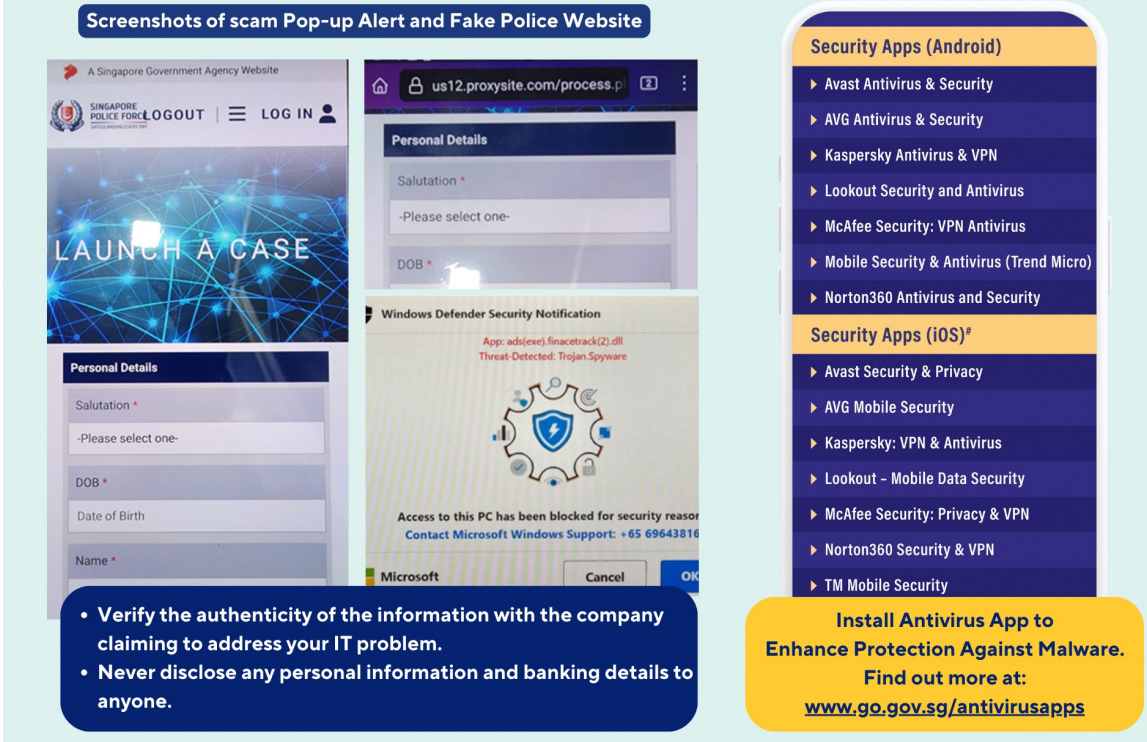
Weekly Scams Bulletin

Received a pop-up notification about your device being attacked? It may be a scam!



Victims receive notification pop-ups on their electronic devices, claiming their devices have been compromised.

These pop-ups contain contact numbers for victims to seek technical support. When victims call the numbers, scammers impersonating Microsoft or Apple technical support staff instruct victims to download software that grants the scammers remote access to their devices.

The call is transferred to another scammer posing as the police, who assists victims in filing a report about the situation via a fake police website. The "police" then directs victims to log into their iBanking accounts or conduct cryptocurrency transactions to aid investigations.

Victims realise they have been scammed when they discover unauthorized transfers or deductions from their bank accounts.

Some Precautionary Measures:

ADD – Anti-virus applications from official app stores to your devices and update it regularly with the latest security patches. Do not install apps or follow computer configuration instructions from unknown callers.

CHECK – Call the Anti-Scam Helpline at 1800-722-6688 to check when you are unsure if a situation you are facing is a scam.

- Verify the authenticity of the information with the company claiming to address your IT problem.
- Never disclose any personal information and banking details to anyone.

TELL – Tell authorities, family, and friends about your scam encounters.

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

诈骗周报

受害者会在电子设备上收到弹出式通知，声称设备已遭入侵。这些弹出式通知包含让受害者寻求技术协助的联系方式。当受害者拨打电话号码时，骗子会冒充微软或苹果的技术人员，指示受害者下载软件好让骗子远程进入他们的设备。

电话之后被转接至假冒警员的骗子。骗子会协助受害者通过虚假警方网站报案。“警察”之后会指示受害者登录他们的网上银行账户或进行加密货币交易以协助调查。此时，骗子会利用受害者早前下载的远程访问软件盗取受害者的银行凭证。

受害者在发现银行账户有未经授权的交易或款项遭扣除时意识到自己被骗了。

一些预防措施：

添加 – 从官方应用程序商店下载防毒应用程序并定期更新最新的安全补丁。切勿遵循未知来电者的指示下载应用程序或更改电脑设置。

查证 – 当您不确定所面临的情况是否是诈骗时，请拨打反诈骗热线 1800-722-6688 查询。

- 向声称解决技术问题的公司验证信息的真实性。
- 切勿向他人透露个人资料及银行资料 。

通报 – 当局、家人和朋友您遭遇的诈骗案件。

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

Buletin Penipuan Mingguan

Mangsa menerima pemberitahuan pop-up pada peranti elektronik mereka. Ia mendakwa peranti mereka telah dikompromi.

Pemberitahuan pop-up tersebut mengandungi nombor telefon untuk mangsa mendapatkan sokongan teknikal. Apabila mangsa menelefon nombor tersebut, penipu yang menyamar sebagai kakitangan sokongan teknikal Microsoft atau Apple mengarahkan mangsa untuk memuat turun perisian yang memberikan penipu akses dari jauh ke peranti mereka.

Panggilan itu dipindahkan kepada penipu lain yang menyamar sebagai polis, yang membantu mangsa dalam memfailkan laporan mengenai situasi itu melalui laman web polis palsu. “Polis” kemudian mengarahkan mangsa untuk log masuk ke dalam akaun iBanking mereka atau melakukan urus niaga mata wang kripto untuk membantu siasatan.

Mangsa akan sedar mereka telah ditipu setelah mereka mendapati pemindahan atau potongan tanpa kebenaran dari akaun bank mereka.

Beberapa langkah berjaga-jaga:

MASUKKAN – Aplikasi antivirus daripada gedung aplikasi rasmi ke peranti anda dan kemas kini ia dengan tetap dengan patch keselamatan terkini. Jangan ikut arahan pemanggil yang tidak dikenali untuk memasang aplikasi atau mengkonfigurasi komputer.

PERIKSA – Hubungi Talian Bantuan Anti-Penipuan di 1800-722-6688 sekiranya anda tidak pasti jika situasi yang sedang anda hadapi ialah satu penipuan.

- Pastikan kesahihan maklumat tersebut dengan syarikat yang mendakwa ia sedang menangani masalah IT anda.
- Jangan sekali-kali mendedahkan sebarang maklumat peribadi dan perbankan anda kepada sesiapa pun.

BERITAHU – Beritahu pihak berkuasa, keluarga, dan kawan-kawan tentang penipuan. Laporkan sebarang komen atau hantaran palsu kepada pentadbir platform dalam talian.

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

வாராந்திர மோசடிகள்

தங்கள் சாதனங்கள் பாதிக்கப்பட்டுள்ளதாகக் கூறி, பாதிக்கப்பட்டவர்கள் தங்கள் மின் சாதனங்களில் அறிவிப்பு பாப் அப்களைப் பெறுவார்கள். இந்த பாப் அப்களில் பாதிக்கப்பட்டவர்கள் தொழில்நுட்ப ஆதரவு நாடுவதற்கான தொடர்பு எண்கள் இருக்கும். பாதிக்கப்பட்டவர்கள் எண்களை அழைக்கும்போது, மைக்ரோசாஃப்ட் அல்லது ஆப்பிள் தொழில்நுட்ப ஆதரவு ஊழியர்களைப் போல ஆள்மாறாட்டம் செய்யும் மோசடிக்காரர்கள், பாதிக்கப்பட்டவர்களின் சாதனங்களுக்கு தொலைதூர அணுகலை வழங்கும் மென்பொருளைப் பதிவிறக்கம் செய்ய மோசடிக்காரர்கள் அறிவுறுத்துவார்கள்.

போலி போலிஸ் இணையத்தளம் மூலம் நிலைமை குறித்து புகார் செய்ய பாதிக்கப்பட்டவர்களுக்கு உதவும் போலிஸ் போல ஆள்மாறாட்டம் செய்யும் மற்றொரு மோசடிக்காரருக்கு இந்த அழைப்பு மாற்றப்படும். விசாரணைகளுக்கு உதவுவதற்காக, "போலிஸ்" பின்னர் பாதிக்கப்பட்டவர்களைத் தங்கள் இணைய வங்கிக் கணக்குள் உள்நுழையவோ அல்லது மெய்நிகர் நாணய பரிவர்த்தனைகளை நடத்தவோ கேட்டுக்கொள்வார்.

இந்த நேரத்தில், பாதிக்கப்பட்டவர்கள் முன்பு பதிவிறக்கம் செய்த தொலைநிலை அணுகல் மென்பொருள் மூலமாக பாதிக்கப்பட்டவர்களின் வங்கி விவரங்களை மோசடிக்காரர்கள் திருடுகின்றனர்.

தங்கள் வங்கி கணக்கில் அங்கீகரிக்கப்படாத பண பரிமாற்றங்கள் அல்லது பணம் கழிக்கப்படுவதைக் கண்டுபிடிக்கும்போது மட்டுமே அவர்கள் மோசடி செய்யப்பட்டுள்ளனர் என்பதை பாதிக்கப்பட்டவர்கள் உணர்வார்கள்.

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - உங்கள் சாதனத்தில் நச்சுநிரல் தடுப்புச் செயலிகளை அதிகாரபூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து மட்டும் பதிவிறக்கம் செய்து, புதிய பாதுகாப்பு அம்சங்களை உடனுக்குடன் சேர்த்திடுங்கள்.செயலிகளை நிறுவவோ அல்லது கணினியின் கட்டமைப்பை மாற்றவோ கேட்கும் அறியப்படாத அழைப்பாளர்களின் வழிமுறைகளைப் பின்பற்றாதீர்கள்.

சரிபார்க்க - நீங்கள் எதிர்நோக்கும் சூழ்நிலை ஒரு மோசடியா என்பது உறுதியாகத் தெரியாவிட்டால், மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைத்து உறுதிப்படுத்திக் கொள்ளவும்.

- உங்கள் தகவல் தொழில்நுட்பப் பிரச்சினையைத் தீர்ப்பதாகக் கூறும் நிறுவனத்துடன் தகவல்களின் உண்மைத்தன்மையைச் சரிபார்க்கவும்.
- தனிப்பட்ட தகவல்கள், வங்கி விவரங்கள் ஆகியவற்றை யாரிடமும் வெளியிடாதீர்கள்

சொல்ல - நீங்கள் மோசடிகளை எதிர்கொண்டால், அதைப் பற்றி அதிகாரிகள், குடும்பத்தார், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள்.

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