এটিএম কার্ডের নিরাপত্তা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

আমাদের দৈনন্দিন জীবনে এটিএম কার্ডের ব্যবহার এখন সর্বত্রই। ডাচ বাংলা ব্যাংক, ব্র্যাক ব্যাংকসহ অন্যান্য ব্যাংকের কল্যাণে দেশের বিভিন্ন জায়গায় গড়ে উঠেছে বিভিন্ন ব্যাংকের এটিএম বুথ। এ ছাড়া ডাচ বাংলা ব্যাংক অন্যান্য ব্যাংকিং সুবিধা দেয়ার জন্য গড়ে তুলেছে ফাস্ট ট্রাক নামের সুবিধা। যেখানে সহজেই টাকা তোলা ও জমা দেয়া যায়। আমাদের দেশে নতুন হলেও এটিএম প্রযুক্তি কিন্তু বেশ পুরনো। স্বয়ংক্রিয় টেলার মেশিন (এটিএম) বাণিজ্যিকভাবে প্রথম চালু হয় ১৯৬০-এর দশকে। ২০০৫ সালের মধ্যে পৃথিবীজুড়ে ১৫ লাখেরও বেশি এটিএম বসানো হয়। এটিএমের প্রবর্তন এক গুরুত্বপূর্ণ প্রযুক্তিগত উন্নতি বলে বিবেচিত হয়, যা আর্থিক সংস্থাগুলোকে তাদের গ্রাহকদের ২৪×৭ ভিত্তিতে পরিসেবা দেয়ার সুযোগ করে দেয়। এটিএম গ্রাহকদের কাছাকাছি এটিএম বুথ থেকে যখন খুশি টাকা তোলার সুযোগ দিয়ে তাদের সুবিধা অনেকটাই বাড়িয়ে দিয়েছে।

আর্কিটেকচার

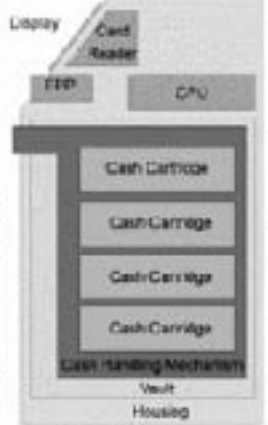
এটিএম মেশিনকে একটি ইউনিট হিসেবে দেখলেও এটি আসলে কয়েকটি কম্পোনেন্টের সমন্বয়ে কাজ করে। অপর দিকে এটিএম মেশিন মাইক্রোকন্ট্রোলারভিত্তিক থাকলেও এখন তা পুরোপুরি পার্সোনাল কমপিউটারের মতো আর্কিটেচার ব্যবহার করে। এই কমপিউটারে ইউএসবি কানেকটরের মাধ্যমে অন্যান্য পেরিফেরাল যুক্ত হয়, এছাড়া থাকে ইথারনেট ও আইপি কমিউনিকেশন। এটি পার্সোনাল কমপিউটারের অপারেটিং সিস্টেম দিয়েই পরিচালিত হয়, যেমন : মাইক্রোসফট এক্সপি।

একটি এটিএমে সাধারণত নিচে উল্লিখিত কম্পোনেন্ট থাকে :

০১. সিপিইউ; ০২. ম্যাগনেটিক বা চিপ কার্ড রিডার; ০৩. পিন কিপ্যাড; ০৪. সিকিউর ক্রিপটো প্রসেসর; ০৫. ডিসপ্লে মনিটর; ০৬. ফাংশন কি (সাধারণত ডিসপ্লের ডান বা বাম পাশে থাকে); ০৭. রেকর্ড প্রিন্টার; ০৮. ভেল্ট, যেখানে টাকা ও অন্যান্য যন্ত্রাংশ রাখা হয়।

সফটওয়্যার

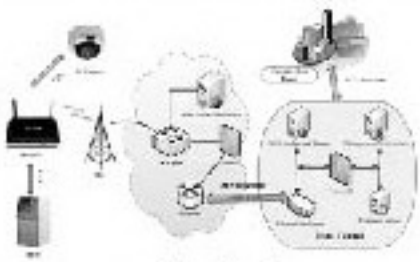
এটিএম মেশিনের বেশিরভাগই চলে মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেমের মাধ্যমে। যদিও ব্রাজিলের কিছু কিছু এলাকায় লিনআক্সভিত্তিক অপারেটিং সিস্টেমেও ব্যবহার হয়। প্রথমদিকে এটিএম মেশিনে ভেন্ডর স্পেসিফিক হার্ডওয়্যার ও সফটওয়্যার ব্যবহার করা হতো। কিন্তু ধীরে ধীরে সেখান থেকে সরে এসে এখন সব এটিএম মেশিনের ভেন্ডরেরা সাধারণত মিডলওয়্যার ব্যবহার করে। বাংলাদেশে ডাচ বাংলা ব্যাংক Nexus Software নামের মিডলওয়্যার ব্যবহার করে। কমিউনিকেশনের জন্য প্রথম দিকে XFS নামের ওপেন সিস্টেম স্ট্যান্ডার্ড ব্যবহার করা হতো। বর্তমান সময়ে এর আগামী প্রজন্মের প্রযুক্তি ActiveXFS ব্যবহার করা হয়।



একটি এটিএম মেশিনের ব্লক ডায়াগ্রাম

নিরাপত্তা ফিচার

০১. সব পিন এনক্রিপশন সাধারণত Encrypting PIN pad (EPP) or



এটিএম নেটওয়ার্ক

PIN Encryption Device (PED) নামের ডিভাইসের মাধ্যমে হয়ে থাকে। এর মাধ্যমে ডাটা সেন্ট্রাল প্রসেসিং ইউনিটে আসার আগেই এনক্রিপটেড হয়ে যায়।

০২. এটিএম মেশিনে এনক্রিপশনের জন্য ট্রিপল DSS এনক্রিপশন মেথড ব্যবহার করা হয়।

০৩. নিরাপত্তার কথা বিবেচনা করে ব্যবহারকারীর পিন নম্বরটি কখনই এটিএম মেশিনের লগ ফাইলে সেভ বা স্টোর করা হয় না।

০৪. Personal Account Number (PAN) টি ছেঁটে নিরাপদ উপায়ে এটিএম মেশিনের লগ ফাইলে সেভ করা হয়। যাতে পরে কেউ সহজেই PAN নম্বরটি বের করতে না পারে।

ব্যাংকের জন্য নিরাপত্তা সতর্কতা

আর্থিক সংস্থাগুলো তাদের এটিএমের সুরক্ষা ব্যবস্থাকে উন্নত করতে এবং জালিয়াতির রাস্তা বন্ধ করতে বিভিন্ন উপায় অবলম্বন করেছে। এর মধ্যে আছে এটিএম স্থাপনের জন্য নিরাপদ স্থান নির্বাচন, নজরদারি ভিডিও ক্যামেরা সংস্থাপন, দূর নিয়ন্ত্রিত পর্যবেক্ষণ, কার্ড নকলরোধী ব্যবস্থা এবং এটিএম অথবা ইন্টারনেটে লেনদেন করার সময়ে গ্রাহকদের ব্যক্তিগত তথ্যগুলো সুরক্ষিত রাখার বিভিন্ন পদ্ধতি সম্পর্কে তাদের সচেতনতা বাড়ানো।

০১. কেন্দ্রীয় অফিস থেকে এটিএম মেশিনের সাথে রিমোট কানেকশনটি সবসময় নিরাপদ হতে হবে। এক্ষেত্রে নিরাপদ ভিপিএন সংযোগ ব্যবহার করা উচিত।

০২. অ্যান্টিভাইরাস ও ম্যালওয়্যার ইনস্টল করতে হবে ও নিয়মিত আপডেট করতে হবে।

০৩. এটিএম নেটওয়ার্কের ট্রাফিক ও অন্য ট্রাফিকে আলাদা চ্যানেলে অ্যাক্সেস করতে হবে।

০৪. এটিএম মেশিনের ডিফল্ট পাসওয়ার্ডটি অবশ্যই পরিবর্তন করে দিতে হবে।

বিভিন্ন ধরনের জালিয়াতি

আপনার অ্যাক্সেস কোডটি মনে করে রাখুন; এটি লিখে রাখবেন না অথবা আপনার সাথে নিয়ে চলবেন না। এমন কোনো অ্যাক্সেস কোড ব্যবহার করবেন না, যা আপনার ওয়ালেটের কোনো শব্দ বা সংখ্যার সাথে মিলে যায়। আপনার অ্যাক্সেস কোড কখনই কাউকে বলবেন না (এমনকি ব্যাংক কর্মচারী, পুলিশ এলেরকেও নয়)। এটিএম কার্ড কাউকে ধার দেবেন না; এটি নগদ টাকা বা ক্রেডিটকার্ড হিসেবে দেখুন। যদি আপনার এটিএম কার্ড হারিয়ে যায়, সাথে সাথে আপনার ব্যাংক অথবা ক্রেডিটইউনিয়নকে জানান।

জালিয়াতেরা কার্ড ঢোকানোর খাপে একটি প্লাস্টিক ফিল্ম ভাঁজ করে ঢুকিয়ে রাখে, যা কার্ডটিকে আটকে রাখে এবং মেশিনকে তা বার করতে দেয় না। অভিজ্ঞোগী গ্রাহক খেয়াল করেন না– কার্ড ঢোকানোর খাপটিতে গণ্ডগোল আছে, বরং মনে করেন কার্ডটি মেশিনে আটকে গেছে।

কার্ডটি একবার আটকে গেলে জালিয়াত ব্যক্তি একজন প্রকৃত কার্ডধারক সেজে ফাঁসে ফেলা গ্রাহককে তার সুরক্ষা কোডটি আরেকবার দেয়ার উপদেশ দেয়। শেষে কার্ডধারক যখন হতাশ হয়ে চলে যান, তখন জালিয়াত ব্যক্তি কার্ডটি বের করে নেয় এবং লুকিয়ে দেখে নেয়া কোডটি মেশিনে ঢোকায়। আরেকটি উপায় হলো ছোট্ট ক্যামেরা এবং 'স্কিমার' নামের একটি যন্ত্র দিয়ে ব্যাংক অ্যাকাউন্টের তথ্যাদি বের করে তা দিয়ে জাল কার্ড তৈরি করা। এই পদ্ধতি কম ঝুঁকিপূর্ণ, কারণ এতে জালিয়াত এবং তার শিকার গ্রাহকের মুখোমুখি সাক্ষাৎ হয় না এবং এর ফলে জাল ব্যক্তি, কার্ডধারককে অনেকটা বেশি নিশ্চিন্ত এবং পাসওয়ার্ডের সুরক্ষা সম্পর্কে তাকে কম সচেতন রাখতে সক্ষম হয়।

এটিএম জালিয়াতির আরেকটি দারুণ উপায় হলো জালিয়াতকারক 'নকল এটিএম মেশিন'-এর ব্যবহার, যেগুলো সফটওয়্যারের মাধ্যমে ওই সব মেশিনে প্রদত্ত পাসওয়ার্ড গ্রহণ করে রেখে দেয়। এরপর নকল কার্ড তৈরি করা হয় এবং চুরি করা পাসওয়ার্ড ব্যবহার করে টাকা তুলে নেয়া হয়। কখনো কখনো এসব জালিয়াতি কার্ডদাসকারী কোম্পানির কর্মচারীদের সাথে ভেতরের যোগসাজশে সংঘটিত হয়। যেভাবেই এসব জালিয়াতি ঘটুক না কেন, এগুলো অবশ্যই অবৈধ এবং সংশ্লিষ্ট দেশের আইনানুযায়ী দন্ডনীয়। তবে শাস্তি হলেও জালিয়াতিতে খোয়া যাওয়া টাকা ফিরে নাও আসতে পারে। তাই দোষীর শাস্তি বিধান অন্যান্য অন্যায়কারীদের সাবধান করলেও

(বাকি অংশ ৩৯ পৃষ্ঠায়)

এটিএম কার্ডের নিরাপত্তা

(৭১ পৃষ্ঠার পর)

খোয়া যাওয়া সম্পদ ফিরে পাওয়ার নিরিখে এটা সেরা পদ্ধতি নাও হতে পারে। সেজন্য প্রতিরোধমূলক সুরক্ষা এবং এটিএম জালিয়াতি ঝুঁকির বীমা করাটাই মনে হয় সঠিক পদক্ষেপ।

সতর্কতা

* আপনার ব্যাংক লেনদেনের সাথে মোবাইল ফোন নম্বর এবং ই-মেইলকে যুক্ত করে রাখুন, যাতে সময়মতো এসএমএস ও ই-মেইল সতর্কবার্তা পেতে পারেন।

* আর্থিক সংস্থা বা ব্যাংক কখনই অনলাইনে আপনার ব্যাংকের বিষয়ে তথ্য জানতে চেয়ে ই-মেইল পাঠাবে না।

* নিয়মিত ক্রেডিট কার্ড ও ব্যাংক অ্যাকাউন্টের বিবরণ পরীক্ষা করুন এবং আপনার লেনদেনগুলোর হিসাব রাখুন।

* আপনার পরিচিতির বিষয়গুলো, যেমন : ঠিকানার পরিবর্তন যথাযথ রাখুন, যাতে চেক বই, বিবরণী, ডেবিট/ক্রেডিট কার্ড সঠিক ঠিকানায় পান।

* ফিশিং আক্রমণ ঠেকানোর জন্য ব্রাউজারটিকে ফিশিংরোধী হতে হবে। কখনই লেনদেন বা উন্নীতকরণের জন্য ই-মেইলের কোনো সূত্রে ক্লিক করবেন না।

* এমন একটি পাসওয়ার্ড নির্বাচন করুন, যা শক্ত অথচ সহজে মনে রাখতে পারবেন। এটিকে নিয়মিত পরিবর্তন করুন।

* ভিশিং হলো ফিশিংয়েরই একটি প্রকারভেদ, যা ই-মেইল পাঠিয়ে গ্রাহকদের প্রলুব্ধ করে গুরুত্বপূর্ণ তথ্যাদি নেয়ার চেষ্টা না করে, সরাসরি অথবা স্বয়ংক্রিয় পদ্ধতিতে ফোন করে ব্যাংক বা ক্রেডিট ইউনিয়নের গ্রাহকদের কাছ থেকে গুরুত্বপূর্ণ তথ্যাদি সংগ্রহ করে নেয়।

* ব্যাংক বা ক্রেডিটকার্ড পরিসেবা দানকারী সংস্থা ফোন করলে তাদের আপনার ব্যক্তিগত তথ্যাদি দেয়ার সময়ে নিজেকে সংযত রাখার চেষ্টা করুন।

* যেসব এটিএম মেশিন স্বাভাবিক লাগছে না, যেমন দেখতে অদ্ভুত কোনো যন্ত্রাংশ অথবা মেশিনে লাগানো কোনো তার ইত্যাদি থেকে সাবধান থাকুন।

* 'নো টেম্পারিং' ফলক দেখুন। অনেক সময় বদমাইশ লোকজন এই ফলক লাগিয়ে রাখে, যাতে কেউ নতুন কোনো যন্ত্রাংশ সম্পর্কে সন্দেহ না করেন।

* জ্যাম হয়ে যাওয়া এটিএম মেশিন থেকে দূরে থাকুন, এগুলো গ্রাহকদের বাধ্য করে অন্য কোনো এটিএম মেশিন ব্যবহার করতে, যেগুলোতে নকল করার যন্ত্র লাগানো আছে। প্রায়শই অপরাধীরা এলাকার অন্যান্য এটিএম মেশিনগুলো অকেজো করে দেয় যাতে ব্যবহারকারীরা অন্য এমন একটি এটিএম মেশিন ব্যবহার করতে যান, যেখানে নকল করার যন্ত্র লাগানো আছে।

* গ্রাহকদের উচিত ব্যাংক অ্যাকাউন্ট নিয়মিত পরীক্ষা করে দেখা তাতে কোনো অবৈধ লেনদেন আছে কি না। যুক্তরাষ্ট্রীয় আইন এটিএম জালিয়াতি থেকে উদ্ভূত ক্ষতির পরিমাণ নির্দিষ্ট করে দিয়েছে এবং বিভিন্ন ব্যাংক অতিরিক্ত কিছু সুরক্ষার ব্যবস্থাও করেছে। গ্রাহকদের উচিত নিজ নিজ আর্থিক সংস্থার সাথে যোগাযোগ করে এ ব্যাপারে বিস্তারিত জেনে নেয়া।

* যদি আপনি এটিএমের আশপাশে কোনো অস্বাভাবিক বা সন্দেহজনক কিছু দেখেন বা আপনার ব্যাংক অ্যাকাউন্টে অবৈধ কোনো লেনদেন দেখেন, তবে সাথে সাথে তা স্থানীয় আইন রক্ষাকর্তাদের এবং আপনার আর্থিক সংস্থা এবং/অথবা এটিএম যেখানে বসানো আছে সেখানে জানান।

* আপনার পিন সর্বদা সুরক্ষিত রাখুন। এই নম্বরটি কাউকে দেবেন না এবং পিন টাইপ করার সময় কিপ্যাডটি ঢাকা দিয়ে নেবেন।

ফিডব্যাক : *jabedmorsheda@yahoo.com*