Issue 23 25 Aug 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

Fake Friend Call Scam

Job Scam

E-Commerce Scam (Rental of Units)

E-Commerce Scam (Electronics)

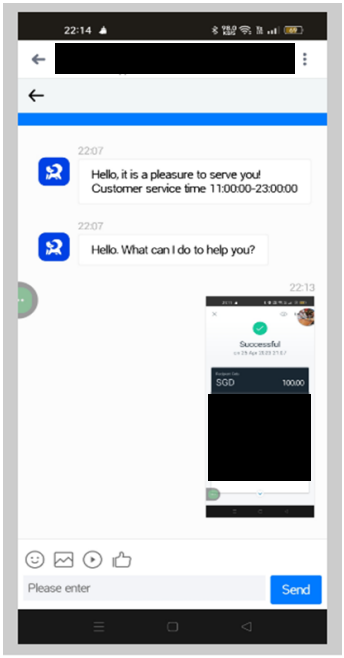
Loan Scams Involving Malicious App Downloads

Scam Tactics

Victims would receive attractive interest rates for loan offers through unsolicited text messages or from advertisements. To apply for the loan, victims would need to download and install an APK file. The APK file is a malware app to collect and send personal data from victims' phones to the scammers.

Scammers would then require them to pay various 'fees' to secure the loans. If victims refused, scammers would extort money from the victims using their personal data collected by the malware app.

Out of fear, victims would transfer money to local bank accounts provided by the scammers.



[Example of the malicious app downloaded by the victim]

Some Precautionary Measures:

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

CHECK – Disable "Install Unknown App" or "Unknown Sources" in your device settings.
Do not grant permission for access to unknown apps.
Check the app's number of downloads and user reviews to ensure it is a reputable and legitimate app.
Legitimate moneylending companies are not allowed to solicit loan applicants over the internet.

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.

Information which malware can extract on one's phone
GPS locations – track user's location
SMS – obtain One-Time Password (OTP) of users
Contact information – access user's contact list and contact numbers of the user's friends/family members
Device information – retrieve information about the user's device. For e.g. whether users are on Android or iOS, or what browser the users are using
Files stored in device storage, including photos, videos, installed apps, documents, etc – such private information can be used by scammers to threaten the users

[Information which malware can extract on one's phone]

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

23 号刊 2023年8月25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

假朋友来电骗局

求职诈骗

电子商务骗局
(单位出租)

电子商务骗局
(电子产品)

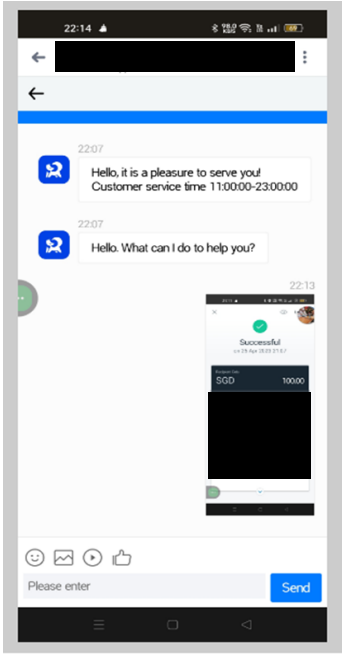
涉及下载恶意软件应用程序的贷款骗局

诈骗手法

受害者会通过未经请求的短信或广告获得具吸引力的贷款利率。受害者需下载并安装APK文档申请贷款。该APK文档是个恶意软件应用程序，并会在收集受害者手机内的个人资料后把资料发送给骗子。

骗子之后会要求受害者支付各种“费用”以便获得贷款。若受害者拒绝，骗子会利用恶意软件应用程序收集的个人资料向受害者进行勒索。

出于恐惧，受害者会将钱转入骗子提供的本地银行账户。



[受害者下载的恶意软件应用程序例子]

一些预防措施：

下载 – 防毒/反恶意软件应用程序并定期为您的设备安装最新的安全补丁。

查看 – 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。

不要授权访问未知应用程序。

查看应用程序的下载和用户评论次数，确保它是一个信誉良好并正当的应用程序。

正当并合法的贷款公司不能在网上招揽贷款申请人。

告知 – 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。

恶意软件可从手机上得到的信息
GPS定位 –追踪用户位置
简讯 -获取用户的一次性密码(OTP)
联系人资料 –访问用户的联系人名单以及用户朋友/家人的联络号码
设备资料 -获得有关用户设备的资料。例如，用户使用的是安卓或苹果手机，以及使用的浏览器
储存在设备储存空间的文档，包括照片、视频、已安装的应用程序、文件等。骗子会利用这些个人资料威胁用户

[恶意软件能从手机内得到的资料]

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

Isu no. 23

25 Ogos 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Pelaburan

Penipuan Panggilan Kawan Palsu

Penipuan Pekerjaan

Penipuan E-Dagang (Penyewaan Rumah)

Penipuan E-Dagang (Barangan Elektronik)

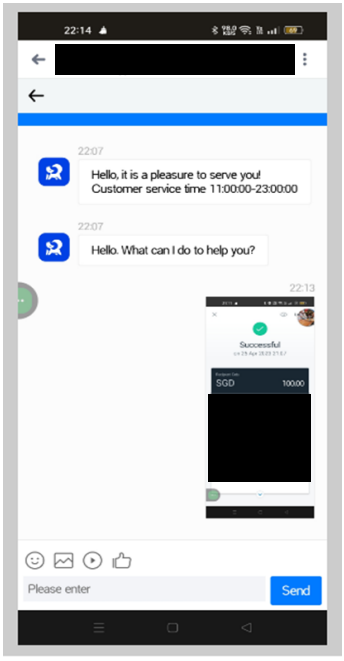
Penipuan Pinjaman yang melibatkan Muat Turun Aplikasi Niat Jahat

Taktik Penipuan

Mangsa akan menerima tawaran pinjaman dengan kadar faedah menarik melalui kiriman teks yang tidak diminta atau daripada iklan. Untuk memohon pinjaman itu, mangsa perlu memuat turun dan memasang sebuah fail APK. Fail APK tersebut adalah perisian hasad yang mengumpul dan menghantar data peribadi daripada telefon mangsa kepada penipu berkenaan.

Penipu akan memerlukan mangsa untuk membayar pelbagai 'yuran' bagi mendapatkan pinjaman itu. Jika mangsa enggan, penipu akan memeras ugut mangsa dengan menggunakan data peribadi mereka yang telah dikumpul oleh aplikasi perisian hasad.

Kerana rasa takut, mangsa akan memindahkan wang ke akaun bank tempatan yang disediakan oleh penipu.



[Contoh aplikasi berniat jahat yang dimuat turun oleh mangsa]

Beberapa langkah berjaga-jaga:

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

PERIKSA – Nyahdayakan "Install Unknown App" (Pasang Aplikasi yang Tidak Diketahui) atau "Unknown Sources" (Sumber yang Tidak Diketahui) di dalam tetapan peranti anda.

Jangan beri keizinan untuk mengakses aplikasi yang tidak diketahui.

Periksa bilangan muat turun dan ulasan pengguna aplikasi untuk memastikan ia mempunyai reputasi yang baik dan sah.

Syarikat pinjaman wang yang sah tidak dibenarkan memancing pemohon pinjaman melalui internet.

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.

Maklumat yang boleh dikeluarkan oleh perisian hasad daripada telefon seseorang
Lokasi GPS – menjejaki lokasi pengguna
SMS – mendapatkan Kata Laluan Guna Sekali (OTP) pengguna
Maklumat hubungan – mengakses senarai hubungan pengguna dan nombor telefon kawan/ ahli keluarga pengguna
Maklumat peranti – mendapatkan semula maklumat tentang peranti pengguna. Contohnya, sama ada pengguna menggunakan Android atau iOS, atau pelayar web apa yang digunakan oleh pengguna
Fail-fail yang disimpan dalam penyimpanan peranti, termasuk gambar, video, aplikasi-aplikasi yang dipasang, dokumen dan sebagainya – maklumat peribadi sedemikian boleh digunakan oleh penipu untuk mengugut para pengguna

[Maklumat yang mana perisian hasad boleh mengeluarkannya daripada telefon seseorang]

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

வெளியீடு எண். 23

25 ஆகஸ்ட் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

முதலீட்டு மோசடி

போலி நண்பர் அழைப்பு மோசடி

வேலை மோசடி

மின்-வர்த்தக மோசடி (ஓர் இடத்தை வாடகைக்கு எடுத்தல்)

மின்-வர்த்தக மோசடி (மின்னணுவியல்)

தீங்கிழைக்கும் செயலியைப் பதிவிறக்கம் செய்வதன் தொடர்பான கடன் மோசடிகள்

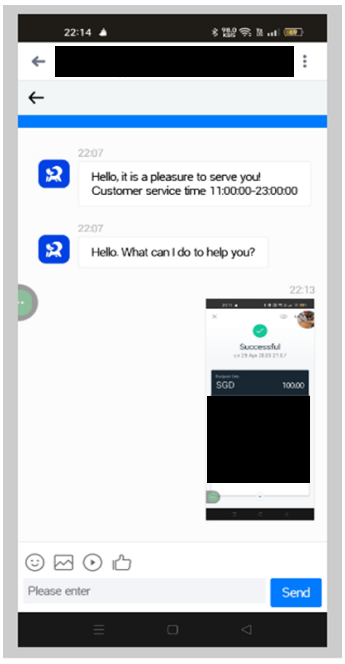
மோசடி உத்திகள்

கோரப்படாத குறுஞ்செய்திகள் அல்லது விளம்பரங்கள் மூலம் வழங்கப்படும் கடன்களுக்கு பாதிக்கப்பட்டவர்கள் கவர்ச்சிகரமான வட்டி விகிதங்கள் பெறுவர். பாதிக்கப்பட்டவர் கடனுக்காக விண்ணப்பிப்பதற்கு, ஒரு APK கோப்பைப் பதிவிறக்கம் செய்து நிறுவ வேண்டும். APK கோப்பு என்பது பாதிக்கப்பட்டவர்களின் தொலைபேசிகளிலிருந்து தனிப்பட்ட தரவுகளை சேகரித்து மோசடிக்காரர்களுக்கு அனுப்புவதற்கான ஒரு தீங்கு விளைவிக்கும் மென்பொருள் செயலியாகும்.

அவர்கள் கடன்களைப் பெறுவதற்கு பல்வேறு 'கட்டணங்களைச்' செலுத்த வேண்டும் என்று மோசடிக்காரர்கள் கூறுவார்கள்.

பாதிக்கப்பட்டவர்கள் மறுத்தால், தீங்கு விளைவிக்கும் மென்பொருள் செயலி மூலம் சேகரிக்கப்பட்ட தனிப்பட்ட தகவல்களைப் பயன்படுத்தி மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களிடமிருந்து பணம் பறிப்பார்கள்.

பயத்தின் காரணமாக, பாதிக்கப்பட்டவர்கள் மோசடிக்காரர்கள் வழங்கும் உள்ளூர் வங்கிக் கணக்குகளுக்கு பணத்தை மாற்றிவிடுவார்கள்.



[பாதிக்கப்பட்டவர் பதிவிறக்கம் செய்த தீங்கிழைக்கும் செயலியின் எடுத்துக்காட்டு]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்கவும் - உங்கள் சாதனத்தில் நச்சுநிரல் தடுப்புச் செயலிகளைப் பதிவிறக்கம் செய்து, புதிய பாதுகாப்பு அம்சங்களை உடனுக்குடன் சேர்த்திடுங்கள்.

சரிபார்க்கவும் - உங்கள் சாதனத்தில் உள்ள "Install Unknown App" அல்லது "Unknown Sources" இயக்கங்களை முடக்கி வைத்திருங்கள்.

உங்களுக்குத் தெரியாத செயலிகளுக்கு அணுகல் உரிமை வழங்காதீர்கள்.

ஒரு செயலி எத்தனை முறை பதிவிறக்கம் செய்யப்பட்டிருக்கிறது என்பதையும், அதன் பயன்பாட்டாளர்களின் கருத்துகளையும் சரிபார்த்து, அது நம்பகமான, சட்டபூர்வமான செயலிதானா என்பதை உறுதி செய்திடுங்கள். சட்டபூர்வமான கடன் கொடுக்கும் நிறுவனங்களுக்கு இணையத்தில் கடன் விண்ணப்பதாரர்களை கோர அனுமதியில்லை.

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

தீங்கு விளைவிக்கும் மென்பொருள் ஒருவரின் தொலைபேசியிலிருந்து எடுக்கக்கூடிய தகவல்
புவியிடங்காட்டி (GPS) - பயனரின் இருப்பிடத்தைக் கண்டறிய முடியும்
குறுஞ்செய்தி - பயனர்களின் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லைப் (OTP) பெற முடியும்
தொடர்புத் தகவல் - பயனரின் தொடர்பு பட்டியல் மற்றும் பயனரின் நண்பர்கள் / குடும்ப உறுப்பினர்களின் தொடர்பு எண்களை அணுக முடியும்
சாதனத் தகவல் - பயனரின் சாதனத்தைப் பற்றிய தகவல்களைப் பெற முடியும். எ.கா., பயனர்கள் Android அல்லது iOS பயன்படுத்துகிறார்களா, பயனர்கள் என்ன இணைய உலாவியைப் பயன்படுத்துகிறார்கள் போன்ற தகவல்கள்
புகைப்படங்கள், காணொளிகள், நிறுவப்பட்ட செயலிகள், ஆவணங்கள் ஆகியவை சாதனத்தில் சேமிக்கப்பட்டுள்ள கோப்புகள் - இத்தகைய தனிப்பட்ட தகவல்களை மோசடிக்காரர்கள் பயன்படுத்தி பயனர்களை அச்சுறுத்தலாம்

[தீங்கு விளைவிக்கும் மென்பொருள் ஒருவரின் தொலைபேசியிலிருந்து எடுக்கக் கூடிய தகவல்கள்]

இந்த மோசடி பற்றிய மேல் விவரங்களுக்கு, பார்வையிடவும் SPF | News (police.gov.sg)