

இந்தத் திரையைப் படிக்க உதவி தேவைப்படும் வாடிக்கையாளர்கள் Apple Play Store இல் Kibo செயலி அல்லது Android Play Store இல் InstaReader செயலியைப் பயன்படுத்தலாம்.

ஒன்லைன் வங்கி தொடர்பான பாதுகாப்பு நடவடிக்கைகள்

- தேசிய அபிவிருத்தி வங்கி பிஎல்சி, ஒன்லைன் வங்கிக்கான பல அடுக்குப் பாதுகாப்புகளைச் செயல்படுத்தியுள்ளதுடன், ஒன்லைன் மோசடிகளில் இருந்து உங்களைப் பாதுகாப்பதற்கு, அதைத் தொடர்ந்து மேம்படுத்தி வருகிறது.

பாதுகாப்பான அமர்வுகள்

- எங்கள் URL முகவரி <https://www.nbdonline.com/> என்று ஆரம்பிப்பதனை நீங்கள் அவதானித்திருப்பீர்கள், இது நீங்கள் பாதுகாப்பான தளத்தில் உள்நுழைந்துள்ளீர்கள் என்பதை உறுதிப்படுத்துகிறது.
- வலது மூலையில் இருக்கும் Padlock () சின்னம் ஒரு புகழ்பெற்ற நிறுவனத்தால் வழங்கப்பட்ட பாதுகாப்பு சான்றிதழை ஒத்திருக்கிறது.
- உங்களது தகவலுக்கு, நீங்கள் NDB ஒன்லைன் வங்கிச் சேவையை இறுதியாகப் பயன்படுத்தியபோது காட்டப்பட்ட தேதி மற்றும் நேரம் குறித்து எச்சரிக்கையாக இருக்கவும்.

குறிமுறையாக்கம் (Encryption)

- பாதுகாப்பான சாக்கெட்ஸ் லேயர்-SSL குறிமுறையாக்கத் தொழில்நுட்பம் ஆனது உங்கள் தகவல்களை யாரும் அணுக முடியாது என்பதை உறுதி செய்வதற்காக உங்கள் ஒன்லைன் வங்கி அமர்வில் கணினியை விட்டு வெளியேறும் முன், உங்கள் தனிப்பட்ட தகவலை குறிமுறையாக்கம் செய்யப் பயன்படுத்தப்படுகிறது.

அமர்வு நேரம் நிறைவடைதல்

- நீங்கள் NDB ஆன்லைன் வங்கி சேவையில் உள்நுழைந்திருக்கும் போது, நீங்கள் ஒரு குறிப்பிட்ட காலத்திற்கு செயலற்ற நிலையில் இருந்தால், அங்கீகரிக்கப்படாத செயல்பாடுகளைத் தவிர்க்க, கணினி தானாகவே உங்களை வெளியேற்றும்.

தன்னியக்கமாக lock out ஆகுதல்

- தவறான உள்நுழைவு முயற்சிகளின் காரணமாக உங்கள் பயனர் அடையாளம்காட்டி(user ID) கணினியால் முடக்கப்படும் அல்லது தடுக்கப்படும்
- சரியான அடையாளத்திற்காக தனிப்பட்ட பயனர் அடையாள இலக்கம் மற்றும் கடவுச்சொல் கொடுக்கப்பட்டுள்ளது.
- நீங்கள் உள்ளீடு செய்ய வேண்டிய பயனர் அடையாள இலக்கம் மற்றும் சரியான கடவுச்சொல்லை இனம் கண்டுள்ளீர்கள். உங்கள் கடவுச்சொல்லை யாருடனும் பகிர்ந்து கொள்ளாமல் இருப்பது அவசியமாகும்.
- ஒரு வாடிக்கையாளராக நீங்கள் முக்கிய பங்காற்றுகிறீர்கள், வங்கியில் ஒன்லைனில் இருக்கும்போது விழிப்புடன் இருக்குமாறும் எச்சரிக்கையுடன் செயல்படுமாறும் கேட்டுக் கொள்ளப்படுகிறீர்கள்.

அங்கீகரிக்கப்படாத நபர் உங்கள் கணக்கை அணுகுவதற்கான வாய்ப்பைக் குறைக்க, பின்வரும் பரிந்துரைகளைப் பின்பற்றவும்.

NDB ஒன்லைன் வங்கிச் சேவையினை சரியான முறையில் அணுகுதல்

- உங்கள் இணைய உலாவியில் சரியான இணையதள முகவரியை (<https://www.neosonline.ndbbank.com/>) தட்டச்சு செய்வதன் மூலம் நீங்கள் உண்மையான NDB வங்கியின் இணையதளத்தை அணுகுவதை உறுதிசெய்யவும்.
- பாதுகாப்பு அறிகுறிகளைச் சரிபார்க்கவும்
- முக்கியமான தகவலை உள்ளிடுவதற்கு முன், நீங்கள் பாதுகாப்பான NDB ஒன்லைன் வங்கிச் சேவைக்கான இணையதளத்தில் இருப்பதை உறுதிசெய்யவும்;
- இணையதள முகவரி ஆனது <http://www.nbdonline.com/> என்பதை விட <https://www.nbdonline.com/> என்று தொடங்குகிறது.

உங்கள் கடவுச்சொல்லைப் பாதுகாத்திருங்கள்

- வங்கியால் உங்களுக்கு வழங்கப்பட்ட ஆரம்ப கடவுச்சொல்லை வேறொருவருக்கு யூதிக்க கடினமாக இருக்கும் வகையில் உடனடியாக மாற்றவும்.

- பின்வருவனவற்றைப் பின்பற்றுவதன் மூலம் வலுவான கடவுச்சொல்லை உருவாக்கவும்.
- எழுத்துக்கள், எண்கள், சிறிய எழுத்து மற்றும் பெரிய எழுத்து ஆகியவற்றின் கலவையுடன் குறைந்தது எட்டு எழுத்துக்கள்
- நீங்கள் எளிதாக நினைவில் வைத்துக் கொள்ளக்கூடியது, ஆனால் மற்றவர்கள் யூகிக்க கடினமாக உள்ளது.
- மின்னஞ்சல் அல்லது இணைய அணுகல் போன்ற பிற ஒன்லைன் சேவைகளை அணுகுவதற்குப் பயன்படுத்தப்பட்டதாக இருக்கக்கூடாது மற்றும் தனிப்பட்டதாகவும் இருத்தல்.
- கடவுச்சொல்லைத் தேர்ந்தெடுக்கும்போது உங்கள் குழந்தையின் பெயர், செல்லப்பிராணியின் பெயர், உங்கள் பிறந்த தேதி போன்றவற்றில் உள்ளவாறான தனிப்பட்ட தகவல்கள்; அல்லது அகராதி வார்த்தைகளைப் பயன்படுத்துவதைத் தவிர்க்கவும், ஏனெனில் இவற்றை பிற நபர்கள் எளிதாக யூகிக்க முடியும்.
- 12345678, abcdefgh போன்ற தொடர்ச்சியான எண்கள் அல்லது எழுத்துக்கள் அல்லது zxcvbnm போன்ற உங்கள் விசைப்பலகையில் அருகிலுள்ள எழுத்துக்களைப் பயன்படுத்தி கடவுச்சொற்களை உருவாக்க வேண்டாம்.
- உங்கள் கடவுச்சொல்லை வங்கி ஊழியர்கள் உட்பட யாருக்கும் தெரிவிக்காதீர்கள் மற்றும் அவற்றை எங்கும் பதிவு செய்யாதீர்கள். உங்கள் கடவுச்சொல் திருடப்பட்டதாக நீங்கள் நினைத்தால் உடனடியாக கடவுச்சொல்லை மாற்றவும்.
- உங்கள் கடவுச்சொல் திருடப்படும் அபாயத்தைக் குறைக்க உங்கள் கடவுச்சொல்லை அடிக்கடி மாற்றவும்.
- நீங்கள் உள்ளீடு செய்யும் ஒன்லைன் கடவுச்சொல் உள்ளிட்ட தரவை நினைவில் வைத்திருக்கும் உங்கள் உலாவியின் தானியங்கு முழுமை அம்சத்தை முடக்கவும், விவரங்களுக்கு உங்கள் உலாவியின் உதவி செயல்பாட்டைப் பார்க்கவும். என் கடவுச்சொல்லை நினைவில் கொள்ளுங்கள் என்ற விருப்பத்தையும் தவிர்க்கவும்.

பாதுகாப்பான உள்நுழைவைப் பயன்படுத்தவும்

- இணைய கஃபேக்கள், இலவச வயர்லெஸ் அணுகல் புள்ளிகள் போன்றவற்றில் பகிரப்பட்ட கணினிகள் அல்லது பொது கணினிகளில் இருந்து NDB ஒன்லைன் வங்கியை அணுகுவதைத் தவிர்க்கவும்.
- பொது கணினிகளைப் பயன்படுத்தும் போது உங்கள் கடவுச்சொல் போன்ற முக்கியமான விவரங்களை ஒருபோதும் மாற்ற வேண்டாம்.
- உங்கள் கணினியைப் பாதுகாக்கவும்.
- NDB ஒன்லைன் வங்கியை நீங்கள் பயன்படுத்தும் கணினியை நீங்கள் அங்கீகரிக்காமல் யாரும் அணுகவில்லை என்பதை உறுதிப்படுத்தவும்.
- நம்பகமான வைரஸ் எதிர்ப்பு மென்பொருளை நிறுவி, அது தொடர்ந்து புதுப்பிக்கப்படுவதை உறுதிசெய்யவும்.
- உங்கள் இயக்க முறைமைக்கான சமீபத்திய பாதுகாப்பு இணைப்புகளைப் பெற உங்கள் கணினியை கட்டமைக்கவும்.
- தீங்கிழைக்கும் செய்நிரல்கள் மற்றும் ஊடுருவல்களை நிகழ்நேரத்தில் கண்டறிய தனிப்பட்ட ஃபயர்வாலைப் பயன்படுத்தவும்.
- இலவச மென்பொருளை இணையத்தில் இருந்தோ அல்லது நம்பகமற்ற ஆதாரங்களில் இருந்தோ நிறுவ வேண்டாம்.

மின்னஞ்சல்களுக்கான முன்னெச்சரிக்கைகள்

- ஒன்லைன் அடையாள மோசடி ஆனது, பெரும்பாலும் ஃபிஷிங் எனப்படும், மோசடி செய்பவர்கள் நம்பகமான வணிகங்களைப் போல ஆள்மாறாட்டம் செய்து ஆயிரக்கணக்கான சீரற்ற மின்னஞ்சல் முகவரிகளுக்கு மின்னஞ்சல்களை அனுப்பும்போது, வைரலைப் பதிவிறக்கி உங்களை ஏமாற்றி அல்லது போலி இணையதளத்தில் கையொப்பமிட்டு தனிப்பட்ட தகவலை வழங்கும்போது நிகழ்கிறது. அத்தகைய மோசடியிலிருந்து உங்களைப் பாதுகாத்துக் கொள்தற்கு:

- உங்கள் கடவுச்சொல், கடனட்டை விவரங்கள், கணக்கு எண் போன்ற தனிப்பட்ட தகவல்களைக் கோரும் மின்னஞ்சல்களுக்கு பதிலளிக்க வேண்டாம்.
- அத்தகைய கோரிக்கையை நீங்கள் பெற்றால், பதிலளிப்பதைத் தவிர்த்து, உடனடியாக வங்கிக்குத் தெரிவிக்கவும்.
- வங்கியைத் தொடர்பு கொள்ளும்போது, NDB ஒன்லைன் வங்கியில் கிடைக்கும் Message to Bank கருவியை பிரத்தியேகமாகப் பயன்படுத்தவும்.
- NDB ஒன்லைன் வங்கி இணையதளத்தை அணுக மின்னஞ்சல்கள் அல்லது மூன்றாம் தரப்பு இணையதளங்களில் உட்பொதிக்கப்பட்ட மீத்தொடுப்புகளைக் (hyperlinks) சொடுக்க வேண்டாம்.
- தொலைபேசியைப் பயன்படுத்தும் போது எச்சரிக்கையுடன் பயன்படுத்தவும். தொலைபேசியில் பேசும் போது யாரோ ஒருவர் போல் நடிப்பது எளிது. ஒரு குறிப்பிட்ட வாடிக்கையாளரைப் பற்றிய தனிப்பட்ட தகவலை விரும்பும் ஒருவராக இருந்தாலும் அல்லது உங்கள் தனிப்பட்ட கணக்குகளில் ஒன்றை அங்கீகரிக்க வேண்டும் என்று கூறுபவர்களாக இருந்தாலும், அழைப்பாளரின் அடையாளத்தை நீங்கள் சாதகமாக சரிபார்க்க முடியாவிட்டால் தொலைபேசியில் தகவலை வழங்க வேண்டாம்.

உங்கள் கணினிகளுக்கான அணுகலைக் கட்டுப்படுத்துங்கள்

- நிச்சயமாக, உங்கள் கணினி இணைய வலையமைப்பினை கடவுச்சொல்லால் பாதுகாக்கப்பட வேண்டும், எனவே உங்கள் விடயங்களில் தலையிட முயல்பவர்கள் அதை இலகுவாக அணுக முடியாது. இருப்பினும், உள் வலையமைப்பு அணுகல் சிக்கல்களையும் நீங்கள் ஆராய வேண்டும். அனைத்து ஊழியர்களுக்கும் முக்கியமான தகவல்களைக் கொண்ட செயலிகள் அல்லது தரவுத்தளங்களுக்கான அணுகல் தேவையா? கடவுச்சொற்கள் இவற்றையும் பாதுகாக்கின்றன, மேலும் தேவைப்படுபவர்களுக்கு மட்டுமே அணுகல் வழங்கப்படுகிறது, இது அடையாள திருட்டை குறைக்க உதவுகிறது.

முன்னாள் ஊழியர்களை உடனடியாக துண்டித்து விடுங்கள்

- உங்கள் வணிகத்திற்காக சில பணியாளர்கள் இனி வேலை செய்யமாட்டார்கள் எனக் கருதும்போது, உங்கள் கணினி வலையமைப்பு மற்றும் நிறுவனத்தின் தரவுகளுக்கான அணுகல் உடனடியாக துண்டிக்கப்படுவதை நீங்கள் உறுதிசெய்ய வேண்டும்.

ஏனைய பாதுகாப்பு நடவடிக்கைகள்

- நீங்கள் கடைசியாக NDB ஒன்லைன் வங்கி சேவையில் உள்நுழைந்த தேதி மற்றும் நேரத்தை எப்போதும் கண்காணிக்கவும். நீங்கள் ஏதேனும் வேறுபாடுகள் இருப்பதாக உணர்ந்தால், உடனடியாக உங்கள் கடவுச்சொல்லை மீட்டமைப்பதுடன் வங்கிக்கும் தெரியப்படுத்துங்கள்.
- உங்கள் கணக்கு அறிக்கைகள் மற்றும் வங்கி இருப்புத் தொகையை தவறாமல் சரிபார்த்து, ஏதேனும் தவறுகள் அல்லது சட்டத்திற்குப் புறம்பான செயல்பாடுகளை நீங்கள் கண்டறிந்தால், உடனடியாக வங்கிக்குத் தெரியப்படுத்துங்கள்.
- ஒன்லைன் வங்கிச் செயல்பாடுகளை மேற்கொள்ளும் போது பிற இணையதளங்களுக்குச் செல்வதைத் தவிர்க்கவும்.
- ஒன்லைன் நிதிச் செயல்பாடுகளைச் செய்யும்போது உங்கள் கணினியைத் தனியாக விட்டுவிடாதீர்கள்.
- ஒவ்வொரு அமர்வுக்குப் பிறகும், உங்கள் கணக்குத் தகவலை அகற்ற, குறிப்பாக நீங்கள் பகிரப்பட்ட கணினியைப் பயன்படுத்தினால், உங்கள் உலாவியின் தற்காலிக சேமிப்பையும் வரலாற்றையும் அழிக்கவும்.

ஏடிஎம்/சிஆர்எம் பயன்பாட்டிற்கான பொதுப் பாதுகாப்புக் குறிப்புகள்

- உங்களை ஒளிந்திருந்து பார்ப்பவர்களைப் பற்றிக் கவனமாக இருங்கள் - உங்கள் தனிநபர் அடையாள எண்ணை(PIN) நீங்கள் தட்டச்சு செய்யும் போது அதைப் பார்க்க முயற்சிக்கும் நபர்கள்.

- உங்கள் பரிவர்த்தனை முடிந்ததும், ஏடிஎம் அல்லது சிஆர்எம் (ATM or CRM) இலிருந்து வெளியேறும் முன் உடனடியாக உங்கள் அட்டையைப் பணத்தையும் மீட்டெடுக்கவும்.
- உங்கள் அட்டை தொலைந்துவிட்டாலோ, திருடப்பட்டாலோ அல்லது இயந்திரத்தில் சிக்கியிருந்தாலோ, தவறாகப் பயன்படுத்தப்படுவதைத் தவிர்க்க உடனடியாக வங்கிக்குத் தெரிவிக்கவும்.
- உங்கள் ஏடிஎம் உங்கள் தனிநபர் அடையாள எண்ணை மனப்பாடம் செய்யுங்கள்; அதை எழுதி வைக்க வேண்டாம்.
- பிறந்தநாள், ஆண்டுவிழாக்கள் அல்லது "1234" அல்லது "0000" போன்ற எளிய வடிவங்களை உங்கள் டெபிட்/கடன் அட்டையின் தனிநபர் அடையாள எண்ணாக (PIN) வைத்திருப்பதைத் தவிர்க்கவும்.
- ஆபத்தைக் குறைக்க உங்கள் தனிநபர் அடையாள எண்ணை அடிக்கடி மாற்றவும்.
- உங்கள் ஏடிஎம் பின்னை வங்கி ஊழியர்கள் உட்பட யாருடனும் பகிர வேண்டாம்.
- தவறான பயன்பாட்டைத் தடுக்க, உங்கள் அட்டையைக் கையாள அல்லது உங்கள் சார்பாக பரிவர்த்தனைகளைச் செய்ய வேறு யாரையும் அனுமதிக்காதீர்கள்.
- நீங்கள் ஒரு சிஆர்எம் (CRM) மூலம் பண வைப்பு/கட்டணம் செலுத்துதலைச் செய்யும்போது, திரையில் உள்ள உறுதிப்படுத்தலைச் சரிபார்த்து, ரசீதைத் தக்கவைத்து, வைப்புச் செய்யப்பட்ட தொகை உங்கள் கணக்கு/கட்டணம் பெறுபவருக்கு வரவு வைக்கப்பட்டுள்ளதா என்பதை உறுதிப்படுத்தவும்.