TRENDING SCAMS IN THE PAST WEEK

Issue no. 08
12 May 2023

Scams to look out for

Phishing Scam through Malware*

You come across a deal for a product or service online. To facilitate payment, you are asked to click on a link and download an application from an unknown source.

ADD ScamShield app on mobile phone to block scam calls and filter scam SMSes. Only download and install applications from official application stores (i.e., Apple Store or Google Play Store).

Fake Friend Call Scam

You receive a phone call from a "friend". You are asked to guess the caller's name. You are then asked to save their new number. A few days later, you are asked to provide financial assistance.

CHECK with your friend through other means or call their original numbers to verify if they were the ones who had called you earlier.

Investment Scam

You are offered an investment with very high returns.

CHECK with official sources, such as the company's official website, to verify the deal. Do not be enticed by the initial positive gains. Do your own due diligence before you invest large sums of money.

E-Commerce/ Property Rental Scam involving Impersonation of Property Agents*

You see a deal online for a property rental on various advertisement sites like Facebook or Carousell, and the agent asked for payment (deposit) even before physical viewing of the property.

CHECK the agent's advertised phone number in the property listing on CEA's Public Register. If the phone number is not registered with CEA, it is likely a scam! Do not transfer money without first viewing the property.

E-Commerce/ Concert Tickets Scam*

You see third-party resellers on online platforms offering the sale of concert tickets. The tickets are usually sold out or in very limited quantities from the authorised seller. If the deal is too good to be true, it is likely a Scam!

CHECK the Transaction Safety Rating (TSR) for platform ratings at https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings and availability of critical anti-scam safety features on the platform when transacting online.

**This scam is new to the top 5 as compared to the previous week.*

Dangers of downloading applications from third party or dubious sites

Scam Tactics

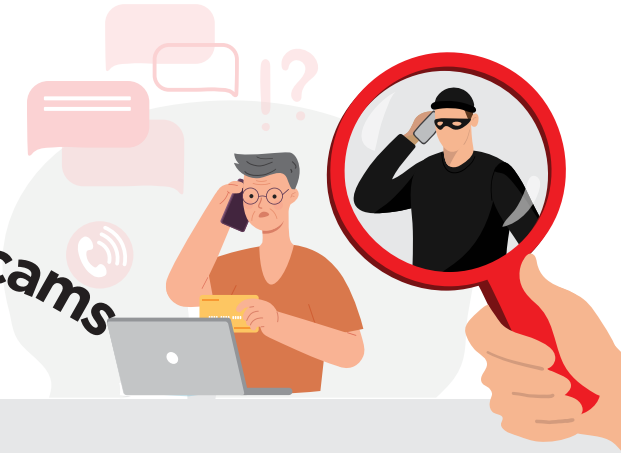
• Downloading applications from third party or dubious sites can lead to malware installed into your devices such as your mobile phones and computers.

• Malware may expose the users' devices to risks including theft of confidential and sensitive data stored in infected devices such as banking credentials, stored credit card numbers and social media account credentials. The attacker will then use these information to perform fraudulent financial transactions or even gain unauthorised access to users' social media accounts to run impersonation scams.

- **Only download and install applications from official application stores (e.g. Apple Store or Google Play Store). Check the application's developer information, number of downloads and user reviews to ensure its legitimacy. Disable "Install Unknown App" or "Unknown Sources" in your device's settings.**
- **Do not grant permission to pop-ups that request for access to your device's hardware or data.**
- **Ensure your devices are installed with updated anti-virus / anti-malware applications that can detect and remove malware. Update your devices' operating systems and applications regularly with the latest security patches.**
- **Do not "jail break" your devices. It's like disabling the brakes on your car. This is dangerous and will make your devices vulnerable to viruses and malwares.**
- **If you suspect that your mobile device may have been exposed to malware infection, turn it to 'flight mode' and perform an anti-virus/ anti-malware scan. Uninstall any unknown applications that are found affected immediately.**

How to protect yourself

I Can ACT Against Scams



Remember to Add, Check and **Tell** (ACT) before making any decisions. And never respond to urgent requests for information or money. Always verify such requests with official websites or sources.

Get the latest advice. Visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

Report scams. Call the Police Hotline at 1800-255-0000 or submit information online at www.police.gov.sg/iwitness. All information will be kept strictly confidential.

Download the free ScamShield app

Detect, block and report scams with the ScamShield app.

GET IT ON Google Play | Download on the App Store

A crime prevention initiative by

NATIONAL CRIME PREVENTION COUNCIL

In collaboration with

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

过去一周
诈骗趋势

八号刊
2023年5月12日

当心骗局

利用恶意软件的钓鱼诈骗*

您在网上看到产品或服务的广告。为方便付款，您被要求点击一个链接并从一个未知来源下载一个应用程序。

在您的手机里下载ScamShield 应用，以拦截诈骗电话和过滤诈骗短信。只从官方应用程序商店（即Apple Store或Google Play Store）下载和安装应用程序。

请参阅第2页以便了解如何更好保护您免受此类诈骗。

假朋友来电

您接到来自“朋友”的电话。来电者要求您猜他的姓名。然后要求您保存他们的新电话号码。几天后，要求您提供经济援助。

通过其他沟通管道或原来的电话号码与您的朋友核实是否打电话给您。

电子商务/租房诈骗*

您在脸书或Carousell 等不同广告网站上看到租房广告，房地产经纪要求在实际看房之前预付押金。

查询该房地产经纪在房地产代理理事会(CEA)公共名册上的公开电话号码。如果电话号码没有在房地产代理理事会公共名册里，那可能是个骗局！在没有看房之前，切勿转账。

投资诈骗

您收到了一项回报率非常高的投资机会。

查看官方消息，如公司的官方网站，以核实这笔交易。不要被初期的利润诱惑。在投入大笔资金前，请务必多加查证。

电子商务/演唱会门票骗局*

您看到第三方转售商在网络平台上销售演唱会门票。门票通常已在授权卖家销售一空或数量有限。如果这笔交易好得难以置信，那很有可能是骗局！

在网上进行交易时，浏览https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings查看平台的交易安全评级（TSR）以及平台是否实施重要的反诈骗安全措施。

*本周新加入前五名的诈骗手法。

⚠ 从第三方或可疑网站下载应用程序的危险性

诈骗手法

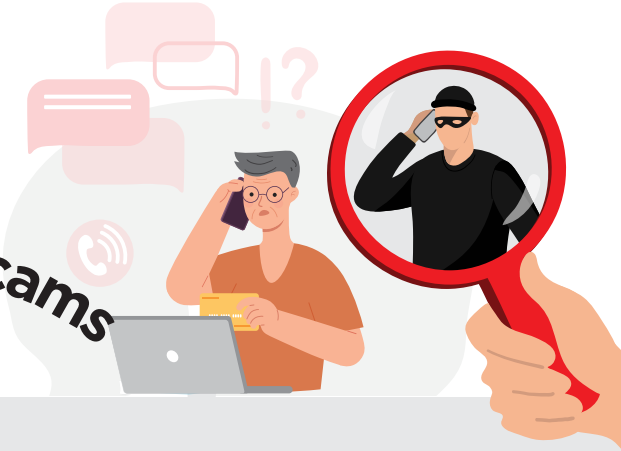
• 从第三方或可疑网站下载应用程序可能会使恶意软件被安装至您的手机、电脑等设备。

• 恶意软件可能导致用户的设备面临各种风险，如让受感染设备中的机密与敏感资料遭窃取。这包括储存在设备里的银行凭证、信用卡号码和社交媒体账号凭证。成功获得资料后，歹徒会利用这些信息进行欺诈性的金融交易，甚至在未经授权的情况下登入用户的社交媒体帐户进行冒充他人骗局。

- 只从官方应用程序商店（例如Apple Store或Google Play Store）下载并安装应用程序。请检查应用程序开发人员信息与下载和用户评论的次数确保它是个正当的应用程序。在设备设置内禁止“安装未知应用程序”或“未知来源”的应用程序。
- 不要授权要求进入设备硬件或数据的弹出式窗口权限。
- 确保您的设备安装了能侦测和删除恶意软件的最新防毒/反恶意软件应用程序。务必定期更新设备的操作系统并确保应用程序受到最新安全补丁的保护。
- 切勿对您的设备进行 "越狱"行为。这犹如使您汽车的刹车器失灵。这是危险的行为并会使您的设备容易受到病毒和恶意软件的攻击。
- 如果您怀疑您的移动设备可能已经受到恶意软件的感染，请将设备转为“飞行模式”，并进行防毒/反恶意软件扫描。立即卸载被发现受的未知应用程序。

⚠ 如何保护自己

I Can ACT Against Scams



在做任何决定前，请谨记下载、查看和告知(ACT)。
千万别回复紧急的信息或金钱要求。
时刻与官方网站或可靠的管道核实此类请求。

上网www.scamalert.sg或拨打反诈骗热线1800-722-6688，获取最新的防范骗案信息。

通报诈骗。拨打警方热线1800-255-0000或上网www.police.gov.sg/iwitness向警方提供诈骗线索。所有资料都将保密。

下载免费的防诈骗应用ScamShield
使用ScamShield应用以侦测，阻止及通报诈骗。

GET IT ON Google Play　Download on the App Store

防范罪案咨询由 NATIONAL CRIME PREVENTION COUNCIL 以及 SINGAPORE POLICE FORCE SAFEGUARDING EVERY DAY 协力带给您

TREND PENIPUAN SEPANJANG MINGGU LEPAS

Isu no.08
12 Mei 2023

Penipuan yang harus diawasi

Penipuan Pancingan Data Melalui Perisian Hasad*

Anda ternampak satu tawaran untuk sebuah produk atau khidmat dalam talian. Untuk memudahkan pembayaran, anda diminta supaya mengklik satu pautan dan memuat turun satu aplikasi dari sumber yang tidak diketahui.

MASUKKAN aplikasi ScamShield ke telefon bimbit anda untuk menyekat panggilan penipuan dan menapis SMS penipuan. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play). Lihat halaman dua untuk butir-butir lanjut bagaimana anda boleh melindungi diri anda dengan lebih baik daripada jenis penipuan ini.

Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada seorang "kawan". Anda diminta supaya meneka nama si pemanggil. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, anda diminta supaya memberi bantuan kewangan.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asal kawan anda untuk memastikan mereka benar-benar telah menelefon anda tadinya.

Penipuan Pelaburan

Anda ditawarkan satu pelaburan dengan pulangan yang sangat tinggi.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran tersebut. Jangan tertarik dengan keuntungan awal yang positif. Lakukan pemeriksaan yang teliti dan wajar sebelum anda melaburkan wang dengan jumlah yang besar.

E-Dagang / Penipuan Sewaan Hartanah melibatkan Penyamaran Ejen Hartanah*

Anda ternampak satu tawaran dalam talian berkenaan sewaan hartanah di pelbagai laman web iklan seperti Facebook dan Carousell, dan pihak ejen meminta bayaran (wang cengkeram) sebelum melihat secara fizikal hartanah tersebut.

PERIKSA nombor telefon ejen yang diiklankan di Daftar Awam CEA. Jika nombor telefon tersebut tidak berdaftar dengan CEA, kemungkinan ianya merupakan penipuan! Jangan pindahkan wang tanpa terlebih dahulu melihat hartanah tersebut.

E-Dagang/ Penipuan Tiket Konsert*

Anda ternampak penjual pihak ketiga di platform dalam talian yang menawarkan penjualan tiket konsert. Tiket-tiket ini selalunya telah habis terjual atau dalam jumlah yang sangat terhad daripada penjual yang sah. Jika tawaran tersebut terlalu bagus untuk dipercayai, kemungkinan ianya merupakan Penipuan!

PERIKSA Rating Keselamatan Urus Niaga (TSR) untuk rating di platform di https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings dan ketersediaan ciri-ciri keselamatan anti penipuan yang kritikal di platform tersebut apabila berurus niaga dalam talian.

**Penipuan ini adalah yang baharu untuk 5 teratas berbanding dengan minggu sebelumnya.*

Bahaya memuat turun aplikasi daripada pihak ketiga atau laman web yang meragukan

Taktik Penipuan

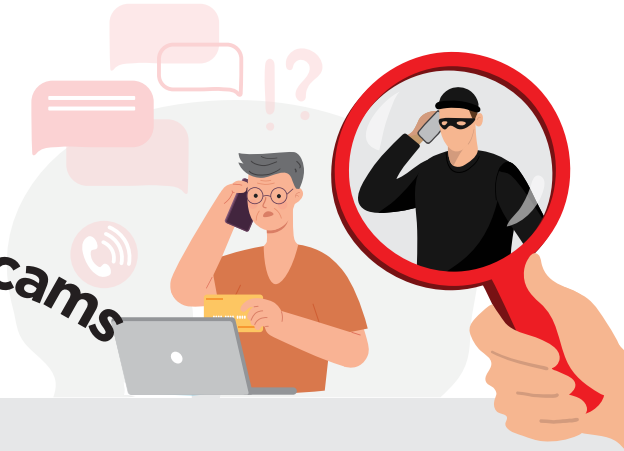
• Memuat turun aplikasi daripada pihak ketiga atau laman-laman web yang meragukan boleh membawa kepada terpasangnya perisian hasad di dalam peranti anda seperti telefon bimbit dan komputer anda.

• Perisian hasad boleh mendedahkan peranti pengguna kepada risiko-risiko termasuklah pencurian data rahsia dan sensitif yang tersimpan di dalam peranti-peranti yang dijangkiti seperti kelayakan perbankan, nombor kad kredit yang tersimpan dan kelayakan akaun media sosial. Penyerang tersebut kemudian akan menggunakan maklumat ini untuk melakukan urus niaga kewangan yang menipu atau mendapatkan akses tanpa kebenaran ke dalam akaun media sosial pengguna untuk menjalankan penipuan penyamaran.

- **Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play). Periksa maklumat pemaju aplikasi tersebut, bilangan muat turun dan ulasan pengguna untuk memastikan kesahihannya. Nyahdayakan "Install Unknown App" (Pasang Aplikasi yang Tidak Diketahui) atau "Unknown Sources" (Sumber yang Tidak Diketahui) di dalam tetapan peranti anda.**
- **Jangan beri keizinan kepada pop-up yang meminta akses ke perkakasan atau data peranti anda.**
- **Pastikan peranti anda telah dipasang dengan aplikasi anti virus / anti perisian hasad yang dikemas kini yang boleh mengesan dan menyingkirkan perisian hasad. Kemas kini sistem operasi dan aplikasi peranti anda dengan tetap dengan patch keselamatan yang terkini.**
- **Jangan "jail break" peranti anda. Ia seperti menyahdayakan brek kereta anda. Ini merbahaya dan boleh menyebabkan peranti anda mudah terdedah dengan virus dan perisian hasad.**
- **Jika anda syak peranti mudah alih anda mungkin telah terdedah kepada jangkitan perisian hasad, tukarkan ia ke 'mod penerbangan' dan lakukan satu imbasan anti virus / anti perisian hasad. Nyahpasang dengan segera sebarang aplikasi yang tidak ketahui yang didapati terjejas.**

⚠ Bagaimana melindungi diri anda

I Can ACT Against Scams



Ingatlah untuk Masukkan (Add), Periksa (Check) dan **Beritahu (Tell)** atau ACT sebelum membuat sebarang keputusan.
Dan jangan membalas sebarang permintaan mendesak untuk maklumat atau wang.
Pastikan selalu kesahihan permintaan-permintaan tersebut daripada laman-laman web atau sumber-sumber rasmi.

Dapatkan nasihat terkini. Lawati www.scamalert.sg atau hubungi Talian Bantuan Anti-Penipuan di 1800-722-6688.

Adukan penipuan. Panggil Talian Hotline Polis di 1800-255-0000 atau hantarkan maklumat dalam talian di www.police.gov.sg/iwitness. Semua maklumat akan dirahsiakan sama sekali.

Muat turun aplikasi percuma yang dipanggil ScamShield
Kesan, sekat dan adu penipuan dengan aplikasi ScamShield.

GET IT ON Google Play | Download on the App Store

Sebuah inisiatif pencegahan jenayah oleh
NATIONAL CRIME PREVENTION COUNCIL

Dengan kerjasama
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

கடந்த வாரத்தின் முன்னணி மோசடிகள்

வெளியீடு எண். 08
12 மே 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

தீங்கிழைக்கும் மென்பொருள் மூலம் தகவல் திருட்டு மோசடி*

இணைய தளத்தில் ஒரு நல்ல பொருளையோ சேவையையோ காண்கிறீர்கள்.

கட்டணம் செலுத்துவதை எளிதாக்க, நீங்கள் ஓர் இணைப்பை கிளிக் செய்து அறியப்படாத தளத்திலிருந்து ஒரு விண்ணப்பத்தைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகள் மற்றும் மோசடி எஸ்எம்எஸ்களைத் தடுக்க கைபேசியில் ஸ்கேம்ஷீல்டு செயலியைச் சேர்க்கவும். அதிகாரப்பூர்வ செயலி ஸ்டோர்களில் (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) இருந்து செயலிகளைப் பதிவிறக்கம் செய்யவும்.

இந்த மோசடி வகையிலிருந்து நீங்கள் எவ்வாறு சிறந்த முறையில் பாதுகாக்கப்படலாம் என்பதைக் குறித்த மேல் விவரங்களுக்குப் பக்கம் இரண்டைப் பார்க்கவும்.

போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, நீங்கள் நிதி உதவி வழங்குமாறு கேட்டுக்கொள்ளப்படுகிறீர்கள்.

உங்கள் நண்பர் உங்களை சற்றுமுன் அழைத்திருந்தார்களா என்பதை மற்ற வழிகள் மூலமாகவோ அல்லது அவர்களின் அசல் எண்ணிலோ தொடர்புக்கொண்டு சரிபார்க்கவும்.

முதலீட்டு மோசடி

மிக உயர்ந்த வருவாய்யைக் கொண்ட ஒரு முதலீடு உங்களுக்கு வழங்கப்படுகிறது.

ஒப்பந்தத்தை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். ஆரம்ப ஆதாயங்களைக் கண்டு கவர்ந்துவிடாதீர்கள். நீங்கள் ஒரு பெரியத் தொகையை முதலீடு செய்வதற்கு முன்பு உங்கள் சொந்த சோதனைகளை மேற்கொள்ளுங்கள்.

மின் வணிகம்/ சொத்துச் சந்தை முகவர்களின் ஆள்மாறாட்டம் சம்பந்தப்பட்ட சொத்து வாடகை மோசடி*

ஃபேஸ்புக் அல்லது கேரோசல் போன்ற பல்வேறு விளம்பர தளங்களில் சொத்து வாடகைக்கான ஒரு ஒப்பந்தத்தை நீங்கள் இணையத்தில் பார்க்கிறீர்கள். சொத்தைப் பார்ப்பதற்கு முன்பே முகவர் பணம் (வைப்புத் தொகை) கேட்டார்.

சொத்து பட்டியலிலுள்ள முகவரின் விளம்பரப்படுத்தப்பட்ட தொலைபேசி எண்ணை CEA-வின் பொதுப் பதிவேட்டில் சரிபார்க்கவும். தொலைபேசி எண் CEA-வில் பதிவு செய்யப்படாவிட்டால் அது ஒரு மோசடியாக இருக்கக்கூடும்! சொத்தை முதலில் பார்க்காமல் பணத்தை மாற்றிவிடாதீர்கள்.

மின்வணிகம்/ இசை நிகழ்ச்சி நுழைவுச் சீட்டு மோசடி*

இணைய தளங்களில் மூன்றாம் தரப்பு மறுவிற்பனையாளர்கள் இசை நிகழ்ச்சிக்கான நுழைவுச் சீட்டுகளை விற்பனைக்கு வழங்குவதாக காண்கிறீர்கள். அங்கீகாரம் பெற்ற விற்பனையாளரிடம் வழக்கமாக எல்லா நுழைவுச் சீட்டுகளுமே விற்றுத்தீர்ந்துவிடும் அல்லது குறைந்த அளவில் தான் அவர்களிடம் நுழைவுச் சீட்டுகள் இருக்கும். ஒப்பந்தம் நம்பத்தகாததாக இருந்தால், அது மோசடியாக இருக்கக்கூடும்.

அந்த தளத்தின் பாதுகாப்பு மதிப்பீட்டை (TSR) https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings என்ற தளத்தில் சரிபார்க்கவும். மேலும், இணையம் வழி பரிவர்த்தனை செய்யும் போது மோசடிகளுக்கு எதிரான பாதுகாப்பு அம்சங்கள் உள்ளனவா என்பதையும் சரிபார்க்கவும்.

*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது

மூன்றாம் தரப்பு அல்லது சந்தேகத்திற்குரிய இடங்களிலிருந்து செயலிகளைப் பதிவிறக்கம் செய்வதால் ஏற்படும் ஆபத்துகள்

மோசடி உத்திகள்

• மூன்றாம் தரப்பு அல்லது சந்தேகத்திற்குரிய தளங்களிலிருந்து செயலிகளைப் பதிவிறக்கம் செய்வது உங்கள் கைபேசிகள் மற்றும் கணினிகள் போன்ற சாதனங்களில் தீங்கு விளைவிக்கும் மென்பொருள் நிறுவப்பட வழிவகுக்கும்.

• தீங்கு விளைவிக்கும் மென்பொருள் பயனர்களின் சாதனங்களை வங்கிச் சேவை உள் நுழைவு விவரங்கள், சேமிக்கப்பட்ட கடன்பற்று அட்டை எண்கள் மற்றும் சமூக ஊடக கணக்கு உள் நுழைவு விவரங்கள் போன்ற பாதிக்கப்பட்ட சாதனங்களில் சேமிக்கப்பட்டுள்ள ரகசிய மற்றும் உணர்வுப்பூர்வமான தரவுகளைத் திருடுவது உள்ளிட்ட அபாயங்களுக்கு உட்படுத்தலாம். தாக்குதல்காரர் பின்னர் இந்த தகவல்களைப் பயன்படுத்தி மோசடி நிதி பரிவர்த்தனைகளைச் செய்வார் அல்லது ஆள்மாறாட்ட மோசடிகளை நடத்த பயனர்களின் சமூக ஊடக கணக்குகளுக்குள் செல்ல அங்கீகரிக்கப்படாத நுழைவுரிமையைப் பெறுவார்.

- அதிகாரப்பூர்வ செயலி ஸ்டோர்களில் (எகா ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) இருந்து செயலிகளை மட்டுமே பதிவிறக்கம் செய்து நிறுவவும். செயலியின் மேம்பாட்டாளர் தகவல், பதிவிறக்கங்களின் எண்ணிக்கை மற்றும் பயனர் மதிப்பாய்வுகள் ஆகியவற்றை சரிபார்த்து அதன் நியாயத்தன்மையை உறுதி செய்யவும். உங்கள் சாதனத்தின் அமைப்புகளில் “அறியப்படாத செயலி” அல்லது “ அறியப்படாத தளங்களை” இயங்காது செய்யவும்.

- உங்கள் சாதனத்தின் வன்பொருள் அல்லது தரவை அணுக கோரும் பாப் அப்களுக்கு அனுமதி வழங்க வேண்டாம்.

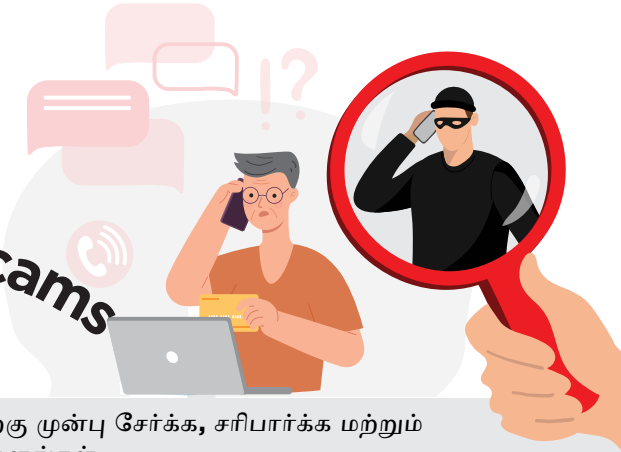
- வைரஸ் தாக்குதல்களிருந்து கணினியைபாதுகாக்கும் புதுப்பிக்கப்பட்ட செயலிகள்/ தீங்கு விளைவிக்கும் மென்பொருள்களைக் கண்டறிந்து அவற்றை அகற்றக்கூடிய மென்பொருள் உங்கள் சாதனங்களில் நிறுவப்படுவதை உறுதி செய்யுங்கள். உங்கள் சாதனங்களின் இயங்குதளங்கள் மற்றும் செயலிகளைச் சமீபத்திய பாதுகாப்பு திட்டுகளுடன் தவறாமல் புதுப்பிக்கவும்.

- உங்கள் சாதனங்களை "ஜெயில் பிரேக்" செய்ய வேண்டாம். இது உங்கள் கார் பிரேக்குகளை இயங்காது செய்வது போன்றது. இது ஆபத்தானது. மற்றும் உங்கள் சாதனங்களை வைரஸ்கள் மற்றும் தீங்கு விளைவிக்கும் மென்பொருள்களால் எளிதில் பாதிக்கப்படும் நிலையை உருவாக்கும்.

- உங்கள் கைப்பேசி சாதனம் தீங்கு விளைவிக்கும் மென்பொருளால் பாதிக்கப்பட்டிருக்கலாம் என்று நீங்கள் சந்தேகித்தால், அதை ‘ ஃப்ளைட் மோடுக்கு ’ திருப்பி, வைரஸ் தாக்குதல்களிருந்து கணினியைப் பாதுகாக்கும் செயலிகள்/ தீங்கு விளைவிக்கும் மென்பொருள்களைக் அகற்றக்கூடிய மென்பொருள் ஆகியவற்றைக் கொண்டு ஸ்கேன் செய்யவும். உடனடியாக பாதிக்கப்பட்ட எந்த அறியப்படாத செயலிகளை அகற்றிவிடவும்.

எப்படி உங்களைப் பாதுகாத்துக்கொள்வது

I Can ACT Against Scams



எந்தவொரு முடிவையும் எடுப்பதற்கு முன்பு சேர்க்க, சரிபார்க்க மற்றும் சொல்ல **(ACT)** நினைவில் கொள்ளுங்கள்.
தகவல் அல்லது பணத்திற்கான அவசர கோரிக்கைகளுக்கு ஒருபோதும் பதிலளிக்காதீர்கள்.
அத்தகைய கோரிக்கைகளை அதிகாரபூர்வ இணையத்தளம் அல்லது ஆதாரங்களுடன் எப்போதும் சரிபார்த்துக்கொள்ளுங்கள்.

ஆக அண்மைய ஆலோசனையைப் பெறுங்கள். www.scamalert.sg இணையத்தளத்தை நாடுங்கள் அல்லது 1800-722-6688 என்ற மோசடி தடுப்பு உதவி எண்ணை அழையுங்கள்.

மோசடிகளை புகார் செய்யுங்கள். 1800-255-0000 என்ற காவல்துறை நேரடித் தொலைபேசி எண்ணை அழையுங்கள் அல்லது www.police.gov.sg/iwitness என்ற இணையதளத்தில் தகவல்களை சமர்ப்பிக்கலாம். அனைத்து தகவல்களும் ரகசியமாக வைத்திருக்கப்படும்.

ஸ்கேம்வீல்ட் செயலியை இலவசமாக பதிவிறக்கம் செய்யுங்கள்.
ஸ்கேம்வீல்ட் செயலியைப் பயன்படுத்தி மோசடிகளைக் கண்டறிந்து, தடுத்து, அவற்றைப் பற்றி புகார் செய்யுங்கள்.

GET IT ON Google Play | Download on the App Store

ஒரு குற்றத் தடுப்பு முன்முயற்சி
NATIONAL CRIME PREVENTION COUNCIL

இணைந்து வழங்குபவர்கள்
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY