সতর্ক থাকুন
এবং অভ্যাস করুন
নিরাপদ ব্যাঙ্কিং ব্যবস্থার

ব্যাঙ্কিং ধ্যায়ান সে

AXIS BANK

অ্যাক্সেস ব্যাঙ্ক দ্বারা এক গ্রাহক পরিষেবার উদ্যোগ

স্বীকৃতি

এই ডকুমেন্টটি প্রস্তুত করা হয়েছে ‘এ বুকলেট অন মোদাস অপার‍্যান্ডী অফ ফাইনান্সিয়াল ফ্রডস্টার্স’-এর মূল পরিযোজনাতে যা প্রকাশিত হয়েছে আরবিআই অমবাডস্ম্যান-এর কার্যালয়ে (মুম্বাই II) মহারাষ্ট্র, গোয়া এবং এই বিষয়ে আমাদের কিছু ইন-হাউস গবেষণার তথ্যের ভিত্তিতে।

মুখবন্ধ

ব্যাঙ্কিং সিস্টেমের ডিজিটাইজেশন গ্রাহকদের সহজে এবং দ্রুতভাবে তাঁদের আর্থিক চাহিদা পূরণে এক নতুন দিগন্ত খুলে দিয়েছে। বর্তমানের পরিস্থিতি আমাদের উৎসাহিত করে যতটা সম্ভব ডিজিটাল হতে যাতে শারীরিক এবং সামাজিক যোগাযোগ কম করা যায়।

আমরা ডিজিটাল ব্যাঙ্কিংয়ের বেড়ে ওঠা সুবিধে যখন আমরা উপভোগ করছি, তখন এছাড়াও আমাদের সচেতন থাকতে হবে সাইবারক্রাইম এবং ব্যাঙ্কিং প্রতারণার বিষয়ে। বেশিরভাগ ক্ষেত্রে, গ্রাহকরা সচেতন না থাকার জন্য প্রতারিত হতে পারেন এবং তার ফল স্বরূপ আর্থিকভাবে ক্ষতিগ্রস্ত হতে হয় যদি তাঁরা এই ব্যাপারে যত্নশীল না হন।

অ্যাক্সেস ব্যাঙ্কে, আমরা আপনার যত্ন নিয়ে থাকি এবং আমরা চেষ্টা করি আপনার চাহিদাগুলোর বিষয়ে নিরাপদে সর্বদা নজর রেখে আপনাকে সাহায্য করতে সময়ে সময়ে গুরুত্বপূর্ণ তথ্যগুলো সরবরাহ করার মাধ্যমে।

এই ডকুমেন্টে আমাদের উদ্দেশ্য হলো সচেতনাবোধ জাগ্রত করা এবং আপনাদের পরিচিতি করানো সন্দেহজনক এবং প্রতারণামূলক কাজকর্মের সঙ্গে যাতে করে তা আজ প্রতিরোধ করা যায়। আমরা মেনে চলবো কিছু লক্ষণীয় কার্যক্রম যা আপনাকে সাহায্য করবে কিভাবে এই ধরনের কাজগুলিকে শনাক্ত করতে, প্রতিরক্ষামূলক কি ধরনের ব্যবস্থা গ্রহণ করবেন এবং কিভাবে তা রিপোর্ট করবেন। এইভাবে সতর্ক থাকলে আপনি এইরকম প্রতারণার শিকার হওয়ার সুযোগ কম করতে পারবেন এবং আর্থিক ক্ষতির হাত থেকে রেহাই পাবেন।

আমরা ভরসা রাখি আপনি এই তথ্যগুলিকে উপযোগী মনে করবেন এবং আপনি উপভোগ করতে পারবেন এক নিরাপদ এবং বিরামহীন ব্যাঙ্কিং অভিজ্ঞতা, যখন আপনি করবেন ব্যাঙ্ক *ধ্যায়ান সে*।

নিরাপদ থাকুন!

এখানে কিছু সাধারণ সতর্কতামূলক ব্যবস্থা এবং ভালো অভ্যাসের কথা বলা হল:

এড়িয়ে চলুন

- অসুরক্ষিত ওয়েবসাইট সাক্ষাৎ বা অপরিচিত ব্রাউজার ব্যবহার
- পাবলিক ডিভাইসে পাসওয়ার্ড সেভ করা
- ফিনান্সিয়াল / কনফিডেন্সিয়াল ই-মেল পাবলিকভাবে ব্যবহার বা ফ্রী নেটওয়ার্ক ব্যবহার
- অপরিচিত উৎস থেকে পাওয়া সন্দেহজনক দেখতে পপ আপস,লিঙ্কস এবং ই-মেলে ক্লিক করা
- ই-মেল এবং অপরিচিত ওয়েবসাইটে সুরক্ষিত শংসাপত্র বা পাসওয়ার্ডস সংরক্ষণ
- ব্যক্তিগত তথ্যাবলি অপরিচিত ব্যক্তির সঙ্গে সোস্যাল মিডিয়াতে শেয়ার করা
- ব্যাঙ্কিং এবং অন্যান্য লেনদেনের একই পাসওয়ার্ড ব্যবহার করা
- অপরিচিত অ্যাপ্লিকেশন্স বা সফ্টওয়্যার ইনস্টল করা
- আপনার মোবাইল বা অন্যান্য ইলেক্ট্রনিক যন্ত্রগুলিকে বা অ্যাপগুলিকে আনলকর্ড রাখা

কখনও নয়

- আপনার পিন (পার্সোনাল আইডেন্টিফিকেশন নম্বর), পাসওয়ার্ড, ক্রেডিট বা ডেবিট কার্ড নম্বর, সিভিভি, চেকবুকের কপি, কেওয়াইসি বিবরণ কাউকে কখনও দেবেন না
- অপরিচিত ডিভাইস থেকে কোনও সংবেদনশীল বা গোপনীয় তথ্যাবলি স্টোর করবেন না

সর্বদা

- আপনার ফোনকে এক শক্তিশালী স্ক্রিন পাসওয়ার্ডে সুরক্ষিত রাখুন
- ব্যবহার করুন দুটি-বিষয়ে অথেনটিকেশন যখনই অ্যাপ্লিকেশন / অ্যাভেলেবল ব্যবহার করবেন
- ইন্টারনেট ব্যাঙ্কিং সেশন সঙ্গে সঙ্গে লগ আউট করুন ব্যবহার করার পরে
- ব্যবহার করুন অ্যানেবল বা ডিজাবল ফিচার বা বৈশিষ্ট্যাবলি এবং সেট-আপ ট্রান্সঅ্যাক্ট আইকন লিমিটস আপনার কার্ডে বা অ্যাকাউন্টে আপনার ব্যবহারের ভিত্তিতে
- ওয়েবসাইটে সিকিউরিটি যাচাই করুন সিকিউরিটি সংকেত দেখে যেমন padlock বা https
- অনলাইনের পেমেন্টের জন্য ব্যবহার করুন সিকিয়র পেমেন্ট গেটওয়েজ
- শক্তিশালী পাসওয়ার্ড রক্ষা করুন যা আবশ্যকভাবে অ্যালফানিউমেরিক এবং বিশেষ ক্যারেক্টারের সংমিশ্রণে এবং তা পরিবর্তন করুন নিয়মিতভাবে
- ব্যবহার করুন ভারচুয়াল কীবোর্ড পাবলিক ডিভাইসে যেহেতু কীস্ট্রোক্স এছাড়াও ধরা যায় কমপ্রোমাইজড ডিভাইস, কীবোর্ড, ইত্যাদিতে
- আপনার ডিভাইসে ইনস্টল করুন অ্যান্টিভাইরাস এবং অ্যান্টি-স্পাইওয়ার, সেগুলিকে আপ-টু-ডেট রাখুন এবং আপডেট ইনস্টল করুন যখন পাওয়া যাবে
- যে-কোনও ইউএসবি ড্রাইভস স্ক্যান করুন / ডিভাইসে স্টোরেজ করুন ব্যবহারের আগে
- আপনার মোবাইল অ্যাপ সুরক্ষিত রাখুন পাসওয়ার্ডে বা কনসীল রাখুন নর্মাল ভিউতে আপনার মোবাইল ফোনে লুকনো স্পেস বৈশিষ্ট্য ব্যবহার করে

#BankingDhyaanSe

অনলাইন / ওয়েবসাইট প্রতারণার সম্পর্কে (1)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী
আপনি কিভাবে সতর্ক এবং নিরাপদ থাকবেন?

অনলাইন পরিচালনা

কিভাবে করা হয়

- প্রতারকরা একটা হুবহু একইরকম ব্যাঙ্কের আসল ওয়েবসাইটের মতো একটা ওয়েবসাইট তৈরী করে
- ওয়েবসাইট লিঙ্কড ছড়িয়ে দেওয়া হয় এসএমএস, সোস্যাল মিডিয়া, ই-মেল ইত্যাদির মাধ্যমে
- এই লিঙ্কগুলো এক্কেবারে আসল ওয়েবসাইটের মতো দেখায় এবং এটি তৈরী করা হয় আপনাকে ফাঁদে ফেলার জন্য। আপনার শংসাপত্র বা সুবেদী এবং গোপনীয় তথ্যবলি এন্টার করা হলে এইসব লিঙ্কে না দেখে এবং ইউআরএল বিবরণ না চেক করে
- যখন আপনি আপনার শংসাপত্র এই ওয়েবসাইটে এন্টার করবেন, তখন সেগুলি ধরা যাবে এবং অপব্যবহৃত হবে প্রতারক দ্বারা

নিরাপত্তার টিপস

- অপরিচিত লিঙ্কগুলো এড়িয়ে চলুন এমনকি এইগুলো আসলের মতো দেখতে হলেও
- কোনও আর্থিক পরিচয়পত্র এন্টার করার আগে ওয়েবসাইটের বিবরণ দেখে নিন

অনলাইন প্রতারণা

কিভাবে করা হয়

- প্রতারক অনলাইনে ন্যায়সঙ্গত ক্রেতা / বিক্রেতা বলে ভান করেন, ইকমার্স প্ল্যাটফর্মে
- আপনার প্রোডাক্টে তারা উৎসাহ দেখান বা প্ররোচিত করার চেষ্টা করেন তাদের থেকে কেনার জন্য অনেক ডিসকাউন্ট বা ইনসেনটিভ দেবেন বলে
- পেমেন্ট করার সময়ে তারা প্রলোভন দেখান ইউপিআই 'রিকোয়েস্ট মানি'-এর আইকন সিলেক্ট করার জন্য যার দ্বারা আপনার ব্যাঙ্ক অ্যাকাউন্ট থেকে টাকা তুলে নেওয়ার চেষ্টা করেন

নিরাপত্তার টিপস

- অনলাইনের প্রোডাক্টে আর্থিক লেনদেন করার জন্য যত্নবান হোন
- আপনি কখনও আপনার পিন বা পাসওয়ার্ড এন্টার করবেন না কোনও টাকা পেতে

#BankingDhyaanSe

অনলাইন / ওয়েবসাইট প্রতারণার সম্পর্কে (2)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী
আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

সন্দেহভাজন সার্চ করার ফলাফল

কিভাবে করা হয়

- প্রতারক কোম্পানির কাস্টমার কেয়ার কোঅর্ডিনেটকে পরিবর্তন করেন এবং সার্চ ইঞ্জিন অপটিমাইজেশন (এসইও) সার্চ করেন তাঁদের নকল নম্বর লাগান সার্চের ফলাফলের ওপরে সোস্যাল মিডিয়ার প্ল্যাটফর্মে
- আপনার ব্যাঙ্ক বা অন্যান্য অর্থনৈতিক তথ্যাবলি বা এনটাইটিজ আপনার ব্যাঙ্ক অ্যাকাউন্টের কাস্টমার কেয়ার কনট্যাক্ট বিবরণ অনলাইনে সার্চ করা হলে, আপনি দুর্ঘটনাজনিতভাবে এই ধরনের না যাচাই করা বা নকল নম্বরে যোগাযোগ করে ফেলেন, তারা আসল ভেবে ধরে নিয়ে
- আপনি শেষমেশ আপনার পার্সোনাল বা গোপনীয় এবং অর্থনৈতিক পরিচয়পত্র তার সঙ্গে শেয়ার করে দেন এবং এর দ্বারা প্রতারিত হন

নিরাপত্তার টিপস

- কাস্টমার কেয়ার কনট্যাক্ট বিবরণ সার্চ করা এড়িয়ে চলুন সার্চ করার জায়গায় যেহেতু প্রতারককারীর দ্বারা প্রতারিত হন ছদ্মবেশে
- ব্যাঙ্ক বা কোম্পানির অফিসিয়াল ওয়েবসাইট সবসময় দেখে নেবেন তাদের আসল কনট্যাক্ট বিবরণের জন্য

স্ক্রিন শেয়ারিং / রিমোটের ব্যবহার

কিভাবে করা হয়

- আপনাকে স্ক্রিন শেয়ারিং অ্যাপ ডাউনলোড করতে বাধ্য করে প্রতারিত করে,প্রতারক আপনার ব্যক্তিগত ডেটা এবং আর্থিক শংসাপত্র আপনার ল্যাপটপে বা মোবাইল ডিভাইসে পেয়ে যায় এবং পরে পেমেন্ট করার সময়ে আপনার ব্যাঙ্কিং এবং পেমেন্ট অ্যাপ ব্যবহার করার সুযোগ পেয়ে যায়

নিরাপত্তার টিপস

- কখনও স্ক্রিন শেয়ারিং অ্যাপ ডাউনলোড করবেন না কোনও অপরিচিত ব্যক্তির
- কোনও স্ক্রিন শেয়ারিং অ্যাপ্লিকেশন ডিঅ্যাক্টিভেট করুন সুনিশ্চিতভাবে কোনও ব্যাঙ্কিং বা ফিনান্সিয়াল অ্যাপ বা ওয়েবসাইট লগিং করার আগে

অন কল / মোবাইল প্রতারণার সম্পর্কে (1)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী
আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

কলগুলি দেখা

কিভাবে এটা করা হয়

- প্রতারণ গ্রাহকদের সঙ্গে যোগাযোগ করেন টেলিফোন কল" সোস্যাল মিডিয়াতে ব্যাঙ্কের এক্সিকিউটিভ, ইত্যাদি বলে আপনার ব্যাঙ্কে সময়ে টোলফ্রী বা কাস্টমার কেয়ার নম্বরের মাধ্যমে
- যিনি কল করেন তিনি চাপ দেন এবং রাজি করানোর চেষ্টা করেন গ্রাহকদের তাঁদের গোপনীয় বিবরণ বা ওটিপি পাঠাতে বিভিন্ন এমাজেন্সী কারণে যেমন এক্ষুনি বাতিল করা হবে আপনার পরিষেবা, কেওয়াইসি নন-কমপ্ল্যান্স, অ্যাকাউন্ট বা কেডিট কার্ড ক্লোজার, ইত্যাদি করে
- আপনার অ্যাকাউন্টের প্রতারণামূলক অ্যাক্টিভিটির মাধ্যমে আপনার গোপনীয় তথ্যগুলির অপব্যবহার করেন

নিরাপত্তার টিপস

- ব্যাঙ্ক বা অন্য কোনও আসল এন্ট্রি কখনও আপনাকে গোপনীয় তথ্য যেমন ইউজার নাম, পাসওয়ার্ড,কার্ড বিবরণ, পিন, সিভিভি, ওটিপি ইত্যাদি শেয়ার করতে বলবে না

মোবাইল অ্যাপের প্রতারণা

কিভাবে করা হয়

- আপনাকে বাধ্য করা হয় আপনার মোবাইল, ল্যাপটপ বা ডেস্কটপে অযাচাইকৃত অ্যাপটিকে প্রলোভন দেখানো হয় হাউনলোড করার জন্য
- এই অ্যাপগুলো লিঙ্ক শেয়ার করা হয় এবং পাঠানো হয় এসএমএস, সোস্যাল মিডিয়া প্ল্যাটফর্মে, ইত্যাদিতে
- এই অ্যাপ্লিকেশনগুলো হয় দূষিত যা অনুমোদন করে প্রতারকদের আপনার ডিভাইস পুরোপুরি ব্যবহার করার

নিরাপত্তার টিপস

- অযাচাইকৃত / অপরিচিত উৎস থেকে কখনও কোনও অ্যাপ্লিকেশন ডাউনলোড করবেন না
- অপরিচিত উৎস থেকে আসা কোনও এসএমএস বা ই-মেল পেলে তা ডিলিট করুন ডাউনলোড করা লিঙ্ক অসচেতনভাবে ক্লিক করা এড়িয়ে

অন কল / মোবাইল প্রতারণার সম্পর্কে (2)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী
আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

ওটিপি ভিত্তিক প্রতরণা

কিভাবে এটি করা হয়

- আপনি একটা এসএমএস পাবেন একজন প্রতারকের কাছ থেকে যাতে ব্যাঙ্ক আপনাকে অফার করছে লোন্স বা আপনার ক্রেডিট সীমা বাড়াবেন বলে এবং মেসেজে দেওয়া নম্বরে আপনাকে যোগাযোগ করতে বলবেন
- যখন আপনি সেই নম্বরে কল করবেন, আপনাকে বলা হবে একটা কিছু ফর্ম ভর্তি (এমনকি অনলাইনে) করার জন্য, যেখানে আপনার ফিনান্সিয়াল বিবরণ দিতে হবে, এতে তাদের কাছে সহজ হয়ে যায় আপনাকে বোঝানো যে আপনাকে ওটিপি বা পিন বিবরণ তাদের শেয়ার করতে হবে, ফলে আপনার আর্থিক ক্ষতি হয়ে যায় এইভাবে

নিরাপত্তার টিপস

- আপনার এটিপি পিন বা ব্যক্তিগত বিবরণ কাউকে শেয়ার করবেন না
- আপনার এসএমএস বা ই-মেল নিয়মিত চেক করুন এটা সুনিশ্চিত করতে যে ওটিপি প্রস্তুত করা হয় আপনাকে না জানিয়ে

জুইস জ্যাকিং

কিভাবে করা হবে

- জুইস জ্যাকিং একধরনের সাইবার চুরি যেখানে একবার আপনার মোবাইল কানেকটেড হয় যে-কোনও অপরিচিত / অযাচাইকৃত চার্জিং পোর্টে, নির্দিষ্ট কোনও অপরিচিত অ্যাপে / ম্যালওয়্যারে ইনস্টল হয় আপনার ডিভাইসে যা কোনও প্রতারক চুরি করতে পারেন, নিয়ন্ত্রণ এবং ব্যবহার করেতে পারেন সংবেদনশীল ডেটা সমূহ,ই-মেল, এসএমএস বা সেভড পাসওয়ার্ডস

নিরাপত্তার টিপস

- সবসময় এড়ান পাবলিক / অপরিচিত চার্জিং পোর্ট / কেবল্স -এর ব্যবহার

#BankingDhyaanSe

অন কল / মোবাইল প্রতারণার সম্পর্কে (3)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী
আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

এসআইএম স্বোয়াপ প্রতারণা

কিভাবে এটি করা হয়

- আপনার অ্যাকাউন্ট বিবরণ এবং প্রমাণীকরণ আপনার রেজিস্টার্ড মোবাইল নম্বরের সঙ্গে সংযুক্ত। প্রতারকরা চেষ্টা করে তা ব্যবহার করার ওটিপি-এর মাধ্যমে এবং সতর্কতার প্রয়োজন হয় আর্থিক লেন দেন আইকন ব্যবহার করার সময়ে তখন একটা নতুন সিম-এর রিপ্লেসমেন্ট করে আপনার মোবাইল নম্বরে
- প্রতারক আপনার মোবাইল অপারেটর-এর রিটেল আউটলেটে প্রবেশ করে নিজের একটা নকল আইডি প্রুফ দেখিয়ে আপনার আসল সিম ব্লক করে দেয় এবং একটা নতুন সিম সংগ্রহ করে আপনার মোবাইল নম্বরে
- অন্যভাবে, তারা আপনাকে ভয় দেখায় বা ভান করে যে তারা আপনার সিম কার্ড আপগ্রেড করে দেবে এসএমএস শেয়ার করে আপনার অপারেটরের সঙ্গে যা আপনার সিমটিকে ডিঅ্যাক্টিভেট করবে এবং তাদের কাছে থাকা সিমটি আপনার মোবাইল ফোনে আবার অ্যাক্টিভেট করবে

নিরাপত্তার টিপস

- সোস্যাল ইঞ্জিনীয়ারিং স্ক্যামস থেকে সাবধান যারা আপনার গোপনীয় তথ্য এবং ব্যক্তিগত ডেটা চুরি করে
- যদি আপনার মোবাইল ফোন হঠাৎ কোনও নেটওয়ার্ক সংযোগ না দেখায়, আপনার মোবাইল সার্ভিস প্রদানকারীর সঙ্গে তৎক্ষনাৎ যোগাযোগ করুন আপনার সার্ভিসের অবস্থা জানতে যাতে সুনিশ্চিত করুন যে কোনও ডুপ্লিকেট সিম আপনার সিম হিসাবে ব্যবহৃত হচ্ছে কি না

প্রতারণার অন্যান্য পদ্ধতি (1)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

সোস্যাল মিডিয়ার মাধ্যমে প্রতারণা

কিভাবে এটি করা হয়

- প্রতারক আপনার সঙ্গে অভিনয় করে এবং নকল অ্যাকাউন্ট তৈরী করে জনপ্রিয় সোস্যাল মিডিয়ার প্ল্যাটফর্মে
- যখন আপনি ফোন আনলক করেন অসাবধানতাবশত: হস্তান্তরিত করেন (একটা এমার্জেন্সি কল তৈরী করা বা মেরামত করা) বা অরক্ষিত হয়ে পড়ে থাকলে, প্রতারক ওটিপি প্রাপ্ত করতে সক্ষম হয় আপনার মোবাইলে যাতে আপনার প্রোফাইল ব্যবহার করা যায় এবং নির্দিষ্ট অ্যাপ্লিকেশন ডেস্কটপ ভারশনে ধরা যায় যাতে আপনার কনট্যাক্ট, অনলাইন প্রোফাইল এবং চ্যাট ম্যাসেজ ব্যবহার করতে পারে
- তারা আপনার বন্ধুদের অনুরোধ পাঠায় জরুরী চিকিৎসাসংক্রান্ত খরচের জন্য, ইত্যাদি

নিরাপত্তার টিপস

- আপনার যোগাযোগগুলির সঙ্গে অনুরোধের মাধ্যমে সরাসরি তাদের সততা যাচাই করুন ফোন করে বা ব্যক্তিগতভাবে কোনও রকম পেমেন্ট করার আগে
- আপনার ফোনটিকে অরক্ষিত রাখবেন না লক না করে

কিউআর স্ক্যান- ভিত্তিক প্রতারণা

কিভাবে এটি করা হয়

- প্রতারক আপনার সঙ্গে যোগাযোগ করবে নানা অজুহাতে এবং আপনাকে প্রলোভন দেখাবে কিউআর কোড স্ক্যান করে পেমেন্ট অ্যাপ ব্যবহারের এবং পেমেন্ট প্রক্রিয়াটি সম্পূর্ণ করতে বলবে।
- এই কিউআর কোডটির পূর্বনির্ধারিত অ্যাকাউন্ট বিবরণ আছে যাতে যে-কোনও নির্দিষ্ট অ্যাকাউন্টে টাকা স্থানান্তরিত করার যা প্রতারক গোপনে আপনাকে কৌশলে আপনার অ্যাকাউন্ট থেকে টাকা স্থানান্তরিত করে নেবে

নিরাপত্তার টিপস

- সতর্ক থাকবেন কোনও কিউআর কোড স্ক্যান করে পেমেন্ট অ্যাপে পেমেন্ট করার সময়ে

প্রতারণার অন্যান্য পদ্ধতি (2)

মোদাস অপার‍্যান্ডি বা কার্যপ্রণালী আপনি কিভাবে সতর্ক এবং নিরাপদে থাকবেন?

লটারী বা জব প্রতারণার স্ক্যাম্‌স

কিভাবে করা হবে

- প্রতারক ই-মেল বা ফোন কল করে আপনাকে জানায় আপনি একটা বড় অ্যামাউন্টের লটারি / পুরস্কার জিতেছেন বা একটা নামকরা কোম্পানির অফিসার হয়ে আপনাকে চাকরির অফার করবেন
- তবে, এই টাকা বা উপহার প্রাপ্ত হওয়ার জন্য বা নির্বাচিত আইকন প্রক্রিয়া সম্পূর্ণ করার জন্য, আপনাকে কিছু টাকা আগে দিতে বলবেন
- আপনাকে যে টাকা দিতে বলবেন তা সাধারণত: লটারি বা পুরস্কারের কম শতকরা হিসেবে হয় বা বিবেচনা করা হয় একটা নিরাপদ চাকরি সংক্রান্ত পেমেন্ট, আপনি হয়তো এই জাতীয় পেমেন্ট করে দেন

নিরাপত্তার টিপস

- কখনও কোনও লটারির কল বা ই-মেলের জন্য কোন পেমেন্ট বা আপনার নিরাপদ শংসাপত্র দেবেন না
- সর্বদা অবিশ্বাস্য লটারি বা অফারের সততার বিষয়ে প্রশ্ন করবেন
- মনে রাখবেন, কোনও আসল কোম্পানি আপনাকে কোনও চাকরির অফার করলে টাকা চাইবেনা

এটিএম কার্ড স্কিমিং

কিভাবে করা হবে

- প্রতারক স্কিমিং যন্ত্র ইনস্টল করে এটিএম মেসিনে ডেটা চুরি করার জন্য, আর একটি নকল কার্ড তৈরী করে এবং আপনার অ্যাকাউন্ট থেকে টাকা তুলে নেয়
- এছাড়াও তারা একটি নকল কীপ্যাডস ইনস্টল করে বা একটা ছোট্ট ক্যামেরার মাধ্যমে আপনার তথ্যের ছবি তুলে রাখে
- এছাড়াও একজন গ্রাহকের অভিনয়ে এটিএম সার্ভিস ব্যবহার করে আপনাকে পিন দিতে বলে, আর আপনি পিন এন্টার করেন বা সাহায্য চান আপনার লেনদেনটি সম্পূর্ণ করার জন্য,যখন আপনি টাকা তুলতে সক্ষম না হন তখন তারা আপনাকে প্রতারিত করে

নিরাপত্তার টিপস

- সতর্ক থাকুন এবং এটা সুনিশ্চিত করুন যে কোনও এক্সট্রা মেসিন ঢোকানো আছে কিনা এটিএম মেসিনের কার্ড ঢোকানোর জায়গায় বা কীপ্যাডে
- কখনও কার্ড বিবরণ এন্টার করবেন না আপনার পাশে কেউ দাঁড়িয়ে থাকলে
- কীপ্যাডটি ঢেকে রাখুন পিন এন্টার করার সময়ে এবং আপনার কার্ড বা পিন কাউকে দেবেন না
- এটিএম থেকে তাড়াতাড়ি বের হয়ে যাবেন যদি কোনও কিছু সন্দেহজনক মনে হয়

#BankingDhyaanSe

অ্যাক্সেস ব্যাঙ্কে রিপোর্ট করুন কোনও সন্দেহজনক বা প্রতারণামূলক ট্র্যান্সঅ্যাক্ট আয়ন বা লেনদেন করা হলে

যদি আপনি কোনও সন্দেহভাজন লেনদেনের সম্মুখীন হন বা প্রতারণামূলক লেনদেন করে থাকেন, আপনি নীচে দেওয়া চ্যানেলে যোগাযোগ করতে পারেন।

- আমাদের ফোন ব্যাঙ্কিং নম্বরে কল করুন: 1860 419 5555 / 1860 500 5555
- আমাদের লিখুন ওখানে://www.axisbank.com/support/
- কোনও অ্যাক্সেস ব্যাঙ্ক শাখায় সাক্ষাৎ করুন

আপনাকে ধন্যবাদ জানাই সময় এবং মনোযোগ দেবার জন্য

#BankingDhyaanSe