

TRENDING SCAMS IN THE PAST WEEK

Issue
no.06
28 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.



E-Commerce/ Property Rental Scam*

You see a deal online for popular items, or property rental, that are priced below market rates.

CHECK with official sources, such as the company’s official website, to verify the deal.



Phishing Scams involving Malicious Applications*

You see a deal online and contacted the “seller”. You are asked to click on a link to download an application to make payment. DO NOT download the application, provide your personal details. Always contact the banks by using their official contact numbers listed on the banks’ official websites or numbers listed at the back of your debit/credit cards.

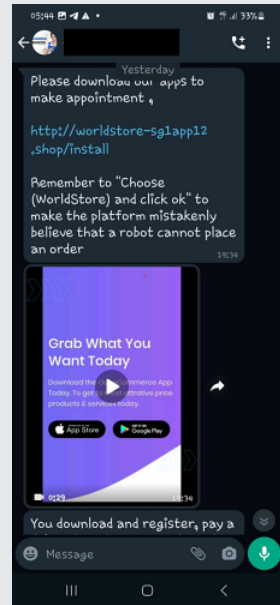
ADD ScamShield app on your mobile phone to protect you from scam SMSes and blacklisted numbers. DO NOT click on links from suspicious SMSes / WhatsApp/ Social Media Messaging Platforms from senders you are not familiar.

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

Beware of Malware!

Scam Tactics

- Victims would come across advertisements for home services or the sale of food items via their social media messaging platforms like Facebook and Instagram.
- Scammers contact victims via social media or WhatsApp and send a URL. Victims are asked to download an application from the URL to book services or buy food, and make payments.
- Victims enter i-banking and/or card details on fake banking login sites within the application to make payments. The application has malware that redirects credentials and OTPs to scammers. Victims only realise they have been scammed when unauthorized transactions or charges have been made on their accounts.



[Conversation between a scammer and victim on WhatsApp]

- **Add ScamShield app and set security features. Ensure that your devices are installed with updated anti-virus/ anti-malware applications and that your devices' operating systems and applications are updated regularly to be protected by the latest security patches. Disable "Install Unknown App" or "Unknown Sources" in your Android phone settings.**
- **Check for scam signs and with official sources. Only download and install applications from official app stores. As an added precaution, check the developer information on the application listing and the number of downloads and user reviews to ensure it is a reputable and legitimate application. Always exercise caution when clicking on advertisements embedded within applications that lead to a third-party website that prompts the download of files. Do not grant permission to persistent pop-ups that request access to your device's hardware or data.**
- **Tell authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately.**

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



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。



电子商务/租房诈骗*

您在网上看到价格低于市价的热门商品或租房交易。

查看官方消息，如公司的官方网站，以核实这笔交易。



涉及恶意应用程序的钓鱼诈骗*

您在网上看到一笔交易并联系“卖家”。您被要求点击一个链接下载应用程序付款。请勿下载应用程序或提供您的个人资料。务必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。

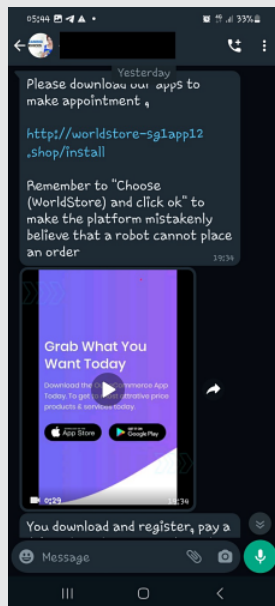
在您的手机里下载ScamShield应用，以屏蔽诈骗短信及黑名单号码。请勿点击来自不熟悉发送者的可疑短信以及WhatsApp或社交媒体即时通讯平台讯息内的链接。

*排名第4和第5的诈骗手法与上周手法类似。

⚠️ 提防恶意软件!

诈骗手法

- 受害者会通过脸书和Instagram等社交媒体即时通讯平台接触到居家服务或售卖食品的广告。
- 骗子会通过社交媒体或WhatsApp联络受害者，并发送一个网址。受害人被要求从网站下载应用程序预订服务或购买食物以及付款。
- 受害者在应用程序内的虚假银行登录页面输入网上银行和/或银行卡细节进行付款。应用程序藏有的恶意软件将身份验证资料和一次性密码转发至骗子。受害者只有在户头里有未经授权的交易或付款后才发现自己被骗了。



[骗子与受害者的WhatsApp聊天记录]

- 下载ScamShield应用程序并设置安全功能。确保您的设备安装了最新的防毒/反恶意软件应用程序。务必定期更新设备的操作系统并确保应用程序受到最新安全补丁的保护。在安卓手机设置内禁止“安装未知应用程序”或“未知来源”的应用程序。
- 查看官方消息并注意诈骗迹象。只从官方应用商店下载和安装应用程序。请检查应用程序列表中的开发人员信息与下载和用户评论的次数作为多一层的安全措施，确保它是一个信誉良好并正当的应用程序。在点击应用程序中引导您至第三方网站并指示您下载文件的广告时，请务必小心。不要授权要求进入设备硬件或数据的持久性弹出式窗口权限。
- 告知当局、家人和朋友诈骗案件趋势。向银行举报任何欺诈性转账。

⚠️ 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

TREND PENIPUAN

SEPANJANG MINGGU LEPAS

Isu
no.06
28 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 E-Dagang/Sewa Hartanah*

Anda melihat satu tawaran dalam talian untuk barangan yang popular, atau sewa hartanah, yang berharga di bawah kadar pasaran.

PERIKSA dengan sumber-sumber rasmi seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut.



Penipuan Pancingan Data Melibatkan Aplikasi Berniat Jahat*

Anda ternampak satu tawaran dalam talian dan menghubungi “penjual”. Anda diminta supaya mengklik satu pautan untuk memuat turun satu aplikasi untuk membuat bayaran. JANGAN muat turun aplikasi tersebut, dan beri butir-butir peribadi anda. Sentiasa hubungi bank menggunakan nombor telefon rasmi mereka yang tersenarai di laman-laman web rasmi bank tersebut atau nombor yang tertera di belakang kad kredit/debit anda.

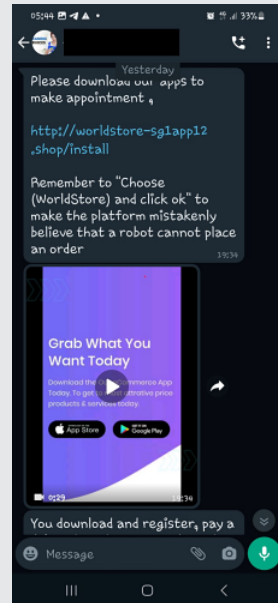
MASUKKAN aplikasi ScamShield di telefon bimbit anda untuk melindungi diri anda daripada penipuan SMS dan nombor yang disenaraihitamkan. JANGAN klik pautan daripada SMS/WhatsApp/Platform Pesanan Sosial Media yang mencurigakan daripada penghantar yang tidak anda kenali.

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

⚠️ Awas dengan Perisian Hasad!

Taktik Penipuan

- Mangsa akan terjumpa iklan-iklan untuk perkhidmatan rumah atau penjualan barang makanan melalui platform pesanan media sosial seperti Facebook dan Instagram.
- Penipu menghubungi mangsa melalui media sosial atau Whatsapp dan menghantar satu URL. Mangsa diminta supaya memuat turun satu aplikasi daripada URL tersebut untuk memesan perkhidmatan atau membeli makanan, dan membuat bayaran.
- Mangsa memasukkan butir-butir perbankan dalam talian dan/atau kad ke laman-laman log masuk perbankan palsu dalam aplikasi tersebut untuk membuat bayaran. Aplikasi tersebut mempunyai perisian hasad yang mengarahkan butiran dan OTP kepada penipu. Mangsa akan hanya sedar mereka telah ditipu apabila urusan niaga atau bayaran tanpa kebenaran telah dibuat di akaun mereka.



[Perualan di WhatsApp antara seorang penipu dan mangsa]

- Masukkan aplikasi ScamShield dan letakkan ciri-ciri keselamatan. Pastikan peranti anda telah dipasang dengan aplikasi anti virus/anti perisian hasad yang dikemas kini dan sistem operasi dan aplikasi peranti anda telah dikemas kini secara tetap agar ia dilindungi dengan patch keselamatan yang terkini. Nyahdayakan “Install Unknown App” (Pasang Aplikasi yang Tidak Diketahui) atau “Unknown Sources” (Sumber yang Tidak Diketahui) di dalam tetapan telefon Android anda.
- Periksa tanda-tanda penipuan dan dengan sumber-sumber rasmi. Muat turun dan pasang aplikasi hanya daripada kedai app yang rasmi. Sebagai perlindungan tambahan, periksa maklumat pemaju di senarai aplikasi dan bilangan muat turun dan ulasan pengguna untuk memastikan aplikasi tersebut bereputasi dan sah. Sentiasa berhati-hati apabila mengklik iklan-iklan yang disematkan dalam aplikasi yang akan menuju ke laman web pihak ketiga yang menggesa anda supaya memuat turun fail. Jangan beri keizinan kepada pop-up berterusan yang meminta akses ke perkakasan atau data peranti anda.
- Beritahu pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Adukan sebarang urusan niaga palsu kepada bank anda dengan segera.

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



முன்னணி மோசடிகள்

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 வருவாய்க்கை 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.



மின் வணிகம் / சொத்து வாடகை மோசடி*

பிரபலமான பொருட்கள் அல்லது சொத்து வாடகைக்கான ஒரு ஒப்பந்தத்தை இணையத்தில் சந்தை விலைகளைக் காட்டிலும் குறைவான விலையில் இருப்பதை நீங்கள் காண்கிறீர்கள்

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும்.



தீங்கிழைக்கும் செயலி சம்பந்தப்பட்ட தகவல் திருட்டு மோசடி*

நீங்கள் கடணம் செலுத்துவதற்கு ஒரு இணைப்பைக் கிளிக் செய்து செயலி ஒன்றைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். செயலியைப் பதிவிறக்கம் செய்யவோ அல்லது உங்கள் தனிப்பட்ட விவரங்களை வழங்கவோ வேண்டாம். எப்போதும் வங்கிகளின் அதிகாரப்பூர்வ இணையத்தளங்களில் பட்டியலிடப்பட்டுள்ள அதிகாரப்பூர்வ தொடர்பு எண்கள் வாயிலாகவோ அல்லது உங்கள் பற்று / கடன்பற்று அட்டைகளின் பின்புறத்தில் பட்டியலிடப்பட்டுள்ள எண்கள் வாயிலாகவோ வங்கிகளை தொடர்பு கொள்ளுங்கள்.

மோசடி குறுஞ்செய்திகளிலிருந்தும் கறப்பப் பட்டியலிடப்பட்ட எண்களிலிருந்தும் உங்களைப் பாதுகாத்துக்கொள்ள ஸ்கேம்ஷீல்ட் செயலியை உங்கள் கைத்தொலைபேசியில் சேர்த்துக்கொள்ளுங்கள். குறுஞ்செய்தி / வாட்ஸ்ஆப் / சமூக ஊடக தளங்களிலிருந்து உங்களுக்கு அறிமுகமில்லாத அனுப்புகளிடமிருந்து வரும் சந்தேகத்துக்குரிய இணைப்புகளை கிளிக் செய்ய வேண்டாம்.

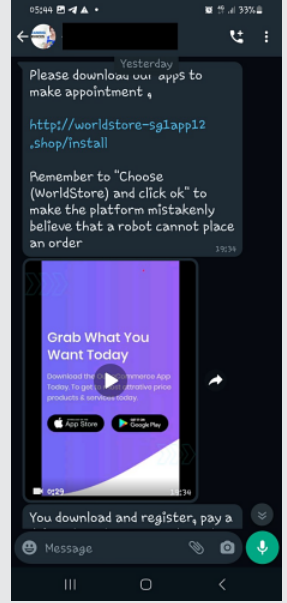
*4-வது மற்றும் 5-வது இடத்தில் உள்ள மோசடிகள், முந்தைய வாரத்துடன் ஒப்பிடும்போது புதிய வகைகளாகும்.



தீங்கு விளைவிக்கும் மென்பொருள் குறித்து எச்சரிக்கையாக இருங்கள்!

மோசடி உத்திகள்

- ஃபேஸ்புக், இன்ஸ்டாகிராம் போன்ற சமூக ஊடக குறுஞ்செய்தித் தளங்கள் மூலம் வீட்டுச் சேவைகளுக்கான விளம்பரங்களையோ உணவுப் பொருட்களின் விற்பனையையோ பாதிக்கப்பட்டவர்கள் காண்பார்கள்.
- மோசடிக்காரர்கள் சமூக ஊடகம் அல்லது வாட்ஸ்ஆப் வழியாக பாதிக்கப்பட்டவர்களைத் தொடர்புகொண்டு, ஒரு இணையத் தளத்தின் முகவரியை அனுப்புகின்றனர். சேவைகளுக்கு முன்பதிவு செய்ய அல்லது உணவு வாங்கி பணம் செலுத்த இணையத் தளத்திலிருந்து ஒரு செயலியை பதிவிறக்கம் செய்யும்படி பாதிக்கப்பட்டவர்கள் கேட்டுக்கொள்ளப்படுகின்றனர்.
- பாதிக்கப்பட்டவர்கள் பணம் செலுத்துவதற்காக செயலியினுள்ள போலி வங்கித் தளங்களில் இணைய வங்கிச் சேவை உள்நுழைவு விவரங்கள் மற்றும்/அல்லது அட்டை விவரங்களை உள்ளிடுவார்கள். தகவல்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் மோசடிக்காரர்களுக்கு அனுப்பும் தீங்கு விளைவிக்கும் மென்பொருள் அந்தச் செயலியில் இருக்கும். அங்கீகரிக்கப்படாத பரிவர்த்தனைகள் அல்லது கட்டணங்கள் தங்கள் கணக்குகளில் செய்யப்படும்போது மட்டுமே தாங்கள் மோசடி செய்யப்பட்டிருப்பதை பாதிக்கப்பட்டவர்கள் உணர்கிறார்கள்.



[வாட்ஸ்ஆப்பில் மோசடிக்காரருக்கும் பாதிக்கப்பட்டவருக்கும் இடையிலான உரையாடல்]

- ஸ்கேம்ஷீல்ட் செயலியைச் சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும். உங்கள் சாதனங்களில் புதுப்பிக்கப்பட்ட நச்சுநிரல் எதிர்ப்பு/ தீங்கு விளைவிக்கும் மென்பொருள் தடுப்பு செயலிகள் நிறுவப்பட்டிருப்பதை உறுதி செய்யுங்கள். உங்கள் சாதனங்களின் இயங்குதளம் மற்றும் செயலிகள் சமீப பாதுகாப்பு திட்டுகளால் பாதுகாக்கப்பட தவறாமல் புதுப்பிக்கப்பட வேண்டும். உங்கள் ஆண்டிராய்ட் தொலைபேசி அமைவுகளில் உள்ள "Install Unknown App" அல்லது "Unknown Sources" என்பதை முடக்கவும்.
- மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். அதிகாரப்பூர்வ செயலிக் கடைகளில் இருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள். ஒரு கூடுதல் முன்னெச்சரிக்கையாக, செயலி பட்டியலில் உள்ள தகவல்கள், பதிவிறக்கங்களின் எண்ணிக்கை மற்றும் பயனர் மதிப்பாய்வுகளின் எண்ணிக்கை ஆகியவற்றை சரிபார்த்து அது ஒரு நம்பகமான, சட்டபூர்வமான செயலி என்பதை உறுதி செய்யுங்கள். பதிவிறக்கம் செய்யத் தூண்டும் மூன்றாம் தரப்பு வலைத்தளத்திற்கு வழிவகுக்கும் செயலிகளுக்குள் பதிந்துள்ள விளம்பரங்களை கிளிக் செய்யும்போது எப்போதும் எச்சரிக்கையுடன் இருக்கவும். உங்கள் சாதனத்தின் வன்பொருள் அல்லது தரவை அணுக கோரும் தொடர்ச்சியான 'பாப் அப்களுக்கு' அனுமதி வழங்க வேண்டாம்.
- மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரியப்படுத்துங்கள்.



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

