ஆன்லைன் பாதுகாப்பு மற்றும் பாதுகாப்பான பயன்பாட்டு வழிகாட்டுதல்கள்

உங்கள் ஆன்லைன் வங்கிச் சேவைகளை பாதுகாப்பாக பயன்படுத்துவதற்கு நாங்கள் பின் வரும் வழியில் உதவி செய்ய முடியும்.

ஒரு வங்கியாக, நாங்கள் பாதுகாப்பு பற்றி சிந்திக்கப் பழகிவிட்டோம். இணையத்தின் வளர்ச்சி நம் அனைவருக்குமே அதிக சௌகரியத்தை வழங்கியுள்ளது, ஆனால் இது புதிய அபாயங்களைக் கொண்டுவருவதால் அவற்றிலிருந்து பாதுகாப்பாக இருக்க வேண்டும். எச்எஸ்பிசியில் உள்ள நாங்கள் உங்கள் கணக்கை அங்கீகரிக்கப்படாதவர்கள் இயக்குவதை தவிர்ப்பதற்காக இத்தொழிலின் நிலையான பாதுகாப்பு, தொழில்நுட்பம் மற்றும் நடைமுறைகளை பயன்படுத்தி வருகிறோம், குறிப்பாக மூன்று முக்கிய துறைகளில் - அதாவது தனியுரிமை, தொழில்நுட்பம் மற்றும் அடையாளம் காணல்.

உங்கள் ஆன்லைன் வங்கிச்சேவையை நாங்கள் எவ்வாறு பாதுகாக்கிறோம் மற்றும் உங்கள் சொந்த ஆன்லைன் பாதுகாப்பை மேம்படுத்த நீங்கள் என்ன நடவடிக்கை எடுக்கலாம் என்பதை அறிய மேலே படிக்கவும்.

கிரெடிட்/டெபிட் கார்டு ஸ்கிம்மிங் அல்லது குளோனிங்

மோசடி செய்வோர் உங்கள் கிரெடிட் அல்லது டெபிட் கார்டில் உள்ள மேக்னடிக் ஸ்ட்ரிப்பில் உள்ள தகவல்களை திருடலாம். அவர்கள் ஏடிஎம் கார்டு ஸ்லாட்டில் ஸ்கிமிங் கருவிகளை மறைத்து வைத்தோ அல்லது நீங்கள் வணிகர்களின் பேமெண்ட் டெர்மினல்களில் பணம் செலுத்தும்போது நீங்கள் கவனிக்காத சமயத்தில் அந்த விவரங்களை திருடுவார்கள். இந்த கருவிகள் உங்கள் கார்டு விவரங்களை ஸ்கேன் செய்து சேமித்து விடும். உங்கள் பின்-ஐ தெரிந்து கொள்வதற்காக மோசடியாளர்கள் ஏடிஎம்இல் அல்லது வணிகர்களின் இடத்தில் கேமராவை மறைத்து வைத்திருப்பார்கள்.

UPI பயன்பாடுகளில் மோசடி அல்லது கட்டண மோசடிகள்

மோசடி செய்பவர்கள் உங்களுக்கு மெசேஜிங் பயன்பாடுகள் வழியாக QR குறியீடுகளை அனுப்பலாம், QR குறியீட்டை ஸ்கேன் செய்யும்படி கேட்கலாம் அல்லது தங்கள் கணக்கில் பணத்தை மாற்றுவதற்கான 'சேகரிப்பு' கோரிக்கையை அங்கீகரிக்கலாம். நீங்கள் விற்கும் ஒரு பொருளை அவர்கள் வாங்க விரும்புகிறார்கள் என்று சொல்வது போன்ற ஒரு போலி கதையை உங்களுக்குச் சொல்லி அவர்கள் உங்களை ஏமாற்ற முயற்சிக்கலாம். அவர்கள் ஒரு வங்கி அல்லது ஷாப்பிங் நிறுவனத்தின் நிர்வாகியாகவும் ஆள்மாறாட்டம் செய்யலாம், பணத்தைத் திருப்பிச் செலுத்துதல், உரிமை கோரப்படாத கேஷ்பேக் சலுகைகள் அல்லது வெகுமதி புள்ளிகளைச் செயல்படுத்த முன்வருவார்கள். சந்தேகத்திற்கு இடமில்லாத பாதிக்கப்பட்டவர்கள் பின்னர் QR குறியீட்டை ஸ்கேன் செய்யலாம் அல்லது அவர்களின் UPI பின்னைப் பயன்படுத்தி 'சேகரி' கோரிக்கையை அங்கீகரிக்கலாம், மோசடி செய்பவரின் கணக்கில் பணத்தை மாற்றலாம்.

வணிக மின்னஞ்சல்கள் மற்றும் மெஸ்ஸேஜ் செயலிகள் மூலம் பண மோசடி

மோசடி செய்பவர்கள் உங்கள் மின்னஞ்சல்கள் அல்லது உரையாடல்கள்/குறுந்தகவல்களை ஹேக் செய்யலாம் அல்லது என்க்ரிப்டெட் செய்திகளை இடைமறித்து உங்களைப் பற்றி மேலும் விவரத்தை அறிந்து கொள்ளலாம். அவர்கள் உங்களைப் பற்றி மேலும் விவரங்களை அறிந்தவுடன், அவர்கள் ஹேக் செய்யப்பட்ட / விட்டுக் கொடுக்கப்பட்ட / ஏமாற்றப்பட்ட ஐடியிலிருந்து செய்திகளை அனுப்பலாம், அன்புக்குரியவரை மருத்துவமனையில் சேர்ப்பது அல்லது புதியதாக செலுத்த வேண்டிய நிலுவைத் தொகை போன்ற நியாயமான நோக்கங்களுக்காக அவசர பணம் செலுத்துமாறு கேட்டுக்கொள்கிறார்கள். அவசர நிலையில் பணம் கோருவதால் அல்லது கோரிக்கையை நம்பலாம் என்று நினைப்பதால் பாதிக்கப்பட்டவர்கள் பணம் செலுத்துவதில் ஏமாற்றப்படலாம். பாதிக்கப்பட்டவர் அவர்களே பணம் செலுத்தியதால், வங்கி அவர்களுக்கு அனுப்பும் பரிவர்த்தனை எச்சரிக்கைகளை கண்டு அவர்கள் பயப்பட மாட்டார்கள். இந்த வகையில் செய்யப்படும் மோசடியை கண்டறிவது கடினம்.

போலி தொடர்பு எண்கள்

மோசடி செய்பவர்கள் வங்கிகள் மற்றும் சேவை வழங்குநர் தொடர்பு மையங்களின் போலி தொடர்பு விவரங்களை வழங்கலாம். பாதிக்கப்பட்டவர்கள் சந்தேகப்படாமல தேடுபொறியைப் பயன்படுத்தி தொடர்பு விவரங்களைத் தேடலாம். மேலும் கொடுக்கப்பட்ட போலி எண்ணை அழைக்கலாம். பின்னர் அவர்கள் ஒரு ''சரிபார்ப்பு செயல்முறை'' க்கு அழைத்துச் செல்லப்படுவார்கள், அங்கு அவர்களை ஏமாற்றி டெபிட் / கிரெடிட் கார்டுகள் மற்றும் வங்கிக் கணக்குகள் பற்றிய முக்கியமான தகவல்களைப் பகிர வைத்துவிடுவார்கள்.

உங்களுக்குத் தேவையான தொடர்பு விவரங்களைத் தேடுவதற்கு நீங்கள் எப்போதும் ஒரு வங்கி அல்லது சேவை வழங்குநரின் அதிகாரப்பூர்வ வலைத்தளத்தைப் பார்வையிடுவதை உறுதிசெய்வதன் மூலம் உங்களைப் பாதுகாத்துக் கொள்ளலாம். கவனமாக இருங்கள் மற்றும் தேடல் முடிவுகளில் காண்பிக்கப்படும் அழைப்பு எண்களை முதலில் சரிபார்க்காமல் அழைப்பதைத் தவிர்க்கவும், அதிலும் குறிப்பாக அவை மொபைல் எண்ணாக இருக்கும் பட்சத்தில்.

ஃபிஷிங் அல்லது ஏமாற்றும் மின்னஞ்சல்கள்

மோசடி செய்பவர்கள் தங்களால் முடிந்தவரை பல மின்னஞ்சல் முகவரிகளுக்கு மின்னஞ்சல் அனுப்புவதன் மூலம் பாதிக்கப்பட்டவர்களை ஃபிஷ் செய்யலாம். ஒரு வங்கி, ஆன்லைன் பணம் செலுத்தும் முறை, சில்லறை விற்பனையாளர் அல்லது அது போன்ற சேவைகளை முறையான அமைப்பின் ஒரு பகுதியாக நடித்து அவர்கள் அடிக்கடி இதைச் செய்கிறார்கள். அவர்கள் தங்கள் போலி அடையாளத்தை தரலாம், எனவே மின்னஞ்சல் மோசடி செய்பவர்களைத் தவிர வேறு யாரோ அனுப்பியது போல் தெரியும்.

தனிப்பட்ட விவரங்கள் அல்லது நிதித் தகவலைக் கேட்கும் மின்னஞ்சல்களுக்கு பதிலளிக்காமல் ஃபிஷிங் மோசடிகளுக்கு ஆளாகி ஏமாறாமல் உங்களைப் பாதுகாத்துக் கொள்ளலாம். சந்தேகத்திற்குரிய மின்னஞ்சல்களில் வரும் இணைப்புகளை நீங்கள் ஒருபோதும் தேர்ந்தெடுக்கக்கூடாது

உங்கள் தனிப்பட்ட அல்லது பாதுகாப்பு விவரங்களை மின்னஞ்சல் மூலம் வெளியிட எச்எஸ்பிசி உங்களை ஒருபோதும் கேட்காது. எச்எஸ்பிசியிலிருந்து வந்ததாகக் கூறி அத்தகைய மின்னஞ்சல்கள் வந்தால், அவற்றிற்கு பதிலளிக்க வேண்டாம். மின்னஞ்சலை உடனடியாக நீக்கிவிடுங்கள். நினைவில் வைத்து கொள்ளுங்கள், உங்கள் விவரங்களை - உங்கள் யூசர் நேம், பாஸ்வேர்டு அல்லது இதர பாதுகாப்பு விவரங்கள் போன்றவற்றை யாருடனும் பகிர்ந்து கொள்ளக்கூடாது.

பண ஆசை அல்லது கூடுதல் வருமானத்திற்கு ஆசை காட்டும் மின்னஞ்சல் மோசடிகள்

பண ஆசை காட்டும் மோசடியில், மோசடி செய்பவர்கள் உங்களிடம் பணப் பரிவர்த்தனைக்கான உதவியை கேட்கலாம். அவர்கள் உங்கள் கணக்கில் பணத்தை பரிவர்த்தனை செய்ய முன்வருவார்கள், எனவே அதன் மூலம் நீங்கள் அதை வேறு கணக்கிற்கு மாற்ற அவர்களுக்கு உதவலாம். இதற்கு பிரதி பலனாக அவர்கள் உங்களுக்கு கமிஷன் தருவதாக சொல்வார்கள்.

பெரும்பாலும் பண மோசடி செய்வதற்காக இதுபோன்ற கோரிக்கைகளை வைத்து அவர்கள் பெரும்பாலும் குற்றங்களில் ஈடுபடுவதால் நீங்கள் அவற்றை புறக்கணிக்க வேண்டும். தெரிந்தே பங்கேற்கும் எவரும் குற்றத்தின் கூட்டாளியாகக் கருதப்படலாம், மேலும் அவர்கள் மீது வழக்கு தொடரப்படலாம். அது உண்மை போலவே இருந்தாலும்கூட, உண்மையில் அது அநேகமாக ஒரு ஏமாற்று வேலை.

முன்கூட்டியே கட்டணம் மோசடி ('419' மோசடிகள்)

மோசடி செய்பவர்கள் நீங்கள் கேட்காத கடிதங்களையோ அல்லது மின்னஞ்சல்களையோ அனுப்பலாம், பெரிய தொகையை பரிவர்த்தனை செய்வதற்கு உதவுவதற்காக தாராளமாக வெகுமதி அளிக்கலாம், பொதுவாக அமெரிக்க டாலர்களில். இந்த மோசடி செய்பவர்களின் நோக்கம் உண்மையில் உங்கள் வங்கி விவரங்களைப் பெறுவதுதான். அவர்கள் பொதுவாக ஒரு கட்டணம், சில வரிகள் அல்லது ஒப்பந்தத்தை முடிக்க லஞ்சம் கொடுக்குப்பதற்காக பணம் கேட்கிறார்கள் - இது முன்பணம் ஆகும். ஏமாற்றப்படுபவர்கள் பொதுவாக மோசடி செய்பவர்களிடம் இதை இழக்கிறார்கள்.

உங்கள் ஆன்லைன் வங்கி விவரங்கள் யாரிடமாவது இருப்பதாக உங்களுக்கு சந்தேகம் எழுந்தால், நீங்கள் ஆன்லைன் வங்கியில் உள்நுழைந்து உடனடியாக உங்கள் கடவுச்சொல்லை மாற்றிவிட வேண்டும். கூடிய விரைவில் நீங்கள் எங்களை தொடர்பு கொண்டு எச்சரிக்க வேண்டும். எங்கள் தொலைபேசி எண்கள் *24x7* செயல்படுகின்றன. எங்கள் ஹாட்லைன் எண்களின் பட்டியலை இங்கே காணலாம்.

சமூக ஊடகங்கள் வாயிலாக ஹேக்ஸ்

மோசடி செய்பவர்கள் பேஸ்புக், வாட்ஸ்அப் அல்லது இன்ஸ்டாகிராம் போன்ற சமூக ஊடக தளங்களில் நெருங்கிய நண்பர் அல்லது உறவினர் போல ஆள்மாறாட்டம் செய்யக்கூடும், அவசரமாக அவர்களுக்கு பணத்தை பரிவர்த்தனை செய்யுமாறும் கேட்டுக்கொள்கிறார்கள். உங்களுக்குத் தெரிந்த ஒருவரிடமிருந்து அழைப்பு முறையானதா என்பதை நீங்கள் அவர்களை அழைப்பதன் மூலமாகவோ அல்லது இதர வழிகள் மூலமோ தொடர்பு கொண்டு அந்த விவரங்களை நீங்கள் சரிபார்க்கலாம்.

விஷ்ஷிங் அழைப்புகள்

மோசடி செய்பவர்கள் வங்கி ஊழியர்கள் அல்லது வாடிக்கையாளர் சேவை நிர்வாகி போன்று ஆள்மாறாட்டம் செய்யக்கூடும் மற்றும் ஏமாறுபவர்களை அவர்களின் வங்கி கணக்கு விவரங்கள் போன்ற முக்கியமான தகவல்களைத் திருடுவதற்காக தொடர்பு கொள்ளலாம். ஏமாற்றப்படுபவர்களின் நம்பிக்கையை பெறுவதற்காக, குற்றவாளிகள் பாதிக்கப்பட்டவருக்கு சமூக பொறியியல் மூலம் திருடப்பட்ட தனிப்பட்ட தகவல்களை வழங்கக்கூடும். அவர்கள் சில நம்பிக்கையை ஏற்படுத்திய பிறகு, மோசடி செய்பவர்கள் தங்கள் வங்கி விவரங்கள் மற்றும் ஒன் டைம் பாஸ்வேர்டுகள் (OTP கள்) போன்ற இரகசிய தகவலை வழங்குவார்கள் என்ற நம்பிக்கையில், சில சிறப்பு சேவை அல்லது திட்டங்களை வழங்கலாம்.

ட்ரோஜன் வைரஸ்கள்

சில கோப்புகள், பக்கங்கள் அல்லது இணைப்புகளை திறக்கச் சொல்லுமாறு கோரிக்கைகளை கொண்ட தேவையற்ற மின்னஞ்சல்களை மோசடி செய்பவர்கள் உங்களுக்கு அனுப்பலாம். ஆனால் அவற்றைத் திறந்தால் அது உங்கள் ஆன்லைன் செயல்பாட்டைக் கண்காணிக்கும் ஒரு மென்பொருளை உங்கள் கணினியில் ரகசியமாக நிறுவும், மேலும் பல்வேறு வலைத்தளங்களில் நீங்கள் தட்டச்சு செய்வதையும் குறித்துக் கொள்ளும். எனவே ஆன்லைனில் ஷாப்பிங் செய்யும் போது உங்கள் கிரெடிட் கார்டு விவரங்களை உள்ளிடும்போது, நீங்கள் உள்ளிட்ட தகவல்களை மோசடி செய்பவர்களால் பார்க்க முடியும்.

ஆன்லைன் பாதுகாப்புக்காக எச்எஸ்பிசி எடுத்துள்ள நடவடிக்கைகள்

பல அடுக்கு முறையில் சரிபார்த்தல்

உங்கள் நிதித் தகவல் தனித்துவமான யூசர் நேம் மற்றும் பாஸ்வேர்டின் அதிநவீன கலவையினாலும், உங்கள் இணைய வங்கி பாதுகாப்பு சாதனம் அல்லது டிஜிட்டல் பாதுகாப்பிற்கான கீ மூலம் உருவாக்கப்பட்ட ஒரு முறை பாதுகாப்புக் குறியீட்டினாலும் பாதுகாக்கப்படுகிறது.

பரிவர்த்தனை சரிபார்ப்பு

கார்டுகளில் 3D பாதுகாப்பான பரிவர்த்தனைகள் இருப்பதால் அவை பரிவர்த்தனை மற்றும் கட்டணம் செலுத்துதல் முறையின் மீதான நம்பிக்கையைப் பாதுகாக்க உதவுகின்றன. பரிவர்த்தனைக்காக உருவாக்கப்பட்ட OTP களை ஒருபோதும் யாருடனும் பகிர்ந்து கொள்ளக்கூடாது.

128-பிட் செக்யூர் சாக்கெட் லேயர் (எஸ்எஸ்எல்) குறியீடு

இணைய வங்கி செயல்பாட்டின் போது அனுப்பப்படும் தகவல்களுக்கு எச்எஸ்பிசி 128 பிட் செக்யூர் சாக்கெட் லேயர் (எஸ்எஸ்எல்) குறியீடுகளைப் பயன்படுத்துகிறது, இது குறியீடுகள் தொழிலின் தரமாக ஏற்றுக்கொள்ளப்படுகின்றன.

தானியங்கி 'டைம்-அவுட்' அம்சம்

ஒரு பாதுகாப்பு நடவடிக்கையாக, உங்கள் இணைய வங்கியை இயக்கும்போது பயன்படுத்தப்படாத சிறிது நேரத்திற்குப் பிறகு அது தானாகவே மூடப்படும் அல்லது காலாவதியாகிவிடும். நீங்கள் இணைய வங்கி சேவையை முடித்ததும் உங்கள் இணைய வங்கி இயக்கத்தை எப்போதும் மூட வேண்டும்.

பாதுகாப்பு சாதனம்/ டிஜிட்டல் பாதுகாப்பு கீ

உங்கள் இணைய வங்கி பாதுகாப்பு சாதனம் / டிஜிட்டல் பாதுகாப்பு கீ ஆன்லைன் பாதுகாப்பை உயர் மட்டங்களுக்கு எடுத்துச் செல்கிறது. உங்கள் கணக்கில் உள்நுழைய நீங்கள் ஏற்கனவே இருக்கும் யூசர் நேம் மற்றும் பாஸ்வேர்டை வழக்கம் போல் உள்ளிட வேண்டும், அதைத் தொடர்ந்து உங்கள் இணைய வங்கி பாதுகாப்பு சாதனம் அல்லது உங்கள் டிஜிட்டல் பாதுகாப்பு கீ மூலம் உருவாக்கப்பட்ட தனிப்பட்ட பாதுகாப்பு குறியீடை உள்ளிட வேண்டும். இந்த இரண்டு நிலை அங்கீகார செயல்முறை உங்கள் இணைய வங்கியை இயக்கும்போது மேம்பட்ட அளவிலான பாதுகாப்பை வழங்குகிறது.

ஆன்லைன் பாதுகாப்பில் உங்கள் பங்கு

இணைய வங்கிப் பாதுகாப்பை உறுதி செய்வதற்கான பின்னே கொடுத்துள்ளபடி செய்ய வேண்டியவற்றைப் பயிற்சி செய்யுங்கள்

செய்ய வேண்டியவை

- உங்கள் கணினி சமீபத்திய வைரஸ் தடுப்பு மற்றும் ஃபயர்வால் பாதுகாப்பு மென்பொருளுடன் எப்போதும் பாதுகாக்கப்படுவதை உறுதிசெய்க. சமீபத்திய பாதுகாப்பு அப்டேட்ஸை தொடர்ந்து தரவிறக்கம் செய்து உங்களுக்கு சமீபத்திய பாதுகாப்பு இருப்பதை உறுதி செய்து கொள்ளவும்.
- உங்களுக்கு மறக்கமுடியாத பாஸ்வேர்டை தேர்வுசெய்க, ஆனால் வேறொருவரால் எளிதாக யூகிக்க முடியாததாக இருக்க வேண்டும். எண் மற்றும் எழுத்துக்களின் சேர்க்கைகளைக் கொண்ட பாஸ்வேர்டுகளை யூகிப்பது கடினமாக இருக்கும் (உதாரணமாக a7g3cy91)
- உங்கள் இணைய வங்கி பாஸ்வேர்டை அடிக்கடி மாற்றவும்.
- ஃபிஷிங் மின்னஞ்சல்களை கண்டு எச்சரிக்கையாக இருங்கள். அனைத்து கடிதங்கள் மற்றும் எழுத்துக்கள் உட்பட முழு மின்னஞ்சல் முகவரியையும் எப்போதும் கவனமாகப் படியுங்கள்.
- ஃபிஷிங் மிகவும் ஒத்த தோற்றமுடைய மின்னஞ்சல் முகவரிகள் மூலம் செய்யப்படுகிறது. உதாரணமாக. hsdc.co.in அல்லது hsbcbank.com. உங்கள் மவுஸ் சுட்டிக்காட்டி அதன் உண்மையான இலக்கை வெளிப்படுத்த URL மீது செலுத்தவும்; இது உங்கள் பிரவுசரின் கீழ் இடது மூலையில் காட்டப்படும். பொருந்தவில்லை என்றால் இணைப்பைக் கிளிக் செய்ய வேண்டாம். URL இல் எழுத்துப்பிழை தவறுகள், இலக்கணத் தவறுகள் அல்லது இடம் மாறியுள்ள எழுத்துக்கள் போன்ற அறிகுறிகளைப் பாருங்கள்
- உங்கள் கணக்கிலிருந்து இனி தேவைப்படாவிட்டால் சேர்க்கப்பட்ட பயனாளிகளை நீக்கவும்
- உங்கள் கணினியிலோ அல்லது பிரவுசரிலோ உள்ள விவரங்களை தானாக சேமிக்கும் செயல்பாட்டை முடக்கவும்
- உங்கள் கணினியின் அமைப்புகள் மற்றும் இணைய பிரவுசர்களை புதுப்பிக்கவும். உற்பத்தியாளர்கள் தங்கள் அமைப்புகள் மற்றும் பிரவுசர்களில் பலவீனங்கள் கண்டறியப்படும்போது தொடர்ந்து பாதுகாப்பு மென்பொருள்களை வெளியிடுகின்றனர். இந்த புதுப்பிப்புகளை உங்கள் மென்பொருள் வழங்குநரிடம் தவறாமல் சரிபார்க்கவும்.
- எச்எஸ்பிசி வலைத்தளத்தை அடைய எப்போதும் பிரவுசரில் எங்கள் URL ஐ தட்டச்சு செய்யவும்.
- பேட்லாக் (🔒) சின்னம் மற்றும் இணையதள சான்றிதழை சரிபார்க்கவும். இணையதள சான்றிதழ் எச்எஸ்பிசிக்கு சொந்தமானது என்பதை உறுதிப்படுத்த நீங்கள் எச்எஸ்பிசி ஆன்லைன் வங்கியில் உள்ளே செல்லும்போது உங்கள் பிரவுசரின் கீழ்ப்பகுதியில் உள்ள பேட்லாக் சின்னத்தை இருமுறை கிளிக் செய்யவும். 'போலி' தளத்தில் உங்கள் விவரங்களை உள்ளிடுவதன் மூலம் நீங்கள் ஏமாற்றப்படுவதில்லை என்பதை இது உறுதி செய்யும்.
- உங்கள் கணக்குகளை தவறாமல் சரிபார்க்கவும். ஏதேனும் பரிவர்த்தனைகள் குறித்து சந்தேகம் இருந்தால், விவரங்களைக் கவனித்து எங்களை அழைக்கவும்.
- ஆன்லைன் வங்கியைப் பயன்படுத்திய பிறகு எப்போதும் லாக் அவுட் பொத்தானைத் தேர்ந்தெடுத்து வெளியேறி விடுங்கள்., நீங்கள் இணையதள சேவைக்காக உள்ளே நுழையும்போது உங்கள் கணினியை கவனிக்காமல் விடாதீர்கள்.
- வங்கிகளின் வாடிக்கையாளர் சேவை எண்கள், ஆன்லைன் ஷாப்பிங் வலைத்தளங்கள் போன்றவற்றை நீங்கள் தேடுகிறீர்களானால் இணையத்தில் புத்திசாலித்தனமாகத் தேடுங்கள். மோசடி செய்பவர்கள் தங்களிடம் உள்ள மொபைல் எண்களை கொடுத்து மோசடி செய்கிறார்கள். வங்கியின் வாடிக்கையாளர் சேவை எண் அல்லது இ-காமர்ஸ் வலைத்தளத்திற்கு பதிலாக மோசடி செய்பவரை நீங்கள் அழைக்க நேரிடலாம்.
- உங்கள் வங்கியின் தொடர்பு மையத்தின் எண்ணை உங்கள் சாதனங்களில் சேமிக்கவும் அல்லது உங்கள் கிரெடிட்/ டெபிட் கார்டின் பின்புறத்தில் அச்சிடப்பட்டிருக்கும் எண்ணைப் பார்க்கவும்.
- உங்கள் தனிப்பட்ட கணினி அல்லது மொபைல் சாதனங்களில் ஸ்க்ரீன் ஷேரிங் பயன்பாடுகளில் எச்சரிக்கையாக இருங்கள். மோசடி செய்பவர்கள் இதுபோன்ற விண்ணப்பங்களை பதிவிறக்கம் செய்ய சொல்லி உங்களை ஏமாற்றி, உங்களிடமிருந்து குறியீட்டைத் தேடி உங்கள் கணக்கை அணுகலாம். அணுகல் அனுமதிக்கப்பட்டதும், அவர்கள் உங்கள் சாதனத்தை தொலைவிலிருந்து கண்காணித்து கட்டுப்படுத்தலாம், மேலும் உங்கள் கணக்குகளிலிருந்து பணம் எடுக்கலாம்.
- உங்கள் இணைய இணைப்பைப் பாதுகாப்பாக வைக்கவும். பாஸ்வேர்டு மூலம் உங்கள் வீட்டு ஒயர்லெஸ் நெட்வொர்க்கை எப்போதும் பாதுகாக்கவும்.
- கமிஷன் அல்லது உதவிக்காகக் கூட உங்கள் கணக்கில் பணம் சேகரிக்க வேண்டிய திட்டங்கள்/ சலுகைகள் குறித்து எச்சரிக்கையாக இருங்கள். அவர்கள் மோசடி செய்பவர்கள் சட்டத்திற்கு புறம்பான வருமானத்தை உங்கள் கணக்கில் அனுப்பலாம். மேலும் பணப் பரிவர்த்தனை செய்யவோ அல்லது அவர்களுக்கு பணத்தை வழங்கவோ உங்களிடம் கேட்கலாம். மோசடி செய்பவர்கள் பணப் பரிமாற்றத்திலிருந்து மறைந்திருப்பார்கள் அதற்காக அவர்கள், உங்களை கணக்கை பலிகடாவாக பயன்படுத்தலாம்.
- மோசடியைப் பற்றி புகார் அளிப்பதற்கு உடனடியாக வங்கியைத் தொடர்பு கொள்ளுங்கள்.

செய்யக்கூடாதவை

- மற்ற சேவைகளுக்கு நீங்கள் பயன்படுத்தும் பாஸ்வேர்டை தேர்வு செய்யாதீர்கள். உங்கள் கடவுச்சொல் இணைய வங்கிக்கு தனிப்பட்டதாக இருக்க வேண்டும்
- நீங்கள் கவனக்குறைவாக மின்னஞ்சல்/எஸ்எம்எஸ் லிங்கை க்ளிக் செய்தால் திறந்த இணைய தளங்களில் ஒருபோதும் யூசர்ஐடி, பாஸ்வேர்டு, கார்டு எண், காலாவதி தேதி போன்றவற்றை கொடுக்கவே கூடாது.
- வங்கி ஊழியர்களிடமிருந்தோ அல்லது வருமான வரித் துறை, ரிசர்வ் வங்கி போன்ற அரசாங்க அமைப்புகளிடமிருந்து வந்ததாகக் கூறினாலும் இது போன்ற விவரங்களைக் கேட்கும் செய்திகளுக்கு பதிலளிக்க வேண்டாம். எச்எஸ்பிசியின் எந்த ஊழியர்களும் இந்த விவரங்களை உங்களிடம் ஒரு போதும் கேட்க மாட்டார்கள்.
- உங்கள் பாஸ்வேர்டுடன் உங்கள் இணைய வங்கி யூசர் நேமை எழுதகூடாது. உங்கள் பாஸ்வேர்டை அடையாளம் காணக்கூடிய வடிவத்தில் எழுதக்கூடாது. உங்கள் இணைய வங்கி பாதுகாப்பு சாதனத்தை/ டிஜிட்டல் பாதுகாப்பு கீயை யூசர் நேமுடன் சேர்த்து வைக்காதீர்கள்.
- உங்கள் மொபைல் வங்கி செயலிகளை புதுப்பித்த நிலையில் வைத்திருங்கள். அதை பதிவிறக்கம் செய்ய மற்றும் அதில் ஏதேனும் புதுப்பிப்புகளைச் செய்ய, உங்கள் சாதனத்தின் அதிகாரப்பூர்வ ஆப் ஸ்டோருக்குச் செல்லவும்.

- நம்பமுடியாத இடங்களிலிருந்து வந்த மின்னஞ்சல்களில் உள்ள இணைப்புகளிலிருந்து மொபைல் வங்கி/ கட்டண செயலிகளை ஒருபோதும் பதிவிறக்கம் செய்யக்கூடாது.
- உங்கள் கார்டு எண் மற்றும் காலாவதி தேதிகளை ஆன்லைன் இணையதளங்களில் சேமித்து வைக்கும்போது மிகவும் கவனமாக இருங்கள். அரிதாகப் பயன்படுத்தப்படும் வலைத்தளங்களில் அல்லது நம்பகமற்ற வலைத்தளங்களில் இந்த விவரங்களை சேமிக்க வேண்டாம்.
- உங்கள் PIN ஐ யாருடனும் பகிர்ந்து கொள்ள வேண்டாம். அதை நீங்கள் மட்டுமே பயன்படுத்த வேண்டும். உங்கள் PIN திருடப்பட்டதாக நீங்கள் சந்தேகித்தால், உடனடியாக அதை மாற்றிவிடவும்.

உங்களிடம் UPI PIN கேட்கப்பட்டால், நீங்கள் பணம் செலுத்துகிறீர்கள் என்பதை நினைவில் கொள்ளுங்கள். பணத்தை பெறுவதற்கு உங்களுக்கு UPI PIN தேவையில்லை.

பொது கணினிகளைப் பயன்படுத்தும் போது எச்சரிக்கையாக இருங்கள்

எப்போதும்

- நீங்கள் கணினியை விட்டு, ஒரு கணம் வெளியேற விரும்பினாலும்கூட, முடிந்த வரையிலும், நீங்கள் உள்நுழைந்திருக்கும் போது கணினியை கவனிக்காமல் விடாதீர்கள்.
- நீங்கள் கணினியிலிருந்து வெளியேறுவதற்கு முன் உங்கள் பிரவுஸிங் வரலாற்றை நீக்கவும்:. இணைய பிரவுசர்கள் உங்கள் பாஸ்வேர்டுகள் மற்றும் நீங்கள் பார்வையிடும் பக்கங்களைப் பற்றிய தகவல்களைச் சேமிக்கும். இணைய பிரவுசர் கருவிகளின் மெனுவுக்குச் சென்று விருப்பங்கள் அல்லது இணைய விருப்பங்களைத் தேர்ந்தெடுக்கவும். பிரவுசரில் எந்த தானியங்கி செயல்பாடும் முழுமையாக முடக்கப்பட்டிருப்பதை உறுதிசெய்து, குக்கீகளை நீக்கி, வரலாற்றை நீக்கிவிடவும்.
- நூலகங்கள், இன்டர்நெட் கஃபேக்கள் மற்றும் பள்ளிகள் உட்பட, பொது இடங்களில் உள்ள கணினிகளைப் பயன்படுத்துவதைத் முடிந்த வரையிலும் தவிர்க்க முயற்சி செய்யுங்கள்.

முக்கியமான தகவல்களைத் தட்டச்சு செய்வதைத் தவிர்க்கவும். நீங்கள் அனைத்து முன்னெச்சரிக்கை நடவடிக்கைகளையும் பின்பற்றினாலும், பொது கணினியில் கீஸ்ட்ரோக் லாகர் எனப்படும் தீங்கிழைக்கும் மென்பொருள் நிறுவப்பட்டிருக்கலாம். இந்த புரோக்கிராம்கள் உங்கள் பாஸ்வேர்டு, ககிரெடிட் கார்டு எண் மற்றும் இதர வங்கி விவரங்களை திருடலாம். முக்கியமான தகவல்களை வெளிப்படுத்தக்கூடிய எந்தவொரு நிதி பரிவர்த்தனைகளையும் தவிர்க்கவும்.

முக்கியமானது – எச்எஸ்பிசி என்று கூறிக்கொள்ளும் நம்பத்தகாத இடங்களிலிருந்து அல்லது தனிப்பட்ட தகவல்களைத் தேடும் தேவையற்ற மின்னஞ்சலை நீங்கள் எப்போதாவது பெற நேர்ந்தால் அவற்றை பற்றி மேலும் விசாரணை செய்ய அவற்றைப் பற்றி **phishing@hsbc.com** என்ற மின்னஞ்சல் முகவரியில் புகார் அளிக்கவும்.