Issue 26 15 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 (Variants)

Loan Scam

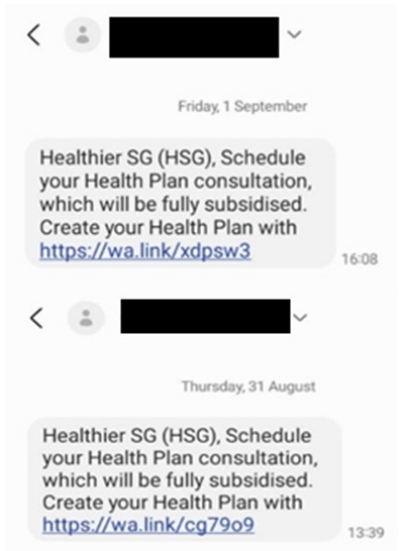
Fake SMS leading to the Download of a Fake HealthHub Application

Scam Tactics

Scammers would send a fake SMS claiming to be from "Healthier SG", asking victims to schedule a fully subsidised Health Plan consultation. The SMS contains a link that directs victims to a WhatsApp chat where they are prompted to download and install an APK file.

The APK file contains malware and allows scammers to gain remote access and control over the victims' devices. The malware also enables scammers to steal passwords stored on the device.

Victims would only know about this malicious app on their devices when unauthorised withdrawals are made from their bank accounts.



[Image of message sent to victims containing WhatsApp link]

Some Precautionary Measures:

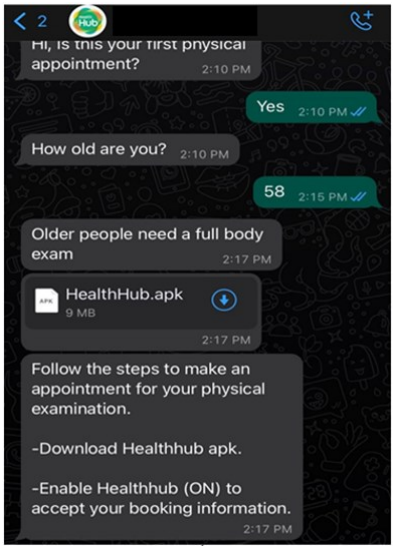
ADD – ScamShield App and set security features (e.g., enable 2FA for banks, social media, Singpass accounts; set transaction limits on internet banking transactions, including PayNow/PayLah).

CHECK – for scam signs and with official sources (e.g. check with ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot, call Anti-Scam Helpline at 1800-722-6688, or visit https://www.scamalert.sg/).

Only download and install apps from official app stores (i.e. Google Play Store for Android).

Official Healthier SG SMSes will always show the registered sender ID "MOH" and will not be sent via mobile phone numbers.

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



[Image of WhatsApp conversation with the scammer]

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

26 号刊 2023年9月15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

投资诈骗

求职诈骗

电子商务骗局
(各种手法)

贷款骗局

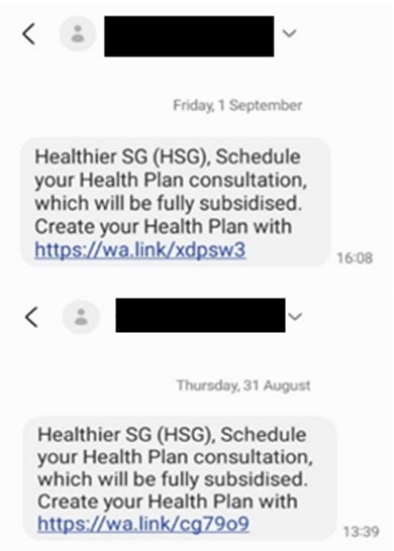
导致下载虚假保健资讯网(HealthHub) 应用程序的虚假短信

诈骗手法

骗子会发送一条声称来自“健康SG计划(Healthier SG)”的虚假短信，要求受害者安排一次全额补贴的保健护理咨询。该短信包含把受害者转往WhatsApp聊天室的链接，并提示受害者下载并安装APK文档。

该APK文档包含恶意软件，使骗子能远程访问和操控受害者的设备。该恶意软件也能让骗子窃取存储在设备里的密码。

受害者只在他们的银行账户出现未经授权提款时，才知道他们设备上存有此恶意应用程序。



[发送给受害者并包含WhatsApp链接的信息截图]

一些预防措施:

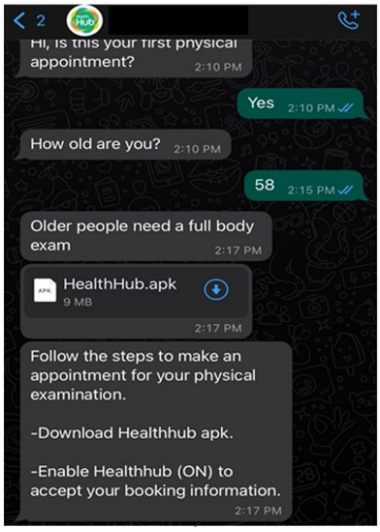
下载 – ScamShield应用程序并设置安全功能（如在银行,社交媒体，Singpass账户启用双重认证；设置银行交易限额，包括 PayNow/PayLah）。

查看 – 官方消息并注意诈骗迹象（如在不确定时与ScamShield WhatsApp 机器人@ https://go.gov.sg/scamshield-bot查询、拨打反诈骗热线1800-722-6688或到www.scamalert.sg了解最新诈骗手法。）

只从官方应用商店下载和安装应用程序 （即Apple Store或Google Play Store）。

官方健康SG计划短信都会显示是由“MOH”（卫生部的英文缩写）发出，并不会通过手机号码发出。

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。



[与骗子的WhatsApp聊天记录]

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

Isu no. 26 15 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 (Varian penipuan)

Penipuan Pinjaman

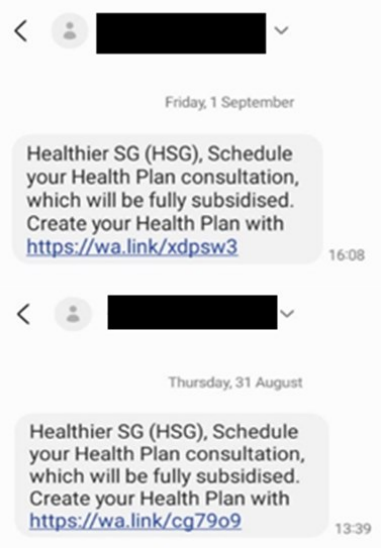
SMS palsu yang membawa kepada Muat turun satu Aplikasi HealthHub Palsu

Taktik Penipuan

Penipu akan menghantar satu SMS palsu yang mendakwa datang daripada "Healthier SG', meminta mangsa supaya menjadualkan satu konsultasi Pelan Kesihatan bersubsidi penuh. SMS tersebut mengandungi sebuah pautan yang mengarahkan mangsa ke sebuah perbualan WhatsApp yang mana mangsa akan didorong supaya memuat turun dan memasang sebuah fail APK.

Fail APK tersebut mengandungi perisian hasad dan membenarkan penipu untuk mendapatkan akses dan kawalan peranti mangsa dari jauh. Perisian hasad ini juga membolehkan penipu untuk mencuri kata laluan yang tersimpan di peranti.

Mangsa hanya akan tahu tentang aplikasi berniat jahat di peranti mereka apabila pengeluaran wang tanpa kebenaran dibuat dari bank akaun mereka.



[Imej pesanan yang dihantar kepada mangsa yang mengandungi pautan WhatsApp]

Beberapa langkah berjaga-jaga:

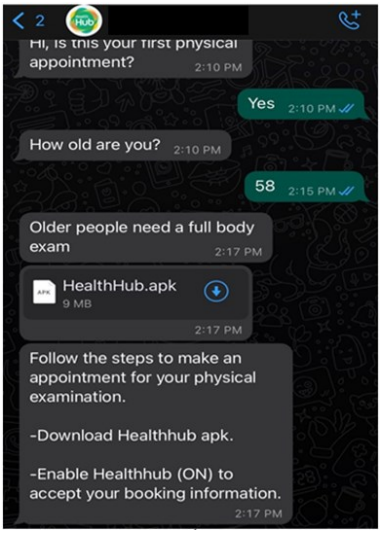
MASUKKAN – Aplikasi ScamShield dan pasangkan ciri-ciri keselamatan (misalnya, dayakan dua-faktor (2FA) untuk bank-bank, media sosial, akaun Singpass; tetapkan had transaksi untuk transaksi perbankan internet, termasuk PayNow /PayLah).

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (misalnya periksa dengan bot ScamShield WhatsApp di https://go.gov.sg/scamshield-bot, atau telefon talian Hotline Antipenipuan di 1800-7222-6688, atau layari https://www.scamalert.sg/)

Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (iaitu Gedung Google Play untuk Android).

SMS Healthier SG yang rasmi akan selalu menunjukkan ID penghantar berdaftar "MOH" dan tidak akan dihantar melalui nombor telefon mudah alih.

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



[Imej perbualan WhatsApp dengan penipu]

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

வெளியீடு எண். 26

15 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 (பல்வேறு வகைகள்)

கடன் மோசடி

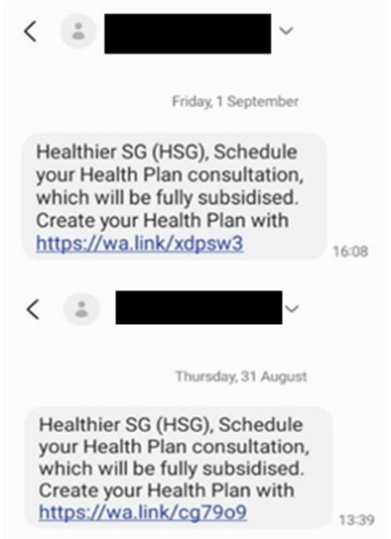
போலி HealthHub செயலியைப் பதிவிறக்கம் செய்ய வழிவகுக்கும் போலி குறுஞ்செய்தி

மோசடி உத்திகள்

மோசடிக்காரர்கள் "Healthier SG" என்ற திட்டத்தின் கீழ் ஒரு போலி குறுஞ்செய்தியை அனுப்புவார்கள். அதில் பாதிக்கப்பட்டவர்கள் இலவச சுகாதாரத் திட்டத்துக்கான ஆலோசனையைப் பெற்றுக்கொள்ள முன்கூட்டியே தேதியைப் பதிந்துகொள்ளுமாறு கேட்டுக்கொள்ளப்படுவார்கள். குறுஞ்செய்தியில் ஒரு வாட்ஸ்ஆப் உரையாடலுக்கான இணைப்பு இருக்கும். இணைப்பை அவர்கள் அழுத்தினால், ஒரு APK கோப்பைப் பதிவிறக்கம் செய்து நிறுவத் தூண்டப்படுவார்கள்.

APK கோப்பில் தீங்கு விளைவிக்கும் மென்பொருள் இருக்கும். இது மோசடிக்காரர்கள் தொலைதூர அணுகலையும் பாதிக்கப்பட்டவர்களின் சாதனங்களின் மீதான கட்டுப்பாட்டையும் பெற அனுமதிக்கிறது. மோசடிக்காரர்கள் சாதனத்தில் உள்ள கடவுச்சொற்களை திருடவும் இந்த தீங்கு விளைவிக்கும் மென்பொருள் அனுமதிக்கிறது.

அங்கீகரிக்கப்படாத பரிவர்த்தனைகள் அவர்களின் வங்கிக் கணக்குகளிலிருந்து செய்யப்படும்போது மட்டுமே பாதிக்கப்பட்டவர்கள் தங்கள் சாதனங்களில் இருக்கும் தீங்கிழைக்கும் செயலியைப் பற்றி அறிந்துகொள்வார்கள்.



[பாதிக்கப்பட்டவர்களுக்கு வாட்ஸ்ஆப் இணைப்பு அடங்கிய குறுஞ்செய்தியின் படம்]

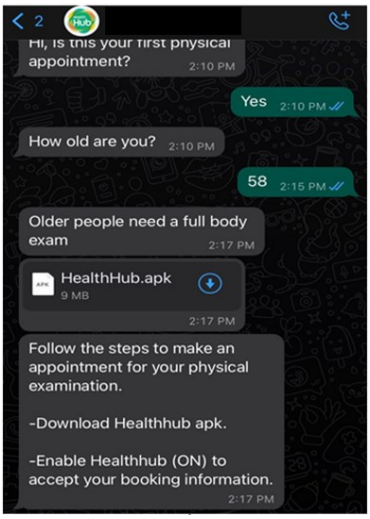
சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்கவும் - ஸ்கேம்ஷீல்டு செயலியைச் சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும் (எ. கா., வங்கிகள், சமூக ஊடகம், Singpass கணக்குகளுக்கு 2FA முறையைச் செயல்படுத்தவும்; PayNow/PayLah உள்ளிட்ட இணைய வங்கிச் சேவை பரிவர்த்தனைகளின் மீது பரிவர்த்தனை வரம்புகளை அமைக்கவும்).

சரிபார்க்கவும் - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (எ. கா. ஸ்கேம்ஷீல்டு வாட்ஸ்ஆப் போட் உடன் https://go.gov.sg/scamshield-bot என்ற இணையத்தளத்திலோ அல்லது https://www.scamalert.sg என்ற இணையத்தளத்திலோ சரிபாருங்கள். 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணையும் நீங்கள் அழைக்கலாம்) அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்து நிறுவுங்கள். (அதாவது, அண்ட்ராய்டுக்கான கூகிள் பிளே ஸ்டோர்)

அதிகாரபூர்வ Healthier SG குறுஞ்செய்திகள் எப்போதும் "MOH" என்ற பதிவு செய்யப்பட்ட அனுப்புநர் அடையாளத்தைக் கொண்டிருப்பதோடு, அவை கைபேசி எண்கள் மூலமாக அனுப்பப்படுவதில்லை.

சொல்லவும் - மோசடிகள் பற்றி அதிகாரிகள், குடும்பத்தினர் மற்றும் நண்பர்களுக்கு தெரியப்படுத்துங்கள். அந்த எண்ணைத் தடுக்க வாட்ஸ்ஆப்பில் புகார் செய்வதோடு, மோசடி பரிவர்த்தனைகள் ஏதேனும் இருந்தால் உடனடியாக உங்கள் வங்கியிடம் தெரிவிக்கவும்.



[மோசடிக்காரருடன் வாட்ஸ்ஆப் உரையாடலின் படம்]

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