यहां भी धोखे,

वहां भी धोखे,

खोजते रहिए इन सब से सुरक्षित बने रहने के मौके!

#BankingDhyaanSe 2.0

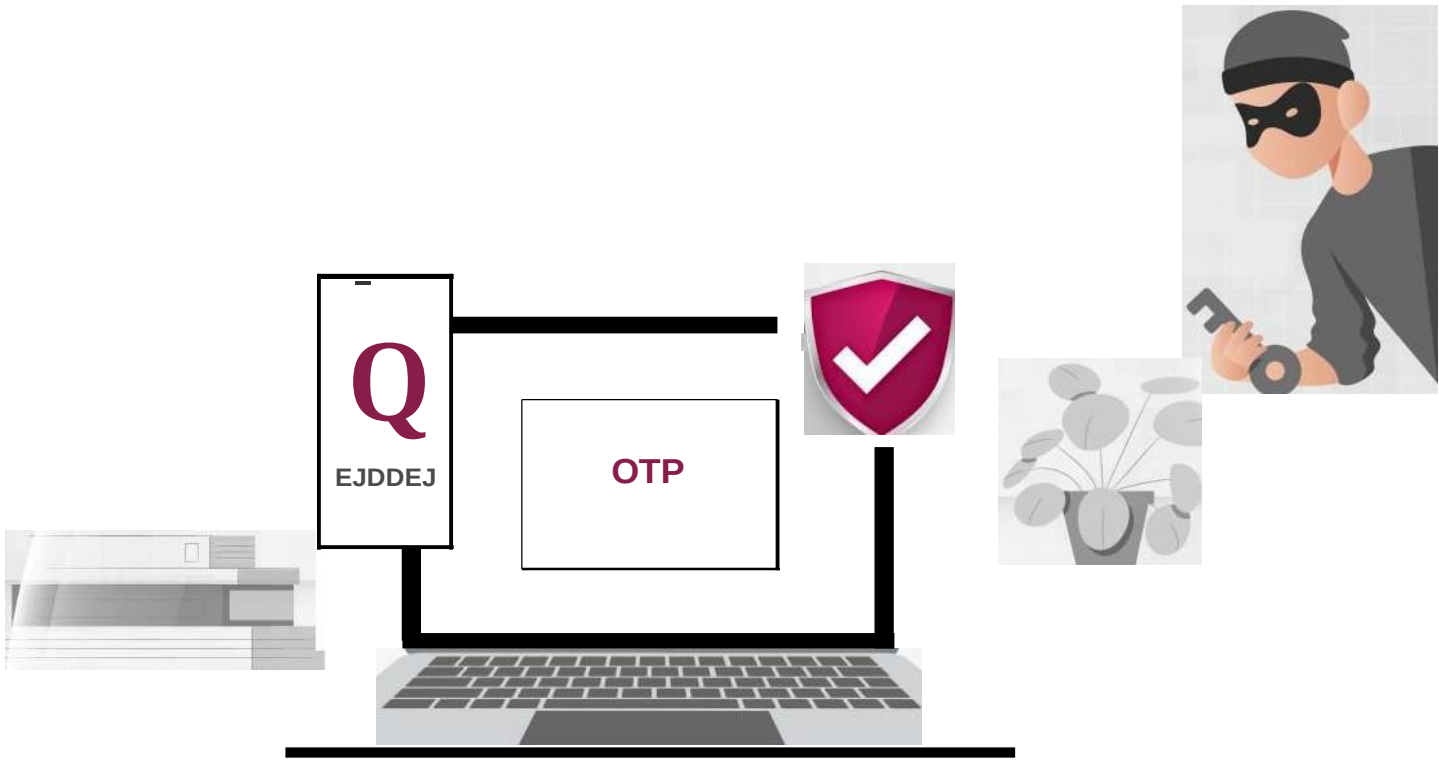
AXIS BANK

आप कड़ी मेहनत करके धन कमाते हैं, तो क्यों न अपनी इस कमाई को सुरक्षित भी रखें?

वित्तीय घोटालों को समझने और उन्हें रोकने के लिए बनाई गई इस **एक्सिस बैंक फ्रॉड अवेयरनेस बुकलेट #BankingDhyaanSe 2.0** में आपका स्वागत है। तेज़ी से प्रगति कर रहे इस डिजिटल दौर में, धोखेबाजों के खिलाफ ज्ञान ही आपकी रक्षा ढाल बन सकती है। यह गाइडबुक आपको अपनी मेहनत से कमाए गए धन की सुरक्षा से जुड़ी बारीकियों, असल जीवन के उदाहरण और व्यावहारिक सुझाव देकर मदद करने के लिए बनी है।

एक्सिस बैंक आपके भरोसेमंद बैंकिंग भागीदार के रूप में, आपकी अपनी किसी भी डिजिटल प्रक्रिया में आत्मविश्वास से आगे बढ़ने में मदद करने के लिए समर्पित है। आइए, साथ मिलकर धोखाधड़ी से बचें और आपके उज्जवल वित्तीय भविष्य को सुरक्षित बनाएं।

ओटीपी स्कैम



आपका वन-टाइम पासवर्ड (OTP) आपके अभेद्य डिजिटल साम्राज्य में दाखिल होने की सुनहरी चाबी की तरह होता है।

आपको अपनी इस कीमती चाबी को धोखेबाज़ों से बचाने के लिए, सतर्क होकर रक्षा करनी होगी!

अपना ओटीपी (OTP) गोपनीय रखें: किसी के साथ फ़ोन कॉल, ई-मेल, टेक्स्ट मैसेज या सोशल मीडिया पर कभी भी अपना ओटीपी साझा न करें और इस बारे में एक मुस्तैद प्रहरी की तरह सतर्क रहें।

हर अनुरोध का सत्यापन करें: किसी भी अनुरोध को सत्यापित करने के बाद ही भरोसा करें। अगर आपको अचानक कोई ओटीपी का अनुरोध मिलता है या अगर आपको शक हो, तो जल्दबाजी न करें। कोई भी प्रतिक्रिया देने से पहले इसकी प्रामाणिकता की जांच करें।

हमेशा आधिकारिक वेबसाइट या ऐप का इस्तेमाल करें: ओटीपी को साझा करने में सावधान रहें। हमेशा सीधे आधिकारिक साइट या ऐप पर जाएं - कोई शॉर्टकट नहीं। इन मामलों में, किसी लिंक पर क्लिक करने के बजाए इसे टाइप करना एक बेहतर विकल्प होता है।

किसी भी अनुरोध में जल्दीबाजी करने पर सावधान रहें: स्कैमर अक्सर आपको अपना OTP साझा करने के लिए दबाव डालने के लिए, इसे जल्द से जल्द करने की ज़रूरत की भावना पैदा करने की कोशिश करते हैं। ऐसे में एक कदम पीछे हटें, गंभीरता से सोचें, और कुछ भी करने से पहले अनुरोध का सत्यापन करें।

2 फ़ैक्टर-ऑथेंटिकेशन का विकल्प एक्टिवेट करें: 2 फ़ैक्टर-ऑथेंटिकेशन (दो-तरफ़ा प्रमाणीकरण) के साथ अपनी सुरक्षा को दोगुना करें। इसके लिए ऐप-आधारित या हार्डवेयर टोकन जैसे मजबूत विकल्प चुनें। वे हमेशा एसएमएस (SMS) ओटीपी से बेहतर होते हैं।

हमेशा याद रखें, बैंक आपसे आपका सीवीवी (CVV), ओटीपी, पिन, कार्ड नंबर, पासवर्ड आदि नहीं पूछेगा। ये विवरण कभी किसी के साथ साझा न करें।

क्रेडिट कार्ड स्कैम

आइए, क्रेडिट कार्ड की धोखाधड़ी को एक धूर्त लुका-छिपी के खेल जैसा समझें। इसमें कोई धोखेबाज़ आपसे अपने असली इरादों को छिपाने की और साथ में आपको धोखा देकर आपसे क्रेडिट कार्ड की जानकारी देखने की कोशिश करता है।

उनके जाल में फंसने से बचने के लिए इन सुझावों को ध्यान में रखें:

धोखेबाज़ों से सावधान रहें: धोखेबाज़ व्यक्ति आपके बैंक या किसी और जानी-पहचानी कंपनी से होने का दिखावा कर सकते हैं। उनकी चाल में न फंसें; उन्हें अपनी पहचान का सत्यापन करने को कहें।

अपने स्टेटमेंट की जांच करें: अपने क्रेडिट कार्ड स्टेटमेंट की नियमित रूप से समीक्षा करें। यदि आपको इसमें कभी कोई अनजाना खर्च या शुल्क दिखे, तो यह लुका-छिपी के खेल में छिपे हुए खिलाड़ियों को ढूंढ लेने जैसा है - उन्हें तुरंत पकड़ें।

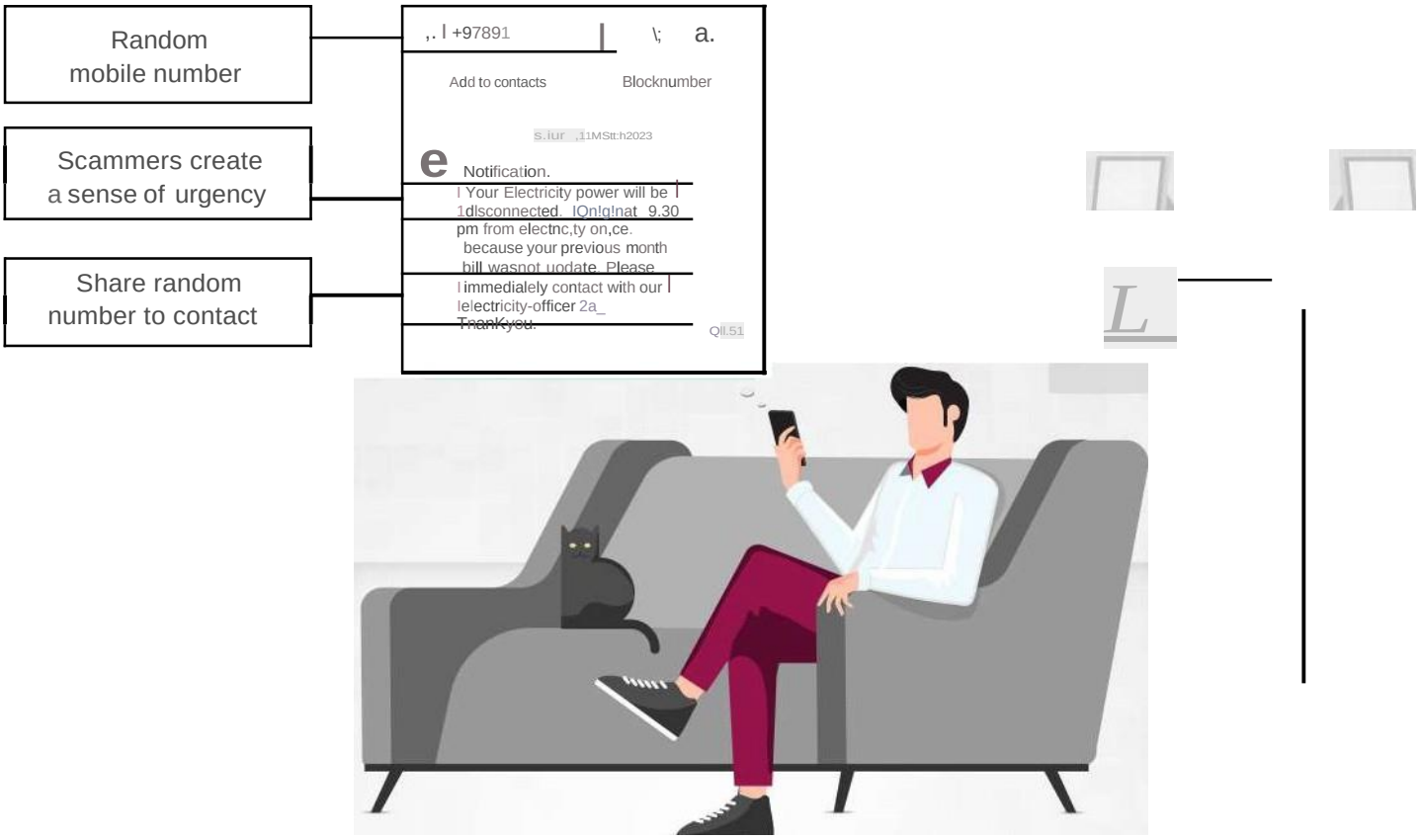
लेन-देन की सीमा निर्धारित करें: अपने सभी भुगतान चैनलों पर लेन-देन करने की एक सीमा निर्धारित करें और इसे अपनी ज़रूरत के अनुसार 'मैनेज यूसेज' सेक्शन में दर्ज करें।

केवल सुरक्षित वेबसाइट: हमेशा ऑनलाइन खरीदारी करते समय इस बात का ख्याल रखें कि वह वेबसाइट सुरक्षित हो (URL में "https" देखें)। यह हमारे खेल के लिए एक सुरक्षित खेल का मैदान चुनने जैसा है।

अपडेट रहें: आजकल के दौर में किए जा रहे घोटाले के समाचार पर नज़र रखें, ठीक वैसे ही जैसे आप खेल में नई रणनीतियां सीखते हैं। इस तरह, आप इन धोखेबाज़ों को मात देने के लिए तैयार रहेंगे।

बिजली के बिल की धोखाधड़ी

किसी फ़र्जी एसएमएस की पहचान कैसे करें?



कल्पना कीजिए: आप घर पर आराम से शाम का आनंद ले रहे हैं, अपना पसंदीदा धारावाहिक देख रहे हैं, तभी आपका फ़ोन एक इनकमिंग मैसेज के साथ बजता है। यह आपका बिजली प्रदाता है, और मैसेज में लिखा है कि आपको अपने नवीनतम बिल में बहुत बड़ी धनराशि का भुगतान करना होगा।

ऐसे में घबराने से पहले, इस बात पर विचार करें: आपके जीवन में बिजली बिल की धोखाधड़ी का मामला किसी गुप्त प्रेत की तरह, बिना किसी चेतावनी के घटित हो सकता है।

कभी भी अपनी गोपनीय जानकारी किसी के साथ साझा न करें और किसी भी अवांछित लिंक पर क्लिक न करें।

बिल का भुगतान करने के लिए केवल आधिकारिक और सुरक्षित वेबसाइट का ही उपयोग करें।

याद रखें, बिजली विभाग से कभी भी आपको कोई व्यक्तिगत जानकारी मांगने या अनजान/ अपंजीकृत नंबरों के माध्यम से भुगतान करने का सुझाव नहीं दिया जाएगा।

जॉब स्कैम

कल्पना कीजिए कि आप नौकरी की लिस्टिंग देख रहे हैं और अचानक आपको एक ऐसा जॉब ऑफ़र मिलता है जो आपकी सोच से भी ज़्यादा अच्छा लगता है। हो सकता है कि इसमें असीमित छुट्टियां, पजामा पहनकर काम करने की सुविधा और डेटा एंट्री के काम के लिए छह अंकों का वेतन मिल रहा हो। आप कहेंगे कि मुझे यही तो चाहिए!

लेकिन ऐसे में "अभी आवेदन करें" बटन दबाने से पहले एक पल ठहरिए!

कंपनी के बारे में रिसर्च करें: इस कंपनी के बारे में ऑनलाइन पता करें और सुनिश्चित करें कि वास्तविक है। धोखेबाज अक्सर किसी विश्वसनीय वेबसाइट के नाम की नकली कंपनियां बना लेते हैं।

कोई भी अग्रिम भुगतान न करें: कोई भी असली नियोक्ता आपसे काम शुरू करने से पहले प्रशिक्षण की सामग्री या कंपनी की पृष्ठभूमि आदि के बारे में जानने के लिए कोई भुगतान करने को नहीं कहेंगे।

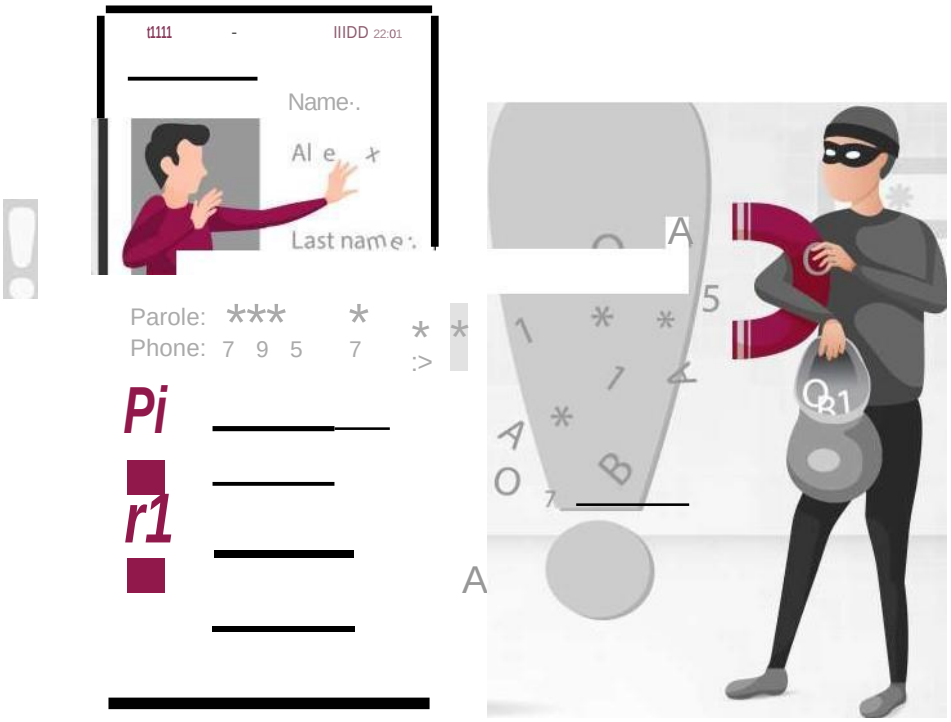
किसी भी संदेह के संकेत पर नज़र रखें: अगर इस नौकरी में आपसे सोशल सिक्योरिटी नंबर या कोई और संवेदनशील वित्तीय जानकारी मांगी जाती है तो इस बारे में सावधान रहें।

नौकरी देने में जल्दबाजी करना: अगर आपको किसी साक्षात्कार या अधिक जानकारी देने के लिए बजाए तुरंत नौकरी की पेशकश कर दी जाती है, तो यह एक धोखाधड़ी का मामला हो सकता है।

अपने मन की आवाज़ सुनें: अगर आपको कुछ भी गड़बड़ लगे, तो अपने अंदर की आवाज़ पर भरोसा कर सावधानी के साथ आगे बढ़ें या वहां से चले जाएं।

याद रखें, नौकरी तलाशते समय भी अपनी व्यक्तिगत और वित्तीय जानकारी की सुरक्षा आपकी पहली प्राथमिकता होनी चाहिए।

कॉल स्पूफ़िंग स्कैम



जिस तरह से एक जादूगर चीज़ों को उनकी वास्तविक पहचान से अलग दिखा सकता है, उसी तरह से धोखा करने वाले स्कैमर आपकी कॉलर आईडी में नकली हेर-फ़ेर करके ऐसा दिखा सकते हैं कि वे जाने-पहचाने और भरोसेमंद व्यक्ति या संगठन है – जैसे इस मामले में, आपका बैंक। यह उनकी असली पहचान को छिपाने के लिए एक डिजिटल नकाब की तरह है।
खुद को ऐसी चालों से बचाने के लिए, इन सुझावों को याद रखें:

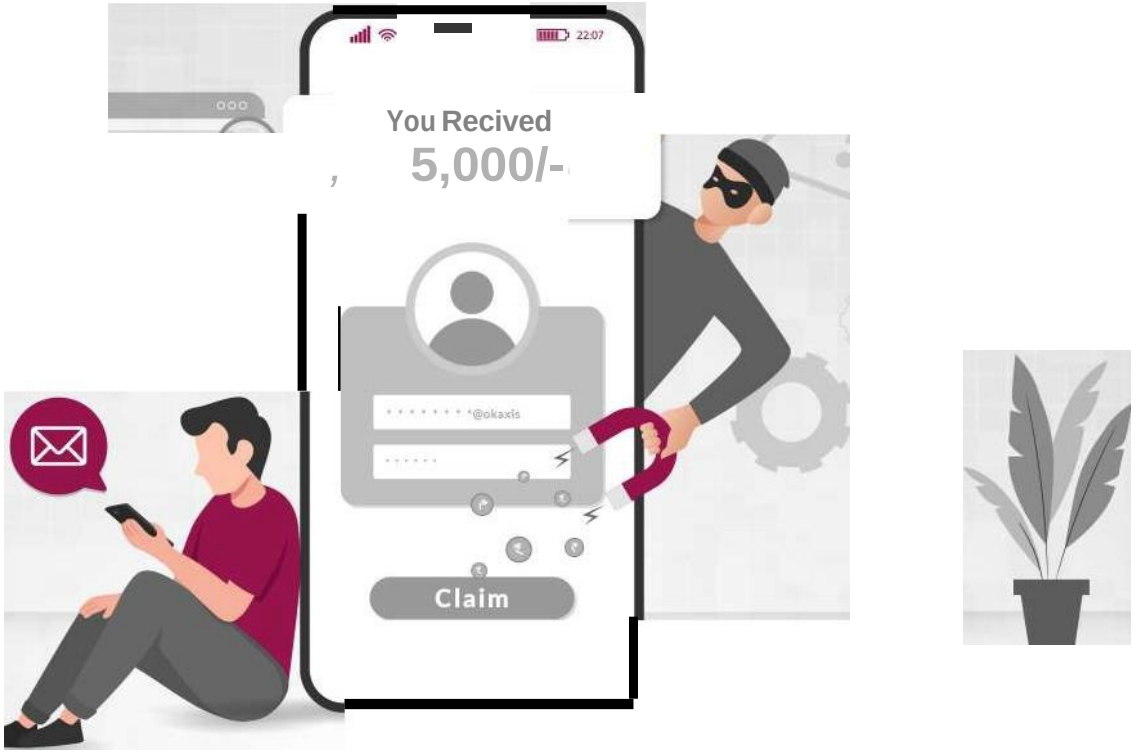
सावधानी से पहचान को सत्यापित करें: भले ही कॉलर आईडी आपको परिचित लगे, लेकिन सावधान बने रहें। अगर कोई व्यक्ति आपसे कोई संवेदनशील जानकारी मांगता है, तो किसी और तरीके से उसकी पहचान को दोबारा सत्यापित करें।
व्यक्तिगत जानकारी साझा न करें: कभी भी फ़ोन पर कोई ही व्यक्तिगत या वित्तीय जानकारी न दें, भले ही कॉल करने वाला व्यक्ति भरोसेमंद क्यों न लगे। कॉल को बंद करें और किसी दूसरे विश्वसनीय नंबर से उसे दोबारा कॉल करें।
निजी जानकारी की सुरक्षा करें: आप जो भी निजी जानकारी ऑनलाइन या सोशल मीडिया पर साझा करते हैं, उसके बारे में सावधान रहें। धोखेबाज़ अक्सर अपनी नकली कॉल को ज़्यादा विश्वसनीय बनाने के लिए इन स्रोतों से मिली जानकारी का इस्तेमाल करते हैं।
कॉल ब्लॉकिंग सेवा का इस्तेमाल करें: अपने फ़ोन वाहक से मिले कॉल-ब्लॉकिंग ऐप या सेवाओं का उपयोग करें। वे किसी संभावित स्कैम कॉल को आने से रोकने में मदद कर सकते हैं।

गूगल या किसी भी सर्च इंजन पर फ़ोन नंबर को न खोजें। अगर आप ऐसा करते हैं, तो किसी संस्था या व्यापारी द्वारा भेजे जाने वाले किसी भी लिंक पर क्लिक न करें।

इसके अलावा, अपने डिवाइस पर केवल अधिकृत एप्लिकेशन स्टोर से ही बैंकिंग एप्लिकेशन के नवीनतम संस्करण को डाउनलोड करें। कृपया समय-समय पर इसके नवीनतम संस्करण के लिए जांच कर लिया करें।

याद रखें, जैसे आप वास्तविक जीवन में किसी नकाबपोश अजनबी पर भरोसा नहीं करते, वैसे ही फ़ोन पर किसी नकाबपोश कॉलर पर भी भरोसा न करें। सावधान रहें!

यूपीआई रिफंड स्कैम



कल्पना कीजिए कि आप अपने फ़ोन पर स्क्रॉल कर रहे हैं और अचानक आपको यूपीआई (UPI) रिफंड का नोटिफ़िकेशन मिलता है, और आप खुशी से झूम उठते हैं! लेकिन एक पल ठहरिए। यह यूपीआई रिफंड धोखाधड़ी करने की कोशिश भी हो सकती है!

यूपीआई या यूनिफाइड पेमेंट्स इंटरफ़ेस हमारी रोज़मर्रा की ज़िंदगी का हिस्सा बन गया है। अपने घर के पास के किराना स्टोर पर भुगतान करने से लेकर फ़ोन रिचार्ज करने और फ़्लाइट टिकट बुक करने तक, हम कई कामों के लिए यूपीआई पेमेंट का इस्तेमाल करते हैं। इसलिए धोखेबाज़ों ने यूपीआई ऐप का इस्तेमाल करके लोगों को ठगने के लिए नए-नए तरीके अपनाने शुरू कर दिए हैं।

कभी भी उनकी आधिकारिक शब्दावली और पेशेवर बोली के झांसे में न आएं। यहां दिए गए सुझावों को ध्यान में रखें:

किसी भी तरह के लिंक से सावधान रहें: हो सकता है कि धोखेबाज़ आपको रिफंड हासिल करने के लिए कोई लिंक भेज कर आपसे पंजीकरण करने को कहे।

दबाव बनाने की तरकीबें: वे जल्दी से धन हासिल करने के लिए आप पर अपना बैंक विवरण या यूपीआई पिन साझा करने का दबाव डालेंगे।

पात्रता को सत्यापित करें: सब से पहले यह देखें कि क्या आप सचमुच रिफ़ंड के लिए पात्र बने हैं। अगर यह उचित और वास्तविक हो, तो किसी विश्वसनीय स्रोत से इसकी जांच करें।

याद रखें, बैंक या कोई अन्य अधिकारी आपसे कभी भी ऐसे संवेदनशील विवरण नहीं मांगेंगे।

फ़िशिंग स्कैम

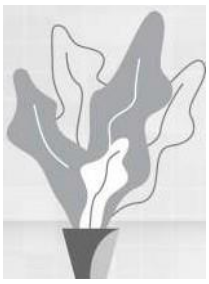
कल्पना कीजिए कि आप एक मछली हैं जो साफ तालाब में शांति से तैर रही है और अपना काम कर रही है। अचानक, एक चमकदार, आकर्षक चारा आपके सामने लटकता है। आप उत्सुक हो जाते हैं लेकिन एक पल के लिए ठहर कर देखें - कुछ तो गड़बड़ है!
डिजिटल क्षेत्र में फ़िशिंग घोटालों में ठीक यही होता है।

जैसे मछली को चारा देकर फंसाया जाता है, ठीक वैसे ही साइबर अपराधी कोई भरोसेमंद व्यक्ति बनकर आपसे संवेदनशील जानकारी हासिल करने की कोशिश करते हैं। वे आपको नकली ईमेल, संदेश या वेबसाइट भेजते हैं जो वैध लग सकती हैं, जिसमें वे अक्सर बैंकों, सोशल मीडिया या आपके बॉस की नकल कर सकते हैं।
इस डिजिटल धोखे से बचने के लिए इन सुझावों को याद रखें:

वेबसाइट के **यूआरएल** (URL) की दोबारा जांच करें: लिंक पर माउस घुमाकर देखें कि वे वास्तव में कहां ले जाते हैं।
कोई भी व्यक्तिगत जानकारी साझा न करें: कानून का पालन करने वाली संस्थाएं ईमेल के माध्यम से आपसे कोई भी संवेदनशील जानकारी नहीं मांगती हैं।
rl2J **शक की निगाह बनाए रखें:** अचानक मिलने वाले अनुरोधों पर कोई भी कार्रवाई करने से पहले अन्य तरीकों से इसके सही होने की जांच करें।
l@l:'\,. **सिक्योरिटी सॉफ्टवेयर को अपडेट करें:** अपने डिजिटल किले को नवीनतम सुरक्षा उपायों से लैस रखें।

एक सावधान मछली की तरह सजग रहें और इंटरनेट के विशाल महासागर में होशियारी के साथ तैरने का आनंद लें।

विशिंग स्कैम



a

आपके फ़ोन की घंटी बजती है, और यह आपके तथाकथित बैंक का 'बेहद ज़रूरी' फ़ोन कॉल है, जिसमें दावा किया जाता है कि आपके खाते से छेड़छाड़ की गई है, या फिर हो सकता है कि यह एक 'बड़ी जीत' वाला कॉल हो है, जिसमें पता चलता है कि आज आपका भाग्यशाली दिन है, और आपने कोई बड़ा ईनाम जीत लिया है!

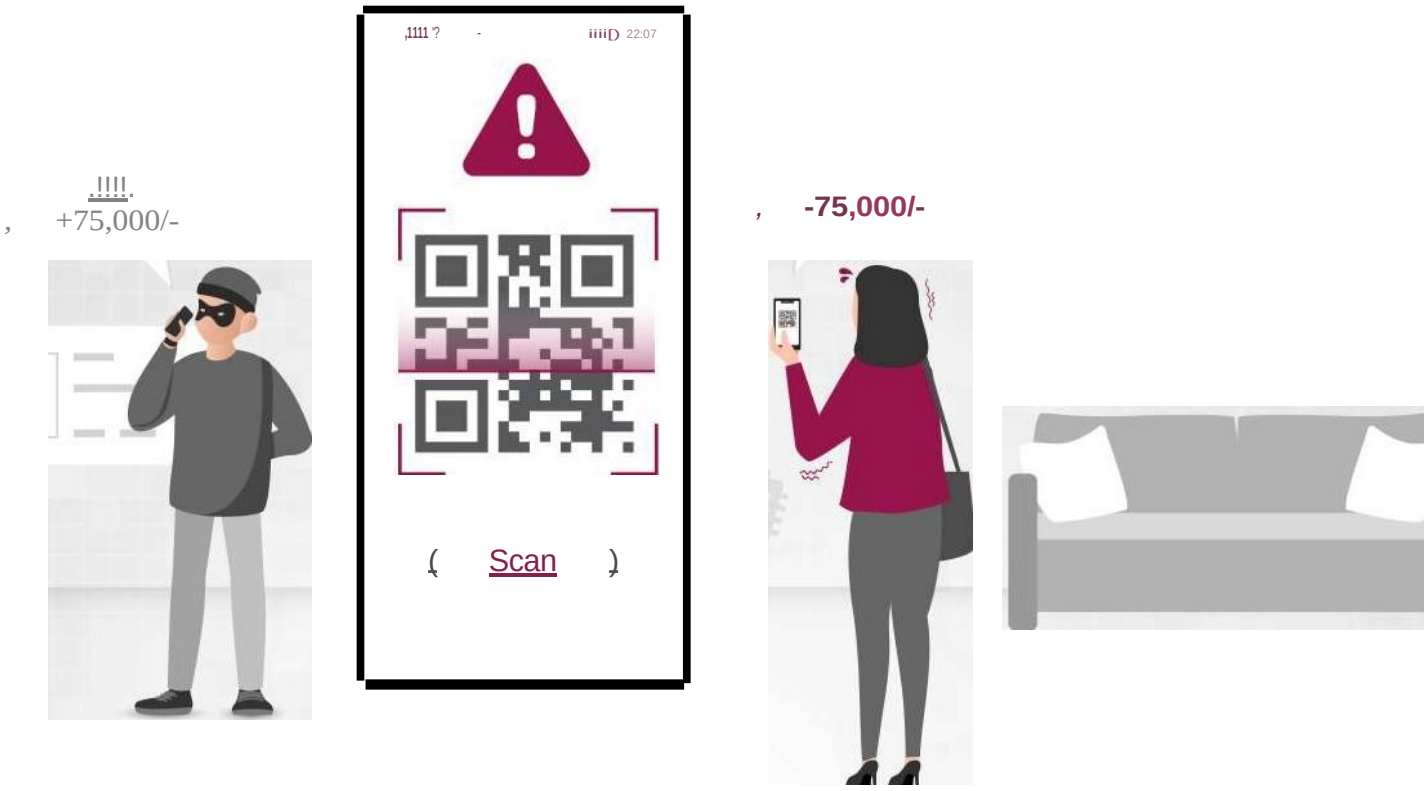
ज़रा, एक पल ठहरें (सचमुच)!

ऐसे धोखे से सुरक्षित रहने के लिए निम्नलिखित सुझाव याद रखें:

- कभी भी फ़ोन पर अपनी व्यक्तिगत जानकारी साझा न करें।
- शरलॉक होम्स की तरह बनें और कॉल करने वाले की असली पहचान का पता लगाएं।
- बेमतलब के झमेले में मत पड़ें! जब वे गर्ममिजाज़ होने की कोशिश करें तो शांत बने रहें।

याद रखें कि ऑनलाइन अजनबियों के साथ जानकारी साझा करने में सावधान रहना चाहिए- अपनी जानकारी को सुरक्षित रखने के लिए होशियार रहें!

UPI स्कैम - रिक्वेस्ट मनी का विकल्प



स्नेहा ने एक ऑनलाइन खरीदारी की ऐप पर अपने फ़र्नीचर का विज्ञापन दिया। एक खरीदार ने खुद को अर्धसैनिक बल का जवान बताते हुए उसे व्हाट्सएप पर भुगतान के लिए एक क्यूआर कोड भेजा। स्नेहा ने उसे स्कैन किया और 75,000 रुपए गंवा दिए।

क्या यह बात आपको पहले भी कहीं सुनी हुई लग रही है? क्या आप यूपीआई (UPI) भुगतान प्लेटफ़ॉर्म का लगातार इस्तेमाल करते हैं और इसलिए यूपीआई धोखाधड़ी का शिकार होने से डरते हैं?

हमेशा याद रखें:

यूपीआई पिन केवल भुगतान करने के लिए इस्तेमाल की जाती है, भुगतान प्राप्त करने के लिए नहीं।

अगर कभी भी आपसे भुगतान प्राप्त करने के लिए यूपीआई पिन मांगा जाता है, तो तुरंत रुक जाएं! बहुत संभावना है कि यह वास्तव में भुगतान लेने का नहीं, बल्कि भुगतान करने अनुरोध हो।

कभी भी अपने ओटीपी, यूपीआई पिन या कोई भी गोपनीय जानकारी किसी के साथ साझा न करें।

किसी भी भुगतान को आरंभ करने से पहले हमेशा यूपीआई एप्लीकेशन में मोबाइल नंबर और नाम को सत्यापित कर लें।

क्यूआर कोड स्कैन की धोखाधड़ी

पेमेंट ऐप पर क्यूआर कोड को सावधानी से स्कैन करें; उनमें धन के लेनदेन के लिए खाते की जानकारी होती है।

कभी भी धन प्राप्त करने के लिए क्यूआर कोड को स्कैन न करें; धन प्राप्त करने के लिए लेनदेन में बारकोड / क्यूआर कोड को स्कैन करना या मोबाइल बैंकिंग पिन (m-PIN), पासवर्ड आदि दर्ज करने की कोई ज़रूरत नहीं होती है।

बहुत संभावना है कि जो खरीदार/विक्रेता आपसे अनुचित जल्दबाजी या उत्सुकता दिखा रहा है, वह कोई धोखेबाज़ है। शांत रहें, हमेशा जल्दीबाजी करने का स्पष्टीकरण मांगें और सभी ज़रूरी सवाल पूछें।

अनजाने मोबाइल ऐप की धोखाधड़ी

आपको किसी एसएमएस (SMS), ईमेल, या किसी लंबे समय से बिछड़े हुए चचेरे भाई का एक संदेश मिलता है, जिसके बारे में आपको कभी पता भी नहीं था। इन सभी में एक लिंक दिया होता है जो आपके पसंदीदा और जाने-पहचाने ऐप से आया हुआ लगता है।
एक मिनट के लिए रुकिए! ये कोई आम डाउनलोड नहीं हैं; ये किसी ऐसी डिजिटल पार्टी के लिए निमंत्रण हैं जिसमें आप आमतौर पर निश्चित रूप से शामिल नहीं होना चाहेंगे!
धोखा देने वाले स्कैमर एसएमएस, ईमेल या सोशल मीडिया के ज़रिए फ़र्जी ऐप लिंक भेजते हैं जो किसी वैध ऐप जैसे दिखते हैं। वे यूज़र को उन पर क्लिक करने के लिए उकसाते हैं, जिससे कोई अनजाने ऐप डाउनलोड हो जाते हैं। इनके इंस्टॉल होने के बाद, स्कैमर आपकी गोपनीय जानकारी और ओटीपी जैसे डिवाइस की हर जानकारी तक पहुंच सकते हैं।

अनजाने स्रोतों से या अजनबियों के द्वारा भेजे गए किसी भी ऐप को डाउनलोड करने से बचें।

डाउनलोड करने से पहले ऐप के पब्लिशर और यूज़र रेटिंग को सत्यापित करें।

किसी भी अनुमति और ऐप रिक्वेस्ट (जैसे कांटैक्ट, फ़ोटो) की समीक्षा करें और केवल ज़रूरी अनुमतियां ही दें।

याद रखें, बैंक या कोई अन्य अधिकारी आपसे कभी भी ऐसी संवेदनशील जानकारी नहीं मांगेंगे।

एटीएम कार्ड स्किमिंग की धोखाधड़ी

एटीएम (ATM) स्किमिंग को डिजिटल पिकपॉकेटिंग की तरह समझें। जब आप पैसे निकालने या अपना बैलेंस चेक करने के लिए एटीएम का इस्तेमाल करते हैं, तो धोखेबाज़ आपके कार्ड की जानकारी रिकॉर्ड करने के लिए मशीन पर छिपे हुए डिवाइस लगा देते हैं। ये डिवाइस नकली कार्ड स्लॉट या छोटे कैमरे की तरह आम तौर पर दिखाई नहीं पड़ने वाले हो सकते हैं।

एटीएम मशीन का निरीक्षण करें: एटीएम को इस्तेमाल करने से पहले हमेशा इसके कार्ड स्लॉट और कीपैड की जांच करें कि कहीं कोई असामान्य सामान, ढीला हिस्सा या छिपा हुआ कैमरा तो नहीं लगा हुआ है।

अपने पिन को ढक कर दर्ज करें: अपने पिन को अपने हाथ या शरीर से ढक लें, ताकि कैमरे या किसी और के लिए इसे देखना मुश्किल हो जाए।

नियमित रूप से स्टेटमेंट की जांच करें: अपने बैंक स्टेटमेंट और लेन-देन पर नज़र रखें। किसी भी अपरिचित गतिविधि मिलने पर अपने बैंक को इसकी तुरंत रिपोर्ट करें।

कॉल से सावधान रहें: अगर कोई व्यक्ति आपके बैंक का कर्मचारी होने का दावा करते हुए कॉल करता है और संवेदनशील जानकारी मांगता है, तो सावधान रहें। बैंक कभी भी फ़ोन पर पिन या पूरा कार्ड नंबर नहीं मांगते हैं।

सुरक्षित एटीएम मशीनों का इस्तेमाल करें: अच्छी रोशनी वाले स्थानों पर लगे या बैंक शाखाओं के पास लगे एटीएम का इस्तेमाल करें, क्योंकि इनके साथ छेड़छाड़ करने की संभावना कम होती है।

अपडेट रहें: अपने आप को बेहतर सुरक्षित रखने के लिए नए घोटालों और धोखाधड़ी की तरकीबों के बारे में जानकारी रखें।

याद रखें, सावधान रहने और इन सुझावों का पालन करने से आप एटीएम कार्ड स्कीमिंग की धोखाधड़ी का शिकार होने से बच सकते हैं और अपने धन को सुरक्षित रख सकते हैं।

रिमोट एक्सेस की धोखाधड़ी

स्कैमर ग्राहकों को स्क्रीन-शेयरिंग ऐप डाउनलोड करने के लिए लालच देते हैं। इसके ज़रिए, वे आपके डिवाइस में घुस कर आप पर जासूसी कर सकते हैं और आपकी वित्तीय जानकारी चुरा लेते हैं। फिर, वे आपके पैसे से शॉपिंग करने निकल पड़ते हैं!
ऐसे घोटालों से बचने के लिए इन सुझावों को याद रखें:

कॉल करने वालों की पहचान को सत्यापित करें: हमेशा कॉल करने वाले व्यक्ति की पहचान की दोबारा जांच करें, इसके लिए आप उस संगठन की आधिकारिक संपर्क जानकारी देख सकते हैं जिसका वे प्रतिनिधित्व करने का दावा करते हैं।

जल्दबाजी में कोई निर्णय न लें: दबाव में आकर कोई निर्णय न लें। किसी को कोई एक्सेस देने या संवेदनशील जानकारी साझा करने से पहले सोचकर फ़ैसला करने के लिए समय लें।

अपने डिवाइस को सुरक्षित रखें: अपने डिवाइस को नवीनतम सिक्योरिटी पैच के साथ अपडेट रखें और हर एक खाते के लिए मजबूत, और अनूठे पासवर्ड का इस्तेमाल करें।

खुद को शिक्षित करें: सामान्य धोखाधड़ी और इन्हें पहचानने के तरीकों के बारे में जानें ताकि आप इन मामलों को पहचान सकें।

अपनी व्यक्तिगत जानकारी की सुरक्षा करें: जब तक आप किसी भी अनुरोध की वैधता के बारे में सुनिश्चित न हों, तब तक फ़ोन, ईमेल या ऑनलाइन रूप से कोई भी व्यक्तिगत या वित्तीय जानकारी साझा करने से बचें।

अपने डिजिटल जीवन में घुसपैठ करने की कोशिश कर रहे दूर बैठे धोखेबाजों के लिए सभी वर्चुअल दरवाजे बंद करने के बारे में सतर्क रहें।
कृपया ध्यान दें – अगर आपको काली/खाली स्क्रीन दिखाई दे, तो अपने सिस्टम पर कोई भी कार्रवाई न करें। यह इस बात का संकेत हो सकता है कि आपकी स्क्रीन को किसी दूसरे व्यक्ति के द्वारा देखा जा रहा है।

सिम स्वैप की धोखाधड़ी

कल्पना कीजिए कि कोई स्कैमर फ़ोन से लूट करने की कोशिश कर रहा है! वे यह कहते हुए आप होने का दिखावा करते हैं कि उनका सिम कार्ड खो गया है, और ऐसे वे आपका नंबर हासिल कर सकते हैं। इस जानकारी के साथ वे आपके ऑनलाइन खातों, जैसे कि आपके बैंक या ईमेल में सेंध लगाकर बड़ी लूट मचा सकते हैं!

इस स्वैप स्कैम से बचें! यहां दिए गए कुछ सुझाव याद रखें।

- अपने सिम कार्ड की जानकारी साझा न करें।
- अपने फ़ोन के नेटवर्क एक्सेस पर नज़र रखें।

  अगर कुछ समय तक आपके सिम पर नेटवर्क न आए तो अपने ऑपरेटर से इसके **डुप्लिकेट सिम** के बारे में जानकारी लेने के लिए संपर्क करें।

दूर बैठे धोखेबाजों को आपके डिजिटल जीवन में घुसपैठ करने की कोशिशों से सुरक्षित रहने के लिए, आपसे वर्चुअल संपर्क करने के सभी तरीकों के बारे में सजग रहें।

किसी लेनदेन की धोखाधड़ी को रिपोर्ट कैसे करें?

इसके लिए **www.axisbank.com** > Support (सपोर्ट) > 'Reach us here'(रीच अस हेयर) सेक्शन तक स्क्रॉल करें > Speak with us (स्पीक विद अस) > 'Report a fraud or Dispute'(रिपोर्ट अ फ्रॉड ऑर डिस्प्यूट) > Report a Fraud (रिपोर्ट अ फ्रॉड) विकल्प को चुनें > अपने मामले के अनुसार, ड्रॉप-डाउन सूची से प्रासंगिक विकल्प चुनें> Call (कॉल) पर क्लिक करें

RBI में शिकायत दर्ज करने के लिए, https://cms.rbi.org.in वेबसाइट पर जाएं।

टोल-फ़्री नंबर 14448 पर कॉल करें (सोमवार से शुक्रवार, सुबह 9:30 बजे से शाम 5:15 बजे तक, राष्ट्रीय अवकाशों को छोड़कर)।

शिकायत की लिखित प्रति भेजें: अपने पत्र/डाक को 'सेंट्रलाइज्ड रिसीट ऐंड प्रोसेसिंग सेंटर, चौथी मंजिल, भारतीय रिज़र्व बैंक, सेक्टर-17, सेंट्रल विस्टा, चंडीगढ़ - 160 017' पर भेजें। पत्र के प्रारूप पर अधिक जानकारी के लिए **https://cms.rbi.org.in** वेबसाइट पर जाएं।

किसी साइबर अपराध की घटना की रिपोर्ट करने के लिए हेल्पलाइन नंबर **155260** या **1930** डायल करें या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल **(www.cybercrime.gov.in)** पर जाएं।
