સુરક્ષિત ઓનલાઈન બેંકિંગ- સેક્યુરીટી ટિપ્સ

સુરક્ષિત બેંકિંગ

તમારા એકાઉન્ટને છેતરપિંડીથી સુરક્ષિત કરો

- ડિબી ઓનલાઈન બેંકિંગમાં લોગીન કરવા પર તમારું કૅસ્ટમર આઈડી/ યુઝર આઈડી અને પાસવર્ડ સ્ટોર કરવા માટે બ્રાઉઝર પર ઓટો સેવનો ઉપયોગ ન કરો.
- કૃપા કરીને તમારી સંપર્ક વિગતો ડોઇશ બેંક સાથે અપડેટ કરો જેથી કરીને તમે ટ્રાન્ઝેક્શન ઓથોરાઇઝેશન માટે વન ટાઇમ પાસવર્ડ મેળવી શકો. વન ટાઇમ પાસવર્ડ એ તમારી નોંધાયેલ સંપર્ક વિગતો પર મોકલવામાં આવેલ 6 અંકનો આંકડાકીય કોડ છે. તમારા લોગીન અને ટ્રાન્ઝેક્શન પાસવર્ડ ઉપરાંત આ પ્રમાણીકરણનું બીજું સ્તર છે.
- એન્ટી-વાયરસ સોફ્ટવેરને કોન્ફીગર કરો અને ખાતરી કરો કે સોફ્ટવેર તમારા કમ્પ્યુટર પર નિયમિતપણે અપગ્રેડ થાય છે.
- તમારા પીસી/ મોબાઇલમાં પાવર-ઓન/ એક્સેસ પાસવર્ડ, તમારા પીસી પર સ્ક્રીનસેવર પાસવર્ડ સેટ કરો, જેથી તમારી સંમતિ વિના તમારા પીસી/ મોબાઇલનો અન્ય કોઈ ઉપયોગ ન કરી શકે.
- કોઈપણ વેબસાઈટ પર અને ઈમેલમાં શંકાસ્પદ લિંક પર ક્લિક કરતી વખતે અને તમારા કમ્પ્યુટર પર અજાણ્યા અથવા અવિશ્વસનીય સોફ્ટવેર ઇન્સ્ટોલ કરતી વખતે અત્યંત સાવચેતી રાખો. એન્ટીવાયરસ સોફ્ટવેર, તમારા કી સ્ટ્રોકને લોગ કરતા માલવેર સામે પર્યાપ્ત નથી અને આમ તમારા પાસવર્ડ સાથે ચેડા કરી શકે છે.
- એક મજબૂત પાસવર્ડ બનાવો -
  - પાસવર્ડ આલ્ફા ન્યુમેરિક હોવા જોઈએ એટલે કે તેમાં અંકો અને અક્ષરો બંને હોવા જોઈએ
  - પાસવર્ડમાં ઓછામાં ઓછા 6 અને વધુમાં વધુ 28 અક્ષરો હોવા જોઈએ
  - પાસવર્ડ્સમાં સ્પેસ ન હોવી જોઈએ
  - !,*,.,),+,=,? જેવા વિશિષ્ટ અક્ષરો માન્ય છે
  - કૅસ્ટમર આઈડીમાંના બધા અક્ષરો તમારા પાસવર્ડમાં ન હોવા જોઈએ.
  - દા.ત. જો તમારું કૅસ્ટમર આઈડી 000011120 છે, તો abcd012 પાસવર્ડ માન્ય પાસવર્ડ નથી.
- તમારા પાસવર્ડ્સ યાદ રાખો. જો તમે તેમને લેખિતમાં રાખવાનું પસંદ કરો છો, તો ખાતરી કરો કે તમને તેને સુરક્ષિત જગ્યાએ રાખો છો.
- ઈન્ટરનેટ બેન્કિંગ પાસવર્ડ્સ (ઇપિન) કેસ સેન્સિટિવ હોય છે.
- ડોઇશ બેંકના સ્ટાફ સહિત કોઈપણને તમારા પાસવર્ડ્સ ક્યારેય જણાવશો નહીં. તમારો પાસવર્ડ પૂછતા કોઈપણ મેઈલનો ક્યારેય જવાબ ન આપો.
- કૃપા કરીને નોંધો કે ડોઇશ બેંક ક્યારેય તમારો પાસવર્ડ પૂછશે નહીં.
- નીચે મુજબ અનુમાન લગાવવામાં સરળ હોય તેવા પાસવર્ડ્સનો ઉપયોગ કરશો નહીં:
  - જન્મ તારીખો, મહિનાઓ અથવા વર્ષો

- ક્રમિક સંખ્યાઓ (દા.ત. 6789)
- નંબર કોમ્બિનેશન, જેનો અનુમાન સરળતાથી લગાવી શકાય (દા.ત. 1111)
- તમારા ટેલિફોન નંબરમાંથી કોઈ નંબર
- તે નંબરોના તે ક્રમમાં કે જે તમારા કોઈપણ કાર્ડ પર છાપવામાં આવ્યા હોય
- સરળતાથી સુલભ અન્ય વ્યક્તિગત ડેટા (દા.ત. ડ્રાઇવિંગ લાઇસન્સ, અથવા તમારી સાથે સરળતાથી જોડાયેલ અન્ય નંબરો)
- પરિવારના સભ્યો, પાળતુ પ્રાણીઓ અથવા શેરીઓના નામ.

— તમારું કૅસ્ટમર આઈડી અને પાસવર્ડ દાખલ કરતી વખતે કૃપા કરીને ખાતરી કરો કે બીજા લોકો તમારી સ્ક્રીન નથી જોતા અને પાછળથી તમારા પર નજર નથી રાખી રહ્યા.

— લોગીન અને ટ્રાન્ઝેક્શન માટે અલગ-અલગ પાસવર્ડનો ઉપયોગ કરવાની ભલામણ કરવામાં આવે છે, જેનાથી તમારી ઓનલાઈન બેંકિંગ એક્સેસની સુરક્ષા વધી શકે.

— બ્રાઉઝર પર હંમેશા URL ટાઈપ કરો (www.deutschebank.co.in અને લોગીન બટન પર ક્લિક કરો), જેથી ખાતરી થાય કે તમે ડોઇશ બેંકની સાચી સાઇટને જ એક્સેસ કરી રહ્યાં છો.

— db ઓનલાઈન બેંકિંગમાં લોગીન કરતી વખતે તમારી છેલ્લી લોગિન તારીખ અને સમય તપાસો. કોઈપણ દુરુપયોગને ટાળવા માટે સમયાંતરે તમારા પાસવર્ડ્સ બદલો.

— સાર્વજનિક અથવા અન્ય વ્યક્તિઓ દ્વારા વપરાતા કમ્પ્યુટર્સમાંથી ઑનલાઇન બેંકિંગ કરવાનું ટાળો. વાયરસથી સંક્રમિત કોમ્પ્યુટરમાંથી તમારા એકાઉન્ટને ક્યારેય એક્સેસ ન કરવું.

— ઓનલાઈન બેંકિંગ કરતી વખતે એકથી વધારે બ્રાઉઝર વિન્ડો ખોલશો નહીં.

— ટ્રાન્ઝેક્શન પૂર્ણ કરી લીધા પછી તરત જ ડિબી ઓનલાઈન બેંકિંગમાંથી લોગઆઉટ કરો. તે વિન્ડો બંધ કરવાની પણ ખાતરી કરો.

— તમારી ઑપરેટિંગ સિસ્ટમ પર 'ફાઇલ એન્ડ પ્રિન્ટિંગ શેરિંગ' ફીચરને અક્ષમ કરો.

— જો તમે તમારી પાસેથી વસૂલવામાં આવેલી રકમ વિશે તમને ખબર નથી, તો કૃપા કરીને તરત જ ડોઇશ બેંકને લેખિતમાં તેની જાણ કરો.

અન્ય કોઈ સમસ્યાના કિસ્સામાં, કૃપા કરીને અમારી 24/7 ફોન બેંકિંગ ટીમને 1860 266 6601# પર કૉલ કરો.

ભારત બહારના ગ્રાહકો +91 22 6601 6601 પર ફોન કરી શકે છે. મુંબઈના ગ્રાહકો 6601 6601 પર પણ ફોન કરી શકે છે. ફોન કરવા પર શુલ્ક લાગુ થાય છે.

ડિબી ઓનલાઈન બેંકિંગની સુરક્ષામાં સુધારો

— તમારા એકાઉન્ટને અનધિકૃત એક્સેસથી સુરક્ષિત કરવા માટે અમે ડિબી ઓનલાઈન બેંકિંગના સતત ઉપયોગના 60 મિનિટ પછી લોગીન પાસવર્ડ ફરીથી માન્ય કરવાનું શરુ કર્યું છે. આ સાથે, જો કોઈ સત્ર 60 મિનિટથી વધુ થઇ જાય, તો તમને ફરીથી લોગિન કરવા માટે કહેવામાં આવશે.

— ઉપરાંત, જો તમારું ડિબી ઓનલાઈન બેંકિંગ લોગીન થયેલ સત્ર 8 મિનિટથી વધુ સમય માટે નિષ્ક્રિય હોય, તો સિસ્ટમ આપમેળે તમને સત્રમાંથી લોગ આઉટ કરી દેશે. નિષ્ક્રિય સમયનો ટ્રૅક

રાખવા માટે, તમે પેજના ઉપરના ડાબા ખૂણા પરના ટાઈમરનો સંદર્ભ લઈ શકો છો અને તે મુજબ તમારા ટ્રાન્ઝેક્શનની યોજના બનાવી શકો છો.

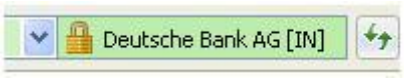
અમે તમારા ઓનલાઈન બેંકિંગ અનુભવને સુરક્ષિત કરવા માટે સુરક્ષાના બહુવિધ સ્તરો પ્રદાન કરીએ છીએ:

— તમારા ટ્રાન્ઝેક્શનને અન્ય લોકોથી સુરક્ષિત રાખવા માટે 256 બીટ ટીએલએસ એન્ક્રિપ્શન.
— કીસ્ટ્રોકને કેપ્ચર કરવા માટે બનાવવામાં આવેલ 'સ્પાયવેર' અને 'ટ્રોજન' પ્રોગ્રામ્સથી તમારું રક્ષણ કરવા માટે વર્ચ્યુઅલ કીપેડ.
— તમારા નાણાકીય ટ્રાન્ઝેક્શનને વધુ સુરક્ષા પૂરી પાડવા માટે પાસવર્ડના બે સ્તર.
— ઓટીપી એ હાલના લોગિન અને ટ્રાન્ઝેક્શન પાસવર્ડ ઓથેન્ટિકેશનના ઉપરાંત, સુરક્ષાનું વધારાનું સ્તર છે. તે 6 અંકનો આંકડાકીય કોડ છે જે તમને, તમારા દ્વારા સંવેદનશીલ/ નાણાકીય ટ્રાન્ઝેક્શન કરવાનો પ્રયાસ કરવા પર તમારી નોંધાયેલ સંપર્ક વિગતો પર મોકલવામાં આવે છે. નીચે દર્શાવેલ ટ્રાન્ઝેકશનને અધિકૃત કરવા માટે ઓટીપી આવશ્યક છે:
    — અન્ય બેંકોના લાભાર્થી બેંક ખાતાઓની નોંધણી
    — બિલની ચૂકવણી
    — ઈ-કોમર્સ ચૂકવણી
    — ડિબી ક્વિકપે
    — એનઇએફટી/ આરટીજીએસ (ટ્રાન્ઝેક્શન મૂલ્ય રૂ. 10,000 અને તેથી વધુ માટે)
    — અન્ય ડોઇશ બેંક ખાતાઓમાં ફંડ ટ્રાન્સફર
    — મોબાઈલ/ ઈમેલ આઈડી બદલવા માટે
    — પ્રોફાઇલમાં ફેરફાર વિશે ચેતવણી આપવા માટે
    — ટ્રાન્ઝેક્શન દરમિયાન જનરેટ થયેલો ઓટીપી ફક્ત તે ટ્રાન્ઝેક્શન માટે 5 મિનિટ સુધી માન્ય છે
— તમારા પાસવર્ડને સુરક્ષિત રાખવા માટે કડક પગલાંઓ.
— તમારા એકાઉન્ટને સુરક્ષિત રાખવા માટે અમે 60 મિનિટના સતત ઉપયોગ પછી લોગીન પાસવર્ડ વેલિડેશનનો વધારાનો સુરક્ષા સ્તર બનાવવામાં આવ્યો છે. તમારું લૉગિન સત્ર અનધિકૃત ઍક્સેસથી સુરક્ષિત છે, તેની ખાતરી કરો. જો તમે ડિબી ઓનલાઈન બેંકિંગને ઍક્સેસ કરવા માંગતા ન હોવ તો, તમે લોગઆઉટ બટન પર ક્લિક કરીને સત્ર સમાપ્ત કરી શકો છો.
— ડોઇશ બેંક, કમ્પ્યુટર્સ પર ટ્રોજન પ્રોગ્રામ્સનું નિરીક્ષણ કરે છે, જેનો ઉપયોગ ડિબી ઓનલાઈન બેંકિંગને ઍક્સેસ કરવા માટે થાય છે. જો કોમ્પ્યુટર પર કોઈ દૂષિત પ્રોગ્રામ જોવા મળે, તો ડોઇશ બેંક તે કોમ્પ્યુટરમાં લોગીન કરતા ગ્રાહકનું ઇન્ટરનેટ ઍક્સેસને અક્ષમ કરી દેશે. અમારી ફોન બેંકિંગ ટીમ તમને તેની જાણ કરશે.

સુરક્ષિત ડેટા ટ્રાન્સફર

એન્ક્રિપ્શન, એ અનધિકૃત પક્ષકારોને માહિતીને વાંચવાથી રોકવા માટે ટ્રાન્સમિશન માટે માહિતીને સ્ક્રૅમ્બલ કરવાની એક પદ્ધતિ છે. એસએસએલ એ એન્ક્રિપ્ટેડ કોમ્યુનિકેશન માટેનું ઇન્ડસ્ટ્રી સ્ટાન્ડર્ડ છે અને તે સુનિશ્ચિત

કરે છે કે ઇન્ટરનેટ પર બેંક સાથે ગ્રાહકની ક્રિયાપ્રતિક્રિયા સુરક્ષિત રહે છે. ડોઇશ બેંક એજી, ભારતમાં, અમે સિક્યોર સોકેટ્સ લેયર (એસએસએલ) સત્રના એન્ક્રિપ્શન માટે VeriSign ના 128-બીટ ડિજિટલ પ્રમાણપત્રનો ઉપયોગ કરીએ છીએ. ડેટાનું આ એન્ક્રિપ્શન, જ્યારે ડેટા ઈન્ટરનેટ દ્વારા આગળ વધી રહ્યો હોય ત્યારે છેડછાડ સામે મજબૂત સુરક્ષા પ્રદાન કરે છે.

તમને પેજની ઉપર એક 

ક્લોઝડ લૉક આયકન જોશો.

વર્ચ્યુઅલ કીપેડ ફીચર

વર્ચ્યુઅલ કીપેડ એ તમારા નિયમિત કીબોર્ડનું ઑનલાઇન પ્રતિનિધિત્વ છે. તમારા પાસવર્ડ પર ક્લિક કરવા માટે તમારા માઉસનો ઉપયોગ કરો. તે તમને કીસ્ટ્રોકને કેપ્ચર કરવા માટે બનાવવામાં આવેલ દૂષિત 'સ્પાયવેર' અને 'ટ્રોજન' પ્રોગ્રામ્સથી રક્ષણ આપે છે. જો તમને કોમ્પ્યુટરની સુરક્ષા અંગે વિશ્વાસ ન હોય તો તમે કમ્પ્યુટરથી લોગીન કરતી વખતે વર્ચ્યુઅલ કીપેડનો ઉપયોગ કરી શકો છો. અસુરક્ષિત વાતાવરણની પરિસ્થિતિમાં સાયબર કાફે અથવા એન્ટી-વાયરસ સોફ્ટવેર અપડેટ કરવામાં ન આવ્યું હોય તેવા મશીનનો સમાવેશ થાય છે.

જ્યારે નિયમિત વર્ચ્યુઅલ કીપેડમાં કીઝને ગતિશીલ રીતે જંબલ કરીને આ થાય છે અને આમ, વપરાશકર્તાઓ માટે અક્ષરો ઇનપુટ કરવું મુશ્કેલ બને છે. ડોઇશ બેંકનું વર્ચ્યુઅલ કીપેડ, આખા કીપેડને, કીઝને જમ્બલ કર્યા વિના ગતિશીલ રીતે જંબલ કરે છે, જેનાથી સુરક્ષા અને સગવડ બંને પ્રાપ્ત થાય છે.

પાસવર્ડ સુરક્ષા

પાસવર્ડ્સ આપમેળે જનરેટ થાય છે, પાસવર્ડ મેઇલર્સ પર છાપવામાં આવે છે, સીલ કરવામાં આવે છે અને મેન્યુઅલ હસ્તક્ષેપ વિના તમારા મેઇલિંગ એડ્રેસ પર મોકલવામાં આવે છે. સુરક્ષા હેતુઓ માટે લોગિન માટે જરૂરી કૅસ્ટમર આઇડી/ યુઝર આઇડી ધરાવતા અન્ય દસ્તાવેજો સાથે પાસવર્ડ મોકલવામાં આવતા નથી. બેંકની સેક્યુરીટી સિસ્ટમમાં તમારા પાસવર્ડ હંમેશા સંપૂર્ણ રીતે ગોપનીય રાખવામાં આવે છે. કૃપા કરીને યાદ રાખો, બેંકના કર્મચારીઓને પણ તમારા પાસવર્ડની માહિતીનું ઍક્સેસ હોતું નથી અને કોઈપણ સંજોગોમાં બેંક કર્મચારીઓ સહિત કોઈપણ સાથે ઓનલાઈન બેંકિંગ પાસવર્ડ શેર કરવો જોઈએ નહીં.

ટ્રાન્ઝેક્શન પાસવર્ડ 90 દિવસમાં સમાપ્ત થાય છે, જે પછી તમને db ઓનલાઇન બંકિગ પર લોગીન કરવા માટે પાસવર્ડ બદલવા માટે સંકેત આપવામાં આવે છે. કૃપા કરીને યાદ રાખો, જો તમે વર્તમાન ટ્રાન્ઝેક્શન પાસવર્ડને નવામાં બદલતી વખતે તમને વર્તમાન પાસવર્ડ યાદ ન હોય, તો તમારે પાસવર્ડના નવા સેટ માટે વિનંતી કરવી પડશે.

જો તમે 180 દિવસથી વધુ સમયથી ડિબી ઓનલાઈન બેંકીંગમાં લોગીન ન કર્યું હોય, તો ડિબી ઓનલાઈન બેંકીંગમાં તમારું ઍક્સેસ, આપમેળે ડી-એક્ટિવેટ થઈ જશે. તેને સક્રિય કરવા માટે કૃપા કરીને અમારી ફોન બેંકિંગ ટીમને 1860 266 6601# પર ફોન કરો.

તમે તમારા સક્રિય ડેબિટ કાર્ડ નંબરનો ઉપયોગ કરીને તરત જ તમારો આઈપીન ઑનલાઇન પણ બનાવી શકો છો. ઓનલાઈન આઈપીન બનાવવા માટે અમે તમને તમારા નોંધાયેલ મોબાઈલ અને ઈમેલ આઈડી પર રેન્ડમ એક્સેસ કોડ (આરએસી) અને યુનિક રેફરન્સ નંબર (યુઆરએન) મોકલીએ છીએ. ત્રણ અમાન્ય પ્રયાસો પર અમે તમારી ઓનલાઈન આઈપીન સુવિધાને બ્લોક કરી દેશું અને તમારા નંબર પર એસએમએસ/ ઈમેલ એલર્ટ મોકલી દેશું.

ફિશિંગ અટેક્સ

'ફિશિંગ અટેક્સ' એ બનાવટી કંપનીના ઈ-મેલ સેન્ડ્રા એડ્રેસનો ઉપયોગ કરીને ઈ-મેલ દ્વારા ગ્રાહકની ગુપ્ત માહિતી મેળવવાના પ્રયાસો છે. આ હુમલાઓમાં ગ્રાહકની જાણીતી અને વિશ્વાસપાત્ર કંપનીઓના બનાવટી ઈ-મેલ એડ્રેસનો ઉપયોગ કરવામાં આવે છે. ગ્રાહકને ઈ-મેલના જવાબ દ્વારા અથવા બનાવટી વેબસાઈટ તરફ દોરી જતી લિંક દ્વારા ગોપનીય એકાઉન્ટ એક્સેસ માહિતી પ્રદાન કરવાનું કહેવામાં આવે છે. પછી ગ્રાહકની જાણ વગર માહિતીનો દુરુપયોગ થઈ શકે છે.

ડોઇશ બેંક ક્યારેય તમારી ગોપનીય અથવા વ્યક્તિગત માહિતી (જેમ કે તમારો એકાઉન્ટ નંબર, ડેબિટ કાર્ડ નંબર, એટીએમ પિન અથવા ઓનલાઈન બેંકિંગ પાસવર્ડ), ઈ-મેલ અથવા એસએમએસ દ્વારા પૂછશે નહીં. ઉપરાંત, તમને ડોઇશ બેંક દ્વારા મોકલવામાં આવેલ કોઈપણ ઈમેઈલરમાં આપેલી લિંક પરથી ક્યારેય લોગીન કરવાનું કહેવામાં આવશે નહીં. જો તમને શંકા હોય કે ડોઇશ બેંકનો દાવો કરતો ઈમેલ કપટપૂર્ણ છે, તો કૃપા કરીને તરત જ બેંકને તેની જાણ કરો.

અજ્ઞાત સ્ત્રોતમાંથી ઈમેલ અટેચમેન્ટ ખોલતા પહેલા તેને સ્કેન કરવાની હંમેશા સલાહ આપવામાં આવે છે.

આઇડલ ટાઈમ લોગ આઉટ

જો તમે તમારા ડિબી ઓનલાઇન બેન્કિંગમાં લોગિન કરો છો અને સત્રને 8 મિનિટ માટે નિષ્ક્રિય છોડી દો છો, તો તમને તમારા એકાઉન્ટમાં અનધિકૃત ઍક્સેસ સામે રક્ષણ આપવા માટે આપમેળે સત્રમાંથી લોગ આઉટ કરી દેવામાં આવશે.

નિષ્ક્રિય સમયને ટ્રૅક કરવામાં મદદ કરવા માટે, તમે સેશન એક્સપાયરી ટાઈમર માટે પેજના ઉપરના ડાબા ખૂણામાં જોઈ શકો છો અને તે મુજબ તમારા ટ્રાન્ઝેક્શનની યોજના બનાવી શકો છો. જો સત્ર સમાપ્ત થઈ ગયું હોય, તો ટાઈમર તમને ફરીથી લૉગિન કરવા માટે સૂચવે છે.

સલામત બેંકિંગ માટેની ટિપ

કાર્ડ અથવા પિનનો અનધિકૃત ઉપયોગ અથવા ખોવાઈ જવા અથવા ચોરી થવાના કિસ્સામાં તરત જ તમારું ડોઇશ બેંક ડેબિટ કાર્ડ બ્લોક કરો

- તમારા નોંધાયેલ મોબાઈલ નંબર પરથી 561615 પર "ફ્રોડ" એસએમએસ કરો
- અમને report.fraud@list.db.com પર ઈમેલ કરો
- ઓનલાઇન છેતરપિંડીની જાણ કરવા માટે અહીં ક્લિક કરો
- અમને અમારા 24/7 ફોનબેંકિંગ નંબર "1860 266 6601*" પર ફોન કરો અને વિકલ્પ 1 પસંદ કરો
- અમને અમારા સમર્પિત ટોલ ફ્રી નંબર "1800 123 6601" પર ફોન કરો

* ભારત બહારના ગ્રાહકો +91 22 6601 6601 પર ફોન કરી શકે છે. મુંબઈના ગ્રાહકો 6601 6601 પર ફોન કરી શકે છે. ફોન કરવા માટે શુલ્ક લાગુ પડે છે.