

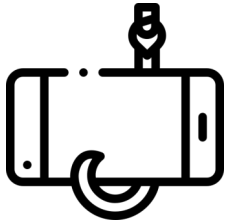
TRENDING SCAMS | IN THE PAST WEEK

Issue

no. 10

26 May 2023

Scams to look out for



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.



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.



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.



Phishing Scam/ Government Calls*

You receive calls from “government officials”. You are asked to provide your banking credentials, OTPs and/ or personal details.

ADD ScamShield app only from the official app stores on your mobile phone to block scam calls and detects scam SMSes from known blacklisted numbers. Do not provide your credentials and OTPs to unknown persons.

See page two for more details on how you can be better protected from this scam type.

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

Call from Government Officials?

Scam Tactics

- Scammers would impersonate government officials such as SPF and MOM, and approach victims via calls (phone call or in-app call, e.g. WhatsApp).
- Scammers would convince victims to provide their banking credentials, OTPs and/ or personal details by claiming that they were involved in money laundering or other crimes.
- Subsequently, victims would find unauthorised transactions made to their bank accounts.



[Screenshot of a scammer pretending to be a "SPF" officer in an in-app call]

- No government agencies will ask for your banking credentials, OTPs or require you to transfer your money to another bank account.
- **ADD** - ScamShield App from official app stores and set security features (e.g., enable two-factor (2FA) for banks, social media, Singpass accounts; set transaction limits on internet banking transactions). Do not send or transfer money to unknown persons.
- **CHECK** - For scam signs such as phone calls from unknown numbers (with or without the "+" prefix) and always refrain from giving out personal information and bank details to callers over the phone.
- **TELL** - Authorities, family and friends about scams and do not be pressured by the caller to act impulsively. 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



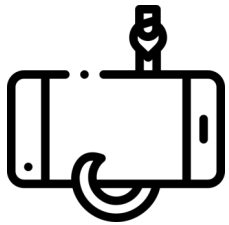
In collaboration with



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

诈骗趋势

当心骗局



涉及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。



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。



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。



钓鱼/ 政府来电*

您会接到来自“政府官员”的电话。您被要求提供您的银行凭证、一次性密码和/或个人资料。

只从官方应用程序商店下载ScamShield 应用程序，拦截诈骗电话和过滤诈骗短信。切勿向身份不明人士提供您的凭证以及一次性密码。

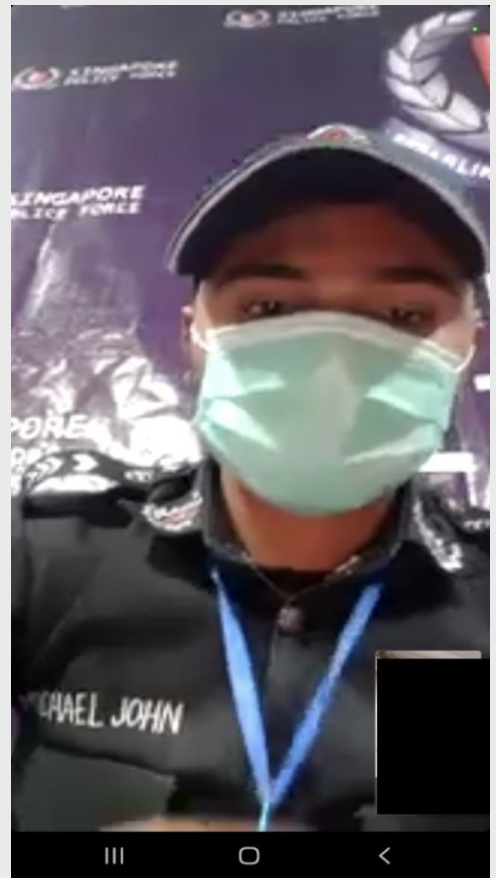
请参阅第2页以便了解如何更好保护您免受此类诈骗。

*本周新加入前五名的诈骗手法。

⚠️ 政府官员来电？

诈骗手法

- 骗子会冒充新加坡警察部队和人力部等政府官员，通过电话（电话或如WhatsApp 的应用程序内电话）联络受害者。
- 骗子会声称受害者涉及洗黑钱或其他罪行以便说服受害者提供他们的银行凭证、一次性密码和/或个人资料。
- 受害者之后会发现他们的银行账户有未经授权的交易。



[冒充“新加坡警察部队”官员的骗子利用应用程序电话拨电的截图]

- 任何政府机构都不会向您索取银行凭证、一次性密码或要求您把钱转到另一个银行账户。
- 从官方应用程序商店下载ScamShield应用程序并设置安全功能（如在银行、社交媒体、Singpass账户启用双重认证；在网上银行设置交易限额）。切勿汇款或转账给身份不明人士。
- 注意如未知来电（或许没有以“+ 65”开头的号码）的诈骗迹象并避免通过电话向来电者透露个人和银行资料。
- 告知当局、家人和朋友诈骗案件趋势。别在来电者的施压下冲动行事。立即向银行举报任何欺诈性交易。

⚠️ 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



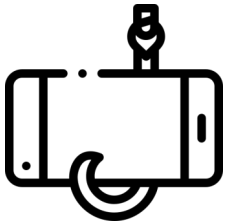
**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

协力带给您

SEPANJANG MINGGU LEPAS

Penipuan yang harus diawasi

Penipuan 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 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 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 Pancingan Data/ Panggilan Pemerintah*



Anda menerima beberapa panggilan daripada “pegawai pemerintah”. Anda diminta supaya memberikan butiran perbankan, OTP dan/atau butir-butir peribadi anda.

MASUKKAN aplikasi ScamShield hanya daripada gedung aplikasi rasmi ke telefon bimbit anda untuk menyekat panggilan penipuan dan mengesan SMS penipuan daripada nombor-nombor yang diketahui telah disenaraihitamkan. Jangan berikan butiran dan OTP anda kepada orang-orang yang tidak dikenali.

Lihat halaman dua untuk butir-butir lebih lanjut bagaimana anda boleh melindungi diri anda dengan lebih baik daripada jenis penipuan ini.



Panggilan daripada Pegawai Pemerintah?

Taktik Penipuan

- Penipu akan menyamar sebagai pegawai pemerintah seperti pegawai SPF dan MOM, dan mendekati mangsa melalui panggilan (panggilan telefon atau panggilan dalam aplikasi, misalnya Whatsapp).
- Penipu akan meyakinkan mangsa-mangsa supaya memberikan butiran perbankan/ OTP dan/ atau butir-butir peribadi mereka dengan mendakwa bahawa mereka telah terbabit dengan pengubahan wang haram atau jenayah lain.
- Seterusnya, mangsa-mangsa akan mendapati transaksi tanpa kebenaran telah dibuat ke atas akaun bank mereka.



[Tangkap layar seorang penipu yang berpura-pura sebagai seorang pegawai "SPF" di dalam sebuah panggilan dalam aplikasi]

- Tiada agensi pemerintah yang akan meminta butiran perbankan, OTP anda atau memerlukan anda supaya memindahkan wang anda ke akaun bank lain.
- **MASUKKAN** – Aplikasi Scamshield daripada gedung aplikasi rasmi dan pasangkan ciri-ciri keselamatan (misalnya, dayakan dua-faktor (2FA) untuk akaun-akaun bank, media sosial, Singpass; tetapkan had transaksi untuk transaksi perbankan internet). Jangan hantar atau pindahkan wang kepada orang-orang yang tidak dikenali.
- **PERIKSA** – Tanda-tanda penipuan seperti panggilan telefon daripada nombor-nombor yang tidak dikenali (dengan atau tanpa awalan "+") dan sentiasa elakkan daripada memberi maklumat peribadi dan butir-butir bank kepada pemanggil melalui telefon.
- **BERITAHU** – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan dan jangan berasa tertekan dengan pemanggil untuk bertindak melulu. Adukan sebarang transaksi menipu 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 hantar-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



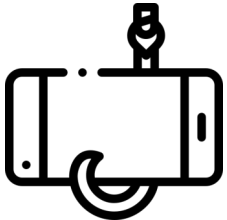
Dengan kerjasama



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

முன்னணி மோசடிகள்

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்



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 ஆள்மாறாட்டம் 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 தரப்பு அல்லது சந்தேகத்திற்குரிய தளங்களிலிருந்தும் அல்ல என்பதை சரிபார்த்து உறுதி செய்யுங்கள்.



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 வருவாய்ப்பைக் 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.



வேலை மோசடி

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

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



தகவல் திருட்டு மோசடி / அரசாங்க அழைப்புகள்*

"அரசாங்க அதிகாரிகளிடமிருந்து" உங்களுக்கு அழைப்புகள் வருகின்றன. உங்கள் வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) மற்றும்/அல்லது தனிப்பட்ட விவரங்களை வழங்குமாறு நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகளைத் தடுக்கவும், கறுப்புப் பட்டியலிடப்பட்ட எண்களிலிருந்து மோசடி குறுஞ்செய்திகளைக் கண்டறியவும், உங்கள் கைபேசியில் உள்ள அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களில் இருந்து மட்டுமே ஸ்கேம்ஷீல்ட் செயலியைச் சேர்க்கவும். தெரியாத நபர்களுக்கு உங்கள் விவரங்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் (OTP) வழங்காதீர்கள்.

இந்த வகை மோசடியிலிருந்து நீங்கள் எவ்வாறு பாதுகாக்கப்படலாம் என்பது பற்றிய மேல் விவரங்களுக்கு பக்கம் இரண்டைப் பார்க்கவும்.

*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது.



அரசாங்க அதிகாரிகளிடமிருந்து அழைப்பா?

மோசடி உத்திகள்

- மோசடி செய்பவர்கள் SPF மற்றும் MOM போன்ற அரசாங்க அதிகாரிகளைப் போல ஆள்மாறாட்டம் செய்வார்கள். மேலும், பாதிக்கப்பட்டவர்களை அழைப்புகள் (தொலைபேசி அழைப்பு அல்லது செயலி அழைப்பு, எ. கா. வாட்ஸ்ஆப்) வழியாக அணுகுவார்கள்.
- மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்கள் பண மோசடி அல்லது பிற குற்றங்களில் ஈடுபட்டதாகக் கூறி அவர்களின் வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTP) மற்றும்/ அல்லது தனிப்பட்ட விவரங்களை வழங்க சம்மதிக்க வைப்பார்கள்.
- அதனைத் தொடர்ந்து, தங்கள் வங்கிக் கணக்குகளில் அனுமதிக்கப்படாத பரிவர்த்தனைகள் செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



[செயலி அழைப்பில் 'SPF' அதிகாரி போல் பாசாங்கு செய்த மோசடிக்காரர் ஒருவரின் ஸ்கிரீன்ஷாட்]

- எந்த அரசாங்க அமைப்புகளும் உங்கள் வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) ஆகியவற்றை கேட்கமாட்டார்கள். உங்கள் பணத்தை வேறொரு வங்கிக் கணக்கிற்கு மாற்றுமாறு அவர்கள் சொல்ல மாட்டார்கள்.
- **சேர்க்க** - அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து ஸ்கேம்ஷீல்ட் செயலியைப் பதிவிறக்கம் செய்து, பாதுகாப்பு அம்சங்களை அமைக்கவும். (எ. கா., வங்கிகள், சமூக ஊடகங்கள், Singpass கணக்குகளுக்கு 2FA பாதுகாப்பு அம்சத்தை செயல்படுத்தவும்; இணைய வங்கிச் சேவை பரிவர்த்தனைகளுக்கு பரிவர்த்தனை வரம்புகளை அமைக்கவும்.) தெரியாத நபர்களுக்கு பணத்தை அனுப்பவோ அல்லது மாற்றவோ கூடாது.
- **சரிபார்க்க** - தெரியாத எண்களிலிருந்து வரும் தொலைபேசி அழைப்புகள் ("+" முன்னிணைப்பு உடன் அல்லது இல்லாமல்) போன்ற மோசடி அறிகுறிகளைக் கண்டறிந்து, தொலைபேசியில் அழைப்பவர்களுக்கு தனிப்பட்ட தகவல்களையும் வங்கி விவரங்களையும் வழங்குவதைத் தவிர்க்கவும்.
- **சொல்ல** - மோசடிகள் பற்றி அதிகாரிகள், குடும்பத்தினர் மற்றும் நண்பர்களுக்கு தெரியப்படுத்துங்கள். அழைப்பவரின் கட்டாயத்தால் அவசரப்பட்டு செயல்படாதீர்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.

 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