

TRENDING SCAMS | IN THE PAST WEEK

Issue

no. 12

9 June 2023

Scams to look out for



Job Scam

You receive a job offer promising high salary with little effort.

CHECK with official sources, such as the company's official website, to verify the job offer.



Fake Friend Call Scam

You receive a phone call from supposedly your "friend". You are asked to guess the caller's name and when you do so, the caller will assume this name. You are then asked to save the friend's new number. A few days later, this so-called friend will call you to ask for money to help him or her for an emergency, mother is in hospital etc.

CHECK with your friend through other means or call the original number to verify if indeed your friend had called you earlier.



Investment Scam

You are offered an investment with very high returns.

CHECK with official sources, such as the company's official website, to verify the deal. Do not be enticed by the initial positive gains. Do your own due diligence before you invest large sums of money.

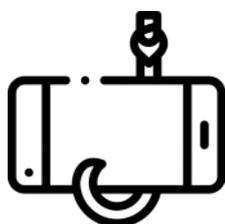


Banking-related phishing scam*

You receive a SMS claiming that your bank account has been suspended or that payment has been made from a new device. You are asked to click on a link to a fake banking login page that prompts you to provide your iBanking credentials, OTPs, or digital token approvals. Subsequently, unauthorised bank transactions would be made on your bank accounts.

CHECK for scam signs with official sources or websites and contact the banks only using the official contact numbers listed on the banks' official websites or numbers listed at the back of your debit/credit cards. Banks do not send out clickable links in SMSes and emails!

(You can find out more about this scam on Page 2)



Phishing Scam involving fake ScamShield app

You come across a deal for a product or service online. To facilitate payment, you are asked to click on a link and download an application from an unknown source. Subsequently, on the pretext of encouraging you to protect yourself against scams, a scammer impersonating a bank staff contacts you and asks you to install the fake ScamShield app via a URL link, and not from the official app stores.

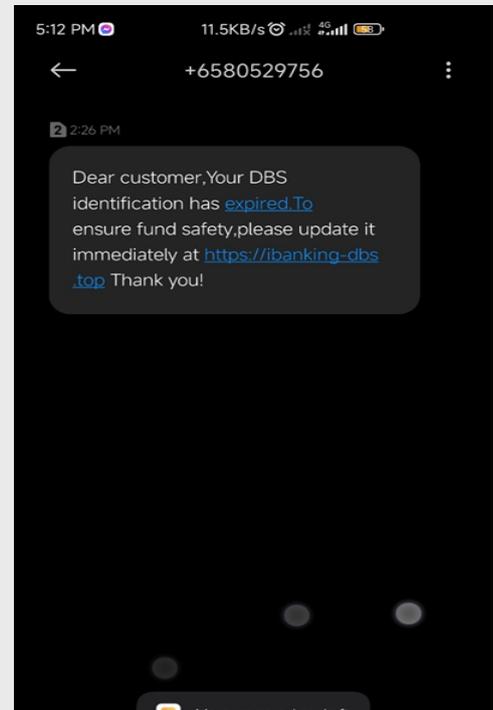
CHECK and ensure that you only download applications from the official application stores and not from any third-party or dubious sites.

* This scam is new to the top 5 as compared to the previous week.

Emerging Scam Trend

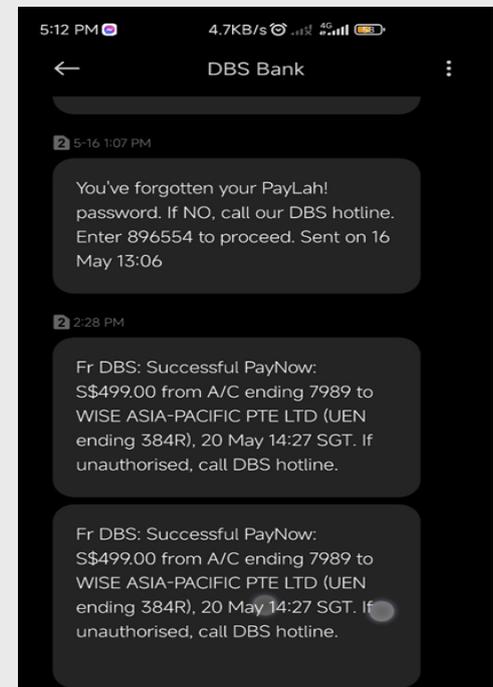
Be careful of fake SMSes from banks!

- Victims received SMSes claiming that their DBS PayLah! or online banking account has been suspended or payment has been made from a new device. Some of these phishing SMS messages may induce a sense of urgency by threatening to suspend the victim's account within an hour.
- These SMSes would provide a link to a fake banking login webpage.
- On the banking login webpage, victims would be prompted to provide their iBanking credentials, OTPs, or digital token approvals.
- Victims would realise they had been scammed when they discovered unauthorised transactions made from their bank accounts.



[Screenshot of a SMS with phishing link used by scammers]

- Banks will not send out SMSes with clickable links. Do not click on such links.
- Always check and verify the authenticity of the claims by contacting the banks directly.
- Never disclose your personal or internet banking details and OTP to anyone, even if they claim to be from the banks.
- Report any fraudulent transactions to your bank immediately.



[Screenshot of SMS notifying the user of unauthorised transactions made on their banking account]

How to protect yourself

I Can
ACT Against Scams



Remember to Add, Check and Tell (ACT) before making any decisions.

And never respond to urgent requests for information or money.

Always verify such requests with official websites or sources.

Get the latest advice. Visit www.scamalert.sg
or call the Anti-Scam Helpline at **1800-722-6688**.

Report scams. Call the Police Hotline at **1800-255-0000** or submit information online at www.police.gov.sg/iwitness. All information will be kept strictly confidential.



Download the free ScamShield app
Detect, block and report scams with the ScamShield app.



A crime prevention initiative by



In collaboration with



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

诈骗趋势

当心骗局



求职诈骗

您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。



假朋友来电

您接到来自“朋友”的电话。来电者在要求您猜他的姓名后会使用您所说的名字。来电者会要求您保存朋友的新电话号码。几天后，这所谓的朋友会拨电给您，以紧急事件或母亲住院等为由要求您提供经济援助。

通过其他沟通管道或原来的电话号码与您的朋友核实是否打电话给您。



投资诈骗

您收到了一项回报率非常高的投资机会。

查看官方消息，如公司的官方网站，以核实这笔交易。不要被初期的利润诱惑。在投入大笔资金前，请务必多加查证。



与银行相关的网络钓鱼诈骗*

您收到一则短信，声称您的银行账户已被冻结或已利用新设备付款。您被要求点击一个链接进入虚假的银行登录网页。网页提示您提供网上银行（iBanking）凭证、一次性密码（OTP）或密码生成器的批准。随后，您的银行账户将出现未经授权的银行交易。

查看官方消息或网站并注意诈骗迹象。只使用银行官方网站或借记卡/信用卡背面所列的官方联络号码与银行联系。银行不会在短信和电邮中发送可点击的链接！

（您可在第2页了解更多关于该骗局的详情）



涉及假ScamShield应用程序的钓鱼诈骗

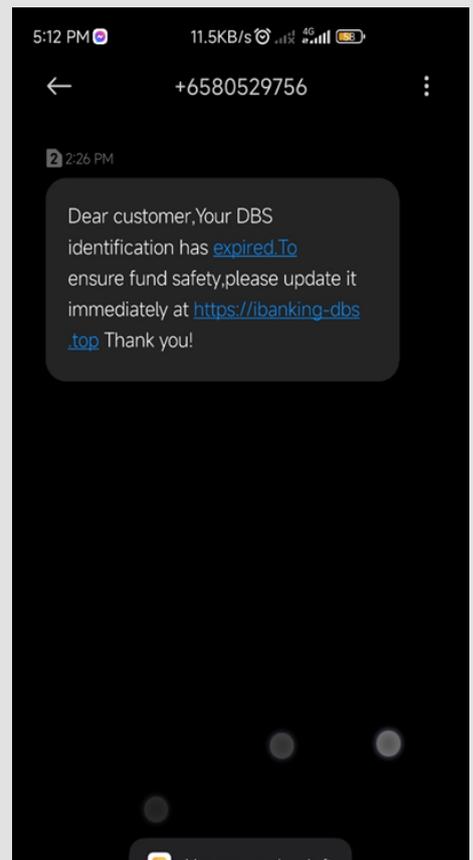
您在网上看到产品或服务的促销。为方便付款，您被要求点击一个链接并从一个未知来源下载一个应用程序。之后，骗子会冒充银行职员与您联系，以鼓励您保护自己免受诈骗为由，要求您通过网站链接安装假的ScamShield应用程序，而并非从官方应用程序商店下载。

检查并确保您只从官方应用程序商店下载应用程序，而不从任何第三方或可疑网站下载应用程序。

⚠️ 新兴诈骗趋势

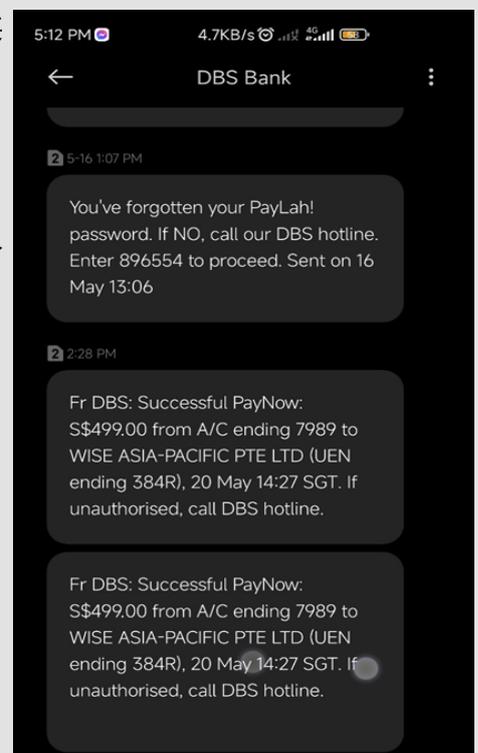
提防冒充银行的短信!

- 受害者收到短信，声称他们的星展银行PayLah! 应用程序或网上银行账户已被冻结或已利用新设备付款。一些钓鱼短信可能会威胁在一小时内冻结账户，从而引发紧迫感。
- 这些短信会提供一个链接把您带到虚假的银行登录网页。
- 在银行登录网页上，受害者被提示提供他们的网上银行（iBanking）凭证、一次性密码（OTP）或密码生成器的批准。
- 受害者发现他们的银行账户有未经授权的交易时意识到他们被骗了。



[骗子使用带有钓鱼网站链接的短信截图]

- 银行不会在短信中发送可点击的链接。切勿点击此类链接。
- 务必直接联系银行以检查并核实短信的真实性。
- 即使对方声称来自银行，切勿向任何人透露您的个人或网上银行资料和一次性密码（OTP）。
- 立即向银行举报任何欺诈性交易。



[通知用户银行账户有未经授权交易的短信截图]

⚠️ 如何保护自己

I Can
ACT Against Scams



在做任何决定前，请谨记下载、查看和告知(ACT)。

千万别回复紧急的信息或金钱要求。

时刻与官方网站或可靠的管道核实此类请求。

上网 www.scamalert.sg 或拨打反诈骗热线 1800-722-6688，获取最新的防范骗案信息。

通报诈骗。拨打警方热线 1800-255-0000 或上网 www.police.gov.sg/iwitness 向警方提供诈骗线索。所有资料都将保密。



下载免费的防诈骗应用ScamShield
使用ScamShield应用以侦测，阻止及通报诈骗。



防范罪案咨询由



以及



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

协力带给您

SEPANJANG MINGGU LEPAS

Penipuan yang harus diawasi



Penipuan Pekerjaan

Anda menerima satu tawaran pekerjaan yang menjanjikan gaji yang lumayan dengan usaha yang sedikit. **PERIKSA** dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran pekerjaan tersebut.



Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada kononnya seorang "kawan". Anda diminta supaya meneka nama si pemanggil dan apabila anda berbuat demikian, pemanggil akan menggunakan nama yang anda teka tersebut. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, pemanggil yang kononnya kawan anda ini akan menghubungi anda untuk meminta wang bagi menolongnya untuk suatu kecemasan, atau emaknya yang berada di hospital, dan sebagainya.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asalnya untuk memastikan dia benar-benar telah menelefon anda tadi.



Penipuan Pelaburan

Anda ditawarkan satu pelaburan dengan pulangan yang sangat tinggi.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut. Jangan tertarik dengan keuntungan awal yang positif. Lakukan pemeriksaan yang teliti dan wajar sebelum anda melaburkan wang dengan jumlah yang besar.



Penipuan pancingan data berkaitan perbankan*

Anda menerima satu SMS yang mendakwa bahawa akaun bank anda telah digantung atau pembayaran telah dibuat daripada satu peranti. Anda diminta supaya mengklik satu pautan halaman log masuk perbankan yang palsu yang meminta anda supaya memberikan butiran iBanking, OTP, atau kelulusan token digital anda. Seterusnya, transaksi bank tanpa kebenaran akan dibuat di akaun bank anda.

PERIKSA tanda-tanda penipuan dengan sumber-sumber atau laman-laman web rasmi dan hubungi pihak bank dengan hanya menggunakan nombor-nombor rasmi yang tersenarai di belakang kad debit/kredit anda. Pihak bank tidak menghantar pautan yang boleh diklik di SMS dan emel!
(Anda boleh mengetahui lebih lanjut tentang penipuan ini di Halaman 2)



Penipuan pancingan data yang membabitkan aplikasi ScamShield palsu

Anda ternampak satu tawaran untuk sebuah produk atau khidmat dalam talian.

Untuk memudahkan pembayaran, anda diminta supaya mengklik satu pautan dan memuat turun satu aplikasi daripada sumber yang tidak diketahui.

Selepas itu, seorang penipu yang menyamar dirinya sebagai seorang kakitangan bank, akan menghubungi anda dengan alasan bahawa dia ingin menggalakkan anda melindungi diri anda daripada penipuan. Dia akan meminta anda memasang aplikasi ScamShield palsu melalui satu pautan URL, dan bukan daripada gedung aplikasi rasmi.

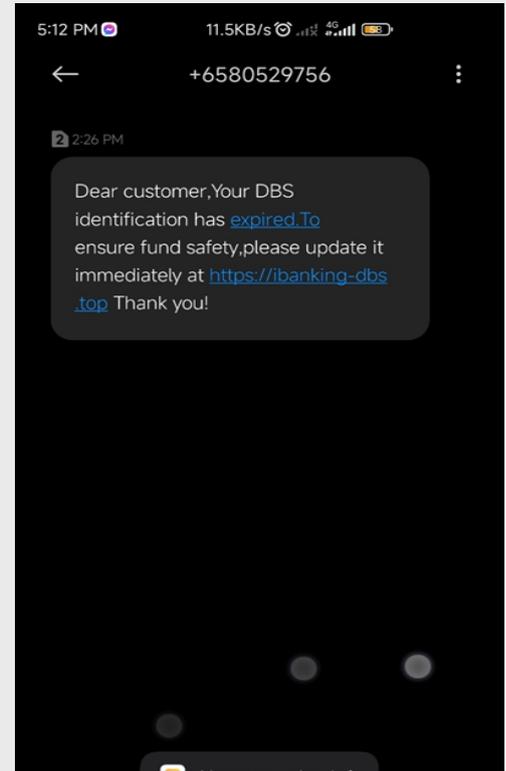
Periksa dan pastikan yang anda hanya memuat turun aplikasi daripada gedung aplikasi rasmi dan bukan daripada sebarang laman web pihak ketiga atau yang meragukan.

*Penipuan ini adalah yang baharu untuk 5 teratas berbanding dengan minggu sebelumnya.

Trend Penipuan yang Baru Muncul

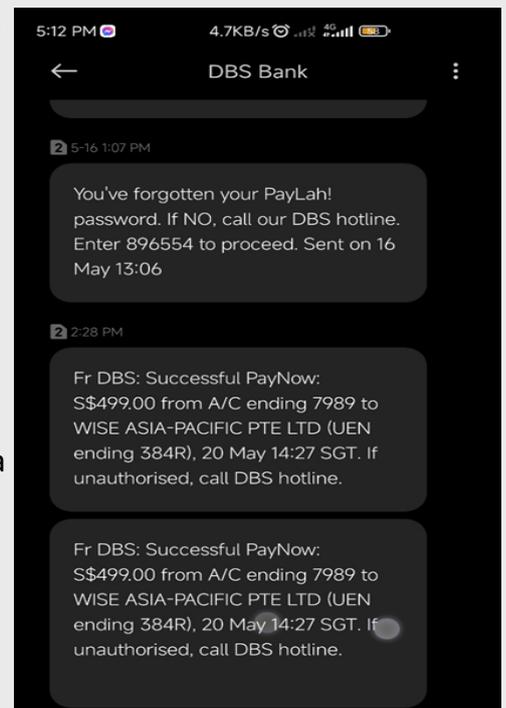
Berhati-hati dengan SMS palsu daripada pihak bank!

- Para mangsa menerima SMS-SMS yang mendakwa DBS PayLah! atau akaun perbankan dalam talian mereka telah digantung atau bayaran telah dibuat daripada satu peranti. Sesetengah daripada pesanan-pesanan SMS pancingan data ini boleh mendorong rasa terdesak dengan mengancam untuk menggantung akaun mangsa dalam masa satu jam.
- SMS-SMS ini akan memberikan satu pautan ke halaman web log masuk perbankan yang palsu.
- Di halaman web log masuk perbankan tersebut, mangsa-mangsa akan diminta supaya memberikan butiran iBanking, OTP, atau kelulusan token digital mereka.
- Mangsa-mangsa akan menyedari bahawa mereka telah ditipu apabila mereka menemui transaksi tanpa kebenaran yang dibuat daripada akaun-akaun bank mereka.



[Tangkap layar satu SMS dengan pautan pancingan data yang digunakan oleh penipu]

- Pihak bank tidak akan menghantar SMS dengan pautan yang boleh diklik. Jangan klik pautan sedemikian.
- Selalu periksa dan sahkan ketulenan dakwaan-dakwaan tersebut dengan menghubungi terus pihak bank.
- Jangan sesekali mendedahkan butir-butir peribadi atau perbankan internet dan OTP anda kepada sesiapa pun, walaupun mereka mendakwa mereka daripada pihak bank.
- Laporkan sebarang transaksi menipu kepada bank anda dengan segera.



[Tangkap layar satu SMS memaklumkan penggunaanya tentang transaksi tanpa kebenaran yang dibuat ke atas akaun bank mereka]

Bagaimana melindungi diri anda

I Can
ACT Against Scams



Ingatlah untuk Masukkan (Add), Periksa (Check) dan Beritahu (Tell) atau ACT sebelum membuat sebarang keputusan.

Dan jangan membalas sebarang permintaan mendesak untuk maklumat atau wang. Pastikan selalu kesahihan permintaan-permintaan tersebut daripada laman-laman web atau sumber-sumber rasmi.

Dapatkan nasihat terkini. Lawati www.scamalert.sg atau hubungi Talian Bantuan Anti-Penipuan di **1800-722-6688**.

Adukan penipuan. Panggil Talian Hotline Polis di **1800-255-0000** atau hantarkan maklumat dalam talian di www.police.gov.sg/iwitness. Semua maklumat akan dirahsiakan sama sekali.



Muat turun aplikasi percuma yang dipanggil ScamShield Kesan, sekat dan adu penipuan dengan aplikasi ScamShield.



Sebuah inisiatif pencegahan jenayah oleh



Dengan kerjasama



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

முன்னணி மோசடிகள்

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்



வேலை மோசடி

நீங்கள் சிறிதும் முயற்சி செய்யாமல், அதிக சம்பளம் வழங்குவதாக உறுதியளிக்கும் ஒரு வேலை வாய்ப்பைப் பெறுகிறீர்கள்.

வேலை வாய்ப்பை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும்.



போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். அவ்வாறு நீங்கள் செய்யும்போது, அழைப்பவர் நீங்கள் குறிப்பிட்ட பெயரை ஏற்றுக்கொள்வார். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, உங்கள் நண்பர் என்று தன்னை அறிமுகப்படுத்திக் கொண்ட இந்த நபர், அவசர நிலைமைக்கு அவருக்கு உதவ பணம் கேட்டு உங்களை அழைப்பார். ஒரு உதாரணத்திற்கு, அவரது தாயார் மருத்துவமனையில் இருக்கிறார் என்று கூறலாம்.

உங்கள் நண்பர் உங்களை சற்றுமுன் அழைத்திருந்தார்களா என்பதை மற்ற வழிகள் மூலமாகவோ அல்லது அவர்களின் அசல் எண்ணிலோ தொடர்புக்கொண்டு சரிபார்க்கவும்.



முதலீடு மோசடி

மிக உயர்ந்த வருவாய்யைக் கொண்ட ஒரு முதலீடு உங்களுக்கு வழங்கப்படுகிறது.

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். ஆரம்ப ஆதாயங்களைக் கண்டு கவர்ந்துவிடாதீர்கள். நீங்கள் ஒரு பெரியத் தொகையை முதலீடு செய்வதற்கு முன்பு உங்கள் சொந்த சோதனைகளை மேற்கொள்ளுங்கள்.



வங்கி பரிவர்த்தனை தொடர்பான தகவல் திருட்டு மோசடி*

உங்கள் வங்கிக் கணக்கு முடக்கப்பட்டுள்ளதாக அல்லது புதிய சாதனத்திலிருந்து பணம் செலுத்தப்பட்டதாகக் கூறும் குறுஞ்செய்தி உங்களுக்குக் கிடைக்கிறது. உங்கள் iBanking விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) அல்லது மின்னிலக்க டோக்கன் ஒப்புதல்களை வழங்க ஒரு போலி வங்கி உள்துறை பக்கத்தின் இணைப்பை கிளிக் செய்யும்படி நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்கள். அதனைத் தொடர்ந்து, அனுமதி அளிக்கப்படாத வங்கி பரிவர்த்தனைகள் உங்கள் வங்கிக் கணக்குகளில் செய்யப்படும். மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்கள் அல்லது இணையத்தளங்களுடன் சரிபார்க்கவும். வங்கிகளின் அதிகாரப்பூர்வ இணையத்தளங்களில் பட்டியலிடப்பட்டுள்ள அதிகாரப்பூர்வ தொடர்பு எண்கள் வாயிலாகவோ அல்லது உங்கள் பற்று / கடன்பற்று அட்டைகளின் பின்புறத்தில் பட்டியலிடப்பட்டுள்ள எண்கள் வாயிலாகவோ வங்கிகளை தொடர்பு கொள்ளுங்கள். கிளிக் செய்யக்கூடிய இணைப்புகளை குறுஞ்செய்திகள் மற்றும் மின்னஞ்சல்களில் வங்கிகள் அனுப்புவதில்லை!

(இரண்டாவது பக்கத்தில் இந்த மோசடி பற்றி மேலும் தெரிந்துகொள்ளலாம்)



போலி ஸ்கேம்ஷீல்ட் செயலி சம்பந்தப்பட்ட தகவல் திருட்டு மோசடி

இணையத்தில் ஒரு பொருள் அல்லது சேவைக்கான ஒப்பந்தத்தை நீங்கள் காண்கிறீர்கள். கட்டணம் செலுத்துவதற்காக, நீங்கள் ஒரு இணைப்பைக் கிளிக் செய்து, ஒரு செயலியைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். அதனைத் தொடர்ந்து, மோசடிகளிலிருந்து உங்களைப் பாதுகாத்துக்கொள்ள உங்களை ஊக்குவிக்கும் சாக்கில், வங்கி ஊழியரைப் போல் ஆன்மாறாட்டம் செய்யும் மோசடிக்காரர் உங்களைத் தொடர்புகொள்கிறார். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களுக்குப் பதிலாக, ஒரு இணையப்பக்க முகவரி வழியாக போலி ஸ்கேம்ஷீல்ட் செயலியை நிறுவுமாறு அவர் உங்களைக் கேட்டுக்கொள்கிறார்.

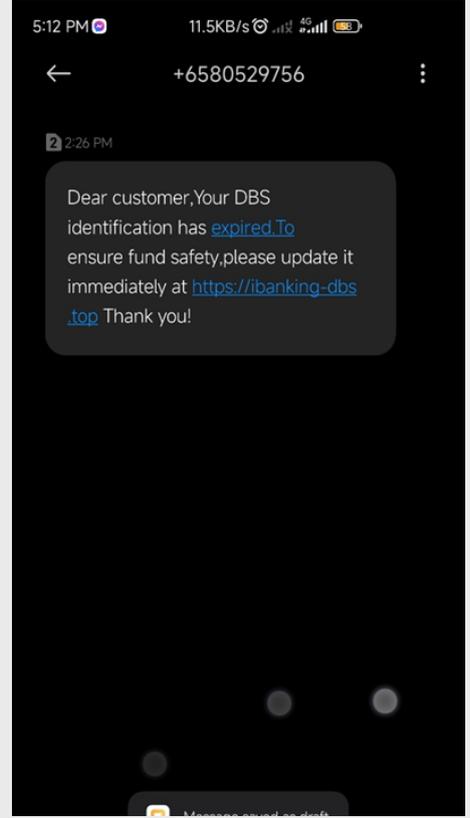
அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளை பதிவிறக்கம் செய்கிறீர்களா என்றும், எந்த மூன்றாம் தர்ப்பு அல்லது சந்தேகத்திற்குரிய தளங்களிலிருந்தும் அல்ல என்பதை சரிபார்த்து உறுதி செய்யுங்கள்.



வளர்ந்து வரும் மோசடிப் போக்கு

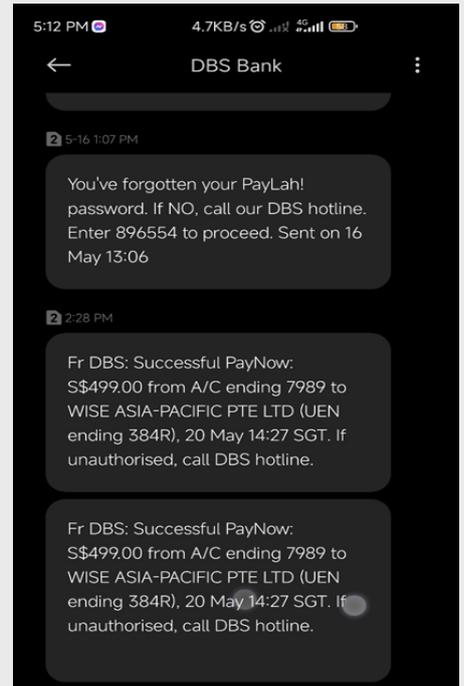
வங்கிகளில் இருந்து வருவதாகக் கூறும் போலி குறுஞ்செய்திகள் குறித்து கவனமாக இருங்கள்!

- தங்களது DBS PayLah! அல்லது இணைய வங்கிக்கணக்கு முடக்கப்பட்டுள்ளது அல்லது புதிய சாதனத்திலிருந்து பணம் செலுத்தப்பட்டுள்ளது என்று கூறும் குறுஞ்செய்தியைப் பாதிக்கப்பட்டவர்கள் பெற்றனர். சில தகவல் திருட்டு குறுஞ்செய்திகளில், ஒரு மணி நேரத்திற்குள் பாதிக்கப்பட்டவரின் கணக்கை முடக்கப் போவதாக மிரட்டுவதன் மூலம் பாதிக்கப்பட்டவர்களை அவசரப்படுத்தலாம்.
- இந்த குறுஞ்செய்திகள் ஒரு போலி வங்கி உள்நுழைவு வலைப்பக்கத்திற்கான இணைப்பை வழங்கும்.
- வங்கி உள்நுழைவு வலைப்பக்கத்தில், பாதிக்கப்பட்டவர்கள் தங்களது iBanking விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTP) அல்லது மின்னிலக்க டோக்கன் ஒப்புதல்களை வழங்குமாறு கேட்கப்படுவார்கள்.
- தங்கள் வங்கிக் கணக்குகளிலிருந்து அனுமதி அளிக்கப்படாத பரிவர்த்தனைகள் நடந்திருப்பதை கண்டுபிடிக்கும்போது தாங்கள் மோசடி செய்யப்பட்டிருப்பதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



[மோசடிக்காரர்கள் பயன்படுத்தும் தகவல் திருட்டு இணைப்பைக் கொண்ட குறுஞ்செய்தியின் ஸ்கிரீன்ஷாட்]

- கிளிக் செய்யக்கூடிய இணைப்புகள் கொண்ட குறுஞ்செய்திகளை வங்கிகள் அனுப்பாது. அத்தகைய இணைப்புகளைக் கிளிக் செய்ய வேண்டாம்.
- எப்போதும் வங்கிகளை நேரடியாகத் தொடர்புகொண்டு தகவல்களின் நம்பகத்தன்மையை சரிபார்க்கவும்.
- உங்கள் தனிப்பட்ட, இணைய வங்கிச் சேவை விவரங்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் (OTP) அவர்கள் வங்கிகளைச் சேர்ந்தவர்கள் என்று கூறினாலும் யாரிடமும் ஒருபோதும் வெளியிடாதீர்கள்.
- எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.



[தங்கள் வங்கிக் கணக்கில் செய்யப்பட்ட அனுமதி அளிக்கப்படாத பரிவர்த்தனைகளைப் பற்றி பயனருக்கு தெரிவிக்கும் குறுஞ்செய்தியின் ஸ்கிரீன்ஷாட்]

⚠ எப்படி உங்களைப் பாதுகாத்துக்கொள்வது

I Can
ACT Against Scams



எந்தவொரு முடிவையும் எடுப்பதற்கு முன்பு சேர்க்க, சரிபார்க்க மற்றும் சொல்ல (ACT) நினைவில் கொள்ளுங்கள்.

தகவல் அல்லது பணத்திற்கான அவசர கோரிக்கைகளுக்கு ஒருபோதும் பதிலளிக்காதீர்கள். அத்தகைய கோரிக்கைகளை அதிகாரபூர்வ இணையத்தளம் அல்லது ஆதாரங்களுடன் எப்போதும் சரிபார்த்துக்கொள்ளுங்கள்.

ஆக அண்மைய ஆலோசனையைப் பெறுங்கள். www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.

மோசடிகளை புகார் செய்யுங்கள். 1800-255-0000 என்ற காவல்துறை நேரடித் தொலைபேசி எண்ணை அழையுங்கள் அல்லது www.police.gov.sg/iwitness என்ற இணையதளத்தில் தகவல்களை சமர்ப்பிக்கலாம். அனைத்து தகவல்களும் ரகசியமாக வைத்திருக்கப்படும்.



ஸ்கேம்ஷீல்ட் செயலியை இலவசமாக பதிவிறக்கம் செய்யுங்கள்.
ஸ்கேம்ஷீல்ட் செயலியைப் பயன்படுத்தி மோசடிகளைக் கண்டறிந்து, தடுத்து, அவற்றைப் பற்றி புகார் செய்யுங்கள்.



ஒரு குற்றத் தடுப்பு முன்முயற்சி



இணைந்து வழங்குபவர்கள்



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY