TRENDING SCAMS | IN THE PAST WEEK

Issue no. 20
4 Aug 2023

Scams to look out for

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 takes on the name you guessed. 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 with an emergency, such as a family member hospitalized.

CHECK with your real friend through other means or by calling their original number to verify if they had indeed called you earlier.

Job Scam

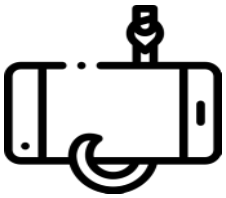
You receive a job offer promising high salary with little effort.

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

Investment Scam

You are offered an investment with very high returns.

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



Phishing Scam (Calls Impersonating Govt Agencies)*

You receive a call from a "government official". You are then asked to provide your banking credentials, OTPs and/ or personal details.

ADD ScamShield app only from the official app stores on your mobile phone. ScamShield blocks scam calls and detects scam SMSes from known blacklisted numbers. Do not provide your credentials and OTPs to unknown persons.

E-Commerce Scam (Others)

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

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.

Please refer to a list of monikers behind such scams at https://go.gov.sg/pnr-ecommerce-scams-involving-electronics-and-concert-tickets.

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

Investment of No Return

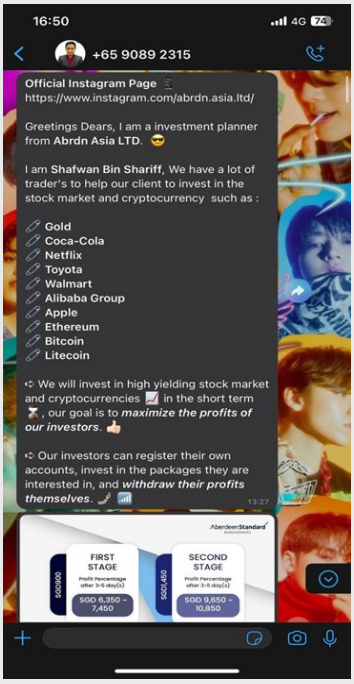
Scam Tactics

- Scammers would approach victims through various channels such as social media platforms and messaging apps to introduce "investment opportunities".
- In one variant, scammers would try to build rapport with victims over time to gain their trust before introducing "investment opportunities" to them. After winning over the trust of the victims, scammers would ask them to conduct transactions under the pretext of "investments".
- Victims would generally receive small profits initially enticing them to believe that their "investments" were real and profitable. However, when they invest larger amounts, they would not be able to withdraw their 'profits' and only then do they realise that they have been scammed.
- In another variant, victims would come across investment ads on social media platforms. After clicking on the ad links, victims would be led to communication apps to contact the scammers.
- Scammers would then lure victims to "invest in opportunities" with high returns in a short time, supported by fraudulent testimonials. Sometimes, victims would be redirected to "investment" websites to provide their personal particulars and card details to register for an account.
- Victims would only realise that they have been scammed when they are not able to withdraw their 'profits' or contact the scammers.
- In some cases, victims would receive calls or messages from scammers to download remote access software (e.g., AnyDesk) onto their devices to receive more information on the "investment" processes. With the remote access, scammers could be able to withdraw all the money from the victims' bank accounts.

[Example of advertisement on Facebook]

Some precautionary measures:

- **ADD -** ScamShield app and set security features (e.g., two-form factor authentication for banks and accounts; set banking transaction limits). Never install software from unverified sources as it will allow scammers to observe your actions or take control of your devices remotely.
- **CHECK** - for scam signs with official sources. Verify the authenticity by:
  - ⇒ asking as many questions as needed to understand the investment fully. Be wary if the company is unable to answer or avoids your questions.
  - ⇒ Checking on the company's information, e.g., owners, directors and management information to assess if the investments are real.
  - ⇒ Confirming the company's and representatives' credentials on the Financial Institutions Directory, Register of Representatives, or check MAS' Investor Alert List.
- **TELL** - authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately.



[Conversation between scammer and victim]

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

20 号刊

2023年8月4日

诈骗趋势

当心骗局

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。

求职诈骗

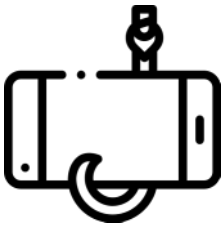
您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

投资诈骗

您收到了一项回报率非常高的投资机会。

请参阅下一页以便了解更多这类诈骗的详情。



钓鱼骗局（冒充政府部门来电）*

您会接到来自"政府官员" 的电话。您被要求提供您的银行凭证、一次性密码和/或个人资料。

只从官方应用程序商店**下载**ScamShield 应用程序，拦截诈骗电话和过滤诈骗短信。切勿向身份不明人士提供您的凭证以及一次性密码。

电子商务骗局（其他）

您在网上看到具吸引力的优惠（如：演唱会门票、电子器材等）并通过一个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。

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。

请参考https://go.gov.sg/pnr-ecommerce-scams-involving-electronics-and-concert-tickets 查看进行这类骗局的绰号名单。

*本周新加入前五名的诈骗手法。

⚠ 零投资回报率

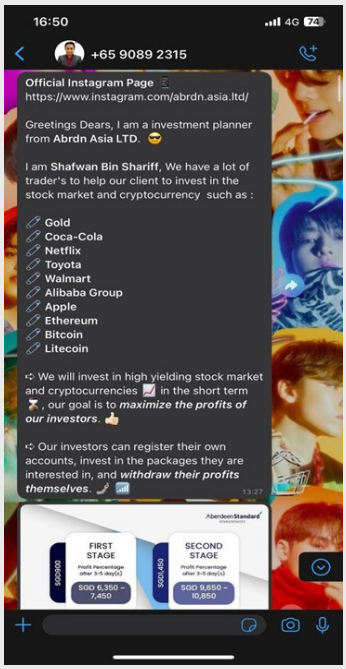
诈骗手法

- 骗子会通过社交媒体平台和即时通讯应用程序等各种渠道向受害者介绍"投资机会"。
- 在骗子使用的其中一种手法中，骗子会先与受害者建立起长期的友谊并在取得他们的信任后介绍他们"投资机会"。骗子在赢取受害者的信任后会以"投资"为借口要求受害者进行交易。
- 受害者一般会在初期得到一些利润，诱使他们相信自己的"投资"是真实的。然而，在投入更多资金但无法提取"利润"时，他们就发现自己被骗了。
- 另一类手法中，受害者会在社交媒体平台上看到投资广告。点击广告链接后，受害者会被引导到通讯应用程序联系骗子。
- 骗子会利用虚假的证词诱骗受害者投资能在短时间取得高回报的"投资机会"。受害者有时会被重新引导到"投资"网站提供他们的个人以及银行卡资料注册账户。
- 受害者是在无法提取"利润"或联络不上骗子的情况下才会意识到自己被骗了。
- 在一些案例中，受害者会接到骗子的电话或信息要求他们下载远程访问软件（如AnyDesk）到设备上，以获取更多有关"投资"过程的信息。能够进行远程访问后，骗子就能提取受害者银行户头里的所有款项。

[脸书广告例子]

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）。切勿从未经认证来源安装软件。这让骗子能远程观察您的一举一动或控制您的设备。
- **查看** – 官方消息并注意诈骗迹象。透过方以下方式确认对方的正当性：
  - ⇒ 为充分了解投资而提出任何必要的问题。如果公司无法回答或回避您的问题，请提高警惕。
  - ⇒ 查看公司的资料，例如业主、董事及管理资料，以评估投资是否属实。
  - ⇒ 在金融机构工商名录、代表名册上确认公司和代表的资格，或查看新加坡金融管理局投资者须警惕名单。
- **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。



[骗子与受害者的聊天记录]

⚠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. 20
4 Ogos 2023

Penipuan yang harus diawasi

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 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 Pelaburan

Anda ditawarkan satu pelaburan dengan pulangan yang sangat tinggi.

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

Penipuan Pancingan Data (Panggilan Menyamar Sebagai Agensi Pemerintah) *

Anda menerima satu panggilan daripada seorang "pegawai pemerintah". Anda diminta supaya memberikan butiran perbankan, OTP dan/atau butir-butir peribadi anda.

MASUKKAN aplikasi ScamShield hanya daripada gedung aplikasi rasmi ke telefon bimbit anda untuk menyekat panggilan penipuan dan mengesan SMS penipuan daripada nombor-nombor yang diketahui telah disenaraihitamkan. Jangan berikan butiran dan OTP anda kepada orang-orang yang tidak dikenali.

Penipuan E-Dagang (Lain-lain)

Anda ternampak satu tawaran menarik (misalnya, tiket konsert, barangan elektronik, dan sebagainya) dalam talian dan anda menghubungi penjual melalui satu aplikasi pesanan. Setelah membuat pembayaran, barang atau khidmat tersebut tidak dihantar, dan penjual tidak dapat dihubungi.

Beli hanya daripada penjual yang sah atau sumber-sumber yang mempunyai reputasi yang baik dan elakkan daripada membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada penjual. **PERIKSA** Rating Keselamatan Urus Niaga (TSR) di https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings untuk mengetahui ciri keselamatan antipenipuan kritikal yang ada padanya untuk melindungi transaksi dalam talian.

Sila rujuk kepada satu senarai nama samaran di sebalik penipuan sedemikian di https://go.gov.sg/pnr-ecommerce-scams-involving-electronics-and-concert-tickets.

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

Pelaburan Tak Kembali

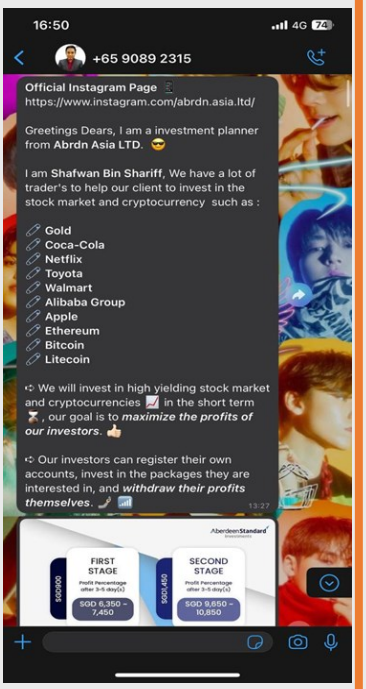
Taktik Penipuan

- Penipu akan mendekati mangsa melalui pelbagai saluran seperti platform media sosial dan aplikasi pesanan untuk mengenalkan “peluang pelaburan”.
- Dalam salah satu pendekatan tersebut, penipu akan berusaha untuk membina perhubungan baik dengan mangsa sedikit demi sedikit bagi mendapatkan kepercayaan mereka sebelum mengenalkan “peluang pelaburan” kepada mereka. Setelah berjaya mendapatkan kepercayaan mangsa, penipu akan meminta mereka supaya melakukan transaksi dengan alasan “pelaburan”.
- Mangsa secara umumnya akan menerima keuntungan kecil pada mulanya, memikat mereka untuk mempercayai bahawa “pelaburan” mereka ini benar. Walau bagaimanapun, apabila mereka melabur dengan jumlah yang lebih besar, mereka tidak akan dapat mengeluarkan ‘keuntungan’ mereka dan barulah ketika itu mereka sedar yang mereka telah ditipu.
- Dalam satu pendekatan lain, mangsa akan ternampak iklan pelaburan di platform media sosial. Setelah mengklik di pautan iklan, mangsa akan dibawa ke aplikasi perhubungan untuk menghubungi penipu.
- Penipu kemudian akan mengumpan mangsa supaya “melabur dalam peluang” dengan pulangan yang tinggi dalam masa yang singkat, dengan disokong oleh testimoni palsu. Kadangkala, mangsa akan diarahkan semula ke laman-laman web “pelaburan” untuk memberikan butir-butir peribadi dan kad mereka untuk mendaftar sebuah akaun.
- Mangsa hanya akan menyedari mereka telah ditipu setelah mereka tidak boleh mengeluarkan ‘keuntungan’ mereka atau menghubungi penipu tersebut.
- Dalam beberapa kes, mangsa akan menerima panggilan atau pesanan daripada penipu untuk memuat turun perisian akses jauh (misalnya, AnyDesk) ke peranti mereka untuk menerima maklumat lanjut mengenai proses “pelaburan” tersebut. Dengan akses jauh ini, penipu akan dapat mengeluarkan kesemua wang daripada akaun bank mangsa.

[Contoh iklan di Facebook]

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). Jangan sekali-kali memasang perisian daripada sumber-sumber yang tidak disahkan kerana ini akan membenarkan penipu memerhatikan perbuatan anda atau menguasai peranti anda dari jauh.
- **PERIKSA** – tanda-tanda penipuan dengan sumber-sumber rasmi. Sahkan ketulenan pelaburan tersebut dengan:
  - Bertanya sebanyak mungkin soalan yang diperlukan untuk memahami sepenuhnya pelaburan tersebut. Berhati-hati dengan syarikat yang tidak dapat menjawab atau mengelak soalan anda.
  - Memeriksa maklumat syarikat, misalnya, maklumat pemilik, pengarah dan pengurusannya untuk menilai jika pelaburannya adalah benar.
  - Mengesahkan kelayakan syarikat dan wakil mereka di Direktori Institusi Kewangan, Pendaftar Wakil, atau periksa Senarai Peringatan Pelabur MAS.
- **BERITAHU** - pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan sebarang transaksi menipu kepada bank anda dengan segera.



[Perbualan antara penipu dan ngsa]

⚠ Bagaimana melindungi diri anda

I Can ACT Against Scams

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

வெளியீடு
எண். 20
4 ஆகஸ்ட் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

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**.

வேலை மோசடி

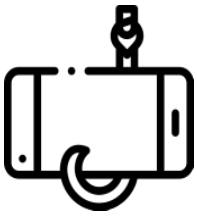
நீங்கள் சிறிதும் முயற்சி செய்யாமல், அதிக சம்பளம் வழங்குவதாக உறுதியளிக்கும் ஒரு வேலை வாய்ப்பைப் பெறுகிறீர்கள்.

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

முதலீட்டு மோசடி

மிக உயர்ந்த வருவாய்யைக் கொண்ட ஒரு முதலீடு உங்களுக்கு வழங்கப்படுகிறது.

இந்த மோசடி வகை பற்றிய மேல் விவரங்களுக்கு, அடுத்த பக்கத்தைப் பார்க்கவும்.



தகவல் திருட்டு மோசடி (அரசாங்க அமைப்புகளைப் போல ஆள்மாறாட்டம் செய்யும் அழைப்புகள்) *

“அரசாங்க அதிகாரி” ஒருவரிடமிருந்து உங்களுக்கு அழைப்பு வருகிறது. உங்கள் வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) மற்றும்/அல்லது தனிப்பட்ட விவரங்களை வழங்குமாறு நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகளைத் தடுக்கவும், கறுப்புப் பட்டியலிடப்பட்ட எண்களிலிருந்து மோசடி குறுஞ்செய்திகளைக் கண்டறியவும், உங்கள் கைபேசியில் உள்ள அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களில் இருந்து மட்டுமே ஸ்கேம்ஷீல்ட் செயலியைச் **சேர்க்கவும்**. தெரியாத நபர்களுக்கு உங்கள் விவரங்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் (OTP) வழங்காதீர்கள்.

இணைய வர்த்தக மோசடி (மற்றவை)

நீங்கள் ஒரு கவர்ச்சிகரமான ஒப்பந்தத்தை (எ. கா., இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள், மின்னணு பொருட்கள் போன்றவை) இணையத்தில் பார்க்கிறீர்கள். பின்னர் நீங்கள் ஒரு செய்தி அனுப்பும் செயலி மூலம் விற்பனையாளரை தொடர்பு கொள்கிறீர்கள். பணம் செலுத்திய பிறகு, பொருள் அல்லது சேவை வழங்கப்படவில்லை, மேலும் விற்பனையாளரையும் தொடர்பு கொள்ள முடியவில்லை.

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.

இத்தகைய மோசடிகளுக்குப் பின்னால் உள்ள பெயர்ப் பட்டியலை https://go.gov.sg/pnr-ecommerce-scams-involving-electronics-and-concert-tickets என்ற இணையத்தளத்தில் பார்க்கவும்.

*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது.

வருவாய் இல்லாத முதலீடு

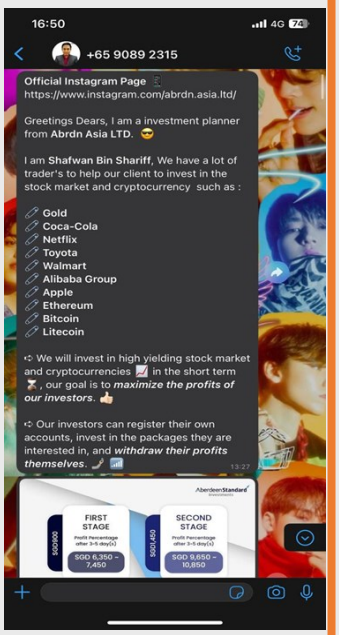
மோசடி உத்திகள்

- "முதலீட்டு வாய்ப்புகளை" அறிமுகப்படுத்த சமூக ஊடகத் தளங்கள், செய்தி அனுப்பும் செயலிகள் போன்ற பல்வேறு வழிகள் மூலம் மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களை அணுகுவர்.
- ஒரு அணுகுமுறையில், மோசடிக்காரர்கள் காலப்போக்கில் பாதிக்கப்பட்டவர்களுடன் நல்லுறவை உருவாக்கி, அவர்களின் நம்பிக்கையைப் பெற "முதலீட்டு வாய்ப்புகளை" அவர்களுக்கு அறிமுகப்படுத்துவார்கள். பாதிக்கப்பட்டவர்களின் நம்பிக்கையை வென்ற பிறகு, "முதலீடுகள்" என்ற சாக்குப்போக்கின் கீழ் பரிவர்த்தனைகளை நடத்துமாறு மோசடிக்காரர்கள் அவர்களிடம் கேட்பார்கள்.
- பாதிக்கப்பட்டவர்கள் பொதுவாக சிறிய இலாபங்களைப் பெறுவார்கள், ஆரம்பத்தில் அவர்களின் "முதலீடுகள்" உண்மையானவை என்று நம்புவதற்கு அவர்களை வசீகரிப்பார்கள். இருப்பினும், அவர்கள் அதிக தொகையை முதலீடு செய்யும் போது, அவர்கள் தங்கள் 'லாபத்தை' திரும்பப் பெற முடியாது, அப்போதுதான் தாங்கள் மோசடி செய்யப்பட்டதை அவர்கள் உணர்வார்கள்.
- மற்றொரு அணுகுமுறையில், பாதிக்கப்பட்டவர்கள் சமூக ஊடகத் தளங்களில் முதலீட்டு விளம்பரங்களைக் காண்பார்கள். விளம்பர இணைப்புகளைக் கிளிக் செய்த பிறகு, பாதிக்கப்பட்டவர்கள் மோசடிக்காரர்களைத் தொடர்புகொள்ள தகவல்தொடர்பு செயலிகளுக்கு இட்டுச் செல்லப்படுவார்கள்.
- மோசடிக்காரர்கள் பின்னர், மோசடி விமர்சனங்களால் ஆதரிக்கப்படும், குறுகிய காலத்தில் அதிக வருமானம் கொண்ட "வாய்ப்புகளில் முதலீடு" செய்ய பாதிக்கப்பட்டவர்களை கவர்ந்திழுப்பார்கள். சில வேளைகளில், பாதிக்கப்பட்டவர்கள் தமது தனிப்பட்ட விவரங்களையும் அட்டை விவரங்களையும் கணக்கிற்குப் பதிவு செய்வதற்கு வழங்குமாறு "முதலீடு" இணையத்தளங்களுக்கு இட்டுச் செல்லப்படுவர்.
- தாங்கள் 'லாபத்தைத்' திரும்பப் பெற முடியாதபோது அல்லது மோசடிக்காரர்களைத் தொடர்புகொள்ள முடியாதபோது மட்டுமே தாங்கள் மோசடி செய்யப்பட்டிருப்பதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.
- சில சந்தர்ப்பங்களில், "முதலீட்டு" செயல்முறைகள் குறித்த கூடுதல் தகவல்களைப் பெறுவதற்காக, தொலை அணுகல் மென்பொருள்களை (எ. கா., AnyDesk) தங்கள் சாதனங்களில் பதிவிறக்கம் செய்ய மோசடிக்காரர்களிடமிருந்து அழைப்புகள் அல்லது செய்திகளைப் பாதிக்கப்பட்டவர்கள் பெறுவார்கள். தொலை அணுகல் மூலம், மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் வங்கிக் கணக்குகளிலிருந்து அனைத்துப் பணத்தையும் எடுக்க முடியும்.

[.:பேஸ்புக் விளம்பரத்தின் ஓர் எடுத்துக்காட்டு]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

- **சேர்க்க** - ஸ்கேம்ஷீல்ட் செயலியை சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும் (எ. கா., வங்கிகளுக்கான two-form factor authentication மற்றும் வங்கிப் பரிவர்த்தனை வரம்புகளை அமைக்கவும்). சரிபார்க்கப்படாத மூலங்களிலிருந்து பெறப்பட்ட மென்பொருளை ஒருபோதும் நிறுவாதீர்கள், ஏனெனில் இது மோசடிக்காரர்கள் உங்கள் செயல்களைக் கவனிக்கவோ அல்லது உங்கள் சாதனங்களைத் தொலைவிலிருந்து கட்டுப்பாட்டுக்குள் கொண்டுவரவோ அனுமதிக்கும்.
- **சரிபார்க்க** - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். நம்பகத்தன்மையை உறுதிப்படுத்த:
  - ⇒ முதலீட்டை முழுமையாகப் புரிந்துகொள்ளத் தேவையான பல கேள்விகளைக் கேளுங்கள். நிறுவனத்தால் பதிலளிக்க முடியாவிட்டால் அல்லது நிறுவனம் உங்கள் கேள்விகளைத் தவிர்த்தால் எச்சரிக்கையாக இருங்கள்.
  - ⇒ முதலீடுகள் உண்மையானவையா என்பதை மதிப்பிட, நிறுவனத்தின் தகவல்கள், எ. கா., உரிமையாளர்கள், இயக்குநர்கள் மற்றும் நிர்வாகத் தகவல்களைச் சரிபார்க்கவும்.
  - ⇒ நிதி அமைப்புகள் கையேடு, பிரதிநிதிகள் பதிவேடு அல்லது MAS-இன் முதலீட்டாளர் எச்சரிக்கை பட்டியலில் நிறுவனத்தின் மற்றும் பிரதிநிதிகளின் சான்றிதழ்களை உறுதிப்படுத்துங்கள்.
- **சொல்ல** - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.



[மோசடிக்காரருக்கும் பாதிக்கப்பட்டவருக்கும் இடையிலான உரையாடல்]

எப்படி உங்களைப்

I Can ACT Against Scams

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