Issue 33 3 Nov 2023

Weekly Scams Bulletin

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

Trending Scams in the past week:

Fake Friend Call Scam

Job Scam

Investment Scam

E-Commerce Scam (Variants)

Phishing Scam (Calls Impersonating Government Agencies)

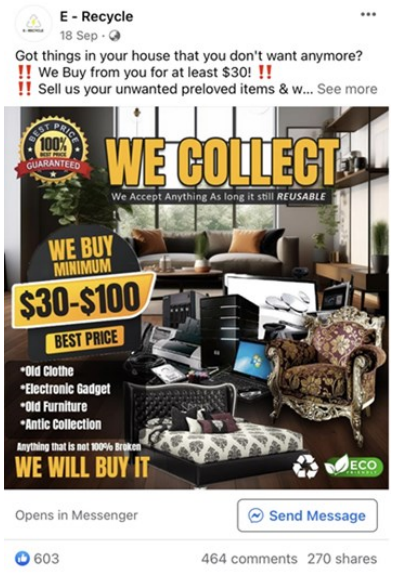
Interested in buying second-hand items from Facebook? Be wary of scammers asking you to download malicious apps to make payment!

Scam Tactics

Scammers would post advertisements for various second-hand items (such as clothes, electronics, furniture) on social media platforms like Facebook. After victims responded to the advertisements, they would be asked to communicate on WhatsApp.

When both parties came to an agreement on the prices for the second-hand goods, victims would be asked to download an Android Package Kit (APK) to receive deposit payment and invoice.

The APK is an application created for Android's operating system, which contains malware, and allow scammers to access to the victim's device to steal banking credentials and passwords. Victims would realise they were scammed after discovering unauthorised transactions were made from their bank accounts.



[Example of a fraudulent Facebook advertisement]

Some Precautionary Measures:

ADD – ScamShield to protect yourself against scam calls and SMSes. Add Anti-virus/anti-malware applications from official app stores to your device and update it regularly with the latest security patches.

CHECK – For scam signs with official sources (e.g. ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot, call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg). Be wary if asked to download unknown apps to purchase or sell items on Facebook.

Check the developer information on the app, the number of app downloads and app user reviews to ensure it is a reputable and legitimate application. Only download from official app stores (i.e. Google Play for Android). Do not grant permissions for access to device hardware or data to unknown apps.

TELL – authorities, family, and friends about scams. Report the number to WhatsApp to initiate in-app blocking and report any fraudulent transactions to your bank immediately.

Anti-Virus 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
Anti-Virus 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.

[List of Recommended Anti-Virus Apps provided by the Cyber Security Agency of Singapore]

For more information on this scam, visit SPF | News (police.gov.sg)

33号刊 2023年11月3日

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:

假朋友来电骗局

求职诈骗

投资诈骗

电子商务骗局
(各种手法)

钓鱼骗局
(冒充政府部门来电)

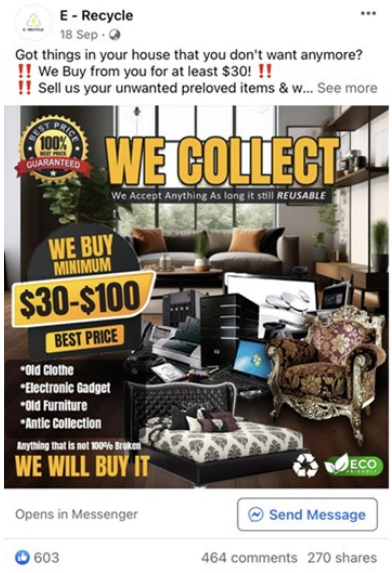
有兴趣从脸书购买二手物品吗?
提防要求您下载恶意应用程序付款的骗子!

诈骗手法

骗子会在如脸书的社交媒体平台刊登各种二手物品的广告(如衣服、电子产品、家具)。回应广告后,受害者会被要求通过WhatsApp沟通。

双方对二手物品价格达成协议后,受害者会被要求下载一个安卓应用程序包(APK)以接收订金付款 和发票。为安卓操作系统创建的安卓软件包含有恶意软件,允许骗子访问受害者的设备窃取银行凭证和密码。

受害者在发现自己的银行账户有未经授权的交易时,意识到自己被骗了。



【具欺诈性的脸书广告列子】

一些预防措施:

添加 – ScamShield 应用程序屏蔽诈骗短信和电话。从官方应用程序商店下载防毒/反恶意软件应用程序并定期更新最新的安全补丁。

查证 – 官方消息并注意诈骗迹象(如查询ScamShield WhatsApp 机器人@ https://go.gov.sg/scamshield-bot、拨打反诈骗热线1800-722-6688或到游览www.scamalert.sg)。若您被要求下载未知的应用程序以便在脸书购买或出售物品,务必保持警惕。

查看应用程序开发人员的信息与下载和用户评论的次数确保它是一个信誉良好并正当的应用程序。只从官方应用程序商店(即Apple Store或Google Play Store)下载。 不要授权未知应用程序访问设备硬件或数据。

通报 – 当局、家人和朋友诈骗案件趋势。立即向WhatsApp 举报号码并启动应用程序内的封锁机制以及向银行举报任何欺诈性的交易。

Anti-Virus 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
Anti-Virus 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.

【新加坡网络安全局推荐的防毒应用程序清单】

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

I Can ACT Against Scams

ADD ScamShield app and security features

CHECK for scam signs and with official sources

TELL Authorities, family and friends

NATIONAL CRIME PREVENTION COUNCIL

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Isu no. 33 3 Nov 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Panggilan Kawan Palsu

Penipuan Pekerjaan

Penipuan Pelaburan

Penipuan E-Dagang (Varian penipuan)

Penipuan Pancingan Data (Panggilan Menyamar Sebagai Agensi Pemerintah)

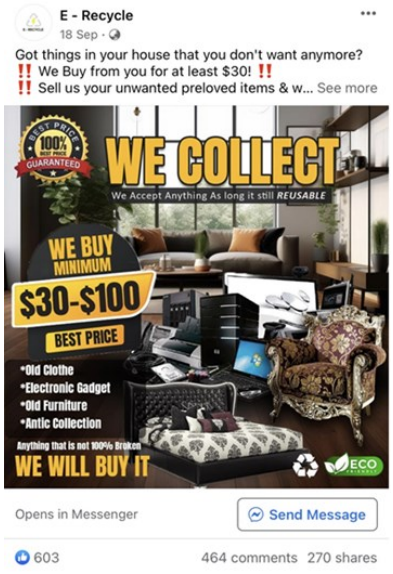
Berminat untuk membeli barangan terpakai di Facebook? Berhati-hati dengan penipu yang meminta anda memuat turun aplikasi berniat jahat untuk membuat bayaran!

Taktik Penipuan

Penipu akan menghantar iklan untuk pelbagai barangan terpakai (seperti pakaian, barangan elektronik, perabot) di platform media sosial seperti Facebook. Setelah mangsa menjawab iklan tersebut, mereka akan diminta supaya berkomunikasi di WhatsApp.

Setelah kedua pihak bersetuju dengan harga untuk barangan terpakai tersebut, mangsa akan diminta supaya memuat turun satu aplikasi Kit Pakej Android (APK) untuk menerima bayaran wang cengkeram dan invois. APK tersebut adalah satu aplikasi yang dicipta untuk sistem operasi Android, yang mengandungi perisian hasad, dan membenarkan penipu mendapatkan akses ke peranti mangsa untuk mencuri butiran dan kata laluan perbankan.

Mangsa akan menyedari bahawa mereka telah ditipu selepas mendapati transaksi tanpa kebenaran telah dibuat daripada akaun bank mereka.



[Contoh sebuah iklan Facebook menipu]

Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi antivirus/antiperisian hasad daripada gedung aplikasi rasmi ke peranti anda dan kemas kini ia dengan tetap dengan patch keselamatan terkini.

PERIKSA - Tanda-tanda penipuan dan dengan sumber-sumber rasmi (misalnya periksa dengan bot ScamShield WhatsApp di https://go.gov.sg/scamshield-bot, telefon Talian Bantuan Antipenipuan di 1800-722-6688, atau layari www.scamalert.sg).

Berhati-hati jika anda diminta supaya memuat turun aplikasi yang tidak dikenali untuk membeli atau menjual barang di Facebook. Perikasa maklumat pemaju di aplikasi tersebut, bilangan muat turun dan ulasan pengguna untuk memastikan aplikasinya mempunyai reputasi yang baik dan sah. Muat turun aplikasi hanya daripada gedung aplikasi rasmi (misalnya Google Play untuk Android).

Jangan beri keizinan untuk akses ke perkakasan atau data peranti ke aplikasi yang tidak diketahui.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan nombor tersebut kepada WhatsApp untuk memulakan penyekatan dalam aplikasi, dan laporkan sebarang transaksi menipu kepada bank anda dengan segera.

Anti-Virus 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
Anti-Virus 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.

[Senarai Aplikasi Antivirus yang Disarankan yang telah disediakan oleh Agensi Keselamatan Siber Singapura]

Untuk maklumat lanjut mengenai penipuan ini, sila layari SPF | News (police.gov.sg)

I Can ACT Against Scams

ADD ScamShield app and security features

CHECK for scam signs and with official sources

TELL Authorities, family and friends

NATIONAL CRIME PREVENTION COUNCIL

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

வெளியீடு எண். 33

3 நவம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

போலி நண்பர் அழைப்பு மோசடி

வேலை மோசடி

முதலீட்டு மோசடி

இணைய வர்த்தக மோசடி (பல்வேறு

தகவல் திருட்டு மோசடி (அரசாங்க அமைப்புகளைப் போல ஆள்மாறாட்டம் செய்யும் அழைப்புகள்)

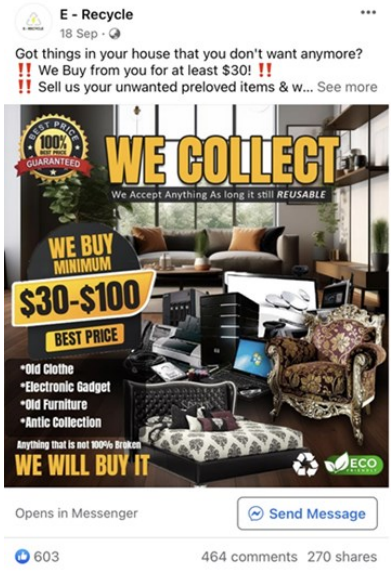
ஃபேஸ்புக்கிலிருந்து பிறர் பயன்படுத்தியப் பொருட்களை வாங்க ஆர்வமா? கட்டணம் செலுத்த தீங்கிழைக்கும் செயலிகளைப் பதிவிறக்கம் செய்யச் சொல்லும் மோசடிக்காரர்கள் குறித்து எச்சரிக்கையாக இருங்கள்!

மோசடி உத்திகள்

மோசடிக்காரர்கள் பிறர் பயன்படுத்திய பல்வேறு பொருட்களின் (ஆடைகள், மின்னணுவியல், அறைகலன் போன்றவை) விளம்பரங்களை ஃபேஸ்புக் போன்ற சமூக ஊடகத் தளங்களில் பதிவு செய்வார்கள். அந்த விளம்பரங்களுக்குப் பாதிக்கப்பட்டவர்கள் பதில் அளித்த பிறகு, அவர்கள் வாட்ஸ்ஆப்பில் உரையாடுமாறு கேட்டுக்கொள்ளப்படுவர்.

இரு தரப்பினரும் பிறர் பயன்படுத்தியப் பொருட்களுக்கான விலைகளை ஒப்புக்கொண்ட பிறகு, வைப்புத் தொகையையும் விலைப்பட்டியலையும் பெறுவதற்கு ஒரு Android Package Kit (APK) செயலியைப் பதிவிறக்கம் செய்யுமாறு பாதிக்கப்பட்டவர்கள் கேட்டுக்கொள்ளப்படுவார்கள். APK என்பது ஆண்ட்ராய்ட் இயங்குதளத்துக்காக உருவாக்கப்பட்ட ஒரு செயலியாகும். இதில் தீங்கு விளைவிக்கும் மென்பொருள் உள்ளது. இது மோசடி செய்பவர்கள் வங்கி உள்நுழைவு விவரங்களையும் கடவுச் சொற்களையும் திருட பாதிக்கப்பட்டவரின் சாதனத்தை அணுக அனுமதிக்கிறது.

அங்கீகரிக்கப்படாத பரிவர்த்தனைகள் தங்கள் வங்கிக் கணக்குகளிலிருந்து செய்யப்பட்ட பிறகு தாங்கள் மோசடி செய்யப்பட்டிருப்பதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



[மோசடி ஃபேஸ்புக் விளம்பரத்தின் உதாரணம்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - உங்கள் சாதனத்தில் நச்சுநிரல் தடுப்புச் செயலிகளை அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டும் பதிவிறக்கம் செய்து, புதிய பாதுகாப்பு அம்சங்களை உடனுக்குடன் சேர்த்திடுங்கள்.

சரிபார்க்க - மோசடி அறிகுறிகளை அதிகாரபூர்வத் தகவல் மூலங்களுடன் சரிபாருங்கள் (எ.கா. ஸ்கேம்ஷீல்டு வாட்ஸ்ஆப் பொட் @ https://go.gov.sg/scamshield-bot நாடலாம், மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம், அல்லது www.scamalert.sg இணையத்தளத்தை நாடலாம்).

ஃபேஸ்புக்கில் பொருட்களை வாங்குவதற்கோ விற்பதற்கோ தெரியாத செயலிகளைப் பதிவிறக்கம் செய்யச் சொன்னால் எச்சரிக்கையாக இருங்கள். செயலியின் உருவாக்குநர் தகவல், பதிவிறக்கங்களின் எண்ணிக்கை மற்றும் பயனர் மதிப்பாய்வுகளை சரிபார்த்து அதன் நம்பகத்தன்மையை உறுதி செய்யவும். அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள் (அதாவது ஆண்ட்ராய்டுக்கான கூகிள் பிளே ஸ்டோர்). தெரியாத செயலிகளுக்கு சாதனத்தின் வன்பொருள் அல்லது தரவை அணுகுவதற்கான அனுமதிகளை வழங்க வேண்டாம்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். அந்த எண்ணைத் தடுக்க வாட்ஸ்ஆப்பில் புகார் செய்வதோடு, எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.

Anti-Virus 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
Anti-Virus 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.

[சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பு வழங்கும் பரிந்துரைக்கப்பட்ட Anti-Virus செயலிகளின் பட்டியல்]

இந்த மோசடி குறித்த மேல் விவரங்களுக்கு, SPF | News (police.gov.sg) இணையத்தளத்தை நாடுங்கள்.