Issue 25 8 Sep 2023

Weekly Scams Bulletin

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

Trending Scams in the past week:

Fake Friend Call Scam

Investment Scam

Job Scam

E-Commerce Scam (Variants)

Social Media Impersonation Scam

Social Media Impersonation Scam Involving Telegram

Scam Tactics

Pretending to be a known contact, scammers take over victims' Telegram accounts by tricking them into disclosing their handphone numbers and Telegram login codes. Scammers would ask victims to:

i) Provide screenshots of chat histories or search results from locating someone on Telegram. The screenshots would contain Telegram login codes.

ii) Help to verify/ unblock a known contact's Telegram account. Victims will be asked to provide their login codes to a fake bot or via a URL link to do so.

iii) Click a URL link to help scammers secure free Telegram memberships.

Upon taking over victims' Telegram accounts, scammers would target victims' contacts and repeat their tactics or ask for loans.

Victims would realise they were scammed when they lose access to their Telegram accounts or when the loans are not recovered.

Some Precautionary Measures:

ADD – ScamShield App and set security features (e.g., enable 2FA for banks, social media, Singpass accounts; set transaction limits on internet banking transactions, including PayNow/PayLah).

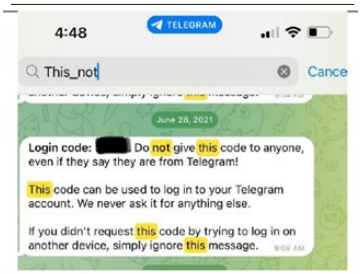
CHECK – for scam signs and with official sources (e.g. check with ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot or call Anti-Scam Helpline at 1800-722-6688 when unsure. Visit www.scamalert.sg to learn about the latest scams).

TELL – Report any fraudulent transactions to your bank immediately.

Block and report the sender to Telegram support if your account has been compromised.

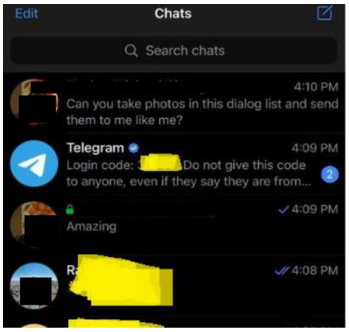
Inform your family and friends about your compromised account so that they don't fall prey.

Report the Telegram takeover incident to SingCERT via https://www.go.gov.sg/singcert-incident-reporting-form



Screenshot of Telegram login code after searching username 'this_not'

[Victims asked to search for a username and provide screenshot]



[Victims asked to provide screenshot of Telegram chat history]

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

25 号刊 2023年9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

投资诈骗

求职诈骗

电子商务骗局
(各种手法)

社交媒体
冒充他人骗局

涉及 Telegram的社交媒体冒充他人骗局

诈骗手法

骗子假装为已知联系人，通过诱骗受害者透露他们的手机号码和Telegram登录号码来接管受害者的Telegram账户。骗子会要求受害者:

i) 提供Telegram聊天记录或搜索结果的截图。截图里包含着Telegram登录号码。

ii) 帮助认证/解锁已知联系人的Telegram帐户。受害者会被要求向虚假机器人或通过链接提供登录号码 。

iii) 点击链接帮助骗子得到免费Telegram会员 。

接管受害者Telegram账户后，骗子会以受害者的联系人为目标并重复他们的手法或要求贷款。

受害者在失去Telegram账户访问权或无法收回贷款数额时，意识到自己被骗了。

一些预防措施:

下载 – ScamShield应用程序并设置安全功能（如在银行,社交媒体，Singpass账户启用双重认证；设置银行交易限额，包括PayNow/PayLah）。

查看 – 官方消息并注意诈骗迹象（在不确定时与ScamShield WhatsApp 机器人@ https://go.gov.sg/scamshield-bot查询或拨打反诈骗热线1800-722-6688。游览www.scamalert.sg了解最新诈骗手法）。

告知 – 立即向银行举报任何欺诈性的交易 。

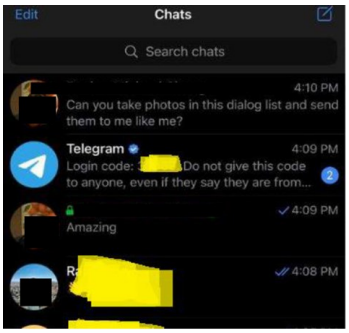
如果您的帐户已被盗用，请封锁并向Telegram举报发件人。

通知家人和朋友您的账户已遭盗用，避免他们成为受害者。

通过https://www.go.gov.sg/singcert-incident-reporting-form向SingCERT举报接管Telegram事件。

Screenshot of Telegram login code after searching username 'this_not'

[受害者被要求搜索用户名字并提供截图]



[受害者被要求提供Telegram聊天记录截图]

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

Isu no. 25 8 Sep 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 Pelaburan

Penipuan Pekerjaan

Penipuan E-Dagang (Varian penipuan)

Penipuan Penyamaran di Media Sosial

Penipuan Penyamaran di Media Sosial melibatkan aplikasi Telegram

Taktik Penipuan

Berpura-pura menjadi salah seorang kenalan yang diketahui, penipu akan mengambil alih akaun Telegram mangsa dengan memperdaya mereka supaya menyerahkan nombor telefon bimbit dan kod log masuk Telegram mereka. Penipu akan meminta mangsa:

i) Berikan tangkap layar sejarah sembang atau hasil carian daripada mengesan seseorang di Telegram. Tangkap layar tersebut akan mengandungi kod log masuk Telegram.

ii) Bantu mengesahkan / melepaskan sekatan akaun Telegram seseorang kenalan yang diketahui. Mangsa akan diminta memberikan kod log masuk mereka kepada satu bot palsu atau melalui pautan URL untuk berbuat demikian.

iii) Klik satu pautan URL untuk membantu penipu mendaftar keanggotaan percuma Telegram.

Sebaik sahaja penipu mengambil alih akaun Telegram mangsa, mereka akan menyasarkan kenalan mangsa dan mengulangi taktik mereka atau meminta pinjaman.

Mangsa hanya akan menyedari mereka sudah ditipu setelah mereka kehilangan akses kepada akaun Telegram mereka atau apabila pinjaman tidak dipulangkan.

Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi ScamShield dan pasangkan ciri-ciri keselamatan (misalnya, dayakan dua-faktor (2FA) untuk bank-bank, media sosial, akaun Singpass; tetapkan had transaksi untuk transaksi perbankan internet, termasuk PayNow /PayLah).

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (misalnya periksa dengan bot ScamShield di WhatsApp @ https://go.gov.sg/scamshield-bot atau telefon talian Hotline Antipenipuan di 1800-7222-6688 bila anda tidak pasti. Sila layari www.scamalert.sg untuk mempelajari tentang penipuan terkini.

BERITAHU – Laporkan sebarang transaksi menipu kepada bank anda dengan segera.

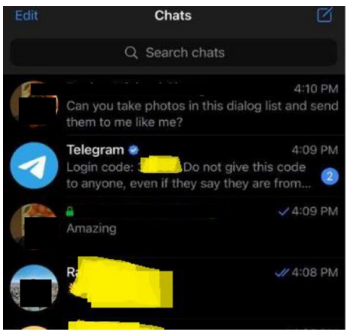
Sekat dan lapor tentang pengirimnya kepada bahagian sokongan Telegram jika akaun anda telah dikompromi.

Maklumkan kepada keluarga dan kawan-kawan anda tentang akaun anda yang telah dikompromi supaya mereka tidak menjadi mangsa.

Laporkan tentang pengambilalihan akaun Telegram kepada SingCERT melalui laman web https://www.go.gov.sg/singcert-incident-reporting-form

Screenshot of Telegram login code after searching username 'this_not'

[Mangsa diminta untuk mencari nama pengguna tertentu dan memberikan tangkap layar]



[Mangsa diminta untuk memberikan tangkap layar sejarah sembang Telegram]

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

வெளியீடு எண். 25

8 செப்டம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

போலி நண்பர் அழைப்பு மோசடி

முதலீட்டு மோசடி

வேலை மோசடி

மின்-வர்த்தக மோசடி (பல்வேறு வகைகள்)

சமூக ஊடக ஆள்மாறாட்ட மோசடி

டெலிகிராம் சம்பந்தப்பட்ட சமூக ஊடக ஆள்மாறாட்ட மோசடி

மோசடி உத்திகள்

மோசடிக்காரர்கள், பாதிக்கப்பட்டவர்களுக்குத் தெரிந்த ஒருவரைப் போல் பாசாங்கு செய்வார்கள். அவர்கள் பாதிக்கப்பட்டவர்களின் டெலிகிராம் கணக்குகளை தங்கள் கட்டுப்பாட்டுக்குள் கொண்டுவர, அவர்களின் கைப்பேசி எண்களையும் டெலிகிராம் உள்நுழைவு குறியீடுகளையும் அவர்களிடமிருந்து ஏமாற்றி வாங்கிக்கொள்வார்கள். மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களிடம் பின்வருபவற்றைக் கேட்பார்கள்:

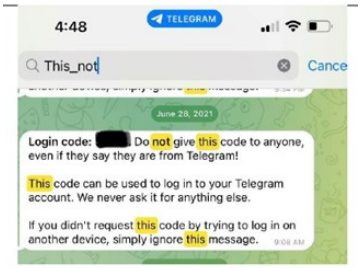
(i) அவர்களுடைய உரையாடல் வரலாறுகளின் ஸ்கிரீன்ஷாட்கள் அல்லது டெலிகிராமில் ஒருவரைக் கண்டுபிடிப்பதின் தேடல் முடிவுகளின் ஸ்கிரீன்ஷாட்கள். அதில் டெலிகிராம் உள்நுழைவு குறியீடுகள் இருக்கும்.

(ii) தெரிந்த தொடர்பின் டெலிகிராம் கணக்கைச் சரிபார்க்க / தடுக்க உதவி கேட்பார்கள். பாதிக்கப்பட்டவர்கள் தங்கள் உள்நுழைவு குறியீடுகளை ஒரு போலி போட் (bot) அல்லது இணையப்பக்க முகவரி (URL) இணைப்பு வழியாக வழங்குமாறு கேட்டுக்கொள்ளப்படுவார்கள்.

(iii) மோசடி செய்பவர்கள் இலவசமாக டெலிகிராமில் உறுப்பினராவதற்கு இணையப்பக்க முகவரி (URL) இணைப்பு ஒன்றைக் கிளிக் செய்ய கேட்டுக்கொள்வார்கள்.

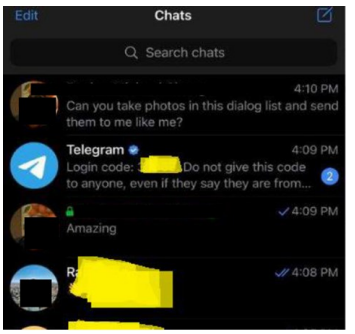
பாதிக்கப்பட்டவர்களின் டெலிகிராம் கணக்குகளைத் தங்கள் கட்டுப்பாட்டுக்குள் கொண்டுவந்தவுடன், மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களின் தொடர்புகளைக் குறிவைத்துத் தங்கள் உத்திகளை மீண்டும் செயல்படுத்துவார்கள் அல்லது கடன் கேட்பார்கள்.

தங்கள் டெலிகிராம் கணக்குகளுக்கான அணுகலை இழக்கும்போது அல்லது கடன்களை திரும்ப பெற முடியாதபோது தாங்கள் மோசடி செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.



Screenshot of Telegram login code after searching username 'this_not'

[பாதிக்கப்பட்டவர்கள் ஒரு பயனர்பெயரைத் தேடி ஸ்கிரீன்ஷாட் வழங்குமாறு கேட்டுக்கொள்ளப்பட்டனர்]



[பாதிக்கப்பட்டவர்கள் தங்கள் டெலிகிராம் உரையாடல் வரலாற்றின் ஸ்கிரீன்ஷாட்டை வழங்குமாறு கேட்டுக்கொள்ளப்பட்டனர்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்கவும் - ஸ்கேம்ஷீல்டு செயலியைச் சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும் (எ. கா., வங்கிகள், சமூக ஊடகம், Singpass கணக்குகளுக்கு 2FA முறையைச் செயல்படுத்தவும்; PayNow/PayLah உள்ளிட்ட இணைய வங்கிச் சேவை பரிவர்த்தனைகளின் மீது பரிவர்த்தனை வரம்புகளை அமைக்கவும்).

சரிபார்க்கவும் - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (எ. கா. ஸ்கேம்ஷீல்டு வாட்ஸ்ஆப் போட் (bot) உடன் https://go.gov.sg/scamshield-bot என்ற இணையத்தளத்தில் சரிபாருங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.) ஆக அண்மை மோசடிகளைப் பற்றி அறிய www.scamalert.sg இணையத்தளத்தை நாடுங்கள்.

சொல்லவும் - மோசடி பரிவர்த்தனைகள் ஏதேனும் இருந்தால் உடனடியாக உங்கள் வங்கியிடம் புகாரளிக்கவும்.

உங்கள் கணக்கு பாதிக்கப்பட்டிருந்தால், அனுப்புநரைத் தடுத்து டெலிகிராமிடம் புகார் செய்யவும்.

உங்கள் குடும்பத்தாரும் நண்பர்களும் மோசடி செய்யப்படாமல் இருக்க, உங்களுடைய பாதிக்கப்பட்ட கணக்கைப் பற்றி அவர்களிடம் சொல்லுங்கள்.

உங்கள் டெலிகிராம் கணக்கு கையகப்படுத்தப்பட்ட சம்பவத்தை https://www.go.gov.sg/singcert-incident-reporting-form வழியாக SingCERT-இடம் புகார் செய்யுங்கள்.

இந்த மோசடி பற்றிய மேல் விவரங்களுக்கு, பார்வையிடவும் SPF | News (police.gov.sg)