எச்சரிக்கையோடு இருங்கள் பாதுகாப்பாக வங்கி பணியை மேற்கொள்ளுங்கள்

பேங்கிங் த்யான் ஸே

உதவியால்

AXIS BANK

ஆக்ஸிஸ் பேங்க் வழங்கும் ஒரு வாடிக்கையாளர் சேவை முயற்சி

ஒப்புகை

ஆர்பிஐ ஓம்புட்ஸ்மென் (மும்பை) மகாராஷ்டிரா, கோவா அலுவலகம் வெளியிட்டுள்ள பண விஷயத்தில் மோசடிகள் செய்யப்படும் முறை பற்றிய ஒரு புத்தகத்தில் இருந்தும் மற்றும் இந்த விஷயத்தில் எங்களின் உள்வட்டார ஆராய்வுகள் சிலவற்றின் கருத்துக்கள் அடிப்படையிலும் இந்த ஆவணம் உருவாக்கப்பட்டுள்ளது.

முன்னுரை

வங்கி சேவை அமைப்பில் டிஜிட்டைசேஷன் வாடிக்கையாளர்களுக்கு அவர்களின் பண தேவைகளை எளிதாகவும் வேகமாகவும் பூர்த்தி செய்து கொள்ள பல புதிய வழிகளை உருவாக்கி உள்ளது. நேரில் வருவதை மற்றும் சமூக ரீதியாக தொடர்பு கொள்வதை இயன்ற வரை குறைவாக்கும் தற்போதைய சூழ்நிலை, எங்களையும் டிஜிட்டல் முறையில் பணிகளை மேற்கொள்ள ஊக்கப்படுத்தி உள்ளது.

டிஜிட்டல் பேங்கிங்கின் அதிகரிக்கும் வசதிகளால் நமக்கு மகிழ்ச்சியே என்றாலும், நாம் மிகவும் அதிகமாக சைபர்க்ரைம் மற்றும் வங்கி பணி மோசடிகளாலும் பாதிக்கப்படுகிறோம். பெரும்பாலான நேரங்களில் வாடிக்கையாளர்கள் அவர்களை அறியாமலேயே இதில் ஏமாற்றப்படுகிறார்கள் மற்றும் அவர்கள் கவனமாக இல்லாமல் இருந்தால் அவர்களுக்கு பண இழப்பும் ஏற்படுகிறது.

ஆக்ஸிஸ் பேங்கில், உங்கள் மீது அக்கறையுடன் நாங்கள் அவ்வப்போது பயன் உள்ள தகவல்களை உங்களுடன் பகிர்ந்து கொள்வதன் மூலம் உங்களை பாதுகாக்க உதவுகிறோம்.

இந்த ஆவணம் தற்போது பரவலாக எங்கும் நடைபெறும் சந்தேகத்திற்கு இடமான மற்றும் மோசடியான நடவடிக்கைகள் பற்றி ஒரு விழிப்புணர்வை உங்களுக்கு ஏற்படுத்துவதற்கான எங்களின் முயற்சி. எவ்வாறு இத்தகைய ஒரு செயலை நாம் அடையாளம் காண்பது மற்றும் நீங்கள் எந்தவிதமான முன்னெச்சரிக்கைகளை பின்பற்ற வேண்டும் மற்றும் இவ்வாறு நடந்தால் அது பற்றி நீங்கள் புகார் அளிப்பது எப்படி என்பது என்பதை நீங்கள் புரிந்து கொள்ள, மோசடி செய்யப்படும் சில முக்கிய விதங்கள் பற்றி நாங்கள் தகவல்களை தொகுத்துள்ளோம். எனவே, நீங்கள் எச்சரிக்கையாக இருந்தால் பண இழப்பு மற்றும் ஏமாற்றப்படும் வாய்ப்புகள் குறைந்து விடும்.

இந்த தகவல் உங்களுக்கு பயன் மிக்கதாக இருக்கும் என்று நம்புகிறோம் மற்றும் கவனத்துடன் வங்கி பணிகளை மேற்கொள்ளும்போது நீங்கள் தொடர்ந்து பாதுகாப்பான வங்கி சேவை அனுபவத்தை பெறலாம்.

பாதுகாப்பாக இருங்கள்!

இதோ சில பொதுவான முன்னெச்சரிக்கை குறிப்புக்கள் மற்றும் சிறப்பான செயல்பாடுகள்:

தவிர்த்து விடுங்கள்

- பாதுகாப்பற்ற இணையதளங்களுக்கு செல்வதை அல்லது உங்களுக்கு தெரியாத பிரவுசர்களை பயன்படுத்துதல்
- பொது கருவிகளில் பாஸ்வேர்டுகளை சேமித்து வைத்தல்
- பொதுவான அல்லது இலவசமான நெட்ஒர்க்குகளில் பணம் சம்பந்தமான/ இரகசியமான மின்னஞ்சல்களை தொடர்பு கொள்தல்
- சந்தேகத்திற்கு இடமாக தோண்றும் பாப் அப்கள், லிங்க்குகள் மற்றும் முன் பின் அறியாத இடங்களில் இருந்து வரும் மின்னஞ்சல்களை கிளிக் செய்தல்
- மின்னஞ்சல்களில் அல்லது முன்பின் அறியாத இணைய தளங்களில் பாதுகாப்பான இரகசியமான தகவல்களை அல்லது பாஸ்வேர்டுகளை ஸ்டோர் செய்து வைத்தல்
- சமூக ஊடகங்களில் உங்களுக்கு அறிமுகமற்ற நபர்களிடத்தில் தனிப்பட்ட தகவல்களை பகிர்ந்து கொள்தல்
- வங்கி பணிகள் மற்றும் இதர பரிவர்த்தனைகளுக்கு ஒரே பாஸ்வேர்டுகளை பயன்படுத்துதல்
- அறிமுகமற்ற அப்ளிகேஷன்கள் அல்லது சாஃப்ட்வேர்களை இன்ஸ்டால் செய்து பயன்படுத்துதல்
- அன்லாக் செய்யாமல் உங்கள் மொபைல் அல்லது இதர எலக்ட்ரானிக் கருவிகளை அல்லது ஆப்களை விட்டு வைத்தல்

ஒரு போதும் செய்யாதீர்கள்

- உங்கள் பின் நம்பரை (பெர்சனல் ஐடென்டிஃபிகேஷன் நம்பர்), பாஸ்வேர்டு, கிரெடிட் அல்லது டெபிட் கார்டு நம்பர்கள், சிவிவி, காசோலை புத்தகத்தின் நகல்கள், கேஒய்சி விபரங்களை யாருடனும் பகிர்ந்து கொள்ள கூடாது.
- முன் பின் தெரியாத கருவிகளில் முக்கியமான அல்லது இரகசியமான தகவல்களை ஸ்டோர் செய்யாதீர்கள்.

எப்போதுமே செய்யுங்கள்

- ஒரு வலுவான ஸ்க்ரீன் பாஸ்வேர்டு மூலம் உங்கள் போனை பாதுகாத்து கொள்ளுங்கள்
- இயன்றவரை உரித்தாகும்/கிடைக்கும் வசதிப்படி இரண்டு-கட்ட சரிபார்ப்பை பயன்படுத்துங்கள்
- பயன்படுத்திய உடனே இன்டர்நெட் வங்கி பணி தளத்தை லாக்அவுட் செய்யுங்கள்
- உங்கள் பயன்பாடு அடிப்படையில் உங்கள் கார்டு அல்லது கணக்கில் என்ஏபிள் அல்லது டிஸ்ஏபிள் அம்சத்தை பயன்படுத்துங்கள் மற்றும் பரிவர்த்தனை வரம்புகளை செட்-அப் செய்து கொள்ளுங்கள்
- பேடுலாக் அல்லது ஹெச்டிடிபிஎஸ் போன்ற செக்யூர்டு சைன்கள் உள்ளதா என்று பார்த்து இணையதளத்தின் பாதுகாப்பு நிலையை சரிபாருங்கள்
- ஆன்லைனில் பணம் செலுத்த பாதுகாப்பான பேமெண்ட் கேட்வேக்களைப் பயன்படுத்துங்கள்
- வலுவான பாஸ்வேர்டுகளை பயன்படுத்துங்கள். இவை ஆல்ஃபாநியுமெரிக் மற்றும் ஸ்பெஷல் கேரக்டர்கள் இரண்டின் சேர்க்கையாக இருப்பது அவசியம் மற்றும் அவ்வப்போது பாஸ்வேர்டுகளை மாற்றிக் கொள்ள வேண்டும்
- பொது கருவிகளில் வர்ச்சுவல் கீபோர்டு பயன்படுத்துங்கள். ஏனெனில் காம்ப்ரமைஸ்டு கருவிகள், கீபோர்டு மூலம் கீஸ்ட்ரோக்குகளை பற்றி தெரிந்து கொள்ள முடியும்.
- உங்கள் கம்ப்யூட்டர்களில் ஆன்டிவைரஸ் மற்றும் ஆன்டி-ஸ்பைவேர் பொருத்துங்கள் மற்றும் அவற்றை முறையாகப் பராமரியுங்கள் மற்றும் இயன்றபோதெல்லாம் அப்டேட்களை இன்ஸ்டால் செய்யுங்கள்
- பயன்படுத்தும் முன் எந்த யுஎஸ்பி டிரைவ்களையும் / ஸ்டோரேஜ் டிவைஸ்களையும் ஸ்கேன் செய்யுங்கள்
- ஒரு பாஸ்வேர்டு மூலம் உங்கள் மொபைல் ஆப்களை பாதுகாத்து கொள்ளுங்கள் அல்லது மொபைல் போன்களில் ஹிடன் ஸ்பேஸ் அம்சம் பயன்படுத்தி யாரும் பார்க்காதபடி அவற்றை மறைத்துக் கொள்ளுங்கள்.

#BankingDhyaanSe

ஆன்லைன் / இணையதள மோசடிகள் பற்றி (1)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

ஆன்லைன் பிஷிங்

இது எப்படி செய்யப்படுகிறது

- மோசடிக்காரர்கள் வங்கியின் அசல் இணையதளம் போலவே தோன்றும் ஒரு இணையதளத்தை உருவாக்குகிறார்கள்
- இந்த இணையதள லிங்க்குகள் எஸ்எம்எஸ், சோஷியல் மீடியா, மின்னஞ்சல் மூலம் அனைவருக்கும் அனுப்பப்படும்
- இந்த லிங்க்குகள் அசல் இணையதளம் போலவே ஏமாற்றும் தோற்றத்தில் இருக்கும். எனவே, நீங்கள் லிங்க்கை மட்டும் பார்த்து விபரமான யுஆர்எல்-ஐ பார்க்காமல் உங்களின் முக்கிய தகவல்களை அல்லது முக்கியமான மற்றும் இரகசிய தகவல்களை என்டர் செய்து விடும் வாய்ப்பு உண்டு.
- நீங்கள் இந்த இணையதளங்களில் உங்களின் முக்கிய தகவல்களை என்டர் செய்யும்போது அவை பிறரால் தெரிந்து கொள்ளப்பட்டு மோசடிக்காரர்களால் தவறாக பயன்படுத்தப்படுகிறது.

பாதுகாப்பு குறிப்புகள்

- அசல் போலவே தோண்றினாலும் உங்களுக்கு தெரியாத லிங்க்குகளை தவிர்த்து விடுங்கள்
- பணம் சம்பந்தமான தகவல்களை என்டர் செய்யும்போது இணையதள விபரங்களை சரிபாருங்கள்

ஆன்லைன் மோசடிகள்

இது எப்படி செய்யப்படுகிறது

- மோசடிக்காரர்கள் ஆன்லைனில், இகாமர்ஸ் ப்ளாட் ஃபார்ம்களில் வாங்குபவர்கள்/விற்பனை செய்பவர்கள் போல நடிப்பது வழக்கம்.
- அவர்கள் உங்கள் தயாரிப்பின் மீது ஆர்வம் காட்டுவார்கள் அல்லது அதிக தள்ளுபடிகள் அல்லது ஊக்கத் தொகைகள் மூலம் அவர்களிடம் இருந்து ஏதேனும் வாங்குமாறு உங்களை மயக்குவார்கள்.
- இந்த விஷயத்தில் எந்தவித பணமும் செலுத்தாமல் அவர்கள் உங்களை யுபிஐ ரிக்வெஸ்டு மணி-ஐ பூர்த்தி செய்யுமாறு மயக்குவார்கள். இதன் மூலம் உங்கள் வங்கி கணக்கில் இருந்து பணத்தை எடுப்பதற்கு முயற்சி செய்வார்கள்.

பாதுகாப்பு குறிப்புகள்

- ஆன்லைன் தயாரிப்புகளுக்காக பண பரிவர்த்தனை செய்யும்போது கவனமாக இருங்கள்
- பணம் பெறுவதற்கு உங்களின் பின் நம்பரை அல்லது பாஸ்வேர்டை என்டர் செய்யுமாறு உங்களிடம் யாரும் ஒருபோதும் கூறக் கூடாது.

ஆன்லைன் / இணையதள மோசடிகள் பற்றி (2)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

சந்தேகத்திற்கு இடமான செர்ச் இன்ஜின் முடிவுகள்

இது எப்படி செய்யப்படுகிறது

- மோசடிக்காரர்கள் நிறுவனங்களின் கஸ்டமர்கேர் கோஆர்டினேட்களை மாற்றி அமைத்து செர்ச் இன்ஜின் ஆப்டிமைசேஷன் (எஸ்இஒ) வை பயன்படுத்தி அவர்களின் போலியான நம்பரை சோஷியல் மீடியா தளங்களில் செர்ச் ரிசல்ட்களில் அனைத்துக்கும் மேற்பகுதியில் வருமாறு செய்து விடுவார்கள்.
- நீங்கள் உங்கள் வங்கி அல்லது இதர பணம் சம்பந்தமான தகவல்/ அமைப்புக்கள் பற்றி கஸ்டமர் கேர் கான்டாக்ட் விபரங்களை ஆன்லைனில் தேடும்போது, தவறுதலாக இத்தகைய சரிபார்க்கப்படாத/போலி எண்களை அசல் என்று நினைத்து தொடர்பு கொள்ள நேரிட்டு விடலாம்.
- இதன் காரணமாக நீங்கள் உங்களின் சொந்த அல்லது இரகசிய மற்றும் பணம் சம்பந்தமான தகவல்களை இவர்களிடம் தெரிவித்து அதன் மூலம் மோசடியில் சிக்கி கொள்ள நேரிடும்.

பாதுகாப்பு குறிப்புகள்

- செர்ச் இன்ஜினில் கஸ்டமர் கேர் தொடர்பு விபரங்களை தேடுவதை தவிர்த்து விடுங்கள். ஏனெனில் மக்களை ஏமாற்றுவதற்கு மோசடிக்காரர்களால் அவை போலியாக உருவாக்கப்பட்டிருக்கலாம்.
- எப்போதுமே உண்மையான தொடர்பு விபரங்களை பெற வங்கிகளின்/ நிறுவனங்களின் அதிகாரப் பூர்வமான இணையதளங்களை பாருங்கள்.

ஸ்க்ரீன் ஷேரிங்/ரிமோட் தொடர்பு

இது எவ்வாறு செய்யப்படுகிறது

- மோசடியாளர்கள் ஸ்க்ரீன் ஷேரிங் ஆப்களை டவுண்லோட் செய்யும்படி உங்களை தூண்டி, உங்கள் சொந்த தகவல் மற்றும் பணம் சம்பந்தமான தகவல்களை உங்களின் லேப்டாப்/மொபைல் கருவிகளை அணுகி பெற முடியும். அதன் பின்னர் அவர்கள் உங்களின் பேங்கிங் மற்றும் பேமெண்ட் ஆப்கள் மூலம் எதற்காகவும் பணம் செலுத்த முடியும்.

பாதுகாப்பு குறிப்புகள்

- எந்த ஒரு முன் பின் தெரியாத நபர்களாலும் பரிந்துரைக்கப்படும் ஸ்க்ரீன் ஷேரிங் ஆப்களை டவுன்லோடு செய்யாதீர்கள்
- எந்த ஒரு பேங்கிங் அல்லது பைனான்ஸியல் ஆப் அல்லது இணையதளத்தில் லாகிங் செய்யும் முன்பு ஏதேனும் ஸ்க்ரீன் ஷேரிங் அப்ளிகேஷனை முதலில் டிஆக்டிவேட் செய்வதை உறுதி செய்து கொள்ளுங்கள்.

ஆன் கால்/மொபைல் மோசடிகள் பற்றி (1)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

விஷிங் அழைப்புகள்

இது எவ்வாறு செய்யப்படுகிறது

- மோசடி செய்பவர்கள் தொலைபேசி அழைப்பு/சோஷியல் மீடியா மூலம் அவர்களை வங்கி அதிகாரிகள் போல காட்டிக் கொண்டு வாடிக்கையாளர்களை தொடர்பு கொள்வார்கள். உங்கள் வங்கியின் கட்டணமற்ற எண் அல்லது கஸ்டமர் கேர் நம்பரிலிருந்து தொடர்பு கொள்வது போல் நடிப்பார்கள்.
- இவ்வாறு அழைப்பவர் வாடிக்கையாளரிடம் வாடிக்கையாளரின் இரகசிய விபரங்களை அல்லது ஓடிபியை பகிர்ந்து கொள்ளும்படி வலியுறுத்து வார்கள் மற்றும் முயற்சிப்பார்கள். இதற்காக அவர்கள் உங்களின் வங்கி சேவைகள் உடனடியாக முடக்கப்படும் என்றும் கேஒய்சி பூர்த்தி செய்யப்படவில்லை என்றும் கணக்கு / கார்டு கணக்கு முதலியவை முடிக்கப்படும் என்றும் பல அவசர நிலை காரணங்களை குறிப்பிட்டு வலியுறுத்துவார்கள்.
- அதன் பின், அவர்கள் நீங்கள் அளிக்கும் தகவல்களை பயன்படுத்தி உங்கள் கணக்கில் மோசடி நடவடிக்கைகளை செய்து விடலாம்.

பாதுகாப்பு குறிப்புகள்

- வங்கியோ/ ஏதேனும் அசல் அமைப்போ உங்களிடம் பயனாளியின் பெயர், பாஸ்வேர்டு, கார்டு விபரங்கள், பின் நம்பர், சிவிவி, ஒடிபி முதலிய எந்த இரகசிய தகவல்களையும் ஒருபோதும் கேட்காது.

மொபைல் ஆப் மோசடிகள்

இது எப்படி செய்யப்படுகிறது

- உங்கள் மொபைல், லேப்டாப் அல்லது டெஸ்க்டாப்பில் சரியானதா என்று அறியப்படாத ஆப்=ஐ டவுண்லோட் செய்யுமாறு உங்களிடம் தந்திரமாகப் பேசி மயக்குவார்கள்.
- இந்த ஆப்களின் லிங்க்குகள் எஸ்எம்எஸ், சோஷியல் மீடியா ப்ளாட் ஃபார்கள் முதலியவை மூலம் பகிர்ந்து கொள்ளப்பட்டு புரமோட் செய்யப்படும்.
- இவை மோசடியான அப்ளிகேஷன்கள். இதன் மூலம் மோசடிக்காரர்கள் உங்கள் கருவியில் /கம்யூட்டரில் உள்ள முழு தகவல்களையும் தொடர்பு கொள்ள முடியும்.

பாதுகாப்பு குறிப்புகள்

- சரியா என்று அறியப்படாத/முன்பின் தெரியாத இடங்களில் இருந்து ஒரு போதும் அப்ளிகேஷனை டவுண்லோட் செய்யாதீர்கள்
- முன்பின் தெரியாத இடங்களில் இருந்து வரும் எஸ்எம்எஸ் / மின்னஞ்சல்களை டெலிட் செய்து விடுங்கள். ஏனெனில் உங்களை அறியாமலேயே நீங்கள் டவுண்லோடு லிங்க்-ல் அதை கிளிக் செய்வதை தவிர்த்து விடலாம்.

ஆன் கால்/மொபைல் மோசடிகள் பற்றி (2)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

ஓடிபி அடிப்படையிலான மோசடி

இது எப்படி செய்யப்படுகிறது

- வங்கி கடன்களை வழங்குவதாகவோ அல்லது கடன் வரம்பை அதிகரிப்பதாகவோ காட்டிக்கொண்டு மோசடி செய்பவரிடமிருந்து நீங்கள் எஸ்எம்எஸ் ஒன்று உங்களுக்கு அனுப்பப்படும் மற்றும் செய்தியில் குறிப்பிடப்பட்டுள்ள எண்ணைத் தொடர்புகொள்ளும்படி உங்களிடம் அவர் கூறுவார்.
- நீங்கள் அந்த எண்ணை அழைக்கும் போது, சில படிவங்களை (ஆன்லைனிலும் கூட) பூர்த்தி செய்யும்படி கேட்பார்கள். அவற்றில் உங்களின் பண விபரங்கள் கொடுக்கப்படும்போது, அவர்கள் ஓடிபி அல்லது பின் நம்பர் விவரங்களை பகிர்ந்து கொள்ளும்படி உங்களை சம்மதிக்க வைப்பார்கள். நீங்கள் அவற்றை பகிர்ந்தால், உங்களின் பணத்தை இழப்பீர்கள்.

பாதுகாப்பு குறிப்புகள்

- யாருடனும் எந்த விதத்திலும் உங்களின் ஓடிபி, பின் நம்பர் அல்லது சொந்த தகவல் விபரங்களை பகிர்ந்து கொள்ளாதீர்கள்.
- உங்களுக்கு தெரியாமல் எந்த ஒடிபியும் உருவாக்கப்படவில்லை என்பதை உறுதி செய்ய உங்களின் எஸ்எம்எஸ் / மின்னஞ்சல்களை அவ்வப்போது சரி பாருங்கள்.

ஜூஸ் ஜேக்கிங்

இது எவ்வாறு செய்யப்படுகிறது

- ஜூஸ் ஜேக்கிங் என்பது ஒரு விதமான சைபர் திருட்டு முறை. இதில் உங்கள் மொபைல் ஏதேனும் அறிமுகமற்ற / சரிபார்க்கப்படாத சார்ஜிங் போர்ட்கள், சில அறிமுகமற்ற ஆப்கள் / மால்வேர் உடன் இணைக்கப்படுகிறது மற்றும் இது உங்கள் கருவியில் இன்ஸ்டால் செய்யப்பட்டு அதன் மூலம் முக்கிய தகவல்கள், மின்னஞ்சல்கள், எஸ்எம்எஸ் அல்லது நீங்கள் சேமித்து வைத்திருக்கும் பாஸ்வர்டுகளை மோசடிக்காரர்கள் திருட அவர்களுக்கு உதவுகிறது.

பாதுகாப்பு குறிப்புகள்

- எப்போதுமே பொதுவான/முன்பின் அறியாத போர்ட்களை/கேபிள்களை பயன்படுத்துவதை தவிர்த்து விடுங்கள்

ஆன் கால்/மொபைல் மோசடிகள் பற்றி (3)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

சிம் ஸ்வாப் மோசடிகள்

இது எவ்வாறு செய்யப்படுகிறது

- உங்களின் கணக்கு விபரங்கள் மற்றும் அங்கீகார நிலை போன்றவை உங்களின் பதிவு செய்யப்பட்ட மொபைல் நம்பர் உடன் இணைக்கப்படுகின்றன. மோசடிக்காரர்கள் உங்கள் நம்பருக்காக ஒரு புதிய சிம் கார்டு மாற்றறிப் பெறுவதன் மூலம் பணம் சம்பந்தமான பரிவர்த்தனைகளை செய்ய ஓடிபி மற்றும் தேவைப்படும் அலெர்ட்களை பெற்று மோசடி செய்ய முடியும்.
- மோசடியாளர் உங்கள் மொபைல் ஆபரேட்டரின் ரீடெய்ல் அவுட்லெட்டுக்கு சென்று ஒரு போலி ஐடி சான்று உடன் நீங்கள்தான் வந்திருப்பதாக காட்டிக் கொண்டு உங்களின் அசல் சிம்-ஐ ப்ளாக் செய்து உங்கள் மொபைல் நம்பருக்காக ஒரு புதிய சிம்-ஐ பெற்றுக் கொள்வார்.
- அதேபோல அவர்கள் உங்கள் ஆபரேட்டர் மூலம் உங்களுக்கு ஒரு எஸ்எம்எஸ் அனுப்பி உங்கள் சிம் கார்டை அப்கிரேடு செய்து கொள்ளுங்கள் என்று உங்களை பயமுறுத்தலாம் அல்லது ஏமாற்றலாம் இதன் மூலம் உங்கள் சிம்-ஐ டி ஆக்டிவேட் செய்து அவர்களிடம் இருக்கும் உங்கள் மொபைல் நம்பருக்கான சிம் கார்டை ஆக்டிவேட் செய்து கொள்வார்கள்.

பாதுகாப்பு குறிப்புகள்

- உங்களின் இரகசிய மற்றும் சொந்த டேட்டாவை திருடும் நோக்கத்தில் செய்யப்படும் இந்த திட்டமிட்டு செய்யப்படும் மோசடி பற்றி எச்சரிக்கையாக இருங்கள்.
- உங்கள் மொபைல் போன் திடீரென ஏதேனும் நெட்ஒர்க் இணைப்பை காட்டாமல் நின்று விட்டால் உங்கள் மொபைல் சர்வீஸ் புரொவைடரை உடனே தொடர்பு கொண்டு, உங்கள் சர்வீஸ் நிலையை பற்றி விசாரியுங்கள். அவ்வாறு விசாரிப்பதால் உங்கள் சிம்-க்காக ஏதேனும் டூப்ளிகேட் சிப் வழங்கப்பட்டுள்ளதா என்று உறுதிப்படுத்திக் கொள்ளலாம்.

இதர மோசடி வகைகள் பற்றி (1)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

சோஷியல் மீடியா மூலம் மோசடிகள்

இது எவ்வாறு செய்யப்படுகிறது

- மோசடிக்காரர்கள் பிரபலமான சோஷியல் மீடியா பிளாட்ஃபார்ம்களில் உங்களைப் போலவே செயல்பட்டு போலியான கணக்குகளை உருவாக்குவார்கள்.
- அன்லாக் செய்யப்படாத உங்கள் போன் யாரிடமாவது தவறுதலாக (ஒரு அவசர நிலை அழைப்புக்காக அல்லது பழுதுபார்ப்பதற்காக) கொடுக்கப்பட்டிருக்கும் போது அல்லது அட்டண்ட் செய்யப்படாமல் வைத்திருக்கும்போது, மோசடியாளர் உங்கள் மொபைலுக்கு அனுப்பப்படும் ஒடிபியை பெற இயலும். அதன் மூலம் உங்களின் புரொஃபைலை தொடர்பு கொண்டு அந்த தகவல்கள் மூலம் சில அப்ளிகேஷன்களை பயன்படுத்தி ஒரு டெஸ்க்டாப் வெர்ஷனை அவர்கள் உருவாக்கலாம். இதன் மூலம் உங்களின் தொடர்புகள், ஆன்லைன் புரொஃபைல், சாட் தகவல்களை அவர்கள் தொடர்பு கொள்வார்கள்.
- அதன் பின் அவசரமாக மருத்துவ உதவிக்கு பணம் தேவை முதலிய சில தேவைகள் எனக் கேட்டு உங்கள் நண்பர்களுக்கு அவர்கள் கோரிக்கைகள் அனுப்புவார்கள்.

பாதுகாப்பு குறிப்புகள்

- எதற்காகவும் பணம் செலுத்தும் முன் உங்கள் தொடர்புகளை தொலைபேசி மூலமாகவோ அல்லது நேரிலோ தொடர்பு கொண்டு கோரிக்கையின் நம்பகத்தன்மையை சரிபாருங்கள்.
- லாக் செய்யாத உங்கள் மொபைலை ஒருபோதும் கவனிக்காமல் இருக்காதீர்கள்.

க்யூஆர் ஸ்கேன் அடிப்படையிலான மோசடிகள்

இது எவ்வாறு செய்யப்படுகிறது

- மோசடிக்காரர்கள் பல காரணங்கள் கூறி பல்வேறு விதமான வகைகளில் உங்களை தொடர்பு கொண்டு பேமெண்ட் ஆப்களை பயன்படுத்தி க்யூஆர்கோட்களை ஸ்கேன் செய்யுமாறு உங்களை மயக்கலாம் மற்றும் அதன் மூலம் பணம் செலுத்தும்படி உங்களிடம் கூறலாம்.
- இந்த க்யூஆர் கோட்கள், எந்த ஒரு குறிப்பிட்ட கணக்கிற்கும் பணத்தை பரிமாற்றம் செய்யும் விதத்தில் முன்னரே உருவாக்கப்பட்டுள்ள கணக்கு விபரங்கள். இதன் மூலம் உங்களை ஏமாற்றி உங்கள் கணக்கிலிருந்து எந்த ஒரு குறிப்பிட்ட கணக்கிற்கும் அந்த மோசடிக்காரர் பணப் பரிமாற்றம் செய்து விடலாம்.

பாதுகாப்பு குறிப்புகள்

- பேமெண்ட் ஆப்களை பயன்படுத்தி ஏதேனும் க்யூஆர் கோட்களை ஸ்கேன் செய்யும்போது எச்சரிக்கையாக இருங்கள்.

இதர மோசடி வகைகள் பற்றி (2)

செய்யப்படும் விதம்
நீங்கள் எச்சரிக்கையாக பாதுகாப்பாக இருப்பது எப்படி?

லாட்டரி பரிசுக்காக அல்லது வேலைக்காக மோசடி செயல்கள்

இது எவ்வாறு செய்யப்படுகிறது

- மோசடிக்காரர்கள் உங்களுக்கு ஒரு பெரும் லாட்டரி பரிசு விழுந்திருப்பதாகவோ கூறிட அல்லது ஒரு பிரபலமான நிறுவனத்தில் இருந்து வேலை நியமன அதிகாரி போல நடித்து உங்களுக்கான வேலை இருப்பதாக கூறிட, உங்களை மின்னஞ்சல் மூலம் அல்லது தொலைபேசி மூலம் தொடர்பு கொள்வார்கள்
- எனினும் இவ்வாறு வேலைக்காகவோ அல்லது லாட்டரிக்கான பணத்தை/நபரிசை பெறுவதற்கு ஏதேனும் சிறிதளவு பணத்தை முதலில் செலுத்தும்படி அவர்கள் உங்களிடம் கூறலாம்.
- இவ்வாறு அவர்கள் கூறும் தொகை பொதுவாக லாட்டரி பரிசு அல்லது வேலையை பெறுவதற்காக அளிக்கப்பட வேண்டிய சிறு சதவிகிதமாகதான் இருக்கும். அதை நம்பி நீங்கள் பணத்தை செலுத்தினால் ஏமாற்றத்துக்கு உள்ளாகலாம்.

பாதுகாப்பு குறிப்புகள்

- லாட்டரி சம்பந்தமான அழைப்புகளுக்காக/ மின்னஞ்சல்களுக்காக பணம் செலுத்தவோ அல்லது உங்கள் இரகசிய தகவல்களை அளிக்கவோ வேண்டாம்.
- நம்பமுடியாத லாட்டரி பரிசு அல்லது சலுகைகளின் நம்பகத்தன்மை பற்றி எப்போதும் கேள்வி கேளுங்கள்.
- நினைவில் கொள்ளுங்கள், வேலை வழங்கும் எந்த உண்மையான நிறுவனமும் உங்களிடம் பணம் கேட்பதில்லை.

ஏடிஎம் கார்டு ஸ்கிம்மிங்

இது எவ்வாறு செய்யப்படுகிறது

- மோசடியாளர்கள் ஏடிஎம்களில் ஸ்கிம்மிங் கருவிகளை பொருத்தி வைப்பார்கள். அதன் மூலம் உங்களின் டேட்டாக்களை திருடி, ஒரு டூப்ளிகேட் கார்டை உருவாக்கி உங்கள் கணக்கில் இருந்து பணத்தை எடுப்பார்கள்.
- மேலும் அவர்கள் உங்களால் என்டர் செய்யப்படும் தகவல்களை பதிவு செய்ய டம்மி கீபேட்கள் அல்லது சிறு காமிராக்களை பொருத்தவும் செய்யலாம்.
- மேலும் அவர்கள் உங்கள் பின் நம்பரை பார்ப்பதற்காக ஏடிஎம் சர்வீஸ்களை பயன்படுத்தும் ஒரு வாடிக்கையாளர் போல நடிப்பார்கள் நீங்கள் அவற்றை என்டர் செய்யும்போது அல்லது உங்களால் பணம் எடுக்க முடியாதபோது, உங்களுக்கு உதவுவது போல் நடிப்பார்கள்.

பாதுகாப்பு குறிப்புகள்

- விழிப்புடன் இருங்கள் மற்றும் ஏடிஎம் மெஷினின் கார்டு செருகும் ஸ்லாட் அல்லது கீபேட்-க்கு அருகில் கூடுதல் சாதனம் எதுவும் இணைக்கப்படவில்லை என்பதை கவனித்து உறுதி செய்து கொள்ளுங்கள்.
- உங்களுக்கு அருகில் நிற்கும் யார் முன்னாலும் கார்டு விவரங்களை என்டர் செய்யாதீர்கள்.
- பின் நம்பரை என்டர் செய்யும்போது கீபேட்-ஐ மூடியபடி செய்யுங்கள், உங்கள் கார்டு அல்லது பின் நம்பரை யாருடனும் பகிராதீர்கள்.
- ஏதேனும் சந்தேகத்திற்குரிய சூழலை உணர்ந்தால், உடனடியாக ஏடிஎம் பகுதியை விட்டு வெளியேறுங்கள்.

#BankingDhyaanSe

சந்தேகத்திற்கு இடமான அல்லது மோசடியான பரிவர்த்தனை என நீங்கள் உணரும் எது பற்றியும் ஆக்ஸிஸ் பேங்கிற்கு தெரிவியுங்கள்

சந்தேகத்திற்கு இடமான பரிவர்த்தனை அல்லது மோசடியான பரிவர்த்தனை செய்யப்பட்டுள்ளது என்று நீங்கள் அறிந்தால் நீங்கள் கீழே குறிப்பிட்டுள்ளவற்றில் எங்களை தொடர்பு கொள்ளுங்கள்:

- எங்களின் போன் பேங்கிங் நம்பர்களை அழையுங்கள்: 1860 419 5555 / 1860 500 5555
- எங்களுக்கு எழுதுங்கள் https://www.axisbank.com/support/
- எங்களின் ஏதேனும் ஆக்ஸிஸ் கிளைக்கு வாருங்கள்

தாங்கள் இதை படிக்க நேரம் செலவிட்டதற்கு நன்றி.

#BankingDhyaanSe