স্কিমিং অ্যাটাক
এটিএম কার্ড জালিয়াতি থেকে বাঁচার উপায়

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

গত কয়েক দিনে বেশ কয়েকটি ব্যাংকের এটিএম বুথ থেকে লাখ লাখ টাকা কে বা কারা তুলে নিয়ে গেছে। সবচেয়ে ক্ষতিগ্রস্ত ব্যাংক সম্ভবত ইস্টার্ন ব্যাংক আর পুলিশের প্রাথমিক প্রতিবেদনে জানা যায়, হয়তো দেশি দুষ্কৃতকারীদের সাথে কয়েকজন বিদেশি অপরাধীও এর সাথে জড়িত। বাংলাদেশ ব্যাংকের প্রাথমিক তদন্তে এটিকে 'স্কিমিং অ্যাটাক' হিসেবে চিহ্নিত করা হয়েছে। স্কিমিং অ্যাটাক উন্নত বিশ্বে অনেক আগে থেকেই বিদ্যমান থাকলেও বাংলাদেশে এটাই বড় মাপের প্রথম অ্যাটাক। বাংলাদেশে ব্যাংকিং খাত যেভাবে ডিজিটালাইজেশন হয়েছে, তাতে এই ধরনের ঘটনা ঘটা স্বাভাবিক ও ভবিষ্যতে আরও ঘটবে। আমরা সবাই যেহেতু এটিএম কার্ড ব্যবহার করি, তাই সবারই এই বিষয়ে প্রাথমিক সতর্কতা অবলম্বন করা উচিত।

স্কিমিং অ্যাটাক কী?

স্কিমিং অ্যাটাক হলো মূলত এটিএম কার্ডের ক্লোন তৈরি করে ও ব্যবহারকারীর পিন নম্বর চুরি করে সেই ব্যবহারকারীর অ্যাকাউন্ট থেকে টাকা তুলে নেয়ার কৌশল।

কীভাবে করা হয়?

প্রথমে এটিএম মেশিনের কার্ড রিডারের ওপর একটি স্কিমিং ডিভাইস লাগানো হয়। যেই ডিভাইসটি এটিএম মেশিনে যে কার্ড প্রবেশ করানো হবে তার ম্যাগনেটিক টেপে ও চিপে যে তথ্য লেখা আছে তা কপি করে তার মেমরিতে স্টোর করে রাখে। পরবর্তী সময় সেই তথ্য দিয়ে অপরাধকারীরা একটি হুবহু নকল কার্ড তৈরি করে, যেখানে কপি করা কার্ডের সব তথ্য থাকে। এটাকে বলা হয় কার্ড ক্লোনিং।

গোপন ভিডিও ক্যামেরা

অ্যাকাউন্ট হোল্ডারের পিন নম্বর নেয়ার জন্য সাধারণত গোপন ক্যামেরা সেট করা হয় এটিএম বুথের কোনো জায়গায়, যা কোন কার্ডের সাথে কোন পিন তা ধারণ করে।

পরবর্তী সময় যেকোনো সময় দুষ্কৃতকারী এসে স্কিমিং ডিভাইস ও ভিডিও ক্যামেরাটি এটিএম বুথ থেকে নিয়ে যায়। এরপর ক্লোন করা কার্ড ও সেই পিন নম্বর ব্যবহার করে ওই অ্যাকাউন্ট হোল্ডারের অ্যাকাউন্ট থেকে টাকা তুলে নিয়ে যায়। অনেক সময় অবশ্য স্কিমিং ডিভাইসের সাথেই ইন্টারনেট কানেকটিভিটি থাকে এবং অ্যাটাকার রিয়েল টাইমেই কার্ডের তথ্য পেয়ে থাকে।

এটিএম স্কিমিং বুঝব কীভাবে?

আপনি যখন জেনেই গেছেন এটিএম স্কিমিং কীভাবে কাজ করে, তাহলে আপনার কাছে এটা প্রতিরোধ করাটা খুব সহজ একটি কাজ। শুধু মনে করে প্রতিবার কার্ড ব্যবহারের আগে কিছু জিনিস লক্ষ করে দেখুন।

* মেশিনে এটিএম কার্ড প্রবেশ করানোর আগে কার্ড প্রবেশের জায়গাটিতে হালকা নড়াচড়া করে দেখে নিন সেটি খুলে আসছে কি না। যদি খুলে আসে, তাহলে বুঝবেন আপনি আসলে একটি স্কিমিং মেশিনে কার্ড প্রবেশ করাচ্ছেন!

* যেকোনো মেশিনে কার্ড প্রবেশের সময় তা খুব মসৃণভাবে মেশিনে প্রবেশ করানো উচিত। যদি কার্ড প্রবেশের সময় আটকে যাওয়ার অনুভূতি পান, তাহলে সতর্কতা অবলম্বন করুন।

* এটিএম বুথের কার্ড রিডারটি ভালো করে পরীক্ষা করে দেখুন। বেশিরভাগ স্কিমিং ডিভাইস অস্বচ্ছ, তাই স্কিমিং ডিভাইস লাগালে কার্ড রিডার থেকে যে সবুজাভ আলোর কিছুক্ষণ পরপর ব্লিংক করে তা ঢেকে যাবে। তাই যদি কার্ড রিডারের এই লাইটটি না দেখা যায় তবে তা এড়িয়ে যেতে হবে। এছাড়া আশপাশের অন্য কোনো ডিভাইস সন্দেহজনক মনে হলে ব্যাংককে জানাতে হবে।

* পিন নম্বর দেয়ার সময় হাত দিয়ে আড়াল করে দেয়া উচিত।

* মোবাইলে ট্রানজেকশন নোটিফিকেশন অন রাখা।

* চাইলে আপনি নাম্বার প্লেটটি নেড়ে দেখতে পারেন সেটি আলগা কি না।

* ওপরের ক্যামেরাটি সাধারণত চোখে পড়ে না। আর তাছাড়া ক্যামেরা সবসময় ওপরেই থাকবে– এমন কথা নেই। বুথের যেকোনো জায়গায় গোপন ক্যামেরাটি থাকতে পারে, যা আপনার নাম্বার প্লেটে প্রবেশ করানো নাম্বারগুলো দেখতে পারবে। তাই পিন নাম্বার প্রবেশের সময় শরীর এবং হাত দিয়ে পুরো জায়গাটি ঢেকে ফেলুন, যাতে কোনো পাশের ক্যামেরাই আপনার পিনটি নোট করতে না পারে।

দিন দিন অপরাধীরা আরও শক্তিশালী হচ্ছে। সহজে ও অল্প দামে পাওয়া প্রযুক্তির কল্যাণে এরা যেকাউকে খুব সহজে বোকা বানাতে সক্ষম! আপনার সতর্কতা অনেক ক্ষেত্রেই আপনাকে রক্ষা করবে এবং আপনার কষ্টের উপার্জন চুরি হওয়া ঠেকাবে। শুধু ব্যাংকের পক্ষে স্কিমিংয়ের মতো বিশাল ফাঁদ মোকাবেলা করা প্রায় অসম্ভব। যত বেশি গ্রাহক স্কিমিংয়ের ব্যাপারে সচেতন হবে, স্কিমারদের পাতানো ফাঁদ তত বেশি দুর্বল হয়ে পড়বে। কোনো বুথে উল্লিখিত কোনো লক্ষণ দেখামাত্র বুথের গার্ডের সাহায্য নিয়ে তা সংশ্লিষ্ট ব্যাংকে জানান। আপনার এই সামান্য উদ্যোগ হয়তো অনেকের কষ্টে কামানো টাকা বাঁচিয়ে দেবে! কজ

ফিডব্যাক : jabedmorshed@yahoo.com

কেন্দ্রীয় ব্যাংকের ছয় দফা নির্দেশনা

গ্রাহকের তথ্য চুরি করে ক্লোন কার্ড বানিয়ে লাখ লাখ টাকা হাতিয়ে নেয়ার ঘটনার পর প্রতিটি এটিএম বুথে জালিয়াতি প্রতিরোধের ব্যবস্থা বাধ্যতামূলক করাসহ ছয় দফা নির্দেশনা জারি করেছে কেন্দ্রীয় ব্যাংক। এতে বলা হয়েছে, জালিয়াতি রোধে ও লেনদেন ঝুঁকিমুক্ত করতে সব এটিএম বুথে এক মাসের মধ্যে 'অ্যান্টি স্কিমিং ও পিন শিল্ড ডিভাইস' বসাতে হবে। নতুন কোনো বুথ খুলতে গেলেও অবশ্যই এসব ব্যবস্থা রাখতে হবে।

ছয় দফা নির্দেশনা

০১. এখন থেকে নতুনভাবে স্থাপিত এটিএম বুথগুলোতে বাধ্যতামূলকভাবে অ্যান্টি স্কিমিং ও পিন শিল্ড ডিভাইস থাকতে হবে। আগে স্থাপিত বুথগুলোতে এক মাসের মধ্যে অ্যান্টি স্কিমিং ও পিন শিল্ড ডিভাইস স্থাপন করতে হবে।

০২. প্রতিদিন এটিএম বুথে সংঘটিত লেনদেনের ভিডিও ফুটেজ যথাযথভাবে পর্যবেক্ষণ করতে হবে এবং তাতে কোনো সন্দেহজনক বিষয় দৃষ্ট হলে কার্যকর ব্যবস্থা নিতে হবে।

০৩. ইতোমধ্যে গ্রাহকের কার্ডের তথ্য ও পিন নম্বর কোনোক্রমে পাচার হয়ে থাকলে সংশ্লিষ্ট সময়ে এটিএম বুথে ব্যবহৃত কার্ডসমূহ চিহ্নিত করে নিজ ব্যাংকের কার্ডসমূহের ক্ষেত্রে গ্রাহককে অবহিত করে কার্ডটি বাতিল এবং যত দ্রুত সম্ভব গ্রাহককে নতুন কার্ড দিতে হবে। গ্রাহক অন্য ব্যাংকের হলে সংশ্লিষ্ট কার্ড প্রদানকারী ব্যাংককে তাৎক্ষণিকভাবে অবহিত করে একই ব্যবস্থা নেয়ার জন্য অনুরোধ করতে হবে। উক্ত ভিডিও ফুটেজ আইনপ্রয়োগকারী সংস্থাকে অবহিতকরণপূর্বক প্রয়োজনীয় ব্যবস্থা নেয়ার জন্য অনুরোধ করতে হবে।

০৪. নিয়মিতভাবে দৈবচয়নের (Random Basis) ভিত্তিতে ব্যাংকের নিজস্ব এটিএম বুথগুলো নিরীক্ষা করে মাসিক ভিত্তিতে বাংলাদেশ ব্যাংকের সংশ্লিষ্ট বিভাগে প্রতিবেদন পাঠাতে হবে।

০৫. এটিএম বুথগুলোতে নিয়োজিত গার্ডদের জাল/জালিয়াতি প্রতিরোধে করণীয় সম্পর্কে প্রয়োজনীয় প্রশিক্ষণ দিতে হবে। এছাড়া টুপি, সানগ্লাস পরিধানকারী ও ব্যাগ বহনকারী গ্রাহকদের ক্ষেত্রে গার্ড সতর্ক থাকবে।

০৬. এটিএম বুথগুলো থেকে টাকা তোলার সাথে সাথে স্বয়ংক্রিয়ভাবে গ্রাহককে মোবাইলে অ্যালার্ট দেয়ার মাধ্যমে লেনদেন সংক্রান্ত তথ্য পাঠাতে করতে হবে।