Issue 39 15 Dec 2023

Weekly Scams Bulletin

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

Trending Scams in the past week:

Job Scam

Investment Scam

Social Media Impersonation Scam

E-Commerce Scam (Variants)

Phishing Scam

Fake advertisements for seasonal products on the rise! If the deal is too good to be true, it probably is.

Scam Tactics

Scammers impersonate airlines or travel agencies to post advertisements offering branded suitcases at low prices.

The advertisements lead to a phishing website that requires victims to provide their credentials, such as their name, email address and payment card details, to secure their purchase.

Victims only realised they had been scammed after discovering unauthorised transactions on their card statements.

Examples of fake luggage advertisements found on Facebook

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 @ https://go.gov.sg/scamshield-bot, or call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg).

Be sure to check with the product's official website if such deals are available. Never share your personal information and payment card details with anyone.

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

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

39号刊 2023年12月15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

投资诈骗

社交媒体
冒充他人骗局

电子商务骗局

钓鱼骗局

季节性产品的假广告数量日益剧增!
如果优惠好得难以置信，那很有可能是假的。

诈骗手法

骗子冒充航空公司或旅行社发布广告，以低价提供名牌行李箱。

广告引导受害者至钓鱼网站并要求他们提供如姓名、电邮地址和付款卡信息的凭证以确认订单。

受害者在发现银行卡账单有未经授权的交易时，才意识到自己被骗了。

【脸书假行李广告的列子 】

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)。

务必查看产品的官方网站核实是否有此类优惠。千万不要与任何人分享您的个人信息和付款卡资料。

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. 39

15 Disember 2023

Buletin Penipuan Mingguan

Satu penerbitan oleh Pasukan Polis Singapura dan Majlis Pencegahan Jenayah Kebangsaan

TREND PENIPUAN SEPANJANG MINGGU LEPAS:

Penipuan Pekerjaan

Penipuan Pelaburan

Penipuan Penyamaran di Media Sosial

Penipuan E-Dagang

Penipuan Pancingan Data

Iklan palsu untuk produk bermusim meningkat! Jika harganya terlalu bagus untuk dipercayai, kemungkinan ianya merupakan penipuan.

Taktik Penipuan

Penipu berpura-pura mereka dari syarikat penerbangan atau agensi pelancongan untuk membuat hantaran iklan yang menawarkan bagasi berjenama dengan harga yang murah.

Iklan tersebut membawa mangsa ke satu laman web pancingan data yang memerlukan mangsa untuk memberikan butiran seperti nama, alamat e-mel dan butir-butir kad bayaran mereka, untuk mendapatkan pembelian mereka.

Mangsa hanya akan menyedari mereka telah ditipu setelah mendapati transaksi tanpa kebenaran dibuat di penyata kad mereka.

Contoh iklan bagasi palsu yang terdapat di Facebook.

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 (misalnya periksa dengan bot ScamShield WhatsApp di https://go.gov.sg/scamshield-bot, telefon Talian Bantuan Antipenipuan di 1800-722-6688, atau layari www.scamalert.sg).

Periksa di laman web rasmi produk tersebut untuk memastikan tawaran sedemikian benar-benar wujud. Jangan sekali-kali berkongsi maklumat peribadi dan butir-butir kad bayaran anda dengan sesiapa pun.

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

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

வெளியீடு எண். 39

15 டிசம்பர் 2023

வாராந்திர மோசடிகள்

சிங்கப்பூர் காவல்துறை மற்றும் தேசிய குற்றத் தடுப்பு மன்றம் வெளியிடும் ஓர் வெளியீடு

நம்பமுடியாததாகத் தோன்றினால், அது போலியானதுதான்.

மோசடி உத்திகள்

விமான நிறுவனங்கள் அல்லது பயண நிறுவனங்களைப் போல ஆள்மாறாட்டம் செய்து குறைந்த விலையில் தனிமுத்திரை பயணப் பெட்டிகளின் விளம்பரங்களை மோசடிக்காரர்கள் பதிவிடுவார்கள்.

பாதிக்கப்பட்டவர்கள் பொருளை வாங்குவதற்கு தங்களின் பெயர், மின்னஞ்சல் முகவரி, கட்டண அட்டை விவரங்கள் போன்ற தகவல்களை தகவல் திருட்டு இணையத்தளம் ஒன்றில் வழங்க வேண்டும்.

தங்கள் வங்கி அட்டை அறிக்கைகளில் அங்கீகரிக்கப்படாத பரிவர்த்தனைகளைப் பார்த்த பின்னரே அவர்கள் மோசடி செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.

:பேஸ்புக்கில் போலி பயணப்பெட்டிக்கான விளம்பரங்களின் எடுத்துக்காட்டுகள்

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 @ https://go.gov.sg/scamshield-bot நாடலாம், அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைக்கலாம், அல்லது www.scamalert.sg இணையத்தளத்தை நாடலாம்).

அத்தகைய ஒப்பந்தங்கள் உள்ளதா என்பதை பொருளின் அதிகாரப்பூர்வ இணையத்தளத்தில் சரிபார்க்கவும்.உங்கள் தனிப்பட்ட தகவல்களையும் கட்டண அட்டை விவரங்களையும் யாரிடமும் பகிர வேண்டாம்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். மோசடி பரிவர்த்தனைகளை உங்கள் வங்கியிடம் உடனடியாகத் தெரியப்படுத்துங்கள்.

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

கடந்த வாரத்தின் முன்னணி மோசடிகள்:

வேலை மோசடி

முதலீட்டு மோசடி

சமூக ஊடக ஆள்மாறாட்ட மோசடி

இணைய வர்த்தக மோசடி

தகவல் திருட்டு மோசடி