ডেবিট ও ক্রেডিট কার্ড চুরি হয়ে যাওয়ার ১৫ উপায়

আনোয়ার হোসেন

ডেবিট বা ক্রেডিট কার্ডে প্রতারণা বাংলাদেশে সাম্প্রতিক সময়ে আলোচিত একটি বিষয়। খবরের কাগজে প্রায়ই দেশী-বিদেশী চক্রের মাধ্যমে সাধারণ গ্রাহকদের ডেবিট বা ক্রেডিট কার্ড জালিয়াতির মাধ্যমে অর্থ হাতিয়ে নেয়ার খবর দেখা যায়। কার্ড জালিয়াতি হচ্ছে গ্রাহকের আইডেন্টি বা কার্ডের তথ্য চুরি করা। কার্ডের জালিয়াতি প্রতিরোধে সবার আগে জানতে হবে কি কি উপায়ে এই খাতে চুরি হতে পারে। তবেই সম্ভব চুরি বা কার্ড জালিয়াতি প্রতিরোধ।

স্কিমিং

এ ক্ষেত্রে জালিয়াত চক্র এটিএম মেশিনের সাথে স্কিমিং ডিভাইস যুক্ত করে দেয়। কার্ড রিডার স্লটে যুক্ত করা স্কিমিং ডিভাইসটি কোনো গ্রাহক তার কার্ড সোয়াইপ করলে বা চার্জ করলে ম্যাগনেটিক স্ট্রিপ থেকে তথ্য কপি করে নেয়। আর কার্ডের পিন নাম্বার পাওয়ার জন্য মেশিনের কাছে ক্যামেরা সেটআপ করে থাকে। ঠিক এমন একটি ঘটনা কিছুদিন আগে বাংলাদেশে সংঘটিত হয়েছে।

কার্ড ট্রাপিং

প্রায়ই মেশিনে কার্ড আটকে যাওয়ার ঘটনা ঘটে। মেশিনে কার্ড ইনসার্ট করে পরে সে কার্ড উদ্ধার করার মাঝখানে চুরি হয়ে যেতে পারে কার্ডের তথ্য।

সোল্ডার সার্ফিং

এটিএম কার্ডের বুথের ভেতর বা বাইরে কার্ড আটকে গেলে বের করতে সাহায্য করার সুযোগ নিয়ে হতে পারে কার্ডের তথ্য চুরি। তাই বন্ধুবেশী জালিয়াতদের কাছ থেকে সতর্ক থাকতে হবে। কার্ডের পিন নাম্বার পেতে তারা সেখানে অপেক্ষা করে থাকতে পারে।

কার্ড পিন ফেলে আসা

কার্ডে পিন নাম্বার লিখে ভুল করে সে কার্ড এটিএম বুথে ফেলে এলে হতে পারে কার্ড জালিয়াতি। এটি এক ধরনের কার্ড জালিয়াতি করার জন্য ভার্চুয়াল আমন্ত্রণের মতো।

অনলাইন লেনদেন

অনিরাপদ প্ল্যাটফর্মে ই-কমার্সে লেনদেন করার সময় কার্ড তথ্য চুরি হয়ে যাওয়ার সম্ভাবনা থাকে। অনিরাপদ ওয়েবসাইটে কার্ডের তথ্য মুছে না ফেলে রেখে দেয়, যা পরে জালিয়াত চক্র ব্যবহার করে।

পারমিং

এই কৌশলে জালিয়াত চক্র কোনো ওয়েবসাইটের মতো করে অবিকল নকল ওয়েবসাইটে ভিজিটরদেরকে নিয়ে যায়। সেসব ওয়েবসাইটে লেনদেন করার সময় বা কার্ডের তথ্য প্রদান করা হলে সেসব তথ্য চুরি হয়ে যায়।

কি স্ট্রোক লগিং

অনিচ্ছাকৃতভাবে কোনো ক্ষতিকর সফটওয়্যার ডাউনলোড করা হলে সেই সফটওয়্যার ব্যবহার করে জালিয়াত চক্র বাটন চাপাকে চিহ্নিত করে এবং পাসওয়ার্ড, ক্রেডিট কার্ড ও ব্যাংকের বিস্তারিত তথ্য চুরি করে।

পাবলিক ওয়াইফাই

স্মার্ট ফোন ব্যবহার করে যারা লেনদেন করতে অভ্যস্ত, তাদের বেলায় পাবলিক ওয়াইফাইয়ের মাধ্যমে কার্ডের বিস্তারিত তথ্য চুরির আশঙ্কা অনেক বেশি থাকে।

ম্যালওয়্যার

এটি একটি ক্ষতিকর সফটওয়্যার, যেটা এটিএম বুথের কমপিউটার সিস্টেম বা ব্যাংকের সার্ভার ধ্বংস করে দিতে পারে। তখন জালিয়াত চক্র খুব সহজেই গোপন সব তথ্য হাতিয়ে নিতে পারে।

মার্চেন্ট বা পয়েন্ট অব সেল থেকে চুরি

কার্ডের তথ চুরি হওয়ার সবচেয়ে সম্ভাবনাময় উপায় হচ্ছে এটি। বিক্রেতাকে কার্ড দেয়া হলে তিনি ক্রেতার কার্ড সোয়াইপ করে পণ্য বা সেবার দাম নিয়ে থাকেন এবং এ কাজের মধ্যেই কার্ডের ম্যাগনেটিক তথ্য চুরি হয়ে যেতে পারে।

ফিশিং অ্যান্ড ভিসিং

ফিশিংয়ের ক্ষেত্রে স্প্যাম মেইলের মাধ্যমে তথ্য চুরি হয়ে থাকে। সেসব স্প্যাম মেইলকে আসল উৎস মনে হতে পারে। ভিসিংও অনেকটা একই রকম। এক্ষেত্রে মোবাইলে ম্যাসেজ বা এসএমএসের মাধ্যমে তথ্য চুরি হয়ে থাকে। এসব কৌশলের মাধ্যমে পাসওয়ার্ড, পিন, অথবা অ্যাকাউন্ট নাম্বার প্রকাশিত হয়ে যায়।

সিম সোয়াইপ ফ্রড

এ ক্ষেত্রে জালিয়াত চক্র মোবাইল অপারেটরদেরকে ভুয়া পরিচয়পত্র প্রদান করে গ্রাহকের ডুপ্লিকেট সিম কার্ড তুলে নিয়ে থাকে। অপারেটর গ্রাহকের আসল সিমটি ডিঅ্যাক্টিভেট করে দেয়। তখন জালিয়াতেরা ওয়ান টাইম পাসওয়ার্ড নিয়ে অনলাইন লেনদেনে সেটা ব্যবহার করে।

অনিরাপদ অ্যাপ

কিছু মোবাইল অ্যাপের মাধ্যমে পিসির গুরুত্বপূর্ণ সব তথ্য চুরি করে বিভিন্ন অনলাইন স্টোরে অনধিকার লেনদেন করা যায়।

কার্ড চুরি, ছিনতাই বা হারিয়ে যাওয়া

ফিশিং বা মেইল হ্যাকের মাধ্যমে পিন, আইডি, পাসওয়ার্ড হাতিয়ে নিয়ে চুরি করা কার্ড ব্যবহার করে লেনদেন করা হতে পারে। তাই কার্ড চুরি হয়ে গেলে সাথে সাথে ব্যাংকের সাথে যোগাযোগ করে কার্ড লেনদেন স্থগিত করে দেয়া উচিত।

অন্যান্য তথ্যকে কার্ডে ব্যবহার

অনেক সময় জালিয়াত চক্র আবেদন ফরম, হারিয়ে যাওয়া বা বাতিল নথিপত্র থেকে তথ্য নিয়ে নতুন কার্ড ইস্যু করে সে কার্ড ব্যবহার করে থাকে কজ