

මෙම තිරය කියවීම සඳහා සහාය අවශ්‍ය ගනුදෙනුකරුවන්ට **Apple Play Store හි Kibo** යෙදුම හෝ **Android Play Store හි InstaReader** යෙදුම භාවිතා කළ හැකිය.

මාර්ගගත බැංකුකරණ ආරක්ෂක පියවර

- ජාතික සංවර්ධන බැංකුව පිළිබඳව, මාර්ගගත බැංකුකරණය සඳහා බහුවිධ ආරක්ෂක ස්ථර ක්‍රියාත්මක කර ඇති අතර මාර්ගගත වංචා වලින් ඔබව ආරක්ෂා කිරීම සඳහා එය අඛණ්ඩව වැඩිදියුණු කරමින් සිටී.

ආරක්ෂිත සැසි

- අපගේ URL ලිපිනය, ඔබව ආරක්ෂිත අඩවියකට පිවිස (logged in) ඇති බව තහවුරු කරනු ලබන <https://kibo.lk> සමඟ ආරම්භ වන බව ඔබට දිස්වනු ඇත.
- දකුණු කෙළවරේ ඇති ඉබ්බාගුරු (Padlock) සංකේතය පිළිගත් සමාගමක් විසින් නිකුත් කරන ලද ආරක්ෂක සහතිකයට සමාන වේ.
- ඔබේ දැනගැනීම සඳහා NDB Bank Online හි දක්වා ඇති අවසන් වරට ඇතුළත් වූ දිනය සහ වේලාව පිළිබඳව පරීක්ෂාකාරී වන්න.

සංකේතනය

- පරිගණකයෙන් පිටවීමට පෙර ඔබේ පුද්ගලික තොරතුරු වෙනත් කිසිවෙකුට කියවිය නොහැකි බව සහතික කිරීම සඳහා ඔබේ පුද්ගලික තොරතුරු සංකේතනය කිරීමට ආරක්ෂිත සොකට් ස්ථරය-SSL සංකේතන තාක්ෂණය ඔබේ මාර්ගගත බැංකු සැසිකාලය තුළ භාවිතා කරනු ලැබේ.

සැසි කාලය අවසන්වීම

- ඔබ NDB Bank Online වෙත පිවිස (logged in) සිටින අතරතුර යම් කාලයක් තුළ අක්‍රියව සිටී නම්, බලයෙන්ම ක්‍රියාකාරකම් වළක්වා ගැනීම සඳහා පද්ධතිය ස්වයංක්‍රීයව ඔබව ඉවත් කරයි (log out).

ස්වයංක්‍රීය අගුළු දැමීම

- වලංගු නොවන පිවිසීම (log in) උත්සාහයන් ගණනාවක් සිදුකළ අවස්ථාවකදී ඔබේ පරිශීලක හැඳුනුම්පත, පද්ධතිය විසින් අක්‍රිය හෝ අවහිර කරනු ලැබේ.
- නිසි හඳුනා ගැනීම සඳහා අනන්‍ය පරිශීලක හැඳුනුම්පතක් සහ මුරපදයක් ලබා දී ඇත.
- ඔබ විසින් ඇතුළත් කරන ලද පරිශීලක හැඳුනුම්පත සහ නිවැරදි මුරපදය ඔබව හඳුනාගෙන ඇත. ඔබ ඔබේ මුරපදය කිසිවෙකු සමඟ බෙදා නොගැනීම අත්‍යවශ්‍ය වේ.
- ගනුදෙනුකරුවෙකු ලෙස ඔබ වැදගත් කාර්යභාරයක් ඉටු කරමින් සිටී, ඔබ බැංකුව සමඟ මාර්ගගතව සිටින අතරතුර සුපරීක්ෂාකාරී වන ලෙස සහ ප්‍රවේශම් සහගත වන ලෙස ඔබෙන් ඉල්ලා සිටීමු.
- අනවසර පුද්ගලයෙකු ඔබේ ගිණුමට ප්‍රවේශ වීමේ අවස්ථාව අඩු කර ගැනීම සඳහා කරුණාකර පහත නිර්දේශ පිළිපදින්න.

නිවැරදි ආකාර NDB බැංකු මාර්ගගත ප්‍රවේශය

- ඔබේ බ්‍රවුසරයට නිවැරදි වෙබ් අඩවි ලිපිනය (<https://www.neosonline.ndbbank.com/>) ටයිප් කිරීමෙන් ඔබ සත්‍ය NDB බැංකු වෙබ් අඩවියට ප්‍රවේශ වන බවට වග බලා ගන්න.
- ආරක්ෂක සංඥාවන් සඳහා පරීක්ෂා කරන්න.
- සංවේදී තොරතුරු ඇතුළත් කිරීමට පෙර සත්‍යාපනය කරගැනීම මගින් ඔබ ආරක්ෂිත NDB බැංකු මාර්ගගත වෙබ් අඩවියේ සිටින බවට සහතික කරගන්න;
- වෙබ් අඩවි ලිපිනය [http:](http://) වෙනුවට [https:](https://) සමඟ ආරම්භ වේ:

ඔබේ මුරපදය ආරක්ෂා කරගැනීම

- බැංකුව විසින් ඔබට මුලින් නිකුත් කරන ලද මුරපදය, වෙනත් අයෙකුට අනුමාන කිරීමට අපහසු වන ආකාරයේ එකකට වහාම මාරු කරන්න.
- පහත සඳහන් ලෙස අනුගමනය කිරීමෙන් ප්‍රබල මුරපදයක් සාදාගන්න.
- අකුරු, අංක, කුඩා අකුරු සහ ලොකු අකුරු සංයෝජනයක් සහිත අවම වශයෙන් අක්ෂර අටක් තිබිය යුතුය.
- ඔබට මතක තබා ගැනීමට පහසු වූද අනෙක් අයට අනුමාන කිරීමට අපහසු වූද මුරපදයක් වීම වැදගත්ය.
- ඔබේ මුරපදය අනන්‍ය විය යුතු අතර විද්‍යුත් තැපෑල හෝ අන්තර්ජාල ප්‍රවේශය ලෙස වූ වෙනත් මාර්ගගත සේවාවන් වෙත ප්‍රවේශ වීම සඳහා භාවිත නොකළ යුතුය.
- මුරපදයක් තෝරාගැනීමේදී ශබ්ද කෝෂ වචන හෝ ඔබේ දරුවාගේ නම, සුරතලාගේ නම, ඔබේ උපන් දිනය වැනි හෝ පුද්ගලික තොරතුරු භාවිත කිරීමෙන් වළකින්න, මේවා වෙනත් කෙනෙකුට පහසුවෙන් අනුමාන කළ හැකිය.
- 12345678, abcdefgh වැනි අනුක්‍රමික අංක හෝ අකුරු හෝ ඔබේ යතුරුපුවරුවේ zxcvbnm වැනි යාබද අකුරු සංයෝජනයක් භාවිත කරමින් මුරපද නිර්මාණය නොකරන්න.
- බැංකු කාර්ය මණ්ඩලය ඇතුළු කිසිවෙකුට ඔබේ මුරපදය කිසි විටෙකත් හෙළි නොකරන්න, ඒවා කොතැනක හෝ සටහන්කර නොතබන්න. ඔබගේ මුරපදය අවදානමට ලක්ව ඇති බව ඔබ විශ්වාස කරන්නේ නම් වහාම මුරපදය වෙනස් කරන්න.
- ඔබගේ මුරපදය අවදානමට ලක්වීමේ අවදානම අවම කිරීම සඳහා ඔබගේ මුරපදය නීතිපතා වෙනස් කරන්න.
- ඔබ ඇතුළත් කරන ඔබගේ මාර්ගගත මුරපදය ඇතුළු දත්ත මතක තබා ගන්නා ඔබගේ බ්‍රවුසරයේ ස්වයංක්‍රීය සම්පූර්ණ කිරීමේ අංගය අක්‍රීය කරන්න. විස්තර සඳහා ඔබගේ බ්‍රවුසරයේ උදව් ශ්‍රිතය බලන්න. තවද, මගේ මුරපදය මතක තබා ගන්න යන විකල්පයෙන් බැහැරවන්න.

ආරක්ෂිත පිවිසුමක් (log in) භාවිත කිරීම

- අන්තර්ජාල කැලේවල මෙන් හවුල් පරිගණක හෝ පොදු පරිගණක, නොමිලයේ වන රැහැන් රහිත ප්‍රවේශ ස්ථාන ආදිය මගින් NDB බැංකු මාර්ගගතව ප්‍රවේශ වීමෙන් වළකින්න.
- පොදු පරිගණක භාවිත කරන විට ඔබේ මුරපදය වැනි සංවේදී තොරතුරු කිසි විටෙකත් වෙනස් නොකරන්න.
- ඔබේ පරිගණකය ආරක්ෂා කරන්න.
- ඔබ NDB බැංකු මාර්ගගතව භාවිත කරනු ලබන පරිගණකය වෙත කිසිවෙකුගේ අනවසර ප්‍රවේශයක් සිදුනොවී ඇති බව සහතික කර ගන්න.
- විශ්වාසදායක ප්‍රති-වයිරස නිෂ්පාදනයක් ස්ථාපනය කර එය නීතිපතා යාවත්කාලීන කර ඇති බව සහතික කරගන්න.
- ඔබේ මෙහෙයුම් පද්ධතිය සඳහා නවතම ආරක්ෂක පැටි (security patches) ලබා ගැනීමට ඔබේ පරිගණකය වින්‍යාස කරන්න.
- අන්තර්ජාලීය වැඩසටහන් සහ ආක්‍රමණයන් තත්‍ය කාලීනව හඳුනා ගැනීම සඳහා පුද්ගලික ෆයර්වෝල් එකක් භාවිත කරන්න.
- අන්තර්ජාලයෙන් හෝ විශ්වසනීයත්වයෙන් තොර මූලාශ්‍රවලින් නොමිලේ මෘදුකාංග බාගත නොකරන්න.

විද්‍යුත් තැපැල් සඳහා ආරක්ෂිත පියවර

- තතුබැම (phishing) ලෙස බොහෝ විට හඳුන්වනු ලබන මාර්ගගත අන්‍යායාචනා වංචාව සිදුවන්නේ වංචාකරුවන් විශ්වාසදායක ව්‍යාපාර ලෙස පෙනී සිටිමින් අහඹු විද්‍යුත් තැපැල් ලිපින දහස් ගණනකට විද්‍යුත් තැපැල් යවන විට, චේතර්මයක් බාගත කිරීමට හෝ ව්‍යාජ වෙබ් අඩවියකට ඇතුළු වී ඔබ රැවටීමට ලක්වී පුද්ගලික තොරතුරු ලබා දෙන විටය. එවැනි වංචාවකින් ඔබව ආරක්ෂා කර ගැනීමට.
- ඔබගේ මුරපදය, ක්‍රෙඩිට් කාඩ් විස්තර, ගිණුම් අංකය වැනි පුද්ගලික තොරතුරු ඉල්ලා සිටින විද්‍යුත් තැපෑලට ප්‍රතිචාර නොදක්වන්න.
- ඔබට එවැනි ඉල්ලීමක් ලැබුනහොත්, ප්‍රතිචාර දැක්වීමෙන් වළකින්න, වහාම බැංකුව වෙත දැනුම් දෙන්න.
- බැංකුව හා සම්බන්ධ වන විට, NDB බැංකු මාර්ගගතව ඇති Message to Bank මෙවලම පමණක් භාවිතා කරන්න.
- NDB බැංකු මාර්ගගත වෙබ් අඩවියට පිවිසීමට (log in) ඊමේල් හෝ තෙවන පාර්ශවීය වෙබ් අඩවිවල ඇතුළත් කර ඇති අධි සබැඳි මත ක්ලික් නොකරන්න.
- දුරකථනය භාවිත කරන විට ප්‍රවේශම්කාරී වන්න. දුරකථනයේ සිටින අතරතුර ව්‍යාජ කෙනෙකු ලෙස පෙනී සිටීම කෙනෙකුට පහසුය. විශේෂිත ගනුදෙනුකරුවෙකු පිළිබඳ පුද්ගලික තොරතුරු අවශ්‍ය කෙනෙකු හෝ ඔබේ පුද්ගලික ගිණුමක් සත්‍යාපනය කිරීමට අවශ්‍ය බව පවසන කෙනෙකු වේවා, ඔබට ඇමතුම්කරුගේ අන්‍යායාචනා ධනාත්මකව තහවුරු කළ නොහැකි නම් දුරකථනයෙන් තොරතුරු ලබා නොදෙන්න.

ඔබේ පරිගණක වෙත ප්‍රවේශය සීමා කිරීම

- ඇත්ත වශයෙන්ම, ඔබේ ව්‍යාපාරය තුළ සැරිසරන ඕනෑම කෙනෙකුට ප්‍රවේශ විය නොහැකි වන පරිදි ඔබේ පරිගණක ජාලය මුරපදයකින් ආරක්ෂා කළ යුතුය. කෙසේ වෙතත්, ඔබ අභ්‍යන්තර ජාල ප්‍රවේශ දුෂ්කරතා ද පරීක්ෂා කළ යුතුය. සියලුම සේවකයින්ට සංවේදී තොරතුරු අඩංගු විය හැකි යෙදුම් හෝ දත්ත සමුදායන් වෙත ප්‍රවේශය අවශ්‍යද? මුරපද මේවා ද ආරක්ෂා කරන අතර, ප්‍රවේශය අවශ්‍ය අයට පමණක් ලබා දෙන අතර එය අන්‍යායාචනා සොරකම් අඩු කිරීමට උපකාරී වේ.

හිටපු සේවකයින්ගේ සබඳතා වහාම විසන්ධි කිරීම

- සේවකයින් තවදුරටත් ඔබේ ව්‍යාපාරය සඳහා සේවය නොකරන විට, ඔබේ පරිගණක ජාලයට සහ සමාගමේ දත්ත වෙත ඔවුන්ගේ ප්‍රවේශය වහාම නවතා ඇති බවට ඔබ සහතික විය යුතුය.

වෙනත් ආරක්ෂක පියවර

- ඔබ අවසන් වරට NDB බැංකු මාර්ගගතව පිවිසුණු (logged in) දිනය සහ වේලාව සැමවිටම නිරීක්ෂණය කරන්න. ඔබට කිසියම් වෙනසක් අනාවරණය වේ නම්, වහාම ඔබේ මුරපදය නැවත සකසා බැංකුවට දැනුම් දෙන්න.
- ඔබේ ගිණුම් ප්‍රකාශන සහ බැංකු ශේෂය නීතිපතා පරීක්ෂා කර, කිසියම් සාවද්‍යතාවයක් හෝ නීති විරෝධී ක්‍රියාකාරකමක් අනාවරණය වුවහොත් වහාම බැංකුවට දැනුම් දෙන්න.
- මාර්ගගත බැංකු මෙහෙයුම් සිදු කරන අතරතුර වෙනත් වෙබ් අඩවිවලට සැරිසැරීමෙන් වළකින්න.
- මාර්ගගත මූල්‍ය ක්‍රියාකාරකම් සිදු කරන අතරතුර ඔබේ පරිගණකය කිසි විටෙකත් හුදකලා නොකරන්න.
- සැම සැසියකටම පසු, ඔබේ ගිණුම් තොරතුරු ඉවත් කිරීම සඳහා ඔබේ බ්‍රවුසරයේ cache සහ ඉතිහාසය හිස් කරන්න, විශේෂයෙන් ඔබ හවුල් පරිගණකයක් භාවිතා කරන්නේ නම් එය සිදුකරන්න.

ATM/CRM භාවිතය සඳහා පොදු ආරක්ෂක උපදෙස්

- උරහිසට ඉහළින් එබිකම්පාන පුද්ගලයන් (shoulder surfers) ගැන සැලකිලිමත් වන්න - ඔබ ටයිප් කරන විට ඔබේ PIN අංකය දෙස බැලීමට උත්සාහ කළ හැකි පුද්ගලයින්.
- ඔබේ ගනුදෙනුව සම්පූර්ණ වූ පසු, ATM හෝ CRM වෙතින් පිටවීමට පෙර වහාම ඔබේ කාඩ්පත සහ මුදල් ලබා ගන්න.
- ඔබේ කාඩ්පත නැතිවූ, සොරකම් කළ, හෝ යන්ත්‍රයේ සිරවූ අවස්ථාවකදී, අනිසි භාවිතය වළක්වා ගැනීම සඳහා වහාම බැංකුවට දැනුම් දෙන්න.
- ඔබේ ATM PIN අංකය මතක තබා ගන්න; එය ලියා නොතබන්න.
- උපන් දින, සංවත්සර වැනි පහසුවෙන් අනුමාන කළ හැකි අංක හෝ "1234" හෝ "0000" වැනි සරල රටා ඔබේ ඩෙබ්ට්/ක්‍රෙඩිට් කාඩ්පත් PIN අංකය ලෙස භාවිත කිරීමෙන් වළකින්න.
- අවදානම අවම කිරීම සඳහා ඔබේ PIN අංකය නිතිපතා වෙනස් කරන්න.
- බැංකු කාර්ය මණ්ඩලය ඇතුළු කිසිවෙකු සමඟ ඔබේ ATM PIN අංකය කිසි විටෙකත් බෙදා නොගන්න..
- විය හැකි අනිසි භාවිතය වැළැක්වීම සඳහා වෙනත් කිසිවෙකුට ඔබේ කාඩ්පත පාවිච්චි කිරීමට හෝ ඔබ වෙනුවෙන් ගනුදෙනු කිරීමට ඉඩ නොදෙන්න.
- ඔබ CRM එකක් හරහා මුදල් තැන්පතුවක්/බිල්පත් ගෙවීමක් සිදු කරන විට, තිරයේ ඇති තහවුරු කිරීම පරීක්ෂා කර රිසිට්පත ලබා ගැනීමෙන් ඔබේ ගිණුමට/බිල්කරුට තැන්පත් කළ මුදල බැර කර ඇති බව තහවුරු කරගන්න.