কেন প্রয়োজন ব্যাংকের সিকিউরিটি সার্টিফিকেশন

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

দেশের ৫২ শতাংশ ব্যাংক বর্তমানে তথ্য নিরাপত্তার উচ্চ ঝুঁকির মধ্যে রয়েছে। এর অর্থ দাঁড়ায়, সাইবার হামলার মতো অতর্কিত হামলার মাধ্যমে ব্যাংকের গুরুত্বপূর্ণ তথ্য যদি কেউ চুরি করার চেষ্টা করে, তবে তা ঠেকানোর সক্ষমতা নেই অর্ধেকের বেশি ব্যাংকের। এই গভীর উদ্বেগজনক তথ্য উঠে এসেছে বাংলাদেশ ইনস্টিটিউট অব ব্যাংক ম্যানেজমেন্টের (বিআইবিএম) এক গবেষণায়। গবেষণায় গত তিন বছরের অবস্থা তুলে ধরা হয়েছে। ২০১৫ সালে তথ্য নিরাপত্তা ঝুঁকিতে থাকা ব্যাংকের সংখ্যা ৫২ শতাংশ। এর মধ্যে অতি উচ্চ ঝুঁকিতে ১৬ শতাংশ, উচ্চ ঝুঁকিতে ৩৬ শতাংশ। ২০১২ সালে এমন ব্যাংকের সংখ্যা ছিল ৭০ শতাংশ। তিন বছরে এই সংখ্যা ১৮ শতাংশ কমলেও তা এখনও পুরো খাতের জন্য অনেক বেশি। ব্যাংক খাতে আইটি জনবলের অভাব এবং এ খাতের উন্নয়নে ব্যাংকের বিনিয়োগ অনীহার কথা গবেষণায় বিশেষভাবে উল্লেখ করা হয়েছে। বলা হয়েছে, আইটি খাতে কর্মরত মোট জনবলের মাত্র ২ শতাংশ আইটিতে কাজ করে। এ খাতে সব মিলিয়ে এখন কাজ করে ১ লাখ ৭৩ হাজার লোক। এর মধ্যে আইটিতে কাজ করে মাত্র চার থেকে সাড়ে চার হাজার লোক।

গবেষণা মতে, ৮৫ শতাংশ ব্যাংকের ঊর্ধ্বতন কর্তৃপক্ষ আইটিতে বিনিয়োগকে বাড়তি খরচ হিসেবে দেখে। যেসব ব্যাংক প্রযুক্তিতে বড় বিনিয়োগ করেছে, তারাও এ খাতের খরচকে ব্যবসায়ের মূল বিনিয়োগ মনে করে না। এ ক্ষেত্রে আরও একটি গুরুত্বপূর্ণ তথ্য হলো, উন্নততর গ্রাহকসেবা ও ব্যাংকিং কার্যক্রমে কর্মদক্ষতা বাড়াতে ৯০ শতাংশ ব্যাংকের আইটি-বিষয়ক সুনির্দিষ্ট কোনো পরিকল্পনা নেই। বলার অপেক্ষা রাখে না, আইটি জনবলের অভাব, এ খাতে বিনিয়োগকে যথোচিত গুরুত্ব না দেয়া এবং আইটি-বিষয়ক কোনো পরিকল্পনা না থাকা প্রকৃতপক্ষে ব্যাংকগুলোকে তথ্য নিরাপত্তা ঝুঁকিতে ফেলে দিয়েছে কিংবা তা বাড়িয়ে দিয়েছে। ব্যাংকের সাথে গ্রাহকের সম্পর্ক ওতপ্রোত। এ সম্পর্ক আস্থা ও বিশ্বাসের বন্ধনে আবদ্ধ। গ্রাহক এই আস্থা ও বিশ্বাস পোষণ করে, ব্যাংকে তার তথ্য ও অর্থ নিশ্চিত ও নিরাপদ থাকবে। ব্যাংকও এই আশ্বাস ও প্রতিশ্রুতি দিয়ে থাকে। ব্যাংক খাত ডিজিটালাইজড হওয়ার পর সাম্প্রতিক বছরগুলোতে কিছু সুবিধার পাশাপাশি কিছু অসুবিধা ও সমস্যাও লক্ষ করা যাচ্ছে। অসুবিধা ও সমস্যাগুলো ব্যাংক-গ্রাহক সম্পর্কের ওপর নেতিবাচক প্রভাব ফেলছে। এটিএম সুবিধা গ্রাহকদের জন্য খুব ফলপ্রসূ বলে বিবেচিত হলে এবং তাদের সময় সাশ্রয় ও ঝামেলামুক্ত করলেও এটিএম কার্ড জালিয়াতির ঘটনায় তারা বিব্রত ও উদ্বিগ্ন। তাদের পক্ষে জালিয়াতি ঠেকানো সম্ভব নয়। আবার ব্যাংকের অপারগতাও প্রমাণিত। এ ধরনের ক্ষেত্রে ব্যাংকের প্রতি আস্থা ও বিশ্বাসে চিড় ধরাই স্বাভাবিক। কারণ তথ্য ও অর্থের নিরাপত্তা থাকছে না। সম্প্রতি বাংলাদেশ ব্যাংকের রিজার্ভ থেকে ১০ কোটি ১০ লাখ ডলার চুরির ঘটনা সর্বমহলে ব্যাপক উৎকণ্ঠার জন্ম দিয়েছে। রাষ্ট্রীয় কোষাগার হিসেবে পরিচিত বাংলাদেশ ব্যাংকের রিজার্ভ থেকেই যদি এভাবে টাকা চুরি হয়ে যায়, টাকার নিরাপত্তা না থাকে, তাহলে অন্যান্য ব্যাংকে তথ্য ও টাকার নিরাপত্তা নিয়ে শংকিত না হয়ে উপায় থাকে না। এই ঘটনার পর ব্যাংক খাতে আইটি নিরাপত্তার বিষয়টি বিশেষভাবে আলোচনায় এসেছে। তথ্য ও অর্থের নিরাপত্তা নিশ্চিত করার বিষয়টি বস্তুতপক্ষে এখন অপরিহার্য দাবি। ব্যাংক খাতে তথ্য ও অর্থের নিরাপত্তা নিশ্চিত করার কোনো বিকল্প নেই। বিদ্যমান বিশৃঙ্খলা, অসমন্বিত ও অনিশ্চিত অবস্থা অব্যাহত থাকলে ব্যাংকের ওপর গ্রাহকদের আস্থা ও বিশ্বাস ব্যাপকভাবে হ্রাস পাবে। গ্রাহকেরা তাদের তথ্য ও অর্থের নিরাপত্তা নিয়ে সমস্যায় পড়বে, এটা যেমন স্বাভাবিক তেমনি ব্যাংক ব্যবসায় ধস নামবে, এমন আশঙ্কাও অমূলক নয়। এ ধরনের পরিস্থিতিতে দেশের অর্থনীতিতে মারাত্মক বিপর্যয় নেমে আসতে পারে। বাংলাদেশ ইনস্টিটিউট অব ম্যানেজমেন্টকে আমরা বিশেষভাবে ধন্যবাদ জানাই এ জন্য, প্রতিষ্ঠানটি একটি জরুরি ও গুরুত্ব বিষয়ের ওপর গবেষণা ও আলোকপাত করেছে। এতে সর্বমহলে সচেতনতা ও তাগিদ বাড়বে। গবেষণায় তথ্য ও অর্থের নিরাপত্তায় কিছু সুপারিশ বা প্রস্তাব দেয়া হয়েছে। এর মধ্যে রয়েছে আইটিতে দক্ষ জনবল নিয়োগ ও আইটি উন্নয়নে আরও বিনিয়োগ করার কথা।

আইটি ক্ষেত্রে, বিশেষ করে সাইবার নিরাপত্তার ক্ষেত্রে সার্টিফিকেশনের ব্যাপক চাহিদা রয়েছে। মূলত এই সার্টিফিকেশনই একজন আইটি প্রফেশনালকে সাইবার নিরাপত্তা পেশায় দক্ষ করে গড়ে তোলে। তাই নিরাপত্তা সার্টিফিকেশন করা মানুষের জন্য কর্মসংস্থানের সুযোগও বেশি। এখন প্রশ্ন হলো, আসলে কোনো কোনো আইটি বা সাইবার সিকিউরিটি সার্টিফিকেশন আসলে কর্মক্ষেত্রে দরকার। এখানে কয়েকটি জনপ্রিয় ও চাহিদাসম্পন্ন সার্টিফিকেশন নিয়ে আলোচনা করা হলো।

০১. পেনটেস্টার (PenTester) : মূলত পেনিট্রেশন টেস্টারেরা কোনো সিস্টেমের নিরাপত্তা ত্রুটি খুঁজে বের করতে সাহায্য করে থাকে। কোনো সফটওয়্যার ডেভেলপার যখন কোনো সফটওয়্যার তৈরি করে তারপর এর নিরাপত্তা ত্রুটি বা নিরাপত্তা টেস্ট করার জন্য মূলত এই পেশার মানুষেরা কাজ করে থাকে। এদেরকে ওয়াইট হ্যাট হ্যাকারও বলা হয়ে থাকে। এরা আপনার সিস্টেমের কোনো দুর্বলতা বের করতে সাহায্য করে। ইসি কাউন্সিল মূলত এই ধরনের পেশার মানুষকে সার্টিফিকেশন দিয়ে থাকে।

০২. সিসা (CISA) : বড় বড় সিস্টেমের ক্ষেত্রে, বিশেষ করে ব্যাংকিংয়ের মতো সিস্টেম যেখানে আর্থিক লেনদেনের বিষয় থাকে সেখানে নিয়মিত অডিট করা খুবই জরুরি। আইটি অডিটের ক্ষেত্রে সবচেয়ে সম্মানিত সার্টিফিকেশন হলো সিসা। এই সার্টিফিকেশনটি আপনাকে ব্যাংকিং সেক্টরের নিরাপত্তা বিভাগে কাজ করার জন্য যোগ্য করে গড়ে তুলবে। আপনি এই সার্টিফিকেশনের মাধ্যমে কোনো একটি সিস্টেমকে কীভাবে নিরাপদ করতে হয় এবং যখন একটি সিস্টেম কাজ করছে তখন নিরাপত্তার নির্দেশনাগুলো ঠিকমতো মেনে চলছে কি না, তা দেখে থাকে। এরা মূলত টেকনিক্যাল ও নন-টেকনিক্যাল সাইবার নিরাপত্তা নিয়ে কাজ করে থাকে। এটা খুবই গুরুত্বপূর্ণ, কারণ যেকোনো আইটি অপারেশনে মানুষ সম্পৃক্ত থাকে। আপনি যত নিরাপদ সিস্টেমই বানান না কেন, যারা এই সিস্টেম ব্যবহার করছে তারা যদি নিরাপত্তার বিষয়গুলো সঠিকভাবে না মানে তবে কোনোভাবেই সিস্টেমকে নিরাপদ রাখা সম্ভব নয়। তাই একজন আইটি সিকিউরিটি অডিটর টেকনিক্যালের পাশাপাশি হিউম্যান ফ্যাক্টরগুলোও নিরীক্ষণ করে থাকে। ISACA নামের প্রতিষ্ঠান এই সার্টিফিকেশনটি পরিচালনা করে থাকে।

০৩. সিআইএসএসপি : এটি আইটি নিরাপত্তার ক্ষেত্রে অন্যতম সম্মানজনক সার্টিফিকেশন। এটি মূলত যারা কয়েক বছর সাইবার সিকিউরিটি নিয়ে কাজ করছেন তাদের জন্য। সুতরাং সহজেই বোঝা যায়, এটি মূলত যারা সাইবার সিকিউরিটি ম্যানেজার হিসেবে কাজ করতে চান বা কাজ করার জন্য নিজেদেরকে তৈরি করতে চান তাদের জন্য। এই সার্টিফিকেশনটি টেকনিক্যাল সাইবার সিকিউরিটির বিষয়গুলো দেখানোর সাথে সাথে সাইবার সিকিউরিটি ম্যানেজমেন্টের বিষয়গুলো নিয়েও আলোচনা করে থাকে। এই সার্টিফিকেশনটি SANS নামের প্রতিষ্ঠানটি পরিচালনা করে থাকে এবং এটি একটি নির্দিষ্ট সময় পরপর রিনিউ করতে হয় কজ

ফিডব্যাক : jabedmorshed@yahoo.com