্রকার যন্ত্রাংশ ব্যবহারে তাদের অনুমতি দেন তিনি। যদিও এদের মধ্যে

অনেক হ্যাকারই আসলে ছিল বিশ্ববিদ্যালয় থেকে ঝরে পড়া শিক্ষার্থী, হ্যাকিংয়ে অনেক বেশী সময় দেওয়ার কারণে গতানুগতিক ধারার পড়াশুনা তাদের দিয়ে সম্ভব হতো না। এই কারণে বিশ্ববিদ্যালয়ের গন্ডি পেরোনোও তাদের দিয়ে সম্ভব হয়নি। এতক্ষণে হয়ত আমাদের এরকম ধারণা হয়েছে যে, আমাদের আজকের হ্যাকাররা খুবই ভদ্রগোছের, তারা শুধু প্রোগ্রামিং ছাড়া আর কিছু করতো না। আমাদের ধারণা যে কতটা ভুল সেটা আরেকটু পরেই বোঝা যাবে।

টেলিফোন তখন যোগাযোগের জন্য খুবই গুরুত্বপূর্ণ মাধ্যম ছিল। আর টেলিফোন কোম্পানী ছিল তাদের অন্যতম টার্গেট। তারা অনেক সময় ব্যয় করে টেলিফোন নেটওয়ার্ক ব্যবহার করে বিভিন্ন জায়গায় কল করতে লাগল শুধুমাত্র কিছু প্যাটার্ন খুজে পাওয়ার জন্য যা দিয়ে বোঝা যায় কীভাবে টেলিফোন সিস্টেম কাজ করে। বিভিন্ন জায়গার কলের টোন প্যাটার্ন বিশ্লেষন করে তারা বুঝতে পারলো কীভাবে কলগুলো রাউটিং (route) করা হয়। টেলিফোন কোম্পানীগুলোর গোপন জার্নালগুলো থেকে তারা টেলিফোন অপারেটর এবং অন্যান্য গুরুত্বপূর্ণ ব্যাক্তিদের সম্পর্কে তথ্য সংগ্রহ করতো। তাদের ডাস্টবিন ঘেটে দেখতো কোনো ডকুমেন্ট পাওয়া যায় কিনা যা তাদের কাজে লাগতে পারে। তারপর রাতের বেলা গোপনে টেলিফোন কোম্পানীর বিল্ডিংয়ে ঢুকে তাদের টেলিফোন লাইনগুলো সেখানে লাগিয়ে দিয়ে আসতো।

তারা বেশকিছু ডিভাইস তৈরি করেছিল যেগুলোকে বলা হয় Blue boxes, Black boxes এবং Red boxes। এই ডিভাইসগুলো তাদের সৃষ্টিশীলতার অনন্য নিদর্শন। এগুলো ব্যবহার করে ফ্রি ফোন কল করা যেত। এছাড়া যেগুলো অনেক গুরুত্বপূর্ণ কল, সেগুলোকে থামিয়ে রাখা এবং একজনের কল অন্য একজনকে দিয়ে দেয়া এধরণের অনেক কাজ করা যেত ঐ ডিভাইসগুলো দিয়ে। এই পুরো প্রক্রিয়াটিকে বলা হয় ফোন ফ্রিকিং (Phone Phreaking)। পুরো ব্যাপারটিই আসলে যথেষ্ট বে-আইনি, অনেকটা চুরি-চামারিও বলা যায়। অবশ্য হ্যাকিং তো চুরি-ডাকাতির মতো ব্যাপারই অনেকটা। বিশ্ববিদ্যালয় কতৃপক্ষও এইসব হ্যাকারদের কর্মকান্ডকে কখনো সমর্থন করতো না। কিন্তু পুরো ব্যাপারটির সাথে একধরণের সৃষ্টিশীলতার ব্যাপার আছে। তাই তারা এগুলো থামানোর চেষ্টাও করে নি। এভাবেই এমআইটিতে গড়ে ওঠে একধরণের হ্যাকিং কালচার যা পরবর্তীতে স্ট্যানফোর্ড, ইয়েল, হার্ভার্ডের মতো বিশ্ববিদ্যালয়গুলোতেও ছড়িয়ে পড়ে।

যাদুঘরে সংরক্ষিত একটি Blue Box, যা দিয়ে ১৯৬০-৭০ এর দিকে ফ্রি ফোন কল করা হত; Image Source: Wikipedia

হার্ভার্ড বিশ্ববিদ্যালয়ের শিক্ষার্থীদের সাথে এই বিশ্ববিদ্যালয়ের

শিক্ষার্থীদের এক প্রকার প্রতিযোগিতা লেগেই থাকতো। ঠিক এই কারণেই বার্ষিক হার্ভার্ড-ইয়েল ফুটবল খেলাতে হ্যাকাররা এসে হানা দিত। তারা হ্যাকিংয়ের ক্ষেত্রে যেসব নৈপুণ্য প্রদর্শন করতো সেগুলোকে প্রাতিষ্ঠানিক জগতের সবচেয়ে বিখ্যাত হ্যাকিংয়ের ঘটনাগুলোর মধ্যে অন্যতম বলা যায়।

এটি শুরু হয়েছিল ১৯৪৮ সালের হার্ভার্ড-ইয়েল ফুটবল চ্যাম্পিয়নশীপ থেকেই। খেলা শুরুর আগের দিন রাতে বেশকিছু হ্যাকার হার্ভার্ড স্টেডিয়ামের মাঠের ভিতর ঢুকে প্রাইমার কর্ড (Primer cord) মাটির ভিতর পুঁতে রেখেছিল। তারা আসলে মাঠে “MIT” শব্দটি বড় করে লিখতে চেয়েছিল ওই কর্ডগুলো বিস্ফোরিত করে। যদিও তাদের এই পরিকল্পনা শেষ পর্যন্ত সফল হয়নি। খেলা শুরুর দিন তারা খুব ভারী ব্যাটারী লাইনড পোশাক পরে মাঠে এসেছিল, যদিও ঐ দিনটি ছিল বেশ রৌদ্রজ্জ্বল। তারা তাদের সেই পোশাকের ভিতর অনেকগুলো ব্যাটারী এনেছিল ওই কর্ডগুলোকে বিস্ফোরিত করার জন্য। ব্যাপারটি বেশ সন্দেহজনক মনে হওয়ায় মাঠের কর্মীরা তাদেরকে ধরে ফেলে। যদিও এমআইটির ডিন ঐসব হ্যাকারদের পক্ষ অবলম্বন করে বলেছিলেন যে, এমআইটির অনেকেই এধরনের যন্ত্রপাতি সাথে নিয়ে ঘোরাফেরা করে। এগুলো আসলে আমাদের মতো যারা প্রযুক্তি সংশ্লিষ্ট ব্যক্তি, তাদের সব সময় কাজে লাগে। কিন্তু তার এই যুক্তি যে শেষপর্যন্ত খুব একটা কাজে আসেনি তা বোঝাই যায়।

এর অনেক পরে ১৯৮২ সালের হার্ভার্ড-ইয়েল ফুটবল খেলাতে এমআইটির হ্যাকাররা অবশ্য সফল হয়। খেলা শুরুর পর হঠাৎ দেখা গেল মাঠের ভিতর একটি বেলুন এবং সেটি ধীরে ধীরে প্রসারিত হচ্ছে। সেই বেলুনে বড় বড় করে লেখা ছিল "MIT"। একসময় বড় হতে হতে বিকট শব্দে বেলুনটা ফেটে গেল। আর গ্যালারী থেকে এমআইটির শিক্ষার্থীদের উল্লাস। গ্যালারীতে হার্ভাডের শিক্ষার্থীদের অংশে অবশ্য তখন পিনপতন নীরবতা, আয়োজকরাও হতভম্ব।

পরেরদিন Boston Herald পত্রিকা এরকম একটি শিরোনাম করে "MIT 1 — Harvard-Yale 0: Tech Pranksters Steal the Show"। এই পুরো ব্যাপারটির জন্য তারা একসপ্তাহ ধরে গোপনে মাঠে এসে বিভিন্ন যন্ত্রপাতি বসানোর কাজ করছিল। তারা ভ্যাকুয়াম ক্লিনার মোটর এবং হাইড্রলিক প্রেসের মতো যন্ত্রপাতি ব্যবহার করেছিল।

এরপর ১৯৯০ সালেও এই একই চ্যাম্পিয়নশীপে ইয়েল বিশ্ববিদ্যালয় একটি ফ্রি কিক নিতে যাবে এমন সময় এমআইটির হ্যাকাররা কীভাবে যেন "MIT" লেখাযুক্ত একটি ব্যানার মাঠে নিয়ে আসেন! ১৯৯৬ সালের খেলার হার্ভার্ডের স্কোরবোর্ড হ্যাক করা হয়।

সেখানে লেখা ছিল VE-RI-TAS। এর পরিবর্তে লিখে দেওয়া হয় HU-GE-EGO মানে huge ego। অন্য একটি বিশ্ববিদ্যালয়ের খেলাতে এভাবে বিঘ্ন ঘঠানোটা তাদের জন্য যে বেশ উপভোগ্য ছিল তা বোঝাই যাচ্ছে।

এমনও ঘটনা শোনা যায় যে একবার একদল শিক্ষার্থী পাখিদের খাবার হার্ভার্ডের মাঠে ছড়িয়ে রেখে যায়। হার্ভাডের ওই মাঠটাতে সেইদিন খুব গুরুত্বপূর্ণ একটা খেলা ছিল। কিন্তু ঝাঁকে ঝাঁকে পাখি এসে বেচারাদের খেলা পন্ড করে দেয়। ব্যাপারটা গুজবও হতে পারে অবশ্য। এমআইটির হ্যাকারদের নিয়ে এতই গুজব ছিল যে, কোনটা তারা করেছে আর কোনটা যে করেনি সেটা বোঝাটাই কষ্টকর হয়ে যেত। একবার তারা কোনো একটি বিখ্যাত পত্রিকার রিপোর্টারকে বলল যে, তারা একটি বিশেষ প্রযুক্তি ব্যবহার করে রুমের ভিতর কৃত্রিম তুষারপাত সৃষ্টি করেছে। বেচারা রিপোর্টার তাদেরকে বিশ্বাস করে পত্রিকায় খবর ছেপে দিল। পরে দেখা গেল পুরো ব্যাপারটিই আসলে নির্জলা মিথ্যা।

এমআইটির হ্যাকারদের পাগলামি এখানেই শেষ না। কিন্তু সবকিছু বলার মতো একটি লেখা যথেষ্ট নয়।

দুনিয়া কাঁপানো ১০ হ্যাকার গ্রুপ

হ্যাক!!! শব্দটা শুনলে আমাদের বেশিরভাগের মাথাতেই হয়তো নিজ নিজ ফেসবুক আইডি চেক করার চিন্তাটা আগে আসে। চেক করে দেখতে ইচ্ছা হয় যে, নিজের একাউন্টখানা ঠিক আছে কিনা। কারণ আর কিছুই না, ফেসবুক একাউন্ট হ্যাকের ঘটনা আমাদের চারপাশে এত ঘটে থাকে যে, আমরা এর বাইরে চিন্তাই করতে পারিনা। অথচ বাইরের জগতে হ্যাকিং কিন্তু শুধু ফেসবুকেই সীমাবদ্ধ নয়। বরং ফেসবুক হ্যাকারদের হ্যাকারের কাতারে ফেলতেই অনেকে নারাজ। এর কারণ জানতে চাইলে আমাদের এখন আলোচনা করা লাগবে বিশ্বের বড় বড় কিছু হ্যাকার গ্রুপ এবং তাদের কর্মকান্ড সম্পর্কে। চলুন তবে বিশ্বের শীর্ষ(স্বীকৃত) দশ হ্যাকার গ্রুপ সম্পর্কে জেনে নেওয়া যাক।

১. Tailored Access Operations, NSA

Snowden মুভিটা দেখেছেন? মুভির পুরো ঘটনাই কিন্তু বাস্তব ঘটনার হুবুহু অনুরূপ। Snowden যদি সব ফাঁস করে না দিত, আমরা সম্ভবত কোনোদিন Tailored Access Operations(TAO) সম্পর্কে জানতেই পারতাম না।এটি ইউএস সরকারের একটি সংস্থা। TAO এর ক্ষমতা অকল্পনীয়। স্নোডেন

এর দেওয়া তথ্যমতে এখন আমরা জানি যে, এই সংস্থাটির প্রায় ৬০০ এর মত কর্মচারী আছে যারা মেরীল্যান্ডের মেইন NSA বিল্ডিং এ কাজ করে। হাওয়াই,জর্জিয়া,টেক্সাস এবং ডেনভার এও এদের শাখা আছে। তাদের কাছে QuantumSquirrel নামক এমন একটি টেকনোলজি আছে, যার মাধ্যমে তারা ইন্টারনেটে যে কোনো স্থান থেকে, যে কোনো ব্যক্তির পরিচয় চুরি করতে পারে এবং সে অনুযায়ী কার্যসিদ্ধি করতে পারে।শুধু তাই নয়। তারা এমনকি বিশ্বের বিভিন্ন টেক-কোম্পানির উপর চাপ প্রয়োগের মাধ্যমে তাদের নিজেদের তৈরি প্রোডাক্টের মাঝেই নিরাপত্তার ফাঁকফোকর রাখে, যেন তাদের ভবিষ্যতে ওইসব যন্ত্রের সিকিউরিটি এক্সেস পেতে সুবিধা হয়।তারা চাইলে বিশ্বের যেকোনো মোবাইল/কম্পিউটার ডিভাইসে ইন্টারনেটের মাধ্যমে এক্সেস নিতে পারে এবং সেই ডিভাইসের মাইক্রোফোন/ক্যামেরা অন করে সেই ডিভাইসের আশেপাশের সকল অডিও এবং ভিডিও ফুটেজ সংগ্রহ করতে পারে।

২. Elderwood Group and 20 other Chinese APTs

Elderwood Group, Axiom, Unit 61398,

Comment Crew, Putter Panda, Hidden Lynx ইত্যাদি বিভিন্ন হ্যাকার গ্রুপের সমন্বয়ে চাইনিজ হ্যাকার সার্কেলটি গঠিত। এদের ফান্ডিং করে স্বয়ং চাইনিজ সরকার। জানামতে এখন পর্যন্ত এদের সবচেয়ে বড় হামলার ঘটনাটি ঘটে ২০১০ সালে। যেটিকে 'অপারেশন অরোরা' নামে উল্লেখ করা হয়েছে।যে অপারেশনের পর গুগল ঘোষনা করে যে,তারা হ্যাক হয়ে গিয়েছিল। এছাড়া এই হ্যাকার গ্রুপটি বিভিন্ন ডিফেন্স ফার্ম, ওয়পন ইন্ডাস্ট্রী, বিজন্যাস ফার্ম ইত্যাদির ওয়েবসাইটও হ্যাক করে থাকে।

৩. *APT28*

এই হ্যাকার গ্রুপটি খুবই এডভান্সড। যতটুকু তথ্য পাওয়া গেছে, তা থেকে জানা যায় যে, এরা রাশিয়ান। এদের ফান্ডিং ও করে খোদ রাশান সরকার। রাশান সরকার তাদেরকে টার্গেট বাছাই করে দেয় এবং তারা সে মোতাবেক কাজ করে।এই গ্রুপটি খুবই কমন হ্যাকিং মেথডস ব্যবহার করে। তারা এপর্যন্ত ন্যাটো, পোলিশ গর্ভনমেন্ট ওয়েবসাইটস, জর্জিয়া মিনিস্ট্রিস এবং OSCE হ্যাক করেছে।

৪. *Dragonfly*

এই হ্যাকার গ্রুপটি আরেকটি স্টেট স্পন্সর্ড হ্যাকার গ্রুপ। এটির

পেছনেও সম্ভবত আছে রাশান সরকার। এরা সাধারণত ইলেক্ট্রিক গ্রীড, এনার্জি ইন্ডাস্ট্রী এবং ইউরোপের ও আমেরিকার বিভিন্ন কন্ট্রোল সিস্টেম কে টার্গেট করে।তারা তাদের spearphishing এবং watering hole এটাকের জন্য সর্বাধিক পরিচিত।তারা বিভিন্ন ইন্ডাস্ট্রী'র ওয়েবসাইটে সিকিউরিটি ব্রীচ তৈরি করে এবং সময় এলে তা দখল করে নেয়।

৫. *Tarh Andishan/Ajax*

নানান প্রতিকুলতার মুখে পড়ে ইরান সরকার সিদ্ধান্ত নিল যে, অনেক হয়েছে! এবার দরকার শক্তিশালী সাইবার ফোর্স। এরই প্রেক্ষিতে তারা দুইটি দল গঠন করে। প্রথমটির নাম 'Tarh Andishan'। এটির ফান্ডিং পুরোটাই সরকার করে থাকে। আরেকটি হলো 'Ajax'j। এটি নানান ইরানিয়ান হ্যাকারদের চুক্তিবদ্ধ করে গঠিত হয়। কিন্তু এর সাথে সরকার সরাসরি সংযুক্ত থাকেনা। Ajax এর সবচেয়ে উল্লেখযোগ্য মিশন হলো 'Operation Saffron Rose'। এই মিশনে তারা ইউএসএ'র ডিফেন্স ইন্ডাস্ট্রী'র বিভিন্ন ওয়েবসাইট দখল করে এবং বিভিন্ন ক্লাসিফাইড তথ্য সরানোর উদ্যোগ নেয়। সেদিক দিয়ে আবার Tarh Andishan এর কাহিনী সম্পূর্ণ অন্যরকম।এদের কাজ মূলত শত্রু দেশের বিভিন্ন এয়ারপোর্ট,গ্যাস-স্ট্যাশল ইত্যাদির সিকিউরিটি সিস্টেমের ক্ষতিসাধন করা।

৬. Anonymous

এই হ্যাকার গ্রুপটি সম্পর্কে আমরা সবাই হয়তো কমবেশি শুনেছি। ধারণা করা হয় যে, সম্ভবত এরাই হচ্ছে দুনিয়ার সবচেয়ে বড় সংঘবদ্ধ হ্যাকার গ্রুপ। পুরো পৃথিবী জুড়ে এদের সদস্য ছড়িয়ে ছিটিয়ে আছে। ২০০৩ সালে এদের উদ্ভব হয়। এদের সংঘবদ্ধতা এমন পর্যায়ে আছে যে, অপারেশন চলাকালে কেউ যদি ধরাও পড়ে, তবুও তাদের অপারেশন চলতে থাকে।বিন্দুমাত্র ক্ষতিগ্রস্থ হয়না। এখন পর্যন্ত এই গ্রুপটি অত্যন্ত সফলতার সাথে অনলাইন এবং অফলাইনে বিভিন্ন অপারেশন চালিয়েছে। তাদের বেশিরভাগ অপারেশনই হচ্ছে anti child pornography, anti-Church of Scientology ইত্যাদি। এত সংঘবদ্ধতার পরেও মজার ব্যপার হলো যে, তাদের নির্দিষ্ট কোনো নেতা নেই। তার মানে তারা কোনো একজনের নির্দেশে কাজ করেনা।আর এ ব্যপারটাই হয়তো তাদেরকে অন্যান্য গ্রুপ থেকে আলাদা করেছে। যদি কেউ নেতৃত্ব নেওয়ার চেষ্টা করে, তবে তারা অত্যন্ত সুচারুভাবে তাকে দলত্যাগে বাধ্য করে।

৭. *Syrian Electronic Army*

এই হ্যাকার গ্রুপটি সিরিয়ান হ্যাকার দের নিয়ে গঠিত এবং

সেইসাথে ইরান ও হিজবুল্লাহ'র সাথেও এদের ভাল যোগাযোগ আছে।বিভিন্ন কর্মকান্ড দ্বারা তারা এরই মধ্যে নিজেদের ক্ষমতা প্রকাশ করেছে।তাদের মূল টার্গেট হলো বিভিন্ন পশ্চিমা গণমাধ্যম।তারা বিভিন্ন মেলওয়ার ব্যবহার করে যে কারও অবস্থান বের করতে সক্ষম।

৮. *Morpho*

এই হ্যাকার গ্রুপটি ২০১১ সাল থেকে এপর্যন্ত অনেক হাই প্রোফাইল ফার্মাসিউটিক্যাল কোম্পানি, ইনভ্যাস্টম্যান্ট কোম্পানির ওয়েবসাইট সফল ভাবে হ্যাক করেছে।অন্যান্য হ্যাকিং গ্রুপের মত এদের পেছনে কোনো রাষ্ট্রের সহায়তা না থাকলেও প্রযুক্তির দিক দিয়ে এরা অন্যদের থেকে কোনো অংশে পিছিয়ে নেই।এদের হিট লিষ্ট থেকে এমনকি মাইক্রোসফট,এপল,ফেসবুক এবং টুইটারও বাদ পড়েনি। এই গ্রুপটি অন্য সবগুলো গ্রুপ থেকে আকারে ছোট কিন্তু সবচেয়ে ইন্টারেস্টিং। তাদের বিভিন্ন সিগন্যাচারের মধ্যে উল্লেখযোগ্য হলো মাল্টিপ্লাটফর্ম ম্যালওয়্যার, ডকুমেন্টেড কোড, বিটকয়েনস ইত্যাদি। তারা সবাই ইংলিশ স্পীকার এবং নিজেদের ট্রেক লুকাতে সিদ্ধহস্ত।

৯. *Chaos Computer*

এই গ্রুপটি হয়তো লিস্টে একমাত্র গ্রুপ, যারা কোনো নীতি মেনে চলে এবং হ্যাকার গ্রুপের মাঝে এরাই হয়তো সবচেয়ে পুরাতন। ১৯৮১ সালের দিকে একদল জার্মান হ্যাকার এই গ্রুপটি প্রতিষ্ঠা করেন। বর্তমানে এই গ্রুপটি শাখা-প্রশাখা বিস্তার করে বিশাল রুপ ধারণ করেছে। এর সদস্যের বেশিরভাগই হলো জার্মানভাষী।তাদের বিভিন্ন নীতিসম্বলিত কাজের জন্য তারা মাঝে মাঝেই সংবাদপত্রের শিরোনাম হয়। যেখানে তাদের গুণগানই করা হয়ে থাকে।

১০. *Bureau 121*

আউটট-ডেটেড টেকনোলোজিন নিয়েও উত্তর কোরিয়ার সরকার হ্যাকিং এর প্রতি যে পরিমাণ আগ্রহ দেখাচ্ছে, তা রীতিমত কৌতুহলদ্দীপক।স্কুল, কলেজ, ইউনিভার্সিটি ইত্যাদি থেকে সরকার প্রতিবছর মেধাবী ছাত্র-ছাত্রীদের রিক্রুট করে নতুন নতুন গ্রুপ গঠন করে। মিলিটারি একাডেমী থেকেও সেই সাথে হ্যাকার নিয়োগ করা হয়ে থাকে।এদের মূল টার্গেটে থাকে মূলত দক্ষিণ কোরিয়া।কিন্তু অন্যান্য দেশের উপরও এরা সুযোগ পেলে আক্রমণ করে।উদাহরণ স্বরুপ বলা যায় যে,কিছুদিন আগে বাংলাদেশ ব্যাংকের রিজার্ভ থেকে যে টাকা চুরি হয়ে গিয়েছিল, তাদের পেছনেও এইসব কোরিয়ান গ্রুপের হাত আছে বলে ধারণা করা হয়ে থাকে।

বাংলাদেশের শিশু হ্যাকারদের গল্প

আমরা অনেকেই হ্যাকার কথাটা শুনেছি কিন্তু অনেকে কর‍্যাকার কী তা কি আমরা সবাই জানি? আমরা শুনে হতবাক হতে পারি যে আমাদের দেশেও অনেক হ্যাকার তো আছেই, আছে কর‍্যাকাররাও।কর‍্যাকাররাওহ্যাকার আবার অন্য ভাষায় বলা যায় এরা হ্যাকারদের গুরু। আমি ১২ বছর বয়সী বাংলাদেশী এক ক্র্যাকারের গল্প বলতে চাই। তার সবার আগে হ্যাকার আর ক্র্যাকারের পার্থক্যটা আমাদের জেনে নিতে হবে।

হ্যাকার শব্দটি আমাদের কাছে খুব পরিচিত কারণ সোশ্যাল মিডিয়ায় বন্ধুদের প্রায়ই কারো না কারো ফেসবুক একাউন্ট হ্যাক হবার দৌলতে। কিছুদিন আগেও আমরা দেখেছি যে 'পাক-ভারত যুদ্ধ যুদ্ধ খেলায়' দুই দেশে অনেক অয়েব সাইট হ্যাক হয়েছে। যা হোক মিডিয়ার বিভিন্ন তথ্য ঘেটে দেখা যায় যে, হ্যাকার হচ্ছে কিছু প্রতিভাবান মানুষ, যারা সব সময় আমাদের তৈরি বিভিন্ন ওয়েবসাইট ও ওয়েবে থাকা তথ্য নষ্ট করার পাঁয়তারা করে। তবে ভালো হ্যাকারের কথাও জানা যায়। তাই বলা যায়, 'হ্যাকার হচ্ছে এমন ব্যক্তি বা গোষ্ঠী, যারা কম্পিউটারের ব্যবস্থার ব্যাপারে সাধারণের চেয়ে বেশি আগ্রহী এবং তারা একটি কম্পিউটার ব্যবস্থার খুঁটিনাটি সব জানতে চায়। তারা সাধারণ মানুষের চেয়ে একটু ভিন্নভাবে একটি কম্পিউটার ব্যবস্থাকে চিন্তা করে। মূলত তারা কম্পিউটার প্রোগ্রামার। তারা অপারেটিং সিস্টেম বা প্রোগ্রামিং ভাষার ব্যাপারে অন্যদের চেয়ে অনেক বেশি জানে। একটি কম্পিউটার ব্যবস্থা বা নেটওয়ার্কের কোথাও কোনো ফাঁক আছে কি না তারা তার খোঁজ করে। সিস্টেম বা নেটওয়ার্কটির ব্যাপারে বিস্তারিত জানে এবং সংশ্লিষ্টদের সেই

সিস্টেমের ত্রুটির ব্যাপারে জানায় এবং এ ত্রুটি কেন হয়, কীভাবে তা বন্ধ করা যায় তাও বের করে। তারা তাদের সংগৃহীত জ্ঞান সবার জন্য মুক্ত করে দেয়। হ্যাকাররা এসব কাজ কোনো অর্থনৈতিক লাভের আশায় করে না'। নিউ হ্যাকারস ডিকশনারি (এমআইটি প্রেস ১৯৯৬) বইয়ে এরিক এস রাইমন্ড হ্যাকারদের সংজ্ঞা দেন এভাবে– 'হ্যাকার হচ্ছে এমন জ্ঞানপিপাসু ব্যক্তি, যে বিভিন্ন প্রোগ্রামেবল সিস্টেমে ঘুরে বেড়াতে পছন্দ করে।' হ্যাকাররা যে শুধু কম্পিউটার সিস্টেমেই ঘুরে বেড়ায় তা নয়, তারা বিভিন্ন সফটওয়্যারের ত্রুটি বের করে সফটওয়্যার প্রতিষ্ঠানকে জানায়। হ্যাকারদের অনেক সময় একালের রবিনহুডও বলা হয়ে থাকে। কারণ, তারা তাদের জ্ঞানের পিপাসা মেটানোর জন্য একটি কম্পিউটার ব্যবস্থায় অনুপ্রবেশকরে এবং এর দুর্বলতা ঠিক করতে সাহায্য করে। পৃথিবীর বিভিন্ন দেশের রাষ্ট্রীয় সংস্থাও হ্যাকারদের কাজে লাগায় তাদের অনলাইন নিরাপত্তা নিশ্চিত করতে। যুক্তরাষ্ট্রের গোয়েন্দা সংস্থা সিআইএ, এফবিআই, কিংবা এপল, গুগল, ইত্যাদি প্রতিষ্ঠানের নিজস্ব হ্যাকার আছে, যারা তাদের সিস্টেমকে বাইরের আঘাত থেকে রক্ষা করে।

হ্যাকারদের সাধারণত তিন ভাগে ভাগ করা হয়ে থাকে। যেমনঃ সাদা টুপি হ্যাকার-এরা কম্পিউটার তথা সাইবার ওয়ার্ল্ডের নিরাপত্তা প্রদান করে। এরা কখনও অপরের ক্ষতি সাধন করে না। এদেরকে ইথিকাল হ্যাকারও বলা হয়ে থাকে। ধূসর টুপি হ্যাকার- এরা এমন একধরনের হ্যাকার যারা সাদা টুপি ও কালো টুপিদের মধ্যবর্তী স্থানে অবস্থান করে। এরা ইচ্ছে করলে কারও ক্ষতি সাধনও করতে পারে আবার উপকারও করতে পারে। কালো টুপি হ্যাকার-হ্যাকার বলতে সাধারনত কালো টুপি হ্যাকারদেরই বুঝায়। এরা সবসময়ই কোন না কোন ভাবে অপরের ক্ষতি সাধন করে। সাইবার ওয়ার্ল্ডে এরা সবসময়ই ঘৃনিত হয়ে থাকে।

এবার আসি ক্র্যাকারের কথায়। কর ্যাকাররাওএকধরনের হ্যাকার। এরা বিভিন্ন সিস্টেমে ঢুকে সেটির অনেক কিছু পরিবর্তন করে কম্পিউটার ভাইরাস দিয়ে সব তথ্য মুছে দেয়। অনেক সময় বিভিন্ন ওয়েবসাইট হ্যাক করে তার বিনিময়ে টাকা দাবি করে। এ ধরনের হ্যাকারকে কর ্যাকার বলা হয়। পৃথিবীর বিভিন্ন দেশে যেসব সাইবার আইন করা হয়েছে, তা মূলত এসব কর ্যাকারের জন্যই করা হয়েছে। কর ্যাকাররা বিভিন্নভাবে কাজ করে। তারা অনেক সময় একটি সিস্টেমে ঢুকে তার সব তথ্য চুরি করে বেরিয়ে আসে, আবার অনেক সময় পুরো সিস্টেমটি ধ্বংস করে দেয়। বিভিন্ন ব্যাংক বা ই-কমার্স সাইট থেকে ক্রেডিট কার্ড চুরি করে তা চোরাই বাজারে এরাই বিক্রি করে। কর ্যাকারদের দুই শ্রেণীতে ভাগ করা যায়। একশ্রেণীর কর ্যাকার আছে, যারা বিভিন্ন প্রোগ্রাম লিখে বা বিভিন্ন কৌশলে একটি সাইট বা সিস্টেমকে আক্রমণ করে অপর দিকে অন্য আরেক দল কর ্যাকার আছে, যারা বিভিন্ন সফটওয়্যার বা টুলের মাধ্যমে একটি সিস্টেমে অবৈধভাবে প্রবেশ করে। এদের ধরার জন্য বিভিন্ন দেশে সাইবার পুলিশ রয়েছে।

এবার আসি বাংলাদেশি হ্যাকার-ক্র্যাকারদের কথায়। একজন বাবা নিত্য দিনের মতোই বাসায় ফিরে খাবার শেষে তার ছেলের সাথে কিছু কথা শেষ করে নেয়। পড়াশুনায় কোন সাহায্য লাগবে কি না তাও জেনে নেয়। তখন দেখে ছেলে খুব মনোযোগ দিয়ে অংক করছে। এই ফাঁকে সেই বাবা তার মেয়ের সাথে ফোনে কথা বলতে বলতে থাকে। বাবা বলছিলেন যে, ‘তোমার ভাই কম্পিউটারে খুব ভালো, তবে তার এক বন্ধু কম্পিটারে এতো ভালো যে, তাকে হ্যাকার বলে অনেকে’। ছেলেটি তার বাবার মুখের কথা কেড়ে নিয়ে ইংরেজী বাংলা মিশিয়ে যা বলল তা এমনঃ ইংরেজী মাধ্যমে পড়া তার বন্ধু ১৩ বছর বয়সী ‘ক’ (নাম বলতে চাই না) ১২ বছর বয়স থেকেই ইউরোপ অ্যামেরিকার সব বড় বড় সেলিব্রেটিদের ভেরিফাইড ফেসবুকে ঢুঁকে পড়তে

পারে। সেখানে গিয়ে সে এমন বিতর্কিত কথা লিখে পোষ্ট দেয় যে তা নিয়ে শুরু হতে পারে তুমুল বিতর্ক যদি ঐ সেলিব্রেটি তা না ডিলিট করেন। এমন দুই চারটি ঘটনা ঘটেনি তা নয়। এটা তার নেশা। এছাড়া একই সার্ভিস প্রভাইডারের মধ্যে থাকলে সে বন্ধুদের কম্পিউটারে ঢুঁকে তাদের হোম ওয়ার্ক চুরি করে, করে। নিজের মোডিফাই করা সফটওয়্যার দিয়ে দূরে বসেই বন্ধুদের কম্পিউটারের কী বোর্ড নিজের দখলে নিয়ে নিতে পারে। ফলে তার বন্ধু কম্পিউটারে কি করছে তা সে জানতে পারে। তার আরেক বন্ধু আছে যে কম্পিউটার গেমের সাইটগুলোতে ঢুঁকে বিনা পয়সায় গেম ডাউনলোড করে নেয়, বাজার থেকে সে গেম কেনে না। এটাই তার নেশা। কম্পিউটার গেমের সাইটগুলোর পাস ওয়ার্ড ভাঙ্গতে নাকি কয়েক মিলিয়ন টাইম তাকে হিট করতে হয়। বাবা হতবাক হয়ে শোনে সাথে শোনে ছেলেটির বোন। ছেলেটি তার বাবাকে জানায় যে, বাংলাদেশের ঢাকা শহরেই আছে এমন অনেক ট্যালেন্টেড শিশু যারা বিভিন্ন সময় এমন অনেক অবাক করার মত ঘটনা ঘটানর ক্ষমতা রাখে। তাই আমরা বাংলাদেশেও বিভিন্ন সফটওয়্যারের ক্র্যাক ভার্সন বাজারে দেখতে পাই। বাংলাদেশের বিভিন্ন ব্যাংক বা আর্থিক প্রতিষ্ঠানেও এদের মত অনেককে নিয়োগ দেয় নিজেদের সাইবার নিরাপত্তার জন্য।

জর্জ হটজ হলেন প্রথম ব্যক্তি, যিনি আইফোন অপারেটিং সিস্টেমের নিরাপত্তা বলয় ভাঙতে পেরেছিলেন। ২০০৭ সালে মাত্র ১৭ বছর বয়সে আইফোন অপারেটিং সিস্টেম আনলক করে চমকে দিয়েছিলেন তিনি। মাত্র ২৬ বছর বয়সেই আন্তর্জাতিক তারকা স্টেটাস অর্জন করে ফেলেছেন জর্জ হটজ। হ্যাকার হিসেবে শুরু করে শেষ পর্যন্ত চালকবিহীন গাড়ি তৈরির প্রযুক্তি আবিষ্কার করে সাড়া ফেলে দিয়েছেন এই তরুণ।

ছোটবেলা থেকেই প্রযুক্তির প্রতি অদ্ভুত আকর্ষণ জর্জের। ১৪ বছর বয়সে

আন্তর্জাতিক ইন্টেল সায়েন্স ও ইঞ্জিনিয়ারিং মেলায় আশ্চর্য রোবট তৈরি করে তিনি প্রতিযোগিতার চূড়ান্ত রাউন্ডে পৌঁছেছিলেন। একটি ঘর স্ক্যান করে তার যথাযথ পরিমাপ কষে ফেলতে সক্ষম হয়েছিল সেই রোবট। বিভিন্ন সংবাদ চ্যানেলের অনুষ্ঠানে তাকে আমন্ত্রণ জানানো হয়। পাশাপাশি তার আনলক করা দ্বিতীয় ৮ জিবি আইফোনটির বদলে সার্টিসেল সংস্থার প্রতিষ্ঠাতা টেরি ডাইডোনের থেকে পান একটি নিশান ৩৫০ জেড স্পোর্টসকার ও ৩টি ৮ জিবি আইফোন। ২০০৯ সালে জর্জ বাজারে আনেন জেলব্রেক টুল।

হ্যাকিং জগতের রবিনহুড খ্যাত হ্যাকার হামজা বেনডেল্লাজ হ্যাকিং বিশ্বে "BX1" নামে পরিচিত। হামজা বেনডেল্লাজ কি একজন হ্যাকিং জগতের নায়ক নাকি শুধুই একজন সাইবার অপরাধী তা নিয়ে মতভেদ আছে।

হামজা বেনডেল্লাজ এবং রাশিয়ান কোডফেন্ডেট কে SpyEye কম্পিউটার ভাইরাস ব্যবহার এবং অমেরিকান ব্যাংক হতে মিলিয়ন ডলার চুরি করার জন্য দণ্ডিত করা হয়। তাকে ২০১৩ সালে থাইল্যান্ডে একটি এয়ারপোর্ট থেকে গ্রেফতার হয়।

২৭ বছর বয়সী আলজেরিয়ার কম্পিউটার বিজ্ঞানে এ স্নাতকের বিরুদ্ধে ২১৭ টির বেশী আমেরিকান ব্যাংক ও আর্থিক প্রতিষ্ঠান থেকে টাকা চুরি করার অভিযোগ করা হয়। ব্যাংক জালিয়াতি, এবং অন্যান্য অভিযোগের জন্য তিনি ১৭ বছরের কারাদণ্ড এবং এবং ২৪ মিলিয়ন ডলার জরিমানার সম্মুখীন হয়েছিলেন। তাঁর হ্যাক কৃত অর্থের পরিমাণ টাকার অংকে হিসাব করলে ১০০ মিলিয়ন ডলার বলে অনুমান করা হয়। হ্যাক কৃত সব অর্থ তিনি নাকি অসহায় দরিদ্র ফিলিস্তিনদের বিলিয়ে দেন। দুনিয়া জুড়ে বেশিরভাগ হ্যাকার বা ক্র্যাকারই শিশু বা কিশোর কিশোরী।

তথ্যঋণঃ নাম প্রকাশে অনিচ্ছুক এক শিশু, সোশ্যাল মিডিয়া, অন্যান্য

অ্যান্ড্রয়েড ফোন হ্যাকিং কতটা ভয়ঙ্কর হতে পারে

এই যুগে মোবাইল ব্যবহার করেন না এমন মানুষ যেমন পাওয়া যাবে না ঠিক তেমনি অ্যান্ড্রয়েড নামটির সাথে পরিচিত নয় এমন মানুষ খুঁজে পাওয়া দুষ্কর। ৭৪.৬৩ শতাংশ মার্কেট শেয়ার নিয়ে অ্যান্ড্রয়েড খুব ভালো গতিতেই এগিয়ে যাচ্ছে জনপ্রিয়তার চরম শেকড়ে। যদি লক্ষ্য করা যায় সারা বিশ্বে স্মার্টফোন ব্যবহারকারীদের মধ্যে অ্যান্ড্রয়েড ব্যবহারকারী সংখ্যা ৮৫.৪০ শতাংশ।

এই থেকেই বোঝা যাচ্ছে অ্যান্ড্রয়েড ফোনগুলো ব্যবহারকারীদের মাঝে কতটা জনপ্রিয়। আর জনপ্রিয় হবে নাই বা কেন যেখানে গুগোল প্লে-স্টোরে অ্যান্ড্রয়েড অপারেটিং সিস্টেম ব্যবহারকারীদের সুবিধার্থে ও বিনোদনের জন্য রয়েছে ৩ মিলিয়নেরও বেশি অ্যাপ্লিকেশন, যা ব্যবহারকারীদের দৃষ্টি আকর্ষণ করেছে। বাংলাদেশের হিসাবে অ্যান্ড্রয়েড ফোনের জনপ্রিয়তা বয়স ভেদে ১০ থেকে ৮০ সবার কাছেই পরিচিত ও চাহিদার শীর্ষে।

যে অপারেটিং সিস্টেমের এত চাহিদা তার দিকে হ্যাকারদের নজর থাকবে না এটাও ভাবা যায় না। আমাদের ইন্টারনেট জগতে বিভিন্ন

জায়গায় হ্যাকাররা তাদের হ্যাকিংয়ের বিভিন্ন রকমের লোভনীয় ফাঁদ পেতে রেখেছে। যার থেকে আমরা কেউই নিরাপদ নই। ইন্টারনেটের বেশিরভাগ স্থানেই হ্যাকারদের ফাঁদ পাতা আছে। আর আমরা যারা সাধারণ মানুষ আমরা না বুঝে এসব ফাঁদে পা দিয়ে নিজেদের বিপদ ডেকে নিয়ে আসি।

হ্যাকাররা প্রথমেই টার্গেট করে মানুষকে তাদের ফাঁদে, তারপর তারা বিভিন্নভাবে মানুষের বিভিন্ন রকমের ক্ষতি করে। যেমন- ব্লাকমেইল করে থাকে, টাকা চাওয়া, থ্রেড দেয়া, সোশ্যাল মিডিয়া অ্যাকাউন্ট হ্যাক করা, ব্যাংক অ্যাকাউন্ট ও বিভিন্ন প্রয়োজনীয় ইনফরমেশন হাতিয়ে নেয়া ইত্যাদি অপকর্ম করে থাকে হ্যাকাররা। এগুলো থেকে বাঁচতে হলে প্রথমেই আমাদের জানতে হবে কিভাবে সতর্ক থাকা যায় অনলাইন জগতে।

অনলাইনে সতর্ক থাকার বিষয়ে ক্রাইম রিসার্চ অ্যান্ড অ্যানালাইসিস ফাউন্ডেশনের (ক্র্যাফ) সভাপতি জেনিফার আলম বলেন, এখন সব বয়সের মানুষের কাছেই একটি স্মার্টফোন থাকে আর তাদের মধ্যে অ্যান্ড্রয়েড ইউজাররাই বেশি। কিন্তু ইউজারদের মধ্যে অনেকেই সতর্কতা অবলম্বন করেন না, সচেতনও না। হ্যাকিং থেকে বাঁচতে প্রথমেই আমাদের সচেতন হতে হবে। আমরা থার্ড পার্টি অ্যাপস কখনই ইউজ করবো না। আর যেসব অ্যাপস ইউজ করবো

সেগুলোর পারমিশনগুলো দেয়ার সময় একটু পড়ে তারপর পারমিশনগুলো দিবো। হুট হাট করে পারমিশন দিলে ডেটা লিক হওয়ার সম্ভাবনা থাকে অনেক বেশি।

তিনি বলেন, বর্তমানে হ্যাকাররা একটি লিংক দিয়ে বলছে এখানে আপনার খারাপ ছবি আছে, এখানে আপনার ফ্যামিলির ছবি আছে। এছাড়া এখন এমনও বলছে, এখানে রেজিস্ট্রেশন করলে বিকাশ থেকে টাকা পাওয়া যাবে ইত্যাদি। এসব লিংকে কখনই ক্লিক করবেন না। এসব ফিশিং লিংক। আপনার মোবাইল থেকে শুরু করে সোশ্যাল মিডিয়া অ্যাকাউন্ট সব কিছুই হ্যাকারদের কন্ট্রোলে চলে যেতে পারে এসব লিংকে ক্লিক করা মাত্রই।

এখন মোবাইল ফোন আমাদের জীবনের একটি অবিচ্ছেদ্য অংশ হয়ে দাঁড়িয়েছে। মোবাইল ছাড়া এক মুহূর্ত ভাবতে পারি না। ছবি তোলা, গান শোনা ছাড়াও অনলাইন কেনাকাটা থেকে শুরু করে আজ প্রায় অনেক কাজই আমরা মোবাইলের মাধ্যমেই করছি। একটি বার ভাবুন, যদি কখনও আপনার মোবাইলটি হ্যাক করে নেয় কোন হ্যাকার তাহলে কী হবে?

আসুন জেনে নেই আপনার মোবাইলটি হ্যাক হলে কী হবে। প্রথমত

হ্যাক হওয়া মোবাইলের অ্যাকাউন্টের ডিটেইলস ও পাসওয়ার্ড পেয়ে যাবে হ্যাকার। মোবাইলের সব ডিটেইলস চলে যাবে হ্যাকারের কাছে। এতে করে আপনার মোবাইলটি রিমোটলি পরিচালনা করতে সুবিধা হবে হ্যাকারের। আপনি মোবাইলে যা টাইপ করবেন সব কিছুর কপি হ্যাকারের কাছে যেতে থাকবে। আপনার মোবাইলের ও ম্যামরি কার্ডে যা স্টোর করা থাকবে সব পেয়ে যাবে হ্যাকার। হ্যাকার চাইলে আপনার মোবাইলের সামনের ও পিছনের ক্যামেরা অন করে আপনাকে লাইভ দেখতে পারবে ও মাইক্রোফোন অন করে আপনি কি বলছেন শুনতে পারবে। ট্র্যাকিং করে আপনি কোথায় আছেন ও কোথায় যাচ্ছেন সব লাইভ দেখতে পারবে। তাহলে একবার ভাবুন কতটা ভয়ংকর হতে পারে আপনার মোবাইলটি যদি হ্যাক হয়। হ্যাকিং থেকে কিভাবে বাঁচা যায় এগুলো আমাদের জানতে হবে।

অনলাইন নিরাপত্তার ব্যাপারে কারিগরি সহায়তাদানকারী প্রতিষ্ঠান ক্র্যাফের আইটি অ্যানালিস্ট রাইয়ান মালিক বলেন, বর্তমানে হ্যাকার থেকে শুরু করে স্ক্রিপ্টক্রিডি সবার টার্গেট থাকে অ্যান্ড্রয়েড ফোন ব্যবহারকারীদের ওপর। কারণ অ্যান্ড্রয়েড ওপেন সোর্স হওয়ার কারণে এর সব কিছুই ওপেন সোর্স। সুতরাং চাইলে একটু কৌশলের মাধ্যমেই অ্যাটাক করা সম্ভব। অ্যান্ড্রয়েড ফোনে এমন কোন অ্যাপ ইন্সটল করা যাবে না যা বাস্তবে কোন কাজের না।

যেমন ভার্চুয়াল হ্যান্ড স্যানিটাইজার, মশা মারার অ্যাপ ও ইত্যাদি এমন অনেক কিছু রয়েছে। অবশ্যই গুগোল প্লে-স্টোরের বাইরে থেকে কোন অ্যাপ ইন্সটল করা যাবে না। অ্যাডভান্স ইউজার জানা ছাড়া অ্যান্ড্রয়েড ফোন রুট করা যাবে না। অ্যাপ পারমিশন দেয়ার আগে অবশ্যই একবার পড়ে নিবেন। অনাকাঙ্ক্ষিত কোন অ্যাপ ইন্সটল করার জন্য কখনই প্লে-প্রোটেকশন অফ করবেন না ও নিরাপত্তার জন্য ভালো মানের অ্যান্টিভাইরাস ব্যবহার করা যেতে পারে। ইন্টারনেটের বেশিরভাগ স্থানেই হ্যাকারদের ফাঁদ পাতা আছে। সুতরাং সচেতনতা ও সতর্কতাই হ্যাকারদের থেকে বাঁচার সবচেয়ে বড় হাতিয়ার।

মোবাইল ফোন সিকিউর রাখার ১৫টি উপায়-

১। কারো দেয়া কোন লিংকে ক্লিক করা যাবে না।

২। অ্যাপ ইন্সটলেশনের ক্ষেত্রে অবশ্যই গুগোল প্লে-স্টোর থেকে অ্যাপ ডাউনলোড ও ইন্সটল করতে হবে।

৩। তৃতীয় পক্ষের দেয়া বা থার্ডপার্টি কোন ওয়েবসাইট থেকে অ্যাপ ডাউনলোড ও ইন্সটল করা যাবে না।

৪। গুগোল প্লে-প্রোটেকশন সবসময় অন রাখতে হবে।

৫। অ্যাপ ইন্সটলের আগে অ্যাপ পারমিশনগুলো চেক করতে হবে।

৬। অ্যাপলিকেশনের সাথে যায় না বা দরকার নেই এমন কোন

পারমিশন দেয়া যাবে না।

৭। ভালো মানের একটি অ্যান্টিভাইরাস ব্যবহার করতে হবে।

৮। খুব প্রয়োজন ছাড়া পাবলিক ওয়াইফাই ইউজ করা যাবে না। আর খুব প্রয়োজনে ব্যবহার করতে হলে ভিপিএন কানেক্ট করে ব্যবহার করুন।

৯। অ্যাডভান্স ইউজার ছাড়া জাস্ট কোন পারটিকুলার অ্যাপ ইন্সটল করার জন্য ফোন রুট করা যাবে না।

১০। অন্য কারো হাতে নিজের ফোন না দেয়াই ভালো।

১১। লোভনীয় কোন অ্যাড বা লিংকে ক্লিক করা থেকে বিরত থাকুন।

১২। লোভনীয় অ্যাপ ইন্সটল করা থেকে বিরত থাকুন।

১৩। অফিশিয়াল ও ট্রাস্টেড সাইট ছাড়া কোথাও থেকে কিছু ডাউনলোড করা থেকে বিরত থাকুন।

১৪। অ্যান্ড্রয়েড ফোনে গুগোল অ্যাকাউন্ট যুক্ত ও সিনক্রোনাইজেশন অন রাখুন, যাতে করে ডেটা হারালে ফেরত পাওয়া যায়।

১৫। সর্বোপরি সতর্কতা ও সচেতন থাকতে হবে।

যে কোন সাইবার ক্রাইম, অনলাইন প্রতারণা ও হ্যারেজমেন্টের শিকার হলে আইন-শৃঙ্খলা বাহিনীকে জানান ও জরুরী প্রয়োজনে জাতীয় জরুরি সেবা ৯৯৯ নাম্বারে ফ্রি কল করুন।

হ্যাকিং থেকে সাইবার যুদ্ধ

১৯৪১ সালের ঘটনা। তখন দ্বিতীয় বিশ্বযুদ্ধ চলছে। যুক্তরাষ্ট্রের নৌঘাঁটি পার্ল হারবার আক্রমণ করে বসে জাপান। যুক্তরাষ্ট্র এর জবাবে জাপানের হিরোশিমা ও নাগাসাকি শহরে দুটি পারমাণবিক বোমা নিক্ষেপ করে। কিন্তু এত শক্ত জবাব দিয়েও তাদের মন ভরল না। তারা খোঁজ করতে থাকে পার্ল হারবার আক্রমণের পেছনে মূল হোতা লোকটি কে? তবে চাইলেই তো আর তা জানা সম্ভব নয়। সে জন্য প্রয়োজন জাপানিরা যে গোপন ভাষায় তাদের যুদ্ধের সংকেত পাঠাত, তার পাঠোদ্ধার করা। তাই যুক্তরাষ্ট্র এবার গোপন সংকেত ভেদ করার জন্য একটি ক্রিপটো-অ্যানালাইসিস প্রকল্প হাতে নিল। এই প্রকল্পের সাংকেতিক বা কোড নেম ছিল, ম্যাজিক (Magic)। দুই বছর পর মার্কিন নৌবাহিনী গোপন সংকেত ভেদ করে পার্ল হারবার আক্রমণের মূল পরিকল্পনাকারী ইসোরোকু ইয়ামামোতোর নাম আর অবস্থানসহ সব তথ্য জোগাড় করে ফেলে। তারপর যথারীতি তাঁকে হত্যাও করে।

ভবিষ্যতের যুদ্ধ ময়দান থেকে কম্পিউটারে সীমাবদ্ধ হয়ে উঠতে পারে। তখন এক একটি কম্পিউটারই হবে এক একটি দূর্গ

ভবিষ্যতের যুদ্ধ ময়দান থেকে কম্পিউটারে সীমাবদ্ধ হয়ে উঠতে

পারে। তখন এক একটি কম্পিউটারই হবে এক একটি দূর্গ

আজকাল কোনো গোপন কোড উদ্ধার করার কথা শুনলে প্রথমেই আমাদের 'হ্যাকিং' শব্দটির কথাই মনে আসে। হ্যাকিংও মূলত একধরনের গোপন সংকেত উদ্ধারের প্রক্রিয়া। তবে হ্যাকিং বলতে আসলে কম্পিউটার বা ইন্টারনেটে অবৈধভাবে প্রবেশ করাকেই বোঝানো হয়। এর পাশাপাশি এটিএম, ব্যাংক, ওয়্যারলেস নেটওয়ার্ক, ওয়াই-ফাই নেটওয়ার্ক, মোবাইল ফোন, ল্যান্ডফোন, এমনকি কোনো ইলেকট্রনিক ডিভাইসও হ্যাকিংয়ের শিকার হতে পারে। দুর্ধর্ষ হ্যাকাররা কোনো একটি কম্পিউটার বা ইন্টারনেট নিরাপত্তাব্যবস্থার দুর্বল দিকগুলো খুঁজে বের করতে বিশেষভাবে দক্ষ। এখন অনেকেই ভাবছ, কম্পিউটার নিরাপত্তাব্যবস্থার দুর্বল দিকটি আবার কেমন? আসলে এ বিষয়টি ভালোমতো বুঝতে হলে আমাদের ইন্টারনেটের গঠন সম্পর্কে একটু জানা প্রয়োজন।

ইন্টারনেট মূলত সারা পৃথিবীতে থাকা অনেকগুলো কম্পিউটারের একটা নেটওয়ার্ক। কম্পিউটারের নেটওয়ার্ক কথাটার অর্থ হলো এই কম্পিউটারগুলো একটি আরেকটির সঙ্গে সংযুক্ত। এই কম্পিউটারগুলোকে বলা হয় ওয়েব সার্ভার। আমরা ব্রাউজার ব্যবহার করে ওয়েবসাইটের যেসব ফাইল, লেখা, ছবি, ভিডিও ইত্যাদি দেখি, তার সবই এসব কম্পিউটারের হার্ডডিস্কে জমা থাকে।

সাইবার অপরাধ আসলে কী?

আমাদের কম্পিউটার বা স্মার্টফোনটি যখন ওই নেটওয়ার্কের সঙ্গে যুক্ত হয়, তখন আমরা পৃথিবীর সমস্ত ওয়েব সার্ভারে থাকা তথ্যগুলো দেখতে পারি। কিন্তু সব তথ্যই কি দেখতে পারি? যেমন ধরো, কেউ কি ইচ্ছে করলেই তোমার ফেসবুক অ্যাকাউন্টের মেসেজগুলো দেখতে পারবে? উত্তর হলো, না। তুমি ছাড়া এগুলো কেউ দেখতে পারবে না। ওয়েব সার্ভারে তথ্য দেখা বা আদান-প্রদান করার জন্য নির্দিষ্ট পোর্ট (Port) বা দরজা আছে। তেমনি একটি দরজা হলো ফেসবুকের অ্যাকাউন্টে ঢোকার দরজা।

ফেসবুকে তোমার মেসেজগুলো দেখার জন্য তোমাকে অ্যাকাউন্টের চাবি (পাসওয়ার্ড) দিয়ে ঢুকতে হবে। ওয়েব সার্ভারে বিভিন্ন ফাইল বা তথ্য দেখার জন্য অনেকগুলো পোর্ট আছে। কম্পিউটারের প্রোগ্রামিং ভাষা ব্যাবহার করে এসব পোর্ট তৈরি করা হয়। তবে হ্যাকাররা প্রোগ্রামিং ভাষা ব্যবহার করে কম্পিউটারের নিরাপত্তাব্যবস্থায় বিভিন্ন ধরনের নির্দেশ দিয়ে এসব নেটওয়ার্কে ঢুকে পড়ে। একবার ঢুকতে পারলে তারা সেই সার্ভারে থাকা বিভিন্ন গোপন তথ্য দেখতে পারে। এমনকি ব্যাংকে থাকা টাকাও ইচ্ছেমতো তুলে নিতে পারে। আবার সেই নেটওয়ার্কের নিরাপত্তাব্যবস্থাটিও ভেঙে দিতে পারে। এই প্রত্যেকটি কাজই ভীষণভাবে অপরাধ। এ ধরনের সাইবার অপরাধীরা যতই চেষ্টা

করুক না কেন, অধিকাংশ সময়ই তারা ধরা পড়ে। আর তাদের জন্য জেল, জরিমানাসহ কঠিন কঠিন সব শাস্তির ব্যবস্থাও আছে বিভিন্ন দেশে। এই যেমন ব্রিটেনে সাইবার অপরাধীর সর্বোচ্চ শাস্তি হিসেবে যাবজ্জীবন এবং মৃত্যুদণ্ডের বিধান রয়েছে। অন্যদিকে যুক্তরাষ্ট্রে রয়েছে যাবজ্জীবন কারাদণ্ডের বিধান। বাংলাদেশেও বিভিন্ন মেয়াদে কারাদণ্ড ও জরিমানার আইন রয়েছে।

সম্প্রতি বাংলাদেশ ব্যাংকের অ্যাকাউন্ট হ্যাক করে যুক্তরাষ্ট্রের ফেডারেল রিজার্ভে থাকা প্রায় ৮০৮ কোটি টাকা লোপাট করেছে হ্যাকাররা। প্রথম আলোয় প্রকাশিত খবর থেকে জানা গেছে, সাইবার বিশেষজ্ঞরা ধারণা করছেন, প্রথমে কোনো একটি পোর্ট ব্যাবহার করে হ্যাকাররা বাংলাদেশ ব্যাংকের নিজস্ব নেটওয়ার্ক ব্যবস্থায় ঢুকে যায়। এরপর তারা বাংলাদেশ ব্যাংকের নেটওয়ার্ক ব্যবহার করে সুইফটের (SWIFT) মাধ্যমে ফেডারেল রিজার্ভের কম্পিউটার ব্যবস্থাকে তাদের ইচ্ছেমতো ফান্ডে টাকা স্থানান্তরের জন্য পরামর্শ দেয়। (একটি ব্যাংক যখন অন্য কোনো ব্যাংকের সঙ্গে লেনদেন করে, তখন সুইফট সিস্টেম নামে একটি বিশেষ ব্যবস্থার সাহায্যে লেনদেন করে)।

ব্যাংকের নিরাপত্তাব্যবস্থায় সাধারণত তিনটি স্তর বা লেয়ার থাকে। কেউ যদি অবৈধভাবে ব্যাংক থেকে টাকা তুলে নিতে চায়, তবে

তাকে তিনটি স্তরের বাধাকেই টপকে যেতে হবে। প্রথম লেয়ারটি প্রবেশকারীর আইপি (IP) অ্যাড্রেসটি পরীক্ষা করে দেখবে। কোন হিসাবে কেমন আইপি থেকে টাকা লেনদেন হয়, ব্যাংকের ডেটাবেইসে সেটা সংরক্ষণ করা থাকে। যদি ডেটাবেইসের সঙ্গে আইপি না মেলে, তবে ব্যাংকের কম্পিউটার স্বয়ংক্রিয় ব্যবস্থার সাহায্যে প্রবেশ করতে বাধা দেবে। যারা হ্যাক করে, তারা নিজেদের পরিচয় গোপন করার জন্য সাধারণত একটি ভুয়া আইপি (প্রক্সি) অ্যাড্রেস দিয়ে কার্য সিদ্ধি করতে চায়। কোনো প্রক্সি শনাক্ত করার সঙ্গে সঙ্গেই ব্যাংকের সিকিউরিটি সিস্টেম তাকে প্রবেশ করতে বাধা দেবে।

দুর্ধর্ষ সাইবার অপরাধীদের কারণে প্রযুক্তি দুনিয়ায় ব্যক্তিগত কোনো কিছুই আর এখন নিরাপদ নয়

দুর্ধর্ষ সাইবার অপরাধীদের কারণে প্রযুক্তি দুনিয়ায় ব্যক্তিগত কোনো কিছুই আর এখন নিরাপদ নয়

কেউ যদি কোনোভাবে প্রথম লেয়ার পার হয়ে যায়, তবে দ্বিতীয় লেয়ারে গিয়েও তাকে বাধার সম্মুখীন হতে হবে। এই লেয়ারে কম্পিউটার দেখে নেয়, টাকা তোলার জন্য যে রিকোয়েস্ট আসছে, তার ডেটা লেন্থ ঠিক আছে কি না। কোনো গ্রাহক যদি তার নিজের ব্যাংক অ্যাকাউন্টে লগইন করে টাকার তোলার অনুরোধ পাঠায়, তবে তার জন্য একটি নির্দিষ্ট ডেটা লেন্থ থাকবে। কিন্তু কেউ যদি

অন্য কোনো পোর্ট ব্যবহার করে কোনো রিকোয়েস্ট পাঠায়, তবে সেই ডেটা লেন্থ কাস্টমারের ডেটা লেন্থের সঙ্গে মিলবে না। ফলে ব্যাংকের কম্পিউটার বুঝতে পারবে যে এটা আমার গ্রাহক না। ফলে সেটি স্বয়ংক্রিয়ভাবে অনুরোধটি বাতিল করে দেবে। যারা দক্ষ হ্যাকার, তারা বিভিন্ন কৌশলে জেনে ডেটা লেন্থ জেনে নেয়। ফলে তারা এই লেয়ারটিও পার হতে পারে।

দ্বিতীয় লেয়ার অতিক্রম করার পর যেটা থাকে, সেটা মূলত ক্রিপটোগ্রাফি বা গোপন সংকেত ভাঙার কাজ। এই লেয়ার অতিক্রম করা তুলনামূলকভাবে বেশি কঠিন। কিন্তু দক্ষ হ্যাকাররা এই লেয়ারটিও অতিক্রম করতে পারে। কোনো হ্যাকার যদি সব কটি লেয়ার অতিক্রম করে ব্যাংকে থেকে টাকা লেনদেন করে ফেলেও, তবু কিন্তু সে নিরাপদ না। কেননা, ব্যাংকের কম্পিউটার তার ডেটাবেইসে এই লেনদেনের সব ধরনের তথ্য সংরক্ষণ করে রাখে। ঠিক কোন সময়ে, কোন আইপি থেকে, কী পরিমাণ টাকা তুলে নেওয়া হয়েছে, তা একটি লগ ফাইলে জমা থাকে। ব্যাংকের প্রশাসক যেকোনো মুহূর্তে অবৈধ লেনদেনকারীকে শনাক্ত করার মতো সব তথ্য দেখতে পারবেন। কিন্তু এমনও কিছু হ্যাকার আছে, যারা এসব কাজে খুবই দক্ষ। তারা ব্যাংকের প্রশাসনিক অ্যাকাউন্টে প্রবেশ করে লগ ফাইলটি খুঁজে বের করে। তারপর সেটা মুছে ফেলে ব্যাংকের সার্ভার থেকে বের হয়ে যায়।

সময়ের সঙ্গে আমরা প্রযুক্তিনির্ভর হয়ে পড়ছি। ব্যাংক লেনদেন থেকে শুরু করে নাসার মহাকাশযান পর্যন্ত প্রায় সবকিছুই এখন কম্পিউটার ও সার্ভার দ্বারা নিয়ন্ত্রণ করা হয়ে থাকে। আর যখনই কোনো কম্পিউটার বা ইলেকট্রনিক ডিভাইস কোনো একটি নেটওয়ার্কের সঙ্গে যুক্ত থাকবে, তখনই সেটা হ্যাক হওয়ার আশঙ্কা থাকে। ফলে ভবিষ্যতের পৃথিবীতে সাইবার আক্রমণের আশঙ্কা প্রবল। মার্কিন নেতৃত্বাধীন সামরিক জোট ন্যাটো মনে করে, আগামী দিনগুলোয় দুই দেশের মধ্যে সাধারণ যুদ্ধের পাশাপাশি সাইবার যুদ্ধের প্রবণতাও মারাত্মকভাবে বৃদ্ধি পেতে পারে।

ইতিমধ্যে এ রকম বেশ কিছু ঘটনা ঘটেছে। প্রথম ঘটনাটি ঘটে ২০০৭ সালের ২৭ এপ্রিল। সোভিয়েত ইউনিয়ন থাকাকালীন একটি সমাধিসৌধ সরিয়ে নেওয়াকে কেন্দ্র করে রাশিয়া এস্তোনিয়ার সঙ্গে বিরোধে জড়িয়ে পড়েছিল। সেই সূত্র ধরে ২০০৭ সালে রাশিয়া সাইবার আক্রমণ শুরু করে। এতে এস্তোনিয়ার ব্যাংক, সরকারি সব ওয়েবসাইট, গণমাধ্যম, পুলিশ এমনকি জাতীয় জরুরি টেলিফোন পর্যন্ত বন্ধ হয়ে যায়। ন্যাটোর সাইবার প্রতিরক্ষাব্যবস্থার প্রধান ইয়ান ওয়েস্ট বিবিসিকে জানিয়েছেন, ন্যাটোর কম্পিউটারব্যবস্থার ওপর প্রতিদিন লাখ লাখ সন্দেহজনক অনুপ্রবেশের চেষ্টা হয়। সাইবার আক্রমণ থেকে বাদ যায়নি বাংলাদেশও। এ ধরনের ঘটনা ভবিষ্যতে বাড়বে বলেই আশঙ্কা করছেন বিশেষজ্ঞরা। তবে কম্পিউটার নিরাপত্তাব্যবস্থার উন্নতির পাশাপাশি প্রযুক্তি ব্যবহারে সতর্কতা নেওয়া হলে এসব আক্রমণ থেকে রক্ষা পাওয়া সম্ভব।

২২ এপ্রিল ২০১৯

ইসলামিক সাইবার সিকিউরিটি একটি অনলাইন ভিত্তিক সংগঠন যা মানুষকে সাইবার অপরাধ সম্পর্কে সচেতন করে, কেউ সাইবার অপরাধের শিকার হলে তাকে সাধ্য মতো সাহায্য করে। দূর্যোগ মোকাবেলায় মানুষকে সচেতন করে এবং বৃক্ষরোপণ, ত্রাণ বিতরণসহ বিভিন্ন সামাজিক উন্নয়নমূলক কাজগুলো করে থাকে।