Issue 37 1 Dec 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

Investment Scam

Fake Friend Call Scam

E-Commerce Scam (Variants)

Phishing Scam

## Impersonator alert! Some tell-tale signs that a WhatsApp account has been compromised.

### Scam Tactics

Scammers would impersonate victims and use victims' compromised WhatsApp accounts to ask for personal details such as ibanking credentials or credit card details and/or urgent loans from people on victims' contact lists. Victims will realise they have been scammed when their WhatsApp contacts ask them to repay the loans or approached them to ask about the unusual requests they received from the victims.

Your family member's/friend's WhatsApp account may be compromised if they contact you and make unusual and urgent requests. Such requests may include asking you to make urgent money transfer(s) to unfamiliar bank accounts or PayNow numbers.

**Slow down and check!** Call (or video call) your family member/friend to check before you make any transfers. **Your** WhatsApp account might be compromised if you notice:

1) **Unusual activity** – Your account has been receiving messages or calls from unknown numbers.

2) **Trouble logging into your accounts** – You cannot access online accounts using your usual passwords and devices.

3) **Unknown linked devices found in your WhatsApp under "Settings".**


*Example of conversation between the scammer and the victim*

### Some Precautionary Measures:

**ADD** – Security features to your WhatsApp account by enabling the 'Two-Step Verification feature. This can be done by opening WhatsApp and going to 'Settings' →'Account' → 'Two-step verification' → 'Enable'. Set a device code and be aware of who has physical access to your phone.

**CHECK** – That you are on WhatsApp Web's official website. Go to WhatsApp settings > linked devices to review all devices linked to your account. To remove a linked device, tap the device > Log Out.

**TELL** – Authorities, family, and friends about scams. Never share your WhatsApp account verification codes, personal information, banking details and OTPs with anyone; report any fraudulent transactions to your bank immediately.

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

37号刊 2023年12月1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

投资诈骗

假朋友来电骗局

电子商务骗局

钓鱼骗局

## 假冒身份警示! 一些表明WhatsApp账户已遭盗用的迹象。

### 诈骗手法

骗子会冒充受害者并利用受害者已遭盗用的WhatsApp账户向联系人索取个人资料，如网上银行 (iBanking) 凭证、信用卡信息和/或要求紧急贷款。受害者在接到WhatsApp联系人要求他们偿还贷款或不寻常请求的通知后才意识到自己被骗了。

当家人/朋友通过WhatsApp向您提出不寻常和紧急请求时，他们的WhatsApp账户可能已遭盗用了。此类请求可包括要求您紧急转账至不熟悉的银行账户或PayNow号码。别急，先确认！在进行任何转账前，请拨打电话或视频通话给您的家人/朋友加以确认。

若您注意到以下情况，您的WhatsApp帐户可能已遭盗用:

1) 不寻常活动- 您的帐户一直接到未知号码的信息或来电。

2) 无法登录账户- 您无法使用常用的设备和密码访问线上账户。

3) 在WhatsApp设置”里出现未知的已绑定设备。


*【骗子和受害者对话的例子 】*

### 一些预防措施:

添加 – 在您的 WhatsApp应用程序设置添加账户“双重认证”安全功能。可通过打开WhatsApp并进入“设置”→“帐户”→“双重认证”→“启用”来完成。为您的设备设置密码并留意能接触您手机的人。

查证 – 确保您访问的是官方网页版 WhatsApp网站。到WhatsApp设置>已绑定设备检查所有与您账户绑定的设备。若想删除绑定设备，请选该设备>登出即可。

通报 – 当局、家人和朋友诈骗案件趋势。切勿与他人分享您WhatsApp账户认证密码、个人资料、银行资料及一次性密码 (OTP) 。立即向银行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. 37 1 Disember 2023

# Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

**TREND PENIPUAN SEPANJANG MINGGU LEPAS:**

Penipuan Penyamaran di Media Sosial

Penipuan Pelaburan

Penipuan Panggilan Kawan Palsu

Penipuan E-Dagang

Penipuan Pancingan Data

## Amaran Penyamar! Beberapa tanda-tanda ketara sesebuah akaun WhatsApp telah dikompromi.

### Taktik Penipuan

Penipu akan menyamar sebagai mangsa dan menggunakan akaun WhatsApp mangsa yang telah dikompromi untuk meminta butir-butir peribadi seperti butiran perbankan internet atau butir-butir kad kredit dan/atau pinjaman segera daripada orang-orang yang berada di dalam senarai kenalan mangsa. Mangsa akan menyedari mereka telah ditipu apabila kenalan WhatsApp mereka meminta mereka supaya membayar semula pinjaman atau memberitahu mereka tentang permintaan pelik yang mereka terima daripada mangsa.

Akaun WhatsApp anggota keluarga/ kawan anda mungkin telah dikompromi sekiranya mereka menghubungi anda dan membuat permintaan pelik dan yang mendesak. Permintaan sedemikian mungkin termasuk meminta anda memindahkan wang dengan segera ke akaun bank atau nombor PayNow yang tidak dikenali. **Jangan terburu-buru dan periksa** telefon (atau buat panggilan video) anggota keluarga/ kawan untuk memeriksa dahulu sebelum membuat sebarang pemindahan.

Akaun WhatsApp **anda** mungkin telah dikompromi jika anda perasan ini:

1) **Aktiviti pelik** – Akaun anda menerima pesanan atau panggilan dari nombor-nombor yang tidak dikenali.
2) **Masalah untuk log masuk ke dalam akaun anda** – Anda tidak dapat mengakses akaun dalam talian menggunakan kata laluan dan peranti biasa anda.
3) **Peranti yang dipautkan yang tidak dikenali terdapat di dalam WhatsApp anda di bawah "Tetapan".**


*Contoh perbualan antara penipu dan mangsa*

### Beberapa langkah berjaga-jaga:

**MASUKKAN** – Ciri-ciri keselamatan ke akaun WhatsApp anda dengan mendayakan ciri 'Pengesahan Dua Langkah '.

Ini boleh dilakukan dengan membuka WhatsApp dan pergi ke 'Tetapan' →'Akaun' → 'Pengesahan Dua Langkah' → 'Dayakan'. Tetapkan sebuah kod peranti dan berhati-hati terhadap sesiapa yang boleh mengakses telefon anda secara fizikal.

**PERIKSA** – Pastikan anda berada di laman web rasmi WhatsApp Web. Pergi ke tetapan WhatsApp > peranti yang dipautkan untuk memeriksa semua peranti yang dipautkan ke akaun anda. Untuk mengeluarkan sebuah peranti yang dipautkan, klik pada peranti tersebut > Log Keluar.

**BERITAHU** – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Jangan sekali-kali berkongsi kod pengesahan akaun WhatsApp, maklumat peribadi, butiran perbankan dan OTP anda dengan sesiapa; laporkan sebarang transaksi menipu kepada bank anda dengan segera.

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

வெளியீடு எண். 37

1 டிசம்பர் 2023

# வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

**கடந்த வாரத்தின் முன்னணி மோசடிகள்:**

சமூக ஊடக ஆள்மாறாட்ட மோசடி

முதலீட்டு மோசடி

போலி நண்பர் அழைப்பு மோசடி

இணைய வர்த்தக மோசடி

தகவல் திருட்டு மோசடி

## ஆள்மாறாட்ட எச்சரிக்கை! ஒரு வாட்ஸ்ஆப் கணக்கு பாதிக்கப்பட்டிருப்பதற்கான சில அறிகுறிகள்.

## மோசடி உத்திகள்

மோசடிக்காரர்கள் பாதிக்கப்பட்டவரைப் போல ஆள்மாறாட்டம் செய்வார்கள். பின்னர் அவர்களின் 'பாதிக்கப்பட்ட வாட்ஸ்ஆப் கணக்கைப்' பயன்படுத்தி இணைய வங்கிச் சேவை விவரங்கள் அல்லது கடன்பற்று அட்டை விவரங்கள் மற்றும் / அல்லது அவசர கடன்கள் போன்ற தனிப்பட்ட விவரங்களைப் பாதிக்கப்பட்டவர்களின் தொடர்பு பட்டியல்களில் உள்ளவர்களிடம் கேட்பார்கள். தங்களது வாட்ஸ்ஆப் தொடர்புகள் கடன்களைத் திருப்பிச் செலுத்துமாறு கேட்டுக்கொள்ளும்போதோ அல்லது பாதிக்கப்பட்டவரிடமிருந்து பெற்ற வழக்கத்திற்கு மாறான கோரிக்கைகளைப் பற்றி கேட்க அவர்களை அணுகும்போதோதான் அவர்கள் மோசடி செய்யப்பட்டிருப்பதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.

உங்கள் குடும்ப உறுப்பினர் / நண்பர் உங்களைத் தொடர்புகொண்டு வழக்கத்திற்கு மாறான, அவசரமான கோரிக்கைகளை முன்வைத்தால் அவர்களின் வாட்ஸ்ஆப் கணக்கு பாதிக்கப்பட்டிருக்கலாம். அத்தகைய கோரிக்கைகளில் அறிமுகமில்லாத வங்கி கணக்குகளுக்கு அல்லது PayNow எண்களுக்கு அவசர பணப்பரிமாற்றம்(கள்) செய்யும்படி உங்களிடம் கேட்பதும் அடங்கும். **அவசரப்படாமல் சரிபாருங்கள்!** நீங்கள் எந்தவொரு நிதி பரிமாற்றத்தையும் செய்வதற்கு முன்பு, உங்கள் குடும்ப உறுப்பினர் / நண்பருக்கு ஒரு தொலைபேசி அழைப்பு அல்லது வீடியோ அழைப்பை செய்து சரிபார்க்கவும்.

நீங்கள் பின்வருபவற்றைக் கவனித்தால், **உங்கள்** வாட்ஸ்ஆப் கணக்கு பாதிக்கப்பட்டிருக்கலாம்:

1) **வழக்கத்திற்கு மாறான செயல்பாடு** - உங்கள் கணக்கு தெரியாத எண்களிலிருந்து செய்திகள் அல்லது அழைப்புகளைப் பெற்று வருகிறது.

2) **உங்கள் கணக்குகளுக்குள் நுழைவதில் சிக்கல்** - உங்கள் வழக்கமான கடவுச்சொற்களையும் சாதனங்களையும் பயன்படுத்தி இணையக் கணக்குகளை நீங்கள் அணுக முடியாது.

3) **உங்கள் வாட்ஸ்ஆப்பின் "அமைப்புகள் (Settings)" -இல் அறியப்படாத இணைக்கப்பட்ட சாதனங்கள் காணப்படுகின்றன.**


*மோசடிக்காரருக்கும் பாதிக்கப்பட்டவருக்கும் இடையிலான உரையாடல்களின் எடுத்துக்காட்டு*

## சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

**சேர்க்க** - 'Two-Step Verification' என்ற 'இரண்டு படிநிலை சரிபார்ப்பு முறை' அம்சத்தை செயல்படுத்துவதன் மூலம் உங்கள் வாட்ஸ்ஆப் கணக்கில் பாதுகாப்பு அம்சங்களைச் சேர்க்கவும். இதனை வாட்ஸ்ஆப்பில் பின்வரும் படிநிலைகள் மூலம் செய்யலாம்: 'அமைப்புகள் (Settings)' → 'கணக்கு (Account)' → 'இரண்டு படிநிலை சரிபார்ப்பு (Two-step verification)' → 'இயலச்செய் (Enable)'. ஒரு சாதனக் குறியீட்டை அமைத்து, உங்கள் தொலைபேசியை யார் நேரடியாக அணுக முடியும் என்பதை அறிந்து கொள்ளுங்கள்.

**சரிபார்க்க** - நீங்கள் வாட்ஸ்ஆப் வெப்" -இன் அதிகாரபூர்வ இணையத்தளத்தைப் பயன்படுத்துவதைச் சரிபார்க்கவும். வாட்ஸ்ஆப் செயலியின் அமைப்புகள் (Settings) > இணைக்கப்பட்ட சாதனங்கள் (linked device) ஆகியவற்றுக்குச் சென்று உங்கள் கணக்குடன் இணைக்கப்பட்ட அனைத்து சாதனங்களையும் மறுஆய்வு செய்யுங்கள். இணைக்கப்பட்ட சாதனத்தை அகற்ற, சாதனத்தைக் கிளிக் செய்து, அதன் பிறகு வெளிச்செல்லவும்.

**சொல்ல** - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். உங்கள் வாட்ஸ்ஆப் கணக்கின் சரிபார்ப்புக் குறியீடுகள், தனிப்பட்ட தகவல்கள், வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் ஆகியவற்றை யாருடனும் பகிர்ந்து கொள்ளாதீர்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்குத் தெரிவிக்கவும்.

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