सुरक्षित ऑनलाइन बँकिंग-सुरक्षा टिप्स

सुरक्षित बँकिंग

आपल्या खात्याचे फसवणुकीपासून रक्षण करा

— डीबी ऑनलाइन बँकिंगमध्ये लॉगिन करताना आपला कस्टमर आय.डी/ युजर आय.डी आणि पासवर्ड साठविण्यासाठी ब्राउझरवर ऑटो सेव्ह वापरू नका.
— कृपया डॉइश बँकेकडे असलेला आपला संपर्क तपशील अद्ययावत करा जेणेकरून व्यवहार अधिकृत करण्यासाठी आपल्याला एक-वेळ (वन टाइम) पासवर्ड मिळू शकेल. एक-वेळ (वन टाइम) पासवर्ड म्हणजे आपल्या नोंदविलेल्या संपर्क तपशीलांवर पाठविलेला 6 अंकी संख्यात्मक कोड असतो. प्रमाणीकरणाचा हा दुसरा स्तर असतो जो आपल्या लॉगिन आणि ट्रान्झॅक्शन पासवर्ड व्यतिरिक्त असतो.
— अँटी-व्हायरस सॉफ्टवेअर कॉन्फिगर करा आणि आपल्या संगणकावर सॉफ्टवेअर नियमितपणे अपग्रेड केले आहे हे सुनिश्चित करून घ्या.
— आपल्या पी.सी /मोबाइल मध्ये पॉवर-ऑन/ ॲक्सेस पासवर्ड घाला, आपल्या पी.सी वर स्क्रीनसेव्हर पासवर्ड घाला. यामुळे इतर कोणालाही आपली संमती न घेता आपला पी.सी/ मोबाइल वापरता येणार नाही.
— कोणत्याही संकेतस्थळ वरील आणि ईमेल मधील संशयास्पद लिंक्सवर क्लिक करताना आणि आपल्या संगणकावर माहीत नसलेले किंवा अविश्‍वसनीय सॉफ्टवेअर स्थापित करताना अत्यंत सावधगिरी बाळगा. अँटीव्हायरस सॉफ्टवेअर स्वतःच पुरेसे नसते, विशेषत: मालवेअर विरूद्ध, जे आपले की स्ट्रोक्स लॉग करते आणि अशा प्रकारे आपला पासवर्ड कोणालाही कळू शकतो.
— मजबूत पासवर्ड तयार करा
    — पासवर्ड अल्फान्यूमेरिक असावा म्हणजेच त्यात अंक आणि अक्षरे दोन्ही असावित
    — पासवर्डमध्ये कमीत कमी 6 अक्षरे आणि जास्तीत जास्त 28 अक्षरे असावीत
    — पासवर्ड मध्ये स्पेसेस असू नयेत
    — विशेष अक्षरे जसे !,*,.,),+,=,? असू शकतात
    — कस्टमर आय.डी मधील सर्व अक्षरे आपल्या पासवर्डमध्ये असू नयेत.

उदाहरणार्थ, जर आपला कस्टमर आय.डी 000011120 असेल तर एबीसीडी012 हा एक वैध पासवर्ड असू शकत नाही.

— आपले पासवर्ड्स लक्षात ठेवा. आपल्याला ते लेखी ठेवायचे असतील, तर ते सुरक्षित ठिकाणी आहेत हे सुनिश्चित करून घ्या.
— इंटरनेट बँकिंग पासवर्ड (आयपिन) केस सेन्सिटिव्ह असतात.
— डॉइश बँकेच्या कर्मचाऱ्यांसह कोणालाही आपला पासवर्ड कधीही सांगू नका. आपला पासवर्ड विचारणाऱ्या कोणत्याही मेलला कधीही उत्तर देऊ नका.
— कृपया लक्षात असू द्या की डॉइश बँक कधीही आपला पासवर्ड विचारणार नाही.
— अंदाज लावणे सोपे असे पासवर्ड्स वापरू नका जसे की:

    — जन्मतारीख, महिने किंवा वर्ष
    — अनुक्रमिक संख्या (उदाहरणार्थ 6789)
    — सहज अंदाज लावता येईल असे संख्या संयोजन (उदाहरणार्थ 1111)
    — आपल्या दूरध्वनी क्रमांकाचे काही भाग
    — आपल्या कोणत्याही कार्डवर ज्या क्रमाने ते छापले जातात त्या क्रमाने क्रमांकांचे भाग
    — इतर सहज उपलब्ध वैयक्तिक माहिती (उदाहरणार्थ ड्रायव्हिंग लायसन्स, किंवा आपल्याशी सहज जोडलेले इतर क्रमांक)
    — कुटुंबातील सदस्यांची, पाळीव प्राण्यांची किंवा रस्त्यांची नावे.

— आपण आपला कस्टमर आय.डी आणि पासवर्ड लिहित असताना इतरांना आपली स्क्रीन दिसत नाही आणि आपण पाठीमागून पाहिले जाणार नाही आहात याची कृपया खात्री करून घ्या.
— आपल्या ऑनलाइन बँकिंग प्रवेशाची सुरक्षितता वाढविण्यासाठी लॉगिन आणि व्यवहारासाठी स्वतंत्र पासवर्ड वापरण्याची शिफारस केली जाते.
— आपण केवळ अस्सल डॉइश बँक साइटवर प्रवेश करीत आहात याची खात्री करण्यासाठी नेहमी ब्राउझरवर (www.deutschebank.co.in आणि लॉगिन बटणावर क्लिक करा) यू.आर.एल टाइप करा
— डीबी ऑनलाइन बँकिंगमध्ये लॉगिन करताना प्रत्येक वेळी आपली शेवटची लॉगिन तारीख आणि वेळ तपासा. वेळोवेळी आपले पासवर्ड बदला आणि कोणताही गैरवापर टाळा.
— सार्वजनिक किंवा वाटून घेतलेल्या संगणकावरून ऑनलाइन बँकिंग करणे टाळा. आपल्या खात्यात कधीही व्हायरसने संक्रमित असलेल्या संगणकावरून प्रवेश करू नका.
— ऑनलाइन बँकिंग करताना अनेक ब्राउझर विंडो उघडू नका.
— आपण आपले व्यवहार पूर्ण करताच डीबी ऑनलाइन बँकिंग मधून लॉग आऊट करा. तसेच आपण ती विंडो बंद केल्याची खात्री करून घ्या.
— आपल्या ऑपरेटिंग सिस्टिमवर 'फाइल अँड प्रिंटिंग शेअरिंग' वैशिष्ट्य अक्षम करा.
— आपल्याकडून आकारलेली रक्कम आपल्याला ओळखता आली नाही तर कृपया त्वरित डॉइश बँकेला तसे लेखी कळवा.

इतर कोणतीही चिंता असल्यास, कृपया 1860 266 6601# वर आमच्या 24/7 फोन बँकिंग टीमला कॉल करा

भारताबाहेरील ग्राहकांनी +91 22 6601 6601 डायल करणे आवश्यक आहे
मुंबईतील ग्राहकांना 6601 6601 या क्रमांकावर सुद्धा कॉल करता येईल. कॉल शुल्क लागू आहेत.

वर्धित डीबी ऑनलाइन बँकिंग सुरक्षा

— आपल्या खात्याचे अनधिकृत प्रवेशापासून संरक्षण करण्यासाठी आम्ही डीबी ऑनलाइन बँकिंग सलग 60 मिनिटांसाठी वापरल्यावर लॉगिन पासवर्डचे पुन्हा प्रमाणीकरण सुरू केले आहे. यासह, 60 मिनिटांपेक्षा अधिक चालणाऱ्या प्रत्येक सत्रासाठी, आपल्याला पुन्हा लॉगिन करण्यास सांगितले जाईल
— तसेच, जर आपले डीबी ऑनलाइन बँकिंग लॉगिन सत्रात 8 मिनिटांपेक्षा जास्त काळ काहीच केले नाही तर सिस्टम आपोआप आपल्याला सत्रातून लॉग आऊट करते. आपल्याला निष्क्रिय वेळेचा मागोवा ठेवण्यास मदत व्हावी म्हणून आपल्याला पृष्ठाच्या वरच्या डाव्या कोपऱ्यातील टाइमरचा संदर्भ घेऊन त्यानुसार आपल्या व्यवहारांचे नियोजन करता येईल.

आम्ही आपला ऑनलाइन बँकिंग अनुभव सुरक्षित करण्यासाठी संरक्षणाचे अनेक थर प्रदान करतो:

— आपला व्यवहार चांभारचौकश्यांपासून सुरक्षित ठेवण्यासाठी 256 बिट टीएलएस एन्क्रिप्शन.
— व्हर्च्युअल कीपॅड जे आपले दुर्भावनापूर्ण 'स्पायवेअर' आणि 'ट्रोजन' प्रोग्राम्सपासून आपले संरक्षण करण्यासाठी कीस्ट्रोक कॅप्चर करता यावेत म्हणून डिझाइन केलेले असतात
— आपल्या आर्थिक व्यवहारांना वाढीव सुरक्षा प्रदान करण्यासाठी पासवर्डचे दोन स्तर.
— ओ.टी.पी हा सध्याच्या लॉगिन आणि ट्रान्झॅक्शन पासवर्ड प्रमाणीकरणाच्या पलीकडे सुरक्षेचा अतिरिक्त थर असतो. प्रत्येक वेळी आपण संवेदनशील/ आर्थिक व्यवहार करण्याचा प्रयत्न करता तेव्हा आपल्या नोंदविलेल्या संपर्क तपशीलांवर पाठविलेला हा 6 अंकी संख्यात्मक कोड असतो. खाली नमूद केलेल्या व्यवहारांना अधिकृत करण्यासाठी ओ.टी.पी आवश्यक असतो:

    — इतर बँकांमधील लाभार्थी बँक खाती नोंदविण्यासाठी
    — बिल देयकांसाठी
    — ई-कॉमर्स देयकांसाठी
    — डीबी क्विकपे साठी
    — एन.ई.एफ.टी/ आर.टी.जी.एस साठी (व्यवहार मूल्य रु. 10,000 किंवा त्यापेक्षा जास्त साठी)
    — इतर डॉइश बँक खात्यांमध्ये निधी हस्तांतरित करण्यासाठी
    — मोबाइल/ ईमेल आय.डी बदलण्यासाठी
    — अलर्ट प्रोफाइल बदलण्यासाठी
    — व्यवहारादरम्यान तयार होणारा ओ.टी.पी त्या व्यवहारासाठी फक्त 5 मिनिटांपर्यंत वैध असतो.

— आपल्या पासवर्डच्या सुरक्षेसाठी कठोर पासवर्ड सुरक्षा उपाय.
— आम्ही 60 मिनिटांच्या सलग वापरानंतर लॉगिन पासवर्ड प्रमाणीकरण करण्याचा अतिरिक्त सुरक्षा थर तयार केला आहे जेणेकरून आपल्या खात्याचे रक्षण करता येईल. हे सुनिश्चित करेल की आपले लॉगिन सत्र अनधिकृत प्रवेशापासून सुरक्षित आहे. आपण डीबी ऑनलाइन बँकिंगमध्ये प्रवेश करू इच्छित नसल्यास, आपल्याला लॉग-आऊट बटणावर क्लिक करता येईल आणि सत्र समाप्त करता येईल.
— डॉइश बँक संगणकावरील ट्रोजन प्रोग्रामवर लक्ष ठेवते जे डीबी ऑनलाइन बँकिंगमध्ये प्रवेश करण्यासाठी वापरले जातात. संगणकावर कोणताही दुर्भावनापूर्ण प्रोग्राम आढळल्यास डॉइश बँक अशा ग्राहकाचा इंटरनेट प्रवेश अक्षम करेल जो त्या संगणकावरून लॉगिन करत आहे. आमची फोन बँकिंग टीम याची माहिती कळवेल.

सुरक्षित डेटाचे हस्तांतरण

अनधिकृत पक्षांना माहिती वाचण्यापासून रोखण्यासाठी एन्क्रिप्शन ही माहिती प्रसारणासाठी वापरण्याची एक पद्धत आहे. एस.एस.एल एन्क्रिप्ट केलेल्या संप्रेषणासाठी उद्योग मानक आहे आणि इंटरनेटवर बँकेशी ग्राहकांचा संवाद सुरक्षित आहे याची खात्री करते. डॉइश बँक ए.जी, भारत येथे, आम्ही सेक्युअर सॉकेट्स लेयर (एस.एस.एल) सत्राच्या एन्क्रिप्शनसाठी व्हेरीसाइनचे 128-बिट डिजिटल प्रमाणपत्र वापरतो. डेटाचे हे एन्क्रिप्शन इंटरनेटद्वारे जेव्हा डेटा फिरत असतो तेव्हा छेडछाडीपासून भक्कम प्रमाणात संरक्षण उपलब्ध करून देते.

पृष्ठाच्या वरच्या बाजूला आपल्याला बंद कुलूपाचे (क्लोज्ड लॉक) आयकॉन दिसेल.

व्हर्च्युअल कीपॅडचे वैशिष्ट्य

व्हर्च्युअल कीपॅड हे आपल्या नेहमीच्या कीबोर्डचे ऑनलाइन रूप आहे. आपला पासवर्ड क्लिक करण्यासाठी आपल्या माऊसचा वापर करा. कीस्ट्रोक कॅप्चर करण्यासाठी डिझाइन केलेल्या दुर्भावनापूर्ण 'स्पायवेअर' आणि 'ट्रोजन' प्रोग्राम्सपासून हे आपले संरक्षण करते. आम्ही आपल्याला शिफारस करतो की आपल्याला संगणकाच्या सुरक्षिततेबद्दल खात्री नसेल तर आपण संगणकावरून लॉगिन करताना आभासी कीपॅड वापरावा. अँटी-व्हायरस सॉफ्टवेअर अद्ययावत केले गेले नाही, असे सायबर कॅफे किंवा मशीन, हे असुरक्षित वातावरणाच्या उदाहरणांमध्ये सामील आहेत.

नेहमीचे व्हर्च्युअल कीपॅड्स कीज गतिशीलपणे मिसळून हे साध्य करतात, परंतु यामुळे वापरकर्त्यांना अक्षरे लिहिणे कठीण होते. डॉइश बँकेचे व्हर्च्युअल कीपॅड संपूर्ण कीपॅडला गतिशीलपणे फिरवतो, यात कीज मिसळल्या जात नाहीत आणि त्यामुळे सुरक्षितता आणि सुविधा दोन्ही प्राप्त होतात.

पासवर्डची सुरक्षा

पासवर्ड आपोआप तयार होतात, पासवर्ड मेलर्स वर छापले जातात, सील बंद केले जातात आणि मानवी हस्तक्षेप न करता आपल्या मेलिंग पत्त्यावर पाठविले जातात. सुरक्षिततेच्या कारणास्तव लॉगिनसाठी आवश्यक ग्राहक आय.डी/ वापरकर्ता आय.डी असलेल्या इतर कोणत्याही कागदपत्रांसह पासवर्ड पाठविले जात नाहीत. आपले पासवर्ड नेहमी बँकेच्या सुरक्षित यंत्रणेत पूर्णपणे गोपनीय ठेवले जातात. कृपया लक्ष असू द्या की बँकेच्या कर्मचाऱ्यांना सुद्धा आपल्या पासवर्डची माहिती उपलब्ध नसते आणि कोणत्याही परिस्थितीत बँक कर्मचाऱ्यांसह कोणालाही ऑनलाइन बँकिंग पासवर्ड सांगू नये.

ट्रान्झॅक्शन पासवर्डची मुदत 90 दिवसांत संपते, त्यानंतर डीबी ऑनलाइन बँकिंगमध्ये लॉगिन करता यावे म्हणून आपल्याला पासवर्ड बदलण्यास सांगितले जाते. कृपया लक्ष असू द्या की जर ट्रान्झॅक्शन पासवर्ड नवीन तयार करताना विद्यमान पासवर्ड आपल्याला घालता आला नाही, तर आपल्याला पासवर्डच्या नवीन सेटसाठी विनंती करावी लागेल.

डीबी ऑनलाइन बँकिंगमध्ये आपण जर का 180 दिवसांपेक्षा जास्त काळ लॉगिन केले नसेल तर डीबी ऑनलाइन बँकिंगचा आपला प्रवेश आपोआप निष्क्रिय करण्यात येतो. कृपया आमच्या फोन बँकिंग टीमला 1860 266 6601# वर कॉल करून तो सक्रिय करून घ्यावा.

आपण आपल्या सक्रिय डेबिट कार्ड क्रमांकाचा वापर करून त्वरित आपला आयपिन ऑनलाइन तयार करू शकता. ऑनलाइन आयपिन निर्मितीसाठी आम्ही आपल्याला आपल्या नोंदविलेल्या मोबाइल आणि ईमेल आय.डी यांच्यावर एक रॅंडम ॲक्सेस कोड (आर.ए.सी) आणि युनिक रेफरन्स नंबर (यू.आर.एन) पाठवतो. तीन अवैध प्रयत्न झाल्यास आम्ही आपली ऑनलाइन आयपिन सुविधा ब्लॉक करतो आणि त्यावर एस.एम.एस/ ईमेल अलर्ट पाठवितो.

फिशिंग अटॅक

'फिशिंग अटॅक' म्हणजे असे प्रयत्न जे बनावट कंपनीच्या ईमेल प्रेषक पत्त्यांचा वापर करून ईमेल द्वारे ग्राहकांच्या प्रवेशाची गोपनीय माहिती मिळवण्यासाठी केले जातात. ग्राहकांच्या ओळखीचे आणि विश्वासार्ह कंपन्यांचे बनावट ईमेल पत्ते या हल्ल्यांमध्ये वापरले जातात. ग्राहकाला ईमेल उत्तराच्या माध्यमातून किंवा बनावट संकेतस्थळाकडे नेणाऱ्या लिंकच्या माध्यमातून गोपनीय खाते प्रवेशाची माहिती देण्यास सांगितले जाते. त्यानंतर ग्राहकाच्या नकळत माहितीचा गैरवापर होऊ शकतो.

डॉइश बँक ईमेल किंवा एस.एम.एस द्वारे आपली गोपनीय किंवा वैयक्तिक माहिती (जसे की आपले खाते क्रमांक, डेबिट कार्ड क्रमांक, ए.टी.एम पिन किंवा ऑनलाइन बँकिंग पासवर्ड) कधीही विचारणार नाही. तसेच, डॉइश बँकेने पाठविलेल्या कोणत्याही ईमेलमध्ये दिलेल्या लिंकवरून लॉगिन करण्यास सांगितले जाणार नाही. डॉइश बँकेचा असल्याचा दावा करणारा ईमेल, फसवा असल्याचा आपल्याला संशय आल्यास ताबडतोब बँकेला तसे कळवा.

अज्ञात स्त्रोताकडून आलेल्या ईमेल अटॅचमेंट उघडण्यापूर्वी त्या स्कॅन करण्याचा सल्ला नेहमीच दिला जातो.

निष्क्रिय वेळ लॉग-आऊट

जर आपण आपल्या डीबी ऑनलाइन बँकिंगमध्ये लॉगिन केले आणि 8 मिनिटांसाठी सत्रात काहीच केले नाही, तर आम्ही आपल्याला सत्रातून आपोआप लॉग आऊट करतो जेणेकरून आपल्या खात्यातील अनधिकृत प्रवेशापासून बचाव करता येईल.

निष्क्रिय वेळेचा मागोवा घेण्यास मदत करण्यासाठी, आपण सत्र समाप्तीच्या टाइमरसाठी पृष्ठाच्या वरचा डावा कोपरा पाहू शकता आणि त्यानुसार आपल्या व्यवहारांचे नियोजन करू शकता. जर सत्र संपले असेल तर टाइमर आपल्याला पुन्हा लॉगिन करण्याचा संकेत देईल.

सुरक्षित बँकिंगसाठी टिप

कार्ड किंवा पिन हरवल्यास किंवा चोरी झाल्यास किंवा अनधिकृतपणे कार्ड वापरल्यास आपले डॉइश बँकेचे डेबिट कार्ड त्वरित ब्लॉक करा

- आपल्या नोंदविलेल्या मोबाइल क्रमांकावरून 561615 वर "फ्रॉड" असा एस.एम.एस पाठवा
- आम्हाला report.fraud@list.db.com येथे ईमेल पाठवा
- ऑनलाइन फसवणुकीची तक्रार करण्यासाठी येथे क्लिक करा
- आमच्या "1860 266 6601*" या 24/7 फोनबँकिंग क्रमांकावर कॉल करा आणि पर्याय 1 निवडा
- आमच्या "1800 123 6601" या समर्पित टोल फ्री क्रमांकावर कॉल करा

* भारताबाहेरील ग्राहकांनी +91 22 6601 6601 डायल करणे आवश्यक आहे.
मुंबईतील ग्राहकांना 6601 6601 या क्रमांकावर सुद्धा कॉल करता येईल. कॉल शुल्क लागू आहेत.