TRENDING SCAMS | IN THE PAST WEEK

Issue no. 14
23 June 2023

Scams to look out for

Job Scam

You receive a job offer promising high salary with little effort.

CHECK with official sources, such as the company's official website, to verify the job offer.

Fake Friend Call Scam

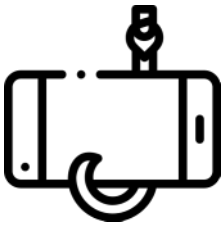
You receive a phone call from supposedly your "friend". You are asked to guess the caller's name and when you do so, the caller will assume this name. You are then asked to save the friend's new number. A few days later, this so-called friend will call you to ask for money to help him or her for an emergency, mother is in hospital etc.

CHECK with your friend through other means or call the original number to verify if indeed your friend had called you earlier.

Investment Scam

You are offered an investment with very high returns.

CHECK with official sources, such as the company's official website, to verify the deal. Do not be enticed by the initial positive gains. Do your own due diligence before you invest large sums of money.



Phishing Scam through Malware

You come across a deal for a product or service online. To facilitate payment, you are asked to click on a link and download an application from an unknown source.

ADD ScamShield app on mobile phone to detect scam messages and block scam calls. Do not click on links sent via any messaging and/or social media platforms by unknown sources. Only download and install applications from official application stores (i.e., Apple Store or Google Play Store).

E-Commerce Scam/ Others*

You come across an attractive item or service (e.g., tour package, concert tickets or electronics) online and contact the seller through messaging app. After making payment, the item or service was not delivered. The seller becomes uncontactable.

CHECK the company's official website, seller's online reviews and ratings. Avoid making advance payments or direct bank transfer to anyone whom you do not know or have not met in person. Do not install any apps that sellers send you via links in messaging platforms. Only download apps from official application stores (Apple Store, Google Play Store).

** This scam is new to the top 5 as compared to the previous week.*

⚠ Emerging Scam Trend

Scams involving malware that infect Android devices to steal funds from CPF and bank accounts

- Victims would come across fake advertisements for products or services (e.g., groceries) on social media platforms. Victims would contact scammers via WhatsApp and scammers would send URLs to victims, asking victims to download applications via the URLs to make payment.
- The applications would contain malware that allow scammers to access victims' devices remotely and steal passwords (e.g., Singpass passcode) stored on their devices. Scammers might also call victims to ask for their Singpass passcodes, by pretending to require the passcodes to create accounts on the applications.
- Victims would be directed to fake online banking login sites to key in their banking credentials and make payment within the applications.
- The malware (with keylogging capabilities) would capture the credentials keyed in by victims for scammers. Scammers would access victims' CPF accounts remotely with the stolen Singpass passcodes and withdraw victims' CPF funds via PayNow. By doing so, the funds will be deposited into victims' bank accounts. Scammers would then access victims' bank accounts and transfer the CPF funds out of the accounts via PayNow.
- The victims would realise the scam and the loss of their CPF funds when they discover unauthorised transactions made on their bank accounts.

[Ads for seafood on Facebook which was a victim's first contact point with the scammer]

Some precautionary measures:

- **ADD** - anti-virus/anti-malware applications to your devices. Update your devices' operating systems and applications regularly to be protected with the latest security patches.
- Disable "Install Unknown App" or "Unknown Sources" in your phone settings. Do not grant permission to persistent pop-ups that request for access to your device's hardware or data.
- **CHECK** - the developer information on the application listing, the number of downloads and user reviews to ensure that it is a reputable and legitimate application.
- Do not download any suspicious APK files as they may contain phishing malware. Only download and install applications from official app stores (i.e., Google Play Store and Apple App Store).
- **TELL** - authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately.

How to protect yourself

I Can ACT Against Scams

Remember to Add, Check and **Tell** (ACT) before making any decisions.

And never respond to urgent requests for information or money.

Always verify such requests with official websites or sources.

Get the latest advice. Visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

Report scams. Call the Police Hotline at 1800-255-0000 or submit information online at www.police.gov.sg/iwitness. All information will be kept strictly confidential.

Download the free ScamShield app

Detect, block and report scams with the ScamShield app.

GET IT ON Google Play | Download on the App Store

A crime prevention initiative by

NATIONAL CRIME PREVENTION COUNCIL

In collaboration with

SINGAPORE POLICE FORCE

SAFEGUARDING EVERY DAY

过去一周

14号刊

2023年6月23日

诈骗趋势

当心骗局

求职诈骗

您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

假朋友来电

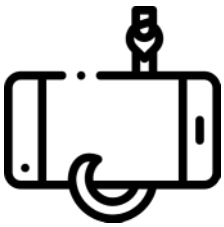
您接到来自"朋友"的电话。来电者在要求您猜他的姓名后会使用您所说的名字。来电者会要求您保存朋友的新电话号码。几天后，这所谓的朋友会拨电给您，以紧急事件或母亲住院等为由要求您提供经济援助。

通过其他沟通管道或原来的电话号码与您的朋友核实是否打电话给您。

投资诈骗

您收到了一项回报率非常高的投资机会。

查看官方消息，如公司的官方网站，以核实这笔交易。不要被初期的利润诱惑。在投入大笔资金前，请务必多加查证。



利用恶意软件的钓鱼诈骗

您在网上看到产品或服务的广告。为方便付款，您被要求点击一个链接并从一个未知来源下载一个应用程序。

在您的手机里下载 ScamShield 应用侦测诈骗短信和拦截诈骗电话。请勿点击由未知来源通过任何通讯和/或社交媒体平台发送的链接。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。

电子商务/其他骗局*

您在网上看到具吸引力的产品或服务（如：旅游配套、演唱会门票、电子产品）并通过通讯应用程序与卖家联系。付款后，您没有收到商品或服务。卖家也失联了。

查看公司的官方网站、卖家在线评论和评级。避免预付款项或通过银行直接转账给不认识或素未谋面的人。切勿安装任何由卖家通过通讯平台发送的链接下载的应用程序。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。

**本周新加入前五名的诈骗手法。*

⚠ 新兴诈骗趋势

涉及恶意软件入侵安卓系统骗取公积金户头和银行账户款项的骗局

- 受害者会在社交媒体平台接触到产品或服务的广告。骗子会在受害者通过WhatsApp联络后发送网站链接给受害者，并要求受害者下载网站链接中的应用程序付款。
- 这些含有恶意软件的应用程序让骗子远程进入受害者的设备盗取储存在设备上的密码（如Singpass）。骗子也可能以需要Singpass密码在应用程序开设账号为由拨电向受害者索取密码。
- 受害者会被转接至假冒的银行登录网站输入银行凭证并在应用程序里付款。
- 具有键盘记录功能的恶意软件会协助骗子得到受害者输入的凭证。骗子会利用盗取的Singpass密码远程进入受害者的公积金户头，并利用PayNow提取受害者的公积金款项。如此一来，款项就会存入受害者的银行账户。骗子过后会进入受害者的银行账户并利用PayNow把钱转出。
- 受害者在发现自己的银行账户有未经授权的交易时意识到自己被骗，公积金存款也已不翼而飞。

[骗子与受害者初次接触所利用的脸书海鲜广告]

一些预防措施：

- **下载** - 防毒/反恶意软件应用程序。务必定期更新设备的操作系统以及应用程序确保设备与应用程序受到最新安全补丁的保护。
- 在手机设置内禁止"安装未知应用程序"或"未知来源"的应用程序。不要授权要求进入设备硬件或数据的持久性弹出式窗口权限。
- **查看** - 应用程序列表中的开发人员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。
- 由于APK文档内或含有钓鱼恶意软件，因此请切勿下载任何可疑的APK文档。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。
- **告知** – 当局、家人和朋友诈骗案件趋势。立即向银行举报任何欺诈性的交易。

⚠如何保护自己

I Can ACT Against Scams

在做任何决定前，**请谨记下载、查看和告知(ACT)。**

千万别回复紧急的信息或金钱要求。

时刻与官方网站或可靠的管道核实此类请求。

上网 www.scamalert.sg 或拨打反诈骗热线 1800-722-6688，获取最新的防范骗案信息。

通报诈骗。拨打警方热线 1800-255-0000 或上网 www.police.gov.sg/iwitness 向警方提供诈骗线索。所有资料都将保密。

下载免费的防诈骗应用ScamShield
使用ScamShield应用以侦测，阻止及通报诈骗。

GET IT ON Google Play　Download on the App Store

防范罪案咨询由

NATIONAL CRIME PREVENTION COUNCIL

以及

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

协力带给您

TREND PENIPUAN | SEPANJANG MINGGU LEPAS

Isu no. 14
23 Jun 2023

Penipuan yang harus diawasi

Penipuan Pekerjaan

Anda menerima satu tawaran pekerjaan yang menjanjikan gaji yang lumayan dengan usaha yang sedikit.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran pekerjaan tersebut.

Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada kononnya seorang "kawan". Anda diminta supaya meneka nama si pemanggil dan apabila anda berbuat demikian, pemanggil akan menggunakan nama yang anda teka tersebut. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, pemanggil yang kononnya kawan anda ini akan menghubungi anda untuk meminta wang bagi menolongnya untuk suatu kecemasan, atau emaknya yang berada di hospital, dan sebagainya.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asalnya untuk memastikan dia benar-benar telah menelefon anda tadi.

Penipuan Pelaburan

Anda ditawarkan satu pelaburan dengan pulangan yang sangat tinggi.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut. Jangan tertarik dengan keuntungan awal yang positif. Lakukan pemeriksaan yang teliti dan wajar sebelum anda melaburkan wang dengan jumlah yang besar.

Penipuan Pancingan Data Melalui Perisian Hasad

Anda ternampak satu tawaran untuk sebuah produk atau khidmat dalam talian. Untuk memudahkan pembayaran, anda diminta supaya mengklik satu pautan dan memuat turun satu aplikasi dari sumber yang tidak diketahui.

MASUKKAN aplikasi ScamShield ke telefon bimbit anda untuk menyekat panggilan penipuan dan menapis SMS penipuan. Jangan klik pada pautan yang dihantar melalui mana-mana platform pesanan dan/atau media sosial oleh sumber yang tidak diketahui. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play).

Penipuan E-Dagang/ Lain-lain*

Anda ternampak satu barang atau khidmat yang menarik (misalnya, pakej pelancongan, tiket konsert atau elektronik) dalam talian dan menghubungi penjual melalui aplikasi pesanan. Setelah membuat pembayaran, barang atau khidmat tersebut tidak dihantar. Penjual tidak dapat dihubungi.

PERIKSA laman web rasmi syarikat tersebut, ulasan dan penilaian dalam talian penjual. Elakkan dari membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada sesiapapun yang tidak anda kenali atau bertemu secara peribadi. Jangan memasang sebarang aplikasi yang dihantar oleh penjual melalui pautan di platform pesanan. Muat turun aplikasi hanya daripada gedung aplikasi rasmi (Gedung Apple, Gedung Google Play).

**Penipuan ini adalah yang baharu untuk 5 teratas berbanding dengan minggu sebelumnya.*

⚠ Trend Penipuan yang Baru Muncul

Penipuan melibatkan perisian hasad yang menjangkiti peranti Android untuk mencuri dana dari akaun-akaun CPF dan bank.

- Mangsa akan ternampak iklan palsu berkenaan produk atau khidmat (misalnya, barang keperluan dapur) di platform media sosial. Mangsa akan menghubungi penipu melalui WhatsApp dan penipu akan meminta mangsa memuat turun aplikasi melalui pautan URL untuk melakukan pembayaran.
- Aplikasi tersebut akan mengandungi perisian hasad yang membenarkan penipu mengakses peranti mangsa dari jauh dan mencuri kata laluan (misalnya, kod pengesahan Singpass) yang tersimpan dalam peranti mereka. Penipu mungkin juga menghubungi mangsa untuk meminta kod pengesahan Singpass, dengan berpura-pura memerlukan kod pengesahan untuk membuka akaun di aplikasi berkenaan.
- Mangsa akan dibawa ke laman log masuk perbankan dalam talian yang palsu untuk memasukkan butiran perbankan mereka dan melakukan pembayaran dalam aplikasi tersebut.
- Perisian hasad (dengan keupayaan "keylogging") akan merakam butiran yang direkodkan melalui ketukan kekunci pada papan peranti oleh mangsa untuk penipu. Penipu akan mengakses akaun CPF mangsa dari jauh dengan kod pengesahan Singpass yang telah dicuri itu dan mengeluarkan dana CPF mangsa melalui PayNow. Dengan berbuat demikian, dana tersebut akan dimasukkan ke dalam akaun bank mangsa. Penipu kemudian akan mengakses akaun bank mangsa dan memindahkan dana CPF keluar dari akaun tersebut melalui PayNow.
- Mangsa akan menyedari penipuan dan kehilangan dana CPF mereka apabila mereka mendapat tahu tentang transaksi tanpa kebenaran yang telah dibuat dalam akaun bank mereka.

[Iklan untuk makanan laut di Facebook di mana ia adalah titik hubungan pertama mangsa dengan penipu]

Beberapa langkah berjaga-jaga:

- **MASUKKAN** – aplikasi anti virus/ anti perisian hasad di peranti anda. Kemas kini sistem operasi dan aplikasi peranti anda dengan kerap agar ia dilindungi dengan patch keselamatan yang terkini.
- Nyahdayakan "Install Unknown App" (Pasang Aplikasi yang Tidak Diketahui) atau "Unknown Sources" (Sumber yang Tidak Diketahui) di dalam tetapan telefon anda. Jangan beri keizinan kepada pop-up berterusan yang meminta akses ke perkakasan atau data peranti anda.
- **PERIKSA** - maklumat pemaju di senarai aplikasi dan bilangan muat turun dan ulasan pengguna untuk memastikan aplikasi tersebut bereputasi dan sah.
- Jangan memuat turun sebarang fail APK yang mencurigakan kerana ia mungkin mengandungi perisian hasad pancingan data. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (iaitu Gedung Google Play dan Gedung Aplikasi Apple).
- **BERITAHU** – pihak berkuasa, keluarga dan kawan tentang penipuan. Laporkan sebarang transaksi menipu kepada bank anda dengan segera.

⚠ Bagaimana melindungi diri anda

Ingatlah untuk Masukkan (Add), Periksa (Check) dan **Beritahu (Tell)** atau ACT sebelum membuat sebarang keputusan.

Dan jangan membalas sebarang permintaan mendesak untuk maklumat atau wang.

Pastikan selalu kesahihan permintaan-permintaan tersebut daripada laman-laman web atau sumber-sumber rasmi.

Dapatkan nasihat terkini. Lawati www.scamalert.sg atau hubungi Talian Bantuan Anti-Penipuan di 1800-722-6688.

Adukan penipuan. Panggil Talian Hotline Polis di 1800-255-0000 atau hantarkan maklumat dalam talian di www.police.gov.sg/iwitness. Semua maklumat akan dirahsiakan sama sekali.

Muat turun aplikasi percuma yang dipanggil ScamShield
Kesan, sekat dan adu penipuan dengan aplikasi ScamShield.

GET IT ON Google Play Download on the App Store

Sebuah inisiatif pencegahan jenayah oleh

NATIONAL CRIME PREVENTION COUNCIL

Dengan kerjasama

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

கடந்த வாரத்தின் | முன்னணி மோசடிகள்

வெளியீடு

எண். 14

23 ஜூன் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

வேலை மோசடி

நீங்கள் சிறிதும் முயற்சி செய்யாமல், அதிக சம்பளம் வழங்குவதாக உறுதியளிக்கும் ஒரு வேலை வாய்ப்பைப் பெறுகிறீர்கள்.

வேலை வாய்ப்பை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் **சரிபார்க்கவும்**.

போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். அவ்வாறு நீங்கள் செய்யும்போது, அழைப்பவர் நீங்கள் குறிப்பிட்ட பெயரை ஏற்றுக்கொள்வார். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, உங்கள் நண்பர் என்று தன்னை அறிமுகப்படுத்திக் கொண்ட இந்த நபர், அவசர நிலைமைக்கு அவருக்கு உதவ பணம் கேட்டு உங்களை அழைப்பார். ஒரு உதாரணத்திற்கு, அவரது தாயார் மருத்துவமனையில் இருக்கிறார் என்று கூறலாம்.

உங்கள் நண்பர் உங்களை சற்றுமுன் அழைத்திருந்தார்களா என்பதை மற்ற வழிகள் மூலமாகவோ அல்லது அவர்களின் அசல் எண்ணிலோ தொடர்புக்கொண்டு **சரிபார்க்கவும்**.

முதலீட்டு மோசடி

மிக உயர்ந்த வருவாய்யைக் கொண்ட ஒரு முதலீடு உங்களுக்கு வழங்கப்படுகிறது.

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் **சரிபார்க்கவும்**. ஆரம்ப ஆதாயங்களைக் கண்டு கவர்ந்துவிடாதீர்கள். நீங்கள் ஒரு பெரியத் தொகையை முதலீடு செய்வதற்கு முன்பு உங்கள் சொந்த சோதனைகளை மேற்கொள்ளுங்கள்.

தீங்கிழைக்கும் மென்பொருள் மூலம் தகவல் திருட்டு மோசடி

இணையத்தில் ஒரு நல்ல பொருளையோ சேவையையோ காண்கிறீர்கள். கட்டணம் செலுத்துவதை எளிதாக்க, நீங்கள் ஓர் இணைப்பை கிளிக் செய்து அறியப்படாத தளத்திலிருந்து ஒரு செயலியைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகள் மற்றும் மோசடி குறுஞ்செய்திகளைத் தடுக்க கைபேசியில் ஸ்கேம்ஷீல்ட் செயலியைச் **சேர்க்கவும்**. செய்தி அனுப்பும் தளங்கள் அல்லது சமூக ஊடகத் தளங்கள் வழியாக தெரியாதவர்களால் அனுப்பப்படும் எந்தவொரு இணைப்புகளையும் கிளிக் செய்ய வேண்டாம். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யவும்.

இணைய வர்த்தக மோசடி / மற்றவை*

நீங்கள் இணையம்வழி ஒரு கவர்ச்சிகரமான பொருள் அல்லது சேவையைப் (எ. கா. சுற்றுப்பயணத் தொகுப்பு, இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள் அல்லது மின்னணுவியல் பொருட்கள்) பார்த்து, செய்தி அனுப்பும் செயலி மூலம் விற்பனையாளரைத் தொடர்புகொள்கிறீர்கள். பணம் செலுத்திய பிறகு, பொருள் அல்லது சேவை வழங்கப்படவில்லை. விற்பனையாளரையும் தொடர்பு கொள்ள முடியவில்லை.

நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம், விற்பனையாளரின் இணைய மதிப்பாய்வுகள் மற்றும் தரநிலைகளை **சரிபார்க்கவும்**. உங்களுக்குத் தெரியாத அல்லது நேரில் சந்திக்காத எவருக்கும் முன்கூட்டியே பணம் செலுத்துவதையோ அல்லது நேரடி வங்கி பரிமாற்றம் செய்வதையோ தவிர்க்கவும். செய்தி அனுப்பும் தளங்களில் உள்ள இணைப்புகள் வழியாக விற்பனையாளர்கள் உங்களுக்கு அனுப்பும் எந்தவொரு செயலிகளையும் நிறுவாதீர்கள். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளை பதிவிறக்கம் செய்யுங்கள்.

*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது.

⚠ வளர்ந்து வரும் மோசடிப் போக்கு

மத்திய சேமநிதி மற்றும் வங்கிக் கணக்குகளிலிருந்து நிதியைத் திருட ஆண்ட்ராய்ட் சாதனங்களைப் பாதிக்கும் தீங்கு விளைவிக்கும் மென்பொருள் சம்பந்தப்பட்ட மோசடிகள்

- பாதிக்கப்பட்டவர்கள் சமூக ஊடகத் தளங்களில் பொருட்கள் அல்லது சேவைகளுக்கான (எ. கா. மளிகைப் பொருட்கள்) போலி விளம்பரங்களைப் பார்ப்பார்கள். பாதிக்கப்பட்டவர்கள் வாட்ஸ்ஆப் மூலம் மோசடிக்காரர்களைத் தொடர்புகொள்வார்கள். மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்கு இணையப்பக்க முகவரிகளை அனுப்புவார்கள். பணம் செலுத்துவதற்கு அவர்கள் இணையப்பக்க முகவரிகள் வழியாக செயலிகளைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுவார்கள்.
- இந்த செயலிகளில் தீங்கு விளைவிக்கும் மென்பொருள் இருக்கும். அவை மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் சாதனங்களை தொலைவிலிருந்து அணுக அனுமதிக்கும். அவர்களின் சாதனங்களில் உள்ள கடவுச்சொற்களை (எ. கா. Singpass கடவு எண்) திருட அனுமதிக்கும். மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களை அழைத்து செயலிகளில் கணக்குகளை உருவாக்க கடவு எண்கள் தேவை என்று பாசாங்கு செய்வதன் மூலம் அவர்களின் Singpass கடவு எண்களைக் கேட்கலாம்.
- பாதிக்கப்பட்டவர்கள் போலி இணைய வங்கி உள்நுழைவு தளங்களில் தங்கள் வங்கித் தகவல்களை வழங்கி, செயலிகளுக்குள் பணம் செலுத்த கேட்டுக்கொள்ளப்படுவார்கள்.
- தீங்கு விளைவிக்கும் மென்பொருள் ஒருவர் என்ன தட்டச்சு செய்கிறார் என்பதைக் கண்டறிந்து, பாதிக்கப்பட்டவர்கள் தட்டச்சு செய்யும் தகவல்களைப் மோசடிக்காரர்களுக்காக பதிவு செய்யும். திருடப்பட்ட Singpass கடவு எண்களுடன் மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் மத்திய சேமநிதி கணக்குகளை தொலைவிலிருந்து அணுகி, அவர்களின் மத்திய சேமநிதி நிதியை PayNow வழியாக எடுப்பார்கள். அவ்வாறு செய்வதன் மூலம், அந்த நிதி பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்குகளில் போடப்படும். மோசடிக்காரர்கள் பின்னர் பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்குகளை அணுகி, மத்திய சேமநிதி நிதியைக் கணக்குகளிலிருந்து PayNow வழியாக மாற்றிவிடுவார்கள்.
- தங்கள் வங்கிக் கணக்குகளில் அனுமதிக்கப்படாத பரிவர்த்தனைகளைக் கண்டுபிடிக்கும்போது மோசடியையும் மத்திய சேமநிதி நிதி இழப்பையும் பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.

[மோசடிக்காரருடன் பாதிக்கப்பட்டவரின் முதல் தொடர்பு .:பேஸ்புக்கில் கடல் உணவுக்கான விளம்பரங்கள் மூலம் ஏற்பட்டது]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

- **சேர்க்க** - உங்கள் சாதனங்களில் வைரஸ் தாக்குதல்களிருந்து பாதுகாக்கும்/ தீங்கு விளைவிக்கும் மென்பொருள்களைக் கண்டறிந்து அவற்றை அகற்றும் செயலிகளை சேர்க்கவும். உங்கள் சாதனங்களின் இயங்குதளங்கள் மற்றும் செயலிகளைச் சமீபத்திய பாதுகாப்பு திட்டுகளுடன் தவறாமல் புதுப்பிக்கவும்.
- உங்கள் சாதனத்தின் அமைவுகளில் உள்ள "Install Unknown App" அல்லது "Unknown Sources" என்பதை முடக்கவும். உங்கள் சாதனத்தின் வன்பொருள் அல்லது தரவை அணுக கோரும் தொடர்ச்சியான பாப் அப்களுக்கு அனுமதி வழங்க வேண்டாம்.
- **சரிபார்க்க** - செயலியின் உருவாக்குநர் தகவல்கள், பதிவிறக்கங்களின் எண்ணிக்கை மற்றும் பயனர் மதிப்பாய்வுகள் ஆகியவற்றை சரிபார்த்து அதன் நம்பகத்தன்மையை உறுதி செய்யவும்.
- சந்தேகத்திற்குரிய APK .:பைல்ஸ் எதையும் பதிவிறக்கம் செய்ய வேண்டாம், ஏனெனில் அவற்றில் தகவல் திருட்டு தீங்கு விளைவிக்கும் மென்பொருள் இருக்கலாம். அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள். (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்).
- **சொல்ல** - மோசடிகள் பற்றி அதிகாரிகள், குடும்பத்தினர் மற்றும் நண்பர்களுக்கு தெரியப்படுத்துங்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.

எப்படி உங்களைப் பாதுகாத்துக்கொள்வது

எந்தவொரு முடிவையும் எடுப்பதற்கு முன்பு **சேர்க்க, சரிபார்க்க** மற்றும் **சொல்ல** (ACT) **நினைவில் கொள்ளுங்கள்.**

தகவல் அல்லது பணத்திற்கான அவசர கோரிக்கைகளுக்கு ஒருபோதும் பதிலளிக்காதீர்கள்.

அத்தகைய கோரிக்கைகளை அதிகாரபூர்வ இணையத்தளம் அல்லது ஆதாரங்களுடன் எப்போதும் சரிபார்த்துக்கொள்ளுங்கள்.

ஆக அண்மைய ஆலோசனையைப் பெறுங்கள். www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.

மோசடிகளை புகார் செய்யுங்கள். 1800-255-0000 என்ற காவல்துறை நேரடித் தொலைபேசி எண்ணை அழையுங்கள் அல்லது www.police.gov.sg/iwitness என்ற இணையதளத்தில் தகவல்களை சமர்ப்பிக்கலாம். அனைத்து தகவல்களும் ரகசியமாக வைத்திருக்கப்படும்.

ஸ்கேம்ஷீல்ட் செயலியை இலவசமாக பதிவிறக்கம் செய்யுங்கள்.
ஸ்கேம்ஷீல்ட் செயலியைப் பயன்படுத்தி மோசடிகளைக் கண்டறிந்து, தடுத்து, அவற்றைப் பற்றி புகார் செய்யுங்கள்.

GET IT ON Google Play | Download on the App Store

ஒரு குற்றத் தடுப்பு முன்முயற்சி

NATIONAL CRIME PREVENTION COUNCIL

இணைந்து வழங்குபவர்கள்

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY