2024 – Issue 2 12 Jan 2024

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

Banks will never send you clickable links via SMS!

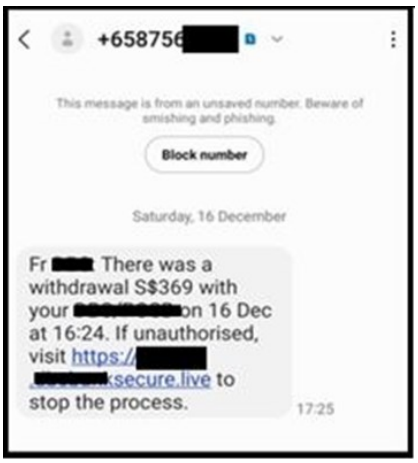
Scam Tactics

Scammers impersonate banks, reaching out to victims via SMS or WhatsApp to phish for victims' online banking usernames, passwords, and One-Time Passwords (OTP).

These messages warn victims on possible unauthorised attempts to access their bank accounts, urging victims to act immediately by clicking the embedded URL links to verify their identity and stop the transactions.

Upon clicking the link, victims would be directed to a fake bank website, to provide their internet banking login credentials.

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



Screenshot of SMS received by victims

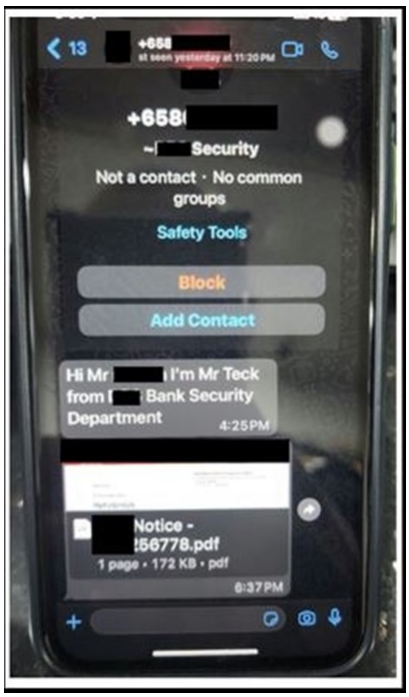
Some Precautionary Measures:

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 check with official sources (e.g. visit www.scamalert.sg or call the Anti-Scam Helpline on 1800-722-6688).

Banks will never send you clickable links via SMS. Look out for tell-tale signs of a phishing website and never disclose your personal or banking credentials, including OTPs to anyone, even one claiming to be a bank officer!

TELL – Authorities, family, and friends about scams. Report any fraudulent transactions to your bank immediately.



Screenshot of WhatsApp message impersonating bank staff

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

2024 – 2 号刊 2024年1月12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

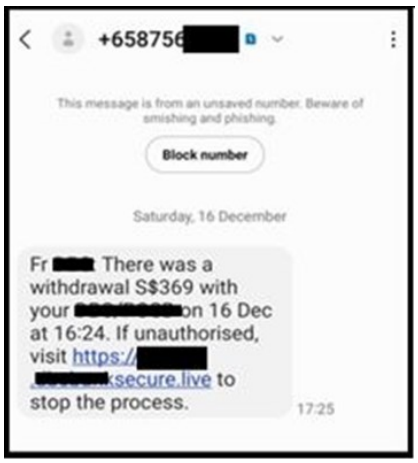
电子商务骗局
（各种手法）

钓鱼骗局

银行不会通过短信发送可点击的链接！

诈骗手法

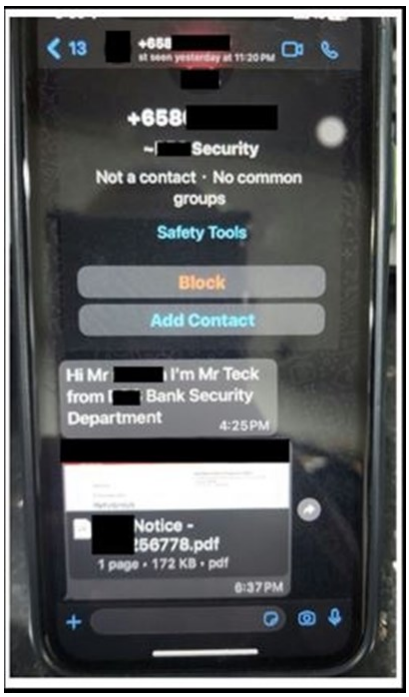
骗子会冒充银行通过短信或WhatsApp联系受害者，利用钓鱼手法获取受害者的网上银行用户名、密码和一次性密码。这些信息警告受害者可能有人试图未经授权进入他们的银行账户，并敦促受害者立即采取行动，点击信息内的网站链接以验证他们的身份并停止交易。



害者和骗子对话的截图

点击链接后，受害者将被引导至一个虚假的银行网站，以提供他们的网上银行登录凭证。

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。



冒充银行工作人员的WhatsApp信息截图

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)。

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)。

银行不会通过短信发送可点击的链接。留意钓鱼网站的迹象。即使对方声称是银行职员也千万不要向任何人透露您的个人或银行凭证，包括你的一次性密码！

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。

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. 2 12 Jan 2024

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

Bank tidak akan menghantar pautan yang boleh diklik melalui SMS!

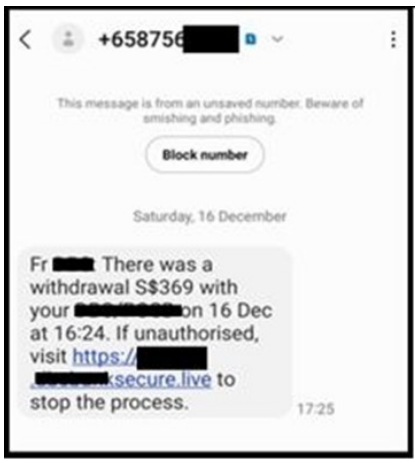
Taktik Penipuan

Penipu menyamar sebagai pihak bank, mendekati mangsa melalui SMS atau WhatsApp untuk memancing data nama pengguna, kata laluan dan Kata Laluan Guna Sekali (OTP) perbankan dalam talian pihak mangsa.

Pesanan tersebut memberi amaran kepada mangsa akan kemungkinan percubaan tanpa kebenaran untuk mengakses akaun bank mereka, menggesa mangsa supaya bertindak segera dengan mengklik pada pautan URL yang termuat di situ untuk memberi pengesahan identiti mereka dan menghentikan transaksi tersebut.

Sebaik sahaja mengklik pada pautan tersebut, mangsa akan diarahkan ke laman web bank yang palsu, untuk memberikan butiran log masuk perbankan internet mereka.

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



Tangkap layar SMS yang diterima mangsa

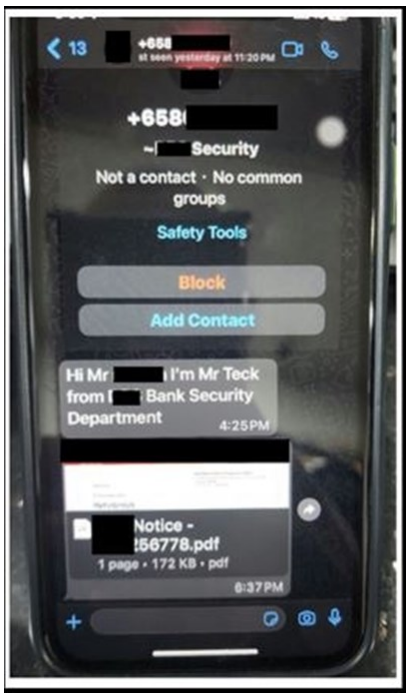
Beberapa langkah berjaga-jaga:

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).

PERIKSA – tanda-tanda penipuan dan dengan sumber-sumber rasmi (boleh layari www.scamalert.sg atau telefon Talian Bantuan Antipenipuan di 1800-722-6688,).

Pihak bank tidak akan sekali-kali menghantar pautan yang boleh diklik melalui SMS kepada anda. Perhatikan tanda-tanda nyata sebuah laman web pancingan data dan jangan sekali-kali mendedahkan butiran peribadi dan perbankan anda, termasuklah OTP kepada sesiapa pun, walaupun kepada seseorang yang mengaku dirinya seorang pegawai bank!

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan sebarang transaksi menipu kepada bank anda dengan segera.



Tangkap layar pesanan WhatsApp yang menyamar sebagai kakitangan bank

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

2024 – வெளியீடு எண். 2

12 ஜனவரி 2024

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

வங்கிகள் உங்களுக்கு குறுஞ்செய்தி மூலம் கிளிக் செய்யக்கூடிய இணைப்புகளை ஒருபோதும் அனுப்பாது!

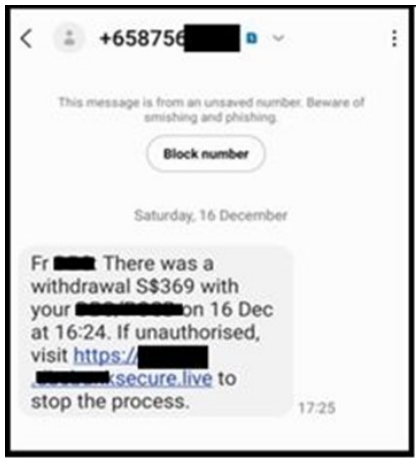
மோசடி உத்திகள்

பாதிக்கப்பட்டவர்களின் இணைய வங்கிப் பயனர் பெயர்கள், கடவுச் சொற்கள், ஒரு முறை கடவுச் சொற்கள் (ஓடிபி) ஆகியவற்றுக்கு குறுஞ்செய்தி மூலமாகவோ வாட்ஸ்ஆப் மூலமாகவோ பாதிக்கப்பட்டவர்களைத் தொடர்புகொண்டு மோசடி செய்பவர்கள் வங்கி அதிகாரிகளைப் போல ஆள்மாறாட்டம் செய்வார்கள்.

இந்தச் செய்திகள் பாதிக்கப்பட்டவர்களின் வங்கி கணக்கை அணுகும் அங்கீகரிக்கப்படாத முயற்சிகள் குறித்து எச்சரிக்கும். அவர்களின் அடையாளத்தைச் சரிபார்க்கவும் பரிவர்த்தனைகளை நிறுத்தவும் செய்தியில் உள்ள இணைய முகவரி இணைப்புகளைக் கிளிக் செய்து உடனடியாக செயல்படுமாறு பாதிக்கப்பட்டவர்கள் வலியுறுத்தப்படுவார்கள்.

இணைப்பை கிளிக் செய்தவுடன், பாதிக்கப்பட்டவர்கள் ஒரு போலி வங்கி இணையத்தளத்தில் தங்கள் இணைய வங்கி உள்நுழைவு விவரங்களை வழங்குமாறு கேட்கப்படுவார்கள்.

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



பாதிக்கப்பட்டவர்கள் பெற்ற குறுந்தகவலின் ஸ்கிரீன்ஷாட்

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

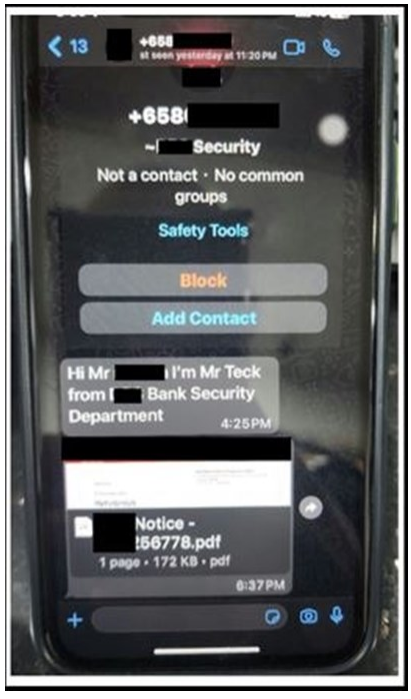
சேர்க்க - ஸ்கேம்ஷீல்டு செயலியைப் பதிவிறக்கம் செய்து, பாதுகாப்பு அம்சங்களை அமைத்திடுங்கள் (எ.கா. வங்கிகளுக்கு இரட்டை மறைச்சொல் முறையையும் (2FA) பன்முக உறுதிப்பாட்டையும் செயல்படுத்தலாம். PayNow உள்ளிட்ட இணைய வங்கிப் பரிவர்த்தனைகளுக்கு வரம்புகளை நிர்ணயிக்கலாம்).

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).

வங்கிகள் உங்களுக்கு குறுஞ்செய்தி வழியாக கிளிக் செய்யக்கூடிய இணைப்புகளை ஒருபோதும் அனுப்பாது. ஒரு தகவல் திருட்டு இணையத்தளம் என்பதற்கான அறிகுறிகள் ஏதேனும் உள்ளனவா என்று சரிபாருங்கள். அவர் ஒரு வங்கி அதிகாரி என்று ஒருவர் கூறினாலும் கூட, ஓடிபி உள்ளிட்ட உங்கள் தனிப்பட்ட அல்லது வங்கி விவரங்களை யாரிடமும் வெளியிடாதீர்கள்!

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள்.

எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உடனடியாக உங்கள் வங்கிக்குத் தெரிவிக்கவும்.



வங்கி ஊழியர்கள் அனுப்பியதாகக் கூறப்படும் வாட்ஸ்ஆப் செய்தியின் ஸ்கிரீன்ஷாட்

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