# மோசடிக்காரர்கள் இங்கே,
# மோசடிக்காரர்கள் அங்கே,
# மோசடி வலையில் சிக்காதீர்கள்!

## #BankingDhyaanSe 2.0

AXIS BANK

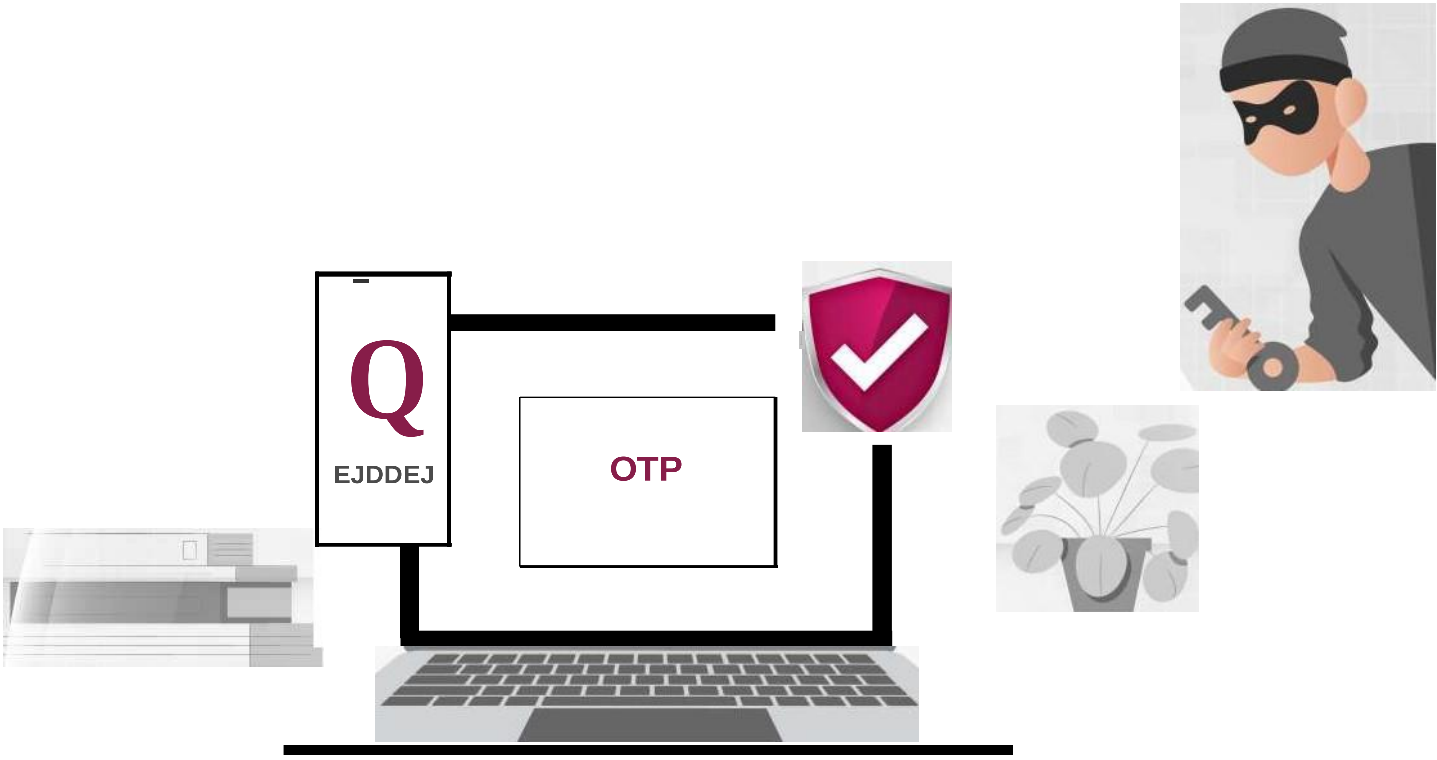
## நீங்கள் கடினமாக உழைத்து சம்பாதிக்கும் பணத்தை,

## ஏன் பாதுகாப்பாக வைக்கக்கூடாது?

ஆக்சிஸ் வங்கி மோசடி விழிப்புணர்வு வழிகாட்டி கையேடு #BankingDhyaanSe 2.0 இற்கு வரவேற்கிறோம், இது நிதி மோசடிகளைப் புரிந்துகொள்வதற்கும் தடுப்பதற்குமான உங்களின் பாதுகாப்புச் சாவி ஆகும். வேகமாக வளர்ந்து வரும் டிஜிட்டல் உலகில், மோசடிக்காரர்களின் மோசடி வலையிலிருந்து தப்பிக்க உதவும் அரணாக இருப்பது, மோசடி பற்றிய உங்களின் விழிப்புணர்வு. இந்த கையேடு உங்களுக்கு நிதி மோசடிகளிலிலிருந்து நீங்கள் கடினமாக சம்பாதித்த பணத்தை பாதுகாப்பதற்கான மதிநுட்பம், நிஜ வாழ்க்கை எடுத்துக்காட்டுக்கள் மற்றும் நடைமுறை உதவிக்குறிப்புகளை வழங்குகிறது.

வங்கிச் சேவையில் உங்களின் நம்பகமான கூட்டாளியாக, நீங்கள் டிஜிட்டல் உலகில் தைரியமாக செயல்பட, ஆக்சிஸ் வங்கி உங்களுக்கு உறுதுணையாக இருக்க அர்பணிக்கப்பட்டுள்ளது. மோசடிகளில் இருந்து நம்மை நாமே பாதுகாத்து பிரகாசமான நிதி எதிர்காலத்தை ஒன்றாக உருவாக்குவோம்.

# OTP மோசடிகள்




ஒரு-முறை கடவுச்சொல் என்பது மற்றவர்களால் அணுக முடியாத உங்கள் டிஜிட்டல் உலகின் மந்திரச் சாவியாகும்.

தந்திரமான மோசடிக்காரர்கள் உங்கள் விலைமதிப்பற்ற சாவியைத் திருடுவதைத் தடுக்க, நீங்கள் தான் உங்கள் டிஜிட்டல் உலகின் பாதுகாவலராக இருக்க வேண்டும்!

OTP-களை ரகசியமாக வைத்திருங்கள்: தொலைபேசி அழைப்புகள், மின்னஞ்சல்கள், குறுஞ்செய்திகள் அல்லது சமூக ஊடகங்கள் மூலம் OTP-களை ஒருபோதும் யாருடனும் பகிர்ந்துகொள்ள வேண்டாம் மற்றும் ஓடிபி பகிர்வது குறித்து ஒரு முனைப்பான பாதுகாவலர் போல விழிப்புடன் இருங்கள்.

கோரிக்கைகளைச் சரிபாருங்கள்: நம்புங்கள் ஆனால் எதையுமே முழுமையாக சரிபாருங்கள். நீங்கள் எதிர்பார்க்காத நேரத்தில் OTP கோரிக்கை வந்தாலோ அல்லது சந்தேகத்திற்கிடமாக இருந்தாலோ, அவசரப்பட வேண்டாம். நீங்கள் OTP-யை செயல்படுத்தும்முன் அதன் நம்பகத்தன்மையை ஒருமுறைக்கு இருமுறை சரிபாருங்கள்.

அதிகாரப்பூர்வ வலைத்தளங்கள் அல்லது செயலிக்களைப் பயன்படுத்துங்கள்: OTP-களைப் பகிரும்போது கவனமாக இருங்கள். எப்போதும் அதிகாரப்பூர்வ தளம் அல்லது செயலிக்களை நேரடியாகப் பார்வையிடுங்கள் - குறுக்குவழிகளைப் பயன்படுத்தாதீர்கள். எப்போதுமே நீங்கள் பெறும் இணைப்புகளைக் கிளிக் செய்வதைவிட, அவற்றை நீங்களே தட்டச்சு செய்து தேடுவது பரிந்துரைக்கப்படுகிறது.

அவசரக் கோரிக்கைகள் குறித்து எச்சரிக்கையாக இருங்கள்: நீங்கள் உங்கள் OTP பகிர்வதை வலியுறுத்த, மோசடிக்காரர்கள் அடிக்கடி உங்களுக்கு ஒரு அவசரநிலை உணர்வை உருவாக்குகிறார்கள். அம்மாதிரியான நேரங்களில், உடனே செயல்படும்முன், ஒரு நொடி பொறுமையாக இருந்து, தெளிவாக சிந்தித்து, அவசர கோரிக்கையை நீங்களே சுயமாக சரிபாருங்கள்.

இரண்டு காரணி அங்கீகாரத்தை இயக்குங்கள்: 2FA (இரண்டு காரணி அங்கீகாரம்) மூலம் பாதுகாப்பை இரட்டிப்பாக்குங்கள். செயலி அடிப்படையிலான அல்லது வன்பொருள் டோக்கன்கள் போன்ற மிகவும் பாதுகாப்பான விருப்பங்களைத் தேர்வு செய்யுங்கள். அவை எப்போதுமே SMS மூலம் பெறப்படும் OTP-களைவிடவும் பாதுகாப்பானதாக இருக்கும்.

வங்கி உங்கள் CVV, OTP, பின் எண், கார்டு எண், கடவுச்சொற்கள் போன்றவற்றை ஒருபோதும் கேட்காது என்பதை நினைவில் கொள்ளுங்கள். அதனால் அத்தகைய ரகசிய விவரங்களை யாருடனும் பகிர வேண்டாம்.

# கிரெடிட் கார்டு மோசடி

கிரெடிட் கார்டு மோசடிகள் ஒரு கண்ணாமூச்சி விளையாட்டை போன்றது. மோசடிக்காரர்கள், அவர்களின் மோசடி செய்யும் உண்மையான நோக்கத்தை மறைத்து, உங்களை ஏமாற்றி, உங்களையே உங்கள் கிரெடிட் கார்டு விவரங்களை கூறவைப்பார்கள்.
அவர்களது இத்தகைய மோசடி வலையில் சிக்காமல் இருக்க, பின்வரும் உதவிக்குறிப்புகளை எப்போதும் நினைவில்கொள்ளுங்கள்:

மோசடிக்காரர்களின் அடையாளத்தை சரிபாருங்கள்: மோசடிக்காரர்கள் உங்கள் வங்கி அல்லது பழக்கமான நிறுவனத்தை சேர்ந்தவர்கள் போல நாடகம் ஆடலாம். அவர்களின் சூழ்ச்சிகளை நம்பி அவர்களின் சதிவலையில் விழ வேண்டாம்; அவர்களின் அடையாளத்தை முழுமையாக சரிபாருங்கள்.

1i

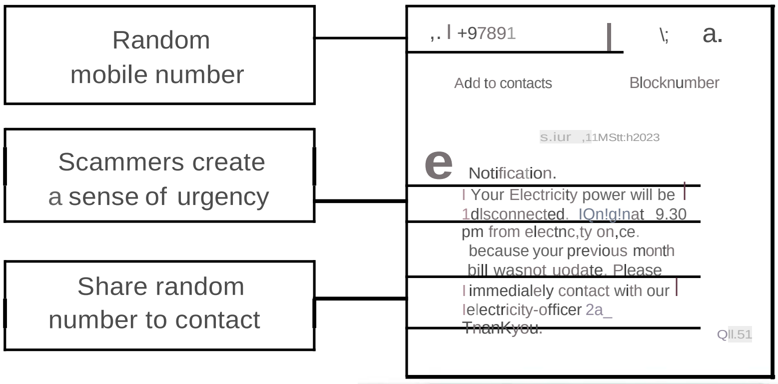
உங்கள் கணக்கு அறிக்கைகளை சரிபாருங்கள்: உங்கள் கிரெடிட் கார்டு கணக்கு அறிக்கைகளை தவறாமல் அடிக்கடி சரிபாருங்கள். நீங்கள் செய்திராத செலவுகள் அல்லது கட்டணங்களை உங்கள் கணக்கு அறிக்கையில் காண நேரிட்டால், அது மோசடிக்காரர்களின் கைவரிசையாக தான் இருக்க முடியும் - அம்மாதிரியான செலவுகள் செய்யப்படுவதை உடனே தடுத்திடுங்கள்.

பணப்பரிவர்த்தனை வரம்புகளை நிர்ணயித்திடுங்கள்: உங்களின் அனைத்து கட்டணச் முறைகளுக்கும் பணப்பரிவர்த்தனை வரம்புகளை உங்கள் தேவைக்கேற்ப நிர்ணயித்து, 'பயன்பாட்டை நிர்வகி' பகுதியை மூலம் அவற்றை அமைத்திடுங்கள். இதன்மூலம் ஒருவேளை உங்கள் ரகசிய விவரங்கள் மோசடிக்காரர்களிடம் சிக்கினாலும்கூட, அவர்கள் அதிக தொகையைத் திருட முடியாது.

பாதுகாப்பான தளங்களை மட்டுமே பயன்படுத்துங்கள்: நீங்கள் ஆன்லைனில் ஷாப்பிங் செய்யும்போது, அந்த ஷாப்பிங் வலைத்தளம் பாதுகாப்பானதா என்பதை உறுதிப்படுத்திக் கொள்ளுங்கள் (URL இல் "https" இருக்கிறதா என்பதைப் பார்க்கவும்). இவ்வாறு செய்வது நீங்கள் உங்கள் ரகசிய விவரங்கள் பாதுகாப்பாக இருப்பதைத் தேர்ந்தெடுப்பதற்குச் சமம்.

புதிய மோசடி யுக்திகள் பற்றி அறிந்துகொள்ளுங்கள்: விளையாட்டில் புதிய உத்திகளைக் கற்றுக்கொள்வது போலவே, சமீபத்திய மோசடி யுக்திகளைக் கண்காணியுங்கள். இதனால், நீங்கள் மோசடிக்காரர்களின் வலையில் சிக்காமல், அவர்களை நீங்கள் முட்டாள்களாக ஆக்கிவிட்டீர்கள்.

## போலியான SMSகளை கண்டறிவது எப்படி?



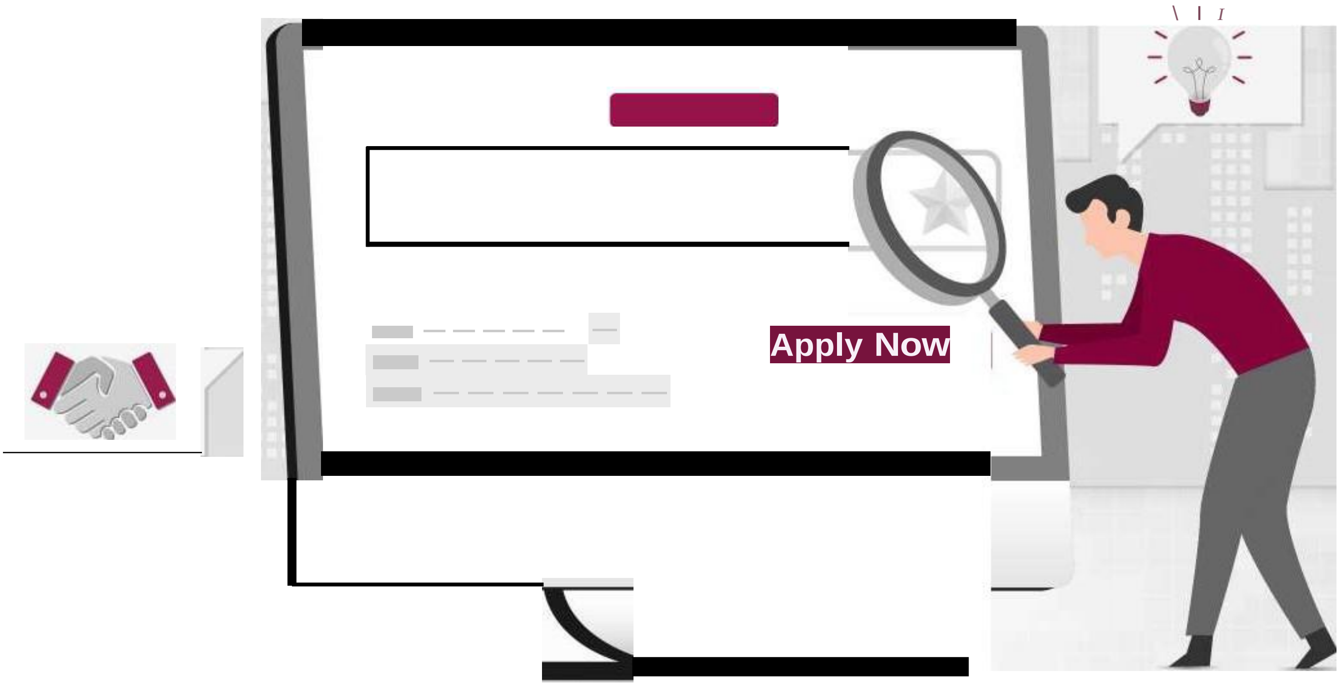
இவ்வாறு கற்பனை செய்யுங்கள்: நீங்கள் உங்கள் வீட்டில் ஓய்வாக அமர்ந்தபடி உங்களின் விருப்பமான ஷோக்களைப் பார்த்து மகிழும் நேரம், உங்கள் ஃபோனில் ஒரு குறுஞ்செய்தியைப் பெறுகிறீர்கள். அந்த குறுஞ்செய்தியை உங்கள் மின்சார வழங்குநர் அனுப்பியதாகவும், அதில் நீங்கள் உங்களின் சமீபத்திய மின்சார கட்டணமாக அதிகத் தொகை செலுத்த வேண்டியிருப்பதாக கூறுகிறார்கள்.
நீங்கள் இதை நினைத்து பதட்டம் அடையும்முன்: இது ஒரு மின்சாரக் கட்டண மோசடி, இதன் மூலம் மோசடிக்காரர்கள் ஒரு திருட்டுத்தனமான மாயத்தோற்றத்தை உருவாக்கி, முன்னறிவிப்பின்றி என்னை சுலபமாக ஏமாற்றிவிடுவார்கள் என்பதை நினைவில்கொள்ளுங்கள்.

F) LW உங்கள் ரகசிய விவரங்களை யாருடனும் பகிராதீர்கள் அல்லது தெரியாத இணைப்புகளைக் கிளிக் செய்யாதீர்கள்.

[!...-•! அதிகாரப்பூர்வ மற்றும் பாதுகாப்பான வலைத்தளங்களை மட்டுமே கட்டணம் செலுத்த ~~பயன்படு~~த்தடுத்துங்கள்.

அறியப்படாத புதிய/பதிவு செய்யப்படாத எண்கள் மூலம் தனிப்பட்ட விவரங்களையோ அல்லது கட்டணத்தையோ மின்சாரத்துறை ஒருபோதும் கேட்பதில்லை என்பதை நினைவில்கொள்ளுங்கள்.

# வேலைவாய்ப்பு மோசடிகள்




நீங்கள் வேலைவாய்ப்புப் பட்டியலை வரிசையாக பார்த்துக்கொண்டே வருகிறீர்கள் என்று கற்பனை செய்துகொள்ளுங்கள், திடீரென்று நீங்கள் ஒரு வேலைவாய்ப்பைக் கண்டு ஆச்சரியப்படுகிறீர்கள். அதன் விவரங்கள் உண்மையானதாக இருக்க முடியாதது போலத் தோன்றுகிறது. டேட்டா என்ட்ரி வேலைவாய்ப்பிற்கு வரம்பற்ற விடுமுறை நாட்கள், வீட்டிலிருந்தபடி சௌகரியமாக வேலை செய்தல், ஆறு இலக்கத்தில் சம்பளம் என நம்ப முடியாத பலன்கள். உடனே "பதிவு செய்யுங்கள்" எனக் கூறப்பட்டிருக்கிறது!
இப்போதே விண்ணப்பிக்கவும்" என்ற பட்டனை அழுத்துவதற்கு முன் சற்று நிதானமாக சிந்தியுங்கள்!

நிறுவனத்தை பற்றி ஆராயுங்கள்: நிறுவனத்தை பற்றி ஆன்லைனில் அலசி ஆராய்ந்து, அது நம்பகமானது என்பதை உறுதிப்படுத்திக்கொள்ளுங்கள். மோசடிக்காரர்கள் பெரும்பாலும் நம்பத்தகுந்த வலைத்தளங்கள் கொண்ட போலி நிறுவனங்களை உருவாக்குகிறார்கள். எனவே, நன்கு ஆராய்ந்து முடிவெடுங்கள்.

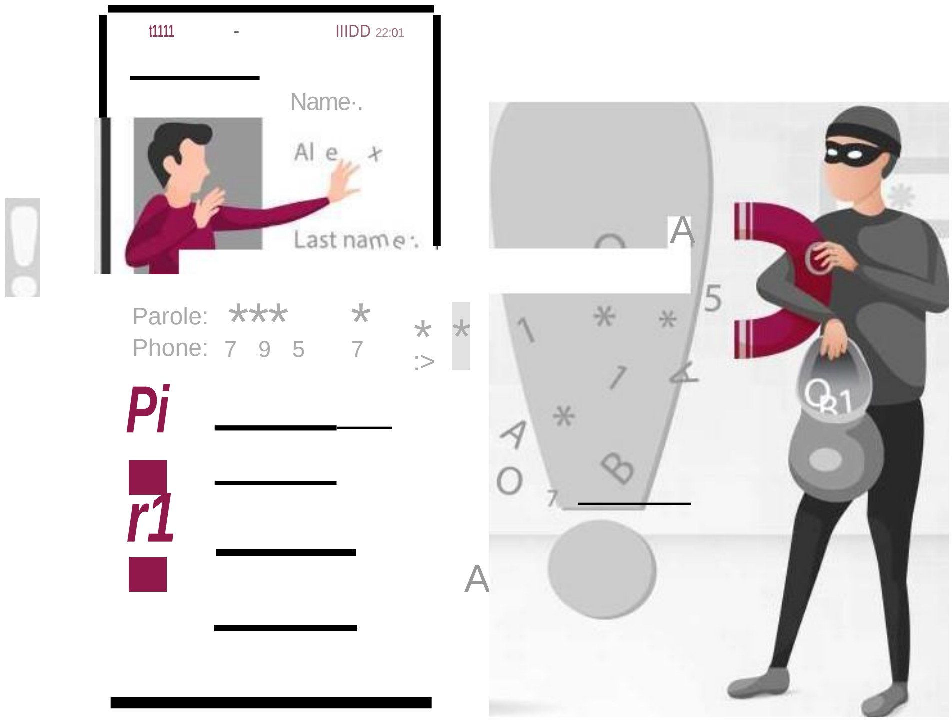
முன்கூட்டியே பணம் செலுத்தாதீர்கள்: உண்மையான வேலை வழங்குநர்கள் நீங்கள் வேலை செய்யத் தொடங்கும் முன் பயிற்சி அளிப்பது, தேவையான கற்றல் வளங்கள் அளிப்பது அல்லது பின்னணி சரிபார்ப்புகளைச் செய்ய பணம் செலுத்த வேண்டும் என உங்களிடம் கேட்க மாட்டார்கள்.

சந்தேகத்திற்குரிய விஷயங்களை கவனியுங்கள்: உங்களின் சமூகப் பாதுகாப்பு எண் அல்லது நிதி விவரங்கள் போன்ற முக்கியமான தகவல்களை உடனே வழங்க வேண்டும் என்று வேலைவழங்குநர்கள் கூறினால் எச்சரிக்கையாக இருங்கள்.
விரைவாக வேலைவாய்ப்பு அளிக்கப்படுதல்: நேர்காணல் இல்லாமல் அல்லது உங்களைப் பற்றி அதிக தகவல் பரிமாற்றம் இல்லாமல் உங்களுக்கு வேலை கிடைத்தால், அது ஒரு மோசடியாக இருக்கலாம்.

உங்கள் உள்ளுணர்வை நம்புங்கள்: ஏதோ ஒன்று சரியில்லாதது போல தெரிந்தால், உங்கள் உள்ளுணர்வை நம்பி எச்சரிக்கையுடன் தொடருங்கள் அல்லது அத்தகைய வேலைவாய்ப்பைத் தவிர்த்துவிடுங்கள்.

தேடும் போது உங்களின் தனிப்பட்ட மற்றும் நிதி விவரங்களைப் பாதுகாப்பது உங்களின் முதல் மையாக இருக்க வேண்டும் என்பதை நினைவில்கொள்ளுங்கள்.

# கால் ஸ்ஃபூபிங் மோசடிகள்

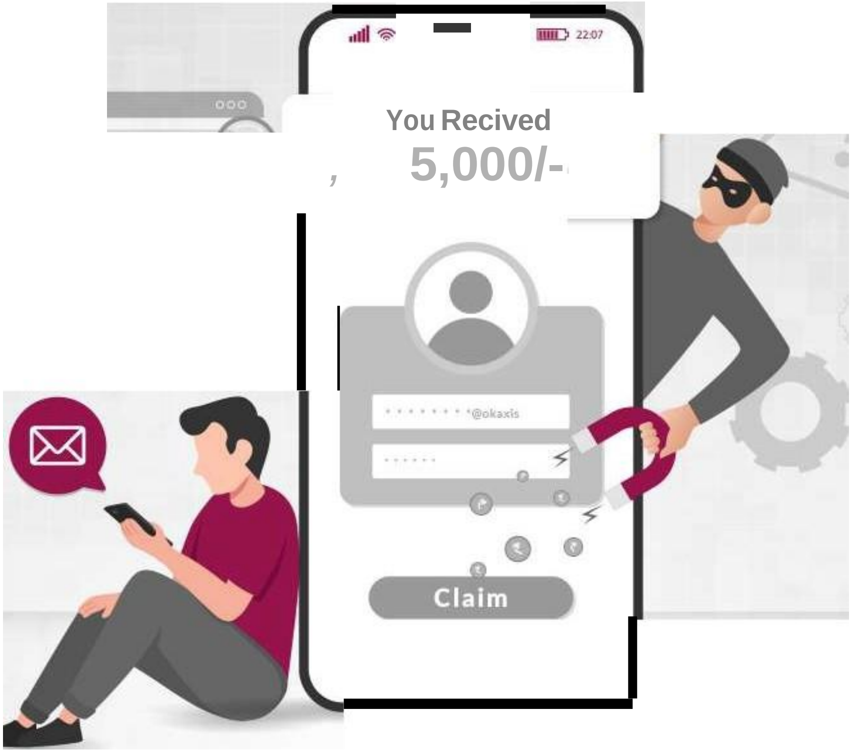



ஒரு மந்திரவாதி எப்படி உண்மையில்லா விஷயங்களை உண்மையென தோன்றச் செய்கிறாரோ, அதுபோலவே மோசடிக்காரர்கள் தங்கள் அழைப்பாளர் ஐடியை நீங்கள் நம்பக்க்கூடியதாக அடையாளபடுத்தி, அதாவது உங்களுக்குத் தெரிந்தவர்கள் அல்லது உங்களின் நம்பிக்கைக்குரியவர்கள் போல - எடுத்துக்கட்டிற்கு, உங்கள் வங்கியைப் போல தங்களை அடையாளப்படுத்திக்கொள்வர். இது அவர்களின் உண்மையான அடையாளத்தை மறைத்து, டிஜிட்டலாக மாறுவேடம் போட்டு மோசடியில் ஈடுபட உதவுகிறது.
இந்த தந்திரமான மோசடியிலிருந்து உங்களைப் பாதுகாத்துக்கொள்ள, பின்வரும் உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்:

எச்சரிக்கையுடன் சரிபாருங்கள்: அழைப்பாளர் ஐடி உங்களுக்கு ஏற்கனவே தெரிந்திருந்தால் கூட, எப்போதுமே ஒரு சந்தேகத்துடன் இருங்கள். யாரேனும் ரகசியத் தகவலைக் கேட்டால், வேறு வழிகள் மூலம் அவரது அடையாளத்தை ஒருமுறைக்கு இருமுறை சரிபாருங்கள்.
எச்சந்தர்ப்பத்திலும் தனிப்பட்ட தகவலை எவருடனும் பகிர வேண்டாம்: அழைப்பாளர் உங்களுக்கு நன்கு தெரிந்தவராக உங்களுக்குத் தோன்றினாலும், தனிப்பட்ட அல்லது நிதித் தகவலை தொலைபேசி மூலம் ஒருபோதும் பகிர வேண்டாம். நீங்கள் பெற்ற அந்த அழைப்பை துண்டித்துவிட்டு, அதே நபரை நீங்கள் பொதுவாக தொடர்புகொள்ளும் நம்பகமான எண்ணைப் பயன்படுத்தி மீண்டும் அழையுங்கள்.
தனிப்பட்ட தகவலை இணையத்தில் பகிராதீர்கள்: இணையத்தில் அல்லது சமூக ஊடகங்களில் நீங்கள் பகிரும் உங்களின் தனிநபர் விவரங்கள் குறித்து எச்சரிக்கையாக இருங்கள். மோசடிக்காரர்கள் தங்களின் ஏமாற்று அழைப்புகளை மிகவும் நம்பத்தகுந்ததாக மாற்ற இந்த ஊடங்கங்கள் மூலம் உங்கள் தனிநபர் தகவல்களை சேகரிக்கின்றனர்.
அழைப்புத் தடுப்பைப் பயன்படுத்தவும்: உங்கள் ஃபோன் கேரியர் வழங்கும் அழைப்புத் தடுப்பு செயலிக்கள் அல்லது அம்சங்களை பயன்படுத்துங்கள். அவை சாத்தியமான மோசடி அழைப்புகளை வடிகட்ட உதவும்.

கூகுள் அல்லது எந்த தேடுபொறியிலும் ஃபோன் எண்களைத் தேட வேண்டாம். நீங்கள் அவ்வாறு தேடினால், நிறுவனம் அல்லது வணிகரால் உங்களுக்கு அனுப்பப்பட்ட எந்த இணைப்புகளையும் ஒருபோதும் கிளிக் செய்ய வேண்டாம்.
கூடுதலாக, அங்கீகரிக்கப்பட்ட அப்ளிகேஷன் ஸ்டோர்களில் இருந்து மட்டுமே வங்கி செயலிக்களின் சமீபத்திய பதிப்புகள் உங்கள் சாதனங்களில் பதிவிறக்கம் செய்யப்பட்டிருப்பதை உறுதிசெய்யுங்கள்.
இதை அவ்வப்போது சரிபார்த்துக்கொள்ளுங்கள்.
நிஜ வாழ்க்கையில் முகமூடி அணிந்த அந்நியரை நீங்கள் நம்பாதது போல், உண்மையான அழைப்பு ஐடியை மறைத்து தொலைபேசி மூலம் உங்களைத் தொடர்புகொள்ளும் எவரையும் நம்பக்கூடாது என்பதை நினைவில்கொள்ளுங்கள். விழிப்புடன் இருங்கள்!

# UPI ரீஃபண்ட் மோசடிகள்



நீங்கள் உங்கள் ஃபோனை சாவகாசமாக ஸ்க்ரோல் செய்து கொண்டிருக்கும்போது, உங்களுக்கு UPI ரீஃபண்ட் ஒன்று இருப்பதாக அறிவிப்பு வருகிறது, உடனே நீங்கள் மிகவும் மகிழ்ச்சி அடைகிறீர்கள்! சற்று பொறுங்கள். இது ஒரு UPI ரீஃபண்ட் மோசடியாக இருக்கலாம்!

UPI அல்லது தி யூனிஃபைடு பேமெண்ட்ஸ் இன்டர்ஃபெஸ் என்பது நமது அன்றாட வாழ்க்கையின் ஒரு அங்கமாக மாறிவிட்டது. உங்கள் உள்ளூர் பெட்டிக்கடைகளில் பணம் செலுத்துவது முதல் ஃபோன்களுக்கு ரீசார்ஜ் செய்வது வரை விமான டிக்கெட்டுகளை முன்பதிவு செய்வது வரை பல்வேறு விஷயங்களுக்கு UPI பேமெண்ட்டைப் பயன்படுத்துகிறோம். UPI செயலிகளைப் பயன்படுத்தி மக்களை ஏமாற்றுவதற்காக மோசடிக்காரர்கள் பல புதிய முறைகளைப் பின்பற்றத் தொடங்கியுள்ளனர்.

அவர்களின் சட்டரீதியான சொற்கள் மற்றும் தொழில்முறை மொழிநடையை நம்பி ஒருபோதும் அவர்களின் மோசடி வலையில் விழ வேண்டாம். இம்மாதிரி மோசடிகளிலிருந்து தப்பிக்க பின்வரும் உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்:

இணைப்புகள் குறித்து ஜாக்கிரதையாக இருங்கள்: மோசடிக்காரர்கள் உங்களுக்கு ஒரு இணைப்பை அனுப்பலாம், பணத்தை ரீஃபண்ட் பெற நீங்கள் அதில் பதிவுசெய்யுமாறு வலியுறுத்துகின்றனர்.

அதிவிரைவாக செயல்படத் தூண்டும் தந்திங்கள்: உங்களுக்கு உடனே ரீஃபண்ட் வேண்டுமென்றால், நீங்கள் உடனே உங்கள் வங்கி விவரங்கள் அல்லது UPI பின் எண்ணை நிரப்புமாறு உங்களுக்கு அழுத்தம் கொடுப்பார்கள்.

உங்கள் ரீஃபண்ட் தகுதியைச் சரிபாருங்கள்: நீங்கள் நிஜமாகவே ரீஃபண்ட் பெறத் தகுதியானவரா என்பதை உறுதிப்படுத்துங்கள். ஆம் என்றால், அது நம்பகமான தகவலா என்பதை ஒருமுறைக்கு இருமுறை சரிபாருங்கள்.

வங்கியோ அல்லது பிற அதிகாரிகளோ இதுபோன்ற முக்கியமான விவரங்களை உங்களிடம் கேட்க மாட்டார்கள் என்பதை நினைவில் கொள்ளுங்கள்.

# ஃபிஷ்ஷிங் மோசடிகள்

நீங்கள் ஒரு தெளிந்த நீர் குளத்தில் நீந்தும் அமைதியான மீன் என்று கற்பனை செய்யுங்கள், நீங்கள் உங்கள் வேலையில் மட்டுமே கவனம் செலுத்துகிறீர்கள். திடீரென்று, ஒரு பளபளப்பான, கவர்ச்சிகரமான இரை கொண்ட தூண்டில் உங்கள் கண்முன் தொங்குகிறது. அது உங்கள் கவனத்தை ஈர்த்து உங்களை ஆர்வமடையச் செய்கிறது, ஆனால் சற்று பொறுங்கள் - ஏதோ சந்தேகத்திற்கிடமாக உள்ளது இல்லையா?!
டிஜிட்டல் உலகில் ஃபிஷிங் மோசடிகள் இப்படி தான் நிகழ்கிறது.

ஒரு மீன் தூண்டிலில் உள்ள இரையால் ஈர்க்கப்பட்டு மாட்டிக்கொள்வது போல, உங்களின் ரகசிய தகவல்களை உங்களை ஏமாற்றி பெற சைபர் குற்றவாளிகள் தங்களை நம்பகமான நபர்களாகக் காட்டிக்கொள்கிறார்கள். அவர்கள் வங்கிகள், சமூக ஊடகங்கள் அல்லது உங்கள் முதலாளி பின்பற்றும் அதே சாயலில் போலி மின்னஞ்சல்கள், செய்திகள் அனுப்புகின்றனர் அல்லது நம்பகமான வலைத்தளங்களைக் கொண்டுள்ளதாகக் தோன்றச்செய்கின்றனர்.
இம்மாதிரியான டிஜிட்டல் மோசடிகளில் நீங்கள் மாட்டிக்கொள்ளாமல் இருக்க, பின்வரும் உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்:

URLகளை இருமுறை சரிபாருங்கள்: நீங்கள் கிளிக் செய்யும் இணைப்பு உங்களை உண்மையாகவே எங்கே எடுத்துச்செல்லும் என்பதை அறிய, அதன் மீது ஒருசில வினாடிகள் உங்கள் மவுசை அசையுங்கள்.

தனிநபர் விவரங்களை யாருடனும் பகிராதீர்கள்: சட்டபூர்வமான நிறுவனங்கள் மின்னஞ்சல் வழியாக ரகசிய தகவல்களை ஒருபோதும் கேட்காது.

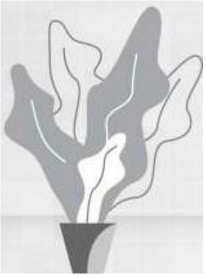
rl2J சந்தேகத்துடன் இருங்கள்: எதிர்பாராத கோரிக்கைகளைப் பெறுகிறீர்களா? செயல்படும் முன் வேறு வழிகளில் ஒன்றுக்கு இரண்டுமுறை சரிபாருங்கள்.

l@l:"\,. செக்கியூரிட்டி சாஃப்ட்வேரைப் புதுப்பியுங்கள்: உங்கள் டிஜிட்டல் விவரங்களை சமீபத்திய சாஃப்ட்வேர் பாதுகாப்புகள் மூலம் பாதுகாக்கவும்.

எச்சரிக்கையாக உள்ள மீனைப் போல, பரந்த இணைய உலகில் ஜாக்கிரதையாக இருந்து எவ்வித டிஜிட்டல் மோசடித் தூண்டிலிலும் மாட்டிக்கொள்ளாமல் புத்திசாலித்தனமாக நீந்தவும்!

# விஷ்ஷிங் மோசடிகள்

a



உங்கள் ஃபோனில் அழைப்பு வருகிறது, நீங்கள் அதை எடுத்து பேசுகிறீர்கள், அந்தப்பக்கம் உங்கள் வங்கி நிர்வாகி போல ஒருவர் பேசுகிறார், அவர் இது ஒரு ‘அவசர அழைப்பு’ என்று கூறி உங்கள் வங்கிக் கணக்கு யாரோ ஒருவரால் அணுகப்பட்டுவிட்டது என்று கூறுகிறார், அல்லது இது ஒரு ‘வெற்றிப்பரிசு அழைப்பு’ என்று கூறி இன்று உங்களுக்கு அதிர்ஷ்டமான நாள் நீங்கள் ஒரு மாபெரும் பரிசை வென்றுள்ளீர்கள் என்று கூறுகிறார்!
அப்படி அவர் சொல்ல நீங்கள் கேட்டால், அந்த அழைப்பை அப்படியே துண்டித்து விடுங்கள்! (சற்றும் சிந்திக்காமல்)

அத்தகைய மோசடிகளிலிருந்து பாதுகாப்பாக இருக்க, பின்வரும் உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்:

I

உங்கள் தனிநபர் விவரங்களை ஃபோன் மூலம் யாருடனும் பகிராதீர்கள்

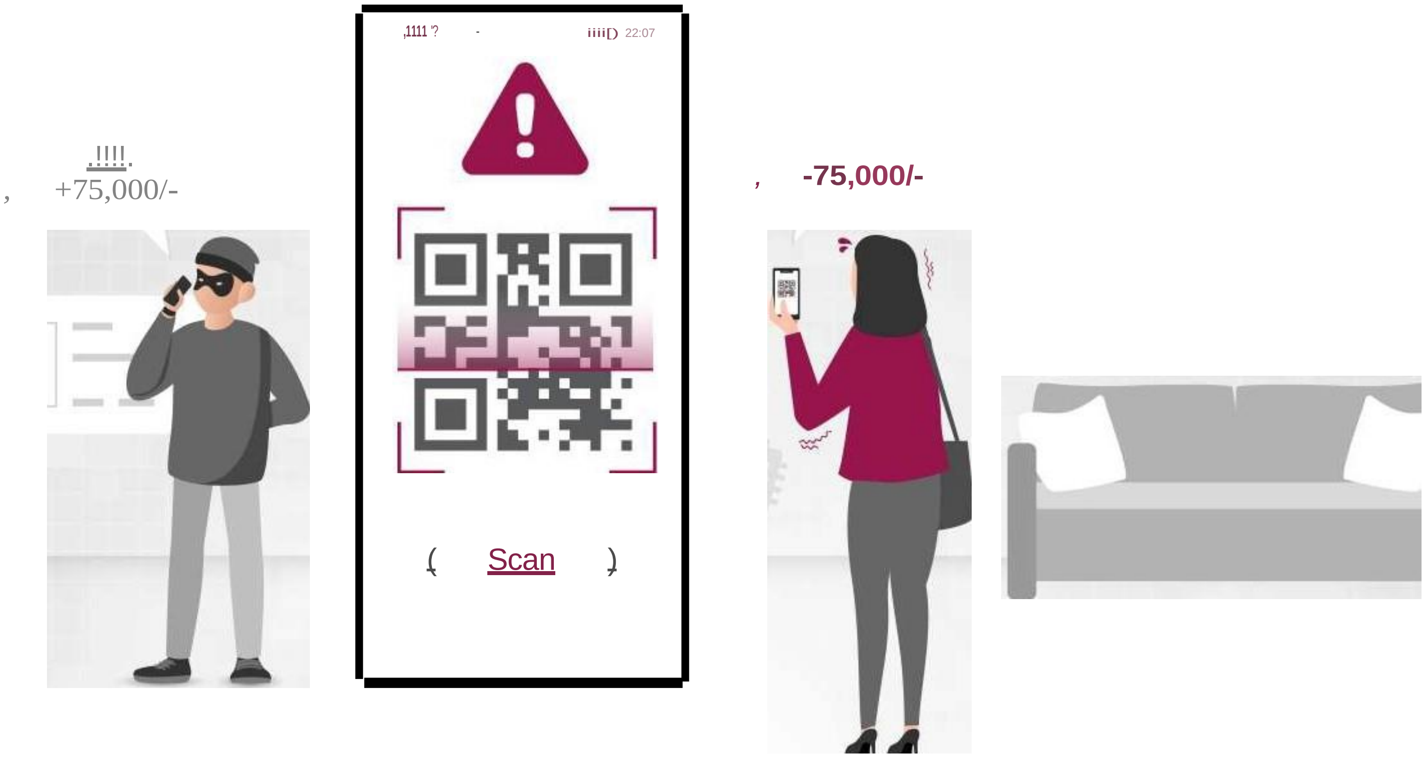
,..,
<@)>
L .J

துப்பறியும் புலியாக இருந்து, அழைப்பாளரின் அசல் அடையாளத்தை சரிபாருங்கள்

எப்படிபட்ட அவசர நிலையை உருவாக்கினாலும், அமைதியாக இருந்து சிந்தித்து செயல்படுங்கள்.

ஆன்லைனில் அந்நியர்களுடன் ரகசியத் தகவலைப் பகிர்வதில் கவனமாக இருக்க நினைவில்கொள்ளுங்கள் - உங்கள் விவரங்களைப் பாதுகாப்பாக வைத்திருக்க சாமர்த்தியமாக இருங்கள்!

# UPI மோசடிகள் - பணம் பெறுவதற்கான கோரிக்கை மோசடி




சினேகா தனது ஃபர்னிச்சரை ஆன்லைல் வாங்கும் மற்றும் விற்கும் செயலியில் விளம்பரப்படுத்தினார். அதை வாங்க விருப்பமுள்ளதாக தெரிவித்த நபர் ஒருவர், தான் துணை ராணுவப் படையில் உள்ளதாகக் கூறிக்கொண்டு, வாட்ஸ்அப் மூலம் பணம் செலுத்துவதற்காக QR குறியீட்டை அனுப்பயுள்ளார். பணத்தை உடனே பெற ஸ்னேகா அந்த QR குறியீட்டை ஸ்கேன் செய்து பார்த்துள்ளார், ஸ்கின் செய்தவுடன் 75,000 பணத்தை இழந்தார்.

இது எங்கோ கேட்டது போல உள்ளதா? நீங்கள் அடிக்கடி UPI பேமெண்ட் பிளாட்ஃபார்ம்களைப் பயன்படுத்துவதால், UPI மோசடிக்கு ஆளாகிவிடுவோமோ என்று பயப்படுகிறீர்களா?

எப்போதும் நினைவில்கொள்ளுங்கள்:

பணத்தைச் செலுத்த மட்டுமே UPI பின் எண் தேவைப்படும், ஒருபோதும் பணம் பெற UPI பின் எண் தேவைப்படாது

நீங்கள் பணத்தைப் பெற உங்கள் UPI பின் கேட்கப்பட்டால், உடனே அந்தப் பரிவர்த்தனையை நிறுத்துங்கள்! ஏனெனில் உண்மையில் அது பணத்தை நீங்கள் பெறாமல் செலுத்துவதற்கான கோரிக்கையாக இருக்கலாம்.

உங்கள் OTP, UPI பின் அல்லது எந்த ரகசிய விவரங்களையும் யாருடனும் பகிராதீர்கள்.

எந்தவொரு பணத்தொகையைச் செலுத்தத் தொடங்கும் முன், UPI செயலியில் உள்ள மொபைல் எண் மற்றும் பெயரை எப்போதும் சரிபாருங்கள்.

**QR குறியீடு ஸ்கேன் மோசடி**

பேமெண்ட் செயலிக்களில் QR குறியீடுகளை எச்சரிக்கையுடன் ஸ்கேன் செய்யுங்கள்; பணப் பரிமாற்றங்களுக்கான கணக்கு விவரங்கள் அவற்றில் உள்ளன.

பணத்தைப் பெற QR குறியீடுகளை ஸ்கேன் செய்ய வேண்டாம்; பார்கோடுகள் / QR குறியீடுகளை ஸ்கேன் செய்வது அல்லது மொபைல் பேங்கிங் பின் (m-PIN), கடவுச்சொற்கள் போன்றவற்றை உள்ளிடுவது பணத்தைப் பெறுவதற்கான பரிவர்த்தனைகளில் தேவையில்லை.

புரிந்துக்கொள்ளமுடியாத பதற்றம் அல்லது அவசரத்தைத் தூண்டும் வாங்குபவர்/விற்பவர் பெரும்பாலும் மோசடிக்காரராக இருக்கலாம். எனவே அமைதியாக இருங்கள், எப்பொழுதும் பணப்பரிவர்த்தனை பற்றித் தெளிவுபடுத்திக்கொள்ளுங்கள் மற்றும் சரியான கேள்விகளைக் கேளுங்கள்.

# அங்கீகரிக்கப்படாத மொபைல் செயலி மோசடிகள்

நீண்ட காலமாக நீங்கள் அறிந்திருந்த உங்கள் அத்தை மகன் போன்ற ஒரு உறவினர் ஒருத்தரிடமிருந்து, உங்களுக்குப் பிடித்த அங்கீகரிக்கப்பட்ட நிறுவனத்திடமிருந்து முறையான செயலி போல இருக்கும் இணைப்புடன் ஒரு SMS, மின்னஞ்சல் அல்லது செய்தியைப் பெறுகிறீர்கள்.
ஒரு நிமிடம் பொறுமையாக சிந்தியுங்கள்! இவை நம்பகமான பதிவிறக்கங்கள் இல்லை; அவை உங்களை டிஜிட்டல் மோசடிக்கு உள்ளாக்கும் அழைப்பிதழ்கள்!
மோசடி செய்பவர்கள் எஸ்எம்எஸ், மின்னஞ்சல் அல்லது சமூக மோசடிக்காரர்கள் ஊடகங்கள் வழியாக போலியான செயலிக்களின் இணைப்புகளை அனுப்புகிறார்கள். பயனர்களை இந்த இணைப்புகளைக் கிளிக் செய்யும்படி தூண்டப்படுகின்றன, இது அவர்கள் அறியாத செயலிக்களின் பதிவிறக்கத்திற்கு வழிவகுக்கிறது. இம்மாதிரி செயலிக்கள் நிறுவப்பட்டதும், ரகசியத் தகவல் மற்றும் OTPகள் உட்பட, மோசடிக்காரர்கள் உங்கள் சாதனத்திற்கான அணுகலையும் பெறுவார்கள்.

அறியப்படாத இடங்களிலிருந்து அல்லது அந்நியர்களின் வேண்டுகோளின் பேரில் செயளிக்களைபி பதிவிறக்குவதை அடியோடு தவிர்த்திடுங்கள்.

செயலிக்களை பதிவிறக்கும் முன் செயலி வெளியீட்டாளர்கள் மற்றும் பயனர் மதிப்பீடுகளைச் சரிபாருங்கள்.

அனுமதிகள் மற்றும் செயலி பயன்பாட்டு கோரிக்கைகளை (எ.கா. தொடர்புகள், புகைப்படங்கள்) மதிப்பாய்வு செய்து தேவயானவற்றிற்கு மட்டுமே அனுமதி வழங்குங்கள்.

வங்கியோ அல்லது பிற அதிகாரிகளோ இதுபோன்ற ரகசிய விவரங்களை உங்களிடம் கேட்க மாட்டார்கள் என்பதை நினைவில்கொள்ளுங்கள்,

## ATM கார்டு ஸ்கிம்மிங் மோசடி

டிஜிட்டல் பிக்பாக்கெட் என்று ஏடிஎம் ஸ்கிம்மிங்கை நினைத்துக்கொள்ளுங்கள். பணத்தை எடுக்க அல்லது உங்கள் கணக்கு இருப்பைச் சரிபார்க்க நீங்கள் ATM ஐப் பயன்படுத்தும் போது, மோசடிக்காரர்கள் உங்கள் கார்டு பின் தகவலைப் அறிந்துகொள்ள, ATM இயந்திரத்தில் மறைக்கப்பட்ட சாதனங்களை அமைக்கின்றனர். இந்த சாதனங்கள் ஒரு போலி கார்டு ஸ்லாட் அல்லது ஒரு சிறிய கேமரா போன்ற கண்ணுக்குத் தெரியாததாக இருக்கலாம்.

**ATM ஐ நன்றாக நோட்டமிடுங்கள்:** ATM ஐப் பயன்படுத்துவதற்கு முன், கார்டு ஸ்லாட் மற்றும் கீபேடில் ஏதேனும் அசாதாரண இணைப்புகள், தளர்வான பாகங்கள் அல்லது மறைக்கப்பட்ட கேமராக்கள் உள்ளனவா என எப்போதும் சரிபாருங்கள்.

**பின் எண்ணை மறைத்து பயன்படுத்துங்கள்:** உங்கள் பின் எண்ணை உள்ளீடும்போது உங்கள் கை அல்லது உடலால் மறைத்துக்கொள்ளுங்கள், இதனால் கேமராக்கள் அல்லது பார்வையாளர்கள் அதைப் பார்ப்பதற்குக் கடினமாக இருக்கும்

**கணக்கு அறிக்கைகளை தவறாமல் சரிபாருங்கள்:** உங்கள் வங்கிக் கணக்கு அறிக்கைகள் மற்றும் பரிவர்த்தனைகளை கண்காணியுங்கள். அவற்றில் நீங்கள் அறிந்திராத பரிவர்த்தனை செயல்பாடுகளைக் கண்டால் உடனடியாக உங்கள் வங்கிக்குத் தெரிவியுங்கள்

**அழைப்புகளின்போது ஜாக்கிரதையாக இருங்கள்:** உங்கள் வங்கியில் இருந்து அழைப்பதாகக் கூறிக்கொண்டு யாராவது உங்களின் ரகசிய தகவல்களைக் கேட்டால், எச்சரிக்கையாக இருங்கள். வங்கிகள் ஃபோன் மூலம் பின் எண்களையோ முழு கார்டு எண்களையோ கேட்பதில்லை

**பாதுகாப்பான ATMகளைப் பயன்படுத்துங்கள்:** நன்கு வெளிச்சம் உள்ள பகுதிகள் அல்லது வங்கிக் கிளைகளுடன் இணைக்கப்பட்டுள்ள ATMகளைப் பயன்படுத்துங்கள், ஏனெனில் அவை சேதமடைந்திருப்பதற்கான வாய்ப்பு குறைவு

சமீபத்திய மோசடித் தகவல் பற்றி அறிந்துகொள்ளுங்கள்: டிஜிட்டல் மோசடிகளிலிருந்து உங்களைச் சிறப்பாகப் பாதுகாத்துக் கொள்வதற்காக, சமீபத்திய மோசடிகள் மற்றும் மோசடி யுக்திகள் பற்றி தொடர்ந்து அறிந்துகொண்டேயிருங்கள்.

விழிப்புடன் இருந்து, இந்த உதவிக்குறிப்புகளைப் பின்பற்றுவது, ATM கார்டு ஸ்கிம்மிங் மோசடிக்கு நீங்கள் பலியாவதைத் தவிர்க்கும் என்பதையும், உங்கள் நிதிகளைப் பாதுகாப்பாக வைத்திருக்கும் என்பதையும் நினைவில்கொள்ளுங்கள்.

# தொலைதூர அணுகல் மோசடி

மோசடிக்காரர்கள் வாடிக்கையாளர்களை திரை-பகிர்வு செயலியை பதிவிறக்கம் செய்ய தூண்டுகிறார்கள். அதன் மூலம், அவர்கள் உங்கள் சாதனத்திற்கான அணுகலைப் பெற்று, உங்களை உளவுபார்த்து, உங்கள் ரகசிய நிதி விவரங்களை திருடுவார்கள். பிறகு, திருடிய உங்கள் பணத்தைப் பயன்படுத்தி அவர்கள் ஜாலியாக ஷாப்பிங் செய்கிறார்கள்!
இத்தகைய மோசடிகளில் இருந்து தப்பிக்க, இந்த உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்:

**அழைப்பாளர்களைச் சரிபாருங்கள்:** உங்களுக்கு அழைப்பவரின் அடையாளத்தை, அவர்கள் பிரதிநிதித்துவப்படுத்துவதாகக் கூறும் நிறுவனத்தின் அதிகாரப்பூர்வ தொடர்புத் தகவலைச் சுயமாக நீங்களே தேடிப்பார்ப்பதன் மூலம், எப்போதும் இருமுறை சரிபாருங்கள்.

**அவசர முடிவுகளை எடுக்காதீர்கள்**: எவ்வித அழுத்தத்தின் பேரிலும், அவசர முடிவுகளை எடுக்க வேண்டாம். ரகசியத் தகவலை அணுகுவதற்கு அல்லது பகிர்வதற்கு முன் சிந்தித்துச் சரிபார்க்க உங்களுக்குத் தேவையான நேரத்தை எப்போதும் எடுத்துக்கொள்ளுங்கள்.

**உங்கள் சாதனங்களைப் பாதுகாத்திடுங்கள்:** சமீபத்திய பாதுகாப்பு செயல்முறைகளுடன் உங்கள் சாதனங்களைப் புதுப்பித்து வைத்திருங்கள், உங்களின் ஒவ்வொரு நிதிக் கணக்கிற்கும் வலுவான, தனித்துவமான கடவுச்சொற்களைப் பயன்படுத்துங்கள்.

**நீங்களே கற்றுக்கொள்ளுங்கள்:** பொதுவான மோசடிகள் மற்றும் தந்தி யுக்திகளைப் பற்றி அறிந்துகொள்ளுங்கள், அவை நிகழும்போது அவற்றை சுலபமாக உங்களால் அடையாளம் காண முடியும்.

**தனிநபர் தகவலைப் பாதுகாத்திடுங்கள்:** கோரிக்கையின் உண்மையான மற்றும் சட்டபூர்வமான தன்மை குறித்து உங்களுக்குத் தெரியாவிட்டால், ஃபோன், மின்னஞ்சல் அல்லது ஆன்லைனில் தனிநபர் அல்லது நிதி விவரங்களைப் பகிர்வது குறித்து எப்போதுமே எச்சரிக்கையாக இருங்கள். உங்கள் ரகசிய டிஜிட்டல் விவரங்களை அறிய முயற்சிக்கும் தொலைநிலை அணுகல் மோசடிக்காரர்களுக்கு எதிராக உங்கள் வெர்ச்சுவல் உலகக் கதவை எப்போதுமே பூட்டிவைத்து விழிப்புடன் இருங்கள்.

தயவுசெய்து கவனத்தில் கொள்ளுங்கள்- கருப்பு / வெற்று திரையை உங்கள் கணினி அல்லது ஃபோனில் நீங்கள் காண நேர்ந்தால், மேற்கொண்டு எவ்வித செயல்பாடுகளையும் செய்ய வேண்டாம். உங்கள் திரை மற்றவர்களுக்குத் தெரியும் என்பதற்கான அறிகுறியாக இது இருக்கலாம்.

# சிம் மாற்று மோசடிகள்

மோசடிக்காரர்கள் ஃபோன் திருட்டில் உங்களை சிக்கவைப்பதை கற்பனை செய்து பாருங்கள்! அவர்கள் உங்களைப் போல் நடித்து, உங்களின் ஃபோன் எண் கொண்ட சிம் கார்டைத் தொலைத்துவிட்டதாகக் கூறி, உங்கள் தொடர்பு எண்ணை அறிந்துகொள்கிறார்கள். அதன் மூலம், உங்கள் வங்கி அல்லது மின்னஞ்சல் போன்ற உங்கள் ஆன்லைன் கணக்குகளுக்கான அணுகலைப் பெற்று அவர்களின் கைவரிசையைக் கட்டிவிடுகின்றன!

சுவாப் மோசடியை தடுத்துநிறுத்துங்கள்! பின்வரும் உதவிக்குறிப்புகளை நினைவில்கொள்ளுங்கள்.

சிம் கார்டு அடையாள விவரங்களை யாருடனும் பகிர வேண்டாம்.

உங்கள் ஃபோனின் நெட்வொர்க் அணுகலைக் கண்காணியுங்கள்.

சிறிது நேரம் நெட்வொர்க் இல்லை என்றால், உங்கள் பெயரில் நகல் **சிம்கள்** உள்ளனவா என்பதைச் சரிபார்க்க உங்கள் ஆபரேட்டரைத் தொடர்புக்கொள்ளுங்கள்.

உங்கள் ரகசிய டிஜிட்டல் விவரங்களை அறிய முயற்சிக்கும் தொலைநிலை அணுகல் மோசடிக்காரர்களுக்கு எதிராக உங்கள் வெர்ச்சுவல் உலகக் கதவை எப்போதுமே பூட்டிவைத்து விழிப்புடன் இருங்கள்.

# மோசடியான பரிவர்த்தனையை எப்படி புகாரளிப்பது?

**www.axisbank.com**ஐப் பார்வையிடுங்கள் > ஆதரவு > 'எங்களை இங்கே அணுகவும்' பகுதிக்கு கீழே ஸ்க்ரோல் செய்யுங்கள் > எங்களுடன் பேசுங்கள் > 'மோசடி அல்லது சர்ச்சையைப் புகாரளிக்கவும்' என்பதைத் தேர்ந்தெடுங்கள் > மோசடியைப் புகாரளியுங்கள் > உங்கள் ட்ராப்-டவுன் கீழ்தோன்றும் பட்டியலில் இருந்து பொருத்தமான விருப்பத்தைத் தேர்வுசெய்யுங்கள்> அழைக்கவும் என்பதைக் கிளிக் செய்யுங்கள்

**ரிசர்வ் வங்கியிடம் புகாரளிக்க, https://cms.rbi.org.in ஐப் பார்வையிடுங்கள்**

**கட்டணமில்லா அழைப்பு எண்ணான** 14448 அழையுங்கள் (திங்கள் முதல் வெள்ளி வரை, தேசிய விடுமுறை நாட்களைத் தவிர்த்து, காலை 9:30 முதல் மாலை 5:15 வரை).

**எழுத்து மூலமாக புகாரளியுங்கள்:** 'மையப்படுத்தப்பட்ட ரசீது மற்றும் செயலாக்க மையம், 4வது தளம், இந்திய ரிசர்வ் வங்கி, துறை -17, சென்ட்ரல் விஸ்டா, சண்டிகர் - 160 017' என்ற முகவரிக்கு கடிதம்/அஞ்சல் அனுப்புங்கள். இதற்கு அனுப்புவதற்கான வடிவமைப்பை அறியவும், மேற்படி விவரங்களுக்கும் https://cms.rbi.org.in ஐப் பார்வையிடுங்கள்.

**சைபர் குற்றத்தைப் புகாரளிக்க,** உதவிஎண் 155260 **அல்லது** 1930 ஐ அழையுங்கள் அல்லது தேசிய சைபர் கிரைம் அறிக்கையிடல் போர்ட்டலில் **(www.cybercrime.gov.in)** நீங்கள் எதிர்கொண்ட சம்பவத்தைப் புகாரளியுங்கள்.