TRENDING SCAMS IN THE PAST WEEK

Issue no. 05
21 April 2023

Scams to look out for

Fake Friend Call Scam

You receive a phone call from a "friend". You are asked to guess the caller's name. You are then asked to save their new number. A few days later, you are asked to provide financial assistance.

CHECK with your friend through other means or call their original numbers to verify if they were the ones who had called you earlier.

Job Scam

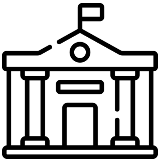
You receive a job offer promising high salary with little effort.

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

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.



Phishing Scam / SMS with Phishing Links*

You receive a text message claiming to be from a bank and you are asked to click on a link to provide your personal details. DO NOT provide your personal details and always contact the banks by using the official contact numbers listed on the banks' official websites or numbers listed at the back of your debit/credit cards.

ADD ScamShield app on your mobile phone to protect you from scam SMSes and blacklisted numbers. DO NOT click on links from suspicious SMSes or from senders you are not familiar.

E-Commerce Scam/ Global Fresh Series*

You see an unusually good deal through an advertisement on an online platform such as Facebook. The product is usually priced below market rates.

CHECK with official sources, such as the company's official website, to verify the deal. DO NOT act on impulse, always safer to check before you commit to any deal.

**4th and 5th ranked scams are new variants as compared to the week before.*

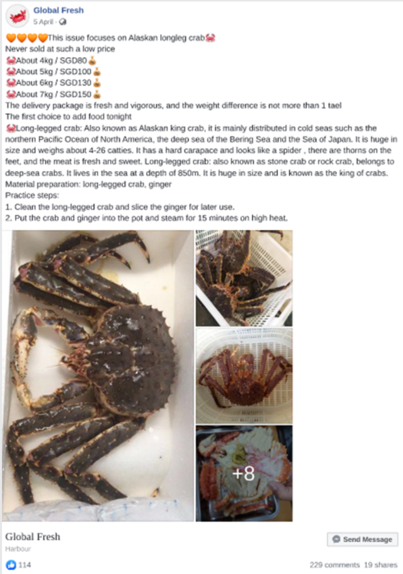
⚠ Not Really Selling Anything!

Scam Tactics

• Scammers pretending to be "sellers" would entice victims by posting offers or sponsored advertisement of food items on online platforms such as Facebook.

• Victims who came across the food deals on Facebook would contact the sellers via Facebook Messenger.

• After confirming the price and order details in Messenger, victims were told to make payment to the seller's bank account via PayNow or make bank transfers to bank accounts. Victims would only realise they have been scammed when they do not receive the goods and/or the "seller" becomes uncontactable. In some cases, victims were even given a pick-up location for self-collection at a non-existent shop.



[Screenshot of Facebook Post]

- **Add ScamShield app and set security features. Do not transfer money to anyone whom you do not know or have not met in person before.**

- **Check for scam signs and with official sources. If the price is too good to be true, it is likely a Scam! Purchase only from authorised sellers or reputable sources and be wary of time-sensitive deals due to limited stocks availability. This is how Scammers make you rush into a deal. Avoid making upfront payments to bank accounts and, whenever possible, avoid making advance payments or direct bank transfers to the seller. Always verify the seller's profile through customer reviews and ratings. Useful to also confirm if the seller has a valid business or shop front.**

- **Tell authorities, family, and friends about scams. Report the fraudulent pages to Facebook.**

How to protect yourself

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.

GET IT ON Google Play | Download on the App Store

A crime prevention initiative by

NATIONAL CRIME PREVENTION COUNCIL

In collaboration with

SINGAPORE POLICE FORCE

SAFEGUARDING EVERY DAY

过去一周

五号刊
2023年4月21日

诈骗趋势

当心骗局

假朋友来电

您接到来自“朋友”的电话。来电者要求您猜他的姓名。然后要求您保存他们的新电话号码。几天后，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。

求职诈骗

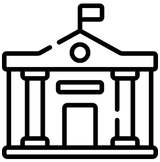
您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

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。



钓鱼骗局/含钓鱼链接的短信*

您收到一则自称来自银行的短信，并要求您点击一个链接以提供您的个人资料。请勿提供您的个人资料，并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。

在您的手机里下载ScamShield应用，以屏蔽诈骗短信及黑名单号码。请勿点击来自不熟悉发送者或可疑号码的链接。

电子商务骗局/ Global Fresh系列*

您在例如脸书的网络平台看见异常好的促销广告而通常此商品的售价低于市场价。

查看官方消息，如公司的官方网站，以核实该促销。请勿冲动行事，在决定交易之前，请务必多加查证。

*排名第4和第5的诈骗手法与上周手法类似。

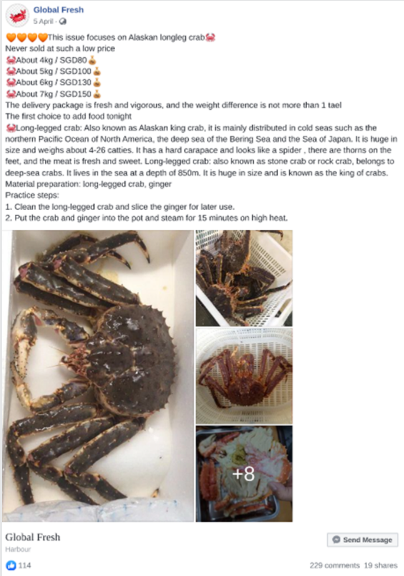
⚠ 其实没在卖！

诈骗手法

- 骗子会假扮“卖家”在网络平台（如脸书）通过赞助广告发布食品优惠诱骗受害者。

- 在脸书上看到食品促销的受害者会通过脸书联络卖家。

- 在脸书与卖家确认价钱和订单详情后，受害者会被要求通过PayNow或银行转账付款。他们只在没收到商品和/或无法联络“卖家”时才意识到自己被骗了。在一些案件里，受害者甚至被安排到一个不存在的商店里取货。



[脸书贴文截图]

- 下载ScamShield应用程序并设置安全功能。不要把钱转给不认识或素未谋面的人。

- 查看官方消息并注意诈骗迹象。如果价钱好得难以置信，那很有可能是骗局! 只向授权卖家或信誉良好的来源购买商品，并提防具时间限制的限量货源促销。这就是骗子诱使您尽快达成交易的方式。尽可能避免预付款项或预先通过银行转账给卖家。务必通过客户点评和评分来核实卖家的资料，及确认卖家拥有店面或实际营业。

- 告知当局、家人和朋友诈骗案件趋势。向脸书举报具欺诈性页面。

⚠ 如何保护自己

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或拔打反诈骗热线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。

GET IT ON Google Play
Download on the App Store

防范罪案咨询由
NATIONAL CRIME PREVENTION COUNCIL
以及
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY
协力带给您

TREND PENIPUAN SEPANJANG MINGGU LEPAS

Isu no.05
21 April 2023

Penipuan yang harus diawasi

Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada seorang “kawan”. Anda diminta supaya meneka nama si pemanggil. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, anda diminta supaya memberi bantuan kewangan.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asal kawan anda untuk memastikan mereka benar-benar telah menelefon anda tadinya.

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 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 / SMS dengan Pautan Pancingan Data*

Anda menerima satu mesej teks yang mendakwa ia datang daripada bank dan anda diminta supaya mengklik satu pautan untuk memberikan butir-butir peribadi anda. JANGAN berikan butir-butir peribadi anda dan sentiasa hubungi pihak bank dengan menggunakan nombor-nombor rasmi yang tersenarai di laman-laman web rasmi bank atau nombor-nombor yang tersenarai di belakang kad-kad debit/kredit anda.

MASUKKAN aplikasi ScamShield di telefon bimbit anda untuk melindungi diri anda daripada penipuan SMS dan nombor yang disenaraihitamkan. JANGAN klik pautan daripada SMS-SMS yang mencurigakan atau daripada penghantar yang tidak anda kenali.

Penipuan E-Dagang/ Siri Global Fresh*

Anda ternampak satu tawaran yang luar biasa bagusnya melalui sebuah iklan di sebuah platform dalam talian seperti Facebook. Produk tersebut biasanya berharga di bawah kadar pasaran.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut. JANGAN bertindak terburu-buru, sentiasa lebih selamat untuk memeriksa dahulu sebelum anda menerima tawaran tersebut.

**Penipuan peringkat ke-4 dan ke-5 adalah varian-varian baru berbanding dengan minggu sebelumnya.*

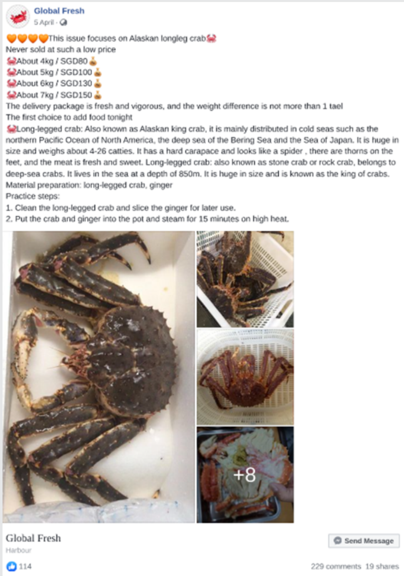
⚠ Sebenarnya tidak menjual apa-apa!

Taktik Penipuan

• Penipu yang berpura-pura sebagai “penjual” akan memikat mangsa dengan menghantar pos tawaran atau iklan-iklan barang makanan yang ditaja di platform dalam talian seperti Facebook.

• Mangsa yang ternampak tawaran makanan tersebut di Facebook akan menghubungi penjual melalui Facebook Messenger.

• Selepas pengesahan butir-butir harga dan pesanan di Messenger, mangsa akan diberitahu supaya membuat bayaran ke akaun bank penjual melalui PayNow atau membuat pemindahan bank ke akaun bank. Mangsa hanya akan menyedari bahawa mereka telah ditipu apabila mereka tidak menerima barangan tersebut dan/atau “penjual” tidak dapat dihubungi. Dalam beberapa kes, mangsa malah diberikan lokasi untuk pengambilan sendiri barangan di sebuah kedai yang tidak wujud.



[Tangkap layar di Pos Facebook]

- **Masukkan aplikasi ScamShield dan letakkan ciri-ciri keselamatan. Jangan pindahkan wang kepada sesiapa yang tidak anda kenali atau jumpa secara peribadi sebelum ini.**

- **Periksa tanda-tanda penipuan dan dengan sumber-sumber rasmi. Jika harganya terlalu baik untuk dipercayai, kemungkinan ianya merupakan Penipuan! Beli hanya daripada penjual yang sah atau sumber-sumber yang bereputasi dan berhati-hati dengan tawaran yang menarik dan sensitif masa di mana hanya ada stok yang terhad. Beginilah cara Penipu membuat anda tergesa-gesa membuat perjanjian. Elakkan membuat bayaran pendahuluan ke bank akaun dan, seberapa boleh, elakkan membayar wang pendahuluan atau pemindahan bank secara langsung kepada penjual. Sentiasa pastikan kesahihan profil penjual melalui ulasan dan penilaian pelanggan. Pastikan juga jika si penjual mempunyai perniagaan atau ruang depan kedai yang sah.**

- **Beritahu pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Adukan halaman-halaman yang palsu kepada Facebook.**

Bagaimana melindungi diri anda

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.

GET IT ON Google Play | Download on the App Store

Sebuah inisiatif pencegahan jenayah oleh

NATIONAL CRIME PREVENTION COUNCIL

Dengan kerjasama

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

கடந்த வாரத்தின் முன்னணி மோசடிகள்

வெளியீடு எண். 05
21 ஏப்ரல் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, நீங்கள் நிதி உதவி வழங்குமாறு கேட்டுக்கொள்ளப்படுகிறீர்கள்.

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

வேலை மோசடி

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

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

முதலீட்டு 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.

தகவல் திருட்டு மோசடி / தகவல் திருட்டு இணைப்புகளைக் கொண்ட குறுஞ்செய்தி*

நீங்கள் ஒரு வங்கியிலிருந்து வருவதாகக் கூறும் ஒரு குறுஞ்செய்தியைப் பெறுகிறீர்கள். உங்கள் தனிப்பட்ட விவரங்களை வழங்க ஒரு இணைப்பை கிளிக் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். உங்கள் தனிப்பட்ட விவரங்களை வழங்காதீர்கள். எப்போதும் வங்கிகளின் அதிகாரப்பூர்வ இணையத்தளங்களில் பட்டியலிடப்பட்டுள்ள அதிகாரப்பூர்வ தொடர்பு எண்கள் வாயிலாகவோ அல்லது உங்கள் பற்று / கடன்பற்று அட்டைகளின் பின்புறத்தில் பட்டியலிடப்பட்டுள்ள எண்கள் வாயிலாகவோ வங்கிகளை தொடர்பு கொள்ளுங்கள்.

மோசடி குறுஞ்செய்திகளிலிருந்தும் கறுப்புப் பட்டியலிடப்பட்ட எண்களிலிருந்தும் உங்களைப் பாதுகாத்துக்கொள்ள ஸ்கேம்ஷீல்ட் செயலியை உங்கள் கைத்தொலைபேசியில் சேர்த்துக்கொள்ளுங்கள். சந்தேகத்துக்குரிய குறுஞ்செய்திகளில் அல்லது உங்களுக்கு அறிமுகமில்லாதவர்களிடமிந்து வரும் இணைப்புகளை கிளிக் செய்ய வேண்டாம்.

மின் வணிக மோசடி/ 'Global Fresh' தொடர்*

ஃபேஸ்புக் போன்ற இணையத்தளத்தின் விளம்பரம் மூலம் வழக்கத்திற்கு மாறான ஒரு நல்ல ஒப்பந்தத்தைக் காண்கிறீர்கள். அந்த பொருள் சந்தை விலைகளைக் காட்டிலும் குறைவான விலையில் இருந்தது.

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். அவசரப்படாதீர்கள், வாங்குவதற்கு முன்பு எப்போதும் சரிபார்ப்பது நல்லது.

*4-வது மற்றும் 5-வது இடத்தில் உள்ள மோசடிகள், முந்தைய வாரத்துடன் ஒப்பிடும்போது புதிய வகைகளாகும்.

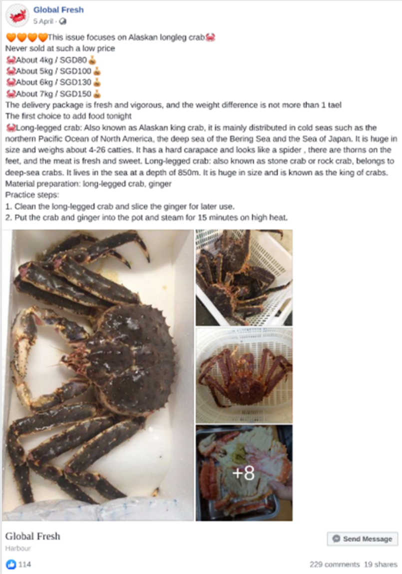
⚠ உண்மையில் எதையும் விற்பதில்லை!

மோசடி உத்திகள்

• ஃபேஸ்புக் போன்ற இணையத்தளங்களில் உணவுப் பொருட்கள் தொடர்பான சலுகைகளை அல்லது விளம்பரங்களை வெளியிட்டு "விற்பனையாளர்கள்" என்று பாசாங்கு செய்யும் மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களை வசீகரிப்பார்கள்.

• ஃபேஸ்புக்கில் உணவு ஒப்பந்தங்களைக் கண்ட பாதிக்கப்பட்டவர்கள், ஃபேஸ்புக் மெசஞ்சர் வழியாக விற்பனையாளர்களைத் தொடர்புகொள்வார்கள்.

• மெசஞ்சரில் விலை மற்றும் ஆர்டர் விவரங்களை உறுதிப்படுத்திய பின்னர், பாதிக்கப்பட்டவர்கள் 'PayNow' வழியாக விற்பனையாளரின் வங்கிக் கணக்கில் பணம் செலுத்துமாறு அல்லது வங்கிக் கணக்குகளுக்கு வங்கி மாற்றல்களைச் செய்யும்படி கூறப்பட்டனர். பாதிக்கப்பட்டவர்கள் பொருட்களைப் பெறாதபோதும், அல்லது "விற்பனையாளரை" தொடர்பு கொள்ள முடியாதபோதும் மட்டுமே, அவர்கள் மோசடி செய்யப்பட்டதை உணருவார்கள். சில சமயங்களில், பாதிக்கப்பட்டவர்கள் தங்கள் பொருட்களை பெற்றுக்கொள்வதற்கு இல்லாத ஒரு கடையின் முகவரி வழங்கப்பட்டது.



[ஃபேஸ்புக் பதிவின் ஸ்கிரீன்ஷாட்]

- ஸ்கேம்ஷீல்ட் செயலியைச் சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும். உங்களுக்குத் தெரியாத அல்லது நேரில் சந்திக்காத எவருக்கும் பணத்தை மாற்றிவிடாதீர்கள்.

- மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். விலை நம்ப முடியாததாக இருந்தால், அது ஒரு மோசடியாகத்தான் இருக்கும்! அங்கீகரிக்கப்பட்ட விற்பனையாளர்கள் அல்லது புகழ்பெற்ற இடங்களிலிருந்து மட்டுமே வாங்குங்கள். குறைந்த அளவில், ஒரு குறிப்பிட்ட காலத்திற்கு மட்டும் கிடைக்கும் ஒப்பந்தங்கள் குறித்து எச்சரிக்கையாக இருங்கள். இப்படித்தான் மோசடிக்காரர்கள் உங்களை அவசரப்படுத்துவார்கள். வங்கிக் கணக்குகளில் முன்பணம் செலுத்துவதைத் தவிர்த்து, முடிந்தவரை, முன்பணம் செலுத்துவதையோ அல்லது விற்பனையாளருக்கு நேரடி வங்கி மாற்றல்களையோ செய்வதைத் தவிர்க்கவும். வாடிக்கையாளர் மதிப்பாய்வுகள் மற்றும் தரமிடல்கள் மூலம் விற்பனையாளரின் சுயவிவரத்தை எப்போதும் சரிபார்க்கவும். விற்பனையாளருக்கு ஒரு செல்லுபடியான வியாபாரம் அல்லது கடை உள்ளதா என்பதை உறுதிப்படுத்துவது நல்லது.

- மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். மோசடி பக்கங்களை ஃபேஸ்புக்கிடம் புகார் செய்யுங்கள்.

⚠ 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.

GET IT ON Google Play | Download on the App Store

ஒரு குற்றத் தடுப்பு முன்முயற்சி
NATIONAL CRIME PREVENTION COUNCIL

இணைந்து வழங்குபவர்கள்
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY