অনলাইন ব্যাংকিং ঝুঁকি ও ব্যবহারকারীর প্রয়োজনীয় সতর্কতা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

ইন্টারনেটের মাধ্যমে ব্যাংকিং কার্যক্রমকে সাধারণত ইন্টারনেট ব্যাংকিং বা অনলাইন ব্যাংকিং বলা হয়। এক্ষেত্রে ইন্টারনেটে যুক্ত হয়ে ব্যাংকের নির্দিষ্ট সুরক্ষিত ওয়েবসাইটের মাধ্যমে একজন গ্রাহক তার ব্যাংক অ্যাকাউন্টে প্রবেশ করেন। অ্যাকাউন্টে প্রবেশের জন্য ব্যাংক গ্রাহককে প্রয়োজনীয় তথ্য (সাধারণত একটি আইডি ও পাসওয়ার্ড) সরবরাহ করে। গ্রাহক সেই প্রয়োজনীয় ও গোপনীয় তথ্য ব্যবহার করে ব্যাংকের নির্দিষ্ট ওয়েবসাইট ব্যবহার করে তার ব্যাংকিং কার্যক্রম পরিচালনা করেন। অনলাইন ব্যাংকিং আর্থিক লেনদেনকে অনেক সহজ করে দেয়। এতে সময় বাঁচে ও ঝামেলা কমে যায় অনেকটা। ছিনতাইয়ের মতো ঘটনাও এড়ানো যায় সহজেই। এতে স্ট্যান্ডিং অর্ডারগুলো সেটআপ করা যায়, ব্যবসায়িক লেনদেনের জন্য অন্য লোকের অ্যাকাউন্টে টাকা পাঠানো যায়, চেকবুকে অর্ডার করা যায়। এমনকি সাধারণ লেনদেনের বাইরেও কিছু বাড়তি সুবিধা দিয়ে থাকে অনলাইন ব্যাংকগুলো। এ জন্যই অনলাইন ব্যাংকগুলো সারাবিশ্বে এত জনপ্রিয়। তবে ধীরে ধীরে বিশ্বজুড়ে অপরাধীদের আক্রমণের প্রধান লক্ষ্যবস্তুও হয়ে উঠছে এটি।

বাংলাদেশে গত এক দশকে অনলাইন ব্যাংকিং সেবা ব্যাপকভাবে বেড়েছে। তবে ব্যাংকগুলো পর্যাপ্ত নিরাপত্তা নিশ্চিত করতে পারছে না। এতে গ্রাহকেরা জালিয়াতির শিকার হচ্ছেন। তাদের অর্থ লুট হচ্ছে। অনেক সময় ব্যাংক কর্মকর্তাদেরও এসব অপকর্মের সাথে জড়িত থাকার প্রমাণ মিলছে। ব্যাংকের অনলাইন বা প্রযুক্তি বিভাগে যারা কাজ করেন, তাদের বেশিরইভাগেরই এ সম্পর্কে পর্যাপ্ত জ্ঞান নেই। ফলে পেশাগত দায়িত্ব পালনের গুরুত্ব সম্পর্কে তারা সচেতন নন। ব্যাংকগুলোও প্রয়োজনীয় প্রশিক্ষণ দিচ্ছে না। আবার নানা কারণে কর্মকর্তারা প্রতিষ্ঠানের প্রতি অসন্তুষ্ট হয়ে পড়েন। এসব কারণে ব্যাংকিং খাতে অনলাইন জালিয়াতির ঘটনা বাড়ছে। সাম্প্রতিককালের 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।

অনলাইন ব্যাংকিংয়ে নানা ধরনের নিরাপত্তা ঝুঁকি রয়েছে। যেমন ফিশিং, যেখানে একজন ধোঁকাবাজ ব্যবহারকারীদেরকে ই-মেইল করে থাকে। এরা নিজেদেরকে বৈধ কোনো প্রতিষ্ঠানের কর্মী বলে পরিচয় দেয়। যাদের মেইল ঠিকানাসহ প্রায় সব বিষয়ই আপনার পরিচিত বৈধ প্রতিষ্ঠানটির মতোই মনে হবে। এরা তাদের অফিসিয়াল কাজে লাগবে এই বলে ব্যবহারকারীর লগইন ডিটেলস চায়। অথবা তাদের ফিশিং সাইটটিতে ঢুকতে বলবে, যা দেখতে প্রায় বৈধ প্রতিষ্ঠানের ওয়েবসাইটের মতোই মনে হবে। এতে মেইলে উল্লিখিত বিষয়ের প্রয়োজনে লগইন ডিটেলস দিতে হয়, যা ধোঁকাবাজদের ওয়েবসাইটে তথ্যগুলো দিয়ে দেয়া ছাড়া আর কিছুই নয়। কিন্তু সুখের বিষয়, এ ধরনের ঝুঁকি থেকে মুক্ত থাকার জন্য কিছু কার্যকর ব্যবস্থা রয়েছে।

ক. ঝুঁকিমুক্ত অনলাইন ব্যাংকিংয়ের জন্য ব্যাংকগুলো কী কী ব্যবস্থা নিতে পারে?

০১. প্রথমেই ইউজার আইডি, পাসওয়ার্ড ও টোকেন/স্মার্টকার্ডগুলোর নিরাপত্তা নিশ্চিত করতে হবে।

০২. স্ট্যান্ডার্ড ১২৮ বিট সিকিউর সকেট লেয়ারের (এসএসএল) মাধ্যমে গ্রাহকের ইন্টারনেট ব্যাংকিং সেশন এনক্রিপ্ট করতে হবে। এটি গ্রাহককে নিশ্চিত করবে, ডাটাগুলো তার কমপিউটার থেকে বের হওয়ার আগেই তা এনকোডেট হয়ে বের হবে।

০৩. নিরাপত্তা বলয়ের চূড়ান্ত ধাপে গোপনীয়তা রক্ষায় সক্ষম এ ধরনের মাল্টিপল ফায়ারওয়াল স্থাপন করতে হবে। সম্পূর্ণ অনলাইন স্থাপনাটি ব্যাংকের নেটওয়ার্ক ও নিরাপত্তা কর্মকর্তারা অবিরাম মনিটর করবেন এবং যদি সিস্টেমে কোনো অবৈধ অনুপ্রবেশকারী ঢুকতে চেষ্টা করে, তাহলে সাথে সাথে অ্যালার্ম বেজে উঠবে।

০৪. সবচেয়ে সেরা অ্যান্টিভাইরাস ইনস্টল করতে হবে এবং তা নিয়মিত আপডেট করতে হবে।

০৫. সিস্টেম অ্যাডমিনদের জন্য সর্বোত্তম পাসওয়ার্ড পলিসি অবলম্বন করতে হবে।

০৬. নিয়মিতভাবে নিরাপত্তা প্যাচসহ অপারেটিং সিস্টেম আপডেট করতে হবে।

০৭. নিয়মিতভাবে সর্বশেষ নিরাপত্তা ঝুঁকি সম্পর্কে পরীক্ষা-নিরীক্ষা করতে হবে এবং অনলাইন নিরাপত্তা ঝুঁকি সম্পর্কেও আপডেট থাকতে হবে।

খ. ঝুঁকিমুক্ত থাকতে গ্রাহকরা কী করতে পারেন?

০১. গ্রাহকের পিসিতে একটি ভালোমানের অ্যান্টিভাইরাস বা অ্যান্টিস্পাইওয়্যার ইনস্টল করতে হবে। বাজারে নরটন, ক্যাস্পারস্কি, জায়ান্ট, মেকাফি, ট্রেন্ড মাইক্রোর মতো ভালোমানের অ্যান্টিভাইরাস পাওয়া যায়।

০২. অ্যান্টিভাইরাস ডেফিনেশন নিয়মিতভাবে আপডেট করতে হবে।

০৩. কোম্পানি বা পারসোনাল ফায়ারওয়াল ইনস্টল করতে হবে।

০৪. মাইক্রোসফটের মতো কোম্পানিগুলো নিয়মিতভাবে প্যাচসহ তাদের অপারেটিং সিস্টেমের আপডেট রিলিজ করে থাকে, যা অপারেটিং সিস্টেমের নিরাপত্তা বাড়িয়ে থাকে। নির্দিষ্ট সময় পরপর অপারেটিং সিস্টেমের আপডেট সম্পর্কে খোঁজখবর নিতে হবে এবং প্রয়োজনে ডাউনলোড সেকশন থেকে তা ডাউনলোড করে আপ-টু-ডেট থাকতে হবে।

০৫. এসএসএল এনাবল ব্রাউজার ব্যবহার করতে হবে, যা ১২৮ বিট এনক্রিপশন সাপোর্ট করে (ইন্টারনেট এক্সপ্লোরার বা তার পরের ভার্সন/নেটসক্যাপ ৪.৭৫ বা পরের ভার্সন/যেকোনো ব্রাউজার, যা ১২৮ বিট এসএসএল এনক্রিপশন সাপোর্ট করে)।

০৬. লগইন ইনফরমেশন টাইপ করার আগে (লগইন ইউজার আইডি/পাসওয়ার্ড/স্মার্টকার্ড পিন/ভাসকো টোকেন পিন) দুটি বিষয় পরীক্ষার মাধ্যমে নিরাপদ চ্যানেল প্রতিষ্ঠা হওয়ার বিষয়টি নিশ্চিত হতে হবে। প্রথমত নিশ্চিত হতে হবে, আপনার ব্যাংক অ্যাড্রেস শুরু হচ্ছে এইচটিটিপিএস//(এইচটিটিপির পরে 'এস' থাকে); দ্বিতীয়ত স্ক্রিনের নিচের দিকে আনব্রোকেন কী অথবা ক্লোজড প্যাডলক দেখা যাবে (প্যাডলকের পজিশন ব্রাউজার টু ব্রাউজার পরিবর্তন হতে পারে)। এ প্যাডলকে ক্লিক করলে 'ব্যাংক সার্ভার অথেনটিকেশন সার্টিফিকেট' দেখা যাবে।

০৭. আপনি যখন সরাসরি ব্যাংক অ্যাড্রেসে লগইন করতে চান, তখন অবশ্যই সংশ্লিষ্ট ডোমেইন নেম ওয়েব ব্রাউজারে টাইপ করতে হবে, কোনো লিঙ্ক অথবা ই-মেইল বা অন্য কোনো ওয়েবসাইটের রিডিরেশন অনুসরণ করবেন না।

০৮. আপনি যদি স্মার্টকার্ড ব্যবহারকারী হন, তবে ব্যবহার শেষ হওয়ার সাথে সাথে কার্ডটি কার্ড রিডার থেকে বের করে ফেলুন।

গ. নিরাপদ রাখার জন্য গ্রাহকদের যা কখনও করা উচিত নয়

০১. পাবলিক বা শেয়ার পিসি থেকে অনলাইন ব্যাংকিং কার্যক্রম থেকে বিরত থাকতে হবে।

০২. লগইন ইনফরমেশন (আইডি/পাসওয়ার্ড/সিকিউরিটি টোকেন পিন/স্মার্টকার্ড পিন/ভাসকো সিরিয়াল নাম্বার) লিখিত বা মৌখিকভাবে কারও সাথে শেয়ার করবেন না।

০৩. পাসওয়ার্ড এবং আইডি কোথাও লিখে রাখবেন না (যেমন কিবোর্ড, ডেস্ক, নোটবুক, পিসির হার্ডডিস্ক, কোনো পোর্টেবল ডিভাইস তথা মোবাইল, থাম্ব ড্রাইভ, ডিসকেট, সিডি ইত্যাদি)।

০৪. লগইন ইনফরমেশন কাউকে ই-মেইল বা ফোনে পাঠাবেন না।

০৫. এমন কোনো ই-মেলের উত্তর দেয়া যাবে না, যাতে আপনার অনলাইন ব্যাংকিং সাইটের লিঙ্ক দেয়া থাকবে বা আপনার লগইন ইনফরমেশন চেয়ে অনুরোধ করা হবে।

ঘ. সবচেয়ে সেরা বিষয়গুলো, যেগুলোর সাথে গ্রাহকদের মানিয়ে নেয়া উচিত

০১. গ্রাহকদেরকে অবশ্যই নিম্নলিখিত পাসওয়ার্ড পলিসি মেনে চলতে হবে :
ক. নিয়মিতভাবে আপনার পাসওয়ার্ড পরিবর্তন করতে হবে (অন্তত মাসে একবার)।
খ. এমন পাসওয়ার্ড ব্যবহার করবেন না, যা সহজেই খুঁজে পাওয়া যায় বা অনুমান করা যায়। যেমন আপনার ইউজার আইডি, টেলিফোন নাম্বার, জন্ম তারিখ বা অন্য কোনো ব্যক্তিগত তথ্য।
গ. পাসওয়ার্ড হতে হবে ন্যূনতম ৮ ডিজিটের।
ঘ. এটি নিশ্চিত করতে হবে, আপনার পাসওয়ার্ডটির মধ্যে যাতে বড় হাতের (A, B, ...) ও ছোট হাতের (a, b, ...) অক্ষর, নাম্বার (1, 2, ...) এবং বিশেষ অক্ষর (@, *, -) থাকে।
ঙ. পাসওয়ার্ডে ধারাবাহিক অক্ষর বা নাম্বার (যেমন abcdef, 12345) অথবা একই নাম্বার বা অক্ষর দু'বারের বেশি ব্যবহারের বিষয়টি (যেমন mmssee, ১২৩২২) পরিহার করা উচিত।
চ. পাসওয়ার্ডে নাম, পারিবারিক নাম, জন্ম দিন, টেলিফোন নাম্বার বা এ ধরনের ডাটা পরিহার করা উচিত।
ছ. যদি আপনার পাসওয়ার্ডটি প্রকাশ হয়ে গেছে বলে মনে হয়, তাহলে সাথে সাথে তা পরিবর্তন করে ফেলুন।
জ. পাসওয়ার্ড পরিবর্তনের সময় লক্ষ রাখতে হবে, নতুন পাসওয়ার্ডটি যেনো সর্বশেষ ৮টি পাসওয়ার্ডের কোনোটির সাথেই না মিলে।
ঝ. বিভিন্ন ফিন্যান্সিয়াল বা নন-ফিন্যান্সিয়াল ওয়েবভিত্তিক সার্ভিসের (যেমন ই-মেইল, অনলাইন শপিং, ডিজিটাল আইডেন্টিফিকেশন এবং অন্যান্য অনলাইন সাবক্রিপশন সার্ভিস ইত্যাদি) জন্য ভিন্ন ভিন্ন পাসওয়ার্ড ও পিন ব্যবহার করতে হবে।
০২. সিকিউরিটি টোকেন (ভাসকো) ও স্মার্টকার্ড সবসময় নিরাপদে রাখুন।
০৩. অটো কমপ্লিট অপশন ডিজ্যাবল করুন (এটি পাসওয়ার্ড সংরক্ষণ করতে পারে, যা অন্যরা ব্যবহার করতে পারবেন)।
০৪. ফাইল এক্সটেনশন (.doc, .jpeg etc) খুঁজে দেখুন। যেহেতু ডাবল এক্সটেনশন ফাইলগুলো সাধারণত ভাইরাস হয়ে থাকে, তাই এগুলো ডিলিট করে দিন।
০৫. অপরিচিত কারও মেইল অ্যাটাচমেন্ট খোলা থেকে বিরত থাকুন। জাঙ্ক বা চেইন মেইল ডিলিট করুন।
০৬. অজ্ঞাত কোনো উৎসের সফটওয়্যার বা প্রোগ্রাম পিসিতে ইনস্টল করা থেকে বিরত থাকুন। বিশ্বস্ত কোনো উৎসের সফটওয়্যার বা প্রোগ্রাম না হলে, তা পিসিতে রান করা থেকে বিরত থাকুন।
০৭. আপনি যখনই পিসি থেকে উঠে যাবেন, তখনই অনলাইন সেশন থেকে লগঅফ করুন।
০৮. মাঝেমধ্যে ব্যাংক অ্যাকাউন্ট ব্যালেন্স পরীক্ষা করা উচিত ও কোনো অসংলগ্নতা দেখলে সাথে সাথে ব্যাংকে রিপোর্ট করুন।
০৯. কোম্পানির ল্যান নেটওয়ার্কের বাইরে কোনো ফাইল শেয়ার করবেন না, বিশেষ করে যখন মডেম, ব্রডব্যান্ড বা ওই ধরনের কোনো মাধ্যমে ইন্টারনেটে যুক্ত থাকবেন।
১০. যেকোনো কন্টাক্ট ডিটেলস পরিবর্তন হলে সাথে সাথে ব্যাংকে জানান, যাতে ব্যাংক আপনাকে সময়মতো যেকোনো তথ্য জানাতে পারে।

ঙ. যথাযথ সচেতনতা প্রয়োগ করুন ও ব্যাংকে জানান

০১. আপনি এমন কোনো ই-মেইল পান যাতে আপনার লগইন ইনফরমেশন চেয়ে অনুরোধ করা হয় (আইডি/পাসওয়ার্ড/সিকিউরিটি টোকেন পিন/স্মার্টকার্ড পিন/ভাসকো সিরিয়াল নাম্বার ইত্যাদি)।
০২. অনলাইন ব্যাংকিং সাইটের লিঙ্কসহ যদি এমন কোনো ই-মেইল পান, যাতে আপনার লগইন ইনফরমেশন চাওয়া হতে পারে।
০৩. আপনি যখন অনলাইন ব্যাংকিং করছেন, তখন আপনার কাছে যদি কোনো ধরনের সন্দেহজনক কিছু মনে হয়।
০৪. এ লেখায় যে ধরনের নিরাপত্তা ফিচারগুলো উল্লেখ করা হয়েছে, তার যেকোনোটি যদি ওয়েবসাইটে না দেখেন (যেমন ব্রাউজারের নিচের কর্নারে লক সাইন না দেখা, লক সাইনে ক্লিক করলে বৈধ সার্টিফিকেট প্রদর্শন না করা বা সাইটটি যদি এইচটিটিপিএস//-এর পরিবর্তে এইচটিটিপি// দিয়ে শুরু হয় ইত্যাদি)।
০৫. আপনি যদি প্রায় একই ধরনের ভুয়া সাইট দেখতে পান কজ

ফিডব্যাক : jabedmorshed@yahoo.com

আইওএস ৭

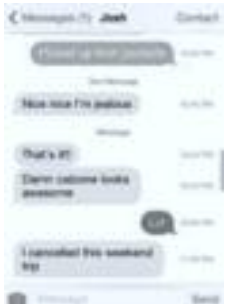
(৭৫ পৃষ্ঠার পর)

এর ফলে বর্তমানে অসংখ্য অ্যাপ তৈরি ও ধারণ করা যাবে।

আইওএস ৭-কে অধিকতর রিডেবল করা

আইওএস ৭ চালু করেছে নতুন সিস্টেমওয়াইড ফন্ট, যা Helvetica Neue হিসেবে পরিচিত। এ ফন্টটি চমৎকার, তবে আগের আইওএসে ব্যবহার হওয়া ফন্টের চেয়ে বেশ সূক্ষ্ম বা পাতলা। যদি কোনো আইটেমকে আপনার ডিভাইসে সামান্য বেশি রিডেবল করতে চান, তাহলে ফন্টকে বোল্ট করতে পারবেন। এ জন্য আপনাকে Settings→General→Accessibility অপশনে গিয়ে পজিশন অপশনে Bold Text-এ টোগাল করতে হবে।

সিরি আগের যেকোনো সময়ের চেয়ে বেশি শক্তিশালী



আইওএস ৭-এ আপনি সিরি-কে ব্যবহার করতে পারবেন বেশ কয়েকটি কাজে, যা আগে সম্ভব ছিল না। উদাহরণস্বরূপ, আপনি সিরি-কে ব্যবহার করতে পারবেন বিভিন্ন সিস্টেম ওয়াইড সেটিংয়ে টোগাল করার জন্য, যেমন ওয়াই-ফাই, স্ক্রিন ব্রাইটনেস ও ব্লুটুথে। আপনি ইচ্ছে করলে সিরি-কে ব্যবহার করতে পারেন আইটিউন রেডিও স্টেশন তৈরি করতে এবং টুইটার ও উইকিপিডিয়ার মতো সাইটে সার্চ করতে পারবেন। এ ছাড়া আপনি সিরি-কে ব্যবহার করতে পারবেন টুইটারে কী ধরনের প্রবণতা চালু আছে তা খুঁজে বের করতে।

প্রত্যেক মেসেজের জন্য ভিউ টাইমস্ট্যাম্পস

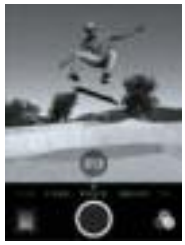
মেসেজ অ্যাপের ক্ষেত্রে ভিউটাইমস্ট্যাম্পস এক চমৎকার নতুন ফিচার হলেও এটি তেমন ব্যাপক সাড়া ফেলতে বা নজর কাড়তে পারেনি। আপনি প্রতিটি মেসেজের জন্য স্বতন্ত্র টাইমস্ট্যাম্পস খুব সহজে চেক করে দেখতে পারবেন যেগুলো সেন্ড এবং রিসিভ করবেন যেকোনো টেক্সট আলোচনায় সুইপ করার মাধ্যমে।

ক্যামেরা অ্যাপে বারস্ট মোড

যথা সময়ে যথাযথ ছবি তোলা কখনো কখনো এক চ্যালেঞ্জিং কাজ হয়ে ওঠে। তাই আইওএস ৭ -এ এ সমস্যা উত্তরণের জন্য চালু করা হয় Burst Mode নামের এক ফিচার।

ক্যামেরা অ্যাপ থেকে ক্যামেরায় শাটারে প্রেস করুন যেমনটি আপনি সাধারণত করে থাকেন, তবে এক্ষেত্রে শাটার চেপে ধরে থাকতে হবে। এর পরপরই আইওএস দ্রুতগতিতে ১০টি ছবি তুলবে এবং যে ছবিটি আপনার দৃষ্টিতে দেখতে সবচেয়ে সুন্দর সে ছবিটিকে বেছে নেয়ার সুযোগ দেবে। তাছাড়া আপনি যদি সিদ্ধান্ত নিতে না পারেন সেরা ছবিটি বেছে নেয়ার ক্ষেত্রে, তাহলেও আইওএস ৭ আপনাকে সহায়তা করবে সেরা ছবিটি নির্বাচন করার ক্ষেত্রে।

সিরির ভয়েজ পরিবর্তন করা



সিরি দৃশ্যে প্রথম মানানসই হয়ে আবির্ভূত হয় আইফোন ফোর এ। এরপর থেকে সিরি ফিচার ব্যাপকভাবে উন্নত থেকে উন্নততর হতে থাকে। আইওএস ৭-এ সিরির একটি নতুন ফিচার হলো একজন মানুষের ভয়েজ প্রদান করা। একাজটি করার জন্য Settings→ General এ এক্সেস করুন এবং তারপর Siri সিলেক্ট করুন। এখান থেকে Voice Gender অপশনে ট্যাব করতে হবে সিরির ভয়েজকে মানানসই ভয়েজে পরিণত করার জন্য কজ

ফিডব্যাক : mahmood_sw@yahoo.com