2024 – Issue 5 2 Feb 2024

Weekly Scams Bulletin

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

Trending Scams in the past week:

Job Scam

Fake Friend Call Scam

Investment Scam

Phishing Scam (Social Media)

Phishing Scam (Bank)

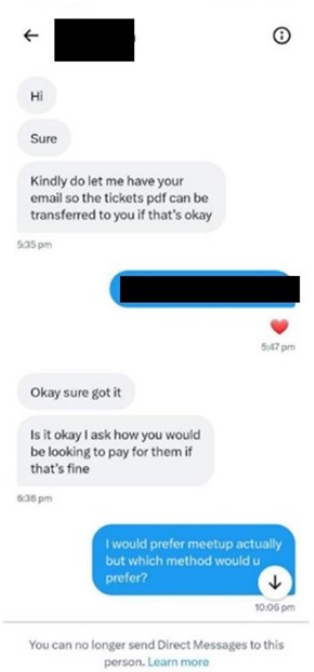
Planning to buy concert tickets from a reseller? Look out for scam signs!

Scam Tactics

Scammers would sell fake concert tickets on e-commerce/ social media platforms, especially on Telegram, Carousell, X, Facebook, and Xiaohongshu.

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

Victims would realise they had been scammed when they do not receive the tickets after making payment, or they find out that their tickets are invalid on the day of the concert.



Example of how scammer promised to email the ticket after payment.

Some Precautionary Measures:

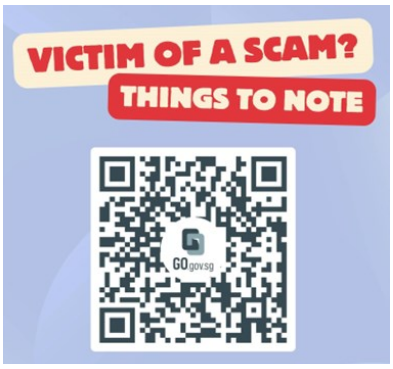
ADD – ScamShield App and security features (e.g., enable Two-Factor Authentication (2FA), Multifactor Authentication for banks and set up transaction limits for internet banking transactions, including PayNow).

CHECK – For scam signs and check with official sources (e.g. visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688).

Avoid making advance payments or direct bank transfers. Use "escrow" payment options that protect buyers by releasing payment to the seller only upon delivery of item/service.

Arrange for a physical meet-up with the seller to verify the authenticity of the physical tickets before making payment. Bear in mind that the party you are dealing with online is a stranger.

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



SPF's Anti-Scam Resource Guide
Information and relevant FAQs for scam victims

Visit www.go.gov.sg/spf-scamresources for a copy of SPF's Anti-Scam Resource Guide.

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

I Can ACT Against Scams

ADD ScamShield app and security features

CHECK for scam signs and with official sources

TELL Authorities, family and friends

NATIONAL CRIME PREVENTION COUNCIL

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

2024 – 5号刊 2024年2月2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

假朋友来电骗局

投资诈骗

钓鱼骗局 (社交媒体)

钓鱼骗局 （银行）

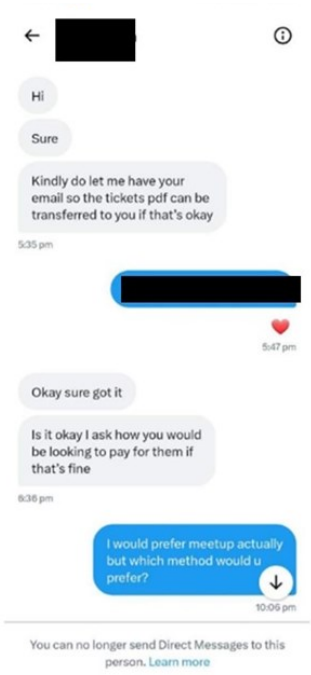
打算向转售商购买演唱会门票吗？注意诈骗迹象！

诈骗手法

骗子会在电子商务/社交媒体平台上出售假演唱会门票，尤其是在Telegram、Carousell、X、脸书和小红书。

为了证明门票的真实性，骗子可能会分享假门票/收据的截图，并承诺在成功付款后将门票以电邮/传送方式交给受害者。

当受害者在付款后没收到门票，或在演唱会当天发现门票无效时，才意识到自己被骗了。



[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：

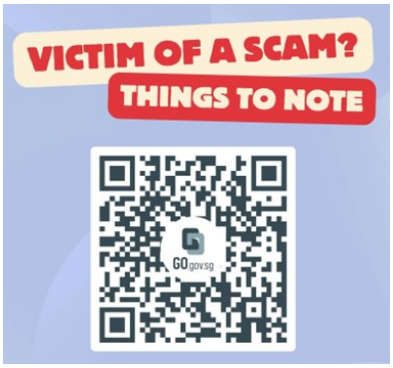
添加 – ScamShield 应用程序并设置安全功能（如在银行账户启用双重或多重认证并设置网络银行交易限额，包括 PayNow)。

查证 – 官方消息并注意诈骗迹象（如游览 www.scamalert.sg查询或拨打反诈骗热线 1800-722-6688)。

避免预付款项或预先通过银行转账给卖家。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。

付款前，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骗子的账户/具欺诈性的广告！



新加坡警察部队的反诈骗资源指南:
为诈骗受害者提供信息及常见问题

请浏览 www.go.gov.sg/spf-scamresources 获取新加坡警察部队反诈骗资源指。

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

I Can ACT Against Scams

ADD ScamShield app and security features

CHECK for scam signs and with official sources

TELL Authorities, family and friends

NATIONAL CRIME PREVENTION COUNCIL

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

2024 – Isu no. 5 2 Feb 2024

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Pekerjaan

Penipuan Panggilan Kawan Palsu

Penipuan Pelaburan

Penipuan Pancingan Data (Media Sosial)

Penipuan Pancingan Data (Bank)

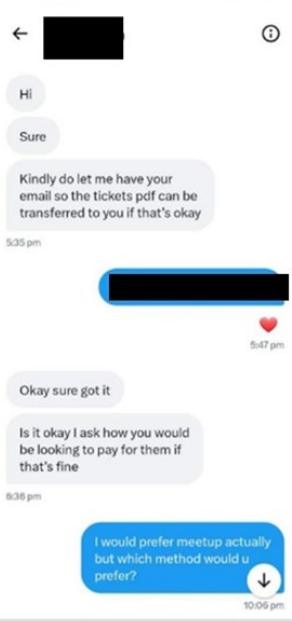
Merancang untuk membeli tiket konsert daripada penjual semula? Perhatikan tanda-tanda penipuan!

Taktik Penipuan

Penipu akan menjual tiket konsert palsu di platform e-Dagang /media sosial, terutamanya di Telegram, Carousell, X, Facebook, dan Xiaohongshu.

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

Mangsa akan menyedari mereka telah ditipu apabila mereka tidak menerima tiket selepas membuat bayaran, atau mereka mendapat tahu bahawa tiket mereka 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).

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (boleh layari www.scamalert.sg atau telefon Talian Bantuan Antipenipuan di 1800-722-6688).

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.

Aturkan sebuah pertemuan secara fizikal dengan penjual untuk mengesahkan ketulenan tiket-tiket tersebut sebelum membuat pembayaran. 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!

Panduan Sumber Antipenipuan SPF: Maklumat dan Soalan yang Lazim ditanya untuk mangsa penipuan

Sila lungsuri www.go.gov.sg/spf-scamresources untuk mendapatkan salinan Panduan Sumber Antipenipuan SPF.

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

2024 – வெளியீடு எண். 5

2 பிப்ரவரி 2024

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

வேலை மோசடி

போலி நண்பர் அழைப்பு மோசடி

முதலீட்டு மோசடி

தகவல் திருட்டு மோசடி (சமூக ஊடகம்)

தகவல் திருட்டு மோசடி (வங்கி)

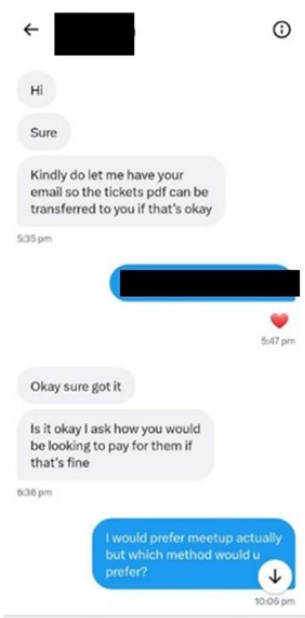
கலைநிகழ்ச்சி நுழைவுச்சீட்டுகளை மறுவிற்பனையாளரிடம் வாங்க நினைக்கிறீர்களா? மோசடி அறிகுறிகளைக் கவனிக்கத் தவறாதீர்கள்!

மோசடி உத்திகள்

மோசடிக்காரர்கள் போலியான கலைநிகழ்ச்சி நுழைவுச்சீட்டுகளை இணைய வர்த்தக / சமூக ஊடகத் தளங்களில் விற்பனை செய்வார்கள். குறிப்பாக, டெலிகிராம், கரோசல், X, ∴பேஸ்புக், சியாவ்ஹொங்ஷு போன்ற தளங்களில்.

நுழைவுச்சீட்டுகள் உண்மையானவை என்பதை நிரூபிக்க, மோசடிக்காரர்கள் போலி நுழைவுச்சீட்டை / ரசீதைப் படமெடுத்து பகிரலாம். பணம் கட்டியவுடன் நுழைவுச்சீட்டுகளை மின்னஞ்சல் செய்வதாக / அனுப்புவதாக அவர்கள் வாக்குறுதியளிப்பார்கள்.

பாதிக்கப்பட்டவர்கள் பணம் கட்டிய பிறகு நுழைவுச்சீட்டுகள் கிடைக்காமல் போகும்போது, அல்லது அந்த நுழைவுச்சீட்டுகள் செல்லுபடியாகாதவை என்பது கலைநிகழ்ச்சி நடைபெறும் நாளில் தெரியவரும்போது மோசடிக்கு உள்ளானதை உணர்வார்கள்.



பணம் செலுத்திய பிறகு நுழைவுச்சீட்டை மின்னஞ்சலில் அனுப்புவதாக மோசடிக்காரர்கள் வாக்குறுதியளித்ததற்கான 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).

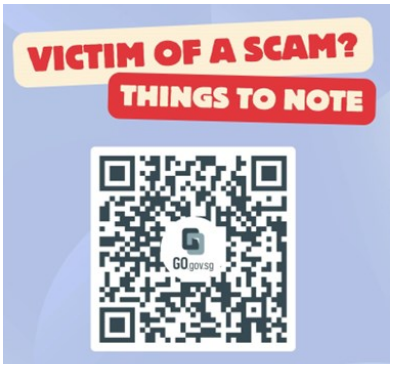
சரிபார்க்க - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (எ.கா. www.scamalert.sg இணையத்தளத்தை நாடலாம் அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம்).

நுழைவுச்சீட்டுகள் பெறப்பட்ட பின்னரே விற்பனையாளருக்கு பணம் கிடைப்பதன் மூலம் வாங்குபவர்களைப் பாதுகாக்கும் "எஸ்க்ரோ (escrow)" கட்டண முறைகளைப் பயன்படுத்துங்கள். முன்பணம் செலுத்துவதையோ நேரடி வங்கி பணமாற்றுகள் செய்வதையோ தவிர்க்கவும்.

பணம் கொடுப்பதற்குமுன் அச்சிடப்பட்ட நுழைவுச்சீட்டுகள் உண்மையானவையா என்பதைச் சரிபார்ப்பதற்காக, விற்பனையாளரை நேரில் சந்திக்க ஏற்பாடு செய்யவும். நீங்கள் இணையம்வழி தொடர்பில் இருப்பவர் முன்பின் தெரியாத அந்நியர் என்பதைக் கவனத்தில் கொள்ளவும்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள்.

மோசடி விளம்பரங்களைப் பற்றி சமூக ஊடகத் தளங்கள், மின் வணிகத் தளங்கள் ஆகியவற்றிடம் புகார் செய்யுங்கள்!



மோசடிக்கு உள்ளானவர்களுக்கான சிங்கப்பூர் காவல் துறையின் மோசடித் தடுப்பு வழிகாட்டி: தகவலும் அடிக்கடி கேட்கப்படும் கேள்விகளும்

மேல்விவரம் அறிய, www.go.gov.sg/spf-scamresources இணையத்தளத்திற்குச் சென்று சிங்கப்பூர் காவல் துறையின் மோசடித் தடுப்பு வழிகாட்டியைப் பார்க்கவும்.

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