ক্রেডিট কার্ড প্রতারণা ঠেকাতে যা জানতে হবে

মুনীর তৌসিফ

অন্যান্য দেশের মতো আমাদের দেশেও ভোক্তা জনগোষ্ঠী এখন ইলেকট্রনিক পেমেন্ট সিস্টেম ব্যাপক হারে ব্যবহার করছে। অপরদিকে সাইবার ক্রিমিনালেরা ক্রমবর্ধমান হারে নানা সৃজনশীল কৌশল নিয়ে হাজির হচ্ছে আপনার-আমার অর্থ চুরি করতে। এ প্রেক্ষাপটে প্রশ্ন এসেছে, কী করে আমরা এদের হাত থেকে নিজেদের নিরাপদ রাখতে পারি। ধরুন, আপনি একটি ক্রেডিট কার্ড বা ডেবিট কার্ডের মালিক। তাহলে সমূহ সম্ভাবনা আছে আপনি সাইবার প্রতারকদের প্রতারণার শিকার হতে পারেন। ঠিক যেমনটি বিশ্বজুড়ে লাখ লাখ মানুষ ক্রেডিট কার্ড প্রতারণার শিকার অহরহ হচ্ছেন। এসব প্রতারক অনলাইন লেনদেনকে তাদের স্বর্ণখনি মনে করে।

বাড়ছে ক্রেডিট কার্ড ব্যবহার

১৯৮০-র দশক থেকে শুরু করে আজ পর্যন্ত উল্লেখযোগ্য হারে ক্রেডিট কার্ড, ডেবিট কার্ড ও প্রি-পেইড কার্ড আন্তর্জাতিকভাবে ব্যবহার বেড়ে চলেছে। ২০১৬ সালের অক্টোবরের নিলসন রিপোর্ট মতে, ২০১৫ সালে সারা বিশ্বে ৩১ ট্রিলিয়ন ডলারেরও বেশি মূল্যের লেনদেন হয়েছে ইলেকট্রনিক সিস্টেমে। এই লেনদেন হয়েছে এসব কার্ডের মাধ্যমে। এই লেনদেনের পরিমাণ ২০১৪ সালের তুলনায় ৭.৩ শতাংশ বেশি। ইউরোপে ২০১৫ সালে আটটি কেনার ঘটনায় সাতটিরই দাম পরিশোধ করা হয়েছে ইলেকট্রনিক উপায়ে। এমনটি সম্ভব হয়েছে Paypal-এর মতো নতুন মানি-ট্রান্সফার সিস্টেম ও বিশ্বব্যাপী ই-কমার্স ছড়িয়ে পড়ার সুবাদে। উন্নয়নশীল দেশগুলোতেও এই ই-কমার্সের পরিধি বাড়ছে, যদিও এসব দেশকে অনলাইন পেমেন্ট সিস্টেম চালুর ব্যাপারে ধীরগতি অবলম্বন করতে দেখা গেছে। আশা করা হচ্ছে, অনলাইন পেমেন্ট বেড়ে চলার প্রবণতা দিন দিন আরও বাড়বে। ফ্লিপকার্ট, স্ন্যাপডিল, অ্যামাজন ইন্ডিয়া, আলিবাবা ও ঝিং ডং ইত্যাদির মতো বড় বড় কোম্পানির সুবাদে ইলেকট্রনিক পেমেন্ট নতুন নতুন ভোক্তা জনগোষ্ঠীর কাছে পৌঁছাচ্ছে ব্যাপকভাবে। উল্লেখ্য, ভারতে ২০১৫ সালের ই-কমার্স মার্কেটে অ্যামাজন ইন্ডিয়ার অবদান ছিল ৮০ শতাংশ এবং ২০১৬ সালে চীনের বাজারে ঝিং ডং-এর অবদান ছিল ৭০ শতাংশ।

বাড়ছে ক্রেডিট কার্ড প্রতারণাও

একটি সমীক্ষা মতে, ২০১৫ সালে প্রতারণার শিকার হয়েছেন ১ কোটি ৩৪ লাখ মানুষ। ২০১৬ সালে এই সংখ্যা ২০ লাখ বেড়ে দাঁড়ায় ১ কোটি ৫৪ লাখ। মোট কথা, ২০১৬ সালে মোট ভোক্তার ৬.১৫ শতাংশই এই প্রতারণার শিকার হয়েছেন। এই সমীক্ষায় শুধু ক্রেডিট কার্ড প্রতারণাই অন্তর্ভুক্ত করা হয়নি, এতে অন্যান্য অনলাইন পেমেন্টের প্রতারণার ঘটনাও রয়েছে। তবে গবেষণা সংস্থাটি জানিয়েছে, বেশিরভাগ আইডেন্টিটি চুরির ঘটনা ক্রেডিট কার্ডের বেলায়ই ঘটেছে। অপরদিকে গবেষণা সংস্থা 'জেভেলিন স্ট্র্যাটেজি অ্যান্ড রিসার্চ' জানতে পেরেছে, ২০১৬ সালে এই প্রতারণা চিহ্নিত

করার পরিমাণ আগের বছরের তুলনায় ১৬ শতাংশ বেড়েছে। এর ফলে সংশ্লিষ্ট ব্যক্তিবর্গকে লোকসান গুনতে হয়েছে ১৬০০ কোটি ডলার, যা ছিল আগের যেকোনো বছরের তুলনায় সর্বোচ্চ।

আরেকটি ক্ষেত্র, যেখানে নানা ধরনের প্রতারণার কথা জানা গেছে, সেটি হচ্ছে 'অ্যাকাউন্ট টেকওভার'। অ্যাকাউন্ট টেকওভারের ঘটনা তখনই ঘটে, যখন চোরেরা কারও অ্যাকাউন্টে ঢুকে পড়ে এর কন্টাক্ট ও ইনফরমেশন পরিবর্তন করে ফেলে। তখন প্রতারকেরা প্রতারণার শিকার ব্যক্তির অজান্তে অবাধে চার্জ করতে পারে। কেননা, কোনো ওয়ার্নিং বা নোটিফিকেশন চোরদের কাছে ফেরত পাঠানো হয় না। ২০১৬ সালে এ ধরনের অ্যাকাউন্ট টেকওভারের ঘটনা আগের বছরের তুলনায় ৬১ শতাংশ বেড়ে ১৪ লাখে পৌঁছে। অপরদিকে ভোক্তার নামে তার অজান্তে নতুন অ্যাকাউন্ট খোলার পরিমাণ ২০১৬ সালে আগের বছরের তুলনায় ৪০ শতাংশ বেড়ে যায় এবং ফলে প্রতারণার শিকার হয় ১৮ লাখ ভোক্তা।

প্রতারণার ধরন

ক্রেডিট কার্ড প্রতারণা নানা ধরনের। আর এগুলো নতুন নতুন প্রযুক্তির সাথে সাথে খুব দ্রুত পরিবর্তন হয়। সে কারণে সব ধরনের অনলাইন প্রতারণার তালিকা তৈরি করা মুশকিল। এখানে দুই ধরনের সাধারণ ক্রেডিট কার্ড প্রতারণার কথা উল্লেখ করা হলো–

card-not-present (CNP) frauds : এটি সবচেয়ে সাধারণ ধরনের ক্রেডিট কার্ড প্রতারণা। এটি ঘটে তখন, যখন প্রতারকেরা কার্ড-মালিকের ইনফরমেশন চুরি করে তা অবৈধভাবে ব্যবহার করে। এ ক্ষেত্রে কার্ডের কোনো ভৌত উপস্থিতি থাকে না। এই দিকটির কথা বিবেচনা করেই এর এ ধরনের নামকরণ। সাধারণত এ ধরনের প্রতারণা ঘটে অনলাইন লেনদেনের সময়। এটি ঘটতে পারে প্রতারকদের পাঠানো তথাকথিত 'ফিশিং' ই-মেইলের ফলে। এ ক্ষেত্রে প্রতারকেরা নিজেদের পরিচয় গোপন রেখে বিশ্বাসযোগ্য প্রতিষ্ঠানের নাম ব্যবহার করে কন্টামিনেটেড লিঙ্কের মাধ্যমে ব্যক্তিগত ও অর্থ সংক্রান্ত তথ্য চুরি করার জন্য।

card-present-frauds : এ ধরনের ক্রেডিট কার্ড প্রতারণা এখন আর তেমন ঘটে না। এরপরও এ ব্যাপারে সতর্ক থাকা দরকার। এটি কখনও কখনও skimming-এর আকার ধারণ করে। এ ক্ষেত্রে একজন অসৎ বিক্রেতা কোনো ভোক্তার একটি কার্ড কোনো ডিভাইসের মাধ্যমে হাতিয়ে নেয়, যে ডিভাইসে ইনফরমেশন মজুদ করা হয়। একবার যদি ওই ডাটা কোনো পণ্য বা সেবা কেনায় ব্যবহার হয়, ভোক্তার অ্যাকাউন্টে তখন তার জন্য চার্জ করা হয়।

এর বাইরে যেকোনো সময় আপনার ক্রেডিট কার্ডটি যেকোনো উপায়ে চুরি যেতে পারে। ▸

যখনই নিশ্চিত হবেন কার্ডটি চুরি হয়ে গেছে, সাথে সাথে আপনি তা কার্ড ইস্যুয়ারকে জানান। হারিয়ে যাওয়া কার্ড কোনোভাবে অন্যের হাতে পড়লে প্রাপক তা ব্যবহার করে আপনার অ্যাকাউন্ট থেকে অর্থ তুলে নেয়ার চেষ্টা চালাতে পারে। তাই এ ক্ষেত্রেও বড় ধরনের ক্ষতি হওয়ার আগেই কার্ড ইস্যুয়ারকে জানাতে হবে। আবার অবৈধভাবে পাওয়া কার্ডে ইনফরমেশন ব্যবহার করে প্রতারক এর একটি নকল কার্ড তৈরি করে তা ব্যবহার করতে পারে। যুক্তরাষ্ট্রে ক্রমবর্ধমান হারে chip-and-PIN (EMV-এর মতো) প্রযুক্তি ব্যবহার করে এ ধরনের প্রতারণা কমিয়ে আনা সম্ভব হয়েছে। ক্রেডিট কার্ড কোম্পানিগুলো চেষ্টা করে ট্র্যানজিটে থাকা কার্ডগুলোর সুরক্ষা দিতে। এরপরও একটি নতুন কার্ড চুরি হয়ে যেতে পারে আপনার মেইলবক্স থেকে। আপনার নাম, জন্মতারিখ, সামাজিক নিরাপত্তা নম্বর ও অন্যান্য ব্যক্তিগত তথ্য ব্যবহার করে প্রতারকেরা আপনার নামে নতুন ক্রেডিট কার্ডের জন্য আবেদন করতে পারে।

ক্রেডিট কার্ডে লেনদেনের মেকানিজম

ক্রেডিট কার্ডে লেনদেন খুবই সরল। অংশত এ কারণে প্রতারকেরা ক্রেডিট কার্ড নিয়ে প্রতারণার কাজটি করার সহজ সুযোগ পায়। ক্রেডিট কার্ড লেনদেন হচ্ছে একটি দুই ধাপের প্রক্রিয়া, তথা টু-স্টেপ প্রসেস : অথরাইজেশন ও সেটলমেন্ট। শুরুতেই যারা লেনদেনের সাথে সংশ্লিষ্ট (গ্রাহক, কার্ড ইস্যুকারী, ব্যবসায়ী ও ব্যবসায়ীর ব্যাংক) কোনো একটি কেনাকাটায় অনুমোদন দেয়া বা প্রত্যাখ্যানের ব্যাপারে তথ্য পাঠায় ও গ্রহণ করে। যদি কেনার কাজটির অনুমোদন দেয়া হয় বা অথরাইজ করা হয়, তবে এর মীমাংসা বা সেটলমেন্ট ঘটে অর্থের বিনিময়ে। আর এই অর্থের বিনিময় চলে অথরাইজেশনের কয়েক দিন পর। একবার কেনার ব্যাপারটি অথরাইজ হয়ে গেলে, তা থেকে ফিরে আসার কোনো সুযোগ নেই। এর অর্থ, প্রতারণা রোধের যাবতীয় পদক্ষেপ নিতে হবে লেনদেনের প্রথম ধাপের সময়েই।

এটি কী করে নাটকীয়ভাবে সরল উপায়ে কাজ করে, তাই দেখা যাক। যখন Visa বা Mastercard-এর মতো কোনো কোম্পানি তাদের ব্র্যান্ড ইস্যু করার জন্য কোনো কার্ড ইস্যুয়ারকে (মনে করেন সোনালী ব্যাংককে) ও কোনো মার্চেন্ট ব্যাংককে লাইসেন্স দেয়, তবে ওই ব্যাংকগুলো লেনদেন চুক্তি শর্ত নির্ধারণ করে। তখন কার্ড ইস্যুয়ার ভৌতভাবে বা বস্তুগতভাবে ভোক্তাদের মাঝে ক্রেডিট কার্ড ইস্যু করে। এই কার্ডের মাধ্যমে কোনো কেনাকাটার জন্য কার্ড হোল্ডার কার্ডটি ভেন্ডরের কাছে দেন (কিংবা অনলাইনে, ম্যানুয়ালি কার্ড ইনফরমেশন ঢোকান), যিনি ভোক্তার ডাটা ফরোয়ার্ড করেন প্রত্যাশিত ক্রয়ের মার্চেন্ট ব্যাংকের কাছে। তখন ব্যাংক প্রয়োজনীয় তথ্য রুট করে বা পাঠায় কার্ড ইস্যুয়ারের কাছে, এর বিশ্লেষণ ও অনুমোদন বা প্রত্যাখ্যানের জন্য। কার্ড ইস্যুয়ারের চূড়ান্ত সিদ্ধান্ত ফেরত পাঠানো হয় মার্চেন্ট ব্যাংক ও ভেন্ডরের কাছে। রিজেকশন বা প্রত্যাখ্যান ইস্যু করা যাবে শুধু দুই পরিস্থিতিতে– যদি কার্ডধারীর অ্যাকাউন্টে অর্থের পরিমাণ কম থাকে, অথবা মার্চেন্ট ব্যাংকে পাঠানো ডাটায় প্রতারণার সন্দেহ থাকে। প্রতারণার ভুল সন্দেহে যার কেনা প্রত্যাখ্যান করা হয়েছে কিংবা কার্ড ইস্যুয়ার যার কার্ড সাময়িকভাবে বন্ধ করে রাখে, তা তার অসন্তুষ্টির কারণ হতে পারে এবং এর ফলে ভেন্ডরের সুনাম বিনষ্ট হতে পারে।

প্রতারণার শিকার হলে কী করবেন?

শত সতর্কতা অবলম্বন করলেও যেকোনো সময় আপনার ক্রেডিট কার্ডটি চুরি হয়ে যেতে পারে। কারণ, আপনি যখন চলেন ডালে ডালে, তখন প্রতারকেরা চলে পাতায় পাতায়। তাই গুরুত্বপূর্ণ হচ্ছে, সব সময় আপনাকে কার্ড অ্যাকাউন্ট মনিটর করা। আপনার কাছে যখনই ধরা পড়ল, আপনার কার্ড আকাউন্টে অননুমোদিত চার্জ করা হচ্ছে, তখন আপনার করণীয় হবে–

দ্রুত যোগাযোগ করুন ক্রেডিট কার্ড কোম্পানির সাথে : অনেকের রয়েছে জিরো-লায়াবিলিটি পলিসি। এর অর্থ আপনার অ্যাকাউন্টের প্রতারণাপূর্ণ চার্জেও কোনো দায় আপনি বহন করবেন না। অধিকন্তু, যুক্তরাষ্ট্রের ফেডারেল ল আপনার ক্রেডিট কার্ডের প্রতারণামূলক চার্জের জন্য আপনার দায় সীমিত করে দিয়েছে। চুরি হওয়া বা হারিয়ে যাওয়া কার্ড সম্পর্কে আপনি কার্ড ইস্যুয়ারের কাছে রিপোর্ট করার আগে যদি কেউ এই চুরি হওয়া বা হারিয়ে যাওয়া কার্ড ব্যবহার করে, তবে আপনি শুধু ৫০ ডলারের দায় বহন করবেন। প্রতারণামূলক ব্যবহারের আগে রিপোর্ট করলে আপনাকে কোনো চার্জের দায় নিতে হবে না। তা ছাড়া যদি শুধু আপনার কার্ড নাম্বার চুরি করে কেউ ব্যবহার করে, তবে কোনো দায় আপনাকে নিতে হবে না।

পরিবর্তন করুন আপনার পাসওয়ার্ড ও পিন : আর কোনো ক্ষতি হয়ে যাওয়ার আগেই এই কাজটি করুন।

অ্যাকাউন্টের গতিবিধি ঘনিষ্টভাবে মনিটর করুন : আপনার ব্যাংক স্টেটমেন্টের ওপর নজর রাখুন। কোনো ধরনের প্রতারণার আভাস পেলে সাথে সাথে ব্যাংক কর্তৃপক্ষকে জানান। আপনার ক্রেডিট রিপোর্টের একটি কপি চেয়ে নিন। দেখুন তাতে প্রতারণার কোনো কিছু আছে কি নেই। আপনি যদি কোনো আইডেন্টিটি থেফটের শিকার হন, তবে ফ্রড সেন্টার ভিজিট করে আপনার ক্রেডিট রিপোর্টে রেড অ্যালার্ট যোগ করুন। প্রতিটি ক্রেডিটরের সাথে সরাসরি যোগাযোগ করুন, তাদেরকে প্রতারণা সম্পর্কে সতর্ক করার জন্য। যদি আপনি Experian-এর সদস্য হন, তবে আপনার জন্য ডেডিকেটেড ফ্রড রি-সলিউশন এজেন্টের কাছে আপনার অ্যাক্সেস থাকবে, যে আপনার জন্য কাজ করবে আপনার ক্রেডিটরের সাথে প্রতারণামূলক তথ্য সংশোধনের ব্যাপারে। উল্লেখ্য, এক্সপেরিয়ান হচ্ছে একটি বৈশ্বিক ইনফরমেশন সার্ভিস গ্রুপ। এরা কাজ করে বিশ্বের ৪০টি দেশে। এর করপোরেট হেডকোয়ার্টার রয়েছে আয়ারল্যান্ড প্রজাতন্ত্রের ডাবলিনে। আর অপারেশন হেডকোয়ার্টার রয়েছে যুক্তরাজ্যের নটিংহ্যামসহ কয়েকটি দেশের বিভিন্ন শহরে।

যেভাবে ঠেকাবেন এই প্রতারণা

ইতালির একটি বিশ্ববিদ্যালয়ের ইন্টার-ডিসিপ্লিনারি ইনস্টিটিউট অব ডাটা সায়েন্সের গবেষক ব্রুনো বুয়নাগুইডি তার এক গবেষণায় পরীক্ষা করে দেখেন, কী করে অগ্রসর মানের পরিসংখ্যানগত ও সম্ভাবনা সংক্রান্ত কৌশল বা ফিজিবিলিটি টেকনিক উন্নততর উপায়ে প্রতারণা চিহ্নিত করতে পারে। সিকুয়েন্সিয়াল অ্যানালাইসিস তথা ধারাবাহিক বিশ্লেষণ নতুন প্রযুক্তি সহযোগে হতে পারে এর চাবিকাঠি। এর জন্য ধন্যবাদ পেতে পারে অব্যাহতভাবে কার্ড-মালিকের খরচ ও ইনফরমেশন মনিটর করার কাজটি। এর জন্য একটি কমপিউটার মডেল তৈরি করা সম্ভব, যা হিসাব করে বের করে জানিয়ে দেবে এমন সম্ভাব্যতা বা প্রবাবিলিটি যে, এই ক্রয়টি হতে পারে প্রতারণামূলক। যদি প্রবাবিলিটি বা সম্ভাব্যতা একটি নির্দিষ্ট মাত্রা ছাড়িয়ে যায়, তখন কার্ড ইস্যুয়ারকে একটি সতর্কবার্তা দিতে হবে।

কোম্পানিটি তখন সিদ্ধান্ত নেবে, কার্ডটিকে কি সরাসরি ব্লক করে দেবে, না আরও তদন্ত চালানো হবে। যেমন– এ ক্ষেত্রে ভোক্তাকে কল করা হতে পারে। এই মডেলে প্রয়োগ করা হয় প্রতারণা চিহ্নিত করার কাজে ব্যবহৃত 'অপটিমাল স্টপিং থিওরি' নামের সুপরিচিত গাণিতিক তত্ত্ব। এই মডেলের শক্তিটা হচ্ছে– এর লক্ষ্য নিহিত হয় এর প্রত্যাশিত পে-অফ সর্বোচ্চ করা অথবা প্রত্যাশিত খরচ সর্বনিম্ন করা। অন্য কথায়, সবগুলো কমপিউটেশনের লক্ষ্য হবে ফ্রিকুয়েন্সি অব ফলস অ্যালার্ম সীমিত করা। ব্রুনো বুয়নাগুইডির গবেষণা চলমান। কিন্তু এরই মধ্যে ক্রেডিট কার্ড প্রতারণার ঝুঁকি উল্লেখযোগ্য মাত্রায় কমিয়ে আনতে তিনি দিয়েছেন কিছু গোল্ডেন রুল।

প্রথমত, কখনই এমন ই-মেইলের লিঙ্কে ক্লিক করবেন না, যেগুলো আপনাকে ব্যক্তিগত তথ্য সরবরাহ করতে বলে। এমনকি যদি সেন্ডারকে আপনার নিজের ব্যাংক বলেও মনে হয়।

দ্বিতীয়ত, যখন কোনো অপরিচিত ক্রেতার কাছ থেকে কিছু কিনতে যাবেন, তখন কেনার আগে ভেন্ডরের নাম গুগল করেন, এ কথা জানতে কনজ্যুমার ফিডব্যাক প্রধানত ইতিবাচক ছিল কি না।

সবশেষে, যখন অনলাইনে পেমেন্ট করতে যাবেন, তখন চেক করে নিন ওয়েব পেজের অ্যাড্রেস https:// দিয়ে শুরু হয়েছে কি না। এটি হচ্ছে সিকিউরড ডাটা ট্রান্সফারের একটি কমিউনিকেশন প্রটোকল এবং এ ব্যাপারটি নিশ্চিত করুন, ওয়েব পেজে কোনো ব্যাকরণগত ভুল কিংবা অদ্ভুত শব্দ আছে কি না। তা নিশ্চিত না হলে হতে পারে এটি আপনার অর্থ সংক্রান্ত ডাটা চুরির একটি অপপ্রয়াস কজ