எச் டி எஃப் சி பேங்க்

SECURE BANKING

இவற்றை பகிராதீர்கள்

ஓடிபி • கார்டு எண் • யூபிஐ பின் • வங்கி விவரங்கள் • கஸ்டமர் ஐடி & பாஸ்வேர்டு

ஃபிஷ்ஷிங் மற்றும் ஸ்மிஷிங் லிங்க்ஸ்

மோசடிகள்

- மோசடி செய்பவர்கள் தேர்டு பார்ட்டி இணையதளத்தை உருவாக்கி பலவிதமான மேடைகள் மூலமாக ஃபிஷ்ஷிங் லிங்க்ஸை அனுப்புகிறார்கள்.
- இந்த லிங்க் உங்களை போலி இணையதளத்திற்கு கொண்டு செல்லும், அங்கு உங்கள் வங்கி விரங்கள் கேட்கப்படும். அவ்வாறு தந்தால் மோசடி செய்பவர்கள் உங்கள் வங்கி விவரங்களை தமக்கு சாதகமாக பயன்படுத்திக் கொள்வார்கள்.

பாதுகாப்பு குறிப்புகள்

- நினைவிருக்கட்டும் எச்டிஎஃப்சி பணியாளர்கள் ஒரு போதும் உங்கள் விவரங்களை கேட்காமாட்டார்கள். சந்தேகம் இருந்தால் உங்கள் கார்டை தடை செய்ய பரிந்துரைப்பார்கள்.

விஷ்ஷிங் அழைப்புகள்

மோசடிகள்

- மோசடியாளர்கள் தம்மை வங்கிப் பணியாளர்கள் என்று கூறிக் கொண்டு மக்களின் நம்பிக்கையை பெற அவசர விஷயங்களை பேசி நடிப்பார்கள்.
- மோசடியாளர் உங்கள் நம்பிக்கையை பெற்ற உடன் அவர்கள் உங்களுக்கு உதவி செய்வதாக கூறி உங்கள் வங்கி விவரங்களை பெற்று மோசடி செய்வார்கள்.

பாதுகாப்பு குறிப்புகள்

- நினைவிருக்கட்டும் எச்டிஎஃப்சி பணியாளர்கள் ஒரு போதும் உங்கள் விவரங்களை கேட்காமாட்டார்கள். விஷ்ஷிங் மோசடியை தவிர்க்க உங்கள் கார்டை தடை செய்வதற்கும், உங்கள் பாஸ்வேர்டை அடிக்கடி மாற்றுவதற்கும் நாங்கள் பரிந்துரைக்கிறோம்

விற்பனை தளங்களை பயன்படுத்தி நடக்கும் மோசடிகள்

மோசடிகள்

- ஆன்லைன் விற்பனை தளங்களில் மோசடியாளர்கள் தம்மை வாங்குவபர்கள் என்று கூறிக்கொண்டு உங்கள் தயாரிப்புகளில் ஆர்வம் காட்டுவார்கள்.
- அவர்கள் உங்களுக்கு பணம் லெுத்துவதற்கு பதிலாக யூபிஐ ஆப்களின் மூலமாக பணம் கோருவார்கள். மேலும் உங்கள் கணக்கிலிருந்து பணம் எடுக்க ஒப்புதல் அளிக்க வற்புறுத்துவார்கள்.

பாதுகாப்பு குறிப்புகள்

- நீங்கள் மோசடி என்று சந்தேகித்தால் அங்கீகாரமற்ற பரிவர்த்தனை பற்றி உங்கள் நிதி நிறுவனத்திற்கு தெரிவிக்கவும். மேலும் நேஷனல் சைபர் கிரைம் ஹெல்ப்லைன் எண் 155260 வில் உங்கள் புகாரை பதிவு செய்யவும்.

போலி ஹெல்ப்லைன் மற்றும் ஸ்க்ரீன் ஷேரிங் ஆப்ஸ்

- இந்த காலத்தில் வாடிக்கையாளர்கள் வியாபாரத்திற்காக ஹெல்ப்லைன் எண்களை நாடுகிறார்கள். மோசடியாளர்கள் இந்த எண்களை மாற்றி அதை அழைப்பதற்கு வாடிக்கையாளர்களை ஊக்குவிக்கிறார்கள்.
- மோசடியாளர்கள் வங்கி அதிகாரிகள் போல நடித்து உங்கள் கருவியில் ஆப்பை டவுன்லோடு செய்ய சொல்லி பிறகு ஸ்க்ரீனை ஷேர் செய்ய சொல்லியோ அல்லது உங்கள் கார்டு விவரங்களை சரிபார்க்க சொல்லியோ உங்கள் கருவியை கட்டுப்படுத்துவார்கள்.
- அவர்கள் உண்மையானவர்கள் என்று நினைத்து நமது ரகசிய விவரங்களை சொல்லுவோம்.

மோசடிகள்

பாதுகாப்பு குறிப்புகள்

- நினைவிருக்கட்டும் எச்டிஎஃப்சி பணியாளர்கள் ஒரு போதும் உங்கள் விவரங்களை கேட்காமாட்டார்கள்.
- முன்பின் தெரியாதவர்களின் ஆப்பை டவுன் லோடு செய்யாதீர்கள். அவர்களிடம் உங்கள் ஸ்க்ரீனை ஷேர் செய்யாதீர்கள்.

சமூக ஊடங்களின் மூலம் ஆள் மாற்றாட்டம்

மோசடிகள்

- மோசடியாளர்கள் பிரபல சமூக ஊடகத் தளங்களில் போலி கணக்குகளை ஏற்படுத்தி மருத்துவக் கட்டணம் அல்லது பணம் செலுத்துமாறு கேட்கிறார்கல்.
- அவர்கள் காலப்போக்கில் உங்கள் நம்பிக்கையை பெற்று உங்கள் தனிப்பட்ட விவரங்களை பயன்படுத்தி உங்களை மிரட்டி பணம் பறிப்பார்கள்.

பாதுகாப்பு குறிப்புகள்

- எப்போதும் ஆன்லைன் அக்கவுண்டுகளின் உண்மையை தன்மையை சரிபார்க்க வேண்டும் என்று நினைவிருக்கட்டும். அவர்கள் ரகசிய தகவல்களை கேட்டால் எச்சரிக்கையாக இருங்கள்.
- மேலும் நேஷனல் சைபர் கிரைம் ஹெல்ப்லைன் எண் 155260 வில் உங்கள் புகாரை பதிவு செய்யவும்.

லாட்டரி மோசடி

மோசடிகள்

- மோசடியாளர்கள் நீங்கள் லாட்டரி ஜெயித்துள்ளீர்கள் என்று உங்களுக்கு மின்னஞ்சல் அனுப்பலாம் அல்லது உங்களை அழைக்கலாம். பணத்தை பெறுவதற்கு நீங்கள் உங்கள் வங்கிக் கணக்கு அல்லது கிரெடிட் கார்டு மூலம் உங்கள் அடையாளத்தை அவர்களுக்கு தரவேண்டும் என்று கேட்கலாம். இவ்வாறு உங்கள் விவரங்கள் பெறப்படும்.
- அவர்கள் லாட்டரி பணம்/சரக்கை அனுப்பி வைக்க ஷிப்பிங் கட்டணம், பரிசீலனைக் கட்டணம் மற்றும் இதர கட்டணங்களுக்காக முன்பணம் கேட்கலாம்.

பாதுகாப்பு குறிப்புகள்

- அழைப்புகள்/எஸ்எம்எஸ்கள்/மின்னஞ்சல்களுக்கு பதில் அளிக்காதீர்கள்.
- நீங்கள் சந்தேகித்தால் அது பற்றி உங்கள் வங்கி அல்லது கிரெடிட் கார்டு வழங்கியோருக்கு தெரிவித்து அசௌகரியத்தை தவிருங்கள்.

சேவையை விரிவுபடுத்துவதற்காக மோசடியாளர்களால் செய்யப்படும் போலிவிளம்பரங்கள்

மோசடிகள்

- மோசடியாளர்கள் வாடிக்கையாளர்களை கவருவதற்காக கவர்ச்சிகரான வங்கிச்சேவை தருவதாக கூறி போலி விளம்பரங்களை உருவாக்குகிறார்கள்.
- இந்த மின்னஞ்சல் முகவரிகள் பொதுவாக வாடிக்கையாளர்களுக்கு நம்பகத்தன்மையை உருவாக்க வங்கி அதிகாரிகள் பயன்படுத்தும் மின்னஞ்சல் முகவரியைப் போலவே இருக்கும்.
- இந்த சேவைகளுக்காக நீங்கள் மோசடியாளர்களை அணுகினால், அவர்கள் பரிசீலனை கத்டணம், விண்ணப்பக் கட்டணம் போன்றவற்றிற்காக முன்பணம் கேட்டு பெற்று, பணத்தை பட்டுவாடா செய்யாமல் மறைந்துவிடுவார்கள்.

பாதுகாப்பு குறிப்புகள்

- நினைவிருக்கட்டும் இம்மாதிரியான உரையாடல்கள் தவிருங்கள். உங்கள் வங்கியில் ரிலேஷன்ஷிப் மேனேஜரிடம் பேசி வங்கிச் சேவைகளை பெறுங்கள்.
- சந்தேகம் இருந்தால் பல கேள்விகளை கேட்கவேண்டும் என்று நாங்கள் பரிந்துரைக்கிறோம்.

ஆன்லைன் வேலை வாய்ப்பு மோசடி

மோசடிகள்

- மோசடியாளர்கள் அப்பாவி வாடிக்கையாளர்களை கவர்வதற்கு வேலை தேடும் பாலி இணையதளங்களை உருவாக்குகிறார்கள்.
- மோசடியாளர்கள் பிரபல நிறுவனங்களின் அதிகாரிகள் போல ஆள்மாறாட்டம் செய்து போலி நேர்காணல்களை செய்து தேர்வை உறுதி செய்கிறார்கள். பிறகு பாதிக்கப்பட்டவரிடம் பயிற்சிதிட்ட கட்டணம் அல்லது விண்ணப்ப கட்டணங்களை செலுத்துமாறு வற்புறுத்திறார்கள்.

பாதுகாப்பு குறிப்புகள்

- வேலை வாய்ப்பு இணையதளங்களின் உண்மைய தன்மையை சரிபார்க்குமாறு வாடிக்கையாளர்களை எச்டிஎஃபி வங்கி ஊக்குவிக்கிறது.
- அறிமுகமில்லா நிறுவனங்களிலிருந்து வரும் பொதுவான மின்னஞ்சல்களுக்கு பதில் அளிக்காதீர்கள். அது மோசடியாக இருக்கலாம்.

ஏடிஎம் கார்டு ஸ்கிம்மிங்

மோசடிகள்

- மோசடியாளர்கள் தம்மை சக வாடிக்கையாளராக கூறிக்கொண்டு அருகில்வந்து, நீங்கள் பின் நம்பரை என்டர் செய்யும்போது அதை பெறலாம்.
- இந்த தகவலை பயன்படுத்தி பிறகு டூப்ளிகேட் கார்டை உருவாக்கி வாடிக்கையாளரின் கணக்கிலிருந்து பணத்தை எடுக்கலாம்.

பாதுகாப்பு குறிப்புகள்

- ஏடிஎம்மை பயன்படுத்தும் முன்பு சந்தேகத்திற்குரிய நடவடிக்கையுள்ளதா என்று பார்க்குமாறு எச்டிஎஃப்சி வங்கி பரிந்துரைக்கிறது.

சிம் ஸ்வாப்

மோசடிகள்

- உங்கள் கணக்கின் பெரும்பாலன தகவல்கள் மற்றும் அங்கீகாரத்திற்காக உங்கள் மொபைல் எண் இணைக்கப்பட்டுள்ளது. எனவே மோசடியாளர்கள் உங்கள் சிம் கார்டை பெற்று அலல்து அதே மாதிரி போலி சிம் கார்டு வாங்கி அதில் ஓடிபியை பெற்று டிஜிடல் பரிவர்த்தனைகளை செய்வார்கள்.
- அவர்கள் பொதுவாக நெட்வொர்க் கம்பெனியிலிருந்து அழைப்பதாக வாடிக்கையாளரை தொடர்பு கொண்டு 3G அல்லது 4G அப்கிரேடு அல்லது சிம் மீது போனஸ் தருவதாக கூறி விவரங்களை பெறுவார்கள்.

பாதுகாப்பு குறிப்புகள்

- வாடிக்கையாளர்களின் மொபைலில் கணிசமான நேரத்திற்கு நெட்வொர்க் இல்லாமல் இருந்தால் சந்தேகப்பட வேண்டும் என்று எச்டிஎஃப்சி பேங்க் வாடிக்கையாளர்களை ஊக்குவிக்கிறது.
- உங்கள் மொபைல் ஆபரேட்டரிடம் பேசி டூப்ளிகேட் சிம் வழங்கப்படவில்லை என்பதை உறுதி செய்து கொள்ளவும்.

போலி ஆவணங்கள் மூலம் மோசடிக் கடன்கள்

மோசடிகள்

- மோசடியாளர்கள் போலி ஆவணங்களை பயன்படுத்தி நிதி நிறுவனங்களிலிருந்து எந்த ஒரு சேவையையும் பெறுவார்கள்.
- NBFC பணியாளர்களின் நம்பகத் தன்மையை சரிபார்க்காமல் KYC தொடர்பான அவணங்களை நிறுவனங்களுடன் பகிரும்போது இம்மாதிரி மோசடிகள் நடக்கலாம்.
- நிதி நிறுவனங்களிலிருந்து பலன்களை பெறுவதற்காக பாதிக்கப்பட்டவர்களின் அடையாள அட்டைகள், வங்கி கணக்கு போன்ற சுய விவரங்களை திருடி கொடுப்பதன் அடிப்படையில் மோசடிக் கடன்களுக்கு ஒப்புதல் அளிக்கப்படுகின்றன.

பாதுகாப்பு குறிப்புகள்

- உங்கள் சுய விவரங்களை பகிர்ந்துகொள்வதற்கு முன்பு NBFC பணியாளர்களின் நம்பகத்தன்மையை எப்போதும் உறுதி செய்து கொள்ள வேண்டும் என்று வாடிக்கையாளர்களுக்கு எச்டிஎஃப்சி வங்கி பரிந்துரைக்கிறது.
- அடையாள திருட்டை தவிர்க்க எப்போதும் உங்கள் அடையாள அட்டைகளை பத்திரமாக வைத்திருங்கள்.

உங்கள் ஆதார் ஓடிபி திருட்டு

மோசடிகள்

- ஆதார் அடிப்படையிலான ஓடிபி மூலம் டிஜிடல் கணக்குகளை தொடங்கலாம்.
- தேர்டு பார்ட்டி வெண்டார்களிடம் வாடிக்கையாளர்கல் தமது UIDAI OTP யை பகிர்ந்து கொள்ளும் நிகழ்வு பல முறை காணப்பட்டுள்ளது. எனவே இதன் உதவியுடன் மோசடியாளர்கள் போலி கணக்குகளை தொடங்குகிறார்கள்.

பாதுகாப்பு குறிப்புகள்

- நினைவிருக்கட்டும், சரிபார்க்கப்படா நிறுவப்னங்களுடன் உங்கள் ஆதார் ஓடிபியை பகிர்ந்து கொள்ளாதீர்கள்.
- எந்த ஒரு தகவலையும் பகிர்ந்து கொள்வதற்கு முன்பு அந்த நபரின் அடையாளதை சரிபாருங்கள்.

எச் டி எஃப் சி பேங்க்

INDIA'S No.1* BANK

SECURE BANKING

For more details,
visit HDFC Bank's Secure Banking Page
https://www.hdfcbank.com/personal/useful-links/security

*ரிடைல் லோன் புக் சைஸ் அடிப்படையில் (அடமானங்கள் தவிர).

ஆதாரம்: நிதி ஆண்டு 19-20 ஆண்டறிக்கை. டிசம்பர் 31, 2020 தேதிப்படி BSE புள்ளிவிவரம் அடிப்படையில் மார்க்கெட் கேப்பிடலைசேஷனில் நம்.1.