Issue 35 17 Nov 2023

## Weekly Scams Bulletin

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

Trending Scams in the past week:



Social Media
Impersonation Scam



Job Scam



Fake Friend Call Scam



**Investment Scam** 



E-Commerce Scam (Variants)

### Received a call from someone claiming to be from the Police? SLOW DOWN and CHECK FOR SCAM SIGNS.

#### **Scam Tactics**

Impersonating bank staff, scammers call victims alleging attempted unauthorised bank transactions were made.

Subsequently, victim would receive another call by scammers, impersonating as Police officers. Victims are informed they are under investigation for money laundering and instructed to transfer their savings into a bank account provided. Victims realise they are scammed when they are unable to access their money.

Such scams are facilitated by a complex network of bank accounts, purchased, or rented by scammers. These accounts allow the victims' monies to be withdrawn from Automated Teller Machines (ATMs) by money mules within the same day.

#### **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 with official sources (e.g. ScamShield WhatsApp bot @ www.go.gov.sg/scamshield-bot, or call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg). No police officer or government official would require you to transfer money to any designated bank accounts. You may call the Police Hotline at 1800-255-000 to check if you are unsure.

Do not allow anyone to access your bank account(s) or Singpass. Our bank accounts and Singpass accounts are for our own use. It is illegal to share them as your accounts may be used to facilitate scams or other crimes.

TELL – Authorities, family, and friends about scams and do not be pressured by the caller to act . Report the number to messaging platforms (e.g., WhatsApp and Telegram) to initiate in-app blocking and report any fraudulent transactions to your bank immediately.



Photo of fake Police warrant card sent to the victim.
The photo used was obtained online.



Photos of seized exhibits

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





35号刊 2023年11月17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:



社交媒体 冒充他人骗局



求职诈骗



假朋友来电骗局





电子商务骗局 (各种手法)

### 接到自称来自警方的来电吗? 放慢脚步并注意诈骗迹象。

#### 诈骗手法

受害者接到骗子冒充银行职员的来电,声称有人试图进行 未经授权的银行交易。受害者之后接到另一通骗子冒充警 方的电话。

受害者被告知他们正在接受涉及洗钱案件的调查,并被指 示将存款转入骗子提供的银行账户。受害者在无法使用存 款时, 意识到自己被骗了。

骗子购买或租用的银行账户所形成的复杂网络为这类骗局 提供便利。这些账户允许钱骡在当天从自动提款机 (ATM)提取受害者的存款。

#### 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 (如查询 ScamShield WhatsApp 机器人@ www.go.gov.sg/scamshield-bot、 拨打反诈骗热线 1800-722-6688 或 到 游 览 www.scamalert.sg)。警方及政府官员不会要求您把款项 转移到任何指定的银行账户。若有疑问,可拨打警方热线 1800-255-000 咨询。

切勿允许任何人访问您的银行或 SingPass 账户。我们的 银行和 SingPass 账户仅供我们自己使用。分享账户是违 法的,因为您的账户可能被用来为诈骗或其他罪案提供便 利。

通报 - 当局、家人和朋友诈骗案件趋势,并不要在来电者 的施压下有任何行动。立即向通讯平台(如 WhatsApp 和 Telegram) 举报该号码以启动应用程序内的屏蔽功能和立 即向银行举报任何欺诈性的交易。

#### **FAKE WARRANT CARD**



【发给受害者并含有伪 造警察证的照片。 骗子所使用的照片是从 网上搜寻到的。】



【遭查获证物的照片】

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





Isu no. 35 17 Nov 2023

## Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN **SEPANJANG MINGGU** LEPAS:



Penipuan Penyamarandi **Media Sosial** 



Penipuan Pekerjaan



Penipuan Panggilan **Kawan Palsu** 



Penipuan Pelaburan



Penipuan E-Dagang (Varian penipuan)

#### Mendapat panggilan daripada seseorang yang mendakwa daripada pihak polis? JANGAN TERBURU-BURU dan PERIKSA TANDA-TANDA PENIPUAN.

#### Taktik Penipuan

Dengan menyamar sebagai kakitangan bank, penipu akan menelefon mangsa sambil mendakwa ada percubaan untuk membuat transaksi bank tanpa kebenaran.

Seterusnya, mangsa akan menerima panggilan lain daripada penipu yang menyamar sebagai pegawai polis. Mangsa akan diberitahu bahawa mereka sedang dalam siasatan untuk pengubahan wang haram dan diarahkan supaya memindahkan wang simpanan mereka ke dalam sebuah akaun bank yang disediakan. Mangsa akan menyedari bahawa mereka telah ditipu apabila mereka tidak boleh mengakses wang mereka.

Penipuan sedemikian dimudahkan oleh satu rangkaian kompleks melibatkan akaun bank yang dibeli atau disewa oleh penipu. Akaun-akaun ini membolehkan wang mangsa dikeluarkan dari mesin juruwang automatik (ATM) oleh keldai wang pada hari yang sama.

#### Beberapa langkah berjaga-jaga:

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

PERIKSA - Tanda-tanda penipuan dan dengan sumber-sumber rasmi (misalnya bot ScamShield WhatsApp di www.go.gov.sg/ scamshield-bot, atau telefon talian bantuan antipenipuan di 1800-722-6688, atau layari www.scamalert.sg). Pegawai polis atau pegawai pemerintah tidak akan sekali-kali meminta anda supaya memindahkan wang ke sebarang akaun bank yang ditetapkan. Anda boleh menelefon Talian Hotline Polis di 1800-255-000 untuk memeriksa jika anda tidak pasti.

Jangan benarkan sesiapapun untuk mengakses akaun bank atau Singpass anda. Akaun bank dan akaun Singpass kita adalah untuk kegunaan kita sahaja. Adalah salah di sisi undang-undang untuk berkongsi akaun-akaun tersebut kerana ia boleh digunakan untuk memudahkan penipuan atau jenayah lain.

BERITAHU - Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan dan jangan rasa tertekan oleh pemanggil untuk bertindak. Laporkan nombor tersebut ke platform pesanan (misalnya WhatsApp dan Telegram) untuk memulakan penyekatan dalam aplikasi dan laporkan sebarang transaksi menipu kepada bank anda dengan segera.

**FAKE WARRANT CARD** WARRANT CARD

Gambar kad waran Polis palsu yang dihantar kepada mangsa. Gambar yang digunakan telah diambil dalam talian.



Gambar barang-barang yang dirampas

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



security features

official sources





வெளியீடு எண். 35 17 நவம்பர் 2023

# வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:



சமூக ஊடக ஆள்மாறாட்ட மோசடி



வேலை மோசடி



போலி நண்பர் அழைப்பு மோசடி



முதலீட்டு மோசடி



இணைய வர்த்தக மோசடி பல்வேறு வகைகள்) யாராவது உங்களைத் தொலைபேசியில் தொடர்புகொண்டு, காவல்துறையிலிருந்து அழைப்பதாகச் சொன்னார்களா? பதறாமல் நிதானித்து, அது மோசடி அழைப்பாக இருப்பதற்கான அறிகுறிகள் உள்ளதா என்பதைக் கவனித்திடுங்கள்.

#### மோசடி உத்திகள்

மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களைத் தொலைபேசியில் அழைத்து, வங்கி ஊழியரைப்போல் பாசாங்கு செய்து, அனுமதியற்ற வங்கிப் பரிவர்த்தனைகளை நிறைவேற்ற முயற்சி செய்யப்பட்டதாகச் சொல்வார்கள்.

அதன்பின், பாதிக்கப்பட்டவருக்கு மோசடிக்காரரிடமிருந்து இன்னொரு அழைப்பு வரும். இம்முறை, மோசடிக்காரர் காவல்துறை அதிகாரிபோல் பாசாங்கு செய்வார். சட்டவிரோத கள்ளப் பணப்புழக்கத்தின் தொடர்பில் பாதிக்கப்பட்டவர்மீது விசாரணை தொடங்கப்பட்டிருப்பதாக மோசடிக்காரர் அவரிடம் கூறுவார். அவரது சேமிப்பை ஒரு வங்கிக் கணக்குக்கு மாற்றும்படி மோசடிக்காரர் உத்தரவிடுவார். பாதிக்கப்பட்டவர் தனது பணத்தை எடுக்க முடியாமல் போகும்போது மோசடிக்கு உள்ளானதை உணர்வார்.

மோசடிக்காரர்கள் வாங்கிய அல்லது வாடகைக்கு எடுத்த வங்கிக் கணக்குகளின் விரிவான கட்டமைப்பு இத்தகைய மோசடிகளுக்குத் துணைபுரிகிறது. பாதிக்கப்பட்டவர்கள் இந்த வங்கிக் கணக்குகளில் பணம் போடும் அதே நாளில் தானியக்க ஏடிஎம் (ATM) சாதனங்களின்வழி பணத்தை எடுத்துக்கொள்ள இந்தக் கணக்குகள் பயன்படுகின்றன.

#### சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

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

சரிபார்க்க - மோசடி அறிகுறிகளை அதிகாரபூர்வத் தகவல் மூலங்களுடன் சரிபாருங்கள் (எ.கா. ஸ்கேம்ஷீல்டு வாட்ஸ்ஆப் பொட் @ www.go.gov.sg/ scamshield-bot நாடலாம், அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம், அல்லது www.scamalert.sg இணையத்தளத்தை நாடலாம்) காவல்துறை அதிகாரி அல்லது அரசாங்க அதிகாரி எவரும், குறிப்பிட்ட வங்கிக் கணக்குகளுக்குப் பணத்தை அனுப்புமாறு உங்களிடம் ஒருபோதும் கூறமாட்டார்கள் உங்களுக்கு உறுதியாக இல்லாவிட்டால், 1800-255-0000 என்ற தொலைபேசி எண்ணில் காவல்துறையை அழைக்கலாம்.

உங்களது வங்கிக் கணக்குகளை அல்லது சிங்பாஸ் கணக்கைப் பயன்படுத்த யாருக்கும் அனுமதி தராதீர்கள். நமது வங்கிக் கணக்குகளும் சிங்பாஸ் கணக்கும் நமது சொந்த பயன்பாட்டுக்கானவை அவற்றைப் பிறருடன் பகிர்வது சட்டவிரோதச் செயலாகும். ஏனெனில், உங்களது கணக்குகள் மோசடிகளுக்கு அல்லது மற்ற குற்றச்செயல்களுக்குப் பயன்படுத்தப்படலாம்..

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள் அந்த எண்ணைத் தடுக்க வாட்ஸ்ஆப்பில் புகார் செய்வதோடு, எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்கு தெரிவிக்கவும்.

**FAKE WARRANT CARD** 



பாதிக்கப்பட்டவருக்கு அனுப்பப்பட்ட போலி காவல்துறை அத்தாட்சி அட்டையின் புகைப்படம். இதில் உள்ள புகைப்படம் இணையத்திலிருந்து எடுக்கப்பட்டது.



பறிமுதல் செய்யப்பட்ட பொருட்களின் புகைப்படங்கள்

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





