DCB BANK

இணைப்பு 7: வாடிக்கையாளர் விழிப்புணர்வு - சைபர் அச்சுறுத்தல்கள் மற்றும் மோசடிகள்

சமூக ஊடக நுட்பங்கள், மொபைல் போன் அழைப்பகள் ஆகியவை உள்ளிட்ட நூதன செயல்பாடுகளைப் பயன்படுத்துவதன் மூலம் பொதுமக்களை ஏமாற்றி, தவறாக வழிநடத்துவது கண்டறியப்பட்டுள்ளது. இதை கருத்தில் கொண்டு, மோசடி செய்திகள், தவறான அழைப்புகள், அறியாத இணைப்புகள், தவறான அறிவிப்புகள், அங்கீகரிக்கப்படாத QR குறியீடுகள் ஆகியவற்றை குறித்து பொது மக்கள் விழிப்புடன் இருக்குமாறு டிசிபி பேங்க் எச்சரிக்கிறது. மேலும் எந்த விதத்திலும் வங்கிகள் மற்றும் நிதி சேவை வழங்குநர்களிடமிருந்து சலுகைகளை/விரைவான பதிலைப் பெறுவதற்கு உறுதி அளிக்கிறது.

மோசடிக்காரர்கள் பயனர் ஐடி, உள்நுழைவு/ பரிவர்த்தனை கடவுச்சொல், ஒரு நேர கடவுச்சொல் (ஒடிபி), பின், சிவிவி, காலாவதி தேதி போன்ற டெபிட்/கிரெடிட் கார்டு விவரங்கள் மற்றும் பிற தனிப்பட்ட தகவல்கள் போன்ற இரகசியமான விவரங்களைப் பெற முயற்சி செய்கிறார்கள். மோசடிக்காரர்களால் பயன்படுத்தப்படும் பொதுவான செயல் முறைகள்:

- விஷிங்-போன் அழைப்புகள் என்பது கேஒய்சி புதுப்பித்தல், கணக்கு/சிம் கார்டின் தடை நீக்குதல், டெபிட் செய்யப்பட்ட தைடகடய கிரெடிட் செய்தல் முதலிய சாக்குபோக்குகளின் கீழ் வங்கி/வங்கி அல்லாத இ-வேலட் வழங்குநர்கள்/ தொலைதொடர்பு சேவை வழங்குநர்களிடமிருந்து வரும் அழைப்புகள் என்று பாசாங்கு இரகசிய விவரங்களை பகிர வாடிக்கையாளர்களை கவர்தல்.
- ஃபிஷிங் - ஏமாற்றப்பட்ட மின்அஞ்சல்கள் மற்றும்/அல்லது எஸ்எம்எஸ் என்பது தங்களுடைய வங்கி/ இ-வேலட் வழங்குநர்களிடமிருந்து வந்த தகவல் எனகருதச் செய்து ரகசிய விவரங்களை பிரித்தெடுக்கும் இணைப்புகளைக் கொண்டிருப்பதாகும்.
- தொலைதூர அணுகல் - வாடிக்கையாளரின் சாதனத்தில் உள்ள தரவை அணுகக்கூடிய பயன்பாட்டை அவர்களின் மொபைல் போன் / கணினியில் பதிவிறக்கம் செய்ய அவர்களை கவர்ந்திழுத்தல்.
- பணத்தைப் பெற உங்கள் யுபிஐ பின் உள்ளிடவும் போன்ற செய்திகளுடன் போலியான பணச்செலுத்த கோரிக்கையை அனுப்புதல் மூலம் யுபிஐ வசூல் கொள்கையை தவறாகப் பயன்படுத்துதல்.
- வலைதளப்பக்கங்கள்/சமூக ஊடகங்கள் மீது வங்கிகள்/ இ-வேலட் வழங்குநர்களின் போலியான தொடர்பு எண்கள் மற்றும் தேடு இயந்திரங்கள் மூலம் காட்டப்படும்.

எந்த டிஜிட்டல் (ஆன்லைன்/மொபைல்) வங்கி/பணச் செலுத்த பரிவர்த்தனைகள் செய்யும்போது உரிய முன்னெச்சரிக்கைகளை எடுத்துக் கொண்டு பாதுகாப்பான வங்கி செயல்பாடுகளை மேற்கொள்ள டிசிபி பேங்க் பொதுமக்களை வலியுறுத்துகிறது. இது நிதிசார் மற்றும்/அல்லது பிற இழப்பை தடுக்க உதவுகிறது.

பாதுகாப்பான டிஜிட்டல் வங்கி நடைமுறைகள்

- கணக்கு எண், உள்நுழைவு ஐடி, கடவுச்சொல், பின், யுபிஐ பின், ஒடிபி,ஏடிஎம்/டெபிட் கார்டு/கிரெடிட் கார்டு விவரங்கள் போன்ற உங்கள் கணக்கு விவரங்களை ஒருபோதும் யாருடனும் பகிர்ந்து கொள்ளக் கூடாது, வங்கி அதிகாரிகளிடம் கூட எவ்வளவு உண்மையானதாக தோன்றினாலும் பகிர்ந்து கொள்ளக் கூடாது.
- கேஒய்சி புதுப்பிக்கப்படாத காரணத்திற்காக உங்கள் கணக்கை முடக்குவதாக அச்சுறுத்தும் வகையில் எந்த போன் அழைப்பு/ மின்னஞ்சல் வந்தாலும் மற்றும் அதை புதுப்பிக்க இணைப்பை கிளிக் செய்ய அறிவுறுத்தினாலும செய்யக் கூடாது. இது இப்போது மோசடிக்கார்கள் கையாளும் நூதன முறையாகும். கேஒய்சி புதுப்பித்தல்/ விரைவுபடுத்தல் குறித்த சலுகைகளுக்கு பதில் அளிக்க வேண்டாம். எப்போதும் வங்கி/வங்கி அல்லாத இ-வேலட் வழங்குநர்கள்/ தொலைதொடர்பு சேவை வழங்குநர்களின் அதிகாரிபூர்வ இணையதளத்தையே அணுகவும் அல்லது கிளையுடன் தொடர்பு கொள்ளவும்.
- உங்கள் போன் அல்லது சாதனத்தின் மீது அறிந்திராக பயன்பாட்டை பதிவிறக்கம் செய்யாதீர்கள். அந்த பயன்பாடு உங்கள் இரகசிய விவரங்களை அணுகுவதற்காக இருக்கலாம்.
- பணத்திற்கான ரசீதை பெறும் நடவடிக்கைகளுக்கு பார்கோடுகள் அல்லது கிகீ குறியீட்டை ஸ்கேன் செய்ய அல்லது எம்பின் ஞள்ளிடத் தேவையில்லை. அவ்வாறு கேட்கப்படும்போது எச்சரிக்கையாக இருக்கவும்.
- எப்போதும் தொடர்பு விவரங்களுக்கு வங்கி/வங்கி அல்லாத இ-வேலட் வழங்குநர்கள்/ தொலைதொடர்பு சேவை வழங்குநர்களின் அதிகாரிபூர்வ இணையதளத்தையே அணுகவும். இணையதள தேடு பொறியில் உள்ள தொடர்பு எண்கள் மொசடியானதாக இருக்கலாம்.
- மின்னஞ்சல்கள் மற்றும் எஸ்எம்எஸ் மூலம் பெறப்பட்ட யுஆர்எல்-கள் மற்றும் டொமைன் பெயர்களின் எழுத்துக்கள் பிழையின்றி இருக்கிறதா என்று பார்க்கவும். ஆன்லைன் வங்கி சேவைகளுக்கு சரிபார்க்கப்பட்ட, பாதுகாப்பான மற்றும் நம்பகமான இணையதளங்களை மட்டும் பயன் படுத்தவும், அதாவது ''https''என்று தொடங்குபவை. சந்தேகத்திற்குரிய யுஆர்எல்அல்லது இணையதளத்தை உடனடியாக உள்ளூர் காவல் நிலையம் / சைபர்கிரைம் கிளைக்கு தெரிவிக்க வேண்டும்.

- நீங்கள் உங்களால் துவக்கப்படாத பரிவர்த்தனைக்காக உங்கள் கணக்கில் டெபிட் செய்ய ஒடிபி-யை பெறும்பட்சத்தில், உடனடியாக உங்கள் வங்கி/ இ-வேலட் வழங்குநருக்கு தெரிவிக்கவும். நீங்கள் செய்யாத பரிவர்த்தனைக்கு உங்களுக்கு டெபிட் எஸ்எம்எஸ் வரும்பட்சத்தில் உடனடியாக உங்கள் வங்கி/ இ-வேலட் வழங்குநருக்கு தெரிவிப்பதுடன், யுபிஐ உள்பட அனைத்து டெபிட் வழிகளையும் தடுத்துவிடவும். உங்கள் கணக்கில் ஏதேனும் மோசடி செயல்பாடு இருப்பதாக சந்தேகித்தால், இணையதளம்/மொபைல் சேவைக்காக ஏதுவாக்கப்பட்ட பயனாளிகளின் பட்டியலை கூடுதலாக சரிபார்க்கவும்.
- உங்கள் வங்கி/இ-வேலட் கணக்குடன் இணைக்கப்பட்ட உங்கள் மின்னஞ்சலின் கடவுச்சொல்லை பகிரக்கூடாது. இ-காமர்ஸ்/ சமூக ஊடக தளங்கள் மற்றும் உங்கள் வங்கிக் கணக்கு மற்றும் உங்கள் வங்கிக் கணக்குடன் இணைக்கப்பட்டுள்ளவற்றிக்கு பொதுவான கடவுச்சொற்களை வைத்துக்கொள்ள வேண்டாம். பொது, திறந்த அல்லது இலவச வை-ஃபை அல்லது இணையதள நெட்வொர்க் மூலமான வங்கி செயல்பாடுகளைத் தவிர்க்கவும்.
- உங்கள் மின்னஞ்சல் உடன் பயனர் ஐடியாக எந்த இணையதளம்/ பயன்பாட்டிலும் பதிவு செய்யும்போது கடவுச்சொல்லாக கடவுச்சொல் என்ற வார்த்தையை அமைக்க வேண்டாம். உங்கள் மின்னஞ்சலை அணுகப் பயன்படுத்தப்படும் கடவுச்சொல் குறிப்பாக உங்கள் வங்கிக் கணக்குடன் இணைக்கப்பட்டிருந்தால் அது தனிப்பட்டதாக இருக்க வேண்டும், மேலும் மின்னஞ்சல் அணுகலுக்கு மட்டும் பயன்படுத்துவதாக இருக்க வேண்டும். வேறு எந்த இணையதளம் அல்லது பயன்பாட்டிற்கு அணுகலுக்கு பயன்படுத்தக் கூடாது.
- வெளிநாட்டு பணம் அனுப்புதல், கமிஷன் பெறுகை, அல்லது லாட்டரி வெல்லுதல் குறித்து இந்திய ரிசர்வ் வங்கியிடம் உங்கள் சார்பாக பணம் டெபாசிட் செய்ய அறிவுறுத்தல் மூலம் தவறாக வழிநடத்தப்படாதீர்கள்.
- உங்கள் நிதி சேவை வழங்குநர்களிடமிருந்து வரும் எச்சரிக்கைகளுக்காக உங்கள் மின்னஞ்சல் மற்றும் போன் செய்திகளை முறையாக சரிபார்க்கவும். உங்கள் கணக்கில் அங்கீகரிக்கப்படாத பரிவர்த்தனை ஏதேனும் இருப்பின், மேலும் இழப்பைத் தடுக்க கார்டு, கணக்கு, வேலட்டை தடுப்பதற்காக, உங்கள் வங்கி/ வங்கிசாரா நிதி நிறுவனம்/ சேவை வழங்குநர்க்கு புகார் அளிக்கவும்.
- உங்கள் ஏடிஎம், டெபிட் மற்றும் கிரெடிட் கார்டுகளை பாதுகாத்திடுங்கள் மற்றும் பரிவர்த்தனைகளுக்கு தினசரி வரம்பை அமைத்துக் கொள்ளுங்கள். மேலும் நீங்கள் உள்நாட்டு/வெளிநாட்டு பயன்பாட்டிற்காக வரம்புகளை அமைத்துக் கொண்டு செயல் படுத்தலாம்/முடக்கலாம்.