

Weekly Scams Bulletin

A publication by the Singapore Police Force and the National Crime Prevention Council

Trending Scams in the past week:



Job Scam



Fake Friend Call Scam



Investment Scam



E-Commerce Scam (Variants)



Phishing Scam (Social Media)

Be wary if asked to download unknown apps to purchase items on Facebook or Instagram.

Scam Tactics

Victims would come across advertisements on Facebook or Instagram promoting the sale of Lunar New Year goodies. Upon clicking on the link of the advertisements, victims would be redirected to WhatsApp, Facebook, or Instagram messaging platforms.

Victims would be directed to download a malicious Android Package Kit (APK) to place their orders. Unknown to the victims, the APK file contains malware that grants scammers remote access to their devices.

Scammers can access victims' banking credentials when they make payments via the APK app. Victims would realise they had been scammed after they discovered unauthorised card/banking transactions.

Some Precautionary Measures:

ADD – ScamShield app to protect yourselves from scam calls and SMSes. Add anti-virus applications and ensure that these apps are updated to detect the latest malware. Also ensure your devices' operating systems and applications are updated regularly to be protected by the latest security patches.

CHECK – For scam signs and check with official sources (e.g. visit www.scamalert.sg or call the Anti-Scam Helpline on 1800-722-6688). Always shop on established e-commerce platforms. Visit www.go.gov.sg/MHAtsr to check the platform's Transaction Safety Rating. Only download applications from official app stores (i.e., Google Play Store for Android).

If you suspect your device has been infected by malware,

- Turn your phone to "flight mode" and switch off the Wi-Fi.
- Run an anti-virus scan on your device.
- Check your bank account/Singpass/CPF for any unauthorised transaction(s) using another device.

As a further precaution, consider doing a "factory reset" of your device and changing important passwords.

TELL – Authorities, family, and friends about scams. Report suspicious content/advertisements to Facebook or Instagram. Initiate in-app blocking by reporting the number linked to the advertisement to WhatsApp/Telegram.

Security Apps (Android)	Subscription*
▶ Avast Antivirus & Security	Free
▶ AVG Antivirus & Security	Free
▶ Kaspersky Antivirus & VPN	Paid
▶ Lookout Security and Antivirus	Paid
▶ McAfee Security: VPN Antivirus	Paid
▶ Mobile Security & Antivirus (Trend Micro)	Paid
▶ Norton360 Antivirus and Security	Paid
Security Apps (iOS)*	Subscription*
▶ Avast Security & Privacy	Free
▶ AVG Mobile Security	Free
▶ Kaspersky: VPN & Antivirus	Paid
▶ Lookout - Mobile Data Security	Paid
▶ McAfee Security: Privacy & VPN	Paid
▶ Norton360 Security & VPN	Paid
▶ TM Mobile Security	Paid

*Subscription fees may be required to unlock more features.
*These apps are unable to scan other iOS apps for malware due to Apple's security restrictions.

CSA's list of recommended anti-virus apps



Screenshots of the fraudulent Facebook advertisement

For more information on this scam, visit [SPF | News \(police.gov.sg\)](https://www.spf.gov.sg/news)



ADD
ScamShield app and security features

CHECK
for scam signs and with official sources

TELL
Authorities, family and friends



SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

诈骗周报

新加坡警察部队和全国罪案防范理事会刊物

过去一周 诈骗趋势:



求职诈骗



假朋友来电骗局



投资诈骗



电子商务骗局
(各种手法)



钓鱼骗局 (社交媒体)

若在脸书或Instagram上购买物品时被要求下载未知应用，请务必小心。

诈骗手法

受害者会在脸书或Instagram上看到农历新年食品促销的广告。一旦点击广告上的链接，受害者将被转接至WhatsApp、脸书、或Instagram 通讯平台。

受害者将被引导下载恶意安卓软件包 (APK) 来下单。受害者不知道该APK文件含有恶意软件让骗子能远程进入他们设备。骗子可以在受害者通过APK应用进行支付时获取受害者的银行凭据。

受害者在发现自己的卡/银行账户有未经授权的交易时意识到自己被骗了。

一些预防措施:

添加 - ScamShield 应用程序屏蔽诈骗短信和电话。添加防毒应用程序并确保这些应用程序已更新，以便侦测最新的恶意软件。务必定期更新您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。

查证 - 官方消息并注意诈骗迹象 (如浏览www.scamalert.sg查询或拨打反诈诈骗热线[1800-722-6688](tel:1800-722-6688))。

务必在信誉良好的电子商务平台购物。浏览 <https://go.gov.sg/mhatsr> 查看平台的交易安全评级。只从官方应用商店下载应用程序 (即Apple Store或Google Play Store)。如果您怀疑您的移动设备已经受到恶意软件的感染，

- 请将手机转为“飞行模式”并关闭无线网络。
- 在手机进行防毒扫描。
- 使用另一台设备检查您的银行帐户/Singpass/CPF是否有未经授权的交易。

请考虑对您的设备进行“恢复出厂设置”并更改重要密码作为更进一步的安全措施。

通报 - 当局、家人和朋友诈骗案件趋势。向脸书或Instagram举报可疑内容/广告。向WhatsApp/Telegram举报与广告相关的号码，以便启动应用内的屏蔽功能。

Security Apps (Android)	Subscription*
▶ Avast Antivirus & Security	Free
▶ AVG Antivirus & Security	Free
▶ Kaspersky Antivirus & VPN	Paid
▶ Lookout Security and Antivirus	Paid
▶ McAfee Security: VPN Antivirus	Paid
▶ Mobile Security & Antivirus (Trend Micro)	Paid
▶ Norton360 Antivirus and Security	Paid
Security Apps (iOS)*	Subscription*
▶ Avast Security & Privacy	Free
▶ AVG Mobile Security	Free
▶ Kaspersky: VPN & Antivirus	Paid
▶ Lookout - Mobile Data Security	Paid
▶ McAfee Security: Privacy & VPN	Paid
▶ Norton360 Security & VPN	Paid
▶ TM Mobile Security	Paid

*Subscription fees may be required to unlock more features.
*These apps are unable to scan other iOS apps for malware due to Apple's security restrictions.

[新加坡网络安全局推荐的防毒应用程序清单]



[具欺诈性的脸书广告截图]

欲了解更多关于这个骗局的信息，请浏览 [SPF | News \(police.gov.sg\)](http://SPF | News (police.gov.sg))



ADD
ScamShield app and security features

CHECK
for scam signs and with official sources

TELL
Authorities, family and friends



SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:



Penipuan Pekerjaan



Penipuan Panggilan Kawan Palsu



Penipuan Pelaburan



Penipuan E-Dagang (Varian penipuan)



Penipuan Pancingan Data (Media Sosial)

Berhati-hati Jika anda diminta memuat turun aplikasi untuk membeli barangan di Facebook atau Instagram.

Taktik Penipuan

Mangsa akan terjumpa iklan di Facebook atau Instagram yang mempromosikan penjualan barangan Tahun Baru Cina.

Sebaik sahaja mangsa klik pada pautan yang terdapat di iklan tersebut, mangsa akan diarahkan ke platform pesanan WhatsApp, Facebook atau Instagram.

Mangsa akan diarahkan untuk memuat turun sebuah Kit Pakej Android (APK) berniat jahat untuk membuat pesanan. Tanpa pengetahuan mangsa, fail APK tersebut mengandungi perisian hasad yang membolehkan penipu mengakses peranti mangsa dari jarak jauh.

Penipu boleh mengakses butiran perbankan mangsa apabila mereka membuat pembayaran melalui aplikasi APK tersebut. Mangsa akan sedar mereka telah tertipu setelah mereka mendapati transaksi kad/perbankan tanpa kebenaran.

Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi Scamshield untuk melindungi diri anda daripada panggilan dan SMS penipuan. Masukkan aplikasi antivirus dan pastikan aplikasi ini dikemas kini untuk mengesan perisian hasad yang terkini. Pastikan juga sistem operasi dan aplikasi peranti anda dikemas kini dengan tetap supaya terlindung dengan patch keselamatan yang terkini.

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (boleh layari www.scamalert.sg atau telefon Talian Bantuan Antipenipuan di 1800-722-6688). Pastikan anda berbelanja di platform e-dagang yang mapan. Layari www.go.gov.sg/MHAtsr untuk memeriksa Rating Keselamatan Urus Niaga platform tersebut. Muat turun aplikasi hanya dari stor aplikasi rasmi (iaitu Google Play Store untuk Android).

Jika anda syak bahawa peranti anda telah dijangkiti perisian hasad,

- Tukar telefon anda ke “flight mode” (mod penerbangan) dan tutup Wi-Fi.
- Jalankan imbasan antivirus di peranti anda.
- Periksa akaun bank/Singpass/CPF anda untuk sebarang transaksi tanpa kebenaran yang menggunakan peranti lain.

Sebagai langkah berjaga-jaga seterusnya, pertimbangkan untuk melakukan “factory reset” (tetapan semula kilang) di peranti anda dan menukar kata laluan yang penting.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan kandungan/iklan yang mencurigakan kepada Facebook atau Instagram. Mulakan sekatan dalam aplikasi dengan melaporkan nombor yang berkaitan dengan iklan kepada WhatsApp/Telegram.

Security Apps (Android)	Subscription*
▶ Avast Antivirus & Security	Free
▶ AVG Antivirus & Security	Free
▶ Kaspersky Antivirus & VPN	Paid
▶ Lookout Security and Antivirus	Paid
▶ McAfee Security: VPN Antivirus	Paid
▶ Mobile Security & Antivirus (Trend Micro)	Paid
▶ Norton360 Antivirus and Security	Paid
Security Apps (iOS)*	Subscription*
▶ Avast Security & Privacy	Free
▶ AVG Mobile Security	Free
▶ Kaspersky: VPN & Antivirus	Paid
▶ Lookout - Mobile Data Security	Paid
▶ McAfee Security: Privacy & VPN	Paid
▶ Norton360 Security & VPN	Paid
▶ TM Mobile Security	Paid

*Subscription fees may be required to unlock more features.
*These apps are unable to scan other iOS apps for malware due to Apple's security restrictions.

Senarai aplikasi antivirus yang disyorkan CSA



Tangkap layar iklan Facebook menipu tersebut

Untuk maklumat lanjut mengenai penipuan ini, sila layari [SPF | News \(police.gov.sg\)](http://SPF | News (police.gov.sg))



ADD
ScamShield app and security features

CHECK
for scam signs and with official sources

TELL
Authorities, family and friends



SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:



வேலை மோசடி



போலி நண்பர் அழைப்பு மோசடி



முதலீட்டு மோசடி



இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)



தகவல் திருட்டு மோசடி (சமூக ஊடகம்)

ஃபேஸ்புக் அல்லது இன்ஸ்டாகிராம் மூலம் பொருள் வாங்குவதற்கு முன்பின் தெரியாத செயலிகளைப் பதிவிறக்கம் செய்யச் சொன்னால் எச்சரிக்கையாக இருங்கள்.

மோசடி உத்திகள்

பாதிக்கப்பட்டவர்கள் சீனப் புத்தாண்டு தின்பண்டங்கள் சலுகை விலையில் விற்கப்படும் விளம்பரங்களை ஃபேஸ்புக்கில் அல்லது இன்ஸ்டாகிராமில் பார்ப்பார்கள்.

அவர்கள் அந்த விளம்பரங்களின் இணைப்பை அழுத்தியவுடன், வாட்ஸ்ஆப், ஃபேஸ்புக் அல்லது இன்ஸ்டாகிராம் தகவல் தளத்துடன் இணைக்கப்படுவார்கள்.

பாதிக்கப்பட்டவர்கள் பொருட்களை வாங்குவதற்கு அபாயகரமான ஆண்ட்ராய்ட் தொகுப்பை (APK) பதிவிறக்கம் செய்ய வழிகாட்டப்படும். அந்த APK கோப்பில் நச்சுநிரல் இருப்பதும், பாதிக்கப்பட்டவர்களின் சாதனங்களை மோசடிக்காரர்கள் தொலைநிலையிலிருந்து கட்டுப்படுத்த அது துணைபுரியும் என்பதும் பாதிக்கப்பட்டவர்களுக்குத் தெரியாது.

பாதிக்கப்பட்டவர்கள் APK செயலி வாயிலாகப் பொருளுக்குப் பணம் செலுத்தும்போது, அவர்களின் வங்கி விவரங்களை மோசடிக்காரர்களால் பெறமுடியும்.

பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்கில் அனுமதியின்றி அட்டை/ வங்கிப் பரிவர்த்தனைகள் செய்யப்பட்டிருப்பது தெரிய வரும்போதுதான் மோசடிக்கு உள்ளாகி இருப்பதை அவர்கள் உணர்வார்கள்.

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - மோசடி அழைப்புகள், குறுந்தகவல்கள் ஆகியவற்றிலிருந்து உங்களைப் பாதுகாத்துக்கொள்ள ஸ்கேம்ஷீல்டு செயலியைப் பதிவிறக்குங்கள்.

நச்சுத்தடுப்புச் செயலிகளைப் பதிவிறக்கம் செய்து, அண்மை நச்சுநிரலைக் கண்டுபிடிக்கும் வகையில் அவை புதுப்பிக்கப்படுவதை உறுதி செய்யுங்கள். அதோடு, அண்மை இடர்காப்பு இயக்கங்களுடன் உங்கள் சாதனங்களைப் பாதுகாக்க, சாதனத்தின் செயலியக்கமும் செயலிகளும் அடிக்கடி புதுப்பிக்கப்படுவதை உறுதி செய்யுங்கள்.

சரிபார்க்க - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (எ.கா. www.scamalert.sg இணையத்தளத்தை நாடலாம் அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம்).

எப்போதுமே பெயர்ப்பெற்ற இணைய வர்த்தகத் தளங்களிலிருந்து மட்டும் வாங்குங்கள். தளங்களின் பரிவர்த்தனை பாதுகாப்புத் தரத்தைக் கண்டறிய www.go.gov.sg/MHAtsr இணையத்தளத்தை நாடுங்கள். அதிகாரபூர்வச் செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள் (அதாவது, ஆண்ட்ராய்ட் செயலியக்கத்திற்கு கூகல் பிளே ஸ்டோர்). உங்கள் சாதனம் நச்சுநிரலால் பாதிக்கப்பட்டிருப்பதாகச் சந்தேகம் எழுந்தால்,

- உங்கள் கைப்பேசியை "flight mode" இயக்கத்திற்கு மாற்றி, Wi-Fi அருகலை இணைப்பை அடைத்துவிடுங்கள்.
- உங்கள் சாதனத்தில் நச்சுத்தடுப்பு சோதனையை மேற்கொள்ளுங்கள்.
- வேறொரு சாதனத்தைப் பயன்படுத்தி உங்கள் வங்கிக் கணக்கு/ சிங்பாஸ் / மத்திய சேம நிதி எதிலாவது அனுமதியின்றி பரிவர்த்தனைகள் செய்யப்பட்டிருக்கிறதா எனப் பாருங்கள்.

கூடுதல் முன்னெச்சரிக்கையாக, உங்கள் சாதனத்தை "factory reset" செய்து, முக்கியமான கடவுச்சொற்களை மாற்றிவிடுங்கள்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். சந்தேகத்திற்குரிய உள்ளடக்கத்தை/ விளம்பரங்களை ஃபேஸ்புக்கிடம் அல்லது இன்ஸ்டாகிராமிடம் புகார் செய்யுங்கள். விளம்பரத்துடன் இணைக்கப்பட்ட எண்ணை வாட்ஸ்ஆப்பிடம் / டெலிகிராமிடம் புகார் செய்வதன்வழி செயலியின் தடுப்பு இயக்கத்தைச் செயல்படுத்துங்கள்.

இந்த மோசடி குறித்த மேல் விவரங்களுக்கு, [SPF | News \(police.gov.sg\)](http://SPF | News (police.gov.sg)) இணையத்தளத்தை நாடுங்கள்.

Security Apps (Android)	Subscription*
Avast Antivirus & Security	Free
AVG Antivirus & Security	Free
Kaspersky Antivirus & VPN	Paid
Lookout Security and Antivirus	Paid
McAfee Security: VPN Antivirus	Paid
Mobile Security & Antivirus (Trend Micro)	Paid
Norton360 Antivirus and Security	Paid
Security Apps (iOS)*	Subscription*
Avast Security & Privacy	Free
AVG Mobile Security	Free
Kaspersky: VPN & Antivirus	Paid
Lookout - Mobile Data Security	Paid
McAfee Security: Privacy & VPN	Paid
Norton360 Security & VPN	Paid
TM Mobile Security	Paid

*Subscription fees may be required to unlock more features.
*These apps are unable to scan other iOS apps for malware due to Apple's security restrictions.

CSA பரிந்துரைக்கும் நச்சுத்தடுப்புச் செயலிகளின் பட்டியல்

facebook Log In

King Corn - Singapore's post

King Corn - Singapore

Cameron Highlands' Sweetest Corn in the World?

White Pearl Corn 白珍珠玉米
Black Pearl Corn 黑珍珠玉米
Yellow Pearl Corn 黄珍珠玉米

King Corn's pearl corn is grown in the nutrient-rich soil of Cameron Highlands.

Cameron Highlands Well Cultivated Maize

White Pearl Corn \$2 / per pcs

Black Pearl Corn \$1.8 / per pcs

Yellow Pearl Corn \$1.3 / per pcs

The more you buy, the more discounts you get

MESSANGER King Corn - Singapore Wholesale and supply shop SEND MESSAGE

ஃபேஸ்புக்கில் வெளியிடப்பட்ட மோசடி விளம்பரத்தின் திரைக்காட்சிகள்

I Can ACT Against Scams

ADD
ScamShield app and security features

CHECK
for scam signs and with official sources

TELL
Authorities, family and friends



SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY