Issue 40 22 Dec 2023

Weekly Scams Bulletin

A publication by the Singapore Police Force and the National Crime Prevention Council

Trending Scams in the past week:

Job Scam

Investment Scam

Fake Friend Call Scam

Social Media Impersonation Scam

E-Commerce Scam (Variants)

Want to buy that popular event/concert ticket? Be careful.

Scam Tactics

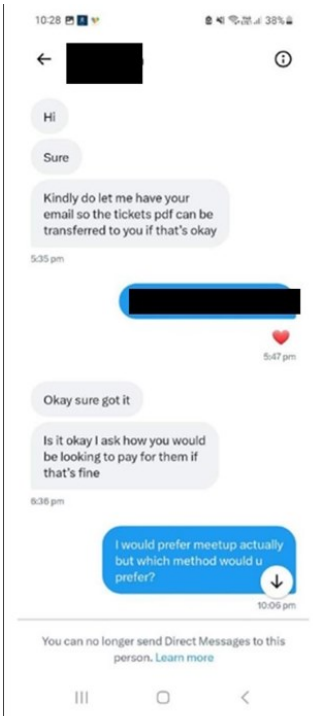
Scammers would post advertisements selling concert tickets on e-commerce/social media platforms (e.g. Carousell, Xiaohongshu, Facebook, Telegram, X). Due to time-sensitive or limited-in-quantity ticket sales, victims would be rushed to make payment.

To prove authenticity, scammers would share screenshots/videos of fake ticket/receipts and promise to email/transfer the tickets to the victims, after successful payment.

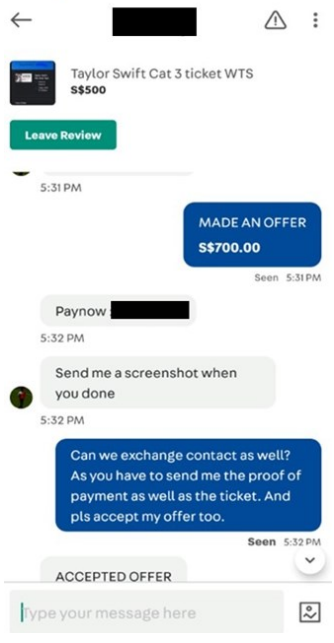
Victims will make payment through virtual credits (e.g iTunes), PayNow or bank transfers and may be asked for additional payments, citing reasons like initial payment was not received.

Victims would realise they had been scammed:
(a) After making payment, there were no delivery of ticket/s and the scammer becomes uncontactable; or

(b) Ticket (s) received were invalid on the day of the concert.



Examples of how scammers promise to email the ticket after payment.



Some Precautionary Measures:

ADD – ScamShield App and security features (e.g., enable Two-Factor Authentication (2FA), Multifactor Authentication for banks and set up transaction limits for internet banking transactions, including PayNow).

Use "escrow" payment options that protect buyers by releasing payment to the seller only upon delivery. Avoid making advance payments or direct bank transfers. Purchase only from authorised sellers and legitimate ticket marketplaces/resellers, such as SISTIC and Ticketmaster.

CHECK – For scam signs and with official sources (e.g. ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot, or call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg). Arrange for a physical meet-up with the seller to verify the authenticity of the physical tickets. Bear in mind that the party you are dealing with online is a stranger.

TELL – Authorities, family, and friends about scams. Report the fraudulent advertisements to the social media and e-commerce platforms!

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

40号刊 2023年12月22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:

求职诈骗

投资诈骗

假朋友来电骗局

社交媒体
冒充他人骗局

电子商务骗局
（各种手法）

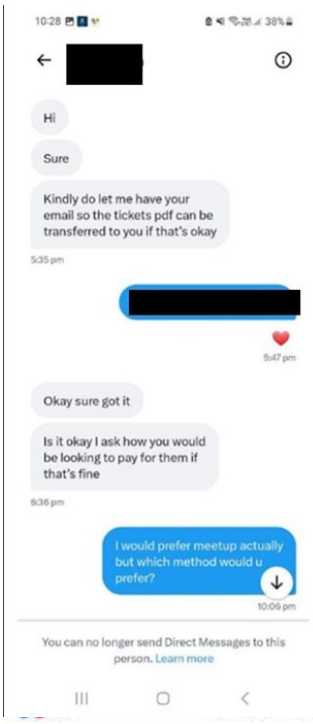
想买热门活动/演唱会门票？请小心。

诈骗手法

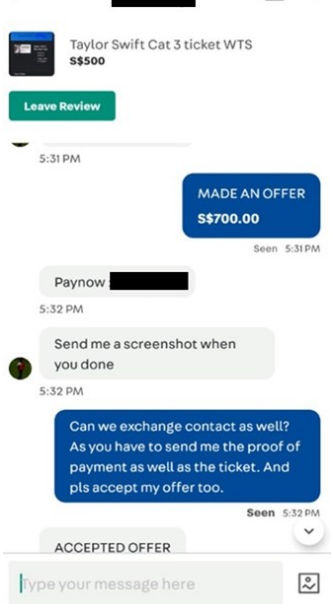
骗子会在电子商务/社交媒体平台（如 Carousell、小红书、脸书、Telegram、X）上刊登销售演唱会门票的广告。由于时间紧迫或门票数量有限，受害者会急着付款。为了证明门票的真实性，骗子会分享假门票/收据的截图/视频，并承诺在成功付款后将门票电邮/传送给受害者。

受害者将通过虚拟信用（如iTunes）、PayNow 或银行转账付款，并可能以未收到首次付款等原因被要求额外付款。 受害者在以下情况发生后才意识到自己被骗了：

(a) 付款后，没交上门票，且无法联系骗子；或
(b) 演唱会当日发现门票无效。



【骗子如何承诺在付款后通过电邮发送门票的例子】



一些预防措施：

添加 – ScamShield应用程序并设置安全功能（如在银行账户启用双重或多重认证并设置网络银行交易限额，包括 PayNow）。

使用“托管” (escrow) 付款选项，仅在交货时向卖方发放付款的安全支付方式。避免预付款项或预先通过银行转账给卖家。只向授权卖家以及正当的售票市场/转售商 (如 SISTIC 和 Ticketmaster) 购买门票。

查证 – 官方消息并注意诈骗迹象（如查询ScamShield WhatsApp 机器人@ https://go.gov.sg/scamshield-bot、拨打反诈骗热线1800-722-6688或到游览 www.scamalert.sg）。安排与卖家会面以核实实体门票的真实性。切记，在网上和您交易的是一个陌生人。

通报 – 当局、家人和朋友诈骗案件趋势。向社交媒体平台和电子商务平台举报具欺诈性的广告！

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

Isu no. 40

22 Disember 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Pekerjaan

Penipuan Pelaburan

Penipuan Panggilan Kawan Palsu

Penipuan Penyamaran di Media Sosial

Penipuan E-Dagang (Varian penipuan)

Ingin membeli tiket acara / konsert popular itu? Berhati-hati.

Taktik Penipuan

Penipu akan menyiarkan iklan yang menjual tiket konsert di platform e-dagang / media sosial (contohnya Carousell, Xiaohongshu, Facebook, Telegram, X). Disebabkan jualan tiket yang sensitif masa atau terhad dalam jumlahnya, mangsa akan didesak untuk membuat pembayaran.

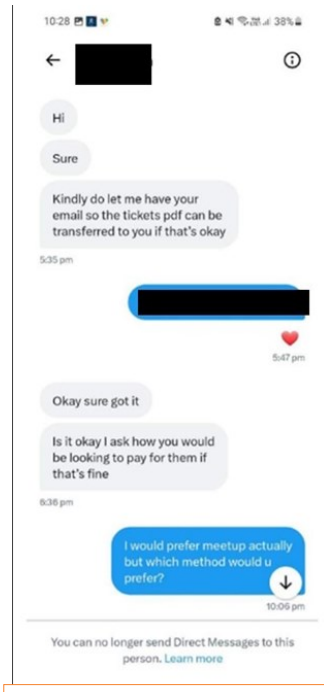
Untuk membuktikan kesahihan tiket tersebut, penipu akan berkongsi tangkap layar atau video tiket / resit palsu dan berjanji untuk menghantar e-mel atau memindahkan tiket kepada mangsa selepas pembayaran berjaya.

Mangsa akan membuat pembayaran melalui kredit maya (contohnya iTunes), PayNow atau pemindahan bank. Mangsa juga mungkin diminta membuat pembayaran tambahan, dengan alasan seperti bayaran awal yang telah dibuat tidak diterima.

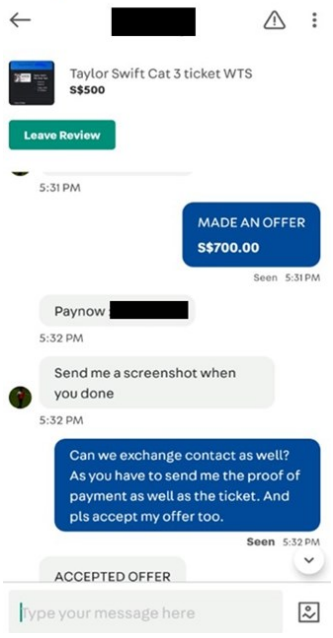
Mangsa akan menyedari mereka telah ditipu apabila:

(a) Tiada penghantaran tiket selepas pembayaran dibuat dan penipu tidak dapat dihubungi; atau

(b) Tiket yang diterima tidak sah pada hari berlangsungnya konsert tersebut



Contoh bagaimana penipu berjanji untuk menghantar tiket menerusi e-mel selepas pembayaran dibuat.



Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi ScamShield dan pasangkan ciri-ciri keselamatan (misalnya, dayakan pengesahan dua-faktor (2FA) untuk bank dan tetapkan had transaksi untuk transaksi perbankan internet, termasuklah PayNow).

Gunakan pilihan pembayaran "escrow" yang melindungi pembeli dengan melepaskan pembayaran kepada penjual hanya selepas penghantaran telah dibuat. Elakkan daripada membuat bayaran pendahuluan atau pemindahan bank secara langsung kepada penjual. Beli hanya daripada penjual yang sah dan pasaran jualan / penjual semula tiket yang sah, seperti SISTIC dan Ticketmaster.

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (misalnya periksa dengan bot ScamShield WhatsApp di https://go.gov.sg/scamshield-bot, telefon Talian Bantuan Antipenipuan di 1800-722-6688, atau layari www.scamalert.sg).

Aturkan sebuah pertemuan secara fizikal dengan penjual untuk mengesahkan ketulenan tiket-tiket tersebut. Ingatlah bahawa pihak yang sedang anda berurusan dalam talian ini ialah orang yang tidak dikenali.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan iklan penipuan tersebut ke platform media sosial dan e-dagang!

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

வெளியீடு எண். 40

22 டிசம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

நீங்கள் ஒரு பிரபலமான நிகழ்ச்சி/கச்சேரி நுழைவுச்சீட்டை வாங்க விரும்புகிறீர்களா? கவனமாக இருங்கள்.

மோசடி உத்திகள்

மின் வணிகம்/சமூக ஊடகத் தளங்களில் (எ.கா. Carousell, Xiaohongshu, Facebook, Telegram, X) கச்சேரி நுழைவுச்சீட்டுகளை விற்கும் விளம்பரங்களை மோசடிக்காரர்கள் பதிவிடுவார்கள். குறுகிய காலக்கட்டத்துக்கோ அல்லது குறைந்த அளவிலோ நுழைவுச்சீட்டு விற்கப்படுவதால், விரைவாக பணம் செலுத்துமாறு பாதிக்கப்பட்டவர்கள் கேட்டுக்கொள்ளப்படுவார்கள்.

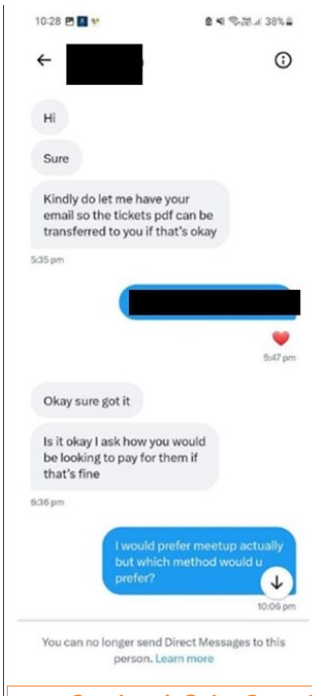
நம்பகத்தன்மையை நிரூபிக்க, மோசடிக்காரர்கள் போலி நுழைவுச்சீட்டுகள் அல்லது ரசீதுகளின் ஸ்கிரீன்ஷாட்கள் அல்லது காணொளிகளைப் பகிர்ந்து கொள்வார்கள். வெற்றிகரமாக பணம் செலுத்திய பிறகு நுழைவுச்சீட்டுகளை மின்னஞ்சல் மூலம் அனுப்புவதாகவோ அல்லது பாதிக்கப்பட்டவருக்கு மாற்றுவதாகவோ அவர்கள் உறுதியளிப்பார்கள்.

மெய்நிகர் கட்டண முறைகள் (எ.கா. ஐடியூன்ஸ்), PayNow அல்லது வங்கி மாற்றங்கள் மூலம் பாதிக்கப்பட்டவர்கள் பணம் செலுத்துவார்கள். ஆரம்பக் கட்டணத்தைப் பெறவில்லை போன்ற காரணங்களை மேற்கோள் காட்டி கூடுதல் பணம் செலுத்துமாறு அவர்கள் கேட்டுக்கொள்ளப்படலாம்.

பின்வருபவை நடக்கும்போது மட்டுமே தாங்கள் மோசடி செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்:

(a) பணம் செலுத்திய பிறகு, நுழைவுச்சீட்டு/கள் அனுப்பப்படாது. அதனுடன் மோசடிக்காரர் தொடர்புகொள்ள முடியாதவராகிவிடுவார்.; அல்லது

(b) இசை நிகழ்ச்சி நடைபெறும் நாளன்று, பெறப்பட்ட நுழைவுச்சீட்டு/கள் செல்லுபடியாகாது.



ஃபேஸ்புக்கில் போலி பயணப்பெட்டிக்கான விளம்பரங்களின் எடுத்துக்காட்டுகள்

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

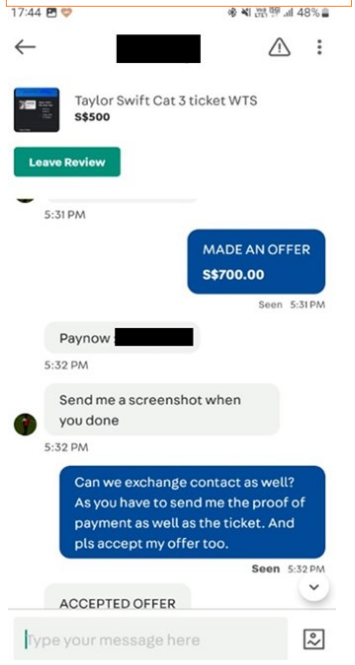
சேர்க்க - ஸ்கேம்ஷீல்டு செயலியைப் பதிவிறக்கம் செய்து, பாதுகாப்பு அம்சங்களை அமைத்திடுங்கள் (எ.கா. வங்கிகளுக்கு இரட்டை மறைச்சொல் முறையையும் (2FA) பன்முக உறுதிப்பாட்டையும் செயல்படுத்தலாம். PayNow உள்ளிட்ட இணைய வங்கிப் பரிவர்த்தனைகளுக்கு வரம்புகளை நிர்ணயிக்கலாம்).

நுழைவுச்சீட்டுகள் பெறப்பட்ட பின்னரே விற்பனையாளருக்கு பணம் கிடைப்பதன் மூலம் வாங்குபவர்களைப் பாதுகாக்கும் "எஸ்க்ரோ (escrow)" கட்டண முறைகளைப் பயன்படுத்துங்கள். முன்பணம் செலுத்துவதையோ நேரடி வங்கி மாற்றங்களையோ செய்வதைத் தவிர்க்கவும். அங்கீகரிக்கப்பட்ட விற்பனையாளர்கள், சிஸ்டிக், டிக்கெட் மாஸ்டர் போன்ற சட்டபூர்வமான நுழைவுச்சீட்டு சந்தைகள்/மறுவிற்பனையாளர்களிடமிருந்து மட்டுமே வாங்குங்கள்.

சரிபார்க்க - மோசடி அறிகுறிகளை அதிகாரபூர்வத் தகவல் மூலங்களுடன் சரிபாருங்கள் (எ.கா. ஸ்கேம்ஷீல்டு வாட்ஸ்ஆப் பொட் @ https://go.gov.sg/scamshield-bot நாடலாம், அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம், அல்லது www.scamalert.sg இணையத்தளத்தை நாடலாம்).

நுழைவுச்சீட்டுகளின் நம்பகத்தன்மையை சரிபார்க்க விற்பனையாளருடன் ஒரு நேரடி சந்திப்புக்கு ஏற்பாடு செய்யுங்கள். நீங்கள் இணையம் வழி தொடர்புக் கொண்ட நபர் ஒரு அந்நியர் என்பதை நினைவில் கொள்ளுங்கள்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். மோசடி விளம்பரங்களைப் பற்றி சமூக ஊடகத் தளங்கள், மின் வணிகத் தளங்கள் ஆகியவற்றிடம் புகார் செய்யுங்கள்!



இந்த மோசடி குறித்த மேல் விவரங்களுக்கு, SPF | News (police.gov.sg) இணையத்தளத்தை நாடுங்கள்.

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

வேலை மோசடி

முதலீட்டு மோசடி

போலி நண்பர் அழைப்பு மோசடி

சமூக ஊடக ஆள்மாறாட்ட மோசடி

இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)