

বাংলাদেশে গত এক দশকে অনলাইন ব্যাংক সেবা ব্যাপকভাবে বেড়েছে। সাম্প্রতিক সময়ের ব্যাংক কার্যক্রম সনাতন রীতি থেকে বেরিয়ে ডিজিটাল ডিভাইসনির্ভর হয়ে পড়ছে। বাংলাদেশে তিনটি ধাপে চলছে ডিজিটাল ব্যাংকিং। এর মধ্যে সীমিতসংখ্যক ব্যাংকেই রয়েছে ইন্টারনেট ব্যাংকিং। এরপরই রয়েছে ‘প্লাস্টিক মানি’ সেবা। বাড়ছে সেলফোনের মাধ্যমে অর্থ লেনদেনের সুবিধা। ইন্টারনেট ব্যাংকিংয়ে ইন্টারনেটে সংযুক্ত হয়ে ব্যাংকের নির্দিষ্ট সুরক্ষিত ওয়েবসাইটের মাধ্যমে গ্রাহক তার ব্যাংক

বাড়ছে। সম্প্রতি ৫০টি জালিয়াতির ঘটনা বিশ্লেষণ করে দেখা যায়, এর মধ্যে প্রযুক্তিনির্ভর জালিয়াতির ঘটনা বাড়ছে। বিশেষ করে এটিএম বুথ ও মোবাইল ব্যাংকিং সংক্রান্ত জালিয়াতির ঘটনা উল্লেখযোগ্য হারে বেড়েছে। সম্প্রতি সোনালী ব্যাংকের অনলাইন অ্যাকাউন্ট থেকে আড়াই লাখ মার্কিন ডলার লুটের ঘটনাও বেশ চাঞ্চল্য সৃষ্টি করেছে। এছাড়া ব্র্যাক ব্যাংকের একটি ঘটনা এবং নিয়মিতভাবে বিকাশের মাধ্যমে প্রতারণার নানা খবরে নতুন করে আলোচিত হচ্ছে অনলাইন ব্যাংকিং। আর তাই সঙ্গত কারণেই আলোচিত হচ্ছে অনলাইন লেনদেনে আমরা কীভাবে নিরাপদ

গ্রাহকের উচিত তার নিজের পাসওয়ার্ড দ্বিতীয় কারও সাথে শেয়ার না করা। এতে এমনিতেই ঝুঁকিমুক্ত থাকবেন গ্রাহক। একই সাথে যেহেতু প্রযুক্তি প্রতিনিয়ত আপডেট হচ্ছে এবং এটি একটি ‘প্রকৌশলগত’ ঝুঁকি, সেহেতু সংশ্লিষ্ট কর্মকর্তাদের নিয়মিত প্রশিক্ষণ এবং বিশেষজ্ঞের পরামর্শকের প্রয়োজনীয়তাও বোধ করছে অনেক ব্যাংকারই। অপরদিকে টেকসই প্রযুক্তির কার্যকর প্রয়োগের ওপর গুরুত্ব দিয়ে ব্যাংকগুলোর নিজস্ব ওয়েবসাইটের বাগ বা নিরাপত্তা ত্রুটি যাচাই করার পরামর্শ দিয়েছেন বিশেষজ্ঞেরা। তারা মনে করেন, কেন্দ্রীয় ব্যাংকের পক্ষ থেকে অফলাইনের মতো অনলাইনেও অডিটের ব্যবস্থা রাখা উচিত। ইন্টারনেট ব্যাংকিংয়ের ক্ষেত্রে তিন স্তরের নিরাপত্তা ব্যবস্থা থাকলেও দক্ষতার সাথে অ্যাপ্লিকেশনের ব্যবহার, নেটওয়ার্ক ম্যানেজমেন্ট এবং এক্সট্রানীল সিকিউরিটি নিশ্চিত করতে পারলে অঘটনের আশঙ্কা কমে আসবে।

কোর ব্যাংকিংয়ের ক্ষেত্রে দেশের ব্যাংকগুলো যথেষ্ট নিরাপদ অবস্থায় আছে। পরিপূর্ণভাবে ন্যাশনাল পেমেন্ট সুইচ (এনপিসি) চালু করা হলে অনলাইন ব্যাংকিংয়ের ঝুঁকি থাকবে না বললেই চলে। আর মোবাইল ব্যাংকিংয়ের ক্ষেত্রে ব্যাংকের সাথে তৃতীয় পক্ষ জড়িত থাকায় এখানে কিছুটা ঝুঁকি দেখা দিয়েছে। তবে গ্রাহকের সচেতনতা বাড়ানো এবং প্রযুক্তি-দক্ষ ব্যাংকার গড়ে তুলতে পারলে অনলাইন ব্যাংকিং পুরোপুরি নিরাপদ থাকবে। অপরদিকে অনলাইন লেনদেন নিরাপদ রাখতে প্রতিটি ব্যাংককে অন্তত ‘টু’ ফ্যাক্টর পরিপালনের ওপর গুরুত্ব দিতে হবে। নেটওয়ার্ক সিকিউরিটি নিশ্চিত করতে নিজস্ব সিকিউরিটি ভিপিএন তৈরি করতে হবে।

সবচেয়ে ঝুঁকির মধ্যে থাকা মোবাইল ব্যাংকিং ব্যবস্থাকে নিরাপদ করতে দেশে ‘পে ওয়েল’ নামে একটি সার্ভিস চালু করছে ক্লাউড ওয়েল লিমিটেড। পে ওয়েল যেকোনো মোবাইল ব্যাংকিং ওয়ালেট থেকে ঝুঁকিবিহীন লেনদেনের সুবিধা দেবে। ফোনের পরিবর্তে পজ মেশিন দিয়ে নিয়ার ফিল্ড কমিউনিকেশন পদ্ধতিতে টাকা লেনদেন বা কেনাকাটার সুযোগ করে দিচ্ছে। এ ক্ষেত্রে নিরাপত্তা ব্যবস্থা জোরদার করতে ফোর লেয়ার সিকিউরিটি ব্যবস্থা নেয়া হয়েছে। এজন্য প্রতিটি মেশিনের একটি আইএমআই নম্বর, এমএসআইএসডিএন ও রিটেইলার আইডি এবং র্যান্ডম পিনকোর্ড ভেরিফাই করে লেনদেন করতে হবে। লেনদেন প্রক্রিয়া নিরাপদ করার পাশাপাশি অনলাইন ব্যাংকিংয়ে ইউএএসবি টোকেন, স্মার্টফোনের মাধ্যমে সফট-টোকেন এবং ফিজিক্যাল ডিভাইস হার্ডটোকেন, প্রতিটি লেনদেনের সময় এসএমএসভিত্তিক সিকিউরিটি ব্যবস্থা নিশ্চিত করা জরুরি। অনলাইন ব্যাংকিং নিরাপদ রাখতে সংশ্লিষ্ট ব্যাংকারদের প্রযুক্তির ব্যবহার বিষয়ে পারদর্শী করে তুলতে উচ্চতর প্রশিক্ষণের ব্যবস্থা, দক্ষ জনশক্তি গড়ে তোলা এবং সর্বোপরি গ্রাহকদেরকে সচেতন করে তুলতে হবে। একই সাথে নিয়মিত হিসাব মনিটরিংয়ের ওপরও গুরুত্ব দিতে হবে।

(বাঁকি অংশ ৭০ পৃষ্ঠায়)

## ব্যাংক খাতের প্রযুক্তি নিরাপত্তা অবস্থান ও করণীয়

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

অ্যাকাউন্টে প্রবেশ করেন।

এজন্য ব্যাংকের পক্ষ থেকে সাধারণত একটি আইডি ও পাসওয়ার্ড সরবরাহ করা হয়। ইন্টারনেট ব্যাংকিংয়ে হিসাবের অনুসন্ধান, নিজের একাধিক অ্যাকাউন্টে অর্থ স্থানান্তর, বিদ্যুৎ, পানি, গ্যাস, ফোন, মোবাইল, ইন্টারনেট ইত্যাদি ইউটিলিটি বিল পরিশোধ, চেক বইয়ের জন্য আবেদন ও পেমেন্ট বাতিল করা যায়। আন্তঃব্যাংক কার্যক্রমের মাধ্যমে ফান্ড ট্রান্সফার করা গেলেও প্রাইম ব্যাংক ছাড়া বাংলাদেশে এখনও অন্য কোনো ব্যাংকের হিসাবে অর্থ স্থানান্তরের সুবিধা নেই। অর্থাৎ এটি শুধু একটি ব্যাংকের মধ্যে সীমাবদ্ধ। তবে ভারতে এই সুযোগ সুবিধা NEFT এবং RTGS-এর মাধ্যমে পাওয়া যায়। ফান্ড ট্রান্সফার, মোবাইল টপআপ, সেলফোনে লেনদেনের তাৎক্ষণিক তথ্য পাঠানোর বিষয়টিই অনলাইন লেনদেনের মধ্যে মুখ্য।

ডিজিটাল ব্যাংকিংয়ের দ্বিতীয় ধাপে রয়েছে ‘প্লাস্টিক মানি’ সেবা। নগদ অর্থ বহনের ঝুঁকি এবং সহজ প্রাপ্যতার সীমাবদ্ধতা কাটিয়ে তাই দিন দিন জনপ্রিয় হয়ে উঠছে ডেবিট ও ক্রেডিট কার্ড। বিদায়ী বছরে আরও একধাপ এগিয়ে অনলাইন ব্যাংকিংয়ে যুক্ত হয়েছে মোবাইল ব্যাংকিং সেবা। মোবাইল ব্যাংকিং নামে পরিচিত এই সেবায় ব্যবহার হচ্ছে সেলফোন নেটওয়ার্ক। প্লাস্টিক কার্ডের জায়গায় বিস্তৃত হচ্ছে ব্যাংকিং লেনদেন অনুমোদিত ‘সিমকার্ড’।

তবে ব্যাংকগুলো পর্যাপ্ত নিরাপত্তা নিশ্চিত করতে পারছে না। এতে গ্রাহকেরা জালিয়াতির শিকার হচ্ছেন। তাদের অর্থ লুট হচ্ছে। ব্যাংকের অনলাইন বা প্রযুক্তি বিভাগে যারা কাজ করেন, তাদের বেশিরভাগেরই এ সম্পর্কে পর্যাপ্ত জ্ঞান নেই। ফলে পেশাগত দায়িত্ব পালনের গুরুত্ব সম্পর্কে তারা সচেতন নন। এছাড়া ব্যাংকগুলোও প্রয়োজনীয় প্রশিক্ষণ দিচ্ছে না। এসব কারণে ব্যাংকিং খাতে অনলাইন জালিয়াতির ঘটনা

থাকতে পারি প্রসঙ্গটি।

সচেতনতা, উচ্চতর দক্ষতা আর খ্রিডি সিকিউরিটি ব্যবস্থা শতভাগ নিশ্চিত না হওয়ায় অনলাইন ব্যাংকিং কার্যক্রম বাড়লেও বাড়ছে নিরাপত্তা ঝুঁকি। আর এই ঝুঁকি সবচেয়ে বেশি দেখা দিয়েছে মোবাইল ব্যাংকিংয়ে। এছাড়া ব্যাংকের ডাটাবেজের সুরক্ষার অভাব, অনলাইন ব্যাংকিংয়ে তৃতীয় পক্ষের ওপর নির্ভরশীলতা, অনলাইন ব্যাংকিং ঝুঁকিমুক্ত করতে গ্রাহক ও স্টাফদের উচ্চতর প্রশিক্ষণের ব্যবস্থা না থাকা এবং গ্রাহকদের মধ্যে সচেতনতা গ্রহণে উদ্যোগ না নেয়ায় সম্প্রতি অনলাইন ব্যাংকিংয়ে প্রতারণা ও জালিয়াতি বাড়ছে।

অনলাইন ব্যাংকিংয়ে তিনটি ক্ষেত্রেই ‘গ্রাহকের গোপন নম্বর’ গোপন না থাকা কিংবা তা চুরি হয়ে যাওয়াটাই বড় প্রতিবন্ধকতা হিসেবে দেখা দিচ্ছে। কোর ব্যাংকিংয়ের ক্ষেত্রে সমস্যা প্রকট না হলেও এডিসিএলের ক্ষেত্রেই নিরাপত্তার ঝুঁকিটা বেশি। এ ক্ষেত্রে এসএমএস মাসকিং, পিন নম্বর চুরি, বুথ থেকে পাসওয়ার্ড হাতিয়ে নেয়া এবং মোবাইল নম্বর মাসকিং ও ফ্রড কলের মতো ঘটনা ঘটেছে। এক গবেষণা মতে, গত তিন মাসে ৭ থেকে ৮ শতাংশ হারে মোবাইল ব্যাংকিংয়ে অপরাধ বেড়েছে। মোট সাইবার অপরাধের প্রায় ১৬ শতাংশই ঘটছে বাণিজ্যিক কারণে। বেশিরভাগ ক্ষেত্রেই ব্যালাস চেক না করে শুধু এসএমএস দেখেই টাকা পরিশোধ করে ক্ষতিগ্রস্ত হচ্ছেন সংশ্লিষ্ট গ্রাহক।

আগামী দিনে স্বাভাবিকভাবেই অনলাইন ব্যাংকিং কার্যক্রম ব্যাপক হারে বেড়ে যাবে, সে ক্ষেত্রে ঝুঁকিও বেড়ে যাবে কয়েকগুণ। কীভাবে অনলাইন লেনদেনের ঝুঁকি মোকাবেলা করা যায় এবং এজন্য ব্যাংকগুলোইবা কী উদ্যোগ নিচ্ছে, সে বিষয়ে সংশ্লিষ্টদের বক্তব্য প্রায় অভিন্ন। এ ক্ষেত্রে গ্রাহকদের মধ্যে পাসওয়ার্ড শেয়ার করার প্রবণতাকে দায়ী করে ব্যাংকারেরা বলছেন,