প্রতারকেরা এখানে আছে,
প্রতারকেরা ওখানেও আছে,

কোথাও এদের ফাঁদে পড়বেন না!

#BankingDhyaanSe 2.0

AXIS BANK

আপনি খুব কষ্ট করে টাকা উপার্জন করেন,

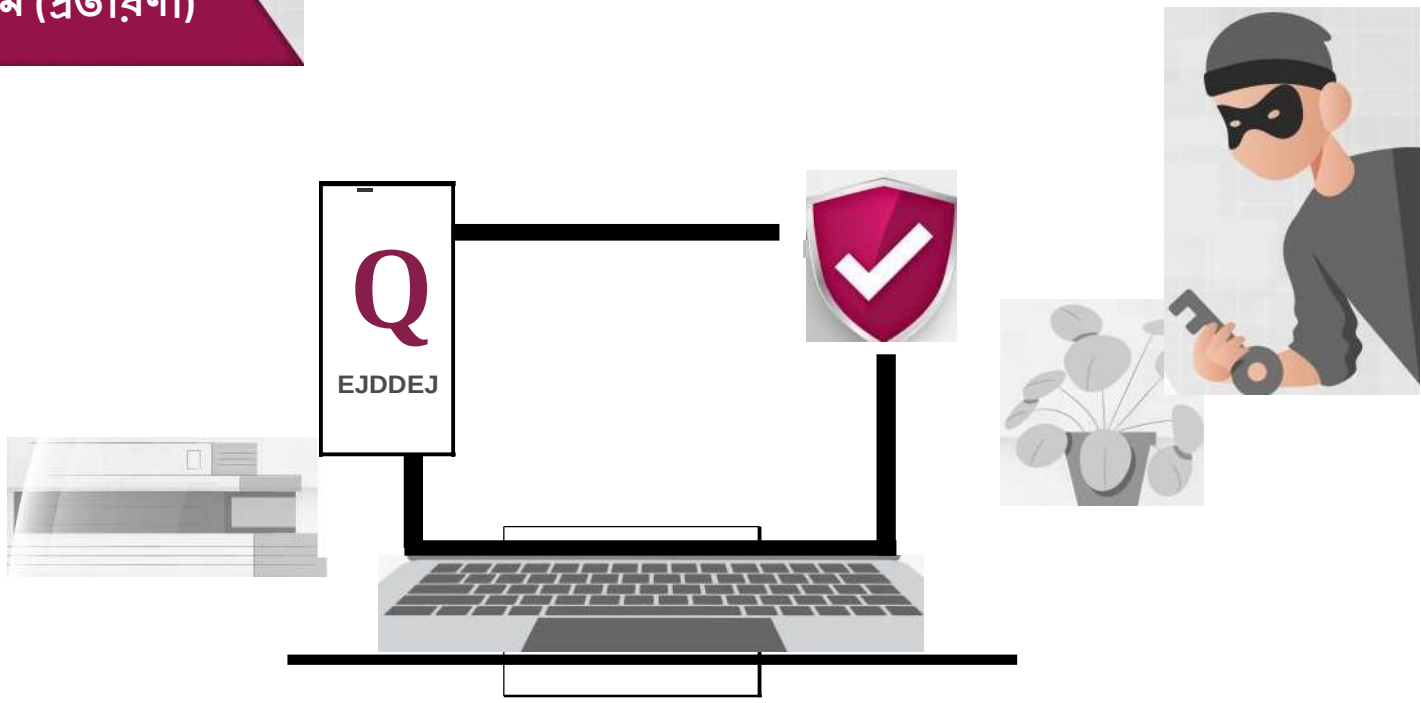
তাহলে কেনো আপনার উপার্জন করা টাকাকে নিরাপদে রাখবেন না?

অ্যাক্সিস ব্যাঙ্ক ফ্রড অ্যাওয়্যারনেস বুকলেট #BankingDhyaanSe 2.0-এ আপনাকে স্বাগত, এটা হলো আর্থিক

কেলেঙ্কারির ব্যাপারে বোঝার এবং সেটাকে প্রতিরোধ করার জন্য আপনার প্রধান চাবিকাঠি। এই যুগে যেখানে ডিজিটাল মাধ্যম খুব দ্রুত বিকশিত হচ্ছে সেখানে এই বিষয়ে জ্ঞান থাকলে তবেই আপনি প্রতারকদের থেকে বাঁচতে পারবেন। এই গাইডবুকটি আপনাকে সমস্যাকে বোঝার, বাস্তব জীবনের উদাহরণ এবং আপনার কষ্ট করে উপার্জন করা টাকাকে নিরাপদে রাখার জন্য কার্যকরী পরামর্শ দেয়।

ব্যাঙ্কিংয়ের ক্ষেত্রে আপনার বিশ্বস্ত পার্টনার হিসেবে, অ্যাক্সিস ব্যাঙ্ক আপনাকে আত্মবিশ্বাসের সাথে ডিজিটাল দুনিয়াকে ব্যবহার করতে সাহায্য করে। আসুন আমরা প্রতারণা থেকে নিরাপদে থাকি এবং একসাথে একটা উজ্জ্বল আর্থিক ভবিষ্যতকে সুরক্ষিত করি।

OTP স্ক্যাম (প্রতারণা)



ওয়ান-টাইম পাসওয়ার্ড হলো আপনার দুর্ভেদ্য ডিজিটাল সাম্রাজ্যকে অ্যাক্সেস করার জন্য একটা মুল্যবান চাবি।

ধূর্ত প্রতারকেরা যাতে আপনার এই মূল্যবান চাবিকে চুরি না করতে পারে তার জন্য আপনাকে সবসময় আপনার দুর্গের প্রহরী হয়ে সেটাকে রক্ষা করতে হবে!

OTP-কে গোপন রাখুন: ফোন কল, ই-মেইল, টেক্সট মেসেজ বা সোশ্যাল মিডিয়ার মাধ্যমে কখনই কারোর সাথে OTP শেয়ার করবেন না আর সবসময় একজন সতর্ক প্রহরীর মতো সতর্ক থাকুন।

অনুরোধকে যাচাই করুন: বিশ্বাস করবেন কিন্তু তবুও যাচাই করে নেবেন। যদি হঠাৎকরে কোনো OTP-এর অনুরোধ আসে বা OTP-টা সন্দেহজনক বলে মনে হয়, সেক্ষেত্রে তাড়াহুড়ো করবেন না। কোনোরকম প্রতিক্রিয়া জানানোর আগে এটা আসল কিনা সেটা দু'বার চেক করে নিন।

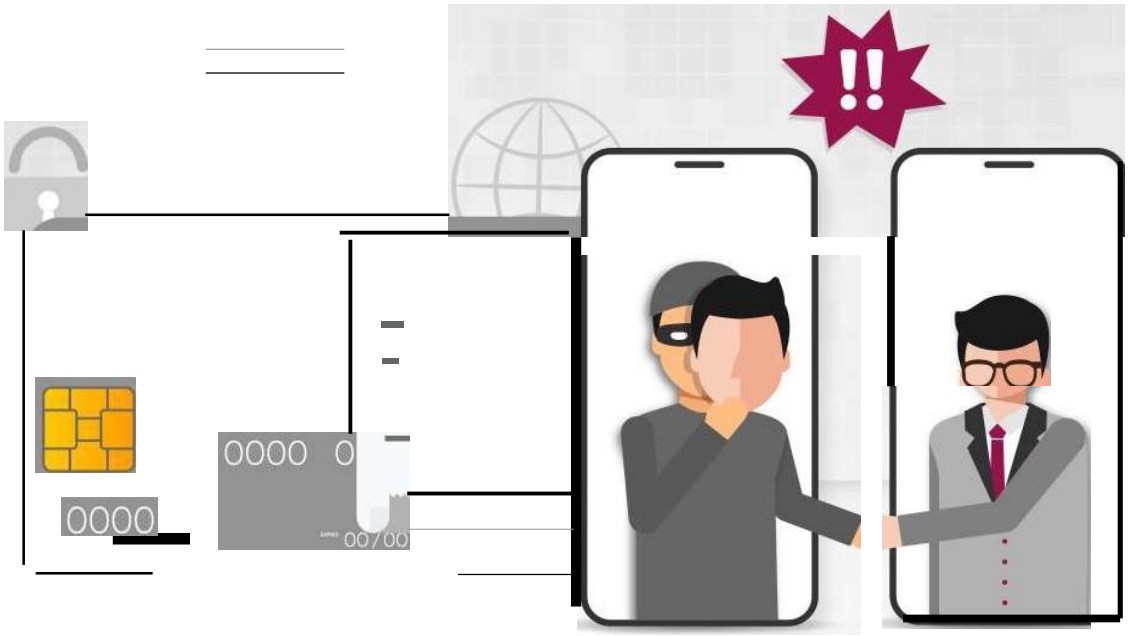
অফিসিয়াল ওয়েবসাইট বা অ্যাপ ব্যবহার করুন: OTP শেয়ার করার সময় সুরক্ষিত থাকুন। সবসময় সরাসরি অফিসিয়াল সাইট বা অ্যাপে যাবেন - কোনো শর্টকাট অবলম্বন করবেন না। কোনো লিংকে ক্লিক না করে টাইপ করুন।

জরুরী অনুরোধের ক্ষেত্রে সতর্ক থাকুন: স্ক্যামাররা (প্রতারক) বেশিরভাগ সময়তেই আপনার OTP-কে তাদের সাথে শেয়ার করার জন্য একটা জরুরী পরিস্থিতি তৈরি করে আপনাকে চাপ দেওয়ার চেষ্টা করে। অপেক্ষা করুন, বিষয়টাকে নিয়ে খুঁটিয়ে চিন্তা করুন, এবং কোনোরকম পদক্ষেপ নেওয়ার আগে স্বাধীনভাবে অনুরোধটাকে যাচাই করুন।

টু-ফ্যাক্টর অথেন্টিকেশনকে সক্রিয় করুন: 2FA (টু-ফ্যাক্টর অথেন্টিকেশন) দিয়ে নিরাপত্তাকে দ্বিগুণ করুন। অ্যাপ-ভিত্তিক বা হার্ডওয়্যার টোকেনের মতো শক্তিশালী বিকল্পগুলিকে বেছে নিন। এগুলো SMS OTP-এর থেকে অনেক বেশি নিরাপদ।

অনুগ্রহ করে মনে রাখবেন, ব্যাঙ্ক আপনার কাছ থেকে আপনার CVV, OTP, PIN, কার্ড নম্বর, পাসওয়ার্ড ইত্যাদি চাইবে না। এই বিবরণগুলি কারোর সাথে শেয়ার করবেন না।

ক্রেডিট কার্ড স্ক্যাম (প্রতারণা)



আসুন ক্রেডিট কার্ডের প্রতারণাকে লুকোচুরির মতো একটা খেলা হিসেবে মনে করি। ঠিক যেমন একজন প্রতারক তার আসল উদ্দেশ্যকে লুকানোর চেষ্টা করে, তারা আপনাকে আপনার ক্রেডিট কার্ডের তথ্যকে তাদের কাছে প্রকাশ করার জন্য আপনার সাথে প্রতারণা করতে পারে।

আপনি যাতে তাদের ফাঁদে না পড়েন তার জন্য এই পরামর্শগুলি মনে রাখবেন:

ফিশারদের (প্রতারক) ব্যাপারে সতর্ক থাকুন: স্ক্যামাররা (প্রতারক) আপনাকে আপনার ব্যাঙ্ক বা পরিচিত কোম্পানির লোক বলে নিজেদের মিথ্যে পরিচয় দিতে পারে। তাদের প্রতারণার ফাঁদে পড়বেন না; তাদের পরিচয়কে যাচাই করুন।

আপনার স্টেটমেন্টগুলি চেক করুন: নিয়মিতভাবে আপনার ক্রেডিট কার্ডের স্টেটমেন্টের উপর লক্ষ্য রাখুন। আপনি যদি এমন কোনো খরচ দেখতে পান যেটা আপনি করেননি বা এমন কোনো চার্জ কেটে নেওয়া হয় যেটা কাটার কথা ছিলো না, সেক্ষেত্রে এমন একটা পরিস্থিতি তৈরি হয় যেখানে আপনাকে একটা খেলার মধ্যে কোনো লুকোনো খেলোয়াড়কে খুঁজে বার করতে হয় - অবিলম্বে এই বিষয়টিকে খুঁটিয়ে দেখুন আর সংশ্লিষ্ট কতৃপক্ষকে এই ব্যাপারে জানান।

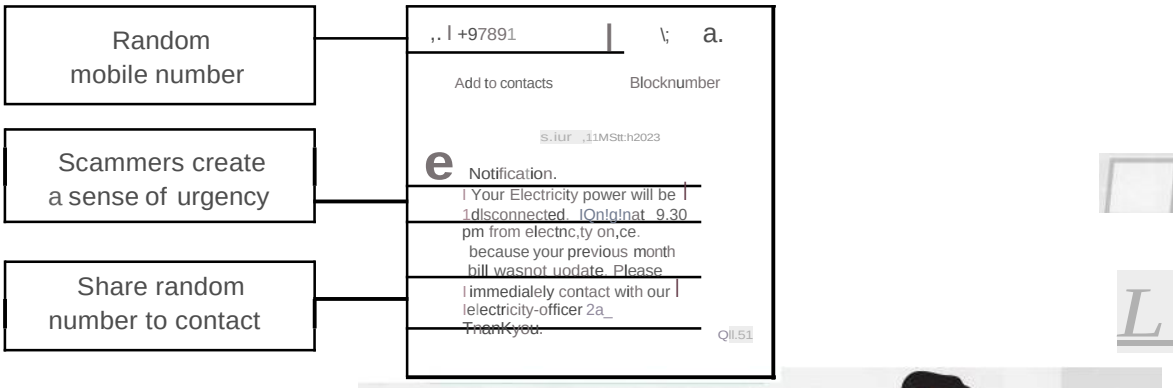
লেনদেনের সীমাকে নির্ধারণ করুন: আপনার সমস্ত পেমেন্ট চ্যানেলে লেনদেনের সীমাকে নির্ধারণ করুন এবং আপনার প্রয়োজন অনুযায়ী 'ম্যানেজ ইউসেজ' বিভাগটিকে কাস্টমাইজ করুন।

শুধুমাত্র সিকিওর (নিরাপদ) সাইট: অনলাইনে কেনাকাটা করার সময়, এটা নিশ্চিত করুন যে ওয়েবসাইটটা যেন সিকিওর (নিরাপদ) হয় ("https" URL দেখুন)। এটা হলো খেলার জন্য একটা নিরাপদ খেলার মাঠ বেছে নেওয়ার মতো।

আপডেট থাকুন: যেমনভাবে আপনি খেলার ক্ষেত্রে নতুন কৌশল শেখেন, ঠিক তেমনভাবেই প্রতারণার (স্ক্যাম) লেটেস্ট কৌশলের ব্যাপারে জেনে রাখুন। এইভাবেই, আপনি প্রতারকদেরকে (স্ক্যামার) বোকা বানাতে পারবেন।

ক্রেডিট কার্ড স্ক্যাম (প্রতারণা)

একটা ফেক (জাল) SMS-কে কিভাবে সনাক্ত করবেন?



বিষয়টাকে এইরকমভাবে ভাবুন: আপনি বিকেলে বাড়িতে বসে আরাম করছেন আর মজা করছেন, আপনার প্রিয় শো দেখছেন, আর তখনই আপনার ফোনটা বেজে ওঠে আর একটা মেসেজ আসে। এটা আপনার ইলেকট্রিক প্রোভাইডরের মেসেজ, এবং তারা দাবি করছে যে আপনার সর্বশেষ বিলের জন্য তারা আপনার কাছ থেকে অতিরিক্ত পরিমাণ টাকা পায়।

আপনি আতঙ্কিত হওয়ার আগে, এটাকে বিবেচনা করে দেখুন: বিদ্যুতের বিলের ক্ষেত্রে জালিয়াতি, অনেকটা ছদ্মবেশী ফ্যান্টমের মতো, যেটা কোনো সতর্কতা না দিয়েই আপনার জীবনে আসতে পারে।

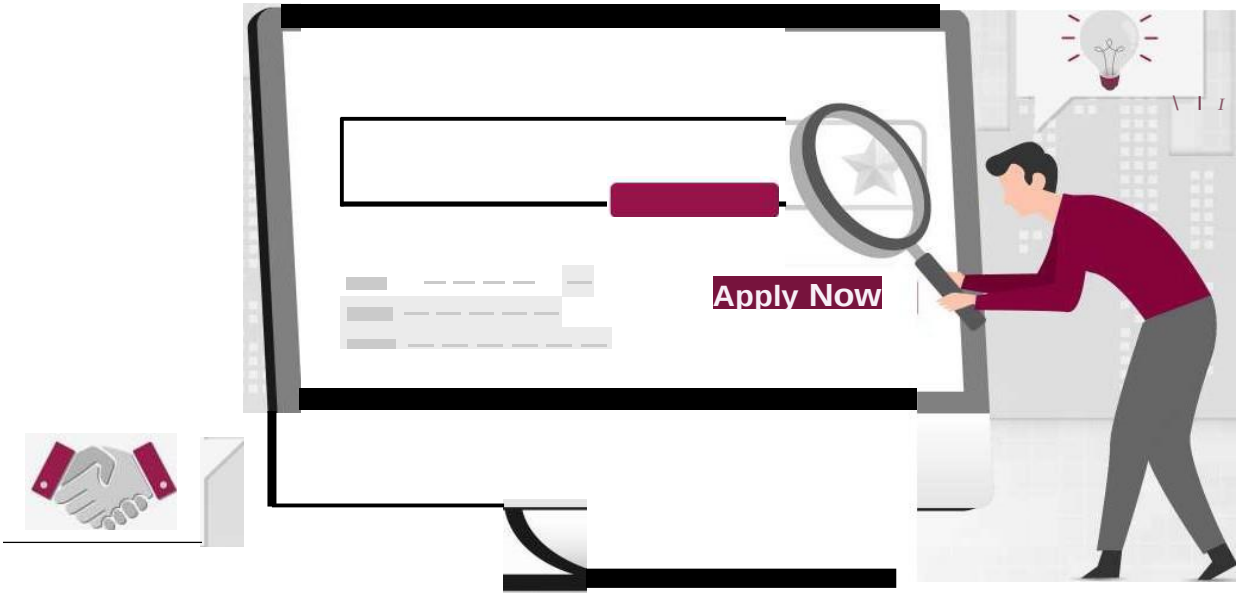
F) LW আপনার গোপনীয় বিবরণ অন্য কারোর সাথে শেয়ার করবেন না বা অযাচিত লিংকগুলোতে ক্লিক করবেন না।

[!...-•! বিল পেমেন্ট করার জন্য শুধুমাত্র অফিসিয়াল এবং সুরক্ষিত ওয়েবসাইট ব্যবহার করুন।

———

মনে রাখবেন, ইলেকট্রিসিটি ডিপার্টমেন্ট (বিদ্যুৎিবভাগ) কখনই যে কোনো/রেজিস্টার না করা নম্বরের মাধ্যমে ব্যক্তিগত বিবরণের ব্যাপারে জিজ্ঞাসা করে না বা পেমেন্ট করতে বলে না।

চাকরির স্ক্যাম (প্রতারণা)



ধরে নিন যে আপনি অনলাইনে চাকরি খুঁজছেন, আর হঠাৎ আপনি এমন একটা চাকরির প্রস্তাব দেখে থেমে গেলেন যেটাকে সত্যিই খুব ভালো চাকরি বলে মনে হচ্ছে। আনলিমিটেড ছুটি, বাড়িতে বসে কাজ করতে হবে এবং ডেটা এন্ট্রির জন্য ছয় সংখ্যার বেতন? সাইন আপ করুন!

অ্যাপ্লাই নাও" বাটনটাতে ক্লিক করার আগে দাঁড়ান!

কোম্পানীর ব্যাপারে খোঁজ করুন: কোম্পানীটার ব্যাপারে অনলাইনে খুঁজুন আর এটা নিশ্চিত করুন যে কোম্পানীটা যেন একটা সঠিক ও নামী কোম্পানী হয়। প্রতারকেরা (স্ক্যামার) প্রায়ই বিশ্বাসযোগ্য ওয়েবসাইট দিয়ে জাল কোম্পানী তৈরি করে।

আগে থেকে কোনো টাকা পেমেন্ট করবেন না: আসল এমপ্লয়াররা (নিয়োগকর্তা) কখনোই আপনাকে কাজ শুরু করার আগে ট্রেনিং, মেটেরিয়াল বা ব্যাকগ্রাউন্ড চেক করার জন্য টাকা পেমেন্ট করতে বলবে না।

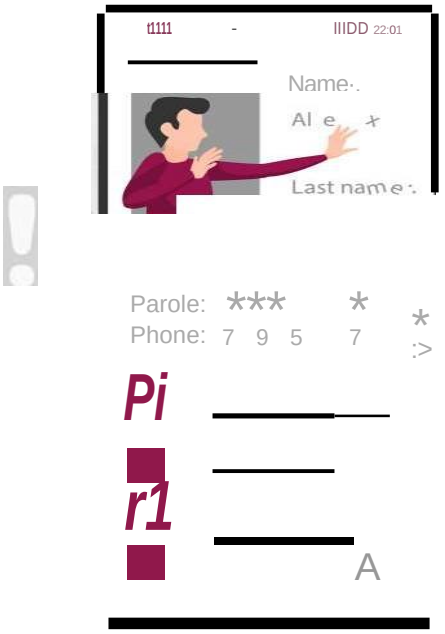
রেড ফ্ল্যাগগুলো দেখে নিন: যদি চাকরির জন্য আপনাকে আগে থেকেই আপনার সোশ্যাল সিকিউরিটি নম্বর বা আর্থিক বিবরণের মতো সংবেদনশীল তথ্য দিতে হয় তাহলে সতর্ক থাকুন।

খুব তাড়াতাড়ি নিয়োগ করা হচ্ছে: ইন্টারভিউ না নিয়েই বা প্রয়োজনীয় তথ্য আদান-প্রদান না করেই যদি আপনাকে স্পটেই চাকরির প্রস্তাব দেওয়া হয়, তাহলে এটা স্ক্যাম (প্রতারণা) হতে পারে।

আপনার মনে কোনো সংশয় থাকলে সেটাকে বিশ্বাস করুন: যদি আপনার মনে কোনো সংশয় হয়, তাহলে নিজের উপর বিশ্বাস রাখুন এবং সাবধানতা অবলম্বন করে এগিয়ে যান বা কাজটা থেকে পিছিয়ে আসুন।

মনে রাখবেন, চাকরি খোঁজার সময় আপনার ব্যক্তিগত এবং আর্থিক তথ্যকে সুরক্ষিত রাখার বিষয়টাকে আপনার সবার প্রথমে গুরুত্ব দেওয়া উচিত।

কল স্ফফিং স্ক্যাম (প্রতারণা)



যেমন একজন জাদুকর কোনো জিনিসকে সেটা আসলে যেমন দেখতে তার থেকে আলাদা করে দেখাতে পারে ঠিক তেমনি স্ক্যামাররা (প্রতারক) আপনার কলার আইডিকে ম্যানিপুলেট করতে পারে যাতে মনে হয় যে তারা এমন কেউ যাকে আপনি চেনেন বা বিশ্বাস করেন - এই ক্ষেত্রে, তারা আপনার ব্যাঙ্ক হিসেবে আপনার কাছে পরিচয় দেয়। এটা হলো তাদের আসল পরিচয়কে লুকোনোর জন্য ডিজিটাল ছদ্মবেশ ধারণ করার মতো ব্যাপার।

এই গোপন কৌশলের থেকে নিজেকে বাঁচানোর জন্য, এই পরামর্শগুলো মনে রাখবেন:

সতর্কতার সাথে যাচাই করুন: যদিও কলার আইডি আপনার কাছে পরিচিত বলে মনে হয়, তবুও সতর্ক থাকবেন। যদি কেউ আপনার কাছ থেকে কোনোরকম সংবেদনশীল তথ্য চায় সেক্ষেত্রে অন্য কোনো মাধ্যম থেকে তাদের পরিচয়কে দ্বিতীয়বার চেক করুন।

ব্যক্তিগত তথ্য শেয়ার করবেন না: ফোনে কখনই ব্যক্তিগত বা আর্থিক তথ্য দেবেন না, এমনকি যিনি কল করছেন তিনি যদি সঠিক ব্যক্তি হন তাও না। ফোনটা কেটে দিন এবং একটা বিশ্বস্ত নম্বর ব্যবহার করে তাঁকে কল ব্যাক করুন।

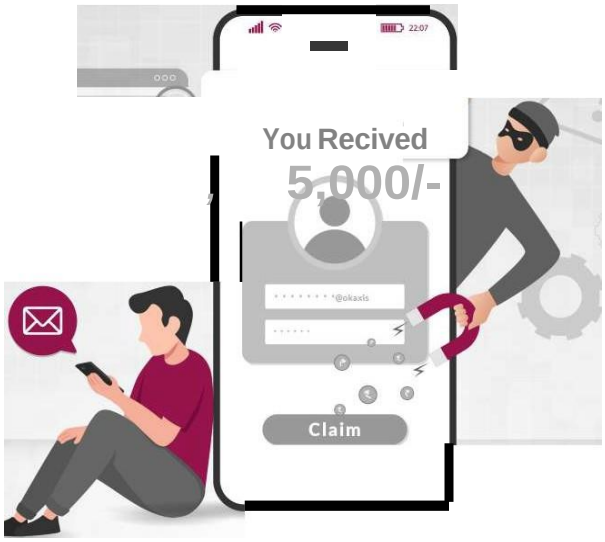
নিজের তথ্যকে ব্যক্তিগত রাখুন: আপনি অনলাইনে বা সোশ্যাল মিডিয়াতে কি ধরণের ব্যক্তিগত বিবরণ শেয়ার করছেন সেই ব্যাপারে সতর্ক থাকুন। স্ক্যামাররা (প্রতারক) প্রায়ই তাদের জালিয়াতি করার জন্য করা কলগুলিকে আরো বিশ্বাসযোগ্য করে তুলতে এই উৎসগুলো থেকে তথ্য সংগ্রহ করে।

কল ব্লকিং করাকে ব্যবহার করুন: আপনার ফোনের ক্যারিয়ারের দ্বারা দেওয়া কল-ব্লকিং অ্যাপ বা ফিচারগুলির ব্যাপারে ভালোভাবে জানুন। এগুলো সম্ভাব্য স্ক্যাম কলকে ফিল্টার করতে সাহায্য করতে পারে।

গুগল বা কোনো সার্চ ইঞ্জিনে ফোন নম্বর সার্চ করবেন না। আপনি যদি সেটা করেন, তাহলে কোনো সত্তা বা ব্যবসায়ীদের দ্বারা পাঠানো কোনো লিংকে ক্লিক করবেন না।
এছাড়াও, অনুগ্রহ করে এটা নিশ্চিত করুন যে আপনার ব্যাঙ্কিং অ্যাপ্লিকেশনগুলির লেটেস্ট ভার্সনকে যেন শুধুমাত্র অনুমোদিত অ্যাপ্লিকেশন স্টোর থেকেই ডাউনলোড করা হয়।
অনুগ্রহ করে মাঝেমধ্যেই এগুলিকে চেক করুন।

মনে রাখবেন যে আপনি যেমন বাস্তব জীবনে মুখোশধারী অপরিচিত ব্যক্তিকে বিশ্বাস করবেন না, ঠিক তেমনি ফোনে মুখোশধারী কলারকেও আপনার বিশ্বাস করা উচিত নয়। সতর্ক থাকুন!

UPI রিফান্ড স্ক্যাম (প্রতারণা)



ধরে নিন যে আপনি আপনার ফোনে স্ক্রোল করছেন আর এমন সময় আপনি একটা UPI রিফান্ডের নোটিফিকেশন দেখতে পান, এবং হঠাৎ আপনি খুব খুশি হয়ে যান !কিন্তু দাঁড়ান। এটা একটা UPI রিফান্ড স্ক্যাম) প্রতারণা (হতে পারে!

UPI বা ইউনিফাইড পেমেন্ট ইন্টারফেস আমাদের রোজকার জীবনের একটা অংশ হয়ে উঠেছে। আপনার স্থানীয় মুদিখানার দোকানে পেমেন্ট করা থেকে শুরু করে ফোন রিচার্জ করা, ফ্লাইটের টিকিট বুক করা পর্যন্ত, আমরা বিভিন্ন স্থানীয় মুদিখানার দোকানে পেমেন্ট করার জন্য, ফোন রিচার্জ করার জন্য, ফ্লাইটের টিকিট বুক করার জন্য UPI পেমেন্ট ব্যবহার করি, আমরা বিভিন্ন জিনিসের জন্য UPI পেমেন্ট ব্যবহার করি। তাই প্রতারকেরা UPI অ্যাপ ব্যবহার করে লোকেদের সাথে প্রতারণা করার জন্য নতুন পদ্ধতি অবলম্বন করতে শুরু করেছে।

তাদের অফিসিয়াল কথাবার্তায় কান দেবেন না এবং তারা অনেক সময় পেশাদার ভাষার কথা বলবে সেগুলোর ফাঁদে পড়বেন না। নিচে দেওয়া পরামর্শগুলো মনে রাখবেন:

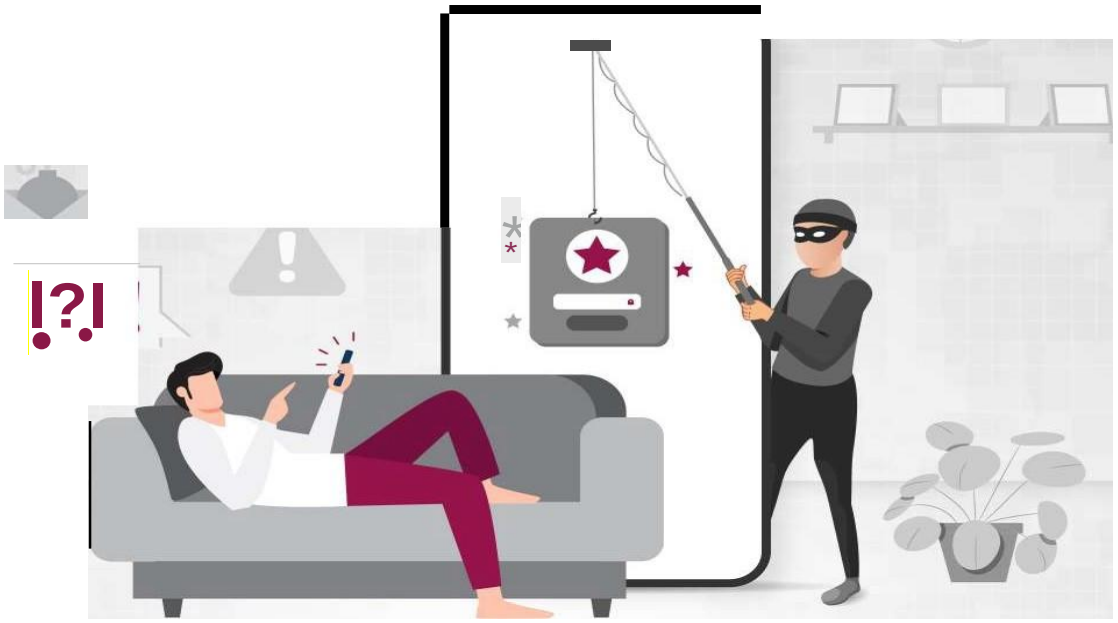
লিংকের ব্যাপারে সতর্ক থাকুন: স্ক্যামাররা) প্রতারক (আপনাকে একটা লিংক পাঠাতে পারে, আর রিফান্ড পাওয়ার লোভ দেখিয়ে আপনাকে রেজিস্টার করার জন্য জোর করে অনুরোধ করতে পারে।

প্রচন্ড পরিমাণে চাপ দেওয়ার কৌশল: তারা আপনাকে তৎক্ষণাৎ টাকার জন্য অবিলম্বে ব্যাঙ্কের বিবরণ বা UPI PIN পূরণ করতে চাপ দেবে।

যোগ্যতাকে যাচাই করুন: এটা নিশ্চিত করুন যে আপনি টাকা রিফান্ড পাওয়ার জন্য যোগ্য কিনা। যদি আপনি যোগ্য হন তাহলে একটা বিশ্বস্ত উৎসের জন্য চেক করুন।

মনে রাখবেন, ব্যাঙ্ক বা অন্যান্য আধিকারিকরা কখনই আপনার কাছ থেকে এই ধরণের সংবেদনশীল বিবরণ বা তথ্য চাইবেন না।

ফিশিং স্ক্যাম (প্রতারণা)



ধরে নিন যে আপনি একটা মাছের মতো নিজের মতো করে একটা পরিষ্কার পুকুরে শান্তিতে সাঁতার কাটছেন। হঠাৎ একটা চকচকে, লোভনীয় টোপ আপনার সামনে ঝুলছে। আপনি এই ব্যাপারে ভীষণ কৌতূহলী, কিন্তু দাঁড়ান - কিছু একটা গড়বড় আছে!

ডিজিটাল ক্ষেত্রে ফিশিং স্ক্যামগুলির (প্রতারণা) সাথে ঠিক এই জিনিসটাই ঘটে।

একটা মাছকে যেমন টোপ দিয়ে লোভ দেখানো হয় ঠিক তেমন ভাবেই সাইবার অপরাধীরা আপনার সাথে প্রতারণা করার জন্য আপনার সামনে একজন বিশ্বস্ত ব্যক্তি হিসেবে নিজেদেরকে জাহির করে যাতে আপনি আপনার সংবেদনশীল তথ্য তাদেরকে দিয়ে দেন। তারা বেশিরভাগ সময়তেই ব্যাঙ্ক, সোশ্যাল মিডিয়া বা আপনার বসের অনুকরণ করেও জাল ইমেল, মেসেজ, বা ওয়েবসাইট পাঠায় যেগুলোকে সঠিক বলে মনে হয়।

এই ডিজিটাল ফাঁদগুলোকে এড়িয়ে যেতে, এই পরামর্শগুলো মনে রাখবেন:

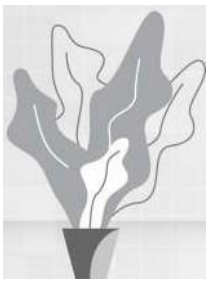
URL-কে দুবার করে চেক করুন: লিংকের উপরে কিছুক্ষণ ঘোরাঘুরি করুন যাতে আপনি বুঝতে পারেন যে সেই লিংকগুলো আসলে আপনাকে কোথায় নিয়ে যাচ্ছে।

ব্যক্তিগত তথ্য শেয়ার করবেন না: বৈধ বা সঠিক সত্তারা ইমেলের মাধ্যমে সংবেদনশীল তথ্য জানতে চাইবে না
rl2J
সন্দেহ প্রকাশ করুন: অপ্রত্যাশিত অনুরোধ? কোনো প্রতিক্রিয়া জানানোর আগে অন্যান্য মাধ্যমের থেকে যাচাই করুন।
l@l:"\.
সিকিউরিটি সফ্টওয়্যারকে আপডেট করুন: আপনার ডিজিটাল পুকুরকে লেটেস্ট নিরাপত্তার ব্যবস্থার সাথে সুরক্ষিত রাখুন।

একটা সতর্ক মাছের মতো, সবসময় সতর্ক থাকুন এবং ইন্টারনেটের বিশাল মহাসাগরে স্মার্টভাবে সাঁতার কাটুন!

ভিশিং স্ক্যাম (প্রতারণা)

a



আপনার ফোনটা বেজে ওঠে, এবং এই কলটা আপনার তথাকথিত ব্যাঙ্কের থেকে আসে যারা দাবি করে যে এটা একটা 'জরুরী' কল আর আপনার অ্যাকাউন্টকে বন্ধ করা হবে, বা এটা এমন একটা কল হতে পারে যেখানে দাবি করা হবে যে আপনি কিছু 'জিতেছেন' আর বলা হতে পারে যে আজকের দিনটা আপনার জন্য খুব ভালো এবং আপনি একটা সারপ্রাইজ জিতেছেন!

ফোনটাকে ধরে থাকুন) সত্যি সত্যি(!

এই ধরণের স্ক্যামের) প্রতারণা (থেকে নিরাপদ থাকতে, নিচে দেওয়া পরামর্শগুলি মনে রাখবেন:

I

কখনই ফোনে আপনার ব্যক্তিগত তথ্য কাউকে দেবেন না।

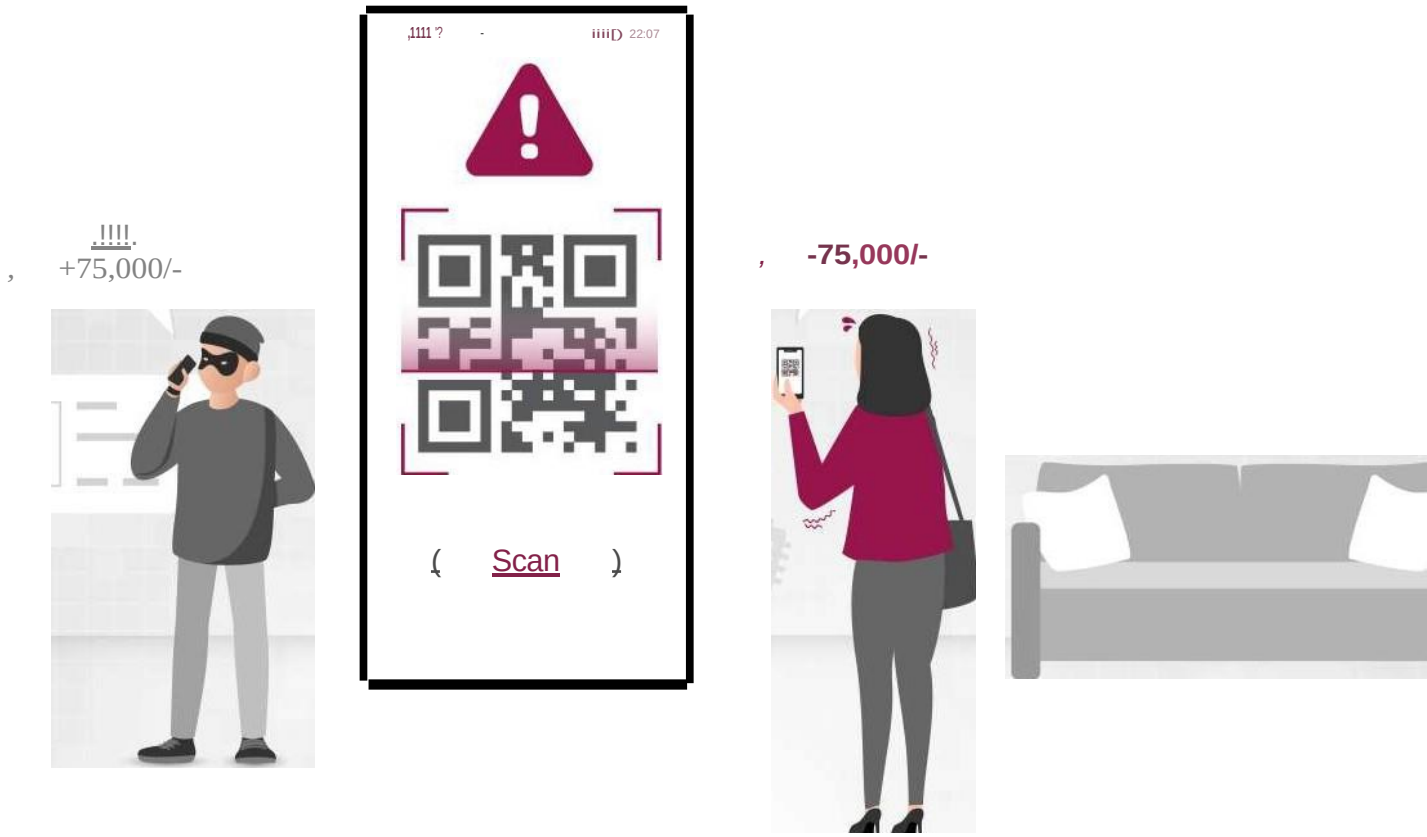
<@)> শার্লক হোমস হয়ে জান এবং সেই কলারের পরিচয়কে যাচাই করুন।

L .J

তাদের নাটকের ফাঁদে পড়বেন না !তারা উত্তেজিত হলে আপনার মাথা ঠান্ডা রাখুন।

লাইনে থাকা কোনো অপরিচিত ব্যক্তিদের সাথে তথ্য শেয়ার করার ব্যাপারে সতর্ক থাকবেন - আপনার জিনিস বা তথ্যকে সুরক্ষিত রাখতে স্মার্ট থাকুন!

UPI স্ক্যাম (প্রতারণা) – টাকার জন্য অনুরোধ করার বিকল্প



স্নেহা অনলাইনে একটা কেনা-বেচা করার অ্যাপে তার ফার্নিচারের বিজ্ঞাপন দিয়েছেন। একজন ক্রেতা, নিজেকে আধাসামরিক বাহিনীর সদস্য বলে দাবি করেন, এবং তিনি হোয়াটসঅ্যাপে পেমেন্ট করার জন্য একটা QR কোড পাঠিয়েছেন। স্নেহা সেটাকে স্ক্যান করে আর তাঁর ₹75,000 টাকা ব্যাঙ্কের থেকে কেটে নেওয়া হয়।

আপনার কি মনে হচ্ছে যে এটা আগেও কোথাও শুনেছেন? আপনি কি মাঝেমধ্যেই UPI পেমেন্ট প্ল্যাটফর্ম ব্যবহার করার কারণে UPI ফ্রডের (জালিয়াতি) শিকার হওয়ার ভয় পাচ্ছেন?
সবসময় মনে রাখবেন:

UPI PIN শুধুমাত্র পেমেন্ট করার জন্য প্রয়োজন হয় আর এটা কোনো পেমেন্ট পাওয়ার জন্য প্রয়োজন হয় না।

যেই মুহূর্তে পেমেন্ট পাওয়ার জন্য আপনার কাছ থেকে আপনার UPI PIN চাওয়া হবে তখনই সতর্ক হয়ে যান! এটা আসলে একটা পেমেন্ট করার জন্য অনুরোধ হতে পারে পেমেন্ট পাওয়ার জন্য অনুরোধ নয়।

আপনার OTP, UPI PIN অথবা কোনো গোপনীয় বিবরণ বা তথ্য অন্য কারোর সাথে শেয়ার করবেন না।

যে কোনো পেমেন্ট শুরু করার আগে সবসময় UPI অ্যাপ্লিকেশনে মোবাইল নম্বর এবং নাম যাচাই করুন।

টাকা পাওয়ার জন্য QR কোড স্ক্যান করবেন না; ফান্ড পাওয়ার জন্য লেনদেনের ক্ষেত্রে বারকোড/QR কোড স্ক্যান করা বা মোবাইল ব্যাঙ্কিং PIN (m-PIN), পাসওয়ার্ড ইত্যাদি দেওয়ার প্রয়োজন নেই।

QR কোড স্ক্যান করার জালিয়াতি

সাবধানতা অবলম্বন করে পেমেন্ট করার অ্যাপে QR কোড স্ক্যান করুন; এর মধ্যে টাকা ট্রান্সফার করার জন্য অ্যাকাউন্টের বিবরণ দেওয়া রয়েছে।

একজন ক্রেতা/বিক্রেতা যদি অকারণে তাড়াহুড়ো করে বা তৎপরতা দেখায় তাহলে সম্ভবত সে একজন প্রতারক। শান্ত থাকুন, সবসময় ব্যাখ্যা চেয়ে নিন এবং প্রয়োজনীয় প্রশ্ন জিজ্ঞাসা করে নেবেন।

যাচাই না করা মোবাইল অ্যাপের জালিয়াতি

আপনি একটা SMS, ইমেইল বা অনেকদিন ধরে যোগাযোগ না থাকা কোনো আত্মীয় যাকে আপনি চেনেন না তার কাছ থেকে একটা মেসেজ পান, আর এই সব ক্ষেত্রেই মেসেজে একটা লিংক থাকে যেটাকে দেখে মনে হয় যে সেটা আপনার প্রিয় অনুমোদিত সত্তার একটা বৈধ অ্যাপ।

এক মিনিট অপেক্ষা করুন !এগুলো পরিচিত ডাউনলোড নয়; এগুলো এমন একটা ডিজিটাল পার্টির আমন্ত্রণ যেটাতে আপনি অবশ্যই যোগ দিতে চান না!

স্ক্যামাররা) প্রতারক (SMS, ইমেইল বা সোশ্যাল মিডিয়ার মাধ্যমে জাল অ্যাপের লিংক পাঠায় যা দেখতে বৈধ লিংকের মতোই হয়। তারা ইউজারদেরকে সেই লিংকে ক্লিক করার জন্য লোভ দেখায় এবং জোর করে, যার ফলে অপরিচিত অ্যাপ ডাউনলোড করতে হয়। অ্যাপটা ইনস্টল করা হয়ে গেলে, স্ক্যামাররা) প্রতারক (গোপনীয় তথ্য এবং OTP সহ ডিভাইসকে সম্পূর্ণভাবে অ্যাক্সেস করতে পারে।

অজানা উৎস থেকে বা অপরিচিত ব্যক্তিদের অনুরোধে অ্যাপ ডাউনলোড করবেন না।

ডাউনলোড করার আগে অ্যাপের পাবলিশার এবং ইউজার রেটিংকে যাচাই করুন।

অনুমতি এবং অ্যাপের অনুরোধগুলিকে রিভিউ করুন) যেমন কনট্যাক্ট, ফটো (এবং শুধুমাত্র যেগুলো প্রয়োজন সেগুলোকেই অনুমতি দিন।

মনে রাখবেন, ব্যাঙ্ক বা অন্যান্য আধিকারিকরা কখনই আপনাকে এই ধরণের সংবেদনশীল তথ্য বা বিবরণের ব্যাপারে জিজ্ঞাসা করবে না।

ATM কার্ড স্কিমিং-এর জালিয়াতি

ATM স্কিমিং-কে ডিজিটাল পকেটমারির মতোই ভাবুন। আপনি যখন টাকা তুলতে বা আপনার ব্যালেন্সকে চেক করার জন্য একটা ATM ব্যবহার করেন, তখন প্রতারকেরা আপনার কার্ডের তথ্যকে রেকর্ড করার জন্য মেশিনে লুকানো ডিভাইস সেট করে রাখে। এই ডিভাইসগুলো একটা জাল কার্ড স্লট বা একটা ছোট ক্যামেরার মতোই সূক্ষ্ম হতে পারে।

ATM-কে ভালোভাবে চেক করে নিন: ATM ব্যবহার করার আগে কোনো অস্বাভাবিক অ্যাটাচমেন্ট, আলগা পার্টস বা লুকানো ক্যামেরার জন্য সবসময় কার্ড স্লট এবং কীপ্যাডকে চেক করুন।

আপনার PIN-কে ঢেকে রাখুন: আপনার PIN দেওয়ার সময় সেটাকে আপনার হাত বা শরীর দিয়ে ঢেকে রাখুন, এর ফলে ক্যামেরাতে আপনার PIN দেখা যাবে না বা অন্য কেউ সেটাকে দেখতে পাবে না।

নিয়মিতভাবে স্টেটমেন্ট চেক করুন: আপনার ব্যাঙ্ক স্টেটমেন্ট এবং লেনদেনের উপর নজর রাখুন। অপরিচিত কাজকর্ম হলে অবিলম্বে সেটার ব্যাপারে আপনার ব্যাঙ্কে অভিযোগ করুন।

কলের ক্ষেত্রে সতর্ক থাকুন: যদি কেউ আপনার ব্যাঙ্ক থেকে কথা বলছে বলে দাবি করে এবং সংবেদনশীল তথ্যের ব্যাপারে জানতে চায়, তাহলে সতর্ক থাকুন।

সুরক্ষিত ATM ব্যবহার করুন: আলোতে পরিপূর্ণ জায়গায় অবস্থিত বা ব্যাঙ্কের শাখার সাথে সংযুক্ত ATM-গুলো ব্যবহার করুন, কারণ সেখানে কারচুপি হওয়ার সম্ভাবনা কম থাকে।

আপডেট থাকুন: নিজেকে আরো ভালোভাবে সুরক্ষিত রাখতে লেটেস্ট স্ক্যাম এবং জালিয়াতির কৌশলের ব্যাপারে অবগত থাকুন।

মনে রাখবেন, সতর্ক থাকলে এবং এই পরামর্শগুলোকে মেনে চললে সেটা আপনাকে ATM কার্ড স্কিমিং জালিয়াতির শিকার হওয়া থেকে বাঁচাতে এবং আপনার টাকাকে সুরক্ষিত রাখতে সাহায্য করতে পারে।

রিমোট অ্যাক্সেস করার মাধ্যমে জালিয়াতি

স্ক্যামাররা (প্রতারক) গ্রাহকদেরকে একটা স্ক্রিন-শেয়ারিং অ্যাপ ডাউনলোড করার জন্য লোভ দেখায়। এটার মাধ্যমে, তারা আপনার ডিভাইসে লুকিয়ে থাকে, আপনার উপর নজর রাখে এবং আপনার আর্থিক তথ্যকে নিয়ে নেয়। তারপর, তারা আপনার টাকাকে ব্যবহার করে কেনাকাটা করতে যায়!
এই ধরণের স্ক্যামকে (প্রতারণা) এড়াতে, এই পরামর্শগুলো মনে রাখবেন:

যারা কল করছে তাদেরকে যাচাই করুন: কলার যে সংস্থার প্রতিনিধিত্ব করার দাবি করে সেই সংস্থার অফিসিয়াল যোগাযোগ করার তথ্যের থেকে সবসময় স্বাধীনভাবে সেই কলারের পরিচয়কে দুবার করে চেক করুন।

তাড়াহুড়ো করে কোনো সিদ্ধান্ত নেবেন না: চাপের মুখে তাড়াহুড়ো করে কোনো সিদ্ধান্ত নেবেন না। অ্যাক্সেস করার অনুমতি দেওয়ার আগে বা সংবেদনশীল তথ্য শেয়ার করার আগে চিন্তাভাবনা এবং যাচাই করার জন্য সময় নিন।

আপনার ডিভাইসকে সুরক্ষিত রাখুন: আপনার ডিভাইসকে লেটেস্ট সিকিউরিটি প্যাচগুলোর সাথে আপডেট রাখুন এবং প্রতিটা অ্যাকাউন্টের জন্য শক্তিশালী, অনন্য পাসওয়ার্ড ব্যবহার করুন।

নিজেকে শিক্ষিত করুন: সাধারণ স্ক্যাম) প্রতারণা (এবং কৌশলের ব্যাপারে জানুন যাতে সেরকম কিছু ঘটলে আপনি সেগুলোকে বুঝতে পারেন।

ব্যক্তিগত তথ্যকে সুরক্ষিত রাখুন: অনুরোধের বৈধতার ব্যাপারে নিশ্চিত না হওয়া পর্যন্ত ফোন, ইমেইল বা অনলাইনে ব্যক্তিগত অথবা আর্থিক তথ্য বা বিবরণ শেয়ার করার বিষয়ে সতর্ক থাকুন।

যে সমস্ত প্রতারকেরা আপনার ডিজিটাল জীবনে উঁকি-ঝুঁকি মারার চেষ্টা করছেন এবং দূর থেকে আপনার ডিজিটাল জীবনকে অ্যাক্সেস করার চেষ্টা করছেন তাদের জন্য আপনার ভার্চুয়াল দরজাকে বন্ধ রাখার ব্যাপারে সতর্ক থাকুন।

অনুগ্রহ করে মনে রাখবেন - যদি আপনি একটা কালো/ব্ল্যাঙ্ক) ফাঁকা (স্ক্রিন লক্ষ্য করেন, তাহলে অনুগ্রহ করে আপনার সিস্টেমে কোনো কাজ করবেন না। এটা একটা সংকেত হতে পারে যে অন্যরা আপনার স্ক্রিন দেখতে পাচ্ছে।

SIM-কে সোয়্যাপ করার মাধ্যমে জালিয়াতি

ধরে নিন যে স্ক্যামাররা) প্রতারক (ফোন চুরি হয়েছে বলে অভিযোগ জানায় !তারা আপনার পরিচয় দেওয়ার ভান করে বলে যে তাদের সিম কার্ড হারিয়ে গেছে, এবং তারা আপনার ফোন নম্বর পেয়ে যায়। এর সাথে, তারা আপনার ব্যাঙ্ক বা ইমেইলের মতো আপনার অনলাইন অ্যাকাউন্টগুলোতে ঢুকে গিয়ে একটা বিশৃঙ্খলা সৃষ্টি করতে পারে! অদলবদল করার কেলেঙ্কারিকে) সোয়্যাপ স্ক্যাম (বন্ধ করুন !নিচে দেওয়া পরামর্শগুলো মনে রাখবেন।

SIM কার্ডের পরিচয়ের বিবরণ শেয়ার করবেন না।

আপনার ফোনের নেটওয়ার্ক অ্যাক্সেসের উপর নজর রাখুন।

।যদি কিছুক্ষণের জন্য কোনো নেটওয়ার্ক না থাকে সেক্ষেত্রে ডুপ্লিকেট SIM আছে কিনা সেটা চেক করার জন্য আপনার অপারেটরের সাথে যোগাযোগ করুন।

যে সমস্ত প্রতারকেরা আপনার ডিজিটাল জীবনে উঁকি-ঝুঁকি মারার চেষ্টা করছেন এবং দূর থেকে আপনার ডিজিটাল জীবনকে অ্যাক্সেস করার চেষ্টা করছেন তাদের জন্য আপনার ভার্চুয়াল দরজাকে বন্ধ রাখার ব্যাপারে সতর্ক থাকুন।

কিভাবে কোনো প্রতারণামূলক লেনদেনের ব্যাপারে অভিযোগ জানাবেন?

www.axisbank.com-এ যান > সাপোর্ট > 'আমাদের সাথে এখানে যোগাযোগ করুন' বিভাগে যাওয়ার জন্য নিচে স্ক্রোল করুন > আমাদের সাথে কথা বলুন > 'জালিয়াতি বা সমস্যার ব্যাপারে অভিযোগ করুন' নির্বাচন করুন > জালিয়াতির ব্যাপারে অভিযোগ করুন > আপনার প্রশ্নের ড্রপ-ডাউনের তালিকা থেকে প্রাসঙ্গিক বিকল্প বেছে নিন > কল করুন-এ ক্লিক করুন

RBI-এর কাছে অভিযোগ জানাতে, https://cms.rbi.org.in-এ যান

টোল-ফ্রি নম্বর 14448-এ **কল করুন**) সোমবার থেকে শুক্রবার, সকাল 9:30 থেকে বিকাল 5:15 পর্যন্ত, জাতীয় ছুটির দিনগুলো বাদ দিয়ে(।

একটা ফিজিক্যাল অভিযোগ করুন: 'সেন্ট্রালাইজড রিসিপ্ট অ্যান্ড প্রসেসিং সেন্টার, 4র্থ ফ্লোর, ভারতীয় রিজার্ভ ব্যাঙ্ক, সেক্টর- 17, সেন্ট্রাল ভিস্তা, চণ্ডীগড় - 160 017-এ চিঠি পাঠান / পোস্ট করুন। প্রয়োজনীয় ফরম্যাটের ব্যাপারে বিস্তারিত জানতে **অনুগ্রহ করে** https://cms.rbi.org.in-এ **যান**।

সাইবার ক্রাইমে অভিযোগ করতে, হেল্পলাইন নম্বর **155260** বা **1930** ডায়াল করুন বা জাতীয় সাইবার ক্রাইম রিপোর্টিং পোর্টালে**) www.cybercrime.gov.in)** ঘটনাটির ব্যাপারে অভিযোগ জানান।