বাংলাদেশে সাইবার অপরাধ

এম. মিজানুর রহমান সোহেল

বাংলাদেশে তথ্যপ্রযুক্তির ব্যবহার দেরি করে শুরু হলেও সাইবার অপরাধের দিক থেকে বাংলাদেশ অন্য অনেক দেশ থেকে এগিয়ে। স্থানীয়ভাবে সাইবার আক্রমণের ক্ষেত্রে বাংলাদেশ পৃথিবীর শীর্ষস্থানে অবস্থান করছে। এ দেশের হ্যাকারেরা দেশে-বিদেশে হ্যাকিং করে বিশ্ব গণমাধ্যমে বারবার জায়গা করে নিয়েছে। নানা কারণে বাংলাদেশে এখন 'সাইবার অপরাধ' শব্দটি ব্যাপক পরিচিত। কিন্তু অবাক করা সত্য হচ্ছে, নিয়ন্ত্রক সংস্থা বিটিআরসি, র‍্যাব বা পুলিশের কাছে বাংলাদেশের সাইবার অপরাধ সংক্রান্ত কোনো পরিসংখ্যান নেই! এমনকি সাইবার অপরাধ নিয়ন্ত্রণ করার জন্য গঠিত বিশেষ টিম বিডি-সিএসআইআরটির (বিডিসার্ট) কাছেও উল্লেখ করার মতো কোনো তথ্য নেই। এরা সরকারি-বেসরকারি ওয়েবসাইট স্ক্যান করাসহ নানা দায়িত্বে থাকলেও তাদের নিজেদের ওয়েবসাইটই দীর্ঘদিন ধরে নিষ্ক্রিয় হয়ে আছে! এমন পরিস্থিতিতে ব্যক্তি-উদ্যোগের বাইরে বাংলাদেশের সাইবার অপরাধ সংক্রান্ত তথ্য-উপাত্ত পাওয়া বেশ কঠিন। তারপরও এ সম্পর্কিত কিছু তথ্য এবং সংশ্লিষ্ট ব্যক্তির সাথে কথা বলে পাঠকের জন্য রচিত হলো বাংলাদেশে সাইবার অপরাধ।

বাংলাদেশে তথ্যপ্রযুক্তির অগ্রযাত্রা আশাব্যঞ্জক। চলমান এ গতিশীলতা বাড়ানোর লক্ষ্যে সরকারিভাবে বিভিন্ন কার্যক্রমও হাতে নেয়া হচ্ছে। বর্তমান বিশ্বে আইসিটি বাদ দিয়ে উন্নয়ন পরিকল্পনা গ্রহণ অকল্পনীয়। এ ক্ষেত্রে সম্পদের প্রয়োজন অনেক কম থাকায় দেশের বিশাল অলস শ্রমকে প্রযুক্তির সাথে সম্পৃক্ত করা গেলে আইসিটিতে অগ্রগামী দেশগুলোর তালিকায় বাংলাদেশের অবস্থান ঈর্ষণীয় পর্যায়ে উত্তরণ ঘটানো সম্ভব। ব্যক্তিগত এবং বেসরকারি প্রতিষ্ঠানে ইতোমধ্যেই ইন্টারনেট ব্যবহারকারীর সংখ্যা ক্রমশ বাড়ছে। ইতোমধ্যে বেশ কিছু সরকারি এবং বেসরকারি প্রতিষ্ঠান, ব্যাংক-বীমা কোম্পানি ইন্টারনেটের মাধ্যমে জনগণকে সেবা দেয়ার কর্মসূচি চালু করেছে। হয়তো অচিরেই উন্নত বিশ্বের মতো আমরাও আইসিটিনির্ভর হয়ে যাব। কিন্তু সে অনুযায়ী এর অপব্যবহারের দিকটি নিয়ে কতটুকু সচেতন আমরা?

সাইবার অপরাধ কী?

'সাইবার অপরাধ' বলতে ইন্টারনেট ব্যবহার করে যে অপরাধ করা হয়, তাকেই বোঝানো হয়। খুব সাধারণ অর্থে সাইবার অপরাধ হলো যেকোনো ধরনের অনৈতিক কাজ, যার মাধ্যম বা টার্গেট উভয়ই হলো কমপিউটার। বাংলাদেশে সাইবার ক্রাইমের পরিচিতি বা এ সংক্রান্ত অপরাধ দমনের জন্য সংশ্লিষ্ট আইনটি অনেকেরই জানা নেই। তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ আমাদের এ বিষয়ে নির্দেশনা দেয়। এ আইনে ইন্টারনেট অর্থ এমন একটি আন্তর্জাতিক কমপিউটার নেটওয়ার্ক, যার মাধ্যমে কমপিউটার, সেলুলার ফোন বা অন্য কোনো ইলেকট্রনিক পদ্ধতি ব্যবহারকারীরা বিশ্বব্যাপী একে অন্যের সাথে যোগাযোগ ও তথ্যের বিনিময় এবং ওয়েবসাইটে উপস্থাপিত তথ্য অবলোকন করতে পারে। সাইবার অপরাধ অতিপরিচিত ও ভীতিকর একটি শব্দ। তথ্য চুরি, তথ্য বিকৃতি, প্রতারণা, ব্ল্যাকমেইল, অর্থ চুরি ইত্যাদি তথ্যপ্রযুক্তির মাধ্যমে করা হলে সেগুলোকে সাধারণ ভাষায় সাইবার অপরাধ বলা হয়। সাইবার অপরাধ মূলত কমপিউটারে ব্যবহৃত কর্মকাণ্ড, যার নেটওয়ার্ক ব্যবহার করে বিশ্বব্যাপী অপরাধ পরিচালিত করে থাকে অপরাধীরা।

এফবিআইর মতে

মার্কিন যুক্তরাষ্ট্রের গোয়েন্দা সংস্থা ফেডারেল ব্যুরো অব ইনভেস্টিগেশনের (এফবিআই) আইসিটি বিশেষজ্ঞদের মতে, সাইবার অপরাধীরা সাধারণত চার ভাগে বিভক্ত : ০১. প্রতিষ্ঠানের অভ্যন্তরীণ লোক (Insiders), ০২. প্রতিষ্ঠানের বাইরের বা অনুপ্রবেশকারী (Hackers), ০৩. ভাইরাস সৃষ্টিকারী/ভাইরাস লেখক (Virus Writers) এবং ০৪ বিভিন্ন অপরাধী চক্র (Criminal Groups)।

বেশিরভাগ ক্ষেত্রে প্রতিষ্ঠানের নিজস্ব বর্তমান বা সাবেক কর্মচারীরা লোভে পড়ে বা অর্থের জন্য প্রতিষ্ঠানের অবকাঠামোগত দুর্বলতাগুলো হ্যাকারদের কাছে প্রকাশ করে। হ্যাকারেরা তাদের কারিগরি জ্ঞান ব্যবহার করে আর্থিক প্রতিষ্ঠানের নেটওয়ার্কের পাসওয়ার্ড ভেঙে প্রতিষ্ঠানের অ্যাকাউন্ট থেকে অর্থ বা প্রয়োজনীয় তথ্য সরিয়ে নেয়, তবে ভাইরাস সৃষ্টিকারীরা আর্থিক লোভে এসব করে না। এরা মূলত কৌতূহলবশে এবং কখনও কখনও বিকৃত মানসিকতা থেকেই এসব করে থাকে। এটা এমনই একটি অপরাধ, যা সংঘটিত করা যায় বিশ্বের যেকোনো প্রান্তে বসে, যেকোনো অবস্থান বা ব্যক্তিকে উদ্দেশ করে। অনেকটা বায়বীয় হওয়ায় এর আলামত সংগ্রহও অসম্ভব। ফলে অপরাধী শনাক্ত করা এবং আইনের হাতে সোপর্দ করা খুবই দুরূহ। সেই সাথে আমাদের দেশের পুলিশ প্রশাসনের কারিগরি জ্ঞানের তুলনায় এসব সাইবার অপরাধী অনেক বেশি আধুনিক ও উন্নত প্রযুক্তিজ্ঞানসম্পন্ন।

সাইবার ক্রাইমে আর্থিক ক্ষতি

প্রতিবছর বিশ্বব্যাপী এসব অপরাধের মাধ্যমে শত শত ডলারের অর্থনৈতিক ক্ষতি হচ্ছে। আন্তর্জাতিকভাবে বিভিন্ন সংস্থা প্রতিবছর সারা বিশ্বে সাইবার অপরাধের কারণে অর্থনৈতিক ক্ষতির পরিমাণের জরিপ প্রকাশ করে। কমপিউটার ইকোনমিক্সের জরিপ অনুযায়ী, ২০০৬ সালে শুধু ভাইরাসের কারণে ক্ষতি হয়েছিল ১৩.৩ বিলিয়ন ডলার। প্রযুক্তিনির্ভর বিশ্বে যেহেতু তথ্য বা অর্থ কাগজের বদলে প্রযুক্তির মাধ্যমে সংরক্ষণ করা হচ্ছে, তাই এ অপরাধের শিকার ওরাই বেশি। ইন্টারপোলের ওয়েবসাইটে দেয়া তথ্যমতে ২০০৭-০৮ সালে বিশ্বে আর্থিক ক্ষতি ছিল ৮ বিলিয়ন কোটি ডলার, ২০১১ সালে ৬৩.৭ বিলিয়ন ডলার এবং আগামী ২০১৭ সালে এর পরিমাণ দাঁড়াবে ১২০.১ বিলিয়ন ডলার। এদিকে বাংলাদেশে ঘটে যাওয়া সাইবার অপরাধগুলো ▸

হ্যাকারেরা হচ্ছে দুর্বল ও রোগাক্রান্ত মানসিকতার মানুষ

লেফটেন্যান্ট কর্নেল জিয়াউল আহসান
প্রধান কর্মকর্তা, ইন্টেলিজেনস উইং, র‍্যাব, প্রধান কার্যালয়

সরকারের দুর্বলতার কারণে হ্যাক হচ্ছে। আর এসব সাইটের নিরাপত্তা দেয়ার জন্য এখানে নেই কোনো যোগ্য লোক। তাই হ্যাকারেরা সহজেই এসব সাইট হ্যাক করতে সক্ষম হচ্ছে।

বাংলাদেশে সাইবার আইন কঠোর করতে হবে। সরকারি বাহিনীর নজরদারি বাড়াতে হবে। হ্যাক হলে আইনে আছে এই অপরাধটি জামিনযোগ্য অপরাধ। কিন্তু এর সাজা বাড়িয়ে অজামিনযোগ্য অপরাধ হিসেবে আইন প্রণয়ন করে তার প্রয়োগ করতে হবে।

এগুলো মূলত ফেইক হ্যাকার। কারণ, যারা অপরাধ করে তারা ঘোষণা দিয়ে অপরাধ করে না। তাদের হুমকি-ধমকি দেখে ভয় পাওয়ার কিছু নেই। হ্যাকারেরা হচ্ছে দুর্বল ও রোগাক্রান্ত মানসিকতার মানুষ। এছাড়া অন্যের তথ্য চুরি করে মজা নেয়া ছাড়া তাদের কোনো কাজ নেই।

বাংলাদেশে প্রতিদিন গড়ে কী পরিমাণ সাইবার হামলা হয় সে সম্পর্কে কোনো পরিসংখ্যান নেই। বাংলাদেশে সাইবার অপরাধ আইন সাইবার অপরাধ প্রতিরোধে যথেষ্ট নয়। অবশ্যই আইন সংশোধন করতে হবে। তা না হলে সাইবার অপরাধ থেকে দেশের মানুষ মুক্তি পাবে না। তারা যা খুশি তাই করে যাবে, কিন্তু আইনের দুর্বলতার কারণে তাদের বিরুদ্ধে কোনো ব্যবস্থা নেয়া যাবে না।

আমি ব্যক্তিগতভাবে কয়েকটি কাজ করেছি। হুমায়ূন আহমেদের স্ত্রী শাওনকে সম্প্রতি ফেসবুকে একজন হুমকি দেয়, তখন আমিই এই কেসটি ডিল করেছি। সাইবার অপরাধ সম্পর্কে আমাদের বিশেষজ্ঞেরা ভালোমতো আইনও জানে না। যাকে আমরা আটক করলাম তাকে কোর্টে নিয়ে গিয়ে প্রথমেই রিমান্ড চাইল। প্রথমে তার নামে মামলা হওয়ার দরকার ছিল এবং তার নামে মামলা করা যাবে কি যাবে না, তা কোর্ট থেকে অনুমতি নেয়ার দরকার ছিল। নিয়ম হচ্ছে আমরা আসামীকে আটক করি। আটক করার পর তাকে কোর্টে হস্তান্তর করে আদালতকে বলতে হবে অভিযুক্তের নামে মামলা রুজু করার জন্য আবেদন প্রার্থী। কোর্ট আবেদন গ্রহণ করলে তাকে গ্রেফতার দেখাবে। পরের দিন তার নামে রিমান্ড চাইবে। এটা হচ্ছে আইন। কিন্তু পুলিশ সরাসরি তার নামে রিমান্ড চাওয়ার ফলে আসামী পক্ষ থেকে শোকজ করা হয় এবং কোর্ট তার জামিন দিয়ে দেয়। আইনের এই সামান্য দুর্বলতার সুযোগ নিয়ে আসামী বের হয়ে এসেছে। শেষ পর্যন্ত এ মামলার কিছুই হয়নি।

যখন আপনি দেখবেন আইনগত কারণে কারও বিচার হচ্ছে না, তখন কিন্তু মানুষ তার আস্থা হারিয়ে ফেলে। এখানে প্রধান সমস্যা মূলত আইনগত। দেখা গেল প্রথমবার ধরলাম সে ছাড়া পেয়ে গেল, দ্বিতীয়বার ধরলাম আবার সে ছাড়া পেয়ে গেল, তৃতীয়বার ধরলাম আবারও সে ছাড়া পেয়ে গেল। এখন আমি নিজেই আস্থা হারিয়ে ফেলি।

অর্থনৈতিক মূল্যমানে বড় ছিল না, কারণ অর্থনৈতিক ব্যবস্থাপনা এখন পর্যন্ত পুরোপুরি তথ্যপ্রযুক্তিনির্ভর নয়। তাই এখানে ক্ষতির পরিমাণ নিরূপণের ব্যবস্থাও নেই। তবে ক্যাসপারস্কির বাংলাদেশের প্রধান প্রবীর সরকার জানান, ২০০৯ সালের জুনে ঢাকা স্টক এক্সচেঞ্জ ভাইরাস আক্রান্ত হয়ে সাময়িক সময়ের জন্য বন্ধ ছিল। সেই অল্প সময়ে বিপুল অর্থনৈতিক ক্ষতি হয়।

বিভিন্ন ধরনের সাইবার অপরাধ

সাইবার আইন ইন্টারনেট আইন হিসেবেও পরিচিত। অন্যদিকে সাইবার অপরাধ পরিচিত সাইবার টেররিজম বা সাইবার সন্ত্রাস নামেও। দু'টি পর্যায়ে এ ধরনের অপরাধমূলক কর্মকাণ্ডকে ভাগ করা সম্ভব। ০১. ইন্টারনেটের মাধ্যমে কমপিউটার, নেটওয়ার্ক অবকাঠামোকে সরাসরি আক্রমণ। ০২. ইন্টারনেটের মাধ্যমে ব্যক্তি ও জাতীয় নিরাপত্তায় ব্যতয় ঘটানো। এ দুই অংশে সাইবার অপরাধও ঘটতে পারে– ০১. ভাইরাস আক্রমণ। ০২. ব্যক্তি/প্রতিষ্ঠান বা রাষ্ট্রীয় ওয়েবসাইট হ্যাকিং। ০৩. মেলওয়্যার স্প্যামিং বা জাঙ্ক মেইল; এটি সম্পূর্ণ ই-মেইলভিত্তিক। ভুয়া আইডি/ই-মেইল অ্যাড্রেস ব্যবহার করে নাম-ঠিকানা, ক্রেডিট কার্ড নাম্বার এমনকি ফোন নাম্বার নিয়ে মিষ্টি কথায় ভোলাতে চেষ্টা করবে অপরাধী চক্র। ফাঁদে পা দিলেই বিপদ! স্প্যাম ফোল্ডারে প্রায়ই এমন মেইল আসে। ০৪. সাইবার স্টকিং বা সাইবার হয়রানি– ই-মেইল বা ব্লগ বা ওয়েবসাইট ব্যবহার করে হুমকি দেয়া, ব্যক্তির নামে মিথ্যাচার/অপপ্রচার, নারী অবমাননা, যৌন হয়রানি। ০৫. ফিশিং– লগইন/অ্যাকসেস তথ্যচুরি, বিশেষত ই-কমার্স, ই-ব্যাংকিং সাইটগুলো ফিশারদের লক্ষ্যবস্তু হয়ে থাকে। র‍্যাপিড শেয়ার সাইটে প্রিমিয়াম অ্যাকাউন্ট অ্যাকসেস তথ্যচুরির মতো ফিশিং ঘটেছে। ফিশারদের দিয়ে মাইস্পেসের লগইন তথ্যও চুরি হয়েছিল। ০৬. অর্থ আত্মসাৎ– ইন্টারনেট থেকে তথ্যচুরি করে ব্যাংকের এক অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে অর্থ স্থানান্তর একটি উদাহরণ। ইন্টারনেটে ব্লগ, ই-মেইল, ফেসবুক ব্যবহার করে মিথ্যা তথ্য দিয়ে অথবা প্রাপ্ত তথ্য ব্যবহার করে অর্থ আত্মসাতের ঘটনাও ঘটে। যেমন কিছুদিন আগে ব্লগার হাসনা হেনা ও রোজলীনের বিরুদ্ধে বেশ কয়েকটি বাংলা ব্লগ থেকে অর্থ জোচ্চুরির অভিযোগ উত্থাপিত হয়। ০৭. সাইবার মাদক ব্যবসায়– পুলিশের চোখ এড়াতে ইদানীং ইন্টারনেট ব্যবহার করে মাদক চালানের ব্যবসায়িক যোগাযোগ বেড়েছে। ০৮. পাইরেসি– সদ্য প্রকাশিত গান ও সিনেমার এমপিথ্রি বা মুভি ফাইল ইন্টারনেটে শেয়ার হয়ে যাচ্ছে। ০৯. ইন্টেলেকচুয়াল প্রোপার্টি– ব্লগ ও ওয়েবসাইট থেকে কোনো লেখা ও ফটোগ্রাফ সহজেই কপি-পেস্ট করে নিজের নামে চালিয়ে দেয়ার প্রবণতা বেড়েছে সাইবার কমিউনিটিতে। ১০. পর্নোগ্রাফি– শিশু পর্নোগ্রাফি ইন্টারনেটে ভয়ঙ্করভাবে বেড়েছে। রগরগে অশ্লীল সাইটগুলোতে অনেক সময় ফাঁদ পেতে থাকে অপরাধীরা। বেশকিছু সাইটে থাকে ক্ষতিকর কমপিউটার ভাইরাস। ক্লিক করতে থাকলে কিংবা এক পর্যায়ে ই-মেইল আইডি (ফ্রি সাবস্ক্রাইব) দিলেও তথ্য চুরি হওয়ার সম্ভাবনা থাকে। পর্নোগ্রাফিতে গোপনে ধারণ করা, অনুমতিহীন ব্যক্তিগত ছবি/ভিডিও প্রকাশ বেড়েছে। ১১. ব্যক্তিগত তথ্য-পরিচয়-ছবি চুরি ও ইন্টারনেটের অপব্যবহার যারা নিয়মিতভাবে ইন্টারনেটে বিচরণ করেন, তাদের আক্রান্ত হওয়ার আশঙ্কা থেকে যায়। ১২. হ্যাকিং– বাংলাদেশে ২০০৮ সালে র‍্যাবের ওয়েবসাইট স্বনামে হ্যাক করে ২১ বছর বয়সী কমপিউটার ইঞ্জিনিয়ারিং পড়ুয়া তরুণ শাহী মির্জা। শুধু তাই নয়, সে বেশ কয়েকটি আইন-শৃঙ্খলা রক্ষাকারী বাহিনীর ওয়েবসাইটে ঢুকতে সক্ষম হয়। র‍্যাবের সদস্যরা তাকে ধরতেও সমর্থ হয় এবং শাহী মির্জা তার অপরাধ স্বীকার করে। তবে মির্জা যা করেছিল তা হলো হ্যাকিং। ১৩. ক্র্যাকিং– ক্র্যাকিং হলো গুরুত্বপূর্ণ তথ্য কিংবা ক্রেডিট কার্ড নাম্বার চুরি করে গোপনে অনলাইন ব্যাংক থেকে ডলার চুরি করা। সে ক্ষেত্রে শাহী মির্জার বক্তব্য অনুযায়ী, বাংলাদেশী ওয়েবসাইটগুলো প্রকৃত বা বৈধ প্যাকেজ সফটওয়্যার ব্যবহার না করার কারণে নিরাপত্তাহীন। হ্যাকিং ও ক্র্যাকিং দুটোই অপরাধ, তবে ক্র্যাকিং মারাত্মক অপরাধ।

বাংলাদেশে সাইবার অপরাধ

বাংলাদেশে যত সাইবার অপরাধের ঘটনা জনসমক্ষে এসেছে, তার বেশিরভাগই হয়েছে শৌখিন ও কাঁচা হ্যাকার/ক্র্যাকারদের দিয়ে। এর আগে পরিচয় লুকিয়ে প্রধানমন্ত্রী শেখ হাসিনাকে (বিরোধীদলীয় নেতা থাকাকালীন) ই-মেইলে হুমকি, আইন প্রয়োগকারী সংস্থার ওয়েবসাইট হ্যাক, বিভিন্ন প্রতিষ্ঠিত ব্যক্তির ব্যক্তিগত তথ্য ও ছবি চুরিসহ আরও অনেক ন্যক্কারজনক ঘটনা ঘটেছে। প্রচলিত সাইবার অপরাধের মধ্যে আছে ফ্রড কিংবা প্রতারণা, ক্রেডিট কার্ডের নাম্বার চুরি, ব্ল্যাকমেইল, পর্নোগ্রাফি, হয়রানি, অনলাইনের মাধ্যমে মাদক পাচার/ব্যবসায় প্রভৃতি। আবার জাল সার্টিফিকেট তৈরি, জাল টাকা বা জাল পাসপোর্ট, বিভিন্ন ধরনের দলিল-দস্তাবেজ কমপিউটারের মাধ্যমে তৈরির ঘটনা অহরহ উদ্ঘাটিত হচ্ছে। ▸

বাংলাদেশে হ্যাকিংয়ের জোয়ার

বাংলাদেশে হ্যাকিংয়ের ঘটনা খুব বেশি পুরনো নয়। ২০১১ সালের একটি ছোট ঘটনাকে কেন্দ্র করে দেশে ব্যাপক হারে হ্যাকিংয়ের ঘটনা ঘটতে থাকে। একইভাবে ২০১১ সালের ৭ জানুয়ারি কুড়িগ্রাম জেলার ফুলবাড়ী উপজেলার অনন্তপুর সীমান্তের ৯৪৭ নাম্বার আন্তর্জাতিক সীমানা পিলারের কাছে একটি ঘটনা ঘটে, যা দেশের তরুণ সমাজের মনে দারুণভাবে পীড়া দেয়। ওইদিন ভারত থেকে বাংলাদেশে ফেরার সময় ফেলানি (১৫) নামে এক কিশোরীকে বিএসএফ গুলি করে হত্যা করে এবং পাঁচ ঘণ্টা তার লাশ কাঁটাতারের সাথে ঝুলন্ত অবস্থায় রাখার পর ভারতে নিয়ে যায়। এ ঘটনার প্রতিবাদ রাষ্ট্রীয়ভাবে করা না হলেও অনলাইনে সাইবার যুদ্ধ করে বাংলাদেশের তরুণ সমাজ দেখিয়ে দিয়েছে বাংলাদেশের মানুষ কী করতে পারে। এ সাইবারওয়ার এত বেশি ভয়াবহ ছিল যে পৃথিবীর তাবৎ মিডিয়া এ ঘটনার কাভারেজ দিয়েছে। এ যুদ্ধ আরও মারাত্মক আকার ধারণ করে ২০১২ সালের ফেব্রুয়ারি মাসে। বাংলাদেশী হ্যাকারেরা ভারতের শক্তিশালী হাজার হাজার ওয়েবসাইট হ্যাক করে নিজেদের অবস্থান জানিয়ে দেয়। এ সময় অনেক ক্ষুদে হ্যাকারের জন্ম হয় বাংলাদেশে। এ হ্যাকারদের অনেকেই এখনও এসএসসি পরীক্ষা দেয়নি। আবার এ বছর এসএসসির অনেক ক্ষুদে হ্যাকারের ফলাফল প্রকাশিত হয়েছে। প্রসঙ্গত, ২০১১ সালের ফেলানি হত্যার প্রতিবাদে ২০১৩ সালের ৭ জানুয়ারি বর্ষপূর্তি উপলক্ষেও ভারতের অনেক সাইট হ্যাক করেছে বাংলাদেশী হ্যাকারেরা এবং তারা জানায়, যতদিন ফেলানি হত্যার বিচার হবে না ততদিন বর্ষপূর্তিতে বড় ধরনের হামলা চালানো হবে।

বাংলাদেশেও বিশ্বসেরা হ্যাকার

উপরের লেখা পড়ে মনে হতে পারে বাংলাদেশী হ্যাকারেরা তো সবে মাত্র এসএসসি পাস। এমনটা ভাবলে ভুল করবেন। কারণ, বাংলাদেশেও রয়েছে বিশ্বসেরা হ্যাকার। রটাটিং রটার, টাইগার ম্যাট বা মেহরাবের কথা জানে না এমন ভিনদেশী হ্যাকার পাওয়া যাবে না। এসব হ্যাকার অনেকবার দেশী ও বিদেশী মিডিয়াতে ঝড় তুলেছে। পৃথিবীর সবচেয়ে শক্তিশালী ওয়েবসাইট গুগল হ্যাক করা কি সহজ না কঠিন? উত্তর নিশ্চয় জানা আছে। তারপরও বাংলাদেশী হ্যাকার টাইগার ম্যাট গুগলের সাইট কয়েক দফায় হ্যাক করে নিজের অবস্থান জানান দিয়েছে। এবার যদি প্রশ্ন করা হয়, পৃথিবীর সবচেয়ে নিরাপদ ব্যাংক সুইস ব্যাংক হ্যাক করা কতটা সহজ? ভাবছেন, এটাও হ্যাক করা যায়? হ্যাঁ, বাংলাদেশী হ্যাকার রটাটিং রটার সেটাও করে দেখিয়েছে! তবে সে ব্যক্তিগতভাবে সৎ বলে কোনো ক্রেডিট ট্রান্সফার করেনি। এ খবরটি সারা পৃথিবীর মিডিয়া ফলাও করে প্রকাশ করেছিল। এমনকি ঘটনার তদন্ত করার জন্য ইন্টারপোল থেকে বাংলাদেশে তদন্ত কর্মকর্তা এসেছিলেন। এমন অনেক হ্যাকারই বাংলাদেশে বাস করে। এ লেখার সাথে বিশ্বসেরা হ্যাকার রটাটিং রটারের একটি ইন্টারভিউ দিতে সক্ষম হয়েছেন এ প্রতিবেদক। সে খোলামেলা অনেক কথা জানিয়েছে। ইন্টারভিউ থেকে অনেক অজানা উঠে এসেছে।

হ্যাকারদের ডেভেলপারে রূপান্তর করলে দেশে সাইবার অপরাধ থাকার কথা নয়

প্রবীর সরকার

নির্বাহী পরিচালক, অফিস এক্সট্র্যাক্টস ও ক্যাসপারস্কি ল্যাব বাংলাদেশ

বাংলাদেশের কমপিউটারগুলোর ওপর নিয়মিত অ্যাটাক হওয়ার দিক থেকে পৃথিবীর ৪২তম দেশ বাংলাদেশ। এটি আমাদের দেশের জন্য একটি ভয়াবহ দুঃসংবাদ। কারণ, যখন বাংলাদেশে পূর্ণাঙ্গভাবে অনলাইন ব্যাংকিং চালু হবে তখন দেখবেন এটি লাফিয়ে লাফিয়ে ৩ বা ৪ নম্বর অবস্থানে চলে আসবে। আপনাকে আগেই বলেছি সাইবার ক্রাইমের চেতনা পরিবর্তন হয়ে গেছে, তাই এখন আশঙ্কাও বাড়ছে হু হু করে। আমাদেরকে এখনই সাবধান হতে হবে। না হলে আমরা বিপদগ্রস্ত হলে তা প্রাথমিক অবস্থায় অনুমানও করতে পারব না। কিন্তু ততক্ষণে বিপদের মহাসমুদ্রে আক্রান্ত হয়ে যাব।

বাংলাদেশের কমপিউটার ডিভাইসগুলো ৯৯ শতাংশ ভাইরাসে আক্রান্ত। এসব ভাইরাসে কোনো না কোনোভাবে আপনার ব্যক্তিগত তথ্য, ব্যাংক অ্যাকাউন্টের তথ্য, মেইল বা ফোন নাম্বারসহ সব তথ্য পাচার হয়ে যাচ্ছে। এখন অনলাইনেই একটি দেশের সাথে আরেকটি দেশের যুদ্ধ হচ্ছে। যেমন ইরানে সম্প্রতি ক্লেইম ভাইরাস ছড়িয়ে দেয়া হয়েছে এবং এখান থেকে তথ্য পাচার হয়ে যাচ্ছে।

শত্রু দেশ ভাইরাস দিয়ে ক্ষতি করার চেষ্টা করেছে, আমাদের দেশে লোকাল ইনফেকশনও আসছে।

অনেকভাবেই আসছে। যেমন পেনড্রাইভ, সিডি, পাইরেটেড সফটওয়্যার, ইন্টারনেটে ফ্রি সফটওয়্যার ডাউনলোড লিঙ্ক, পর্নোগ্রাফি ইত্যাদি জায়গা থেকে এগুলো আসছে। এছাড়া একটি নতুন পিসি ইনস্টল করার সময় পাইরেটেড সফটওয়্যার ইনস্টল করে দেয়া হচ্ছে। ফলে জন্মগতভাবেই সে ভাইরাসে আক্রান্ত হয়ে যাচ্ছে।

সাইবার অপরাধ প্রতিরোধের সম্পূর্ণ দায়িত্ব সরকারের। সাইবার অপরাধ প্রতিরোধ করার জন্য সরকারের একটি নীতিমালা থাকতেই হবে। আইএসপি, সার্ভিস প্রোভাইডার বা যারা কমপিউটার ব্যবসায়ের সাথে জড়িত, তাদের প্রত্যেকটি জায়গায় চেক অ্যান্ড ব্যালেন্স ফর্মুলা থাকতে হবে। ইন্টারনেটের আপলোড স্পিড কমিয়ে দেয়া কিন্তু কোনো সমাধান নয়। সরকারের কাজ হলো মানুষকে সচেতন করে গড়ে তোলা। তাদেরকে জানাতে হবে ডিজিটাল লাইফের প্রটেকশন সম্পর্কে। এছাড়া ব্যাংকগুলোকে হয়তো তাদের অ্যান্টিভাইরাস ব্যবহার করতে হবে।

আগের সাইবার অপরাধ আর বর্তমানের সাইবার ক্রাইমের মধ্যে অনেক পার্থক্য রয়েছে। আগের দিনে ভাইরাস তৈরি করা হতো শখ করে। অথবা মজা করে বন্ধুর পিসির তথ্য মুছে দেয়ার জন্য অপরাধ করা হতো। কিন্তু এখন সাইবার অপরাধ হচ্ছে অর্থনৈতিক ইস্যুতে। আপনার ডাটা নিয়ে অন্যত্র বিক্রি করে দেয়া হচ্ছে।

বাংলাদেশী হ্যাকারদের নিয়ে যদি কাজ করতে হয় তাহলে হ্যাকার কমিউনিটি করার প্রয়োজন আছে বলে আপনি মনে করেন?

না। আমার কাছে মনে হয় হ্যাকার কমিউনিটি নামটিই নেগেটিভ। আমরা তাদেরকে হ্যাকার কমিউনিটি হিসেবে চিহ্নিত করব কেনো? আমরা তাদেরকে ডেভেলপার বলতে পারি। হ্যাকিং কিন্তু একটি ক্রিমিনাল টার্ম। যারা হ্যাকিং করছে তারা অপরাধ করছে। আমরা জানি যে তারা হ্যাক করে। কিন্তু আমাদের দায়িত্ব হবে তাদেরকে পজিটিভলি গ্রহণ করা। দেশে যেহেতু সফটওয়্যার কমিউনিটি রয়েছে তাদেরকেও এই কমিউনিটির সাথে নিয়ে কাজ করতে হবে। হ্যাকারদের ডেভেলপারে রূপান্তর করলে দেশে সাইবার অপরাধ থাকার কথা নয়।

বাংলাদেশের হ্যাকার সংগঠন

বাংলাদেশে মোটামুটি সক্রিয় প্রায় ডজনখানেক হ্যাকার সংগঠন রয়েছে। এগুলোর বেশিরভাগ নিজেদের পরিচয় দেয়ার মতো কোনো ঠিকানা বা ওয়েবসাইট নেই। এগুলো মূলত সোশ্যাল মিডিয়ার সহযোগিতায় নিজেদের মধ্যে আন্তঃসম্পর্ক রক্ষা করে চলে। বাংলাদেশের হ্যাকার সংগঠনের মধ্যে আছে : বাংলাদেশ গ্রে হ্যাট হ্যাকারস; বাংলাদেশ ব্ল্যাক হ্যাট হ্যাকারস; ব াংলাদেশ সাইবার আর্মি; মুসলিম সাইবার শেল; এক্সপেয়ার সাইবার আর্মি; টিম হ্যাকসোসেস; সাইলেন্ট হ্যাকার; সাইবার ৭১; অ্যানোনিমাস বাংলাদেশ; আননৌন গ্ল্যাডিয়েটরস ইন্টারন্যাশনাল; বাংলাদেশী হ্যাকটিভিস্ট।

সাইবার যুদ্ধের ফল

আনুষ্ঠানিকভাবে কোনো দেশের সরকারই তাদের হ্যাক হওয়া ওয়েবসাইটের কোনো তালিকা প্রকাশ না করায় এ সাইবার যুদ্ধের ফল নিশ্চিত করে ▸

আইটি নিরাপত্তায় পর্যাপ্ত বাজেট রাখতে হবে

তপন কান্তি সরকার
প্রেসিডেন্ট, সিটিও ফোরাম বাংলাদেশ

বাংলাদেশে সাইবার অপরাধের সূচনাটা সম্ভবত 'ট্রোজান হর্স' বা 'ই-মেইল স্পাম' অ্যাটাক দিয়ে শুরু হয়েছিল। এরপরে এখন পর্যন্ত বড় ধরনের কোনো ঘটনা ঘটেনি। তথাপিও কিছুদিন আগে 'ফেলানি' নামে যে 'সাইবার যুদ্ধ' হলো, সেটা কিন্তু অ্যালার্মিং। কারণ, আমাদের ছেলেরা কিন্তু একেবারে পিছিয়ে নেই, তা প্রমাণিত হয়েছে এবং তাই আমাদের সতর্ক দৃষ্টি রাখতে হবে।

যদি নেটওয়ার্কের নিরাপত্তা ব্যবস্থা শক্তিশালী হয় এবং 'ফুটপ্রিন্ট' চিহ্নিত করতে পারা যায়, তাহলে খুব সহজে কোনো লিগ্যাল অ্যাকশনে দ্রুত ফল পাওয়া যাবে। তবে মূলত এ ব্যাপারটা পুরোপুরি Proactive Measures-এর ওপর নির্ভর করে। মানে ব্যাংকগুলোকে আগে থেকে সজাগ থাকতে হবে। আইটি নিরাপত্তায় পর্যাপ্ত বাজেট রাখতে হবে। এ ক্ষেত্রে কোনো আপোস করা যাবে না।

আমার জানা মতে, বাংলাদেশে সব ব্যাংক আন্তর্জাতিক মান অনুসরণ করছে। যেমন– আইএসও ২৭০০২ স্ট্যান্ডার্ড ইত্যাদি।

আইটি নিরাপত্তায় পর্যাপ্ত বাজেট রাখতে হবে। নিয়োজিত মানবসম্পদের সঠিক প্রশিক্ষণ নিশ্চিত করতে হবে, নিয়মিত পরিদর্শন ও উন্নয়ন করতে হবে এবং কমপিউটার ব্যবহারকারীদের জন্য 'ইউজার অ্যাওয়্যারনেস' প্রোগ্রাম নিয়মিত করতে হবে।

হ্যাকিং টুল বা হ্যাকিং প্রতিরোধ সম্পর্কে যারা ভালো বুঝে, তাদের কি দেশের জন্য কাজে লাগানো যেতে পারে? যেমনটা ফেসবুক বা গুগলের মতো বড় প্রতিষ্ঠানগুলো করে থাকে? আমি এ ব্যাপারে সম্পূর্ণ একমত। আমাদের দায়িত্ব হবে এসব মেধাবী হ্যাকারকে পরিকল্পিতভাবে কাজে লাগানো।

সিটিও ফোরাম অলাভজনক প্রতিষ্ঠান। তাই নিরাপত্তা দেয়ার কোনো পরিকল্পনা নেই। তবে আমরা এ বিষয়ে বিগত বছরগুলোতে এবং এ বছরেও উল্লেখযোগ্য পরিমাণে সেমিনার আয়োজন করেছি। এসব সেমিনারে দেশী-বিদেশী আইটি সিকিউরিটি এক্সপার্টেরা বক্তব্য রেখেছেন এবং মতামত দিয়েছেন। আমরা সবগুলো সেমিনার থেকে তা সংকলন করার চেষ্টা করেছি, যা খুব শিগগিরই আমরা প্রকাশ করতে পারব। এর মাধ্যমেই অনেকের অনেক কিছুই জানার সুযোগ হবে। সাইবার নিরাপত্তা নিয়ে যারা কাজ করতে চায় তাদেরও এটি কাজে লাগবে।

বলা যায় না। তবে বিভিন্ন সংবাদমাধ্যমে প্রকাশিত খবরের পরিপ্রেক্ষিতে বাংলাদেশী হ্যাক হওয়া ওয়েবসাইটের তুলনায় অধিক সংখ্যক ভারতীয় ওয়েবসাইট হ্যাক হওয়ার তথ্য পাওয়া যায়। গত ১৩ ফেব্রুয়ারি দৈনিক প্রথম আলোয় প্রকাশিত সংবাদে বাংলাদেশীদের হ্যাক করা ভারতীয় ওয়েবসাইটের সংখ্যা বলা হয় প্রায় ১০ হাজার। অপরদিকে ভারতীয় হ্যাকারেরা ৩০০ ওয়েবসাইট হ্যাক করেছে বলে জানায়। তবে এ সংখ্যাটা আনুষ্ঠানিকভাবে কোনো এক পক্ষের জয় ঘোষণার জন্য যথেষ্ট কি না তা বিবেচনাসাপেক্ষ। যেহেতু এ হ্যাকিংয়ের মাধ্যমে মূলত ভারতীয় সীমান্ত হত্যার প্রতিবাদ করা হয়। এই প্রতিবাদ গণমাধ্যমে ফলাও করে প্রকাশ হয় বলে এই উদ্দেশ্য সফল হয় বলে অনুমিত হয়।

বিদেশী গণমাধ্যমে বাংলাদেশ-ভারত সাইবার যুদ্ধ

এই সাইবার যুদ্ধের ক্ষয়ক্ষতি যখন দৃশ্যমান হতে শুরু করে, তখন বিভিন্ন বাংলাদেশী ও ভারতীয় সংবাদমাধ্যমের পাশাপাশি বিদেশী সংবাদমাধ্যমও সংবাদটি গুরুত্বের সাথে ছাপায়। ইয়াহু নিউজ 'Bangladeshis say they hacked 20,000 Indian websites' শিরোনামে হ্যাকারদের বক্তব্য গুরুত্ব সহকারে প্রকাশ করে। দ্য টাইমস অব ইন্ডিয়া শিরোনাম করে 'Bangladesh group hacks BSF website to 'avenge border killings'। এছাড়া এরা এদের অনলাইন সংস্করণে একটি ভিডিও রিপোর্টও প্রকাশ করে। সাপ্তাহিক ট্যাবলয়েড Blitz লিড নিউজ করে শিরোনাম দেয় 'Bangladesh-India Cyber War Continues'। চীনের সাংহাই ডেইলি শিরোনাম করে 'Nearly 20,000 Indian sites get hacked by Bangladesh groups protesting border killings...'। দ্য হ্যাকার নিউজ এই সাইবার যুদ্ধ নিয়ে 'Indian and Bangladeshi Hackers Destroying Cyber Space of Each Other' শিরোনামের লেখায় উল্লেখ করে, 'They Call it 'Cyber war' - But in Actual They Are Destroying Cyber Space of Their Own Country by Defacing Sites for a Matter That Can`t Be Solved by Ministry Like This.'।

সাইবার অপরাধের প্রতিরোধে সরকারি উদ্যোগ

সাইবার অপরাধ প্রতিরোধে সহায়তার জন্য সরকারি উদ্যোগে বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশনের (বিটিআরসি) অধীনে ২৫ জানুয়ারি ২০১২ বিভিন্ন মোবাইল ফোন অপারেটর, ইন্টারনেট সার্ভিস প্রোভাইডার (আইএসপি), পিএসটিএন, ইন্টারন্যাশনাল ইন্টারনেট গেটওয়ে ও সাইবার ক্যাফের প্রতিনিধিদের সমন্বয়ে বাংলাদেশ কমপিউটার সিকিউরিটি ইনসিডেন্ট রেসপন্স টিম (বিডি-সিএসআইআরটি) গঠন করা হয়। বিশেষ দলটির রাষ্ট্র এবং সমাজবিরোধী বিভিন্ন ওয়েবসাইট শনাক্ত করে প্রয়োজনীয় ব্যবস্থা নেয়ার জন্য কাজ করার কথা। এ সংক্রান্ত যেকোনো তথ্য ও পরামর্শ নতুন এই ওয়েবসাইটটির মাধ্যমে পাওয়ার ঘোষণা দেয়া হলেও সাইটে কিছুই নেই। কমপিউটার ও সাইবার অপরাধ বিষয়ে সহায়তা ও পরামর্শের জন্য http ://www.csirt.gov.bd ঠিকানায় যোগাযোগ করতে বলা হয়েছে। অথবা contact@csirt.gov.bd ঠিকানায় মেইল করার কথাও বলা আছে। সব ধরনের সাইবার অপরাধের শিকার যেকোনো ভিকটিমের নিরাপত্তা ও গোপনীয়তা রক্ষা করেই সমস্যা অনুযায়ী এখান থেকে পরামর্শ দেয়া হবে বলে ঘোষণা দেয়া হয়। কিন্তু অভিযোগ রয়েছে এখানে মেইল করলে কখনই উত্তর পাওয়া যায় না, সেখানে ব্যবস্থা নেয়ার তো প্রশ্নই ওঠে না।

বিডি-সিএসআইআরটির কার্যপরিধি

রাষ্ট্রীয়, সমাজ, রাজনৈতিক ও ধর্মীয় বিদ্বেষ ছড়ায় এমন ওয়েবসাইট শনাক্ত করাই এই দলের মূল কাজ। অপরাধীদের চিহ্নিত করে আইন অনুযায়ী ব্যবস্থা নেয়ার সুপারিশ করে দলটি। অভিযোগ প্রমাণিত হলে অপরাধীকে ২ থেকে সর্বোচ্চ ৫ বছরের সাজা এবং ৫ লাখ থেকে সর্বোচ্চ ৫ কোটি টাকা জরিমানা দিতে হতে পারে। টেলিযোগাযোগ নিয়ন্ত্রণ আইনের ৬৯ ধারা অনুযায়ী এ শাস্তি দেয়া হবে। কোনো ওয়েবসাইটে ক্ষতিকর কিছু থাকলে তাৎক্ষণিকভাবে তা বন্ধ নাও করা হতে পারে। এ ক্ষেত্রে অপরাধীদের খুঁজে বের করে আইনের আওতায় নিয়ে আসাই এই টিমের মূল লক্ষ্য। তবে গুরুতর কোনো অপরাধ বা যা দ্রুত সিদ্ধান্ত নেয়া উচিত, সে ক্ষেত্রে এ টিম কমিশনকে জানিয়ে তাৎক্ষণিক ব্যবস্থা নিতে পারবে।

নিরাপত্তাদাতা নিজেই যখন নিরাপদ নয়!

অবাক না হওয়ার উপায় নেই! যিনি নিরাপত্তা দেবেন তিনি নিজেই যদি নিরাপত্তাহীনতায় ভোগেন তাহলে অবস্থা কি হয় তা কি আর বোঝানোর দরকার আছে? বাংলাদেশে সাইবার নিরাপত্তার দায়িত্ব নিয়েছে বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন তথা বিটিআরসি। কিন্তু দুর্ভাগ্যজনক হলেও সত্য, বিটিআরসির ওয়েবসাইট নিজেই নিরাপত্তাহীনতায় রয়েছে। গত ২৫ জানুয়ারি ২০১২ বিভিন্ন মোবাইল ফোন অপারেটর, ইন্টারনেট সার্ভিস প্রোভাইডার (আইএসপি), পিএসটিএন, ইন্টারন্যাশনাল ইন্টারনেট গেটওয়ে ও সাইবার ক্যাফের প্রতিনিধিদের সমন্বয়ে বাংলাদেশ কমপিউটার সিকিউরিটি ইনসিডেন্ট রেসপন্স টিম (বিডি-সিএসআইআরটি) গঠন করা হয়। তাদের একটি নিজস্ব ওয়েবসাইটও রয়েছে। বলা হয়েছে, কমপিউটার ও সাইবার অপরাধ বিষয়ে সহায়তা ও পরামর্শের জন্য http://www.csirt.gov.bd ঠিকানায় যোগাযোগ করুন। তাদের নিজেদেরই তো সাইট নেই! এ ব্যাপারে ▸

ক্যাসপারস্কির বাংলাদেশের প্রধান বিপণন কর্মকর্তা প্রবীর সরকার এই প্রতিবেদককে জানিয়েছেন, দেশে ভালো একটি উদ্যোগ দেখে আমি আগ্রহী হয়ে নিজে তাদের মেইলে ফ্রি অ্যান্টিভাইরাস দেয়ার প্রস্তাব পাঠিয়েছি। কিন্তু তারা কোনো ধরনের সাড়া দেয়নি। মেইলের উত্তরই যদি না পাওয়া যায় তাহলে তাদের কাজ কী? কীভাবে তারা মেইলে সহযোগিতা করছে?

বাংলাদেশে সাইবার অপরাধ প্রতিরোধে আইন

তথ্যপ্রযুক্তি আইন ২০০৬-এর ৫৬ ধারায় বলা হয়েছে,

(১) যদি কোনো ব্যক্তি জনসাধারণের বা কোনো ব্যক্তির ক্ষতি করার উদ্দেশ্যে বা ক্ষতি হবে এটি জানা সত্ত্বেও এমন কোনো কাজ করেন, যার ফলে কোনো কমপিউটার রিসোর্সের কোনো তথ্যবিনাশ, বাতিল বা পরিবর্তিত হয় বা তার মূল্য বা উপযোগিতা কমে যায় বা অন্য কোনোভাবে একে ক্ষতিগ্রস্ত করে।

(২) এমন কোনো কমপিউটার সার্ভার, কমপিউটার নেটওয়ার্ক বা অন্য কোনো ইলেকট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ করার মাধ্যমে এর ক্ষতিসাধন করেন যাতে তিনি মালিক বা দখলদার নন, তাহলে তার এই কাজ হবে একটি হ্যাকিং অপরাধ। কোনো ব্যক্তি হ্যাকিং অপরাধ করলে তিনি অনূর্ধ্ব ১০ বছর কারাদণ্ডে দণ্ডিত হবেন। এক কোটি টাকা অর্থদণ্ডে দণ্ডিত হতে পারেন বা উভয় দণ্ড দেয়া যেতে পারে।

তথ্যপ্রযুক্তি আইন ২০০৬-এর ৫৭ ধারায় বলা হয়েছে, যদি কোনো ব্যক্তি ইচ্ছে করে ওয়েবসাইটে বা অন্য কোনো ইলেকট্রনিক বিন্যাসে এমন কিছু প্রকাশ বা সম্প্রচার করেন, যা মিথ্যা ও অশ্লীল বা সংশ্লিষ্ট অবস্থা বিবেচনায় কেউ পড়লে বা শুনলে নীতিভ্রষ্ট বা অসৎ হতে উদ্বুদ্ধ হতে পারে বা যার মাধ্যমে মানহানি ঘটে, আইনশৃঙ্খলার অবনতি ঘটে বা ঘটার সম্ভাবনা সৃষ্টি হয়, রাষ্ট্র বা ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয় বা ধর্মীয় অনুভূতিতে আঘাত করে বা করতে পারে বা এ ধরনের তথ্যাদির মাধ্যমে কোনো ব্যক্তি বা সংগঠনের বিরুদ্ধে উস্কানি দেয়া হয়, তাহলে তার এই কাজ অপরাধ বলে গণ্য হবে। কোনো ব্যক্তি এ ধরনের অপরাধ করলে তিনি অনধিক ১০ বছর কারাদণ্ডে দণ্ডিত হতে পারেন এবং অনধিক এক কোটি টাকা অর্থদণ্ডে দণ্ডিত হতে পারেন।

তথ্যপ্রযুক্তি আইন ২০০৬-এর ৬৮ ধারায় বলা হয়েছে, সরকার সরকারি গেজেটে প্রজ্ঞাপন দিয়ে এই আইনের অধীন সংঘটিত অপরাধের দ্রুত ও কার্যকর বিচারের উদ্দেশ্যে এক বা একাধিক সাইবার ট্রাইব্যুনাল গঠন করতে পারবে। গঠিত সাইবার ট্রাইব্যুনালে সুপ্রিম কোর্টের সাথে পরামর্শ করে সরকার একজন দায়রা জজ বা একজন অতিরিক্ত দায়রা জজকে মামলা পরিচালনার দায়িত্ব দেবে। অনুরূপভাবে নিযুক্ত একজন বিচারক নিয়ে এই ট্রাইব্যুনাল 'সাইবার ট্রাইব্যুনাল' নামে অভিহিত হবে। এই ধারার অধীন গঠিত সাইবার ট্রাইব্যুনালকে পুরো বাংলাদেশের স্থানীয় অধিক্ষেত্র অথবা এক বা একাধিক দায়রা অধিক্ষেত্র প্রদান করা যেতে পারে। ট্রাইব্যুনাল তথ্যপ্রযুক্তি আইন ২০০৬-এর আইনের অধীন অপরাধের বিচার করবেন।

৭৪ ধারায় বলা হয়েছে, ফৌজদারি কার্যবিধিতে যা কিছুই থাকুক না কেন, এ উদ্দেশ্যে বিশেষ ট্রাইব্যুনাল গঠন না হওয়া পর্যন্ত এই আইনের অধীন অপরাধ দায়রা আদালত কর্তৃক বিচার্য হবে। সরকার সরকারি গেজেট, প্রজ্ঞাপন দিয়ে এক বা একাধিক সাইবার আপিল ট্রাইব্যুনাল গঠন করতে পারে। সাইবার আপিল ট্রাইব্যুনাল অধীন সাইবার ট্রাইব্যুনাল বা দায়রা আদালত কর্তৃক ঘোষিত রায় বা আদেশের বিরুদ্ধে আপিল শুনবে ও নিষ্পত্তি করবে।

তথ্য ও যোগাযোগ প্রযুক্তি (সংশোধন) আইন-২০০৯-এর ৮ম অধ্যায়ে (ধারা ৫৪ থেকে ৮৪) কমপিউটার সম্পর্কিত অপরাধ, তদন্ত, বিচার ও দণ্ড ইত্যাদি বিষয়ে বিশদ নির্দেশনা দেয়া হয়েছে। এই আইনের ৭৬ নং ধারা অনুসারে অপরাধ তদন্তের ক্ষমতা– ▸

সাইবার ক্রাইম গোয়েন্দাবৃত্তির আধুনিক সংস্করণ

ড. মোহাম্মদ ইউনুছ আলী
সহযোগী অধ্যাপক, সিএসই, বুয়েট

সাইবার ক্রাইম এক ধরনের ক্রাইম। তাই আমি এর বিপক্ষে। সাইবার ক্রাইম হচ্ছে আগের দিনের গোয়েন্দাবৃত্তির আধুনিক সংস্করণ। আগে সাইবার ক্রাইম মানুষ একভাবে করলেও এখন তা তিনভাবে সংঘটিত হচ্ছে। প্রথমটি অর্থনৈতিকভাবে লাভবান হওয়ার জন্য কোনো মূল্যবান জিনিসকে টার্গেট করে চুরি করা; যেমন ব্যাংক বা ক্রেডিট কার্ড থেকে চুরি করা। দ্বিতীয়টি দেশভিত্তিক সাইবার যুদ্ধ; যেমন কিছুদিন আগে ভারত-বাংলাদেশে হয়েছে এবং তৃতীয়টি জাতীয় সাইবার যুদ্ধ; যেমন চীন হয়তো আমেরিকাতে করেছে। এ তিনটিই খারাপ। আপনাকে না জানিয়ে কোনো কিছু চুরি করা মানেই অপরাধ। তাই এটা সম্পূর্ণভাবেই অবৈধ।

আমরা দেখেছি ১৫ থেকে ২৬ বছর বয়সীরাই সাইবার ক্রাইমের সাথে বেশি জড়িত। তরুণ বয়সে এরা চ্যালেঞ্জ নিতে ভালোবাসে বলে এখানে তাদের পদচারণা বেশি। আর যারা ম্যাথ বা কমপিউটার ব্যাকগ্রাউন্ডের ছাত্র, তারাই হ্যাকিং জগতে বেশি আসছে। সাধারণত এসব হ্যাকার শখের বসে হ্যাক করা শুরু করলেও শেষ পর্যন্ত অনেকেই সিরিয়াস ক্রাইমের সাথে সম্পৃক্ত হয়ে যাচ্ছে।

হ্যাকাররা সব সময়ই কমপিউটারের ওপর বেশি জ্ঞান রাখার চেষ্টা করে। কমপিউটারের এ জ্ঞানকে যারা কাজে লাগায় তাদেরকে দুইভাগে ভাগ করা যায়। এক. যারা ভালো উদ্দেশ্যে এ জ্ঞান ব্যবহার করে তাদেরকে আমরা অ্যানালিস্ট বলি। দুই. যারা এ জ্ঞানকে খারাপ উদ্দেশ্যে ব্যবহার করে তাদেরকে আমরা হ্যাকার বলি। ডেভেলপাররা একটি সিস্টেম ডিজাইন করার পর এর বিভিন্ন ধরনের ম্যাথমেটিক্যাল টেকনিক চালিয়ে দেখেন যে এটা হ্যাক করা যায় কি না। আর হ্যাকারেরা এ টেকনিকগুলোই কাজে লাগিয়ে অনেক কঠিন সিস্টেমকেও ব্রেক করার কাজে ব্যবহার করে। ফলে তাদের পক্ষে হ্যাক করা সহজ হয়ে যায়।

সাইবার ক্রাইমের সবই মন্দ। সাইবার ক্রাইমের মাধ্যমে প্রচুর অর্থনৈতিক ক্ষতিসাধিত হয়। চুরি-ডাকাতি যেমন অন্যায়, সাইবার ক্রাইমও একই ধরনের অন্যায়। ইন্টারনেট থেকে কেউ যদি পাসওয়ার্ড চুরি করে কিছু দেখে বা হ্যাক করে তা সম্পূর্ণভাবে নৈতিকতার দিক থেকেও অন্যায়। এছাড়া কেউ যদি দেশের জাতীয় কোনো ডাটা ফাঁস করে দেয়, তার মাধ্যমে দেশ বিপদে পড়তে পারে। কোনো ব্যবসায়িক প্রতিষ্ঠানের তথ্য ফাঁস হলেও প্রতিপক্ষ থেকে তারা বিপদে পড়তে পারে। নারীদের গোপন কোনো ছবি বা ভিডিও প্রকাশ করে দিলে সে সামাজিকভাবে বয়কট হতে পারে। সাধারণ ক্রাইম আর সাইবার ক্রাইমের মধ্যে কোনো তফাৎ নেই।

সাইবার ক্রাইম থেকে উত্তরণের অনেক উপায় রয়েছে। প্রথমত আমরা যখন কোনো সিস্টেম ডেভেলপ করি, তখন তার নিরাপত্তা টেস্ট করতে হবে। এটা করা আমাদের প্রথম কাজ। কিন্তু আমরা তা করি না। এটা করতে পারলে হ্যাকিং অনেকাংশেই কমে যাবে। আবার আমরা প্রায় সময় কোনো সিস্টেম রান করার পরই সরাসরি তা চালু করে দেই। যার ফলে হ্যাকিং হচ্ছে। তা ছাড়া আমাদের সার্ভারগুলো ছড়িয়ে ছিটিয়ে না রেখে এগুলোকে একটি নির্দিষ্ট জায়গা থেকে নিয়ন্ত্রণ করা উচিত। এরপর তা উচ্চমানের প্রযুক্তি ব্যবহার করে নিরাপত্তা দিলে হ্যাকিং হওয়ার সম্ভাবনা কমে যাবে। এরপর ব্যবহারকারীদের ট্রেনিং দেয়া উচিত। কি করা উচিত আর কি করা অনুচিত, তা তাদের বুঝিয়ে দিলে তারা সচেতন হবে। সে ক্ষেত্রেও হ্যাকিং কমে যাবে। ডাটাবেজে অ্যাক্সেস কন্ট্রোল করতে হবে। কাকে কী পরিমাণ অ্যাক্সেস দেয়া হবে, তা সিস্টেম ডেভেলপারকে সময় নির্ধারণ করে দিতে হবে। আমরা সবাইকে অ্যাক্সেস দেই বলে হ্যাকিং হওয়ার সম্ভাবনা বেড়ে যায়। এসব সিকিউরিটি নিশ্চিত করতে পারলে সাইবার হ্যাকিং ৯০ শতাংশ কমে যাবে।

বিদেশী হ্যাকার আক্রান্ত বাংলাদেশী সাইট রিস্টোর করাই সাফল্য

রটাটিং রটার
প্রতিষ্ঠাতা এডমিন, বাংলাদেশ গ্রে হ্যাট হ্যাকারস

সাধারণত হ্যাকারদের কার্যক্রমের ধরন ৩টি ভাগে ভাগ করা হয় : ০১. হোয়াইট হ্যাট হ্যাকার; ০২. ব্ল্যাক হ্যাট হ্যাকার; ০৩. গ্রে হ্যাট হ্যাকার।

হোয়াট হ্যাট হ্যাকার সাধারণত পেনিস্ট্রেশন টেস্টার হয়ে থাকে। এরা হ্যাক করে না। ব্ল্যাক হ্যাট হ্যাকার সাধারণত ক্ষতি অথবা ধ্বংসের উদ্দেশ্যেই হ্যাক করে থাকে। গ্রে হ্যাট হ্যাকার হলো হোয়াট ও ব্ল্যাক হ্যাটের সংমিশ্রণ। এরা ক্ষতির উদ্দেশ্যে হ্যাকও করতে পারে আবার সাইটের দুর্বলতা ধরিয়ে দেয়ার মাধ্যমে উপকারও করতে পারে। আমাদের সংগঠনের নামের সার্থকতা হলো, আমরা শুধু বাইরের দেশের সাইট হ্যাক করি এবং বাংলাদেশের কোনো সাইট হ্যাক হলে তা নিজ দায়িত্বে ঠিক করে দিই এবং কেউ যদি সাহায্য চায় তাকে সাহায্য করা হয়। এটা শুধু বাংলাদেশ গ্রে হ্যাট হ্যাকারসের নয়, সারা পৃথিবীর সব গ্রে হ্যাট হ্যাকারদের মূলমন্ত্র।

আমাদের কার্যক্রম সুশৃঙ্খল চেন অব কমান্ডে পরিচালিত হয়। যেখানে প্রতিটি সদস্য সুন্দরভাবে তাদের নিজ নিজ কাজ সম্পন্ন করে।

বিভিন্ন স্কোয়াডে ভাগ করা আছে আমাদের ক্রুরা। প্রতি ঘণ্টায় কমপক্ষে চার জন অনলাইনে থাকে। এমনকি যে সময় বাংলাদেশে সবাই ঘুমিয়ে যায় সে সময় আমাদের প্রবাসী ভাই, যারা আমাদের ক্রু হিসেবে আছে, তারা অনলাইনে থাকে। যেন কোনো বাংলাদেশী সাইট হ্যাকের খবর পেলেই ঠিক করে দিতে পারে। মিরর জোনগুলোতে পৃথিবীর কোন ওয়েবসাইটকে হ্যাক করল তা সেকেন্ডের মধ্যেই দেয়া হয়। আমরা সেখান থেকেই খবর পাই আমাদের দেশের কোন কোন সাইট কারা হ্যাক করেছে। এক হিসেবে বলতে পারেন, ২৪ ঘণ্টার মধ্যে ১ মিনিটের জন্যও থেমে থাকে না আমাদের কার্যক্রম।

আমাদের সংগঠনের সাথে কেউ কাজ করতে চাইলে তাদের জন্য প্রধান শর্ত গ্রুপের চেন অব কমান্ড মেনে চলতে হবে এবং গ্রুপের প্রতিটি নিয়ম যেকোনো অবস্থাতে মেনে চলতে হবে।

সাইবার যুদ্ধগুলোতে আমাদের বিজয়ই হলো আমাদের স্মরণীয় দিন এবং যখন আমরা দেশী সাইট রিস্টোর করি, সেই দিনই আমাদের কাছে সবচেয়ে স্মরণীয় দিন হয়ে থাকে।

এ পর্যন্ত আমাদের হ্যাকড সাইটের তালিকায় ২৫ হাজার সাইটের নাম আছে। তবে আমরা শুধু সাইটের সংখ্যাকেই বড় মনে করি না, ভালোমানের সাইট হ্যাক করাই ভালো হ্যাকারের লক্ষণ। আমাদের সিস্টেম অ্যাডমিন আবলাজ ইভার হলো বাংলাদেশী হ্যাকিং গ্রুপগুলোর মধ্যে সবচেয়ে ভয়ঙ্কর হ্যাকার। এমন কোনো কঠিন সাইট নেই যা সে হ্যাক করেনি। আর তাছাড়া আরেক সিস্টেম অ্যাডমিন মেহেরাব ফেরদৌসের গুগল মালাওয়ি হ্যাকের কৃতিত্ব আছে। আর গোলাম কিবরিয়া তো নিজের ছবি দিয়েই হ্যাক করে। আসল কথা হলো আমরা একটি পরিবার।

গত বছর আমরা সুইস ব্যাংক হ্যাক করি। তাদের সদস্যদের যত অ্যাকাউন্ট ইনফো, জমা টাকার পরিমাণ সবকিছু সারা পৃথিবীর সামনে উন্মুক্ত করে দিই, যা পৃথিবীর সব মিডিয়াতে গুরুত্বের সাথে প্রকাশিত হয়। এই রেকর্ড আজ পর্যন্ত পৃথিবীর কোনো হ্যাকার ভাঙতে পারেনি।

(১) ফৌজদারি কার্যবিধিতে যা কিছুই থাকুক না কেন, নিয়ন্ত্রক বা নিয়ন্ত্রক হতে এ উদ্দেশ্যে ক্ষমতাপ্রাপ্ত কোন কর্মকর্তা বা সাব-ইন্সপেক্টরের পদমর্যাদার নয় এমন কোনো পুলিশ কর্মকর্তা এই আইনের অধীন কোনো অপরাধ তদন্ত করবেন।

(২) এই আইনের অধীন অপরাধসমূহ অ-আমলযোগ্য (non-cognizable) হবে। এ আইনের সঠিক উপস্থাপন ও আইনের বিষয়ে জনসচেতনতা সৃষ্টি করা অপরিহার্য। যা সাইবার অপরাধ নিয়ন্ত্রণে উল্লেখযোগ্য ভূমিকা পালন করতে পারে। প্রসঙ্গত, ২০০১ সালে টেলিকমিউনিকেশন আইন পাস করা হলেও সাইবার অপরাধ সমস্যা সমাধানের ক্ষেত্রে এই আইনের তেমন কোনো প্রয়োগ লক্ষ করা যাচ্ছে না। ২০০৬ সালে সাইবার অপরাধ নিয়ন্ত্রণের জন্য একটি বিলের খসড়া মন্ত্রিসভায় অনুমোদন পেলেও আজও তা সংসদে উত্থাপিত হয়নি।

দেশে সাইবার অপরাধ প্রতিরোধে নেই আলাদা ইউনিট

বেশ কিছুদিন আগে ঢাকা মেট্রোপলিটন পুলিশ বা ডিএমপির গোয়েন্দা বিভাগে একটি সাইবার অপরাধ ইউনিট চালু করার সিদ্ধান্ত নেয়া হলেও এই ইউনিট চালানোর জন্য প্রয়োজনীয় মানবসম্পদ ও কারিগরি সহায়তা বাংলাদেশে নেই বলে জানা গেছে। বিচ্ছিন্নভাবে কিছু কর্মকর্তাকে বিদেশ থেকে প্রশিক্ষণ দিয়ে নিয়ে আসা হয়েছিল। কিন্তু শুধু বিদেশে যাওয়ার মতো অভিজ্ঞতা অর্জনের বাইরে এরা তেমন কোনো প্রযুক্তিগত দক্ষতা অর্জন করতে পারেনি বলেও জানা গেছে। তবে বিশেষজ্ঞেরা মনে করছেন, জরুরি ভিত্তিতে বাংলাদেশে একটি আলাদা সাইবার অপরাধ ইউনিট গঠন দরকার। সাইবার অপরাধ বাংলাদেশে এই মুহূর্তে একটি বড় আইনগত সমস্যা না হলেও বাংলাদেশ যে গতিতে তথ্যপ্রযুক্তির সুপার হাইওয়েতে বিচরণ শুরু করেছে, তাতে অচিরেই এটি একটি বড় সমস্যা হিসেবে আবির্ভূত হবে। যেহেতু সাইবার অপরাধের কোনো সীমারেখা নেই, তাই বহির্বিশ্ব থেকে এদেশে এবং এদেশ থেকে বহির্বিশ্বের অন্য দেশেও এ ধরনের অপরাধ সম্পন্ন হতে পারে। তাই বিষয়টি ভাবতে হবে বাস্তবতার আলোকে সময়ের নিরিখে।

বাংলাদেশে সাইবার আইনে সমস্যা ও সমাধান

ইংল্যান্ড বিশ্বে প্রথম সাইবার আইন প্রণেতা হিসেবে তৈরি করে কমপিউটার মিসইউজ অ্যাক্ট ১৯৯০। ই-অপরাধ প্রতিরোধে ২০০৮ সালে জাতীয় ই-অপরাধ ইউনিটও গঠন করা হয়। ভারতে তৈরি হয় তথ্যপ্রযুক্তি আইন ২০০০। বাংলাদেশে সাইবার আইন প্রণয়নে মিশ্র আলোচনা জারি থাকলেও একটা তথ্য অনেকের কাছেই অস্পষ্ট রয়ে গেছে। বাংলাদেশে ২০০৬ সালে তথ্যপ্রযুক্তি ও যোগাযোগ আইন তৈরি করা হয় এবং ২০০৯ সালে এই আইনে কিছু পরিমার্জন করা হয়। ধরে নেয়া যাক, এ তথ্যপ্রযুক্তি আইনই আমাদের সাইবার নিরাপত্তা নিশ্চিত করতে প্রয়োগ হবে। সমস্যা হলো, আমাদের দেশে আইন থাকলেও আইনি অব্যবস্থাপনা নিয়ে জনসাধারণের ক্ষোভ হরহামেশাই দেখা গেছে। নাগরিকদের সামাজিক নিরাপত্তা ও অধিকারই যেখানে নিশ্চিত নয়, সেখানে ইন্টারনেটে ব্যক্তি নিরাপত্তা দাবি করা বাতুলতাই। তদুপরি, রাষ্ট্রীয় প্রচারণার অভাবে নাগরিকদের আইনি অধিকার দিতে কোন আইনে কী প্রতিকার লাভ সম্ভব, তা নাগরিকদের কাছে অজানাই থেকে যায়। অবশ্য ঘোষিত তথ্যপ্রযুক্তি আইন সাইবার অপরাধ শনাক্তকরণ ও বিচারকাজ পরিচালনায় কতটা যুগোপযোগী তা প্রশ্নসাপেক্ষ। তাছাড়া প্রযুক্তি প্রতিনিয়ত উন্নত হচ্ছে, তাতে অপরাধের ধরনও পাল্টে যাচ্ছে। এজন্য সাইবার আইন বিষয়ে গবেষণার দাবি রাখে। সাইবার আইন শুধু রাষ্ট্রের অভ্যন্তরীণ প্রযুক্তি অবকাঠামোতে সংঘটিত সাইবার অপরাধের জন্য প্রযোজ্য হবে তা নয়। একজন বাংলাদেশী ইন্টারনেট ব্যবহার করে প্রবাস থেকেও বাংলাদেশে অপরাধমূলক কাজ পরিচালনা করতে পারেন। তাই সাইবার অপরাধীকে শনাক্তকরণে প্রয়োজনীয় সাইবার তথ্য বিনিময়ে ও সর্বোপরি অপরাধীকে আইনের আওতায় আনতে দুটি দেশের মধ্যে বিশেষ সাইবার নীতিমালা থাকতে হবে। সাইবার অপরাধ মনিটরিং ও অভিযোগ দায়ের করার জন্য জাতীয় সাইবার সেল গঠন করা জরুরি। এ সেলের প্রযুক্তিগত সুবিধা উন্নততর হতে হবে যেনো কোনো অভিযোগের প্রেক্ষিতে অভিযুক্তের ইন্টারনেট গতিবিধি ট্র্যাকিং, ট্রেসিং করে অকাট্য তথ্য দ্রুততার সাথে আদালতে পেশ করা সম্ভব হয় কজ

ফিডব্যাক : mmrsohelbd@gmail.com