Issue 28 29 Sep 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

Social Media Impersonation Scam

Phishing Scam (Calls Impersonating Government Agencies)

Beware of the links you click on: New variant of malware can control your device

Scam Tactics

Scammers would post advertisements for various items/ services (Food purchase, Home Cleaning, Pet Grooming, etc.) on social media platforms like Facebook/Instagram. Once the victim shows interest, the conversation would transit to WhatsApp.

Scammers would provide links to download an APK file that require granting access rights, for the victim to pay a deposit for the services via bank transfer. The APK file contains malware that steal the victim's banking credentials during the transfer.

Scammers would perform unauthorised transactions from the victim's bank accounts before remotely initiating a factory reset of the victims' devices.

Unauthorised transactions would only be noticed subsequently when victims re-install the banking apps on their devices or call the bank.

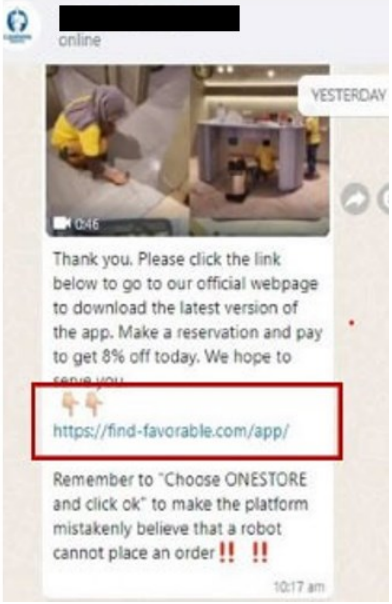
[Example of a fraudulent Facebook advertisement selling food products]

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.



[Victim of a fraudulent cleaning service advertisement invited to download application through a malicious link]

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

28 号刊 2023年9月29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
- 社交媒体冒充他人骗局
- 钓鱼骗局(冒充政府部门来电)

当心所点击的链接：新版的恶意软件可操控您的设备

诈骗手法

骗子会在如脸书，Instagram的社交媒体平台刊登各种服务的广告（购买食品、居家清洁、宠物美容等）。一旦受害者表现有兴趣，对话就会转移至WhatsApp。

骗子会提供需要授予访问权限的APK文档链接让受害者下载，以便通过银行转账支付服务定金。

APK文档含有可在转账过程中窃取受害者银行凭证的恶意软件。

骗子会从受害者的银行账户进行未经授权的交易，然后远程启动受害者设备的出厂重置。

受害者只有在重新安装银行应用程序或联系银行时才发现未经授权的交易。

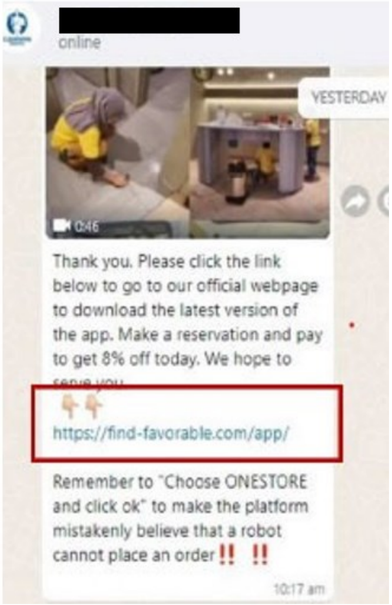
一些预防措施：

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。

[销售食品的欺诈性脸书广告例子]



[欺诈性清洁服务广告的受害者受邀通过恶意链接下载应用程序]

欲了解更多关于这个骗局的信息，请浏览 SPF | News

Isu no. 28 29 Sep 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 Penyamarandi Media Sosial
- Penipuan Pancingan Data (Panggilan Menyamar Sebagai Agensi Pemerintah)

Berhati-hati dengan pautan yang anda klik: Varian perisian hasad baharu yang boleh mengawal peranti anda

Taktik Penipuan

Penipu akan menyiarkan iklan di platform media sosial seperti Facebook/Instagram, untuk pelbagai perkhidmatan (Pembelian makanan, Pembersihan Rumah, Dandanan Haiwan Peliharaan, dan sebagainya.). Sebaik sahaja mangsa menunjukkan minat, perbualan akan beralih ke WhatsApp.

Penipu akan mengirimkan pautan untuk memuat turun sebuah fail APK yang memerlukan pemberian hak akses, untuk mangsa membayar wang pendahuluan untuk perkhidmatan tersebut melalui pemindahan bank.

Fail APK tersebut mengandungi perisian hasad yang mencuri butiran perbankan mangsa semasa pemindahan bank tersebut.

Penipu akan melakukan transaksi tanpa kebenaran daripada akaun bank mangsa sebelum memulakan tetapan semula kilang peranti mangsa dari jauh.

Mangsa hanya akan menyedari transaksi tanpa kebenaran telah dibuat apabila mereka memasang semula aplikasi perbankan pada peranti mereka atau ketika mereka menghubungi bank.

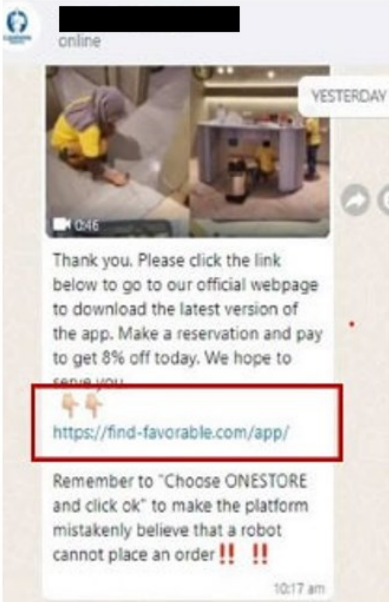
[Contoh iklan palsu yang menjual produk makanan di media sosial Facebook]

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.



[Mangsa satu iklan palsu yang menawarkan perkhidmatan pembersihan telah dijemput untuk memuat turun aplikasi melalui pautan berniat jahat]

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

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

போலி நண்பர் அழைப்பு மோசடி

வேலை மோசடி

முதலீட்டு மோசடி

சமூக ஊடக ஆள்மாறாட்ட மோசடி

தகவல் திருட்டு மோசடி (அரசாங்க அமைப்புகளைப் போல ஆள்மாறாட்டம் செய்யும் அழைப்புகள்)

நீங்கள் கிளிக் செய்யும் இணைப்புகள் குறித்து எச்சரிக்கையாக இருங்கள்: புதிய வகை தீங்கு விளைவிக்கும் மென்பொருளால் உங்கள் சாதனத்தைக் கட்டுப்படுத்த முடியும்

மோசடி உத்திகள்

ஃபேஸ்புக்/இன்ஸ்டகிராம் (Facebook/Instagram) போன்ற சமூக ஊடகத் தளங்களில் பல்வேறு சேவைகளுக்கான (உணவு வாங்குதல், வீட்டைச் சுத்தம் செய்தல், செல்லப்பிராணி பராமரிப்பு போன்றவை) விளம்பரங்களை மோசடிக்காரர்கள் இணையத்தில் பதிவிடுவார்கள். பாதிக்கப்பட்டவர் ஆர்வம் காட்டியவுடன், உரையாடல் வாட்ஸ்ஆப்பில் தொடரும்.

வங்கி பரிமாற்றம் மூலம் சேவைகளுக்கான வைப்புத்தொகையைச் செலுத்துவதற்கு மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்கு அணுகல் உரிமைகளை வழங்கும் APK கோப்பைப் பதிவிறக்கம் செய்யும் இணைப்புகளை வழங்குவார்கள்.வங்கி பரிமாற்றத்தின் போது பாதிக்கப்பட்டவரின் வங்கித் தகவல்களைத் திருடும் தீங்கு விளைவிக்கும் மென்பொருள் APK கோப்பில் உள்ளது.

மோசடிக்காரர்கள் பாதிக்கப்பட்டவரின் வங்கிக் கணக்குகளிலிருந்து அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைச் செய்வார்கள். அதன் பிறகு, தொலைவிலிருந்தே சாதனங்களில் உள்ள அனைத்தையும் அழித்து மீண்டும் தொடங்கும்படி (factory reset) செய்வார்கள்.

பாதிக்கப்பட்டவர்கள் தங்கள் சாதனங்களில் வங்கிச் செயலிகளை மீண்டும் நிறுவும்போதோ அல்லது வங்கியை அழைக்கும்போதோ மட்டுமே அவர்கள் அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைக் கவனிப்பார்கள்.

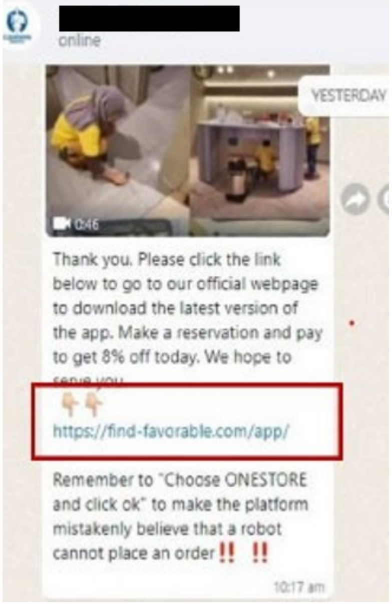
[உணவுப் பொருட்களை விற்கும் போலி ஃபேஸ்புக் விளம்பரத்தின் உதாரணம்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

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

சரிபார்க்க - 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.



[தீங்கிழைக்கும் இணைப்பின் மூலம் செயலியைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்பட்ட போலி துப்புரவு சேவை விளம்பரத்தால் பாதிக்கப்பட்ட ஒருவர்]

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