HSBC

অনলাইন সুরক্ষা এবং সুরক্ষিত ব্যবহার সংক্রান্ত পথনির্দেশিকা

এখানে রইল কিভাবে আমরা একত্রে আপনার অনলাইন ব্যাঙ্কিং সুরক্ষিত রাখতে আপনাকে সাহায্য করতে পারি।

ব্যাঙ্ক হিসাবে, আমরা সুরক্ষার ব্যাপারে ভাবনাচিন্তা করতে অভ্যস্ত। ইন্টারনেটের বিকাশ আমাদের সকলের জন্যে অধিক নমনীয় সুবিধা প্রদান করেছে, কিন্তু সাথে নতুন-নতুন ঝুঁকি নিয়ে এসেছে যার বিরুদ্ধে অবশ্যই সতর্ক থাকতে হবে। এইচএসবিসি'তে, আমরা যেকোন অননুমোদিত প্রাপ্ততা থেকে আপনার অ্যাকাউন্টকে সুরক্ষিত রাখতে তিনটি মুখ্য ক্ষেত্র - গোপনীয়তা, প্রযুক্তি এবং শনাক্তকরণের ওপর আলোকপাত করে, শিল্পোদ্যোগ মানক সুরক্ষা প্রযুক্তি এবং রীতিসমূহ ব্যবহার করি।

আসুন এটা পড়ে দেখুন কিভাবে আমরা আপনার অনলাইন ব্যাঙ্কিং সুরক্ষা করি এবং আপনার নিজস্ব অনলাইন সুরক্ষা উন্নত করতে আপনিও কি কি পদক্ষেপ নিতে পারেন।

প্রতারণার নানা প্রকার

এমন অনেক উপায় আছে যার দ্বারা প্রতারক আপনাকে প্রতারণা করে তাকে আপনার ব্যক্তিগত এবং সুরক্ষা বিবরণ দেওয়ার চেষ্টা করাতে পারে। তারপর তারা এইসব বিবরণ ব্যাঙ্কের সঙ্গে আপনার আর্থিক তথ্য প্রাপ্ততায় ব্যবহার করে এবং আপনার অ্যাকাউন্ট থেকে তাদের অ্যাকাউন্টে পেমেন্টের বন্দোবস্ত করে নেয়।

ক্রেডিট/ডেবিট কার্ড স্কিমিং/ক্লোনিং

আপনার ক্রেডিট বা ডেবিট কার্ডের চুম্বকীয় পট্টি থেকে তথ্য চুরি করতে পারে। তারা এটিএম'র কার্ড স্লটে স্কিমার ডিভাইসকে লুকিয়ে রাখার দ্বারা বা মার্চেন্ট পেমেন্ট টার্মিনালে আপনার মনোযোগ না দেওয়ার ক্ষেত্রে এটা করে। এইসব ডিভাইস আপনার কার্ডের বিবরণ স্ক্যান এবং মজুত করে। আপনার পিন চুরি করতে, প্রতারকরা এটিএম'য়ে বা বাণিজ্যিক প্রতিষ্ঠানে একটা বিচক্ষণ জায়গায় ক্যামেরা রাখতে পারে।

ইউপিআই অ্যাপ্লিকেশনে কেলেঙ্কারি বা পেমেন্ট প্রতারণা

প্রতারকরা আপনাকে মেসেজিং অ্যাপ্লিকেশনের মাধ্যমে QR কোড পাঠিয়ে, আপনাকে QR কোড স্ক্যান করতে বা প্রতারকের অ্যাকাউন্টে টাকা ট্রান্সফার করার 'Collect' অনুরোধ অনুমোদন করতে বলতে পারে। ওরা মিথ্যে কাহিনী শুনিয়ে আপনাকে ফাঁদে ফেলার চেষ্টা করতে পারে এই বলে যে আপনি, বিক্রী করছেন যে প্রোডাক্ট সেটা তারা কিনতে চায়। তারা ব্যাঙ্ক বা শপিং কোম্পানীর একজন এগজিকিউটিভের ভান ক'রে, আপনার জন্যে রিফাণ্ড, দাবিহীন ক্যাশব্যাক অফার বা রিওয়ার্ড পয়েন্টস প্রসেস করার অফার দেবে। নিঃসন্দেহ হয়ে এই ফাঁদে পড়া ব্যক্তি তখন হয়ত QR কোড স্ক্যান করে বা নিজের UPI PIN ব্যবহার ক'রে 'Collect' অনুরোধ অনুমোদন করে, যেটা পক্ষান্তরে প্রতারকের অ্যাকাউন্টে অর্থ হস্তান্তর করে।

বাণিজ্যিক ই-মেইল এবং মেসেজিং অ্যাপ্লিকেশনের মাধ্যমে পেমেন্ট প্রতারণা

প্রতারকরা আপনার সম্বন্ধে অধিক জানতে আপনার ই-মেইল বা চ্যাটসমূহে হ্যাক করতে বা আনএনক্রিপ্টেড মেসেজ ইন্টারসেপ্ট করতে পারে। একবার তারা আপনার সম্বন্ধে অধিক জানলে, তারা হ্যাক করা/আপস করা/নকল করা আইডি থেকে মেসেজ পাঠিয়ে, আপনার প্রিয়জনের হাসপাতালে ভর্তি বা বকেয়া বিল যেটা একটা নতুন অ্যাকাউন্টে পেমেন্ট করার দরকার হবে এমন আপাতদৃষ্টিতে বৈধ উদ্দেশ্যের জন্যে আপনাকে জরুরি পেমেন্ট করার কথা বলতে পারে। প্রতারিত ব্যক্তিরা বিশ্বাস বা জরুরিতার কারণে ফাঁদে পড়ে প্রতারকের অ্যাকাউন্টে পেমেন্ট করে দিতে পারেন। আর প্রতারিত ব্যক্তিরা নিজেরাই পেমেন্ট করছেন বলে, লেনদেনের সতর্কতার দ্বারা তাঁরা সতর্কিত হবেন না, যেটা তাঁদেরকে ব্যাঙ্ক পাঠায়। এই ধরণের প্রতারণার সন্ধান করা কঠিন।

নকল যোগাযোগের নাম্বার :

প্রতারকরা ব্যাঙ্ক বা পরিষেবা প্রদানকারী যোগাযোগ কেন্দ্রের নকল যোগাযোগের বিবরণ প্রদান করতে পারে। সন্দেহ না করা প্রতারিত ব্যক্তিরা একটা সার্চ ইঞ্জিন ব্যবহার করে যোগাযোগের বিবরণ দেখে এবং নকল নাম্বারে কল করতে পারেন। তারপর তাঁরা একটা ''যাচাইকরণ প্রক্রিয়ার'' মধ্যে দিয়ে যাবেন, যেখানে তাঁরা ফাঁদে পড়ে নিজেদের ডেবিট*ক্রেডিট কার্ড এবং ব্যাঙ্ক অ্যাকাউন্টের ব্যাপারে সংবেদনশীল তথ্য ভাগীদারি করবেন। আপনার প্রয়োজনীয় যোগাযোগের বিবরণ দেখার জন্যে আপনি সর্বদা ব্যাঙ্ক বা পরিষেবা প্রদানকারীর অফিসিয়াল ওয়েবসাইট দেখে নিশ্চিত করে নিজেকে রক্ষা করতে পারেন। সজাগ থাকুন এবং প্রথমে চেক না করে, সন্ধান করা ফলাফলে প্রদর্শিত নাম্বারে কল করা এড়ান, বিশেষতঃ মোবাইল নাম্বার হলে।

ফিশিং বা স্পুফিং ই-মেইল

প্রতারকরা যতটা পারেন অনেক ই-মেইল ঠিকানায় একটা ই-মেইল পাঠানোর দ্বারা প্রতারিত ব্যক্তিদের ফিশ করতে পারে। তারা এটা প্রায়শঃ একটা ব্যাঙ্ক, অনলাইন পেমেন্ট সার্ভিস, রিটেলার বা অন্য সমরূপ পরিষেবার মতো একটা বৈধ সংস্থার অংশ হবার ভান করেন। তারা নিজেদের আইডি স্পুফ করতে পারে, যাতে ই-মেইল প্রতারকরা নিজেরা ছাড়া অন্য কারোর দ্বারা পাঠানো হয়েছে এমন দেখতে মনে হবে।

ব্যক্তিগত বা আর্থিক তথ্য জিজ্ঞেস করা ই-মেইলের প্রতি সাড়া না দেওয়ার দ্বারা ফিশিং স্ক্যামের বিরুদ্ধে আপনি নিজেকে রক্ষা করতে পারেন। সন্দেহজনক ই-মেইলে আপনি কখনোই লিঙ্কস সিলেক্ট করবেন না।

এইচএসবিসি কখনোই ই-মেইল মারফৎ আপনার ব্যক্তিগত বা সুরক্ষা বিবরণ প্রকাশ করতে আপনাকে বলবে না। এইচএসবিসি থেকে দাবি করা এমন ই-মেইল আপনি প্রাপ্ত করলে, তার প্রতি সাড়া দেবেন না। ই-মেইল অবিলম্বে মুছে ফেলবেন। আর মনে রাখুন, কখনোই আপনার প্রমাণপত্রাদি - যেমন আপনার পদবি, পাসওয়ার্ড বা অন্যান্য বিবরণ কারোর সঙ্গে শেয়ার করবেন না।

মানি মিউল বা অতিরিক্ত আয় ই-মেইল কেলেঙ্কারী

একটা মানি মিউল কেলেঙ্কারীতে, প্রতারকরা অর্থ হস্তান্তর সহযোগে সাহায্যের জন্যে আপনাকে বলতে পারে। তারা আপনার অ্যাকাউন্টে অর্থ হস্তান্তর করা অফার করতে পারে, যাতে আপনি আরেকটা অ্যাকাউন্টে এই অর্থ হস্তান্তরে তাদেরকে সাহায্য করতে পারেন। পরিবর্তে, তারা আপনাকে একটা কমিশন দেবে বলবে।

আপনাকে এমনসব অনুরোধ অগ্রাহ্য করতে হবে, যেহেতু তারা অর্থ পাচারের মতো অপরাধে প্রায়শঃ জড়িত থাকে। কোনও ব্যক্তি যিনি জেনেশুনে অংশ নেন, তিনি অপরাধ সম্পন্ন করেছেন বিবেচিত হবে এবং মামলার সম্মুখীন হবেন। যদি কোনও অনুরোধ অত্যন্ত ভাল লাগে, তাহলে সম্ভবতঃ এটা একটা প্রতারণা!

অগ্রিম ফী প্রতারণা (''419''কেলেঙ্কারী)

প্রতারকরা অবাঞ্ছিত পত্র বা ই-মেইল বার্তা পাঠাতে পারে। যেটাতে তারা আপনাকে সাধারণতঃ ইউএস ডলারে, বিপুল পরিমাণ অর্থ স্থানান্তর করায় তাদের সাহায্য করার জন্যে একটা উদার পুরস্কার অফার করে। আসলে এইসব প্রতারক আপনার ব্যাঙ্কিং বিবরণ পেতে চায়। তারা সাধারণতঃ আপনাকে সওদা সম্পূর্ণ করতে ফী, কিছু কর বা ঘুষ পে করতে বলবে - এটা হলো অগ্রিম ফী। সাধারণতঃ এটা প্রতারিতদের লোকসান ঘটাবে।

কারোর কাছে আপনার অনলাইন ব্যাঙ্কিং বিবরণ আছে সন্দেহ হলে, আপনাকে অনলাইন ব্যাঙ্কিং লগ অন এবং অবিলম্বে আপনার পাস ওয়ার্ড বদলাতে হবে। আমাদের সতর্ক করতে যত শীঘ্র সম্ভব আপনি আমাদের কল করবেন। আমাদের লাইন 24/7* পাওয়া যায়। আপনি এখানে আমাদের হটলাইন নাম্বারগুলোর তালিকা পাবেন।

সোশ্যাল মিডিয়া হ্যাকস

প্রতারকরা ফেসবুক, হোয়াটসঅ্যাপ বা ইনষ্টগ্রামের মতো সোশ্যাল মিডিয়া প্ল্যাটফর্মে ছদ্মবেশী ঘনিষ্ট বন্ধু বা আত্মীয় হিসাবে জরুরি ভিত্তিতে আপনাকে অর্থ হস্তান্তর করতে বলতে পারে। এক্ষেত্রে আপনি জানেন এমন কাউকে কল করার দ্বারা বা অন্যান্য চ্যানেল মাধ্যমে যোগাযোগ করে তাঁর থেকে অনুরোধ ন্যায়সঙ্গত কিনা পরীক্ষা করতে পারেন।

ভিশিং কল

প্রতারকরা ছদ্মবেশী ব্যাঙ্ক ষ্টাফ বা কাষ্টমার সার্ভিস একজিকিউটিভ হতে পারে এবং সম্ভাব্য প্রতারিতদের কল করতে পারে সংবেদনশীল তথ্য যেমন তাঁদের ব্যাঙ্ক অ্যাকাউন্ট বিবরণ চুরি করতে। একজন প্রতারিতের বিশ্বাস জয় করতে, অপরাধীরা প্রতারিতকে অল্প ব্যক্তিগত তথ্য দিতে পারে যা সোশ্যাল ইঞ্জিনিয়ারিং মাধ্যমে চুরি করা হয়েছে। প্রতারিতদের কিছুটা বিশ্বাস স্থাপন হওয়ার পর, প্রতারকরা কিছু বিশেষ সার্ভিস বা প্রোডাক্ট অফার করতে পারে, এই আশায় যে প্রতারিতরা নিজেদের ব্যাঙ্ক বিবরণ এবং এককালীন পাসকোডস (OTPs)-এর মতো গোপন তথ্য প্রদান করবেন। ব্যাঙ্কের কল সেন্টারে যোগাযোগ করে তাঁর থেকে অনুরোধ ন্যায়সঙ্গত কিনা পরীক্ষা করতে পারেন, কোনও তথ্য শেয়ার করার আগে।

ট্রোজান ভাইরাস

প্রতারকরা আপনাকে ফাইলস, পেজেস বা অ্যাটাচমেন্টস সম্বলিত অযাচিত ই-মেইলস পাঠাতে পারে, যেটা আপনাকে ওপেন করতে বলবে। কিন্তু ওগুলো ওপেন করা মানে আপনার কম্প্যুটারে অজ্ঞাতসারে একটা প্রোগ্রাম ইনষ্টল হবে, যেটা আপনার অনলাইন কার্যকলাপ, এমনকি বিভিন্ন ওয়েবসাইটে আপনি কি টাইপ করছেন নিরীক্ষণ করে। তাই অনলাইন শপিংয়ের সময় আপনার ক্রেডিট কার্ড বিবরণ আপনি এন্টার করার ক্ষেত্রে, প্রতারকরা আপনার এন্টার করা তথ্য দেখতে সক্ষম হবে।

অনলাইন সুরক্ষার জন্যে এইচএসবিসি নানা পদক্ষেপ গ্রহণ করেছে

বহু-স্তরীয় লগঅন যাচাইকরণ

আপনার আর্থিক তথ্য একটা অনন্য ব্যবহারকারীর নাম এবং পাসওয়ার্ডের সঙ্গে-সঙ্গে আপনার বাস্তবিক সিকিউরিটি ডিভাইস বা ডিজিটাল সিকিওর কি'র দ্বারা তৈরী হওয়া একটা এককালীন সুরক্ষা কোডের একটা বাস্তবধর্মী সমন্বয়ের দ্বারা সুরক্ষিত হয়।

লেনদেন যাচাইকরণ

কার্ডের ওপর 3D সুরক্ষিত লেনদেন, পেমেন্ট সিষ্টেমে লেনদেন এবং বিশ্বাস সুরক্ষিত করায় সাহায্য করে। লেনদেনের জন্যে তৈরী হওয়া OTPs কখনো কারোর সঙ্গে শেয়ার করবেন না।

128-বিট সিকিওর সকেট লেয়ার (SSL) এনক্রিপশন

ইন্টারনেট ব্যাঙ্কিং সেশন চলাকালীন তথ্য প্রেরিতের জন্যে এইচএসবিসি ব্যবহার করে 128-বিট সিকিওর সকেট লেয়ার (SSL) এনক্রিপশন, যেটা এনক্রিপশনের জন্যে ইণ্ডাষ্ট্রী ষ্ট্যাণ্ডার্ড হিসাবে প্রচলিত।

স্বয়ংক্রিয় 'টাইম-আউট' বৈশিষ্ট্যতা

সুরক্ষা পদক্ষেপ হিসাবে, আপনার ইন্টারনেট ব্যাঙ্কিং সেশন স্বয়ংক্রিয়ভাবে বন্ধ বা টাইম-আউট হয়ে যাবে ব্যবহৃত না হওয়ার একটা সময়কাল পর। আপনার কাজ শেষ হয়ে যাওয়ার ক্ষেত্রে সব সময় আপনার ইন্টারনেট ব্যাঙ্কিং সেশন বন্ধ করে দেবেন।

সুরক্ষা সাধন / ডিজিটাল সুরক্ষিত চাবিকাঠি

আপনার বাস্তবিক সুরক্ষা সাধন / ডিজিটাল সুরক্ষিত চাবিকাঠি উচ্চতর পর্যায়ে অনলাইন সুরক্ষা নেয়। আপনার অ্যাকাউন্টে লগ অন করতে আপনার দরকার স্বাভাবিক মতো আপনার বিদ্যমান থাকা ব্যবহারকারীর নাম এবং পাসওয়ার্ড, এর অনুসরণে আপনার বাস্তবিক সুরক্ষা সাধন বা ডিজিটাল সুরক্ষিত চাবিকাঠির

দ্বারা তৈরী হওয়া অনন্য সুরক্ষা কোড এন্টার করা। এই 2-পর্যায় প্রমাণীকরণ প্রক্রিয়া আপনার ইন্টারনেট ব্যাঙ্কিং প্রাপ্ততার ক্ষেত্রে সুরক্ষার একটা বর্ধিত মাত্রা আপনাকে প্রদান করে।

অনলাইন সুরক্ষায় আপনার ভূমিকা

ইন্টারনেট ব্যাঙ্কিং সুরক্ষা সুনিশ্চিত করতে এইসব করণীয় এবং অকরণীয় অভ্যাস করুন

করণীয়

- সব সময় আপনার কম্প্যুটার লেটেষ্ট অ্যান্টি-ভাইরাস এবং ফায়ারওয়াল সুরক্ষা সহযোগে সুরক্ষিত হওয়া সুনিশ্চিত করুন। আপনার লেটেষ্ট সুরক্ষা থাকা সুনিশ্চিত করতে নিয়মিতরূপে ডাউনলোড আপডেট করুন।
- এমন এক পাসওয়ার্ড বেছে নিন যেটা আপনার কাছে স্মরণযোগ্য কিন্তু অন্য কারোর দ্বারা আন্দাজ করা সহজ নয়। বর্ণমালা এবং সংখ্যাসূচক অক্ষরসমূহের সমন্বয় সম্বলিত পাসওয়ার্ড সাধারণতঃ আন্দাজ করা কঠিন হয় (যেমন a7g3cy91)।
- নিয়মিত ভিত্তিতে আপনার ইন্টারনেট ব্যাঙ্কিং পাসওয়ার্ড পরিবর্তন করুন।
- ফিশিং ই-মেইলস থেকে সাবধান। সব সময় সমস্ত অক্ষর এবং সংখ্যা সমেত সমগ্র ই-মেইল ঠিকানা মন দিয়ে পড়ুন।
- অত্যন্ত সমরূপ দেখতে ই-মেইল ঠিকানাসমূহ ফিশিং করা হয়। যেমন hsdc.co.in বা hsbcbank.com. এর প্রকৃত গন্তব্যস্থল উন্মোচন করতে URL-এর ওপর আপনার মাউস পয়েন্টার রোল করান ; এটা আপনার ব্রউসারের বাঁদিকের নীচের কোণায় প্রদর্শিত হয়। অমিল হলে লিঙ্কে ক্লিক করবেন না। সেক্ষেত্রে URL'য়ে বানান ভুল, মন্দ ব্যাকরণ বা গোলমেলে অক্ষরসমূহের মতো লক্ষণগুলোর জন্যে সতর্ক হোন।
- আর প্রয়োজন না থাকলে, আপনার অ্যাকাউন্ট থেকে অ্যাডেড বেনিফিসিয়ারীজ মুছে ফেলুন।
- আপনার কম্প্যুটার বা ব্রউসার্সে কার্যকারিতা নিষ্ক্রিয় করুন, যদি না আর প্রয়োজন হয়।
- আপনার সিষ্টেম এবং ওয়েব ব্রউসার আপডেটেড রাখুন। নির্মাতারা নিয়মিতরূপে সুরক্ষা প্যাচেস প্রকাশ করে, যখন তাদের সিষ্টেমস এবং ব্রউসার্সে দুর্বলতা আবিষ্কৃত হয়। নিয়মিত ভিত্তিতে এইসব আপডেটের জন্যে আপনার সফ্টওয়্যার প্রদানকারীর কাছে পরীক্ষা করুন।
- এইচএসবিসি ওয়েবসাইটে পৌঁছতে সব সময় ব্রউসারে আমাদের URL টাইপ করুন।
- প্যাডলক সিম্বল এবং সাইট সার্টিফিকেট পরীক্ষা করুন। এইচএসবিসি'র অন্তর্ভুক্ত সাইট সার্টিফিকেট সুনিশ্চিত করতে, এইচএসবিসি অনলাইন ব্যাঙ্কিংয়ে আপনি লগ-ইন করার ক্ষেত্রে আপনার ব্রউসারের তলায় প্যাডলক সিম্বলে ডবল-ক্লিক করুন। এটা 'জাল' সাইটে আপনার বিবরণ এন্টার করে আপনার প্রতারিত না হওয়া সুনিশ্চিত করবে।
- নিয়মিতরূপে আপনার অ্যাকাউন্ট পরীক্ষা করুন। কোনও লেনদেনের ব্যাপারে সন্দেহ থাকলে, বিবরণ লিখে নিন আর আমাদের কল করুন।
- অনলাইন ব্যাঙ্কিং ব্যবহার করার পর সব সময় লগ-আউট করুন। শুধু লগ-আউট বাটন সিলেক্ট করুন এবং সার্ভিসে আপনি লগ থাকার সময় কখনোই আপনার PC থেকে অনুপস্থিত থাকবেন না।
- আপনি ব্যাঙ্কের কাষ্টমার কেয়ার নাম্বার, অনলাইন শপিং ওয়েবসাইট ইত্যাদি খুঁজলে, ইন্টারনেটে বিচক্ষণতার সঙ্গে সন্ধান করুন। প্রতারক তাদের প্রচালনা করা মোবাইল নাম্বার্স সহযোগে ফলাফলগুলো ফেরৎ দিতে সন্ধানগুলো হেরফের করে। আপনি হয়ত ব্যাঙ্কের কাষ্টমার কেয়ার নাম্বার বা ই-কমার্স ওয়েবসাইটের পরিবর্তে প্রতারককে কল করার ফাঁদে পড়তে পারেন।
- আপনার ব্যাঙ্কের যোগাযোগ কেন্দ্রের নাম্বার আপনার ডিভাইসে ষ্টোর করুন বা আপনার ক্রেডিট/ডেবিট কার্ডের পিছনদিকে লেখা নাম্বার উল্লেখ করুন।
- আপনার পার্সোনাল কম্প্যুটার বা মোবাইল ডিভাইসে স্ক্রীন শেয়ারিং অ্যাপ্লিকেশন্সের ব্যাপারে সাবধান হবেন। প্রতারকরা এমনসব অ্যাপ্লিকেশন ডাউনলোড করা এবং আপনার থেকে কোড চাওয়ার দ্বারা অ্যাকসেস লাভ করার ফাঁদে আপনাকে ফেলতে পারে। একবার অ্যাকসেস অনুমোদনযোগ্য হলে, তারা দূর থেকে আপনার ডিভাইস দেখতে ও নিয়ন্ত্রণ করতে পারে, এমনকি আপনার অ্যাকাউন্ট থেকে পেমেন্ট সম্পন্ন করতেও পারে।
- আপনার ইন্টারনেট কানেকশন সুরক্ষিত করুন। সব সময় একটা পাসওয়ার্ড সহযোগে আপনার হোম ওয়্যারলেস নেটওয়ার্ক সুরক্ষা করুন।
- নানা স্কীম/অফারের ব্যাপারে সাবধান থাকুন, যেগুলোর আপনার অ্যাকাউন্টে অর্থ সংগ্রহ করতে আপনাকে দরকার, এমনকি কমিশন বা সাহায্যের জন্যেও। প্রতারকরা অপরাধের আয় আপনার অ্যাকাউন্টে পাঠাবে এবং আপনাকে অর্থ হস্তান্তর বা তাদেরকে নগদ দিতে বলবে। প্রতারক অর্থের পথে নিজেকে নিয়ে যেতে চায় না এবং আপনাকে মানি মিউল হিসাবে ব্যবহার করতে পারে।
- প্রতারণা জানাতে অবিলম্বে ব্যাঙ্কে যোগাযোগ করুন।

অকরণীয়

- এমন পাসওয়ার্ড বেছে নেবেন না যেটা আপনি অন্যান্য সার্ভিসের জন্যে ব্যবহার করেন। আপনার পাসওয়ার্ড ইন্টারনেট ব্যাঙ্কিংয়ের প্রতি অনন্য হতে হবে।
- আপনার ইউজারআইডি, পাসওয়ার্ড, কার্ড নাম্বার, অন্তিম তারিখ CVV ইত্যাদির মতো বিবরণ ওয়েবপেজে প্রকাশ করবেন না, যেটা ই-মেইল/SMS'য়ে লিঙ্ক অসাবধনতাবশতঃ ক্লিক হওয়ার ক্ষেত্রে ওপেন হয়।
- এমন বিবরণের জন্যে জিজ্ঞেস করা মেসেজের প্রতি সাড়া দেবেন না, এমনকি সেগুলো ব্যাঙ্কের কর্মচারীর থেকে বা সরকারি প্রতিষ্ঠান যেমন আয়কর দপ্তর, ভারতীয় রিজার্ভ ব্যাঙ্ক ইত্যাদির থেকে দাবি করলেও। এইচএসবিসি'র কোনও কর্মচারী এইসব বিবরণের জন্যে আপনাকে কখনোই কল বা জিজ্ঞেস করবেন না।

- আপনার পাসওয়ার্ডের সঙ্গে একত্রে আপনার ইন্টারনেট ব্যাঙ্কিং ব্যবহারকারীর নাম লিখবেন না। আপনার পাসওয়ার্ড একটা চেনার মতো আকারে লিখবেন না এবং কখনোই আপনার বাস্তবিক সুরক্ষা সাধন/ডিজিটাল সুরক্ষিত চাবিকাঠির সঙ্গে আপনার লগ অন বিবরণ কখনো ছেড়ে যাবেন না।
- আপনার মোবাইল ব্যাঙ্কিং অ্যাপ্লিকেশন আপডেটেড রাখুন। এটা ডাউনলোড এবং এটাতে কোনও আপডেট করতে, আপনার ডিভাইসের অফিসিয়াল অ্যাপ স্টোরে যাবেন।
- বিশ্বস্তহীন সূত্র থেকে ই-মেইলে লিঙ্ক থেকে মোবাইল ব্যাঙ্কিং/পেমেন্ট অ্যাপ্লিকেশন কখনো ডাউনলোড করবেন না।
- অনলাইন ওয়েবসাইটে আপনার কার্ড নাম্বার এবং অন্তিম তারিখ স্টোর করায় সাবধান হবেন। এইসব বিবরণ বিশ্বস্তহীন ওয়েবসাইট বা কদাচিৎ ব্যবহৃত ওয়েবসাইটে স্টোর করবেন না।
- অন্য কারোর সঙ্গে আপনার PIN কখনো শেয়ার করবেন না। এটা নিজের জন্যে ব্যবহার করুন। আপনার PIN আপস হয়েছে সন্দেহ করার হ'লে, এটা অবিলম্বে পরিবর্তন করবেন।

আপনাকে UPI PIN জিজ্ঞেস করলে, মনে রাখুন, আপনি একটা পেমেন্ট করছেন। একটা পেমেন্ট প্রাপ্ত করতে UPI PIN দরকার হয় না।

পাবলিক কম্প্যুটার ব্যবহার করার সময় সতর্ক থাকুন

সব সময়

- লগ আউট করুন, যদি আপনি কম্প্যুটার ছেড়ে যান, এমনকি যদি সেটা এক মুহূর্তের জন্যেও হয়। সম্ভব হলে, আপনি লগ ইন থাকার ক্ষেত্রে অনুপস্থিত থাকার অবস্থায় কম্প্যুটার ছেড়ে যাবেন না।
- আপনি কম্প্যুটার লগ আউট করার পূর্বে আপনার ব্রউসিং ইতিহাস মুছে ফেলুন : ইন্টারনেট ব্রউসার্স আপনার পাসওয়ার্ড এবং আপনার ভিজিট করা পেজেস সম্বন্ধে তথ্য স্টোর করে। ইন্টারনেট ব্রউসারের টুলস মেন্যুতে যান এবং অপশন্স বা ইন্টারনেট অপশন্স সিলেক্ট করুন। ব্রউসারে কোনও অটো কমপ্লিট ফাংশন অফ করা আছে কিনা নিশ্চিত হোন, যেকোন কুকিজ মুছে ফেলুন, আর ইতিহাস খালি করে দিন।
- লাইব্রেরী, ইন্টারনেট কাফে এবং স্কুলে যারা থাকে তারা সমেত, এটাতে আপনি সাহায্য করতে পারলে, আপনার ব্যাঙ্কিং করতে পাবলিক কম্প্যুটার ব্যবহার করা এড়াতে চেষ্টা করুন।

সংবেদনশীল তথ্য টাইপ করা এড়ান। এমনকি আপনি সব সাবধানতা পালন করলেও, একটা পাবলিক কম্প্যুটারে কিস্ট্রোক লগার নামক বিদ্বেষপরায়ণ সফ্টওয়্যার ইনষ্টল করা থাকতে পারে। এইসব প্রোগ্রাম আপনার পাসওয়ার্ড, ক্রেডিট কার্ড নাম্বার এবং ব্যাঙ্ক বিবরণ চুরি করতে পারে। সংবেদনশীল তথ্য উন্মোচন করবে এমন যেকোন আর্থিক লেনদেন করা এড়ান।

গুরুত্বপূর্ণ - আপনি কখনো এইচএসবিসি থেকে দাবি করা বিশ্বস্তহীন সূত্র থেকে ই-মেইল প্রাপ্ত করলে বা একটা অযাচিত ই-মেইল আপনার ব্যক্তিগত তথ্য চাইলে, সেগুলোর আগে তদন্ত করতে আমাদের জন্যে **phishing@hsbc.com**'য়ে রিপোর্ট করুন।