Issue 24 1 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

Investment Scam

Job Scam

E-Commerce Scam (Concert Tickets)

Social Media Impersonation Scam

Scams Involving Malicious Dating Applications

Scam Tactics

Victims would receive in-app messages from scammers posing as females on TikTok or over dating applications before being asked to transit to WhatsApp.

Victims would be enticed to do a one-to-one video call while naked, date a girl or access nude female videos/ photographs.

Victims would then receive a link over WhatsApp to download and install an APK file. The APK file is a malware app that collects and sends personal data from victims' phones to the scammers.

After downloading and installing the APK file, scammers would retrieve victims' banking credentials once they log in to internet banking accounts. Subsequently, victims would discover unauthorised transactions on their banking accounts.

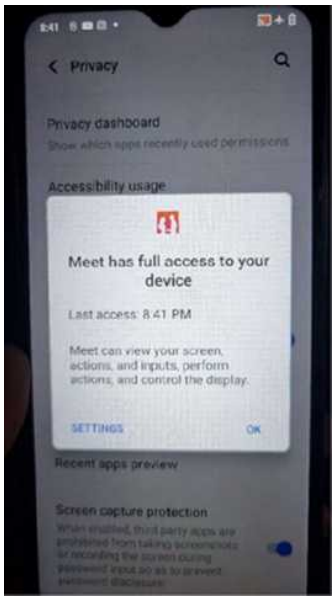
[Example of conversation asking the victim to download a malicious dating app]

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.



[Example of compromised device that gave full access to a malicious dating app]

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

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

投资诈骗

求职诈骗

电子商务骗局
(演唱会门票)

社交媒体
冒充他人骗局

涉及恶意软件约会应用程序的骗局

诈骗手法

受害者会在TikTok或约会应用程序中收到骗子假冒女性所发出的讯息。受害者之后被要求转移到WhatsApp。

受害者会被引诱进行一对一裸聊、与女生约会或观看女性裸体的视频/照片。

受害者会在WhatsApp收到链接下载并安装APK文档。

该APK文档是个恶意软件，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。

下载并安装APK文档后，骗子会在受害者登录网上银行账户时获得受害者的银行凭证。受害者过后会发现他们的银行账户有未经授权的交易。

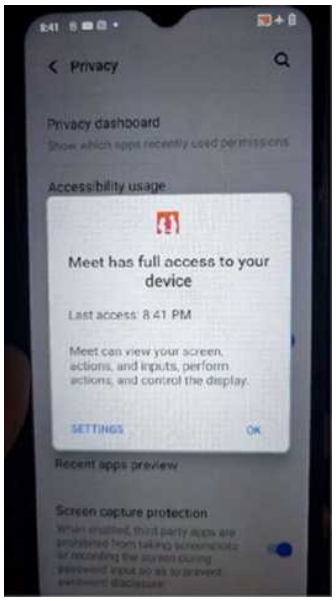
[要求受害者下载恶意软件约会应用程序的对话例子]

一些预防措施:

下载 – 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 。

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。



[设备因允许恶意软件约会应用程序所有权限而遭入侵的列子]

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

Isu no. 24 1 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 Pelaburan

Penipuan Pekerjaan

Penipuan E-Dagang (Tiket Konsert)

Penipuan Penyamaran di Media Sosial

Penipuan Melibatkan Aplikasi Cari Jodoh Berniat Jahat

Taktik Penipuan

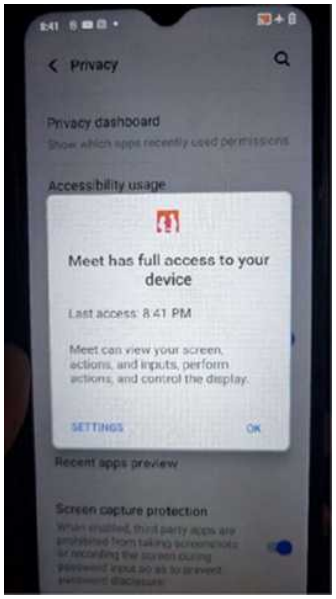
Mangsa akan menerima pesanan dalam aplikasi daripada penipu yang menyamar sebagai wanita di TikTok atau melalui aplikasi cari jodoh sebelum diminta untuk berpindah ke WhatsApp.

Mangsa akan dipikat supaya membuat panggilan video satu dengan satu semasa dalam keadaan bogel, membuat janji temu dengan seorang wanita atau mengakses video/gambar wanita bogel. Mangsa kemudian akan menerima satu pautan melalui WhatsApp untuk dimuat turun dan memasang satu fail APK. Fail APK tersebut merupakan sebuah aplikasi perisian hasad yang mengumpul dan menghantar data peribadi daripada telefon mangsa kepada penipu.

Setelah memuat turun dan memasang fail APK tersebut, penipu akan mendapatkan semula butiran perbankan mangsa sebaik sahaja mereka log masuk ke dalam akaun bank internet.

Seterusnya, mangsa akan mendapati adanya transaksi tanpa kebenaran di akaun perbankan mereka.

[Contoh perbualan meminta mangsa supaya memuat turun satu aplikasi cari jodoh berniat jahat]



[Contoh peranti yang telah dikompromi yang memberikan akses penuh ke sebuah aplikasi cari jodoh berniat jahat]

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.

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

வெளியீடு எண். 24

1 செப்டம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

போலி நண்பர் அழைப்பு மோசடி

முதலீட்டு மோசடி

வேலை மோசடி

மின்-வர்த்தக மோசடி (இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள்)

சமூக ஊடக ஆள்மாறாட்ட மோசடி

தீங்கிழைக்கும் டேட்டிங் செயலிகள் தொடர்பான மோசடிகள்

மோசடி உத்திகள்

டிக்டாக் அல்லது டேட்டிங் செயலிகளில் பெண்கள் போல் நடிக்கும் மோசடிக்காரர்களிடமிருந்து பாதிக்கப்பட்டவர்கள் செய்திகளைப் பெறுவார்கள். பின்னர், அவர்களை வாட்ஸ்ஆப் மூலம் தொடர்பு கொள்ளுமாறு கேட்டுக்கொள்வார்கள்.

பாதிக்கப்பட்டவர்கள் நிர்வாணமாக வீடியோ அழைப்புகள் (video call) செய்ய, ஒரு பெண்ணை டேட் செய்ய அல்லது நிர்வாணமான பெண் காணொளிகள் / புகைப்படங்களை அனுக தூண்டப்படுவார்கள். பாதிக்கப்பட்டவர்கள் பின்னர் ஒரு APK கோப்பினை பதிவிறக்கம் செய்து நிறுவுவதற்கான இணைப்பை வாட்ஸ்ஆப் மூலம் பெறுவார்கள். APK கோப்பு என்பது தீங்கு விளைவிக்கும் மென்பொருள் செயலியாகும். இது பாதிக்கப்பட்டவர்களின் தொலைபேசிகளில் இருந்து தனிப்பட்ட தரவுகளை சேகரித்து மோசடிக்காரர்களுக்கு அனுப்புகிறது.

APK கோப்பைப் பதிவிறக்கம் செய்து பொருத்திய பிறகு, பாதிக்கப்பட்டவர்கள் தங்கள் இணைய வங்கிச் சேவை கணக்குகளில் உள்நுழைந்தவுடன் அவர்களின் வங்கிச் சான்றுகளை மோசடிக்காரர்கள் பெற முடியும். அதனைத் தொடர்ந்து, பாதிக்கப்பட்டவர்கள் தங்கள் வங்கிக் கணக்குகளில் அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைக் கண்டுபிடிப்பார்கள்.

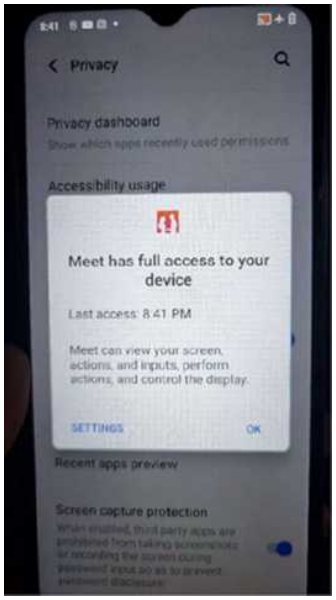
[தீங்கிழைக்கும் டேட்டிங் செயலியைப் பதிவிறக்கம் செய்யும்படி பாதிக்கப்பட்டவரைக் கேட்டுக்கொள்ளும் உரையாடலின் உதாரணம்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

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

சரிபார்க்கவும் - 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.

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



[தீங்கிழைக்கும் டேட்டிங் செயலிக்கு முழு அணுகல் வழங்கப்பட்டதால் சாதனம் பாதிக்கப்பட்டதற்கான எடுத்துக்காட்டு]

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