सुरक्षित ऑनलाइन बैंकिंग - सुरक्षा सुझाव

सुरक्षित बैंकिंग

अपने खाते को धोखाधड़ी से बचाएं

— डीबी ऑनलाइनबैंकिंग में लॉग इन करते समय अपनी ग्राहक आईडी/ यूजर आईडी और पासवर्ड संग्रहीत करने के लिए ब्राउज़र पर ऑटो सेव का उपयोग न करें।

— कृपया ड्यूश बैंक के साथ अपना संपर्क विवरण अपडेट करें ताकि आप लेनदेन प्राधिकार के लिए वन टाइम पासवर्ड प्राप्त कर सकें। वन टाइम पासवर्ड आपके पंजीकृत संपर्क विवरण पर भेजा गया 6 अंकों का संख्यात्मक कोड है। यह आपके लॉगिन और लेनदेन पासवर्ड के अलावा प्रमाणीकरण का दूसरा स्तर है।

— एंटी-वायरस सॉफ़्टवेयर कॉन्फ़िगर करें और सुनिश्चित करें कि सॉफ़्टवेयर आपके कंप्यूटर पर नियमित रूप से अपग्रेड किया जाता है।

— अपने पीसी/ मोबाइल में पावर-ऑन/ एक्सेस पासवर्ड, अपने पीसी पर स्क्रीनसेवर पासवर्ड लगाएं, ताकि कोई भी आपकी सहमति के बिना आपके पीसी/ मोबाइल का उपयोग न कर सके।

— किसी भी वेबसाइट और ईमेल पर संदिग्ध लिंक पर क्लिक करते समय और अपने कंप्यूटर पर अज्ञात या अविश्वसनीय सॉफ़्टवेयर इंस्टॉल करते समय अत्यधिक सावधानी बरतें। एंटीवायरस सॉफ़्टवेयर अपने आप में विशेष रूप से मैलवेयर के विरुद्ध पर्याप्त नहीं है जो आपके कुंजी स्ट्रोक को लॉग करता है और इस प्रकार आपके पासवर्ड से समझौता कर सकता है।

— एक मजबूत पासवर्ड बनाएं -

  — पासवर्ड अल्फा न्यूमेरिक होना चाहिए यानी इसमें अंक और अक्षर दोनों होने चाहिए
  — पासवर्ड में कम से कम 6 अक्षर और अधिकतम 28 अक्षर होने चाहिए
  — पासवर्ड में रिक्त स्थान की अनुमति नहीं है
  — विशेष वर्ण जैसे !,*,.,),+,=,? की अनुमति दी जाती है
  — ग्राहक आईडी के सभी अक्षर आपके पासवर्ड में मौजूद नहीं होने चाहिए।
  — जैसे यदि आपकी ग्राहक आईडी ००००१११२० है, तो पासवर्ड एबीसीडी०१२ वैध पासवर्ड नहीं है।

— अपने पासवर्ड याद रखें। यदि आप उन्हें लिखित रूप में रखते हैं, तो सुनिश्चित करें कि वे सुरक्षित स्थान पर हैं।

— इंटरनेट बैंकिंग पासवर्ड (आईपीआईएन) संवेदनशील अक्षर होते हैं।

— ड्यूश बैंक के कर्मचारियों सहित किसी को भी अपना पासवर्ड न बताएं। आपका पासवर्ड मांगने वाले किसी भी ईमेल का जवाब न दें।
— कृपया ध्यान दें कि ड्यूश बैंक कभी भी आपका पासवर्ड नहीं मांगेगा।
— अनुमान लगाने में आसान पासवर्ड का उपयोग न करें जैसे:
    — जन्म तिथियां, महीने या वर्ष
    — अनुक्रमिक संख्याएँ (जैसे ६७८९)
    — संख्या संयोजन जिनका आसानी से अनुमान लगाया जा सकता है (जैसे ११११)
    — आपके टेलीफ़ोन नंबर के भाग
    — संख्याओं के भाग उसी क्रम में जिस क्रम में वे आपके किसी भी कार्ड पर मुद्रित होते हैं
    — अन्य व्यक्तिगत डाटा जो आसानी से पहुंच योग्य (जैसे ड्राइविंग लाइसेंस, या अन्य नंबर जो आपसे जुड़ा हुआ हो)
    — परिवार के सदस्यों, पालतू जानवरों या सड़कों के नाम।

— जब आप अपना ग्राहक आईडी और पासवर्ड दर्ज करते हैं, तो कृपया सुनिश्चित करें कि कोई भी आपकी स्क्रीन नहीं देख पा रहा है और आप को पीछे से भी कोई नहीं देख रहा है।
— यह सलाह दी जाती है कि लॉगिन और लेनदेन के लिए अलग-अलग पासवर्ड का उपयोग किया जाए क्योंकि यह आपकी ऑनलाइन बैंकिंग पहुंच की सुरक्षा को बढ़ाएगा।
— यह सुनिश्चित करने के लिए कि आप केवल वास्तविक ड्यूश बैंक साइट तक पहुंच रहे हैं, हमेशा ब्राउज़र पर यूआरएल टाइप करें (www.deutschebank.co.in और लॉगिन बटन पर क्लिक करें)।
— हर बार जब आप डीबी ऑनलाइनबैंकिंग में लॉगिन करें तो अपको अंतिम लॉगिन तिथि और समय को भी जांचना चाहिए। और किसी भी दुरुपयोग से बचने के लिए समय-समय पर अपना पासवर्ड बदलते रहें।
— सार्वजनिक या सांझे कंप्यूटर से ऑनलाइन बैंकिंग करने से बचें। कभी भी अपने खाते को ऐसे कंप्यूटर से एक्सेस न करें जो वायरस से संक्रमित हो।
— ऑनलाइन बैंकिंग करते समय एकाधिक ब्राउज़र विंडो न खोलें।
— जैसे ही आप अपना लेनदेन पूरा कर लें, डीबी ऑनलाइनबैंकिंग से लॉग आउट करें। यह भी सुनिश्चित करें कि आप वह विंडो बंद कर दें।
— अपने ऑपरेटिंग सिस्टम पर 'फ़ाइल और प्रिंटिंग शेयरिंग' सुविधा को असमर्थ करें।
— यदि आप नहीं जानते कि आपसे कितनी राशि ली गई है, तो कृपया तुरंत ड्यूश बैंक को लिखित रूप में इसकी रिपोर्ट करें।

किसी अन्य विषय के मामले में, कृपया हमारी 24/7 फोन बैंकिंग टीम को 1860 266 6601 पर कॉल करें।

भारत से बाहर के ग्राहकों को +91 22 6601 6601 डायल करना होगा। मुंबई के ग्राहक भी 6601 6601 पर कॉल कर सकते हैं। कॉल शुल्क लागू है।

उन्नत डीबी ऑनलाइनबैंकिंग सुरक्षा

— आपके खाते को अनधिकृत पहुंच से सुरक्षित रखने के लिए हमने डीबी ऑनलाइनबैंकिंग के 60 मिनट के निरंतर उपयोग के बाद लॉगिन पासवर्ड पुनः सत्यापन की शुरुआत की है। इसके साथ ही, ६० मिनट से अधिक के प्रत्येक सत्र के लिए, आपको फिर से लॉगिन करने के लिए कहा जाएगा

— इसके अतिरिक्त, यदि आपका डीबी ऑनलाइनबैंकिंग लॉग इन सत्र ८ मिनट से अधिक समय तक निष्क्रिय रहता है, तो सिस्टम स्वचालित रूप से आपको सत्र से लॉग आउट कर देता है। निष्क्रिय समय पर नज़र रखने में मदद के लिए, आप पृष्ठ के ऊपरी बाएँ कोने पर टाइमर का संदर्भ ले सकते हैं और उसके अनुसार अपने लेनदेन की योजना बना सकते हैं।

हम आपके ऑनलाइन बैंकिंग अनुभव को सुरक्षित रखने के लिए सुरक्षा के और कई सुझाव प्रदान करते हैं:

— 256 बिट टीएलएस एन्क्रिप्शन प्रणाली आपके लेनदेन को चौकन्नी नजरों से सुरक्षित रखेगी।

— आपको दुर्भावनापूर्ण 'स्पाइवेयर' और 'ट्रोजन' प्रोग्राम से बचाने के लिए वर्चुअल कीपैड कीस्ट्रोक्स कैप्चर करने के लिए डिज़ाइन किया गया है।

— आपके वित्तीय लेनदेन को बेहतर सुरक्षा प्रदान करने के लिए पासवर्ड को दो स्तर का किया गया।

— ओटीपी मौजूदा लॉगिन और लेनदेन के लिए पासवर्ड प्रमाणीकरण सुरक्षा की एक अतिरिक्त सुविधा है। यह एक 6 अंकों का संख्यात्मक कोड है जो आपके पंजीकृत संपर्क विवरण पर भेजा जाता है, हर बार जब आप संवेदनशील/ वित्तीय लेनदेन का प्रयास करते हैं। नीचे उल्लिखित लेनदेन को अधिकृत करने के लिए ओटीपी आवश्यक है:

  – अन्य बैंकों के लाभार्थी बैंक खातों का पंजीकरण
  – बिल भुगतान
  – ई-कॉमर्स भुगतान
  – डीबी क्विकपे
  – एनईएफटी/ आरटीजीएस (लेन-देन मूल्य आईएनआर १०,००० और उससे अधिक के लिए)
  – अन्य इ्यूश बैंक खातों में धनराशि स्थानांतरण
  – मोबाइल/ ईमेल आईडी परिवर्तन
  – अलर्ट प्रोफ़ाइल परिवर्तन

- किसी लेन-देन के दौरान उत्पन्न ओटीपी केवल उस लेन-देन के लिए ५ मिनट तक वैध होता है।

— आपके पासवर्ड को सुरक्षित रखने के लिए कड़े पासवर्ड सुरक्षा उपाय।

— आपके खाते की सुरक्षा के लिए हमने 60 मिनट के निरंतर उपयोग के बाद लॉगिन पासवर्ड सत्यापन की एक अतिरिक्त सुरक्षा परत बनाई है। यह सुनिश्चित करेगा कि आपका लॉगिन सत्र अनधिकृत पहुंच से सुरक्षित है। यदि आप डीबी ऑनलाइनबैंकिंग का उपयोग नहीं करना चाहते हैं, तो आप लॉग-आउट बटन पर क्लिक कर सकते हैं और सत्र समाप्त कर सकते हैं।

— ड्यूश बैंक उन कंप्यूटरों पर ट्रोजन प्रोग्रामों की निगरानी करता है जिनका उपयोग डीबी ऑनलाइनबैंकिंग तक पहुंचने के लिए किया जाता है। यदि कंप्यूटर पर कोई दुर्भावनापूर्ण प्रोग्राम पाया जाता है, तो ड्यूश बैंक उस कंप्यूटर से लॉगिंग करने वाले ग्राहक की इंटरनेट एक्सेस को अक्षम कर देगा। हमारी फ़ोन बैंकिंग टीम इसकी सूचना देगी.

सुरक्षित डेटा स्थानांतरण

एन्क्रिप्शन अनधिकृत पक्षों को जानकारी पढ़ने से रोकने के लिए ट्रांसमिशन के लिए जानकारी को खंगालने की एक विधि है। एसएसएल एन्क्रिप्टेड संचार के लिए उद्योग मानक है और यह सुनिश्चित करता है कि इंटरनेट पर बैंक के साथ ग्राहक की बातचीत सुरक्षित है। ड्यूश बैंक एजी, भारत में, हम सिक्योर सॉकेट लेयर (एसएसएल) सत्र के एन्क्रिप्शन के लिए वेरीसाइन से १२८-बिट डिजिटल प्रमाणपत्र का उपयोग करते हैं। डेटा का यह एन्क्रिप्शन इंटरनेट के माध्यम से डेटा स्थानांतरित होने के दौरान छेड़छाड़ के खिलाफ मजबूत सुरक्षा प्रदान करता है।

आपको पृष्ठ के शीर्ष पर एक बंद लॉक आइकन दिखाई देगा।

वर्चुअल कीपैड सुविधा

वर्चुअल कीपैड आपके नियमित कीबोर्ड का एक ऑनलाइन प्रतिनिधित्व है। अपने पासवर्ड पर क्लिक करने के लिए अपने माउस का उपयोग करें। यह आपको दुर्भावनापूर्ण 'स्पाइवेयर' और 'ट्रोजन' प्रोग्राम से बचाता है जो कीस्ट्रोक्स को कैप्चर करने के लिए डिज़ाइन किए गए हैं। यदि आप कंप्यूटर की सुरक्षा के बारे में आश्वस्त नहीं हैं तो हम अनुशंसा करते हैं कि आप कंप्यूटर से लॉग इन करते समय वर्चुअल कीपैड का उपयोग करें। असुरक्षित वातावरण के उदाहरणों में साइबर कैफे या ऐसी मशीन शामिल है जहां एंटी-वायरस सॉफ़्टवेयर अपडेट नहीं किया गया है।

जबकि नियमित वर्चुअल कीपैड कुंजियों को गतिशील रूप से जोड़कर इसे प्राप्त करते हैं, इससे उपयोगकर्ताओं के लिए वर्णों को इनपुट करना मुश्किल हो जाता है। ड्यूश बैंक का वर्चुअल कीपैड चाबियों को इधर-उधर किए बिना पूरे कीपैड को गतिशील तरीके से घुमाता है, जिससे सुरक्षा और सुविधा दोनों प्राप्त होती है।

पासवर्ड सुरक्षा

पासवर्ड स्वचालित रूप से उत्पन्न होते हैं, पासवर्ड मेलर्स पर मुद्रित होते हैं, सील किए जाते हैं और मैन्युअल हस्तक्षेप के बिना आपके मेलिंग पते पर भेजे जाते हैं। सुरक्षा उद्देश्यों के लिए लॉगिन के लिए आवश्यक ग्राहक आईडी/ उपयोगकर्ता आईडी वाले किसी भी अन्य दस्तावेज़ के साथ पासवर्ड नहीं भेजे जाते हैं। आपके पासवर्ड को बैंक के सुरक्षित सिस्टम में हर समय पूरी तरह से गोपनीय रखा जाता है। कृपया ध्यान दें कि बैंक के कर्मचारियों के पास भी आपके पासवर्ड की जानकारी तक पहुंच नहीं है और किसी भी परिस्थिति में ऑनलाइन बैंकिंग पासवर्ड को बैंक कर्मचारियों सहित किसी के साथ साझा नहीं किया जाना चाहिए।

लेनदेन पासवर्ड 90 दिनों में समाप्त हो जाता है, जिसके बाद आपको डीबी ऑनलाइनबैंकिंग पर लॉगिन करने के लिए पासवर्ड बदलने के लिए कहा जाता है। कृपया ध्यान दें कि यदि आप मौजूदा लेनदेन पासवर्ड को नए में बदलते समय दर्ज करने में असमर्थ हैं, तो आपको पासवर्ड के नए सेट के लिए अनुरोध करना होगा।

यदि आपने 180 दिनों से अधिक समय तक डीबी ऑनलाइनबैंकिंग में लॉग इन नहीं किया है, तो डीबी ऑनलाइनबैंकिंग तक आपकी पहुंच स्वचालित रूप से निष्क्रिय हो जाती है। इसे सक्रिय करने के लिए कृपया हमारी फोन बैंकिंग टीम को 1860 266 6601# पर कॉल करें।

आप अपने सक्रिय डेबिट कार्ड नंबर का उपयोग करके तुरंत अपना आईपिन ऑनलाइन भी बना सकते हैं। ऑनलाइन आईपिन निर्माण के लिए हम आपको आपके पंजीकृत मोबाइल और ईमेल आईडी पर एक रैंडम एक्सेस कोड (आरएसी) और अद्वितीय संदर्भ संख्या (यूआरएन) भेजते हैं। तीन अमान्य प्रयासों के मामले में हम आपकी ऑनलाइन आईपिन सुविधा को ब्लॉक कर देंगे और उस पर एक एसएमएस/ ईमेल अलर्ट भेज देंगे।

फ़िशिंग हमले

'फ़िशिंग हमले' जाली कंपनी ई-मेल प्रेषक पते का उपयोग करके ई-मेल के माध्यम से गोपनीय ग्राहक पहुंच जानकारी प्राप्त करने का प्रयास है। इन हमलों में ग्राहक द्वारा ज्ञात और विश्वसनीय कंपनियों के जाली ई-मेल पते का उपयोग किया जाता है। ग्राहक को ई-मेल उत्तर द्वारा या जाली वेबसाइट पर जाने

वाले लिंक के माध्यम से गोपनीय खाता पहुंच जानकारी प्रदान करने के लिए कहा जाता है। तब ग्राहक की जानकारी के बिना जानकारी का दुरुपयोग किया जा सकता है।

ड्यूश बैंक कभी भी ई-मेल या एसएमएस के माध्यम से आपकी गोपनीय या व्यक्तिगत जानकारी (जैसे आपका खाता नंबर, डेबिट कार्ड नंबर, एटीएम पिन या ऑनलाइन बैंकिंग पासवर्ड) नहीं मांगेगा। साथ ही, आपको ड्यूश बैंक द्वारा भेजे गए किसी भी ईमेल में दिए गए लिंक से लॉगिन करने के लिए कभी नहीं कहा जाएगा। यदि आपको संदेह है कि ड्यूश बैंक से होने का दावा करने वाला कोई ईमेल धोखाधड़ी वाला है, तो कृपया तुरंत बैंक को इसकी सूचना दें।

अज्ञात स्रोत से आए ईमेल अटैचमेंट को खोलने से पहले हमेशा स्कैन करने की सलाह दी जाती है।

निष्क्रिय समय लॉग-आउट

यदि आप अपने डीबी ऑनलाइनबैंकिंग में लॉग इन करते हैं और सत्र को 8 मिनट के लिए निष्क्रिय छोड़ देते हैं, तो हम आपके खाते में अनधिकृत पहुंच से बचाने के लिए स्वचालित रूप से आपको सत्र से लॉग आउट कर देते हैं।

निष्क्रिय समय को ट्रैक करने में सहायता के लिए, आप सत्र समाप्ति टाइमर के लिए पृष्ठ के ऊपरी बाएं कोने को देख सकते हैं और तदनुसार अपने लेनदेन की योजना बना सकते हैं। यदि सत्र समाप्त हो गया है तो टाइमर आपको फिर से लॉगिन करने का संकेत देगा।

सुरक्षित बैंकिंग सुझाव

खो जाने या चोरी होने या कार्ड या पिन के अनधिकृत उपयोग के मामले में अपने ड्यूश बैंक डेबिट कार्ड को तुरंत ब्लॉक करें

— अपने पंजीकृत मोबाइल नंबर से 561615 पर "FRAUD" एसएमएस करें
— हमें reports.fraud@list.db.com पर ईमेल करें
— किसी धोखाधड़ी की ऑनलाइन रिपोर्ट करने के लिए यहां क्लिक करें
— हमें हमारे 24/ 7 फोनबैंकिंग नंबर "1860 266 6601" पर कॉल करें और विकल्प 1 चुनें
— हमें हमारे समर्पित टोल फ्री नंबर "1800 123 6601" पर कॉल करें।

*भारत से बाहर के ग्राहकों को +91 22 6601 6601 डायल करना होगा। मुंबई के ग्राहक 6601 6601 पर भी कॉल कर सऽकते हैं। कॉल शुल्क लागू है।