

CUSTOMER AWARENESS

Do's and Don'ts for Safe Banking



1. Secure Your Banking Information

Always secure your debit card and keep it in a safe place. Memorize your ATM/debit card PIN, and avoid writing it on anything. Change your passwords and PINs regularly, especially for internet and mobile banking.

2. Monitor Your Accounts

Regularly check your transaction history for any unauthorized activities. Immediately report any suspicious transactions to the bank through:
Customer care: 022 6868 1414
Email: customercare@finobank.com
Fraud reporting email: reportfraud@finobank.com
Use Fino Payments Bank's mobile app to monitor your account and block/unblock your cards as needed.

3. Use Strong Security Measures

Keep your mobile banking apps, operating systems, and antivirus software updated. Enable multi-factor authentication (MFA) wherever possible for an additional layer of security.

4. Beware of Phishing Scams

Only click on links from trusted sources. Check for the official Fino Payments Bank website or contact through their known channels. Be cautious of unsolicited emails, calls, or messages asking for sensitive information. Look for phishing red flags: grammar mistakes, strange URLs, and urgent requests for personal details.

5. Conduct Safe Transactions

When using ATMs or POS terminals, check for skimming devices or any suspicious activities. Always shield the keypad when entering your PIN at ATMs or during online payments.

6. Report Fraud Immediately

If you suspect fraud, immediately report it to the bank through:
Customer care: 022 6868 1414
Fraud reporting email: reportfraud@finobank.com
Also, report to local law enforcement or the cybercrime cell for further action.



1. Avoid Sharing Personal Details

Never share your debit card number, CVV, OTP, or PIN with anyone, even if they claim to be from Fino Payments Bank. Do not share your banking passwords, OTPs, or account details over phone, SMS, or email. Do not handover your debit card to anyone for withdrawals, transactions or for any purpose.

2. Do Not Fall for Fraudulent Communication

Be cautious of calls, SMS, or emails asking for sensitive information. Never respond to unsolicited communications that ask for your personal banking information. Remember, Fino Payments Bank will never ask for your bank balance, card details, PIN, or password.

3. Avoid Using Unsecure Networks

Refrain from doing online banking on public Wi-Fi or shared networks like those in cafes or libraries. Avoid using cyber cafes or public computers for internet banking transactions.

4. Don't Store Confidential Information

Do not save your banking passwords or PINs in easily accessible places or on your phone. Avoid writing down sensitive data, such as passwords or card numbers, and instead memorize them.

5. Do Not Use Untrusted Websites or Apps

Ensure that you only download the Fino Payments Bank app from authorized app stores like Google Play or Apple's App Store. Avoid conducting transactions on websites that don't have "https://" in their URL or lack trusted security certificates.

6. Don't Share Your Mobile or Internet Banking Access

Avoid sharing access to your mobile banking app or internet banking portal with anyone.

Additional Awareness Tips

Identity Theft: Be cautious of sharing personal details like your Aadhaar number, PAN card, or other ID proofs unless absolutely necessary and only with trusted sources.

Fraudulent Loan Offers: If you receive an unexpected offer for a loan or financial product, verify the authenticity directly with Fino Payments Bank through official channels before proceeding.

Vishing (Voice Phishing): Be wary of callers impersonating bank employees or customer service agents who ask for your financial details or passwords. If you're unsure, hang up and contact the bank via official channels.

Fake Customer Care Numbers: Always verify the bank's contact numbers directly from the official website or app. Fraudsters often post fake customer care numbers on the internet to lure victims into sharing their banking details.

UPI Transactions: When making UPI payments, verify the recipient's details carefully. Fraudsters may try to trick you into transferring money to the wrong account.

Suspicious Links and Emails: Avoid clicking on suspicious links sent via email or SMS. Fraudsters may use these to steal your information or install malware on your device.

ग्राहक जागरूकता

सुरक्षित बैंकिंग के लिए क्या करें और क्या न करें

क्या करें

1. अपनी बैंकिंग जानकारी सुरक्षित रखें

अपने डेबिट कार्ड को हमेशा सुरक्षित रखें और उसे सुरक्षित स्थान पर रखें।
अपने एटीएम / डेबिट कार्ड पिन को याद रखें और इसे किसी भी चीज़ पर ना लिखें।
अपने पासवर्ड और पिन को नियमित रूप से बदलें, खासकर इंटरनेट और मोबाइल बैंकिंग के लिए।

2. अपने खातों की निगरानी करें

किसी भी अनधिकृत गतिविधि के लिए नियमित रूप से अपने लेन-देन इतिहास की जाँच करें।
किसी भी संदिग्ध लेन-देन की तुरंत बैंक को रिपोर्ट करें
ग्राहक सेवा: 022 6868 1414 | ईमेल: customercare@finobank.com
धोखाधड़ी की रिपोर्टिंग ईमेल: reportfraud@finobank.com
अपने खाते की निगरानी करने और आवश्यकतानुसार अपने कार्ड को ब्लॉक/अनब्लॉक करने के लिए फिनो पेमेंट्स बैंक के मोबाइल ऐप का उपयोग करें।

3. मजबूत सुरक्षा उपायों का उपयोग करें

अपने मोबाइल बैंकिंग ऐप, ऑपरेटिंग सिस्टम और एंटीवायरस सॉफ्टवेयर को अपडेट रखें।
सुरक्षा की एक अतिरिक्त परत के लिए जहाँ भी संभव हो मल्टी-फैक्टर ऑथेंटिकेशन (MFA) सक्षम करें।

4. फ़िशिंग स्कैम से सावधान रहें

केवल विश्वसनीय स्रोतों से लिंक पर क्लिक करें। आधिकारिक फ़िनो पेमेंट्स बैंक वेबसाइट देखें या उनके ज्ञात चैनलों के माध्यम से संपर्क करें। संवेदनशील जानकारी मांगने वाले अनचाहे ईमेल, कॉल या संदेशों से सावधान रहें।
फ़िशिंग रेड फ्लैग देखें: व्याकरण की गलतियाँ, अजीब URL और व्यक्तिगत विवरण के लिए तत्काल अनुरोध।

5. सुरक्षित लेन-देन करें

ATM या POS टर्मिनल का उपयोग करते समय, स्कimming डिवाइस या किसी भी संदिग्ध गतिविधि की जाँच करें। ATM पर या ऑनलाइन भुगतान के दौरान अपना पिन दर्ज करते समय हमेशा कीपैड को ढकें।

6. धोखाधड़ी की तुरंत रिपोर्ट करें

यदि आपको धोखाधड़ी का संदेह है, तो तुरंत बैंक को इसकी रिपोर्ट करें:

ग्राहक सेवा: 022 6868 1414

धोखाधड़ी की रिपोर्टिंग ईमेल: reportfraud@finobank.com

इसके अलावा, आगे की कार्रवाई के लिए स्थानीय कानून प्रवर्तन या साइबर अपराध सेल को रिपोर्ट करें।

क्या न करें

1. व्यक्तिगत विवरण साझा करने से बचें

कभी भी अपना डेबिट कार्ड नंबर, CVV, OTP या पिन किसी के साथ साझा न करें, भले ही वे फिनो पेमेंट्स बैंक से होने का दावा करें। फ़ोन, SMS या ईमेल पर अपने बैंकिंग पासवर्ड, OTP या खाते का विवरण साझा न करें। निकासी, लेनदेन या किसी भी उद्देश्य के लिए अपना डेबिट कार्ड किसी को न दें।

2. धोखाधड़ी वाले संचार के झांसे में न आएं

संवेदनशील जानकारी मांगने वाले कॉल, SMS या ईमेल से सावधान रहें। कभी भी ऐसे अनचाहे संचार का जवाब न दें जो आपकी व्यक्तिगत बैंकिंग जानकारी मांगते हैं। याद रखें, फिनो पेमेंट्स बैंक कभी भी आपका बैंक बैलेंस, कार्ड विवरण, पिन या पासवर्ड नहीं पूछेगा।

3. असुरक्षित नेटवर्क का उपयोग करने से बचें

सार्वजनिक वाई-फाई या कैफ़े या लाइब्रेरी जैसे साझा नेटवर्क पर ऑनलाइन बैंकिंग करने से बचें। इंटरनेट बैंकिंग लेनदेन के लिए साइबर कैफ़े या सार्वजनिक कंप्यूटर का उपयोग करने से बचें।

4. गोपनीय जानकारी संग्रहीत न करें

अपने बैंकिंग पासवर्ड या पिन को आसानी से सुलभ स्थानों या अपने फ़ोन पर सेव न करें। पासवर्ड या कार्ड नंबर जैसे संवेदनशील डेटा को लिखने से बचें और इसके बजाय उन्हें याद रखें।

5. अविश्वसनीय वेबसाइट या ऐप का उपयोग न करें

सुनिश्चित करें कि आप फिनो पेमेंट्स बैंक ऐप को केवल Google Play या Apple के ऐप स्टोर जैसे अधिकृत ऐप स्टोर से ही डाउनलोड करें। ऐसी वेबसाइट पर लेनदेन करने से बचें जिनके URL में "https://" न हो या जिनमें विश्वसनीय सुरक्षा प्रमाणपत्र न हों।

6. अपना मोबाइल या इंटरनेट बैंकिंग एक्सेस साझा न करें

अपने मोबाइल बैंकिंग ऐप या इंटरनेट बैंकिंग पोर्टल का एक्सेस किसी के साथ साझा करने से बचें।

अतिरिक्त जागरूकता सुझाव:

पहचान की चोरी: अपने आधार नंबर, पैन कार्ड या अन्य पहचान प्रमाण जैसे व्यक्तिगत विवरण को साझा करने से सावधान रहें जब तक कि बिल्कुल आवश्यक न हो और केवल विश्वसनीय स्रोतों के साथ।

धोखाधड़ी वाले ऋण प्रस्ताव: यदि आपको ऋण या वित्तीय उत्पाद के लिए कोई अप्रत्याशित प्रस्ताव प्राप्त होता है, तो आगे बढ़ने से पहले आधिकारिक चैनलों के माध्यम से सीधे फिनो पेमेंट्स बैंक से प्रामाणिकता सत्यापित करें।

विशिंग (वॉयस फ़िशिंग): बैंक कर्मचारियों या ग्राहक सेवा एजेंटों का रूप धारण करने वाले कॉल करने वालों से सावधान रहें जो आपके वित्तीय विवरण या पासवर्ड मांगते हैं। यदि आप अनिश्चित हैं, तो फ़ोन काट दें और आधिकारिक चैनलों के माध्यम से बैंक से संपर्क करें।

नकली ग्राहक सेवा नंबर: हमेशा आधिकारिक वेबसाइट या ऐप से सीधे बैंक के संपर्क नंबरों को सत्यापित करें। जालसाज अक्सर पीड़ितों को अपने बैंकिंग विवरण साझा करने के लिए लुभाने के लिए इंटरनेट पर नकली ग्राहक सेवा नंबर पोस्ट करते हैं।

UPI लेनदेन: UPI भुगतान करते समय, प्राप्तकर्ता के विवरण को सावधानीपूर्वक सत्यापित करें। जालसाज आपको गलत खाते में पैसे ट्रांसफर करने के लिए धोखा देने की कोशिश कर सकते हैं।

संदिग्ध लिंक और ईमेल: ईमेल या एसएमएस के माध्यम से भेजे गए संदिग्ध लिंक पर क्लिक करने से बचें। धोखेबाज़ इनका इस्तेमाल आपकी जानकारी चुराने या आपके डिवाइस पर मेलवेयर इंस्टॉल करने के लिए कर सकते हैं।

ये क्या करें और क्या न करें आपको संभावित धोखाधड़ी से बचाने और फ़िनो पेमेंट्स बैंक के साथ सुरक्षित बैंकिंग सुनिश्चित करने में मदद करेंगे।
अपनी व्यक्तिगत और वित्तीय जानकारी को सुरक्षित रखने के लिए सूचित और सतर्क रहें!

કસ્ટમર જાગૃતિ સેફ બેંકિંગ માટે શું કરવું અને શું નહીં

કરવું:

1. તમારી બેંકિંગ માહિતીને સુરક્ષિત કરો

તમારા ડેબિટ કાર્ડને હંમેશા સુરક્ષિત રાખો અને તેને સુરક્ષિત જગ્યાએ રાખો. તમારા એટીએમ, ડેબિટ કાર્ડનો પિન યાદ રાખો અને તેને કોઈપણ વસ્તુ પર લખવાનું ટાળો. તમારા પાસવર્ડ અને પિન નિયમિતપણે બદલો, ખાસ કરીને ઇન્ટરનેટ અને મોબાઇલ બેંકિંગ માટે.

2. તમારા એકાઉન્ટ્સ પર નજર રાખો

કોઈપણ અનઓથોરાઇઝ્ડ એક્ટિવિટી માટે તમારી ટ્રાન્સેક્શન હિસ્ટરીને નિયમિતપણે તપાસો. કોઈપણ શંકાસ્પદ ટ્રાન્સેક્શનની જાણ તરત જ બેંકને કરો:

કસ્ટમર કેર: 022 6868 1414

ઇમેઇલ: customercare@finobank.com

ફ્રોડ રિપોર્ટિંગ ઇમેઇલ: reportfraud@finobank.com

તમારા એકાઉન્ટને મોનિટર કરવા માટે ફિનો પેમેન્ટ્સ બેંકની મોબાઇલ એપ્લિકેશનનો ઉપયોગ કરો અને જરૂરિયાત મુજબ તમારા કાર્ડને બ્લોક/અનબ્લોક કરો.

3. મજબૂત સુરક્ષા પગલાંનો ઉપયોગ કરો

તમારી મોબાઇલ બેંકિંગ એપ્સ, ઓપરેટિંગ સિસ્ટમ અને એન્ટિવાયરસ સોફ્ટવેર અપડેટ રાખો.

સુરક્ષાના વધારાના સ્તર માટે શક્ય હોય ત્યાં મલ્ટી-ફેક્ટર ઓથેન્ટિકેશન (MFA) અનેબલ કરો.

4. ફિશિંગ સ્કેમ્સથી સાવચેત રહો

માત્ર ટ્રસ્ટેડ સોર્સિસમાંથી લિંક્સ પર ક્લિક કરો. ફિનો પેમેન્ટ્સ બેંકની સત્તાવાર વેબસાઇટ તપાસો અથવા તેમની જાણીતી ચેનલો દ્વારા સંપર્ક કરો. સેન્સિટિવ માહિતી માટે પૂછતા અવાંછિત ઇમેઇલ્સ, કોલ્સ અથવા સંદેશાઓથી સાવચેત રહો. ફિશિંગ લાલ્ચ ફ્લેગ્સ માટે જુઓ: વ્યાકરણની ભૂલો, વિચિત્ર URL અને વ્યક્તિગત વિગતો માટે તાત્કાલિક વિનંતીઓ.

5. સુરક્ષિત ટ્રાન્સેક્સન કરો

ATM અથવા POS ટર્મિનલનો ઉપયોગ કરતી વખતે, સ્ક્રિમિંગ ડિવાઇસિસ અથવા કોઈપણ શંકાસ્પદ એક્ટિવિટી માટે તપાસો. એટીએમ પર અથવા ઓનલાઇન પેમેન્ટ દરમિયાન તમારો પિન દાખલ કરતી વખતે હંમેશા કીપેડને સુરક્ષિત રાખો.

6. ફ્રોડની તાત્કાલિક જાણ કરો

જો તમને ફ્રોડની આશંકા હોય, તો તરત જ બેંકને આની જાણ કરો:

કસ્ટમર સંભાળ: 022 6868 1414

ફ્રોડ રિપોર્ટિંગ ઇમેઇલ: reportfraud@finobank.com

ઉપરાંત, આગળની કાર્યવાહી માટે સ્થાનિક કાયદા અમલીકરણ અથવા સાયબર ક્રાઇમ સેલને જાણ કરો.

ન કરવું:

1. અંગત વિગતો શેર કરવાનું ટાળો

તમારો ડેબિટ કાર્ડ નંબર, CVV, OTP અથવા PIN ક્યારેય કોઈની સાથે શેર કરશો નહીં, પછી ભલે તેઓ ફિનો પેમેન્ટ્સ બેંકના હોવાનો દાવો કરે. તમારા બેંકિંગ પાસવર્ડ, OTP અથવા ખાતાની વિગતો ફોન, SMS અથવા ઇમેઇલ પર શેર કરશો નહીં. વિથડ્રોઅલ, ટ્રાન્સેક્શન અથવા કોઈપણ હેતુ માટે તમારું ડેબિટ કાર્ડ કોઈને પણ ન આપો.

2. છેતરપિંડી કોમ્યુનિકેશન માટે પડશો નહીં

કોલ્સ, SMS અથવા સેન્સિટિવ માહિતી માટે પૂછતા ઇમેઇલથી સાવધ રહો. તમારી અંગત બેંકિંગ માહિતી માટે પૂછતા અનિચ્છનીય કોમ્યુનિકેશનનો ક્યારેય જવાબ આપશો નહીં. યાદ રાખો, ફિનો પેમેન્ટ્સ બેંક તમારા બેંક બેલેન્સ, કાર્ડની વિગતો, PIN અથવા પાસવર્ડ ક્યારેય પૂછશે નહીં.

3. અસુરક્ષિત નેટવર્કનો ઉપયોગ કરવાનું ટાળો

સાર્વજનિક Wi-Fi અથવા કાફે અથવા લાઇબ્રેરી જેવા શેર કરેલા નેટવર્ક પર ઓનલાઇન બેંકિંગ કરવાનું ટાળો. ઇન્ટરનેટ બેંકિંગ ટ્રાન્સેક્સન માટે સાયબર કાફે અથવા સાર્વજનિક કમ્યુટર્સનો ઉપયોગ કરવાનું ટાળો.

4. ગોપનીય માહિતી સ્ટોર કરશો નહીં

તમારા બેંકિંગ પાસવર્ડ અથવા પિન સરળતાથી સુલભ સ્થળોએ અથવા તમારા ફોનમાં સાચવશો નહીં. સેન્સિટિવ ડેટા, જેમ કે પાસવર્ડ અથવા કાર્ડ નંબર લખવાનું ટાળો અને તેના બદલે તેને યાદ રાખો.

5. અનટ્રસ્ટેડ વેબસાઇટ્સ અથવા એપ્સનો ઉપયોગ કરશો નહીં

ખાતરી કરો કે તમે Google Play અથવા Appleના એપ સ્ટોર જેવા ઓફીસીઅલ એપ સ્ટોર્સ પરથી જ ફિનો પેમેન્ટ્સ બેંક એપ્લિકેશન ડાઉનલોડ કરો છો. એવી વેબસાઇટ્સ પર ટ્રાન્સેક્શન કરવાનું ટાળો કે જેનાં URL માં "https://" નથી અથવા ટ્રસ્ટેડ સેક્યુરીટી સર્ટિફિકેટ્સ નથી.

6. તમારો મોબાઇલ અથવા ઇન્ટરનેટ બેંકિંગ એક્સેસ શેર કરશો નહીં

તમારો મોબાઇલ બેંકિંગ એપ્લિકેશન અથવા ઇન્ટરનેટ બેંકિંગ પોર્ટલની એક્સેસ કોઈપણ સાથે શેર કરવાનું ટાળો.

વધારાની જાગૃતિ ટિપ્સ:

ઓળખની ચોરી: તમારા આધાર નંબર, પાન કાર્ડ અથવા અન્ય ID પ્રૂફ જેવી વ્યક્તિગત વિગતો શેર કરવામાં સાવધ રહો સિવાય કે એકદમ જરૂરી હોય અને માત્ર ટ્રસ્ટેડ સોર્સિસ સાથે. ફ્રોડયુક્ત લોન ઓફર્સ: જો તમને લોન અથવા નાણાકીય પ્રોડક્ટ માટે અણધારી ઓફર મળે છે, તો આગળ વધતા પહેલા ઓફીસીઅલ ચેનલો દ્વારા સીધા જ ફિનો પેમેન્ટ્સ બેંક સાથે ઓફીસીઅલ ચકાસો. વિશીંગ (વોઈસ ફિશીંગ): બેંક કર્મચારીઓ અથવા કસ્ટમર સેવા એજન્ટોનો ઢોંગ કરતા કોલ્સથી સાવચેત રહો જેઓ તમારી નાણાકીય વિગતો અથવા પાસવર્ડ માંગે છે. જો તમને ખાતરી ન હોય, તો અટકી જાઓ અને ઓફીસીઅલ ચેનલો દ્વારા બેંકનો સંપર્ક કરો. નકલી કસ્ટમર કેર નંબર્સ: હંમેશા ઓફીસીઅલ વેબસાઇટ અથવા એપ પરથી સીધા બેંકના સંપર્ક નંબરોની ચકાસણી કરો. ફ્રોડ કરનારાઓ ઘણીવાર પીડિતોને તેમની બેંકિંગ વિગતો શેર કરવા માટે લલચાવવા માટે ઇન્ટરનેટ પર નકલી કસ્ટમર સંભાળ નંબરો પોસ્ટ કરે છે. UPI ટ્રાન્સેક્સન: UPI ચૂકવણી કરતી વખતે, પ્રાપ્તકર્તાની વિગતો કાળજીપૂર્વક ચકાસો. ફ્રોડ કરનારાઓ તમને ખોટા ખાતામાં પૈસા ટ્રાન્સફર કરવા માટે છેતરવાનો પ્રયાસ કરી શકે છે. શંકાસ્પદ લિંક્સ અને ઇમેઇલ્સ: ઇમેઇલ અથવા SMS દ્વારા મોકલવામાં આવેલી શંકાસ્પદ લિંક્સ પર ક્લિક કરવાનું ટાળો. ફ્રોડ કરનારાઓ આનો ઉપયોગ તમારી માહિતી ચોરી કરવા અથવા તમારા ઉપકરણ પર માલવેર ઇન્સ્ટોલ કરવા માટે કરી શકે છે.

ಗ್ರಾಹಕರ ಜಾಗೃತಿ

ಸುರಕ್ಷಿತ ಬ್ಯಾಂಕಿಂಗ್‌ಗೆ ಮಾಡಬೇಕಾದ ಮತ್ತು ಮಾಡಬಾರದ ನಿಯಮಗಳು

ಮಾಡಬೇಕಾದವು

1. ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ

ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಅನ್ನು ಯಾವಾಗಲೂ ಸುರಕ್ಷಿತವಾಗಿರಿಸಿ ಮತ್ತು ಸುರಕ್ಷಿತ ಸ್ಥಳದಲ್ಲಿ ಇರಿಸಿ. ನಿಮ್ಮ ಎಟಿಎಮ್, ಡೆಬಿಟ್ ಕಾರ್ಡ್ ನಂಬರ್‌ಗಳನ್ನು ನೆನಪಿನಲ್ಲಿ ಇಟ್ಟುಕೊಳ್ಳಿ ಮತ್ತು ಅದನ್ನು ಬರೆದಿಟ್ಟುಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ ರೆಗ್ಯೂಲರ್ ಆಗಿ ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಮತ್ತು ಪಿನ್‌ಗಳನ್ನು ಬದಲಾಯಿಸಿ, ವಿಶೇಷವಾಗಿ ಇಂಟರ್ನೆಟ್ ಮತ್ತು ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಮತ್ತು ಪಿನ್‌ಗಳನ್ನು ರೆಗ್ಯೂಲರ್ ಆಗಿ ಬದಲಾಯಿಸಿ.

2. ನಿಮ್ಮ ಖಾತೆಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ

ಯಾವುದೇ ಅನಧಿಕೃತ ಚಟುವಟಿಕೆಗಳ ಬಗ್ಗೆ ತಿಳಿಯಲು ನಿಮ್ಮ ಟ್ರಾನ್ಸಾಕ್ಷನ್ ಹಿಸ್ಟರಿಯನ್ನು ರೆಗ್ಯೂಲರ್ ಆಗಿ ಪರಿಶೀಲಿಸಿ. ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ವಹಿವಾಟುಗಳನ್ನು ಈ ಕೆಳಗಿನ ಮಾರ್ಗಗಳ ಮೂಲಕ ಬ್ಯಾಂಕ್‌ಗೆ ತಕ್ಷಣವೇ ವರದಿ ಮಾಡಿ:

ಕಸ್ಟಮರ್ ಕೇರ್: 022 6868 1414

ಇಮೇಲ್: customercare@finobank.com

ವಂಚನೆ ವರದಿ ಮಾಡುವ ಇಮೇಲ್: reportfraud@finobank.com

ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಲು ಮತ್ತು ಅಗತ್ಯಕ್ಕೆ ತಕ್ಕಂತೆ ನಿಮ್ಮ ಕಾರ್ಡ್‌ಗಳನ್ನು ಬ್ಲಾಕ್/ಅನ್‌ಬ್ಲಾಕ್ ಮಾಡಲು ಫಿನೋ ಪೇಮೆಂಟ್ಸ್ ಬ್ಯಾಂಕ್ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಶನ್ ಬಳಸಿ.

3. ಬಲವಾದ ಭದ್ರತಾ ಕ್ರಮಗಳನ್ನು ಬಳಸಿ

ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳು ಮತ್ತು ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಅಪ್ಡೇಟ್ ಮಾಡುತ್ತಾ ಇರಿ. ಭದ್ರತೆಯ ಹೆಚ್ಚುವರಿ ಪದರಕ್ಕಾಗಿ ಸಾಧ್ಯವಾದಲ್ಲಿ ಲಾ ಮಲ್ಟಿ-ಫ್ಯಾಕ್ಟರ್ ಅಥಂಟಿಕೇಶನ್ (MFA) ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

4. ಫಿಶಿಂಗ್ ಹಗರಣಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲಗಳಿಂದ ಬಂದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಮಾತ್ರ ಕ್ಲಿಕ್ ಮಾಡಿ. ಅಧಿಕೃತ ಫಿನೋ ಪೇಮೆಂಟ್ಸ್ ಬ್ಯಾಂಕ್ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ಪರಿಶೀಲಿಸಿ ಅಥವಾ ಅವರ ತಿಳಿದಿರುವ ಚಾನಲ್‌ಗಳ ಮೂಲಕ ಸಂಪರ್ಕಿಸಿ. ಅಪೇಕ್ಷಿಸದ ಇಮೇಲ್‌ಗಳು, ಕರೆಗಳು ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕೇಳುವ ಸಂದೇಶಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ಫಿಶಿಂಗ್ ರೆಡ್ ಫ್ಲಾಗ್‌ಗಳನ್ನು ಗಮನಿಸಿ: ವ್ಯಾಕರಣದ ತಪ್ಪುಗಳು, ವಿಚಿತ್ರ ಯುಆರ್‌ಎಲ್ (URL) ಗಳು ಮತ್ತು ವೈಯಕ್ತಿಕ ವಿವರಗಳಿಗಾಗಿ ತುರ್ತು ವಿನಂತಿಗಳು.

5. ಸುರಕ್ಷಿತ ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸಿ:

ATMಗಳು ಅಥವಾ POS ಟರ್ಮಿನಲ್‌ಗಳನ್ನು ಬಳಸುವಾಗ, ಸ್ಕ್ರೀಮ್‌ಗಳ ಸಾಧನಗಳು ಅಥವಾ ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಎಟಿಎಮ್‌ಗಳಲ್ಲಿ ಅಥವಾ ಆನ್‌ಲೈನ್ ಪಾವತಿಗಳ ಸಂದರ್ಭದಲ್ಲಿ ನಿಮ್ಮ ಪಿನ್ ನಮೂದಿಸುವಾಗ ಯಾವಾಗಲೂ ಕೀಪಾಡ್ ಅನ್ನು ಮುಚ್ಚಿರಿ.

6. ವಂಚನೆಯನ್ನು ತಕ್ಷಣವೇ ವರದಿ ಮಾಡಿ:

ನಿಮಗೆ ವಂಚನೆಯ ಬಗ್ಗೆ ಅನುಮಾನ ಬಂದರೆ, ತಕ್ಷಣವೇ ಈ ಕೆಳಗಿನ ಮಾರ್ಗಗಳಿಂದ ವರದಿ ಮಾಡಿ:

ಕಸ್ಟಮರ್ ಕೇರ್: 022 6868 1414

ವಂಚನೆ ವರದಿ ಮಾಡುವ ಇಮೇಲ್: reportfraud@finobank.com

ಮತ್ತಷ್ಟು ಕ್ರಮಕ್ಕೆ ಸ್ಥಳೀಯ ಕಾನೂನು ಅನುಷ್ಠಾನ ಅಥವಾ ಸೈಬರ್ ಕ್ರೈಮ್ ಸೆಲ್ ಕೂಡ ವರದಿ ಮಾಡಿ.

ಮಾಡಬಾರದವು

1. ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ

ನಿಮ್ಮ ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಸಂಖ್ಯೆ, CVV, OTP, ಅಥವಾ PIN ಅನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ, ಅವರು ಫಿನೋ ಬ್ಯಾಂಕಿನಿಂದ ಎಂದು ಹೇಳಿಕೊಂಡರೂ ಸಹ. ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಒಟಿಪಿಗಳು ಅಥವಾ ಖಾತೆಯ ವಿವರಗಳನ್ನು ಫೋನ್, ಎಸ್‌ಎಮ್‌ಎಸ್ ಅಥವಾ ಇಮೇಲ್ ಮೂಲಕ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಹಣ ಹಿಂಪಡೆಯುವಿಕೆ, ವಹಿವಾಟು ಅಥವಾ ಯಾವುದೇ ಉದ್ದೇಶಕ್ಕಾಗಿ ನಿಮ್ಮ ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಅನ್ನು ಯಾರಿಗೂ ಹಸ್ತಾಂತರಿಸಬೇಡಿ.

2. ಮೋಸದ ಸಂವಹನಕ್ಕೆ ಬಲಿಯಾಗಬೇಡಿ

ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕೇಳುವ ಕರೆಗಳು, ಎಸ್‌ಎಮ್‌ಎಸ್ ಅಥವಾ ಇಮೇಲ್‌ಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನು ಕೇಳುವ ಅಪೇಕ್ಷಿಸದ ಸಂವಹನಗಳಿಗೆ ಎಂದಿಗೂ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ. ನೆನಪಿಡಿ, ಫಿನೋ ಪೇಮೆಂಟ್ಸ್ ಬ್ಯಾಂಕ್ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಬ್ಯಾಲೆನ್ಸ್, ಕಾರ್ಡ್ ವಿವರಗಳು, ಪಿನ್ ಅಥವಾ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ.

3. ಅಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ

ಪಬ್ಲಿಕ್ ವೈ-ಫೈ, ಅಥವಾ ಕಛೇರಿಗಳು ಅಥವಾ ಲೈಬ್ರರಿಗಳಂತಹ ಜಾಗಗಳಲ್ಲಿ ಹಂಚಿಕೊಂಡ. ನೆಟ್‌ವರ್ಕ್‌ಗಳಲ್ಲಿ ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಡುವುದಕ್ಕೆ ಹೋಗಬೇಡಿ. ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ವಹಿವಾಟುಗಳಿಗಾಗಿ ಸೈಬರ್ ಕಛೇರಿಗಳು ಅಥವಾ ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.

4. ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಸ್ಕ್ರೋಲ್ ಮಾಡಬೇಡಿ

ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಪಿನ್‌ಗಳನ್ನು ಸುಲಭವಾಗಿ ಲಭ್ಯವಾಗುವ ಸ್ಥಳಗಳಲ್ಲಿ ಅಥವಾ ಫೋನ್‌ನಲ್ಲಿ ಉಳಿಸಬೇಡಿ. ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಕಾರ್ಡ್ ಸಂಖ್ಯೆಗಳಂತಹ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಬರೆಯುವುದನ್ನು ತಪ್ಪಿಸಿ ಅದರ ಬದಲಿಗೆ ಅವುಗಳನ್ನು ನೆನಪಿಟ್ಟುಕೊಳ್ಳಿ.

5. ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಬೇಡಿ

ಗೂಗಲ್ ಪ್ಲೇ ಅಥವಾ ಆಪಲ್ ನ ಆಪ್ ಸ್ಟೋರ್‌ನಂತಹ ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳಿಂದ ಮಾತ್ರ ನೀವು ಫಿನೋ ಪೇಮೆಂಟ್ಸ್ ಬ್ಯಾಂಕ್ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿದ್ದೀರಿ ಎಂದು. ಚಿತ್ರಪಡಿಸಿಕೊಳ್ಳಿ. ತಮ್ಮ URL ನಲ್ಲಿ "https://" ಇಲ್ಲದ ಅಥವಾ ವಿಶ್ವಾಸಾರ್ಹ ಭದ್ರತಾ ಪ್ರಮಾಣಪತ್ರಗಳನ್ನು ಹೊಂದಿರದ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ವಹಿವಾಟು ನಡೆಸುವುದನ್ನು ತಪ್ಪಿಸಿ.

6. ನಿಮ್ಮ ಮೊಬೈಲ್ ಅಥವಾ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಪ್ರವೇಶವನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ

ಯಾರೊಂದಿಗೂ ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್ ಅಥವಾ ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಪ್ರೋಟೆಕ್ಟ್ ಪ್ರವೇಶವನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಹೆಚ್ಚುವರಿ ಜಾಗೃತಿ ಸಲಹೆಗಳು:

ಗುರುತಿನ ಕಳ್ಳತನ: ನಿಮ್ಮ ಆಧಾರ್ ಸಂಖ್ಯೆ, ಪಾನ್ ಕಾರ್ಡ್ ಅಥವಾ ಇತರ ಗುರುತಿನ ಪ್ರಮಾಣ ಪತ್ರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವಾಗ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ. ಸಂಪೂರ್ಣ ಅಗತ್ಯವಿದ್ದಾಗ ಮಾತ್ರ ಮತ್ತು ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲಗಳೊಂದಿಗೆ ಮಾತ್ರ ಹಂಚಿಕೊಳ್ಳಿ. ಮೋಸದ ಸಾಲದ ಆಫರ್‌ಗಳು: ನೀವು ನಿರೀಕ್ಷಿಸದ ಸಾಲ ಅಥವಾ ಆರ್ಥಿಕ ಉತ್ಪನ್ನದ ಆಫರ್ ಅನ್ನು ಸ್ವೀಕರಿಸಿದರೆ, ಅಧಿಕೃತ ಮಾರ್ಗಗಳ ಮೂಲಕ ನೇರವಾಗಿ ಫಿನೋ ಪೇಮೆಂಟ್ಸ್ ಬ್ಯಾಂಕ್‌ನೊಂದಿಗೆ ಖಚಿತಪಡಿಸಿಕೊಂಡು ನಂತರವೇ ಮುಂದುವರೆಯಿರಿ. ವಿಶಿಂಗ್ (ವಾಯ್ಸ್ ಫಿಶಿಂಗ್): ಬ್ಯಾಂಕ್ ಸಿಬ್ಬಂದಿ ಅಥವಾ ಗ್ರಾಹಕ ಸೇವಾ ಪ್ರತಿನಿಧಿಗಳಂತೆ ಕರೆ ಮಾಡಿ ಹಣಕಾಸು ವಿವರಗಳು ಅಥವಾ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಕೇಳುವ ನಕಲಿ ಕರೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ. ನಿಮಗೆ ಅನುಮಾನ ಬಂದರೆ ಕರೆಯನ್ನು ಸ್ವೀಕರಿಸಬೇಡಿ ಮತ್ತು ಅಧಿಕೃತ ಮಾರ್ಗಗಳ ಮೂಲಕ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ. ನಕಲಿ ಗ್ರಾಹಕ ಸೇವಾ ಸಂಖ್ಯೆ: ಬ್ಯಾಂಕ್ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಯನ್ನು ಯಾವಾಗಲೂ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ದೃಢೀಕರಿಸಿ, ಮೋಸಗಾರರು ಹಲವು ವೇಳೆ ನಕಲಿ ಗ್ರಾಹಕ ಸೇವಾ ಸಂಖ್ಯೆಯನ್ನು ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ ಪ್ರಕಟಿಸಿ ಗ್ರಾಹಕರ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ. UPI ವಹಿವಾಟುಗಳು: UPI ಪಾವತಿಗಳನ್ನು ಮಾಡುವಾಗ, ಸ್ವೀಕರಿಸುವವರ ವಿವರಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಪರಿಶೀಲಿಸಿ. ಮೋಸಗಾರರು ನಿಮ್ಮ ಹಣವನ್ನು ತಪ್ಪು ಖಾತೆಗೆ ವರ್ಗಾಯಿಸಲು ಯತ್ನಿಸಬಹುದು. ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳು ಮತ್ತು ಇಮೇಲ್‌ಗಳು: ಇಮೇಲ್ ಅಥವಾ SMS ಮೂಲಕ ಕಳುಹಿಸಲಾದ ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ. ಮೋಸಗಾರರು ಇವುಗಳನ್ನು ನಿಮ್ಮ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ಅಥವಾ ನಿಮ್ಮ ಸಾಧನದಲ್ಲಿ ಮಾಲ್‌ವೇರ್ ಅನ್ನು ಸ್ಥಾಪಿಸಲು ಬಳಸಬಹುದು.

ଗ୍ରାହକ ସଚେତନତା

ସୁରକ୍ଷିତ ବ୍ୟାଙ୍କିଂ ପାଇଁ କ'ଣ କରିବେ ଏବଂ କ'ଣ କରିବେ ନାହିଁ

କ'ଣ କରିବେ

କ'ଣ କରିବେ ନାହିଁ

1. ଆପଣଙ୍କର ବ୍ୟାଙ୍କିଂ ସମ୍ପର୍କିତ ସୂଚନାକୁ ସୁରକ୍ଷିତ ରଖନ୍ତୁ

ଆପଣଙ୍କର ଡେବିଟ୍ କାର୍ଡକୁ ସର୍ବଦା ସୁରକ୍ଷିତ ରଖନ୍ତୁ ଏବଂ ଏହାକୁ ଏକ ସୁରକ୍ଷିତ ସ୍ଥାନରେ ରଖନ୍ତୁ। ଆପଣଙ୍କର ATM, ଡେବିଟ୍ କାର୍ଡର PIN ଟିକୁ ମନେରଖନ୍ତୁ ଏବଂ ଏହାକୁ କୌଣସି ଜିନିଷ ଉପରେ ଲେଖନ୍ତୁ ନାହିଁ। ବିଶେଷକରି ଇଣ୍ଟରନେଟ୍ ଏବଂ ମୋବାଇଲ୍ ବ୍ୟାଙ୍କିଂ କ୍ଷେତ୍ରରେ ନିୟମିତ ଭାବରେ ଆପଣଙ୍କର ପାସୱାର୍ଡ ଏବଂ PIN ପରିବର୍ତ୍ତନ କରନ୍ତୁ।

2. ଆପଣଙ୍କ ଆକାଉଣ୍ଟଗୁଡ଼ିକ ଉପରେ ନଜର ରଖନ୍ତୁ:

ଯେକୌଣସି ଅନଧିକୃତ କାର୍ଯ୍ୟକଳାପ ପାଇଁ ନିୟମିତ ଭାବରେ ଆପଣଙ୍କ ନେଣ ଦେଣର ଇତିହାସକୁ ଯାଞ୍ଚ କରନ୍ତୁ।

ଯେକୌଣସି ସନ୍ଦେହଜନକ କାରବାର ହେଲେ ତୁରନ୍ତ ବ୍ୟାଙ୍କକୁ ଏହି ମାଧ୍ୟମରେ ରିପୋର୍ଟ କରନ୍ତୁ:

ଗ୍ରାହକ ସେବା: 022 6868 1414

ଇମେଲ୍: customercare@finobank.com

ଠକେଇ ପାଇଁ ରିପୋର୍ଟ ଇମେଲ୍: reportfraud@finobank.com

ଆପଣଙ୍କ ଆକାଉଣ୍ଟ ଉପରେ ନଜର ରଖିବା ପାଇଁ ଏବଂ ଆବଶ୍ୟକ ଅନୁସାରେ ଆପଣଙ୍କ କାର୍ଡଗୁଡ଼ିକୁ ବ୍ଲକ୍/ଅନବ୍ଲକ୍ କରିବା ପାଇଁ Fino Payments Bank ର ମୋବାଇଲ୍ ଆପ୍ ବ୍ୟବହାର କରନ୍ତୁ।

3. ଦୃଢ଼ ସୁରକ୍ଷା ବ୍ୟବସ୍ଥା ବ୍ୟବହାର କରନ୍ତୁ

ଆପଣଙ୍କର ମୋବାଇଲ୍ ବ୍ୟାଙ୍କିଂ ଆପ୍, ଅପରେଟିଂ ସିଷ୍ଟମ୍ ଏବଂ ଆଣ୍ଟିଭାଇରସ୍ ସଫ୍ଟୱେର୍ ଗୁଡ଼ିକୁ ଅପଡେଟ୍ ରଖନ୍ତୁ। ସୁରକ୍ଷାର ଏକ ଅତିରିକ୍ତ ସ୍ତର ପାଇଁ ଯେଉଁଠାରେ ସମ୍ଭବ ମଲ୍ଟି-ଫ୍ୟାକ୍ଟର ଅଥେଣ୍ଡେନ୍ସିଆସନ୍ (MFA) ସକ୍ଷମ କରନ୍ତୁ।

4. ଫିସିଂ ଠକେଇ ପ୍ରତି ସାବଧାନ ରୁହନ୍ତୁ

କେବଳ ବିଶ୍ୱସ୍ତ ଉତ୍ସରୁ ଆସିଥିବା ଲିଙ୍କଗୁଡ଼ିକ ଉପରେ କ୍ଲିକ୍ କରନ୍ତୁ। ଅଫିସିଆଲ ଫିନୋ ପେମେଣ୍ଟସ୍ ବ୍ୟାଙ୍କ ୱେବସାଇଟ୍ ଯାଞ୍ଚ କରନ୍ତୁ କିମ୍ବା ସେମାନଙ୍କର ଜଣାଶୁଣା ଚ୍ୟାନେଲ ମାଧ୍ୟମରେ ଯୋଗାଯୋଗ କରନ୍ତୁ। ଅବାଞ୍ଛିତ ଇମେଲ୍, କଲ୍ କିମ୍ବା ସମ୍ବେଦନଶୀଳ ସୂଚନା ମାଗୁଥିବା ମେସେଜଗୁଡ଼ିକ ପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ। ଫିସିଂ ସତର୍କୀକରଣ: ବ୍ୟାଙ୍କର ଟୁଟି, ଅଜବ URL ଏବଂ ବ୍ୟକ୍ତିଗତ ବିବରଣୀ ପାଇଁ ଜରୁରୀ ଅନୁରୋଧ କ୍ଷେତ୍ରରେ ସତର୍କ ରୁହନ୍ତୁ।

5. ସୁରକ୍ଷିତ କାରବାର କରନ୍ତୁ

ATM କିମ୍ବା POS ଟର୍ମିନାଲ ବ୍ୟବହାର କରିବା ସମୟରେ, ଷ୍ଟିମିଂ ଡିଭାଇସ୍ କିମ୍ବା କୌଣସି ସନ୍ଦେହଜନକ ଗତିବିଧିକୁ ଯାଞ୍ଚ କରନ୍ତୁ। ATM ରେ କିମ୍ବା ଅନଲାଇନ୍ ପେମେଣ୍ଟ ସମୟରେ ଆପଣଙ୍କର PIN ଭରଣ କରିବା ସମୟରେ ସର୍ବଦା କାପ୍ୟାଚ୍ କୁ ଘୋଡ଼ାଇ ରଖନ୍ତୁ।

6. ଠକେଇର ତୁରନ୍ତ ରିପୋର୍ଟ କରନ୍ତୁ

ଯଦି ଆପଣଙ୍କୁ ଠକେଇର ସନ୍ଦେହ ହୁଏ, ତେବେ ତୁରନ୍ତ ବ୍ୟାଙ୍କକୁ ଏହି ମାଧ୍ୟମରେ ରିପୋର୍ଟ କରନ୍ତୁ:

ଗ୍ରାହକ ସେବା: 022 6868 1414

ଠକେଇ ପାଇଁ ରିପୋର୍ଟ ଇମେଲ୍: reportfraud@finobank.com

ଏହା ସହିତ, ପରବର୍ତ୍ତୀ କାର୍ଯ୍ୟାଳୟଗୁଡ଼ିକ ପାଇଁ ସ୍ଥାନୀୟ ଆଇନ ପ୍ରବର୍ତ୍ତନ କିମ୍ବା ସାଇବର ଅପରାଧ ସେଲ୍ କୁ ରିପୋର୍ଟ କରନ୍ତୁ।

1. ବ୍ୟକ୍ତିଗତ ବିବରଣୀ ସେୟାର କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ

ଯଦିଓ କେହି ନିଜକୁ Fino Payments Bank ର ବୋଲି ଦାବି କରନ୍ତି ତଥାପି ସେମାନଙ୍କ ସହ ଆପଣଙ୍କର ଡେବିଟ୍ କାର୍ଡ ନମ୍ବର, CVV, OTP କିମ୍ବା PIN ଆଦି ସେୟାର କରନ୍ତୁ ନାହିଁ।

ଆପଣଙ୍କର ବ୍ୟାଙ୍କିଂ ପାସୱାର୍ଡ, OTP କିମ୍ବା ଆକାଉଣ୍ଟ ବିବରଣୀ ଫୋନ୍, SMS, କିମ୍ବା ଇମେଲ୍ ମାଧ୍ୟମରେ ସେୟାର କରନ୍ତୁ ନାହିଁ।

ଆପଣଙ୍କର ଡେବିଟ୍ କାର୍ଡକୁ ଟଙ୍କା ଭିତ୍ତି, ଆର୍ଥିକ କାରବାର କିମ୍ବା କୌଣସି ଉଦ୍ଦେଶ୍ୟ ପାଇଁ କାହାକୁ ହସ୍ତାନ୍ତର କରନ୍ତୁ ନାହିଁ।

2. ଠକେଇର ଶିକାର ହେଉଥିବା ଭଳି ଯୋଗାଯୋଗ ଠାରୁ ଦୂରେଇ ରୁହନ୍ତୁ

ସମ୍ବେଦନଶୀଳ ସୂଚନା ମାଗୁଥିବା କଲ୍, SMS କିମ୍ବା ଇମେଲ୍ ପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ।

ଆପଣଙ୍କର ବ୍ୟକ୍ତିଗତ ବ୍ୟାଙ୍କିଂ ସୂଚନା ମାଗୁଥିବା ଅନାବଶ୍ୟକ ଯୋଗାଯୋଗର କେବେବି ଉତ୍ତର ଦିଅନ୍ତୁ ନାହିଁ।

ମନେରଖନ୍ତୁ, ଫିନୋ ପେମେଣ୍ଟସ୍ ବ୍ୟାଙ୍କ କେବେବି ଆପଣଙ୍କର ବ୍ୟାଙ୍କ ବାଲାନ୍ସ, କାର୍ଡ ବିବରଣୀ, PIN କିମ୍ବା ପାସୱାର୍ଡ ମାଗେ ନାହିଁ।

3. ଅସୁରକ୍ଷିତ ନେଟୱାର୍କ ବ୍ୟବହାର କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ

ପବ୍ଲିକ୍ ୱାଇ-ଫାଇ, କାଫି କିମ୍ବା ଲାଇବ୍ରେରୀରେ ଉପଲବ୍ଧ ହେଉଥିବା ମାଗଣା ନେଟୱାର୍କରେ ଅନଲାଇନ୍ ବ୍ୟାଙ୍କିଂ କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ।

ଇଣ୍ଟରନେଟ୍ ବ୍ୟାଙ୍କିଂ କାରବାର ପାଇଁ ସାଇବର କାଫି କିମ୍ବା ପବ୍ଲିକ୍ କମ୍ୟୁଟର ବ୍ୟବହାର କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ।

4. ଗୋପନୀୟ ସୂଚନା ସଂରକ୍ଷଣ କରନ୍ତୁ ନାହିଁ

ଆପଣଙ୍କର ବ୍ୟାଙ୍କ ପାସୱାର୍ଡ କିମ୍ବା ପିନ୍ ନମ୍ବରକୁ ଖୋଲା ସ୍ଥାନରେ କିମ୍ବା ଆପଣଙ୍କ ଫୋନ୍‌ରେ ସଂରକ୍ଷଣ କରନ୍ତୁ ନାହିଁ।

ପାସୱାର୍ଡ କିମ୍ବା କାର୍ଡ ନମ୍ବର ଭଳି ସମ୍ବେଦନଶୀଳ ତଥ୍ୟ ଲେଖିବା ପରିବର୍ତ୍ତେ ସେଗୁଡ଼ିକୁ ମନେ ରଖନ୍ତୁ।

5. ଅବିଶ୍ୱସନୀୟ ୱେବସାଇଟ୍ କିମ୍ବା ଆପ୍ ବ୍ୟବହାର କରନ୍ତୁ ନାହିଁ

ନିଶ୍ଚିତ କରନ୍ତୁ ଯେ ଆପଣ କେବଳ Google Play କିମ୍ବା Apple ର App Store ପରି ଅଧିକୃତ ଆପ୍ ଷ୍ଟୋରରୁ Fino Payments Bank ଆପ୍ ଡାଉନଲୋଡ୍ କରୁଛନ୍ତି। ଯେଉଁ ୱେବସାଇଟ୍‌ଗୁଡ଼ିକର URL ରେ "https://" ନାହିଁ କିମ୍ବା ଯେଉଁ ୱେବସାଇଟ୍ ଗୁଡ଼ିକରେ ବିଶ୍ୱସନୀୟ ସୁରକ୍ଷା ପ୍ରମାଣପତ୍ର ନାହିଁ, ସେଠାରେ ଆର୍ଥିକ କାରବାର କରିବାରୁ ନିବୃତ୍ତ ରୁହନ୍ତୁ।

6. ଆପଣଙ୍କ ମୋବାଇଲ୍ କିମ୍ବା ଇଣ୍ଟରନେଟ୍ ବ୍ୟାଙ୍କିଂର ଲଗ୍ ଇନ ଆଇଡି ଏବଂ ପାସୱାର୍ଡ ସେୟାର କରନ୍ତୁ ନାହିଁ

ଆପଣଙ୍କର ମୋବାଇଲ୍ ବ୍ୟାଙ୍କିଂ ଆପ୍ କିମ୍ବା ଇଣ୍ଟରନେଟ୍ ବ୍ୟାଙ୍କିଂ ପୋର୍ଟାଲର ଲଗ୍ ଇନ ଆଇଡି ଏବଂ ପାସୱାର୍ଡ କାହା ସହିତ ସେୟାର କରନ୍ତୁ ନାହିଁ।

ଅତିରିକ୍ତ ସଚେତନତା ଟିପ୍ସ:

ପରିଚୟ ଚୋରି: ସମ୍ପୂର୍ଣ୍ଣ ଆବଶ୍ୟକ ନହେଲେ ଏବଂ କେବଳ ବିଶ୍ୱସ୍ତ ଉତ୍ସ ସହିତ ଆପଣଙ୍କର ଆଧାର ନମ୍ବର, ପାନ କାର୍ଡ, କିମ୍ବା ଅନ୍ୟାନ୍ୟ ପରିଚୟ ପ୍ରମାଣ ପରି ବ୍ୟକ୍ତିଗତ ବିବରଣୀ ସେୟାର କରିବାରେ ସତର୍କ ରୁହନ୍ତୁ। ଠକେଇମୂଳକ ରଣ ଅଫର: ଯଦି ଆପଣ କୌଣସି ରଣ କିମ୍ବା ଆର୍ଥିକ ଉତ୍ସାହ ପାଇଁ ଅପ୍ରତ୍ୟାଶିତ ପ୍ରସ୍ତାବ ପାଆନ୍ତି, ତେବେ ଆଗକୁ ବଢ଼ିବା ପୂର୍ବରୁ ଅଫିସିଆଲ ଚ୍ୟାନେଲ ମାଧ୍ୟମରେ ସିଧାସଳଖ ଫିନୋ ପେମେଣ୍ଟସ୍ ବ୍ୟାଙ୍କ ସହିତ ଏହାର ସତ୍ୟତା ଯାଞ୍ଚ କରନ୍ତୁ। ଭିସିଂ (ଭଏସ୍ ଫିସିଂ): ବ୍ୟାଙ୍କ କର୍ମଚାରୀ କିମ୍ବା ଗ୍ରାହକ ସେବା ଏଜେଣ୍ଟଙ୍କ ପରିଚୟ ଦେଇ କଲ୍ ମାଧ୍ୟମରେ ଆପଣଙ୍କ ଆର୍ଥିକ କାରବାର ବିବରଣୀ କିମ୍ବା ପାସୱାର୍ଡ ମାଗୁଥିବା ଲୋକଙ୍କଠାରୁ ସତର୍କ ରୁହନ୍ତୁ। ଯଦି ଆପଣ ନିଶ୍ଚିତ ନୁହଁନ୍ତି, ତେବେ ଫୋନ୍ କାଟି ଦିଅନ୍ତୁ ଏବଂ ଅଫିସିଆଲ ଚ୍ୟାନେଲ ମାଧ୍ୟମରେ ବ୍ୟାଙ୍କ ସହିତ ଯୋଗାଯୋଗ କରନ୍ତୁ। ନକଲି ଗ୍ରାହକ ସେବା ନମ୍ବର: ସର୍ବଦା ଅଫିସିଆଲ ୱେବସାଇଟ୍ କିମ୍ବା ଆପ୍ ରୁ ସିଧାସଳଖ ବ୍ୟାଙ୍କର ଯୋଗାଯୋଗ ନମ୍ବର ଯାଞ୍ଚ କରନ୍ତୁ। ଠକମାନେ ପ୍ରାୟତଃ ଲୋକମାନଙ୍କୁ ସେମାନଙ୍କର ବ୍ୟାଙ୍କ ବିବରଣୀ ସେୟାର କରିବାକୁ ପ୍ରଲୋଭିତ କରିବା ପାଇଁ ଇଣ୍ଟରନେଟ୍ରେ ନକଲି ଗ୍ରାହକ ସେବା ନମ୍ବର ପୋଷ୍ଟ କରିଥାନ୍ତି। UPI କାରବାର: UPI ପେମେଣ୍ଟ କରିବା ସମୟରେ, ପ୍ରାପ୍ତକର୍ତ୍ତାଙ୍କ ବିବରଣୀକୁ ସାବଧାନତାର ସହ ଯାଞ୍ଚ କରନ୍ତୁ। ଠକମାନେ ଆପଣଙ୍କୁ ଭୁଲ ଆକାଉଣ୍ଟକୁ ଟଙ୍କା ସ୍ଥାନାନ୍ତର କରିବାକୁ ଚେଷ୍ଟା କରିପାରନ୍ତି। ସନ୍ଦେହଜନକ ଲିଙ୍କ୍ ଏବଂ ଇମେଲ୍: ଇମେଲ୍ କିମ୍ବା SMS ମାଧ୍ୟମରେ ପଠାଯାଇଥିବା ସନ୍ଦେହଜନକ ଲିଙ୍କ୍ ଉପରେ କ୍ଲିକ୍ କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ। ଠକମାନେ ଏଗୁଡ଼ିକୁ ଆପଣଙ୍କ ସୂଚନା ଚୋରି କରିବା ପାଇଁ କିମ୍ବା ଆପଣଙ୍କ ଡିଭାଇସ୍‌ରେ ମାଲୱେର୍ ସଂସ୍ଥାପନ କରିବା ପାଇଁ ବ୍ୟବହାର କରିପାରନ୍ତି।

కస్టమర్ అవగాహన: సురక్షిత బ్యాంకింగ్ కోసం చేయదగినవి మరియు చేయకూడనివి

చేయదగినవి

1. మీ బ్యాంకింగ్ సమాచారాన్ని సురక్షితంగా ఉంచుకోండి
మీ డెబిట్ కార్డును ఎల్లప్పుడూ భద్రంగా ఉంచుకోండి మరియు దానిని సురక్షితమైన స్థలంలో ఉంచండి.
మీ ఎటిఎం, డెబిట్ కార్డ్ పిన్ ని జ్ఞాపకం ఉంచుకోండి మరియు దేనిపైన అయినా దానిని వ్రాయడం మానండి.
ముఖ్యంగా ఇంటర్నెట్ మరియు మొబైల్ బ్యాంకింగ్ కోసం మీ పాస్వర్డ్ లు మరియు పిన్లను క్రమం తప్పకుండా మార్చండి.

2. మీ ఖాతాలను పర్యవేక్షించండి
ఏవైనా అనధికార కార్యకలాపాల కోసం మీ లావాదేవీ చరిత్రను క్రమం తప్పకుండా చెక్ చేసుకోండి.
ఏవైనా అనుమానాస్పద లావాదేవీలను వెంటనే బ్యాంకుకు వీటి ద్వారా తెలియజేయండి:
కస్టమర్ కేర్: 022 6868 1414
ఇమెయిల్: customercare@finobank.com
మోసాన్ని రిపోర్టు చేసే ఇమెయిల్: reportfraud@finobank.com
మీ ఖాతాను పర్యవేక్షించడానికి మరియు అవసరమైనప్పుడు మీ కార్డులను బ్లాక్/అన్ బ్లాక్ చేయడానికి ఫీనో పేమెంట్స్ బ్యాంక్ యొక్క మొబైల్ యాప్ ని ఉపయోగించండి.

3. బలమైన భద్రతా చర్యలను ఉపయోగించండి
మీ మొబైల్ బ్యాంకింగ్ యాప్ లు, అప్రెటింగ్ సిస్టమ్ లు మరియు యాంటివైరస్ సాఫ్ట్వేర్ లను అప్డేట్ గా ఉంచుకోండి.
అదనపు భద్రతా కవచం కోసం సాధ్యమైన చోట్లా బహుళ-కారకాల అధికరణ (MFA)ని సక్రియం చేసుకోండి.

4. ఫిషింగ్ స్కామ్ ల పట్ల అప్రమత్తంగా ఉండండి
విశ్వసనీయమైన మూలాల నుండి వచ్చే లింక్ లపై మాత్రమే క్లిక్ చేయండి. అధికారిక ఫీనో పేమెంట్స్ బ్యాంక్ వెబ్ సైట్ కోసం సరిచూసుకోండి లేదా వారి తెలిసిన మార్గాల ద్వారా సంప్రదించండి.
సున్నితమైన సమాచారాన్ని కోర్ అవాంఛిత ఇమెయిల్లు, కాల్స్ లేదా సందేశాల పట్ల జాగ్రత్తగా ఉండండి.
ఫిషింగ్ ఎర్ర జెండాలు కోసం చూడండి: వ్యాకరణ దోషాలు, వింతైన URL లు మరియు వ్యక్తిగత వివరాల కోసం అత్యవసర అభ్యర్థనలు.

5. సురక్షిత లావాదేవీలను నిర్వహించండి
ATMలు లేదా POS టెర్మినల్స్ ఉపయోగిస్తున్నప్పుడు, స్కిమ్మింగ్ పరికరాలు లేదా ఏవైనా అనుమానాస్పద కార్యకలాపాల కోసం చెక్ చేయండి.
ATMల వద్ద లేదా ఆన్లైన్ చెల్లింపుల సందర్భంగా మీ పిన్ను ఎంటర్ చేసేటప్పుడు ఎల్లప్పుడూ కీప్యాడ్ను కప్పి ఉంచుకోండి.

6. మోసాన్ని వెంటనే రిపోర్టు చేయండి
మీరు మోసాన్ని గనక అనుమానించినట్లయితే, వెంటనే బ్యాంకుకు వీటి ద్వారా తెలియజేయండి:
కస్టమర్ కేర్: 022 6868 1414
మోసాన్ని రిపోర్టు చేసే ఇమెయిల్: reportfraud@finobank.com
అంతే కాకుండా, తదుపరి చర్య కోసం స్థానిక చట్ట అమలు యంత్రాంగం లేదా సైబర్ క్రైమ్ సెల్కు తెలియజేయండి.

చేయకూడనివి

1. వ్యక్తిగత వివరాలను పంచుకోవడం మానండి
తాము ఫీనో పేమెంట్స్ బ్యాంక్ నుండి వచ్చినట్లు చెప్పుకున్నప్పటికీ సైతం మీ డెబిట్ కార్డ్ నంబర్, CVV, OTP లేదా PIN ని ఎవరితోనూ పంచుకోవద్దు. మీ బ్యాంకింగ్ పాస్వర్డ్, OTP లేదా ఖాతా వివరాలను ఫోన్, SMS లేదా ఇమెయిల్ ద్వారా తెలియజేయవద్దు.
వీటిద్రాయల్స్, లావాదేవీలు లేదా ఏ ఉద్దేశ్యానికైనా సరే మీ డెబిట్ కార్డును ఎవరి చేతికి అప్పగించవద్దు.

2. మోసపూరిత కమ్యూనికేషన్ పట్ల ఎరగా మారవద్దు
సున్నితమైన సమాచారాన్ని అడిగే కాల్స్, SMS లేదా ఇమెయిల్స్ పట్ల చాలా జాగ్రత్తగా ఉండండి.
మీ వ్యక్తిగత బ్యాంకింగ్ సమాచారాన్ని అడిగే అవాంఛిత కమ్యూనికేషన్లకు ఎప్పటికీ స్పందించవద్దు.
గుర్తుంచుకోండి, ఫీనో పేమెంట్స్ బ్యాంక్ మీ బ్యాంక్ బ్యాలెన్స్, కార్డు వివరాలు, పిన్ లేదా పాస్వర్డ్ను ఎప్పటికీ అడగదు.

3. అసురక్షిత నెట్వర్క్ లను ఉపయోగించడం మానండి
పబ్లిక్ వై-ఫై లేదా కేఫెలు లేదా బ్రెజరిలలో ఉన్నటువంటి పంపక నెట్ వర్క్లలో ఆన్లైన్ బ్యాంకింగ్ చేయకుండా ఉండండి.
ఇంటర్నెట్ బ్యాంకింగ్ లావాదేవీల కోసం సైబర్ కేఫెలు లేదా పబ్లిక్ కంప్యూటర్లను ఉపయోగించడం మానండి.

4. రహస్యమైన సమాచారాన్ని నిల్వ చేయవద్దు:
మీ బ్యాంకింగ్ పాస్వర్డ్లు లేదా పిన్లను సులభంగా ప్రాప్యత చేసుకోగల ప్రదేశాలలో లేదా మీ ఫోన్లో సేవ్ చేయవద్దు.
పాస్వర్డ్లు లేదా కార్డ్ నంబర్లు వంటి సున్నితమైన డేటాను వ్రాసి ఉంచుకోవడం మానుకోండి మరియు బదులుగా వాటిని జ్ఞాపకం ఉంచుకోండి.

5. నమ్మదగని వెబ్ సైట్లు లేదా యాప్లను ఉపయోగించవద్దు
మీరు ఫీనో పేమెంట్స్ బ్యాంక్ యాప్ను Google Play లేదా Apple యొక్క యాప్ స్టోర్ వంటి అధికృత యాప్ స్టోర్ల నుండి మాత్రమే డౌన్లోడ్ చేసుకునేలా నిర్ధారించుకోండి.
URL లో "https://" లేని లేదా విశ్వసనీయమైన భద్రతా సర్టిఫికేట్లు లేని వెబ్ సైట్లపై లావాదేవీలు నిర్వహించడం మానుకోండి.

6. మీ మొబైల్ లేదా ఇంటర్నెట్ బ్యాంకింగ్ ప్రాప్యతను పంచుకోవద్దు
మీ మొబైల్ బ్యాంకింగ్ యాప్ లేదా ఇంటర్నెట్ బ్యాంకింగ్ పోర్టల్ ప్రాప్యతను ఎవరితోనైనా సరే పంచుకోవడం మానుకోండి.
అదనపు అవగాహన చిట్కాలు:
గుర్తింపు చోరీ: మీ ఆధార్ నంబర్, పాన్ కార్డ్ లేదా ఇతర గుర్తింపు ఋజువుల వంటి వ్యక్తిగత వివరాలను కచ్చితంగా అవసరమైతే తప్ప మరియు విశ్వసనీయ వర్గాలతో మాత్రమే పంచుకునేటప్పుడు జాగ్రత్తగా ఉండండి. మోసపూరితమైన లోన్ ఆఫర్లు: మీరు ఊహించని విధంగా లోన్ లేదా ఆర్థిక ఉత్పాదన ఆఫర్లను అందుకుంటే, కొనసాగే ముందుగా అధికారిక మార్గాల ద్వారా ఫీనో పేమెంట్స్ బ్యాంకుతో నేరుగా అధికరణను వెరిఫై చేసుకోండి. విషింగ్ (స్వరం అనుకరణ): మీ ఆర్థిక వివరాలు లేదా పాస్వర్డ్లను అడుగుతూ బ్యాంకు ఉద్యోగులు లేదా కస్టమర్ సర్వీస్ ఏజెంట్ల వలె నటించే కాలర్ల పట్ల అప్రమత్తంగా ఉండండి. మీకు కచ్చితంగా తెలియకపోతే, కాల్ నిలిపి ఉంచి అధికారిక మార్గాల ద్వారా బ్యాంకును సంప్రదించండి. నకిలీ కస్టమర్ కేర్ నంబర్లు: ఎల్లప్పుడూ అధికారిక వెబ్ సైట్ లేదా యాప్ నుండి నేరుగా బ్యాంక్ సంప్రదింపు నంబర్లను వెరిఫై చేసుకోండి. మోసగాళ్లు తరచుగా ఇంటర్నెట్ యందు నకిలీ కస్టమర్ కేర్ నంబర్లను పోస్ట్ చేసి బాధితులు తమ బ్యాంకింగ్ వివరాలను పంచుకునేలా ప్రలోభపెడుతుంటారు. యుపిఐ లావాదేవీలు: యుపిఐ చెల్లింపులు చేస్తున్నప్పుడు, స్వీకర్త వివరాలను జాగ్రత్తగా వెరిఫై చేసుకోండి. మోసగాళ్లు మిమ్మల్ని మోసగించి తప్పుడు ఖాతాకు డబ్బును బదిలీ చేయించడానికి ప్రయత్నించవచ్చు. అనుమానాస్పద లింక్లు మరియు ఇమెయిల్స్: ఇమెయిల్ లేదా SMS ద్వారా పంపించబడిన అనుమానాస్పద లింక్లపై క్లిక్ చేయడం మానుకోండి. మోసగాళ్లు మీ సమాచారాన్ని దొంగిలించడానికి లేదా మీ పరికరంలో మాల్వేర్ను ఇన్ స్టాల్ చేయడానికి వీటిని ఉపయోగించుకోవచ్చు.