2024 – Issue 1 5 Jan 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

Fake Friend Call Scam

Investment Scam

E-Commerce Scam (Variants)

Phishing Scam

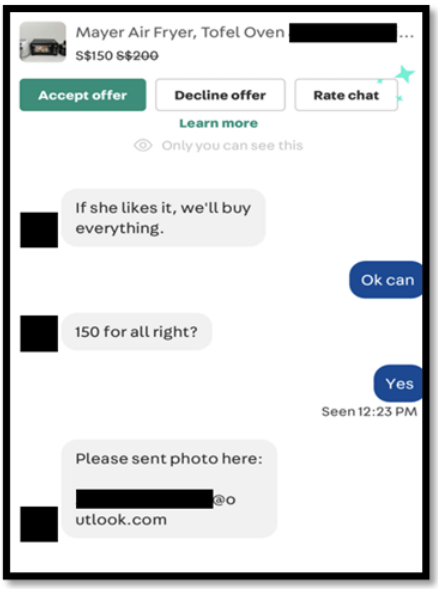
Selling items online? Beware of fake buyers!

Scam Tactics

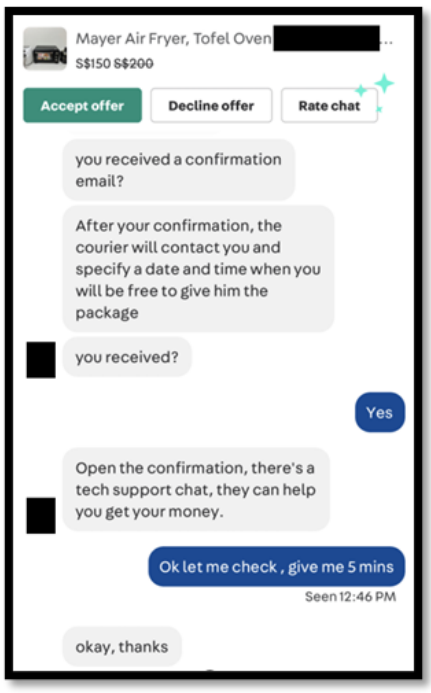
Scammers would pose as interested buyers to items on platforms such as Carousell and Facebook. After agreeing to the purchase, scammers would send a malicious URL link or QR code (through email, in-app messaging, or WhatsApp) on the pretext for victims to receive payment or to pay for courier arrangements to deliver the item.

Upon clicking on the links or scanning the QR codes, victims would be directed to a fake website to provide their internet banking login credentials, credit card details and/or One-Time Password (OTP).

Victims would realise they had been scammed after they were notified or discovered unauthorised card/banking transactions.



Screenshots of conversations between the victim and scammer



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). Never disclose your personal or internet banking details and OTP to anyone.

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).

Do not click on dubious URL links and always verify the authenticity of URL links. If in doubt, always verify the authenticity of the information with the e-commerce platform directly.

TELL – Authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately and report any suspicious user and fraudulent transaction from the online marketplace to the e-commerce platform.

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

2024 – 1 号刊 2024年1月5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

电子商务骗局
（各种手法）

钓鱼骗局

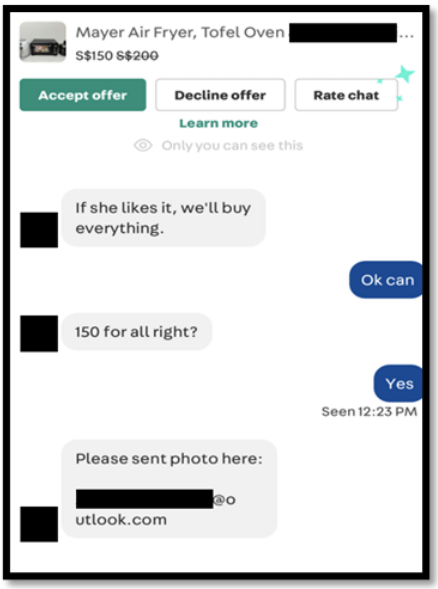
假网站日益剧增：警惕钓鱼诈骗迹象！

诈骗手法

骗子会在Carousell和脸书等平台上假装有兴趣购买商品。同意购买后，骗子会假借付款或支付快递费用为由，通过电子邮件、应用程序或WhatsApp向受害者发送一个恶意链接或二维码。

一旦点击链接或扫描二维码，受害者将被转接至一个虚假银行网站以提供网上银行登录凭证、信用卡信息和/或一次性密码 (OTP)。

受害者在收到通知或发现自己的信用卡/银行账户有未经授权的交易时意识到自己被骗了。



受害者和骗子对话的截图

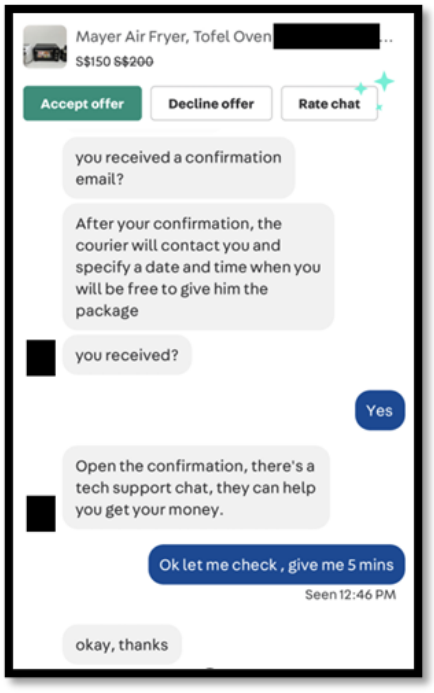
一些预防措施：

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)。切勿向任何人透露您的个人或网上银行资料以及一次性密码（OTP）。

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)。

切勿点击可疑链接并务必确认链接的真实性。若有疑问，务必直接向电子商务平台核实信息的真实性。

通报 – 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，并向电子商务平台举报任何可疑用户以及具欺诈性的交易。



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

2024 – Isu no. 1 5 Jan 2023

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 E-Dagang (Varian penipuan)

Penipuan Pancingan Data

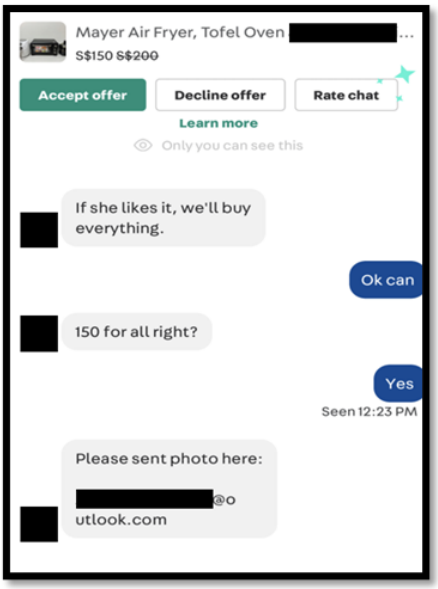
Menjual barangan secara dalam talian? Berhati-hati dengan pembeli palsu!

Taktik Penipuan

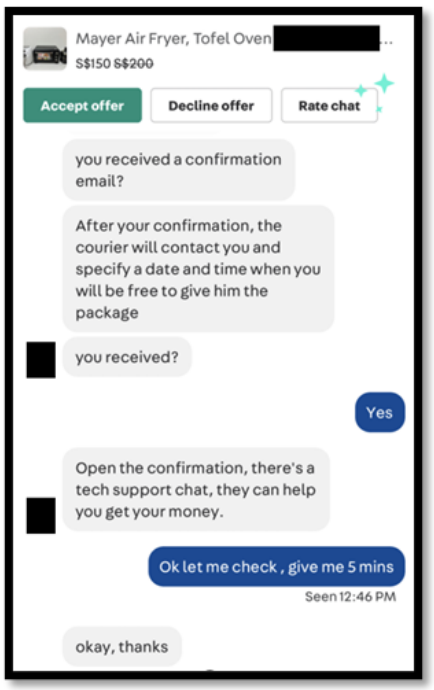
Penipu akan berpura-pura menjadi pembeli yang berminat untuk membeli barangan di platform seperti Carousell dan Facebook. Selepas bersetuju dengan pembelian itu, penipu akan menghantar pautan URL atau kod QR berniat jahat (melalui e-mel, mesej dalam aplikasi, atau WhatsApp) dengan alasan bahawa mangsa memerlukannya untuk menerima bayaran atau membayar pengaturan perkhidmatan kiriman cepat bagi menghantar barangan tersebut.

Selepas mengklik pada pautan URL atau mengimbas kod QR tersebut, mangsa akan diarahkan ke laman web palsu untuk memasukkan butiran log masuk perbankan internet, butiran kad kredit dan / atau Kata Laluan Sekali Guna (OTP).

Mangsa akan menyedari mereka telah ditipu setelah mereka dimaklumkan atau mendapat tahu adanya transaksi kad / perbankan tanpa kebenaran.



Tangkap layar perbualan antara mangsa dan penipu



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). Jangan sekali-kali mendedahkan butiran peribadi atau perbankan internet dan OTP anda kepada sesiapa.

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). Jangan klik pada pautan URL yang meragukan dan sentiasa pastikan ketulenan pautan URL tersebut. Jika berasa ragu, sentiasa sahkan kesahihan maklumat dengan platform e-Dagang secara langsung.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan sebarang transaksi penipuan kepada bank anda dengan segera dan laporkan mana-mana pengguna yang mencurigakan dan sebarang transaksi menipu daripada pasaran dalam talian kepada platform e-dagang tersebut.

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

2024 – வெளியீடு எண். 1

5 ஜனவரி 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

வேலை மோசடி

போலி நண்பர் அழைப்பு மோசடி

முதலீட்டு மோசடி

இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)

தகவல் திருட்டு மோசடி

நீங்கள் இணையத்தில் பொருட்களை விற்பனை செய்கிறீர்களா? போலியான வாங்குபவர்கள் குறித்து கவனமாக இருங்கள்!

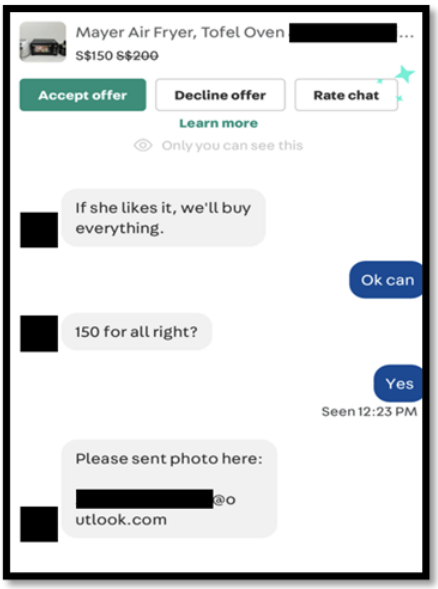
மோசடி உத்திகள்

கேரோசல், ஃபேஸ்புக் போன்ற தளங்களில் விற்கப்படும் பொருட்களை வாங்க விருப்பமுள்ளவர்களைப் போல மோசடிக்காரர்கள் ஆள்மாறாட்டம் செய்வார்கள்.

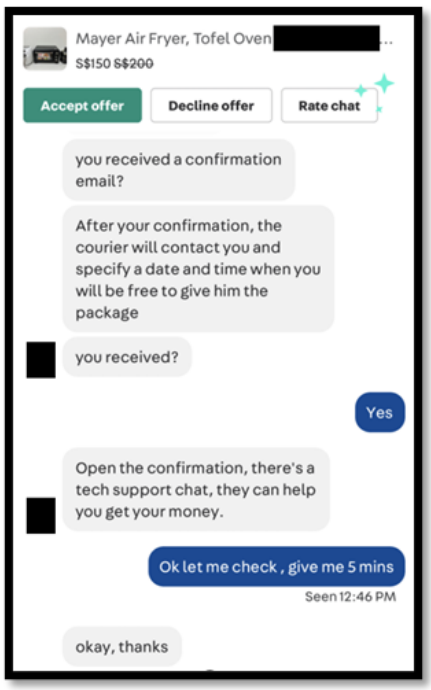
வாங்குவதற்கு ஒப்புக் கொண்ட பிறகு, பாதிக்கப்பட்டவர் பணம் பெறுவதற்கு அல்லது பொருளை வழங்குவதற்கான கூரியர் ஏற்பாடுகளுக்கு அவர்கள் பணம் செலுத்துவதற்கு போன்ற காரணங்களை மேற்கோள் காட்டி, மோசடிக்காரர்கள் தீங்கிழைக்கும் இணையத்தள முகவரி அல்லது விரைவுத் தகவல் குறியீட்டை மின்னஞ்சல், செயலி வழி குறுஞ்செய்தி அல்லது வாட்ஸ்ஆப் மூலம் அனுப்புவார்கள்.

இணைப்புகளைக் கிளிக் செய்த பிறகு அல்லது விரைவுத் தகவல் குறியீடுகளை ஸ்கேன் செய்த பிறகு, பாதிக்கப்பட்டவர்கள் தங்கள் இணைய வங்கி உள்நுழைவு விவரங்கள், கடன்பற்று அட்டை விவரங்கள் மற்றும்/அல்லது ஒரு முறை கடவுச் சொல் ஆகியவற்றை போலி இணையத்தளத்தில் வழங்குமாறு கேட்கப்படுவார்கள்.

அது பற்றி அவர்களுக்குத் தெரிவிக்கப்பட்ட பிறகு அல்லது அங்கீகரிக்கப்படாத அட்டை/வங்கி பரிவர்த்தனைகளைக் கண்டுபிடித்த பிறகு அவர்கள் மோசடி செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



பாதிக்கப்பட்டவருக்கும் மோசடிக்காரருக்கும் இடையிலான உரையாடல்களின் ஸ்கிரீன்ஷாட்கள்



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). உங்கள் தனிப்பட்ட அல்லது இணைய வங்கி விவரங்களையும், உங்கள் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் யாரிடமும் சொல்லாதீர்கள்.

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). சந்தேகத்திற்குரிய இணையத்தள முகவரிகளை கிளிக் செய்ய வேண்டாம். எப்போதும் இணையத்தள முகவரி இணைப்புகளின் நம்பகத்தன்மையை சரிபார்க்கவும். உங்களுக்கு சந்தேகம் இருந்தால், தகவல்களின் உண்மைத்தன்மையை மின் வர்த்தகத் தளத்துடன் நேரடியாகச் சரிபார்க்கவும்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். எந்தவொரு மோசடி பரிவர்த்தனை பற்றியும் உடனடியாக உங்கள் வங்கியிடம் புகார் செய்யவும். இணையச் சந்தையில் எந்தவொரு சந்தேகத்திற்கிடமான பயனரையும் மோசடி பரிவர்த்தனையையும் மின்-வர்த்தகத் தளத்திடம் புகார் செய்யவும்.

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