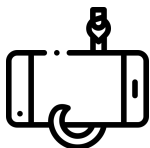


# TRENDING SCAMS IN THE PAST WEEK

Issue  
no. 09  
19 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 will contact you and ask you to install the fake ScamShield app via a URL link.

See page two for more details on this scam type.



### 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.



### 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 involving impersonation of real estate agents or authorised personnel

You see a deal online for a property rental on various advertisement sites like Facebook or Carousell, and the agent or “authorised personnel” asked for payment (deposit) even before physical viewing of the property.

**CHECK** the agent’s advertised phone number in the property listing on CEA’s Public Register. If the phone number is not registered with CEA, it is likely a scam! Do not transfer money without first viewing the property.



### E-Commerce/ Concert Tickets Scam

You see third-party resellers on online platforms offering the sale of concert tickets. Sellers would claim that the ticket sales are time-sensitive or have limited availability, to convince buyers into making advanced payment for the tickets.

Purchase only from authorised sellers or reputable sources and avoid making advance payments or direct bank transfers to sellers. **CHECK** the platform’s Transaction Safety Rating (TSR) at <https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings> to know what critical anti-scam safety features it has to protect online transactions.

# Phishing Scam involving fake ScamShield app

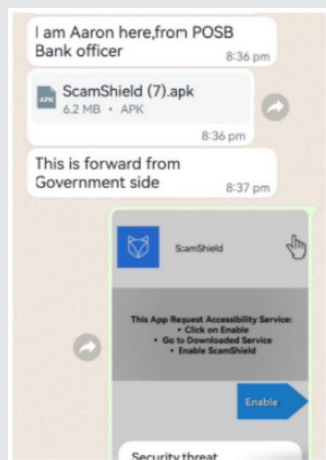
## Scam Tactics

- Victims would come across advertisements for sales of food items via social media platforms. Victims would contact the scammers via WhatsApp and the scammers would send a URL to the victims.

- The scammers would then inform the victims to download an application via the URL to purchase the items and make payment. Unauthorised transactions would be made from victims' bank accounts or credit cards.

- After making the unauthorised transactions, the scammers would impersonate as bank staff and call the victims. The scammer would then recommend victims to download a fake ScamShield app using a URL link, on the pretext of getting the victim to protect himself/herself against scams and make a report via the fake ScamShield app.

- Scammers would insist that the URL link provided is legitimate and would insist for victims to not download the ScamShield app from official app stores.



*[Screenshot of conversation between victim and the "bank staff" whereby the victim was asked to install the fake ScamShield app]*

- Be aware of the dangers of downloading applications from third-party or dubious sites. Doing so can lead to malware being installed on victims' mobile devices. Scammers will trick victims into installing malware-infected applications that are provided via URL links and not from official app stores.
- Only download and install applications from official application stores. Disable "Install Unknown App" or "Unknown Sources" in your device's settings.
- To find out more on downloading the ScamShield app on your mobile devices, please refer to the official guide at <https://www.scamshield.org.sg/setup-guide>.
- To find out more about malware and the preventive steps that users can take to protect their devices, please refer to Cyber Security Agency of Singapore (CSA) SingCERT advisory at <https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008>.

# 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](http://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](http://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

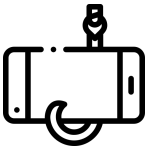


In collaboration with



## 诈骗趋势

### 当心骗局



#### 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。

请参阅第2页以便了解更多这类诈骗的详情。



#### 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。



#### 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/冒充房地产经纪或授权人员的租房诈骗

您在如脸书或Carousell的多个广告网站上看到租房广告，房地产经纪或“授权人员”要求您在实际看房之前预付押金。

查询该房地产经纪在房地产代理理事会(CEA)公共名册上的公开电话号码。如果电话号码没有在房地产代理理事会公共名册里，那可能是个骗局！切勿在看房前转账。



#### 电子商务/演唱会门票骗局

您看到第三方转售商在网络平台上销售演唱会门票。卖家会声称售票有时间限制或数量有限以说服买家预付款项。

只向授权卖方或信誉良好的来源购买并避免预付款项或通过银行直接转账给卖方。浏览

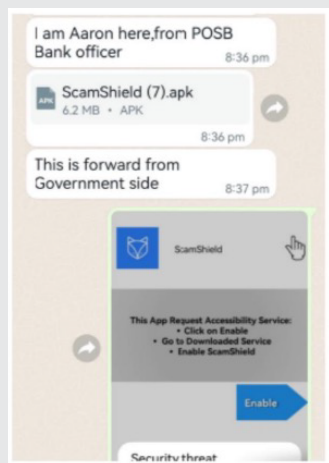
<https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>查看平台的交易安全评级(TSR)以便了解该平台有哪些保护网上交易的重要反诈骗安全措施。



# ⚠ 涉及ScamShield应用程序的钓鱼诈骗

## 诈骗手法

- 受害者会在社交媒体平台接触到售卖食品的广告。骗子会在受害者通过WhatsApp联络后发送网站链接给受害者。
- 骗子会请受害者通过网站链接下载应用程序购买物品并付款。受害者的银行账户或信用卡之后会有未经授权的交易。
- 进行未经授权的交易后，骗子会冒充银行职员打电话给受害者。骗子会以鼓励受害者保护自己免受诈骗为由，建议受害者使用网站链接下载假的ScamShield应用程序并在假的ScamShield应用程序里举报诈骗案件。
- 骗子会坚持所提供的网站链接是正当的，并坚持不让受害者从官方应用程序商店下载ScamShield应用程序。



[受害者与“银行职员”对话的截图，受害者被要求安装假的ScamShield应用程序]

- 请了解从第三方或可疑网站下载应用程序的危险性。这会使恶意软件被安装至受害者的移动设备。骗子会诱骗受害者通过非官方应用程序商店的网站链接安装受恶意软件感染的应用程序。
- 只从官方应用程序商店下载并安装应用程序。在设备设置内禁止“安装未知应用程序”或“未知来源”的应用程序。
- 请浏览<https://www.scamshield.org.sg/setup-guide>的官方指南了解更多在您移动设备下载ScamShield应用程序的详情。
- 请浏览<https://www.csa.gov.sg/alerts-advisories/advisories/2021/ad-2021-008>参考新加坡网络安全局（CSA）电脑紧急反应组的公告以了解更多有关恶意软件的信息以及用户可采取的防范措施。

# ⚠️ 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](http://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](http://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

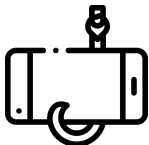
# TREND PENIPUAN

# SEPANJANG MINGGU LEPAS

Isu  
no.09

19 Mei 2023

## 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 dari 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.

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



### 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 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.



### E-Dagang / Penipuan Sewaan Hartanah melibatkan penyamaran ejen hartanah atau kakitangan yang dibenarkan

Anda ternampak satu tawaran dalam talian berkenaan sewaan hartanah di pelbagai laman web iklan seperti Facebook atau Carousell, dan pihak ejen atau “kakitangan yang dibenarkan” meminta bayaran (wang cengkeram) sebelum melihat secara fizikal hartanah tersebut.

**PERIKSA** nombor telefon ejen yang diiklankan di Daftar Awam CEA. Jika nombor telefon tersebut tidak berdaftar dengan CEA, kemungkinan ianya merupakan penipuan! Jangan pindahkan wang tanpa terlebih dahulu melihat hartanah tersebut.



### E-Dagang/ Penipuan Tiket Konsert

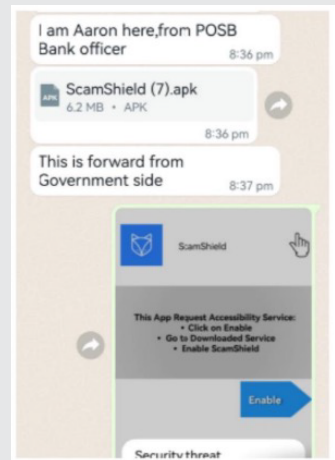
Anda ternampak penjual pihak ketiga di platform dalam talian yang menawarkan penjualan tiket konsert. Penjual akan mendakwa bahawa jualan tiket adalah sensitif masa atau mempunyai ketersediaan terhad, untuk meyakinkan pembeli membuat pembayaran awal untuk tiket.

Beli hanya daripada penjual yang sah atau sumber-sumber yang bereputasi, dan elakkan daripada membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada penjual. **PERIKSA** Rating Keselamatan Urus Niaga (TSR) untuk rating platform itu dan untuk mengetahui ciri keselamatan anti-penipuan kritikal yang ada padanya untuk melindungi transaksi dalam talian.

# Penipuan Pancingan Data membabitkan aplikasi ScamShield palsu

## Taktik Penipuan

- Mangsa akan ternampak iklan-iklan yang menjual barang makanan (seperti otak-otak) melalui platform media sosial. Mangsa akan menghubungi penipu melalui WhatsApp dan penipu kemudian akan menghantar satu petunjuk sumber seragam (URL) kepada mangsa.
- Penipu kemudian akan memberitahu mangsa supaya memuat turun aplikasi yang terdapat di URL tersebut untuk membeli barangan tersebut, dan untuk membuat pembayaran. Transaksi tanpa kebenaran akan dilakukan dari akaun bank atau kad kredit mangsa.
- Selepas membuat transaksi tanpa kebenaran itu, penipu akan menyamar sebagai kakitangan bank dan menghubungi mangsa. Penipu kemudian akan mengesyorkan supaya mangsa memuat turun sebuah aplikasi ScamShield palsu menggunakan satu pautan URL, dengan alasan bahawa mangsa akan dapat melindungi dirinya daripada penipuan dan supaya mangsa dapat membuat laporan di aplikasi ScamShield palsu tersebut.
- Penipu akan berkeras bahawa pautan URL yang diberikan itu adalah sah dan akan memberitahu mangsa supaya jangan memuat turun Aplikasi ScamShield daripada gedung aplikasi rasmi.



*[Shot layar perbualan antara mangsa dan 'kakitangan bank' di mana mangsa diminta memasang aplikasi ScamShield palsu itu]*

- Berjaga-jaga bahaya memuat turun aplikasi daripada pihak ketiga atau laman web yang meragukan. Tindakan sedemikian boleh menyebabkan perisian hasad dipasang pada peranti mudah alih mangsa. Penipu akan menipu mangsa supaya memasang aplikasi yang dijangkiti perisian hasad yang telah disediakan melalui pautan URL dan bukan dari gedung aplikasi rasmi.
- Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi. Nyahdayakan "Install Unknown App" (Pasang Aplikasi yang Tidak Diketahui) atau "Unknown Sources" (Sumber yang Tidak Diketahui) di dalam tetapan peranti anda.
- Untuk mengetahui lebih lanjut mengenai memuat turun aplikasi ScamShield pada peranti mudah alih anda, sila rujuk kepada panduan rasmi di <https://www.scamshield.org.sg/setup-guide>.
- Untuk mengetahui lebih lanjut tentang perisian hasad dan langkah pencegahan yang boleh diambil oleh pengguna untuk melindungi peranti mereka, sila rujuk kepada makluman SingCERT Agensi Keselamatan Siber Singapura (CSA) di <https://www.csa.gov.sg/alerts-advisories/Advisories/2021/ad-2021-008>.

# 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](http://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](http://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

# கடந்த வாரத்தின்

வெளியீடு  
எண் 09  
19 மே 2023

## 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 மோசடிகாரர் உங்களைத் தொடர்புகொண்டு, ஒரு இணையப்பக்க முகவரியின் இணைப்பு மூலம் போலி ஸ்கேம்ஷீல்ட் செயலியை நிறுவச் சொல்வார்.

இந்த மோசடி வகை குறித்த மேல் விவரங்களுக்கு பக்கம் இரண்டைப் பார்க்கவும்.



#### 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 அழைத்திருந்தாரா என்பதை மற்ற வழிகள் மூலமாகவோ அல்லது அவர்களின் அசல் எண்ணிலோ தொடர்புகொண்டு சரிபார்க்கவும்.



#### முதலீடு மோசடி

மிக உயர்ந்த வருவாயைக் 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.



#### இணைய வர்த்தகம் / சொத்துச் சந்தை முகவர்கள் அல்லது அங்கீகரிக்கப்பட்ட பணியாளர்களின் ஆள்மாறாட்டம் சம்பந்தப்பட்ட சொத்து வாடகை மோசடி

ஃபேஸ்புக் அல்லது கேரோஸ் போன்ற பல்வேறு விளம்பர தளங்களில் சொத்து வாடகைக்கான ஒரு ஒப்பந்தத்தை நீங்கள் இணையத்தில் பார்க்கிறீர்கள். சொத்தைப் பார்ப்பதற்கு முன்பே முகவர் அல்லது "அங்கீகரிக்கப்பட்ட பணியாளர்" பணம் (வைப்புத் தொகை) கேட்டார்.

சொத்து பட்டியலிலுள்ள முகவரின் விளம்பரப்படுத்தப்பட்ட தொலைபேசி எண்ணை CEA-வின் பொதுப் பதிவேட்டில் சரிபார்க்கவும். தொலைபேசி எண் CEA-வில் பதிவு செய்யப்படாவிட்டால் அது ஒரு மோசடியாக இருக்கக்கூடும்! சொத்தை முதலில் பார்க்காமல் பணத்தை மாற்றிவிடாதீர்கள்.



#### இணைய வர்த்தகம் / இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள் மோசடி

இணையத் தளங்களில் மூன்றாம் தரப்பு மறுவிற்பனையாளர்கள் இசை நிகழ்ச்சிக்கான நுழைவுச் சீட்டு விற்பனையை வழங்குவதை நீங்கள் காண்கிறீர்கள். நுழைவுச்சீட்டு விற்பனை குறைந்த அளவில், ஒரு குறிப்பிட்ட காலத்திற்கு மட்டும் கிடைக்கக்கூடியவை என்று விற்பனையாளர்கள் கூறி, வாங்குபவர்களை நுழைவுச்சீட்டுகளுக்கு முன்கூட்டியே பணம் செலுத்த சம்மதிக்க வைப்பார்கள்.

அங்கீகரிக்கப்பட்ட விற்பனையாளர்கள் அல்லது நம்பகமான இடங்களிலிருந்து மட்டுமே வாங்குங்கள். மேலும், விற்பனையாளர்களுக்கு முன்கூட்டியே பணம் செலுத்துதல் அல்லது நேரடி வங்கி மாற்றல்களைச் செய்வதைத் தவிர்க்கவும். இணையப் பரிவர்த்தனைகளைப் பாதுகாக்க என்ன மோசடி எதிர்ப்பு பாதுகாப்பு அம்சங்கள் உள்ளன என்பதை அறிய,

<https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings> என்ற

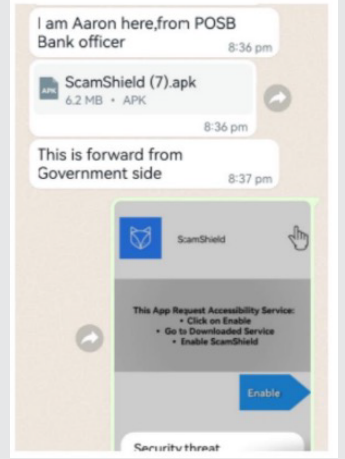
இணையத்தளத்தில் பரிவர்த்தனை பாதுகாப்பு மதிப்பீடுகளை (TSR) சரிபார்க்கவும்.



# போலி ஸ்கேம்ஷீல்ட் செயலி சம்பந்தப்பட்ட தகவல் திருட்டு மோசடி

## மோசடி உத்திகள்

- சமூக ஊடகத் தளங்கள் வழியாக உணவுப் பொருட்களின் விற்பனைக்கான விளம்பரங்களை பாதிக்கப்பட்டவர்கள் காண்பார்கள். பாதிக்கப்பட்டவர்கள் வாட்ஸ்ஆப் மூலம் மோசடிக்காரர்களைத் தொடர்புகொள்வார்கள். பிறகு, மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்கு ஒரு இணையப்பக்க முகவரியை (URL) அனுப்புவார்கள்.
- உணவுப் பொருட்களை வாங்குவதற்காக இணையப்பக்க முகவரியில் காணப்படும் செயலியைப் பதிவிறக்கம் செய்யுமாறும், பணம் செலுத்துமாறும் மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களிடம் சொல்வார்கள். அனுமதிக்கப்படாத பரிவர்த்தனைகள் பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்குகள் அல்லது கடன்பற்று அட்டைகள் ஆகியவற்றிலிருந்து செய்யப்படும்.
- இந்த அனுமதிக்கப்படாத பரிவர்த்தனைகளைச் செய்த பிறகு, மோசடிக்காரர்கள் வங்கி ஊழியர் போல ஆள்மாறாட்டம் செய்து பாதிக்கப்பட்டவரைத் தொடர்புகொள்வார்கள். மோசடிக்காரர், போலியான ஸ்கேம்ஷீல்ட் செயலியை ஒரு இணையப்பக்க முகவரி மூலம் பதிவிறக்கம் செய்யும்படி பாதிக்கப்பட்டவரைப் பரிந்துரைப்பார். மோசடிகளுக்கு எதிராக பாதிக்கப்பட்டவர் தன்னைப் பாதுகாத்துக்கொள்ள வேண்டும் என்று கூறி, போலியான ஸ்கேம்ஷீல்ட் செயலியில் புகார் அளிக்குமாறு மோசடிக்காரர் கேட்டுக்கொள்வார்.
- வழங்கப்பட்ட இணையப்பக்க முகவரி நம்பகமானது என்றும் அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து ஸ்கேம்ஷீல்ட் செயலியைப் பதிவிறக்கம் செய்ய வேண்டாம் என்றும் மோசடிக்காரர்கள் வலியுறுத்துவார்கள்.



[போலி ஸ்கேம்ஷீல்ட் செயலியை நிறுவச் சொன்ன 'வங்கி ஊழியருக்கும்' பாதிக்கப்பட்டவருக்கும் இடையிலான உரையாடலின் ஸ்கிரீன்ஷாட்]

- மூன்றாம் தரப்பு அல்லது சந்தேகத்திற்குரிய தளங்களிலிருந்து செயலிகளைப் பதிவிறக்கம் செய்வதால் ஏற்படும் ஆபத்துகள் பற்றி அறிந்திருங்கள். அவ்வாறு செய்வதால் பாதிக்கப்பட்டவர்களின் கைபேசிச் சாதனங்களில் தீங்கு விளைவிக்கும் மென்பொருள் பொருத்தப்படலாம். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களுக்கு பதிலாக இணையப்பக்க முகவரி இணைப்புகள் வழியாக தீங்கு விளைவிக்கும் மென்பொருளால் பாதிக்கப்பட்ட செயலிகளை நிறுவக் கூறி மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களை ஏமாற்றுவார்கள்.
- அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள். உங்கள் சாதனத்தின் அமைவுகளில் உள்ள "Install Unknown App" அல்லது "Unknown Sources" என்பதை முடக்கவும்.
- உங்கள் கைப்பேசியில் ஸ்கேம்ஷீல்ட் செயலியைப் பதிவிறக்கம் செய்வது குறித்து மேலும் தெரிந்துகொள்ள, <https://www.scamshield.org.sg/setup-guide> என்ற அதிகாரத்துவ வழிகாட்டியைப் பார்க்கவும்.
- தீங்கு விளைவிக்கும் மென்பொருள் மற்றும் பயனர்கள் தங்கள் சாதனங்களைப் பாதுகாக்க எடுக்கக்கூடிய தடுப்பு நடவடிக்கைகள் பற்றி மேலும் அறிய, <https://www.csa.gov.sg/alerts-advisories/advisories/2021/ad-2021-008> என்ற சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பு (CSA) SingCERT ஆலோசனையைப் பார்க்கவும்.



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](http://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](http://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