TRENDING SCAMS | IN THE PAST WEEK

Issue
no. 19
28 Jul 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.

See the next page for more details on this scam type.

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.

E-Commerce Scam (Concert Tickets)

You see third-party resellers on online platforms offering the sale of concert tickets. Sellers would claim that the ticket sales are time-sensitive or have limited availability, to convince buyers into making advanced payment for the tickets.

Purchase only from authorised sellers or reputable sources and avoid making advance payments or direct bank transfers to sellers. **CHECK** the platform's Transaction Safety Rating (TSR) at https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings to know what critical anti-scam safety features it has to protect online transactions.

Phishing Scam (Fake Buyers)

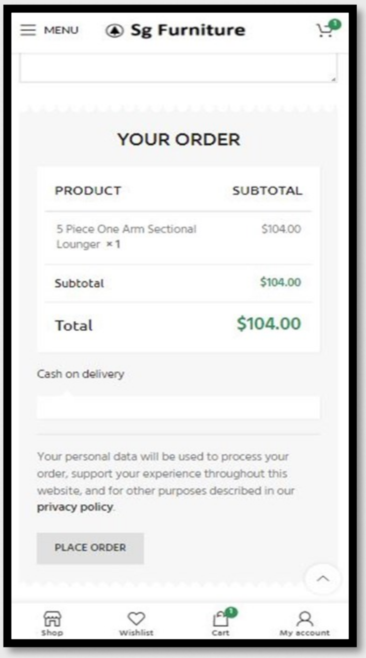
You sell items online. Buyers would claim to be interested in buying your items. To receive payment from an interested buyer, you are asked to click on a URL link or scan a QR code to receive payment.

CHECK - Do not click on dubious URL links and always verify the authenticity of URL links.

Your Friend or A Scammer?

Scam Tactics

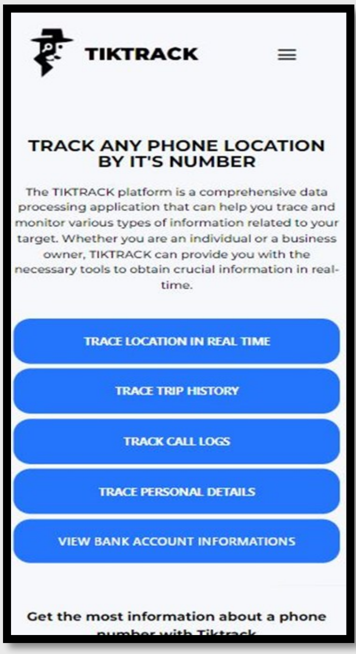
- Victims would receive phone calls from unknown numbers (with or without "+65" prefix). The scammers would claim to be a friend and would ask the victims to guess his/her identity. When victims provide the name of a friend that they believed the caller could be, the scammers would immediately assume that identity of the said friend and would then within the same conversation ask the victims to update their contact details.
- Subsequently, the scammers would contact the victims to ask for a loan as he/she is unable to perform a banking transaction or is experiencing financial difficulties. Victims would only discover they had been scammed after contacting their actual friends, or when their loans were not returned as promised.
- A new variant has also been seen where scammers would send the victims malicious links and ask victims to help them with simple tasks such as making a small value purchase, restaurant reservation or to track a missing phone. These malicious links will lead victims to phishing sites and/or download APK file, an app created for Android's operating system.
- After keying their banking credentials or card details to make payments, victims will discover unauthorised transactions from their bank accounts or incur charges to their credit cards.
- Downloading and installing the app containing malware will allow scammers to access victims' devices remotely and steal passwords stored in the devices. Scammers can then access the victim's banking accounts and transfer all their monies out of their accounts.



[Screenshot whereby victim was asked to install an app to help purchase sofa]

Some precautionary measures:

- **ADD** - ScamShield app and set security features (e.g., two-form factor authentication for banks and accounts; set banking transaction limits). Do update your device with the latest patches and install an anti-virus/anti-malware app. 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** - for scam signs with official sources (e.g., visit www.scamalert.sg or call the Anti-Scam Helpline on 1800-722-6688). Verify whether the request is legitimate by checking with your family and friends through alternative means. Check the developer information, the number of downloads and user reviews to ensure it is a reputable and legitimate application. Only download and install apps from official app stores (i.e., Google Play Store for Android).
- **TELL** - authorities, family, and friends about scams. Beware of unusual requests from someone claiming you know via phone/WhatsApp calls. Report the number to WhatsApp to initiate in-app blocking and report any fraudulent transactions to your bank immediately.



[Screenshot whereby victim was asked to install an app to track the scam-mer's missing phone]

How to protect yourself

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

19 号刊

2023年7月28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。

请参阅下一页以便了解更多这类诈骗的详情。

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。

电子商务骗局（演唱会门票）

您看到第三方转售商在网络平台上销售演唱会门票。卖家会声称售票有时间限制或数量有限以说服买家预付款项。

只向授权卖方或信誉良好的来源购买并避免预付款项或通过银行直接转账给卖方。浏览https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings查看平台的交易安全评级（TSR）以便了解该平台有哪些保护网上交易的重要反诈骗安全措施。

钓鱼骗局（假买家)

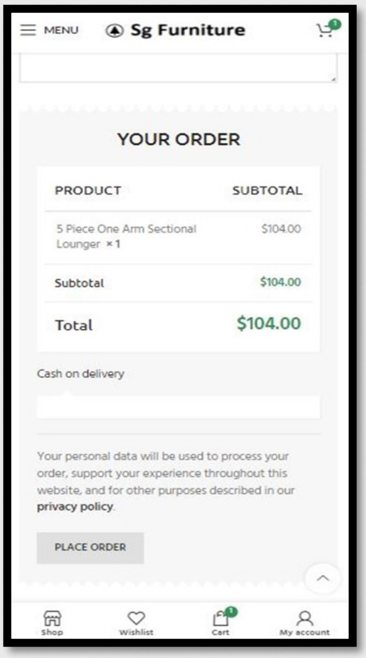
您在网上销售物品。买家会声称有兴趣购买您的物品。您被要求点击网站链接或扫描二维码以接收感兴趣买家的付款。

查看 – 切勿点击可疑链接并务必确认链接的真实性。

真或假朋友？

诈骗手法

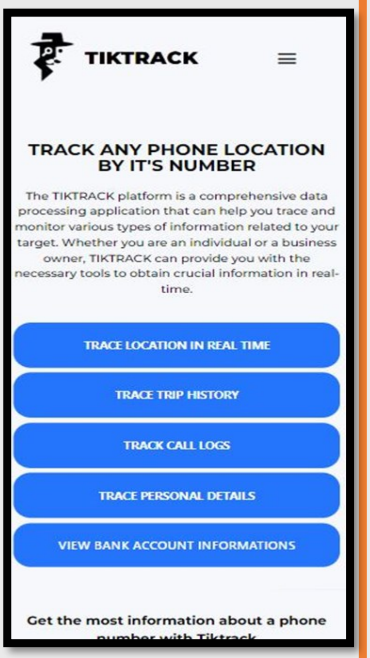
- 受害者会接到来自未知号码的电话（或许没有以"+65"开头的号码）。骗子会称自己是受害者的朋友，并要求受害者猜他/她的身份。当受害者提供一个他们相信是来电者的朋友名字时，骗子会立即使用这个朋友的身份，然后在同一通电话中要求受害者更新他们的联系方式。
- 之后，骗子会联系受害者称银行转账出现问题或有财务困难并要求向受害者借款。受害者只在联系他们真正的朋友后，或当借出的款项没按照承诺归还时，才意识到自己被骗了。
- 在新手法中，骗子也向受害者发送恶意链接，要求受害者帮忙完成一些简单的任务，如小额购物，预订餐馆或追踪丢失的手机。这些恶意链接会引导受害者进入钓鱼网站和/或下载为安卓系统创建的应用程序APK文档。
- 在输入银行凭证或信用卡详情进行付款后，受害者会发现他们的银行账户中有未经授权的交易，或信用卡被收取费用。
- 下载并安装含有恶意软件的应用程序能让骗子远程进入受害者的设备盗取储存在设备上的密码。骗子便能进入受害者的银行户头，并将账户里的钱全数转移出去。



[受害者被要求安装一个应用程序来帮助购买沙发的截图]

一些预防措施：

- **下载** - ScamShield应用程序并设置安全功能（如在银行和账户启用双重认证；设置银行交易限额）。务必定期更新设备并使用最新安全补丁程序，且安装最新的防毒/反恶意软件应用程序。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** - 官方消息并注意诈骗迹象（如：游览www.scamalert.sg 或拨打反诈骗热线1800-722-6688）。务必通过其他方式向家人和朋友确认该要求是否属实。请检查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。只从官方应用程序商店（即安卓使用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。提防通过电话/ WhatsApp来电称认识您，并提出不寻常的要求的人。向WhatsApp举报该号码以启动应用程序内的屏蔽功能和立即向银行举报任何欺诈性的交易。



[受害者被要求安装一个应用程序来追踪骗子丢失的手机的截图]

⚠ 如何保护自己

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 | Isu no. 19

28 Jul 2023

SEPANJANG MINGGU LEPAS

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.

Lihat halaman seterusnya untuk butir-butir lanjut bagi jenis penipuan sebegini.

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 E-Dagang (Tiket Konsert)

Anda ternampak penjual pihak ketiga di platform dalam talian yang menawarkan penjualan tiket konsert. Penjual akan mendakwa bahawa jualan tiket adalah sensitif masa atau mempunyai ketersediaan terhad, untuk meyakinkan pembeli membuat pembayaran awal untuk tiket.

Beli hanya daripada penjual yang sah atau sumber-sumber yang bereputasi, dan elakkan daripada membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada penjual. **PERIKSA** Rating Keselamatan Urus Niaga (TSR) untuk rating platform itu dan untuk mengetahui ciri keselamatan antipenipuan kritikal yang ada padanya untuk melindungi transaksi dalam talian.

Penipuan Pancingan Data (Pembeli Palsu)

Anda menjual barang dalam talian. Pembeli akan mengaku berminat untuk membeli barang anda. Untuk menerima bayaran daripada seorang pembeli yang berminat, anda diminta supaya mengklik satu pautan URL atau mengimbas satu kod QR untuk menerima bayaran.

PERIKSA - Jangan klik pautan URL yang meragukan dan sentiasa pastikan ketulenan pautan URL tersebut.

Kawan Anda atau Seorang Penipu?

Taktik Penipuan

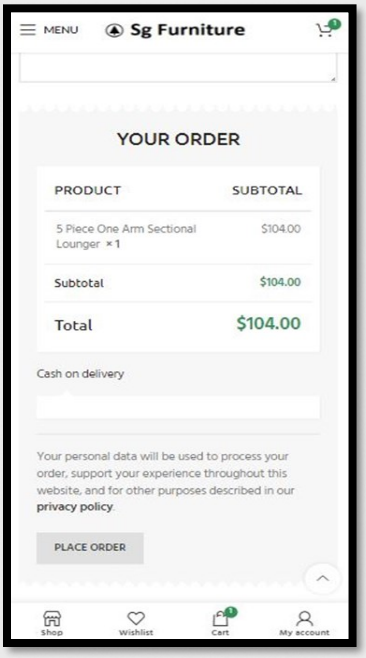
- Mangsa akan menerima panggilan telefon daripada nombor-nombor yang tidak dikenali (dengan atau tidak dengan awalan "+65"). Penipu akan mengaku sebagai kawan dan akan menyuruh mangsa meneka siapa mereka. Apabila mangsa memberikan nama seorang kawan yang mereka percaya ialah si pemanggil itu, penipu dengan segera akan menggunakan identiti kawan tersebut dan kemudian, dalam perbualan yang sama, meminta mangsa supaya mengemas kini butir-butir hubungan mereka.

- Seterusnya, penipu akan menghubungi mangsa untuk meminta pinjaman kerana dia tidak dapat melakukan transaksi perbankan atau sedang menghadapi kesulitan kewangan. Mangsa hanya mengetahui mereka telah ditipu setelah dihubungi oleh kawan sebenar mereka, atau setelah pinjaman mereka tidak dikembalikan seperti yang dijanjikan.

- Satu varian baru juga telah muncul di mana penipu akan menghantar pautan berniat jahat kepada mangsa dan meminta mangsa supaya membantu mereka dengan tugas-tugas mudah seperti membuat pembelian bernilai kecil, tempahan restoran atau menjejaki sebuah telefon yang hilang. Pautan-pautan berniat jahat ini akan mengarahkan mangsa ke laman-laman web pancingan data dan/atau memuat turun fail APK, sebuah aplikasi yang dicipta untuk sistem operasi Android.

- Setelah memasukkan butiran perbankan atau butir-butir kad mereka untuk membuat bayaran, mangsa akan mendapati adanya transaksi tanpa kebenaran daripada akaun bank mereka atau kad kredit mereka dikenakan caj.

- Memuat turun dan memasang aplikasi yang mengandungi perisian hasad akan membenarkan penipu mendapat akses ke dalam peranti mangsa dari jauh dan mencuri kata laluan yang tersimpan di dalam peranti tersebut. Penipu kemudian akan mendapat akses ke dalam akaun perbankan mangsa dan memindahkan kesemua wang mangsa keluar dari akaun mereka.



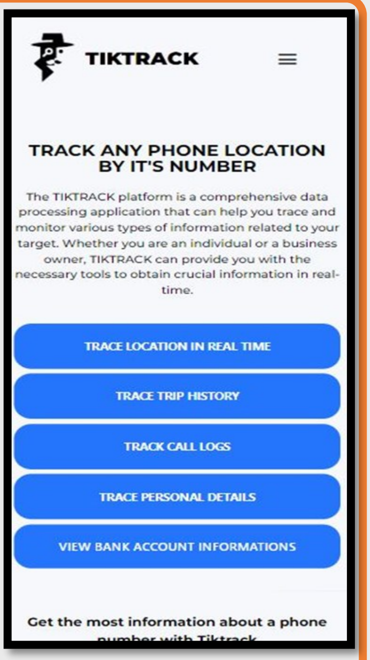
[Tangkap layar di mana mangsa diminta supaya memasang sebuah aplikasi untuk menolong membeli sofa]

Beberapa langkah berjaga-jaga:

- **MASUKKAN** - aplikasi ScamShield dan tetapkan ciri-ciri keselamatan (misalnya, pengesahan dua-jenis faktor untuk bank dan akaun; tetapkan had transaksi perbankan). Kemas kini peranti anda dengan patch keselamatan terkini dan pasang sebuah aplikasi antivirus/antiperisian hasad. 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** – tanda-tanda penipuan dengan sumber-sumber rasmi (misalnya, lawati www.scamalert.sg atau telefon Talian Bantuan Antipenipuan di 1800-722-6688). Pastikan permintaan tersebut adalah sah dengan membuat pemeriksaan dengan keluarga dan kawan anda melalui cara alternatif lain. Periksa maklumat pemaju aplikasi tersebut, bilangan muat turun dan ulasan pengguna untuk memastikan aplikasinya mempunyai reputasi yang baik dan sah. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (Gedung Google Play untuk Android).

- **BERITAHU** - Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Berhati-hati dengan permintaan yang luar biasa daripada seseorang yang mendakwa anda mengenalinya melalui panggilan telefon/WhatsApp. Laporkan nombor tersebut kepada WhatsApp untuk memulakan penyekatan dalam aplikasi, dan laporkan sebarang transaksi menipu kepada bank anda dengan segera.



[Tangkap layar di mana mangsa telah diminta supaya memasang sebuah aplikasi untuk mengesan telefon penipu yang hilang]

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 Antipenipuan 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. 19

28 ஜூலை 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.

இந்த மோசடி வகை பற்றிய மேல் விவரங்களுக்கு, அடுத்த பக்கத்தைப் பார்க்கவும்.

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.

இணைய வர்த்தக மோசடி (இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள்)

இணையத் தளங்களில் மூன்றாம் தரப்பு மறுவிற்பனையாளர்கள் இசை நிகழ்ச்சிக்கான நுழைவுச் சீட்டு விற்பனையை வழங்குவதை நீங்கள் காண்கிறீர்கள். நுழைவுச்சீட்டு விற்பனை குறைந்த அளவில், ஒரு குறிப்பிட்ட காலத்திற்கு மட்டும் கிடைக்கக்கூடியவை என்று விற்பனையாளர்கள் கூறி, வாங்குபவர்களை நுழைவுச்சீட்டுகளுக்கு முன்கூட்டியே பணம் செலுத்த சம்மதிக்க வைப்பார்கள்.

அங்கீகரிக்கப்பட்ட விற்பனையாளர்கள் அல்லது நம்பகமான இடங்களிலிருந்து மட்டுமே வாங்குங்கள். மேலும், விற்பனையாளர்களுக்கு முன்கூட்டியே பணம் செலுத்துதல் அல்லது நேரடி வங்கி மாற்றல்களைச் செய்வதைத் தவிர்க்கவும். இணையப் பரிவர்த்தனைகளைப் பாதுகாக்க என்ன மோசடி எதிர்ப்பு பாதுகாப்பு அம்சங்கள் உள்ளன என்பதை அறிய, https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings என்ற இணையத்தளத்தில் பரிவர்த்தனை பாதுகாப்பு மதிப்பீடுகளை (TSR) **சரிபார்க்கவும்**.

தகவல் திருட்டு மோசடி (வாங்குபவர் போல் நடித்தல்)

நீங்கள் இணையத்தில் பொருட்களை விற்கிறீர்கள். வாங்குபவர்கள் உங்கள் பொருட்களை வாங்குவதில் ஆர்வம் காட்டுவதாகக் கூறுவார்கள். ஆர்வமுள்ள வாங்குபவரிடமிருந்து பணம் பெற, நீங்கள் ஒரு இணையப்பக்க முகவரி (URL) இணைப்பை கிளிக் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள் அல்லது கட்டணம் பெற விரைவுத் தகவல் (QR) குறியீட்டை ஸ்கேன் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள்.

சரிபார்க்கவும் - சந்தேகத்திற்குரிய இணையப்பக்க முகவரி (URL) இணைப்புகளை கிளிக் செய்ய வேண்டாம் மற்றும் எப்போதும் இணையப்பக்க முகவரி (URL) இணைப்புகளின் நம்பகத்தன்மையை சரிபார்க்கவும்.

உங்கள் நண்பரா அல்லது மோசடிக்காரரா?

மோசடி உத்திகள்

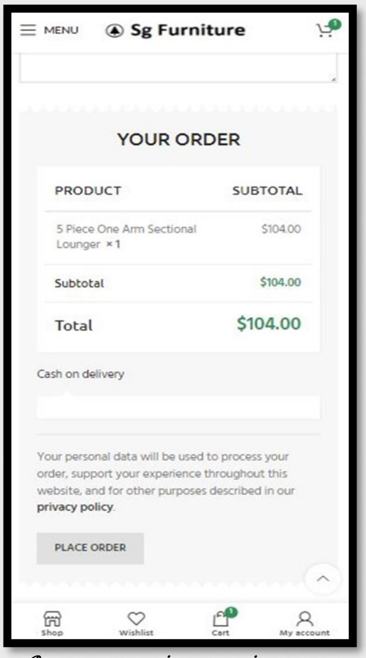
- பாதிக்கப்பட்டவர்கள் அறியப்படாத எண்களிலிருந்து தொலைபேசி அழைப்புகளைப் பெறுவார்கள் (“+65” முன்னிணைப்புடன் அல்லது இல்லாமல்). மோசடிக்காரர்கள் தன்னை ஒரு நண்பர் என்று கூறிக்கொண்டு, பாதிக்கப்பட்டவர்களை தங்களின் அடையாளத்தை யூகிக்கும்படி கேட்பார்கள். பாதிக்கப்பட்டவர்கள் அழைப்பவர் இருக்கலாம் என்று நம்பும் ஒரு நண்பரின் பெயரை வழங்கிய பிறகு, மோசடிக்காரர்கள் உடனடியாக அந்த நண்பரின் அடையாளத்தை எடுத்துக்கொள்வார்கள். பின்னர் அதே உரையாடலில் அவர்கள் பாதிக்கப்பட்டவர்களைத் தொடர்பு விவரங்களைப் புதுப்பிக்கச் சொல்வார்கள்.

- அதைத் தொடர்ந்து, மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களைத் தொடர்புகொண்டு, அவர்கள் வங்கிப் பரிவர்த்தனையைச் செய்ய இயலாததாலோ அல்லது நிதிச் சிக்கல்களை அனுபவிப்பதாலோ கடன் கேட்பார்கள். தமது உண்மையான நண்பர்களைத் தொடர்புகொண்ட பின்னர் அல்லது அவர்களது கடன்கள் வாக்குறுதியளிக்கப்பட்டவாறு திருப்பித் தரப்படாத சந்தர்ப்பங்களில் மட்டுமே தாம் மோசடி செய்யப்பட்டிருந்ததை பாதிக்கப்பட்டவர்கள் கண்டுபிடிப்பார்கள்.

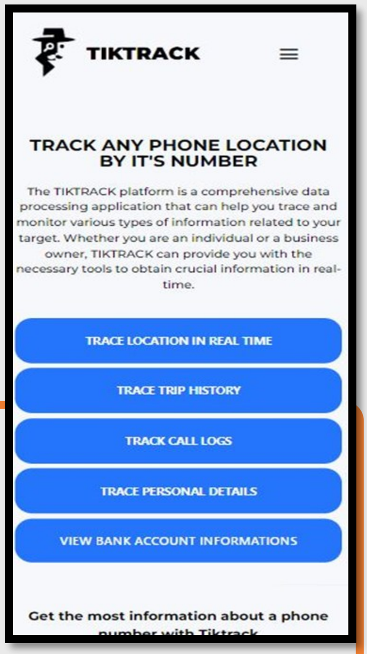
- மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களுக்கு தீங்கிழைக்கும் இணைப்புகளை அனுப்பி, சிறிய மதிப்புள்ள ஒரு பொருளை வாங்குவது, உணவகத்தில் முன்பதிவு செய்ய உதவுவது அல்லது காணாமல் போன தொலைபேசியைக் கண்காணிப்பது போன்ற எளிய பணிகளுக்கு உதவுமாறு பாதிக்கப்பட்டவர்களிடம் கேட்பது ஒரு புதிய வகையாகும். இந்த தீங்கு விளைவிக்கும் இணைப்புகள் பாதிக்கப்பட்டவர்களை தகவல் திருட்டு தளங்களுக்கு இட்டுச் செல்லும் மற்றும் / அல்லது ஆண்ட்ராய்டு இயங்குதளத்துக்காக உருவாக்கப்பட்ட ஒரு செயலியான APK ஃபைல்லை பதிவிறக்கம் செய்யும்.

- பணம் செலுத்துவதற்காக அவர்களின் வங்கிச் சான்றுகள் அல்லது அட்டை விவரங்களை உள்ளிட்ட பிறகு, பாதிக்கப்பட்டவர்கள் தங்கள் வங்கிக் கணக்குகளில் அங்கீகரிக்கப்படாத பரிவர்த்தனைகள் அல்லது அவர்களின் கடன்பற்று அட்டைக்கு கட்டணம் விதிக்கப்பட்டிருப்பதைக் கண்டுபிடிப்பார்கள்.

- தீங்கு விளைவிக்கும் மென்பொருள் கொண்ட செயலியைப் பதிவிறக்கம் செய்து நிறுவுவதன் மூலம் மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் சாதனங்களைத் தொலைவிலிருந்து அணுக முடியும். சாதனங்களில் சேமித்து வைக்கப்பட்டுள்ள கடவுச்சொற்களை அவர்களால் திருட முடியும். மோசடிக்காரர்கள் பின்னர் பாதிக்கப்பட்டவரின் வங்கிக் கணக்குகளை அணுகி அவர்களின் கணக்குகளிலிருந்து பணத்தை எடுக்கலாம்.



[சோபாவை வாங்க உதவும் செயலியை நிறுவுமாறு பாதிக்கப்பட்டவர் கேட்டுக்கொள்ளப்பட்ட ஸ்கிரீன்ஷாட்]



[மோசடிக்காரரின் தொலைபேசியைக் கண்காணிக்க செயலியை நிறுவுமாறு பாதிக்கப்பட்டவர் கேட்டுக்கொள்ளப்பட்டதன் ஸ்கிரீன்ஷாட்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

- **சேர்க்க** - ஸ்கேம்ஷீல்ட் செயலியை சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும் (எ. கா., வங்கிகளுக்கான two-factor (2FA) அல்லது multifactor authentication மற்றும் இணைய வங்கிச் சேவை பரிவர்த்தனைகளில் பரிவர்த்தனை வரம்புகளை அமைக்கவும்). உங்கள் சாதனத்தை சமீபத்திய திட்டுக்களுடன் புதுப்பித்து வைரஸ் தாக்குதல்களிருந்து பாதுகாக்கும்/ தீங்கு விளைவிக்கும் மென்பொருள்களைக் கண்டறிந்து அவற்றை அகற்றும் செயலியை நிறுவவும். 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** - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (எ.கா. www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.) கோரிக்கை உண்மையானதா என்பதை சரிபார்க்க மாற்று வழிகள் மூலம் உங்கள் குடும்பத்தினரையும் நண்பர்களையும் கேளுங்கள். 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).
- **சொல்ல** - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். தொலைபேசி / வாட்ஸ்ஆப் அழைப்புகள் மூலம் உங்களுக்குத் தெரியும் என்று கூறும் ஒருவரிடமிருந்து வரும் வழக்கத்துக்கு மாறான வேண்டுகோள்களைக் குறித்து எச்சரிக்கையாக இருங்கள். அந்த எண்ணைத் தடுக்க வாட்ஸ்ஆப்பில் அந்த எண்ணைப் பற்றி புகாரளிக்கவும். அதோடு, மோசடி பரிவர்த்தனைகள் ஏதேனும் இருந்தால் உடனடியாக உங்கள் வங்கிக்கு புகாரளிக்கவும்.

⚠ 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