Issue 27 22 Sep 2023

Weekly Scams Bulletin

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

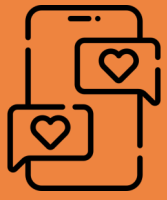
Trending Scams in the past week:

Investment Scam

Job Scam

Fake Friend Call Scam

E-Commerce Scam (Variants)



Credit-for-Sex

E-Commerce Scams: Avoid paying through links or third-party apps

Scam Tactics

Scammers would post attractive listings/advertisements online (Facebook, Carousell, Instagram/Telegram) featuring the latest products, like handphones. Once the victim shows interest, the conversation would transit to WhatsApp.

Scammers would provide links that require victims to download an APK file:

(a) To secure the order and/or make payment; or

(b) After making a payment via PayNow/bank transfer, victim is informed the order cannot be fulfilled and the link/download will facilitate the refund.

The APK file contains malware, to collect and send personal data from victims' phones to the scammers.

Victims would realise they had been scammed when goods were not received, seller became unresponsive or unauthorised bank transactions were made from their accounts.

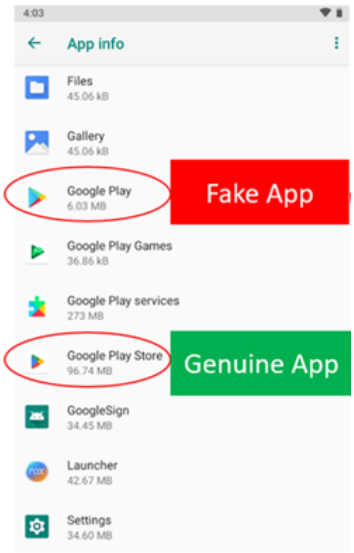
[Scammer acting as "bank staff" inviting victim to download fake ScamShield App]

Some Precautionary Measures:

ADD – Anti-virus/anti-malware applications from official app stores to your device and update it regularly with the latest security patches.

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.



[Screenshot of How Genuine and Fake Apps Appear in Your ICT Devices]

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

27 号刊 2023年9月22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:

投资诈骗

求职诈骗

假朋友来电骗局

电子商务骗局
（各种手法）

充值援交

电子商务骗局: 避免通过链接或第三方应用程序付款

诈骗手法

骗子会在网上（脸书，Carousell，Instagram/Telegram）发布如手机等最新产品的广告/清单。一旦受害者表示对产品感兴趣，骗子就会把对话转移到WhatsApp继续。

骗子会提供链接，要求受害者下载APK文档:

(a) 以确认订单和/或付款；或

(b) 利用PayNow /银行转账付款后，受害者被告知无法履行订单 ，而链接/下载APK文档将方便退款。

该APK文档含有恶意软件，用来收集受害者手机里的个人资料，并将这些资料发送给骗子。

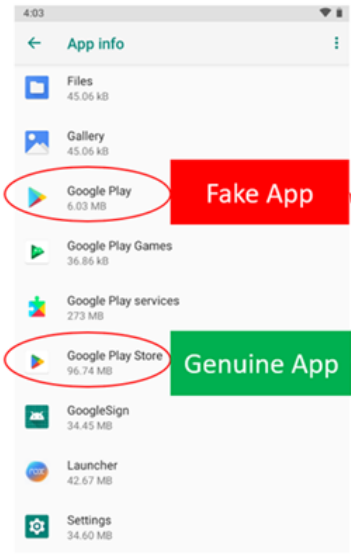
[骗子充当'银行职员'，邀请受害者下载假的 ScamShield 应用程序]

一些预防措施：

添加 – 官方应用程序商店内的防毒/反恶意软件应用 程序并定期更新最新的安全补丁。

查证 – 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。



[正当与假冒应用程序在您的资讯及通讯科技设备上所呈现的样貌截图]

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. 27 22 Sep 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Pelaburan

Penipuan Pekerjaan

Penipuan Panggilan Kawan Palsu

Penipuan E-Dagang (Varian penipuan)

Kredit-untuk-Seks

Penipuan E-Dagang: Elakkan daripada membayar melalui pautan atau aplikasi pihak ketiga

Taktik Penipuan

Penipu akan menyiarkan penyenaraian atau iklan yang menarik di platform dalam talian (Facebook, Carousell, Instagram/Telegram) yang menampilkan produk terkini, seperti telefon bimbit. Sebaik sahaja mangsa menunjukkan minat, perbualan akan beralih ke WhatsApp.

Penipu akan mengirimkan pautan yang memerlukan mangsa memuat turun sebuah fail APK:

(a) Untuk menjamin pesanan pembelian tersebut dan/atau membuat pembayaran; atau

(b) Selepas membuat pembayaran melalui PayNow/ pemindahan bank, mangsa dimaklumkan pesanan pembelian tersebut tidak dapat dipenuhi dan pautan /muat turun tersebut akan memudahkan urusan pembayaran balik.

Fail APK tersebut mengandungi perisian hasad, untuk mengumpul dan menghantar data peribadi daripada telefon mangsa kepada penipu.

Mangsa hanya akan menyedari mereka sudah ditipu apabila barang tidak diterima, penjual menjadi tidak responsif atau transaksi bank tanpa kebenaran telah dibuat di akaun bank mereka.

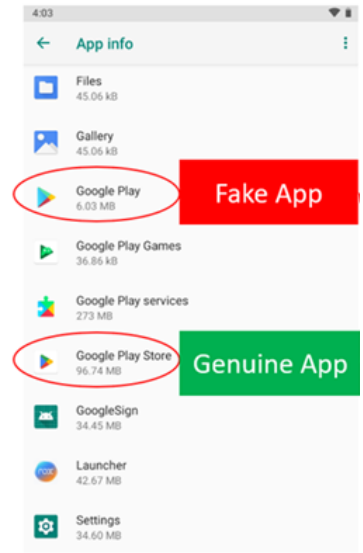
[Penipu yang menyamar sebagai seorang "kakitangan bank" menjemput mangsa untuk memuat turun Aplikasi ScamShield palsu]

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 – 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.



[Tangkap layar Bagaimana Aplikasi Tulen dan Palsu Muncul dalam Peranti ICT Anda]

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. 27

22 செப்டம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி

முதலீட்டு மோசடி

வேலை மோசடி

போலி நண்பர் அழைப்பு மோசடி

இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)

பாலியல் தொடர்பான பண மோசடி

இணைய வர்த்தக மோசடிகள்: இணைப்புகள் அல்லது மூன்றாம் தரப்பு செயலிகள் மூலம் பணம் செலுத்துவதைத் தவிர்த்திடுங்கள்

மோசடி உத்திகள்

கைப்பேசி போன்ற சமீபத்திய தயாரிப்புகளைக் கொண்ட கவர்ச்சிகரமான பட்டியல்கள் / விளம்பரங்களை மோசடிக்காரர்கள் இணையத்தில் (எ.கா. பேஸ்புக், கேரோசல், இன்ஸ்டாகிராம் / டெலிகிராம்) பதிவிடுவார்கள். பாதிக்கப்பட்டவர் ஆர்வம் காட்டியவுடன், உரையாடல் வாட்ஸ்ஆப்பில் தொடரும்.

APK கோப்பைப் பதிவிறக்கம் செய்வதற்கான இணைப்புகளை மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்கு வழங்குவார்கள்:

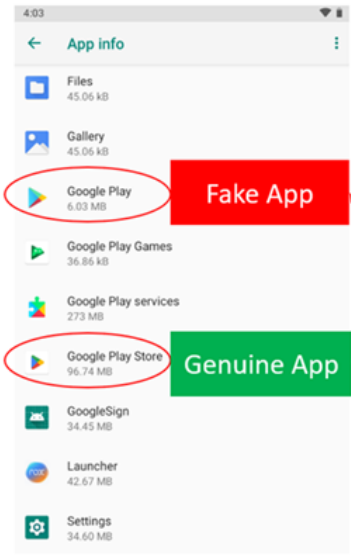
(a) ஆர்டரை உறுதிப்படுத்த மற்றும் / அல்லது கட்டணம் செலுத்த; அல்லது

(b) PayNow / வங்கி பரிமாற்றம் மூலம் பணம் செலுத்திய பிறகு, அந்த ஆர்டரை நிறைவேற்ற முடியாது என்றும், அந்த இணைப்பு / பதிவிறக்கம் பணத்தைத் திரும்பப் பெருவதற்கு வழிவகுக்கும் என்றும் பாதிக்கப்பட்டவருக்கு தெரிவிக்கப்படுகிறது.

APK கோப்பில் தீங்கு விளைவிக்கும் மென்பொருள் இருக்கும். இது பாதிக்கப்பட்டவர் தொலைபேசிகளில் இருந்து தனிப்பட்ட தரவுகளை சேகரித்து மோசடிக்காரர்களுக்கு அனுப்பும்.

தங்கள் பொருட்களைப் பெறாதபோது, விற்பனையாளர் பதிலளிக்காதபோது அல்லது அங்கீகரிக்கப்படாத வங்கி பரிவர்த்தனைகள் அவர்களின் கணக்குகளில் செய்யப்படும்போது மட்டுமே தாங்கள் மோசடி செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள்.

[போலி ஸ்கெம்ஷீல்டு செயலியைப் பதிவிறக்கம் செய்ய பாதிக்கப்பட்டவரைக் கேட்டுக்கொள்ளும் "வங்கி ஊழியராக" நடிக்கும் மோசடிக்காரர்]



[உங்கள் தகவல் தொடர்பு தொழில்நுட்ப சாதனங்களில் உண்மையான மற்றும் போலி செயலிகள் எப்படி இருக்கும் என்பதற்கான ஸ்கிரீன்ஷாட்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

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

சரிபார்க்க - 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.

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