Issue 38 8 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** 



Social Media Impersonation Scam



**E-Commerce Scam** (Variants)

### The year-end festive season is here: Stay safe, stay alert!

### **Scam Tactics**

With the upcoming festive period and peak online sales season, everyone is reminded to stay vigilant as scammers may take the opportunity to target online shoppers.

Scammers may post enticing deals for items (such as festive food items, electronics, hotel room booking, tour packages and concert tickets) and become uncontactable after payment is made.

Always shop on well-established e-commerce platforms and check the platform's safety rating on MHA's Transaction Safety Ratings for major e-commerce platforms at https://go.gov.sg/mhatsr.

You should also check the credibility of the seller based on his/her customer reviews before you transact.

If you are expecting a parcel delivery, do not click on links provided in unsolicited messages or emails.

Learn preventive measures you can take to protect yourself and your loved ones against scams from the new ACT Campaign song (https://go.gov.sg/ACT2023).

Together, we can ACT against scams!



Visit go.gov.sg/ACT2023 to have a listen!



https://go.gov.sg/act2023

### **Some Precautionary Measures:**

ADD - ScamShield App and security features (e.g., add an anti-virus app on your mobile devices, enable Two-Factor Authentication (2FA), Multifactor Authentication for your online accounts and set up transaction limits for internet banking transactions, including PayNow).

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).

TELL - Authorities, family, and friends about scams. Never disclose your personal or banking credentials, including One Time Passwords (OTPs) to anyone. Report any fraudulent transactions to your bank and the Police immediately.

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







38号刊 2023年12月8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:



假朋友来电骗局



求职诈骗



投资诈骗



社交媒体 冒充他人骗局



电子商务骗局 (各种手法)

## 年底佳节将至:注意安全,提高警惕!

### 诈骗手法

佳节与网络销售旺季将至, 骗子或许会趁机向网上购物的您下手。在此提醒大家提高警 惕。

骗子可能会在网上发布诱人的优惠(如节庆食品、电子产品、酒店订房、旅游配套和演唱 会门票)。骗子在买家付款后就失联了。

务必在信誉良好的电子商务平台购物,并游览https://go.gov.sg/mhatsr查看大型电子商务平 台的内政部交易安全评级。

在进行交易前, 您也应查看卖家的客户评论以了解他/她的可信度。

即使您有包裹在送往您的路上,切勿点击未经请求的短信或电邮提供的链接。

通过新的防诈骗歌曲(https://go.gov.sg/act2023)了解保护自己和亲人免受诈骗的预防措 施。

我们同心协力, 齐心防诈!



游览 go.gov.sg/ACT2023 听听新防诈骗歌曲!



https://go.gov.sg/act2023

### -些预防措施:

添加 - ScamShield应用程序并设置安全功能(如在手机添加防毒应用程序、在网上账户启 用双重或多重认证并设置网络银行交易限额,包括 PayNow)。

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)。

通报 - 当局、家人和朋友诈骗案件趋势。 切勿向任何人透露您的个人或网上银行资料。这 包括任何的一次性密码(OTP)。立即向银行及警方举报任何欺诈性的交易。

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







Isu no. 38 8 Disember 2023

## Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN
SEPANJANG MINGGU
LEPAS:



Penipuan Panggilan Kawan Palsu



Penipuan Pekerjaan



Penipuan Pelaburan



Penipuan Penyamaran di Media Sosial



Penipuan E-Dagang (Varian penipuan)

## Musim perayaan hujung tahun sudah tiba: Kekal selamat, berwaspadalah!

### **Taktik Penipuan**

Memandangkan musim perayaan dan musim puncak jualan dalam talian yang bakal menjelang tidak lama lagi, semua orang diingatkan supaya sentiasa berwaspada kerana penipu boleh mengambil kesempatan ini untuk menyasarkan pembeli dalam talian.

Penipu mungkin menyiarkan tawaran menarik untuk barangan (seperti barangan makanan perayaan, elektronik, tempahan bilik hotel, pakej pelancongan dan tiket konsert) dan tidak dapat dihubungi selepas pembayaran telah dibuat.

Sentiasa membeli-belah di platform e-dagang yang mantap dan periksa rating keselamatan urus niaga pelbagai platform e-dagang utama di Rating Keselamatan Urus Niaga MHA <a href="https://go.gov.sg/mhatsr">https://go.gov.sg/mhatsr</a>.

Anda juga harus memeriksa kredibiliti penjual berdasarkan ulasan para pelanggannya sebelum anda berurus niaga.

Jika anda sedang menantikan penghantaran sebuah pakej, jangan klik pada pautan yang disediakan dalam pesanan atau emel yang tidak diminta.

Pelajari langkah-langkah pencegahan terhadap penipuan yang boleh anda ambil untuk melindungi diri dan orang yang anda sayangi melalui lagu baharu Kempen ACT (<a href="https://go.gov.sg/act2023">https://go.gov.sg/act2023</a>).

Bersama-sama kita boleh Bertindak Menentang Penipuan!





Layari go.gov.sg/act2023 untuk mendengar!

#### Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi ScamShield dan pasangkan ciri-ciri keselamatan (misalnya, masukkan aplikasi antivirus ke peranti mudah alih anda, dayakan Pengesahan Dua-Faktor (2FA), Pengesahan Pelbagai Faktor untuk akaun dalam talian anda dan tetapkan had transaksi untuk transaksi perbankan internet, termasuklah PayNow).

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

**BERITAHU** - Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan.

Jangan sekali-kali dedahkan butiran peribadi atau perbankan anda, termasuk Kata Laluan Sekali (OTP) kepada sesiapa pun.

Laporkan sebarang transaksi menipu kepada bank anda dan pihak Polis dengan segera.

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







வெளியீடு எண். 38 8 டிசம்பர் 2023

# வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:



போலி நண்பர் அழைப்பு மோசடி



வேலை மோசடி



முதலீட்டு மோசடி



சமுக ஊடக ஆள்மாறாட்ட மோசடி



இணைய வர்த்தக மோசடி

(பல்வேறு வகைகள்)

## ஆண்டு இறுதி விழாக்காலம் வந்துவிட்டது: பாதுகாப்பாகவும் விழிப்பாகவும் இருங்கள்!

### மோசடி உத்திகள்

வரவிருக்கும் பண்டிகை காலத்தினாலும் அதிக எண்ணிக்கையில் இணையம் மூலம் பொருட்களை வாங்கும் காலக்கட்டத்தினாலும் மோசடிக்காரர்கள் இணையம் மூலம் பொருட்களை வாங்கும் மக்களைக் குறிவைக்கக்கூடும் என்பதால் அனைவரும் விழிப்புடன் இருக்க வேண்டும் என்று நினைவூட்டப்படுகிறது.

மோசடிக்காரர்கள் பொருட்களை (பண்டிகை உணவு பொருட்கள், எலக்ட்ரானிக்ஸ், ஹோட்டல் அறை முன்பதிவு நுழைவுச்சீட்டுகள், சுற்றுப்பயணத் தொகுப்புகள், இசை நிகழ்ச்சி நுழைவுச்சீட்டுகள் போன்றவை) கவர்ச்சிகரமான விலையில் விற்கலாம். பணம் செலுத்திய பிறகு, அவர்களைத் தொடர்பு கொள்ள (முடியாது.

எப்போதும் நன்கு அறியப்பட்ட மின் வர்த்தகத் தளங்களிலிருந்து வாங்குங்கள். https://go.gov.sg/mhatsr-இல் முக்கிய மின் வர்த்தகத் தளங்களுக்கான உள்துறை அமைச்சின் பரிவர்த்தனை பாதுகாப்பு மதிப்பீடுகளை (TSR) சரிபார்க்கவும்.

நீங்கள் பரிவர்த்தனை செய்வதற்கு முன்பு விற்பனையாளரின் வாடிக்கையாளர் மதிப்பாய்வுகளின் அடிப்படையில் விற்பனையாளரின் நம்பகத்தன்மையையும் நீங்கள் சரிபார்க்க வேண்டும்.

நீங்கள் பார்சலை எதிர்பார்த்துக்கொண்டிருந்தால், தெரியாத செய்திகள் அல்லது மின்னஞ்சல்களில் உள்ள இணைப்புகளைக் கிளிக் செய்ய வேண்டாம்.

அன்புக்குரியவர்களையும் எதிராக உங்களையும் உங்கள் நீங்கள் மோசடிகளுக்கு பாதுகாக்க மேற்கொள்ளக்கூடிய தடுப்பு நடவடிக்கைகளைப் பற்றி புதிய ACT இயக்கப் பாடலிலிருந்து கற்றுக்கொள்ளுங்கள் (https://go.gov.sg/ACT2023).



பாடலை கேட்க go.gov.sg/ <u>ACT2023</u> என்ற இணையத்தளத்தை நாடுங்கள்!



### சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - ஸ்கேம்ஷீல்டு செயலியைப் பதிவிறக்கம் செய்து, பாதுகாப்பு அம்சங்களை அமைத்திடுங்கள் (எ.கா. உங்கள் கைப்பேசிச் சாதனங்களில் வைரஸ் எதிர்ப்பு செயலியைச் சேர்த்து, உங்கள் இணைய மறைச்சொல் முறையையும் பன்(ழக கணக்குகளுக்கு இரட்டை (2FA) உறுதிப்பாட்டையும் செயல்படுத்தலாம். PayNow உள்ளிட்ட இணைய வங்கிப் பரிவர்த்தனைகளுக்கு நிர்ணயிக்கலாம்).

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

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) உட்பட, உங்களது தனிப்பட்ட அல்லது வங்கி விவரங்களை யாரிடமும் ஒருபோதும் வெளியிடாதீர்கள்.

மோசடி பரிவர்த்தனைகளை உங்கள் வங்கியிடம் உடனடியாகத் தெரியப்படுத்துங்கள்.

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



#### **ADD**



