Issue 36 24 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

Investment Scam

Fake Friend Call Scam

E-Commerce Scam (Variants)

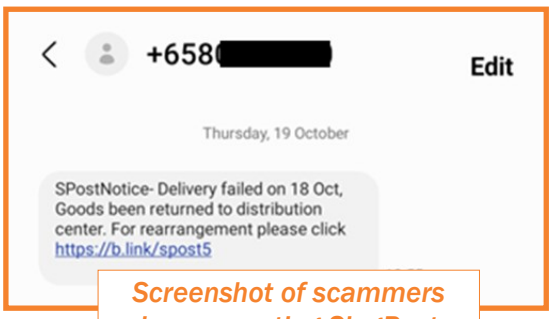
Parcel on the way? Don't be quick to click the link! Beware of parcel delivery phishing scams.

Scam Tactics

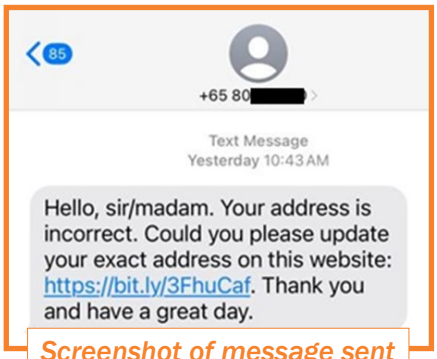
Victims would receive a text message/email from scammers impersonating postage and/or eCommerce logistics companies such as SingPost. The text message/email would request for additional payment to facilitate the delivery of their purchased items and contain a phishing link.

Upon clicking the phishing link, victims would be led to a fake website to make payment and key in their personal, banking/credit card information. With this information, the scammers would conduct unauthorized transactions.

Victims would realise they were scammed after discovering unauthorised transactions were made from their bank accounts or credit cards.



Screenshot of scammers impersonating SingPost



Screenshot of message sent by scammers

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).

Delivery charges are usually paid upfront when purchases are made. Always verify the authenticity of the information with the official website or sources, even if you are expecting the delivery of a parcel and do not click on links provided in unsolicited messages or emails.

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 immediately.

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

36号刊 2023年11月24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

投资诈骗

假朋友来电骗局

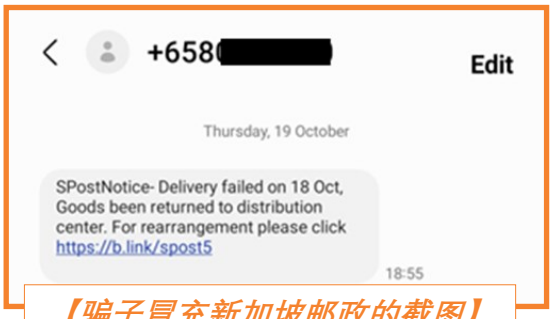
电子商务骗局
(各种手法)

包裹在路上？别急着点击链接! 小心提防包裹运送钓鱼诈骗。

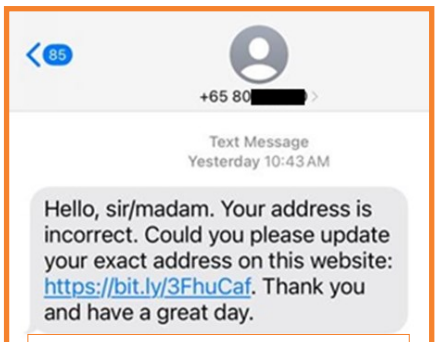
诈骗手法

受害者会收到骗子冒充例如新加坡邮政的邮政和/或电商物流公司发送的短信或电邮。该短信或电邮要求受害者支付额外费用以运送所购买的物品。短信或电邮会包含钓鱼链接。

点击钓鱼链接后，受害者将被引导至一个虚假网站输入个人以及银行/信用卡信息进行付款。有了这些信息，骗子会进行未经授权的交易。受害者在发现自己的银行账户或信用卡有未经授权的交易时，意识到自己被骗了。



【骗子冒充新加坡邮政的截图】



【骗子发送的信息截图】

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@www.go.gov.sg/scamshield-bot、拨打反诈骗热线 1800-722-6688 或到游览 www.scamalert.sg)。

运费一般是在购物时提前支付的。即使您的确有包裹在送往您的路上，也务必通过官方网站或来源核实信息的真实性并切勿点击未经请求的短信或电邮内提供的链接。

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)。 立即向银行举报任何欺诈性交易。

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

Isu no. 36 24 Nov 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 Pekerjaan

Penipuan Pelaburan

Penipuan Panggilan Kawan Palsu

Penipuan E-Dagang (Varian penipuan)

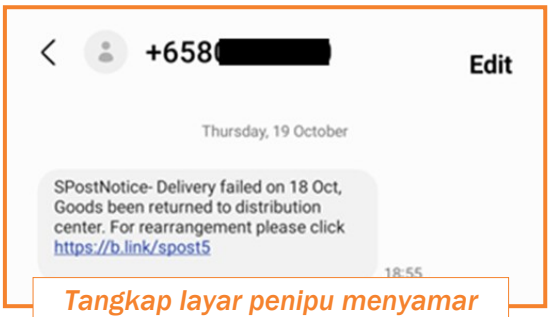
Ada pakej dalam perjalanan? Jangan terlalu cepat untuk klik pautan yang diberi! Berhati-hati dengan penipuan pancingan data penghantaran pakej.

Taktik Penipuan

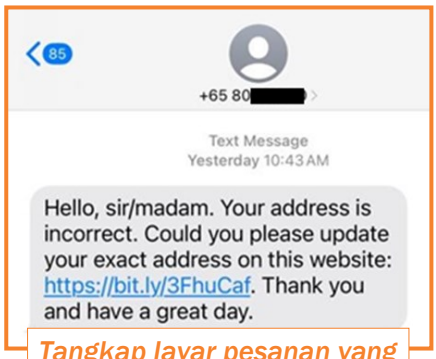
Mangsa akan menerima sebuah pesanan teks/emel daripada penipu yang menyamar sebagai syarikat logistik bayaran pos dan/atau eDagang seperti SingpPost. Pesanan teks/emel tersebut akan meminta bayaran tambahan untuk memudahan penghantaran barangan yang telah dibeli dan mengandungi satu pautan pancingan data.

Sejurus sahaja diklik pautan pancingan data tersebut, mangsa akan dibawa ke satu laman web palsu untuk membuat bayaran dan memasukkan maklumat peribadi, perbankan/kad kredit mereka. Dengan maklumat tersebut, penipu akan melakukan transaksi tanpa kebenaran.

Mangsa akan menyedari bahawa mereka telah ditipu selepas mendapati transaksi tanpa kebenaran telah dibuat daripada akaun bank atau kad kredit mereka.



Tangkap layar penipu menyamar sebagai syarikat SingPost



Tangkap layar pesanan yang dihantar oleh penipu

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).

Bayaran penghantaran selalunya telah dibayar dahulu apabila pembelian dibuat. Pastikan selalu kesahihan maklumat dari laman web atau sumber-sumber rasmi walaupun anda sedang menantikan penghantaran sebuah pakej, dan jangan klik pada pautan yang disediakan dalam pesanan atau emel yang tidak diminta.

BERITAHU – Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Jangan sekali-kali dedahkan butiran peribadi dan perbankan anda, termasuk Kata Laluan Sekali (OTP) kepada sesiapa pun. Laporkan sebarang transaksi menipu kepada bank anda dengan segera.

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

வெளியீடு எண். 36

24 நவம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

சமூக ஊடக ஆள்மாறாட்ட மோசடி

வேலை மோசடி

முதலீட்டு மோசடி

போலி நண்பர் அழைப்பு மோசடி

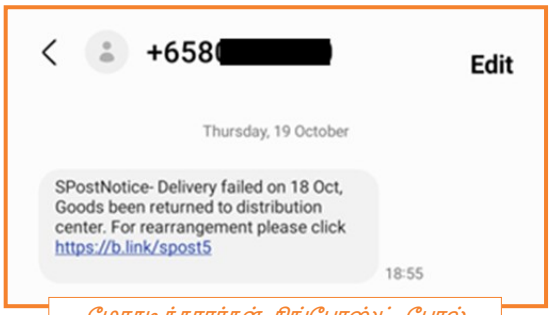
இணைய வர்த்தக மோசடி (பல்வேறு வகைகள்)

பொட்டலம் வந்து கொண்டிருக்கிறதா? அந்த இணைப்பைச் சட்டென அழுத்தாதீர்கள்!

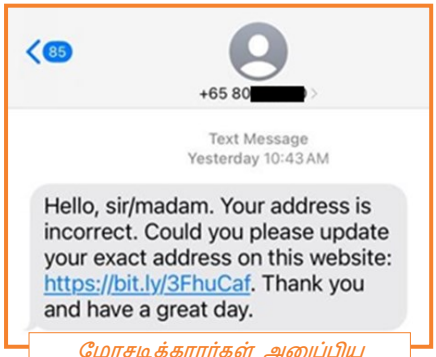
மோசடி உத்திகள்

பாதிக்கப்பட்டவர்களுக்கு சிங்போஸ்ட் போன்ற தபால் மற்றும்/அல்லது இணைய வர்த்தகத் தளவாட நிறுவனங்களைப் போல் பாசாங்கு செய்யும் மோசடிக்காரர்கள் குறுந்தகவல் / மின்னஞ்சல் அனுப்புவார்கள். பாதிக்கப்பட்டவர்கள் வாங்கிய பொருட்களை அவர்களுக்கு அனுப்பி வைக்க கூடுதல் கட்டணம் செலுத்தச் சொல்லும் அந்தக் குறுந்தகவலில் / மின்னஞ்சலில், தகவல் திருடும் இணைப்பு உள்ளடங்கி இருக்கும்.

தகவல் திருடும் இணைப்பை அழுத்தியவுடன், பாதிக்கப்பட்டவர்கள் போலி இணையத்தளத்திற்கு இட்டுச் செல்லப்படுவார்கள். அந்த இணையத்தளத்தில் தங்களது தனிப்பட்ட, வங்கி / கடன் அட்டை விவரங்களை உள்ளிட்டு அவர்கள் கட்டணம் செலுத்துவார்கள். அந்தத் தகவலுடன், மோசடிக்காரர்கள் அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைச் செய்வார்கள்.



மோசடிக்காரர்கள் சிங்போஸ்ட் போல் பாசாங்கு செய்வதைக் காட்டும் திரைக்காட்சி



மோசடிக்காரர்கள் அனுப்பிய தகவலின் திரைக்காட்சி

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 - 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).

பொருட்களை வாங்கும்போதே விநியோகக் கட்டணமும் வழக்கமாகச் செலுத்தப்பட்டுவிடும். நீங்கள் ஒரு பொட்டலத்தின் வருகையை எதிர்பார்த்துக் கொண்டிருந்தாலும், உங்களுக்குக் கிடைத்த தகவல் உண்மையானதுதானா என்பதை அதிகாரபூர்வ இணையத்தளத்தில் அல்லது மூலங்களில் எப்போதும் உறுதி செய்து கொள்ளுங்கள். தாமாக அனுப்பப்படும் தகவல்களில் அல்லது மின்னஞ்சல்களில் உள்ள இணைப்புகளை ஒருபோதும் அழுத்தாதீர்கள்.

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

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