সাইবার ক্রাইম ঠেকাবেন যেভাবে

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

দেশে অনলাইন ব্যবহারকারীর সংখ্যা যেমন বাড়ছে, তেমনি জ্যামিতিক হারে বাড়ছে সাইবার অপরাধ। তাই এই সাইবার অপরাধ প্রতিরোধ ও দমন একটি চ্যালেঞ্জ হয়ে দাঁড়িয়েছে। কোনো থানার অধীনস্থ এলাকায় যদি খুনের মতো অপরাধ সংঘটিত হয়, তাহলে পুলিশ প্রয়োজনীয় ব্যবস্থা নেয় অপরাধের আলামত সংগ্রহের। তেমনি সাইবার অপরাধের ক্ষেত্রেও কিছু অত্যাবশ্যক ব্যবস্থা নিতে হয়। সেসব ব্যাপারে আমাদের আইনশৃঙ্খলা রক্ষাকারী বাহিনী এখনও শতভাগ সক্ষম ও সচেতন নয়। উন্নত বিশ্ব সাইবার অপরাধ নিয়ে যথেষ্ট সতর্ক ও সচেতন। এ ব্যাপারে আমাদের কিছুটা ঘাটতি রয়েছে। সম্প্রতি দেশে যেসব সাইবার অপরাধ সংঘটিত হয়েছে, তার ভেতরে প্রধান হচ্ছে ব্যক্তিগত হয়রানি। কারও সম্পর্কে মানহানিকর বা আপত্তিকর কথা ও ছবি পোস্ট করা। সামাজিক মাধ্যমের ব্যাপক প্রসারের ফলে এই অপরাধের মাত্রা অনেক বেড়েছে। বিশেষ করে নারী সংক্রান্ত বিষয়ে সাইবার অপরাধের মাত্রা বেশি। অনেকে ক্ষতিগ্রস্ত হওয়ার পর আইনশৃঙ্খলা রক্ষাকারী বাহিনীর কাছে যাচ্ছে। অনেকে লজ্জা বা সঙ্কোচের জন্য সেটাও করছে না।

বাস্তবতা হলো ইন্টারনেট খুলে দিয়েছে সব বন্ধ দরজা। এখন বিশ্ব চলে এসেছে হাতের মুঠোয়। তথ্যপ্রযুক্তির মাধ্যমেই দেশে উন্নয়ন ঘটবে। বাংলাদেশের আউটসোর্সিং কর্মীদের দক্ষতা অন্য যেকোনো দেশের সাথে তুলনা করা যায়। গত বছর ইন্টারনেট ব্যবহারের দিক থেকে বাংলাদেশ বিশ্বে ৫৪তম অবস্থানে ছিল। দেশে আউটসোর্সিংয়ে ব্যাপকভাবে তরুণেরা এগিয়ে আসার পেছনে বড় কারণ বর্তমান সরকার তথ্যপ্রযুক্তিবান্ধব বলে। আউটসোর্সিংয়ে পাঁচ বছরে কর্মসংস্থানের টার্গেট দুই লাখ করার পদক্ষেপ গ্রহণে প্রমাণিত হয়েছে বিপুলসংখ্যক চাকরিপ্রত্যাশী উচ্চশিক্ষিত তরুণ-তরুণী। তবে বাংলাদেশের শতকরা ৭০ ভাগ মানুষ গ্রামে বাস করে। তাদের ইন্টারনেট সুবিধা দেয়ার জন্য সরকার কাজ করছে। সাড়ে চার হাজারের বেশি ইউনিয়নে তথ্যকেন্দ্র খোলা হয়েছে। বেশ কিছু এলাকায় ওয়াইফাই চালু করা হয়েছে। বর্তমান সরকার গোটা দেশকে শতভাগ নেটওয়ার্কের আওতায় আনার জন্য কাজ করে যাচ্ছে। ৬৪টি জেলা ও ১৯৭টি উপজেলা ফাইবার অপটিক্যাল নেটওয়ার্কের আওতায় রয়েছে। পর্যায়ক্রমে সব উপজেলাকে এর আওতায় আনা হবে। দেশের তরুণেরা বর্তমানে এই সেক্টর থেকে প্রতিবছর ২০ কোটি মার্কিন ডলার আয় করছেন।

এমন পরিস্থিতিতে সাইবার নিরাপত্তা নিশ্চিত করতে এ সংক্রান্ত অপরাধ দমনে সর্বোচ্চ ১৪ বছরের শাস্তির বিধান রেখে 'ডিজিটাল নিরাপত্তা আইন' করার সিদ্ধান্ত নিয়েছে সরকার। আইনটির অধীনে 'সাইবার ইমার্জেন্সি রেসপন্স টিম' গঠন করা হচ্ছে। এ ছাড়া অপরাধের ধরন অনুযায়ী সর্বনিম্ন শাস্তিও নির্ধারণ করে দেয়া হবে। রাষ্ট্রীয় পর্যায়ে সাইবার নিরাপত্তা যেমন গুরুত্বপূর্ণ, তেমনি ব্যক্তিগত পর্যায়ে সচেতনতা বাড়নোও খুবই গুরুত্বপূর্ণ। যদি প্রত্যেকে এ ব্যাপারে সচেতন হয়, তবে অনেক ক্ষেত্রেই অনেক ধরনের সাইবার অপরাধ এড়ানো সম্ভব। বিশেষ করে নারীদের প্রতি অনলাইন অপরাধের বেশিরভাগই সাইবার নিরাপত্তা সম্পর্কে তাদের অজ্ঞতার কারণে ঘটে থাকে। সরকারও ইদানিং এর গুরুত্ব অনুধাবন করে সারাদেশে ১০ হাজার মেয়েদের স্কুলে সাইবার নিরাপত্তা সম্পর্কে সচেতনতামূলক প্রশিক্ষণ দিয়েছে। এখানে ব্যক্তিগত পর্যায়ে সাইবার নিরপত্তায় করণীয় সম্পর্কে আলোচনা করা হলো।

ব্যক্তিগত তথ্যের নিরাপত্তায় সতর্কতা

প্রয়োজনে হোক আর অপ্রয়োজনে, প্রতিদিন আমরা ই-মেইল, সামাজিক যোগাযোগমাধ্যম ও নানা ওয়েবসাইট ব্যবহার করছি। তবে তথ্য বিনিময়ের এ মাধ্যমগুলো ব্যবহারে সামান্য অসাবধানতায় আপনার ব্যক্তিগত তথ্য সাইবার অপরাধীদের কাছে পাচার হয়ে যেতে পারে। সাধারণত তরুণেরা এ ধরনের ঝুঁকিতে বেশি থাকে। নতুন ইন্টারনেট ব্যবহারকারীদের ক্ষেত্রেও একই কথা প্রযোজ্য। ব্যক্তিগত তথ্য সুরক্ষায় মুঠোফোন বা ট্যাবের পর্যাপ্ত নিরাপত্তা নিশ্চিত তো করবেনই, এই ছয়টি কাজ থেকেও বিরত থাকবেন–

০১. বিনামূল্যের ওয়াইফাই ব্যবহার

সর্বসাধারণের জন্য বিনামূল্যে ব্যবহারের ওয়াইফাই সাধারণত নিরাপদ হয় না। হ্যাকার চাইলে এই নেটওয়ার্কে ডাটা বিনিময়ের সময় আপনার তথ্য হাতিয়ে নিতে পারে । ধরুন, কোনো পাবলিক ওয়াইফাই ব্যবহার করে ব্রাউজ করা কোনো ওয়েবসাইটে দেয়া ই-মেইল, পাসওয়ার্ড কিংবা অন্য কোনো তথ্যে প্রবেশ করলেন। একই নেটওয়ার্ক ব্যবহার করছে এমন তৃতীয় কোনো ব্যবহারকারীর কাছে ডাটা চলে যেতে পারে। এ জন্য খুব প্রয়োজন না হলে উন্মুক্ত ওয়াইফাই ব্যবহার করা থেকে বিরত থাকুন এবং ব্যবহারের আগে নিশ্চিত হয়ে নিন নেটওয়ার্কটি নিরাপদ কি না।

০২. ই-মেইলে অতি ব্যক্তিগত তথ্য প্রদান করা

যোগাযোগের মাধ্যমগুলোর মধ্যে এখনও ই-মেইল জনপ্রিয়তার শীর্ষে। ই-মেইল পাঠানোর আগে নিশ্চিত হয়ে নিন ঠিকানা ঠিক আছে কি না। ব্যক্তিগত তথ্য পাঠানো কিংবা সংযুক্তি যোগ করার আগে তাই সচেতনতা অবলম্বন করা উচিত।

০৩. সামাজিক যোগাযোগ মাধ্যমগুলোর অবাধ ব্যবহার

সামাজিক যোগাযোগ মাধ্যমগুলোতে আপনি আপনার জীবনের অনেক গুরুত্বপূর্ণ মুহূর্ত ভাগাভাগি করে থাকেন। আপনার গোপনীয়তা রক্ষার সেটিংস ও নেটওয়ার্কের নিরাপত্তা জোরদার হওয়ার পরও আপনার শেয়ার করা ব্যক্তিগত তথ্য অন্য কারও হাতে চলে যেতে পারে। ফলে সাইবার অপরাধীরা আপনার অনাকাঙ্ক্ষিত তথ্য অনলাইনে ছড়িয়ে দিতে পারে, যা আপনার ভার্চুয়াল পরিচিতি কিংবা ব্যক্তিগত জীবন বিপদের মুখে ফেলে দেবে।

০৪. না বুঝে অনলাইন ফরম পূরণ করা

আজকাল অনেক ওয়েবসাইটে প্রবেশ করতে হলে কিছু ব্যক্তিগত তথ্যে প্রবেশ করতে হয়। বেশিরভাগ তথ্য ওয়েবসাইটে ব্যবহারের প্রয়োজন হলেও তথ্য দেয়ার ব্যাপারে সাবধানতা অবলম্বন করাই ভালো। ওয়েবসাইটে তথ্য দেয়ার আগে তাদের গোপনীয়তার নীতি পড়ে নিশ্চিত হয়ে নিন আপনার দেয়া তথ্যগুলো কী কী কাজে ব্যবহার করা হবে।

০৫. দুর্বল ও সহজ পাসওয়ার্ড ব্যবহার করা

জটিল পাসওয়ার্ড মনে রাখা কিছুটা কঠিন বলে অনেকেই সহজে অনুমান করা যায় এমন পাসওয়ার্ড ব্যবহার করেন। এতে আপনার তথ্য ঝুঁকির মধ্যে পড়ে। তাই বড় ও ছোট হাতের অক্ষর, সংখ্যা ও চিহ্নের সমন্বয়ে তৈরি পাসওয়ার্ড ব্যবহার করুন। প্রতিটি ওয়েবসাইটের জন্য ভিন্ন পাসওয়ার্ড ব্যবহার করুন। সম্ভব হলে কিছুদিন পরপর পুরনো পাসওয়ার্ড বদলে ফেলুন।

০৬. স্মার্ট ওয়াচ

হাতে স্টাইলিশ স্মার্ট ওয়াচ। দর্শনে 'হিরো হিরো' ফিল হলেও আপনার ব্যক্তিগত তথ্যের নিরাপত্তার ক্ষেত্রে তা একেবারেই জিরো। স্মার্ট ওয়াচ থেকে আপনার ব্যবহৃত তথ্য খুব সহজেই হ্যাক করতে পারে হ্যাকারেরা, এমনটাই দাবি করা হয়েছে একটি গবেষণায়। ওই গবেষণায় দাবি করা হয়েছে, স্মার্ট ওয়াচের মোশন সেন্সর দিয়ে একজন হ্যাকার খুব সহজেই স্মার্ট ওয়াচ ব্যবহারকারীর তথ্য ব্যবহার করতে পারবে।

গবেষণায় দেখা গেছে, একটি রেগুলার কিবোর্ড (ল্যাপটপ অথবা ডেস্কটপ) থেকে খুব সহজেই স্মার্ট ওয়াচে ব্যবহৃত তথ্যাদির যাবতীয় নথি পাওয়া সম্ভব। অ্যাক্সিলোমিটার ও গ্যারিস্কোপ সিগন্যাল হাতে থাকা স্মার্ট ওয়াচের মাইক্রো মোশনগুলোকে অ্যাক্সেস করতে পারে এবং সেগুলো থেকে ইংরেজি হরফে সব নথি একজন হ্যাকারের কাছে পৌঁছে যায়। তাই স্মার্ট ওয়াচ ব্যবহারে সতর্ক থাকতে হবে কজ

ফিডব্যাক : jabedmorshed@yahoo.com