Issue 07/24

6 December 2024

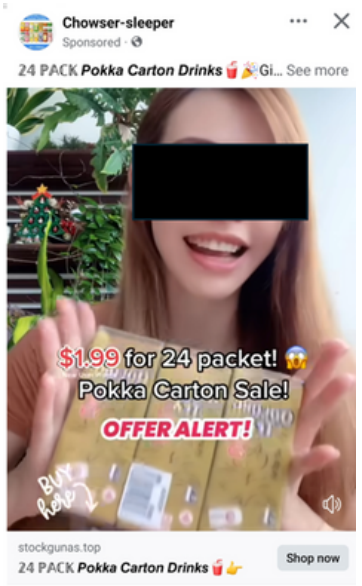
MONTHLY SCAMS BULLETIN

Beware of fake advertisements that trick victims into downloading malware

Scammers post fake advertisements on Facebook and Instagram offering attractive deals for products/services. When victims respond to the advertisement, the 'seller' requests screensharing to guide victims to:

- Disable anti-malware protection;
- Download apps outside of the official app store to make payment or delivery arrangements.

These apps contain malware and allows scammers access and control of victims' devices.



Be careful when using payment methods like bank transfers, gift cards, or cryptocurrency. These are preferred by scammers and do not protect you as the buyer.

- Only download apps from official app stores
- Never share the screens of your devices with others, especially when making money transfers.
- Never disable the security features (e.g., Google Play Protect) of your devices. This leaves your devices vulnerable to malware.
- Regularly update your devices' operating system and applications to ensure that they contain the latest security patches.

If you are unsure if something is a scam, call and check with the ScamShield Helpline at 1799.

1. Switch your device to Flight Mode and turn off your Wi-Fi connection immediately to disconnect from the Internet.
2. Report unauthorised transactions in your bank and/or Singpass.
3. Lodge a police report at any Neighbourhood Police Centre or online.

You are advised not to do a factory reset before reporting the incident to the police as this could hinder investigations.

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

诈骗月刊

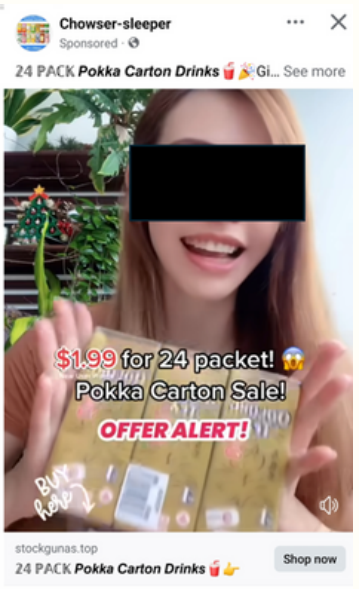
警惕诱导受害者下载恶意软件的假广告

骗子在脸书和 Instagram 上发布虚假广告，提供诱人的产品或服务优惠。当受害者回应广告时，“卖家”会要求屏幕共享以指导受害者做出以下动作：

⚠ 关闭反恶意软件保护;

⚠ 从非官方应用商店下载应用程序以完成支付或送货安排。

这些应用程序含有恶意软件并允许骗子进入以及控制受害者的设备。



请在使用例如银行转账、礼品卡或加密货币的支付方式时多加谨慎。
这些骗子偏爱的支付方式对买家权益毫无保障。

- 只从官方应用程序商店下载应用程序
- 尤其是进行转账时切勿将设备屏幕共享给他人。
- 切勿关闭设备的安全功能（例如 Google Play保护机制)。这会使您的设备容易受到恶意软件的攻击。
- 定期更新设备的操作系统和应用程序以确保它们含有最新的安全补丁。

当您不确定是否是诈骗时，请拨打1799 与ScamShield热线查询。

1. 将手机转为“飞行模式”并关闭无线网络以断开与互联网的连接。
2. 举报银行和/或Singpass账户里未经授权的交易。
3. 在线上或到邻里警局报案。

在向警方报案前，
请不要重置设备为出厂设置因为这可能会影响调查进度。

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

Isu 07/24

6 Disember 2024

BULETIN PENIPUAN BULANAN

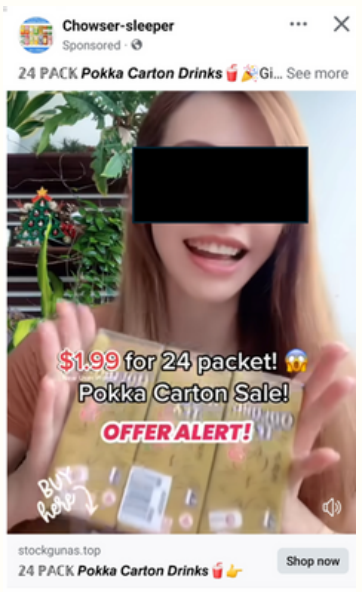
Berhati-hati dengan iklan palsu yang memperdaya mangsa supaya memuat turun perisian hasad

Penipu menyiarkan iklan palsu yang menawarkan tawaran harga menarik untuk produk atau perkhidmatan di Facebook dan Instagram. Mangsa akan menjawab iklan tersebut, dan 'penjual' kemudian akan meminta perkongsian skrin untuk membimbing mangsa untuk:

⚠ Nyahdayakan perlindungan daripada perisian hasad;

⚠ Muat turun aplikasi yang di luar gedung aplikasi rasmi untuk membuat pembayaran atau mengatur perkhidmatan penghantaran.

Aplikasi-aplikasi ini mengandungi perisian hasad dan membolehkan penipu mengakses dan mengawal peranti mangsa.



Berhati-hati apabila menggunakan kaedah pembayaran seperti pemindahan bank, kad hadiah, atau mata wang kripto. Kaedah pembayaran seperti ini diutamakan oleh penipu dan tidak melindungi anda sebagai pembeli.

- Muat turun aplikasi hanya daripada gedung aplikasi rasmi
- Jangan sekali-kali berkongsi skrin peranti anda dengan sesiapa, terutamanya apabila membuat pemindahan wang.
- Jangan sekali-kali nyahdayakan ciri-ciri keselamatan (contohnya, Google Play Protect) bagi peranti anda. Ini akan membiarkan peranti anda terdedah kepada perisian hasad.
- Kemas kini sistem operasi dan aplikasi peranti anda dengan tetap untuk memastikan ia mengandungi patch keselamatan terkini.

Sekiranya anda tidak pasti jika sesuatu itu adalah penipuan, periksa dengan menghubungi Talian Bantuan ScamShield di 1799.

1. Pindahkah telefon anda ke Mod Penerbangan dan segera putuskan sambungan telefon dari internet dengan mematikan Wi-Fi anda.
2. Laporkan transaksi yang tidak dibenarkan dalam akaun bank dan atau Singpass.
3. Buat laporan polis di Pusat Polis Kejiranan atau secara dalam talian.

Anda dinasihatkan supaya tidak membuat tetapan semula kilang peranti anda sebelum melaporkan kejadian itu kepada polis kerana ini boleh menghalang siasatan.

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

வெளியீடு 07 / 24

மாதாந்திர மோசடிகள்

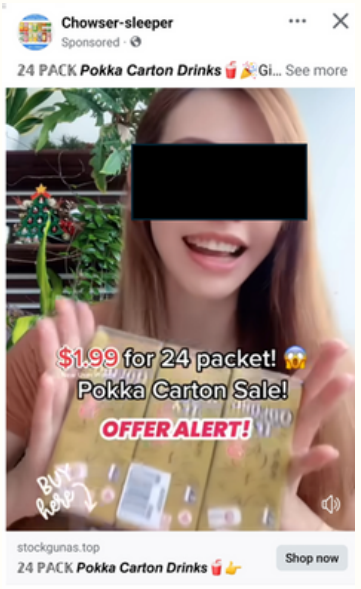
6 மார்கழி 2024

தந்திரமாக நச்சுநிரலைப் பதிவிறக்கம் செய்யவைக்கும் போலி விளம்பரங்களிடம் எச்சரிக்கையாக இருங்கள்

மோசடிக்காரர்கள் சலுகை விலையில் பொருட்கள்/சேவைகள் வழங்குவதாக ஃபேஸ்புக், இன்ஸ்டாகிராம் வலைத்தளங்களில் போலி விளம்பரங்களை வெளியிடுவார்கள். அந்த விளம்பரங்களைப் பார்த்துவிட்டுத் தொடர்பு கொள்வோரிடம், காட்சித்திரையைப் பகிரும்படி "விற்பனையாளர்" கேட்டுக் கொள்வார். அதன்பின்:

- நச்சுநிரல் தடுப்பை நீக்கச் சொல்லி வழிகாட்டுவார்;
- அதோடு, பணம் செலுத்துவதற்காக அல்லது வீட்டுக்கு அனுப்பிவைக்க ஏற்பாடு செய்வதற்காக, அதிகாரபூர்வ செயலி விநியோகத் தளங்களுக்கு வெளியிலிருந்து செயலிகளைப் பதிவிறக்கம் செய்யச் சொல்வார்.

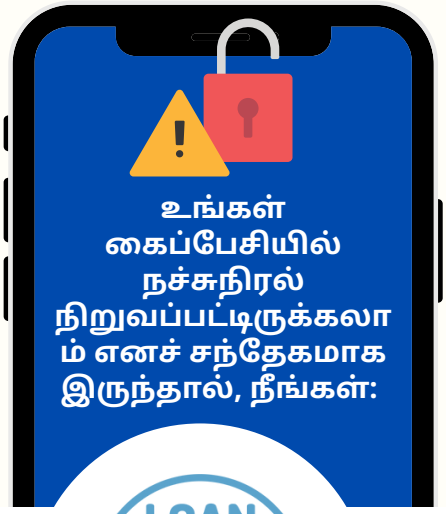
இந்தச் செயலிகளில் இருக்கும் நச்சுநிரல், பாதிக்கப்பட்டவர்களின் கைப்பேசிகளை மோசடிக்காரர்கள் தங்கள் கட்டுப்பாட்டின்கீழ் வைத்திருப்பதற்குப் பயன்படும்.



வங்கிப் பணமாற்று, அன்பளிப்பு அட்டைகள் அல்லது கிரிப்டோகரன்சி போன்ற பணம் செலுத்தும் முறைகளைப் பயன்படுத்தும்போது கவனமாக இருங்கள். இத்தகைய பணம் செலுத்தும் முறைகளைய மோசடிக்காரர்கள் விரும்புவார்கள். இவை பணம் செலுத்துவோருக்கு எந்தவிதப் பாதுகாப்பும் அளிப்பதில்லை.

- அதிகாரபூர்வ செயலி விநியோகத் தளங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள்
- உங்கள் கைப்பேசிகளின் திரைகளை மற்றவர்களுடன் பகிர வேண்டாம், குறிப்பாக பணப் பரிமாற்றம் செய்யும் போது.
- உங்கள் கைப்பேசிகளின் பாதுகாப்பு அம்சங்களை (எ.கா. கூகல் பிளே ப்ரோடெக்ட்) ஒருபோதும் நீக்காதீர்கள். இந்தப் பாதுகாப்பு நீக்கப்பட்டால், உங்கள் கைப்பேசிகள் நச்சுநிரலால் பாதிக்கப்படலாம்.
- உங்கள் கைப்பேசிகளின் இயங்குமுறையிலும் செயலிகளிலும் அண்மைப் பாதுகாப்பு அம்சங்களைச் செயல்படுத்த, வழக்கமான முறையில் புதுப்பித்திடுங்கள்.

நீங்கள் எதையேனும் மோசடி எனச் சந்தேகித்தால், ScamShield உதவித் தொலைபேசிச் சேவையை 1799 என்ற எண்ணை அழைத்து உறுதிப்படுத்திக் கொள்ளுங்கள்.



1. இணையத் தொடர்பைத் துண்டிக்க, உடனடியாக உங்கள் கைப்பேசியை விமானப்பயண இயக்கத்திற்கு (Flight Mode) மாற்றிவிட்டு, அருகலை (Wi-Fi) இணைப்பை அடைத்துவிடுங்கள்.
2. உங்கள் பரிவர்த்தனைகளை உங்கள் வங்கி மற்றும்/அல்லது சிங்பாஸ்க்கு தெரிவிக்கவும்.
3. ஏதாவதொரு அக்கம்பக்கக் காவல் நிலையத்தில் அல்லது இணையம்வழி காவல்துறையிடம் புகார் செய்யுங்கள்.

காவல்துறையிடம் சம்பவத்தைப் புகார் செய்வதற்குமுன் கைப்பேசியை ஆரம்பநிலைக்கு (factory reset) மாற்றியமைக்காமல் இருப்பது நல்லது. அவ்வாறு செய்வதால் புலனாய்வு பாதிக்கப்படலாம்.

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources