TRENDING SCAMS | IN THE PAST WEEK

Issue no. 13
16 June 2023

Scams to look out for

Job Scam

You receive a job offer promising high salary with little effort.

CHECK with official sources, such as the company's official website, to verify the job offer.

Fake Friend Call Scam

You receive a phone call from supposedly your "friend". You are asked to guess the caller's name and when you do so, the caller will assume this name. You are then asked to save the friend's new number. A few days later, this so-called friend will call you to ask for money to help him or her for an emergency, mother is in hospital etc.

CHECK with your friend through other means or call the original number to verify if indeed your friend had called you earlier.

Investment Scam

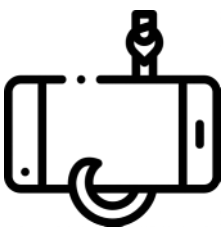
You are offered an investment with very high returns.

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.

Banking-related phishing scam

You receive a SMS claiming that your bank account has been suspended or that payment has been made from a new device. You are asked to click on a link to a fake banking login page that prompts you to provide your iBanking credentials, OTPs, or digital token approvals. Subsequently, unauthorised bank transactions would be made on your bank accounts.

CHECK for scam signs with official sources or websites and contact the banks only using the official contact numbers listed on the banks' official websites or numbers listed at the back of your debit/credit cards. Banks do not send out clickable links in SMSes and emails!



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 detect scam messages and block scam calls. Do not click on links sent via any messaging and/or social media platforms by unknown sources. Only download and install applications from official application stores (i.e., Apple Store or Google Play Store).

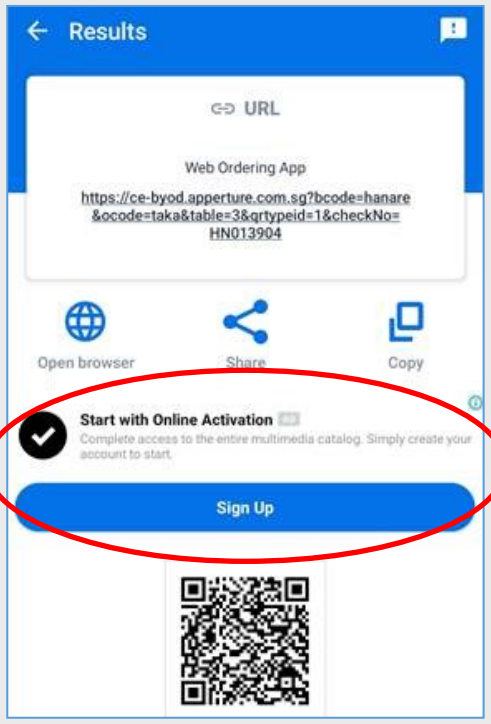
** This scam is new to the top 5 as compared to the previous week.*

⚠ Emerging Scam Trend

Protect Yourself from Malicious QR

QR codes are used by businesses to facilitate digital payments and services. They are not inherently harmful, but scammers could make use of malicious QR codes to trick victims and expose them to threats. These are some common threats involving QR codes:

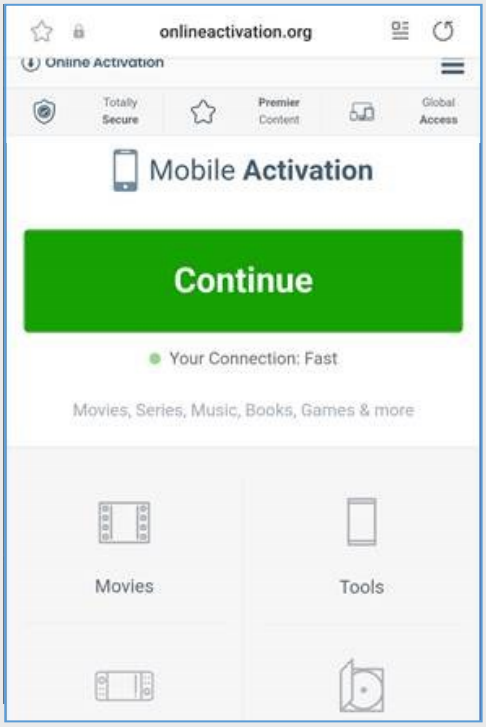
- Phishing – Malicious QR codes are used to redirect victims to phishing websites acting as legitimate ones to steal sensitive information. For example, victims will be redirected to fake banking login sites to key in banking credentials and/or credit card details for payment.
- QR Code Swaps – Legitimate QR codes displayed at businesses are tampered with to trick victims into directing payment to the scammer's bank account instead of the intended recipient.
- Malware Infection – Malicious QR codes can be embedded with links that when scanned and accessed, results in the download and installation of malware onto the victim's device, leading to unauthorised access or data breaches.



[Advertisement banner that prompts victims to create an account]

Some precautionary measures against malicious QR codes:

- Check the source. Avoid scanning codes received via social media messaging platforms and/or from unknown sources.
- Examine physical QR codes for any signs of tampering. If it appears to have been pasted over the original code, do not scan it and check with the company/store.
- After scanning any QR codes, always inspect the website address to ensure that it is the intended URL. Check for misspelt domains or unfamiliar addresses. If suspicious, do not access the website.
- For payments, review the transaction details displayed before confirming payment. Check that the amount, recipient and other information are accurate. If unsure, check with the company/store.
- If scanning the QR code results in requests to download apps, be extra vigilant. Only download and install applications from official application stores *(i.e., Apple Store or Google Play Store)*.



[Phishing website requesting for victim's credit card details]

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

13号刊

2023年6月16日

诈骗趋势

当心骗局

求职诈骗

您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

假朋友来电

您接到来自"朋友"的电话。来电者在要求您猜他的姓名后会使用您所说的名字。来电者会要求您保存朋友的新电话号码。几天后，这所谓的朋友会拨电给您，以紧急事件或母亲住院等为由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。

投资诈骗

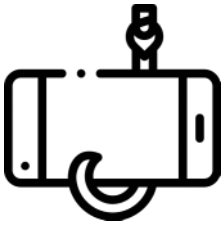
您收到了一项回报率非常高的投资机会。

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。

与银行相关的网络钓鱼诈骗

您收到一则短信，声称您的银行账户已被冻结或已利用新设备付款。您被要求点击一个链接进入虚假的银行登录网页。网页提示您提供网上银行（iBanking）凭证、一次性密码（OTP）或密码生成器的批准。随后，您的银行账户将出现未经授权的银行交易。

查看官方消息或网站并注意诈骗迹象。只使用银行官方网站或借记卡/信用卡背面所列的官方联络号码与银行联系。银行不会在短信和电邮中发送可点击的链接!



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 应用侦测诈骗短信和拦截诈骗电话。请勿点击由未知来源通过任何通讯和/或社交媒体平台发送的链接。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。

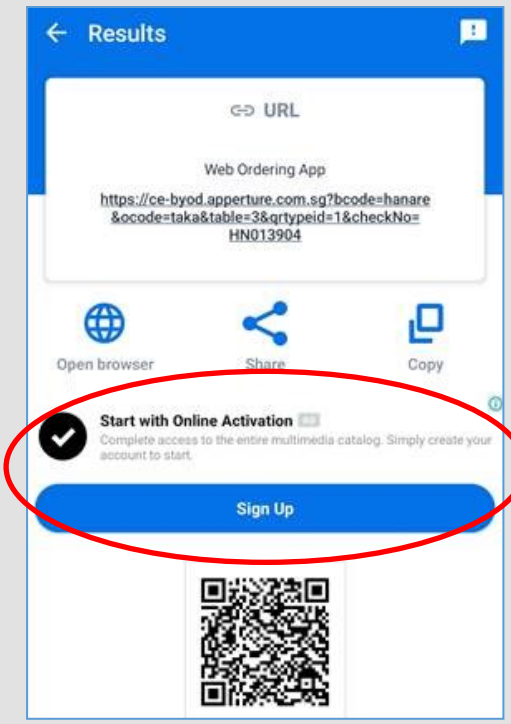
**本周新加入前五名的诈骗手法。*

新兴诈骗趋势

保护自己免受恶意二维码侵害

企业使用二维码提供数码付款和服务。二维码本身并无害，但骗子可以利用恶意二维码欺骗受害者，让他们受到诈骗威胁。以下是一些常见的二维码威胁：

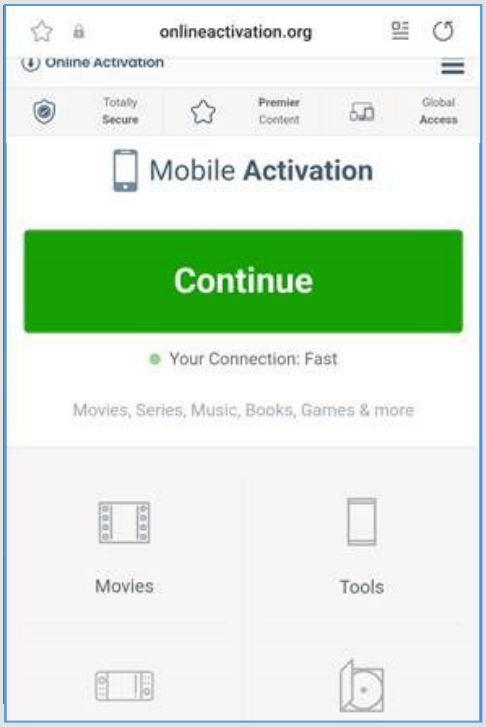
- 钓鱼 - 恶意二维码将受害者转接至伪装成官方网站的钓鱼网站。目的就是为了偷取个人资料。例如：受害者会被转接至假冒的银行登录网站输入银行和/或信用卡资料来付款。
- 偷龙转凤二维码 - 商家展示的正当二维码被篡改，导致受害者直接付款至骗子的银行户头，而不是真正的收款人银行户头。
- 恶意软件感染 - 恶意二维码内或含有恶意软件链接。当扫描和进入这些链接时，恶意软件将被下载并安装在受害者的电子设备。这将导致未经授权的访问或数据泄露。



[提示受害者开设账户的广告]

针对恶意二维码的一些防范措施：

- 查看来源。避免扫描来自社交媒体平台和/或未知来源的二维码。
- 检查实体二维码是否有被篡改的迹象。若原有的二维码看似被其他二维码重叠过的痕迹，别扫描并向公司/商店查询。
- 扫描二维码后，请务必检查网址确保它是您想进入的网址。查看是否有拼写错误或不熟悉的网址。若有可疑之处，请不要进入网站。
- 关于付款，请在确认付款前查看显示的交易详细信息。检查金额，收款人和其他信息是否准确。若不确定，请咨询公司/商店。
- 若在扫描二维码后被要求下载应用程序，请务必格外警惕。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。



[索取受害者信用卡资料的钓鱼网站]

⚠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 | Isu no. 13

16 Jun 2023

SEPANJANG MINGGU LEPAS

Penipuan yang harus diawasi

Penipuan Pekerjaan

Anda menerima satu tawaran pekerjaan yang menjanjikan gaji yang lumayan dengan usaha yang sedikit.

PERIKSA dengan sumber-sumber rasmi, seperti laman web rasmi syarikat tersebut, untuk memastikan kesahihan tawaran pekerjaan tersebut.

Penipuan Panggilan Kawan Palsu

Anda menerima satu panggilan telefon daripada kononnya seorang "kawan". Anda diminta supaya meneka nama si pemanggil dan apabila anda berbuat demikian, pemanggil akan menggunakan nama yang anda teka tersebut. Anda kemudian diminta supaya menyimpan nombor baru si pemanggil tadi. Beberapa hari kemudian, pemanggil yang kononnya kawan anda ini akan menghubungi anda untuk meminta wang bagi menolongnya untuk suatu kecemasan, atau emaknya yang berada di hospital, dan sebagainya.

PERIKSA dengan kawan anda melalui cara lain atau telefon nombor asalnya untuk memastikan dia benar-benar telah menelefon anda tadi.

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.

Penipuan pancingan data berkaitan perbankan

Anda menerima satu SMS yang mendakwa bahawa akaun bank anda telah digantung atau pembayaran telah dibuat daripada satu peranti. Anda diminta supaya mengklik satu pautan halaman log masuk perbankan yang palsu yang meminta anda supaya memberikan butiran iBanking, OTP, atau kelulusan token digital anda. Seterusnya, transaksi bank tanpa kebenaran akan dibuat di akaun bank anda.

PERIKSA tanda-tanda penipuan dengan sumber-sumber atau laman-laman web rasmi dan hubungi pihak bank dengan hanya menggunakan nombor-nombor rasmi yang tersenarai di belakang kad debit/kredit anda. Pihak bank tidak menghantar pautan yang boleh diklik di SMS dan emel!

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. Jangan klik pada pautan yang dihantar melalui mana-mana platform pesanan dan/atau media sosial oleh sumber yang tidak diketahui. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play).

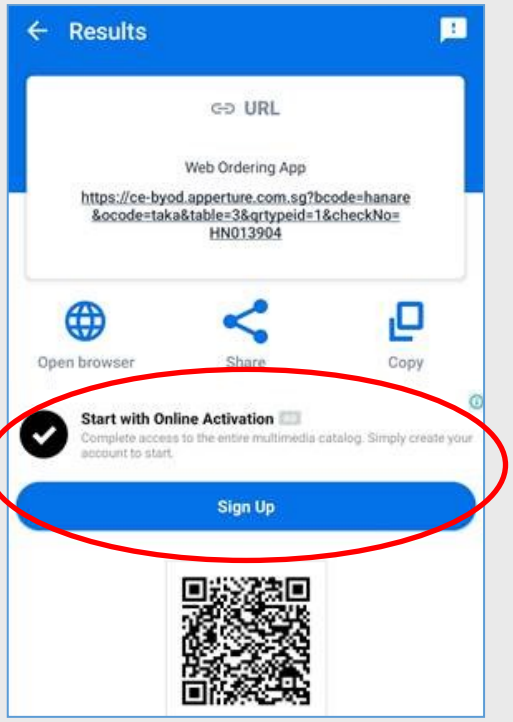
**Penipuan ini adalah yang baharu untuk 5 teratas berbanding dengan minggu sebelumnya.*

⚠ Trend Penipuan yang Baru Muncul

Melindungi diri anda daripada Kod QR Berniat Jahat

Kod QR digunakan oleh banyak perniagaan untuk memudahkan pembayaran dan perkhidmatan digital. Mereka sememangnya tidak berbahaya, tetapi penipu boleh menggunakan kod QR berniat jahat untuk menipu mangsa dan mendedahkan mereka kepada ancaman. Ini adalah beberapa ancaman yang lazim berlaku yang melibatkan kod QR:

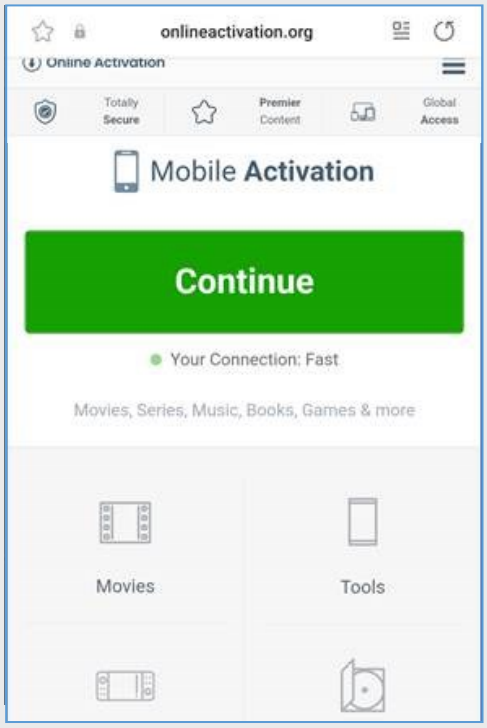
- Pancingan Data – Kod QR berniat jahat digunakan untuk mengarahkan mangsa ke tapak web pancingan data yang menyamar sebagai tapak web yang sah untuk mencuri maklumat sensitif. Sebagai contoh, mangsa akan diarahkan ke tapak log masuk perbankan palsu untuk memasukkan butiran perbankan dan/atau butiran kad kredit untuk pembayaran.
- Pertukaran Kod QR – Kod QR sah yang dipaparkan di perniagaan diusik untuk memperdaya mangsa agar mengarahkan pembayaran ke akaun bank penipu dan bukannya penerima yang ditujukan.
- Jangkitan Perisian Hasad – Kod QR berniat jahat boleh disematkan dengan pautan-pautan yang apabila diimbas dan diakses, akan mengakibatkan perisian hasad dimuat turun dan dipasang pada peranti mangsa, dan ini akan membawa kepada akses tanpa kebenaran atau pelanggaran data.



[Sepanduk iklan yang menggesa mangsa untuk mencipta akaun]

Beberapa langkah berjaga-jaga terhadap kod QR berniat jahat:

- Periksa sumber. Elakkan daripada mengimbas kod yang diterima melalui platform pesanan dan/atau daripada sumber yang tidak diketahui.
- Periksa kod QR fizikal untuk sebarang tanda yang ia telah diusik. Jika ia kelihatan telah ditampal pada kod tulen, jangan imbas dan periksa dengan syarikat/kedai.
- Selepas mengimbas sebarang kod QR, sentiasa periksa alamat tapak web untuk memastikan bahawa ia adalah petunjuk sumber seragam (URL) yang dimaksudkan. Semak domain yang salah eja atau alamat yang tidak dikenali. Jika mencurigakan, jangan akses laman web.
- Untuk pembayaran, semak butiran transaksi yang dipaparkan sebelum mengesahkan pembayaran. Semak sama ada jumlah, penerima dan maklumat lain adalah tepat. Jika tidak pasti, periksa dengan syarikat/kedai.
- Perlu lebih berwaspada jika mengimbas kod QR menyebabkan permintaan untuk memuat turun aplikasi. Muat turun dan pasang aplikasi hanya daripada gedung aplikasi rasmi (misalnya, Gedung Apple atau Gedung Google Play).



[Tapak web pancingan data yang meminta butiran kad kredit mangsa]

⚠ 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. 13

16 ஜூன் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

வேலை மோசடி

நீங்கள் சிறிதும் முயற்சி செய்யாமல், அதிக சம்பளம் வழங்குவதாக உறுதியளிக்கும் ஒரு வேலை வாய்ப்பைப் பெறுகிறீர்கள்.

வேலை வாய்ப்பை சரிபார்க்க, நிறுவனத்தின் அதிகாரப்பூர்வ இணையத்தளம் போன்ற அதிகாரப்பூர்வ ஆதாரங்களுடன் **சரிபார்க்கவும்**.

போலி நண்பர் அழைப்பு மோசடி

உங்களுக்கு ஒரு "நண்பரிடமிருந்து" தொலைபேசி அழைப்பு வருகிறது. அழைப்பவரின் பெயரை யூகிக்க நீங்கள் கேட்கப்படுகிறீர்கள். அவ்வாறு நீங்கள் செய்யும்போது, அழைப்பவர் நீங்கள் குறிப்பிட்ட பெயரை ஏற்றுக்கொள்வார். பின்னர் அவர்களின் புதிய எண்ணைத் தொலைபேசியில் பதிவு செய்துக்கொள்ளும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள். சில நாட்களுக்குப் பிறகு, உங்கள் நண்பர் என்று தன்னை அறிமுகப்படுத்திக் கொண்ட இந்த நபர், அவசர நிலைமைக்கு அவருக்கு உதவ பணம் கேட்டு உங்களை அழைப்பார். ஒரு உதாரணத்திற்கு, அவரது தாயார் மருத்துவமனையில் இருக்கிறார் என்று கூறலாம்.

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.

வங்கி பரிவர்த்தனை தொடர்பான தகவல் திருட்டு மோசடி

உங்கள் வங்கிக் கணக்கு முடக்கப்பட்டுள்ளதாக அல்லது புதிய சாதனத்திலிருந்து பணம் செலுத்தப்பட்டதாகக் கூறும் குறுஞ்செய்தி உங்களுக்குக் கிடைக்கிறது. உங்கள் iBanking விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) அல்லது மின்னிலக்க டோக்கன் ஒப்புதல்களை வழங்க ஒரு போலி வங்கி உள்நுழைவு பக்கத்தின் இணைப்பை கிளிக் செய்யும்படி நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்கள். அதனைத் தொடர்ந்து, அனுமதி அளிக்கப்படாத வங்கி பரிவர்த்தனைகள் உங்கள் வங்கிக் கணக்குகளில் செய்யப்படும்.

மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்கள் அல்லது இணையத்தளங்களுடன் **சரிபார்க்கவும்**. வங்கிகளின் அதிகாரப்பூர்வ இணையத்தளங்களில் பட்டியலிடப்பட்டுள்ள அதிகாரப்பூர்வ தொடர்பு எண்கள் வாயிலாகவோ அல்லது உங்கள் பற்று / கடன்பற்று அட்டைகளின் பின்புறத்தில் பட்டியலிடப்பட்டுள்ள எண்கள் வாயிலாகவோ வங்கிகளை தொடர்பு கொள்ளுங்கள். கிளிக் செய்யக்கூடிய இணைப்புகளை குறுஞ்செய்திகள் மற்றும் மின்னஞ்சல்களில் வங்கிகள் அனுப்புவதில்லை!

தீங்கிழைக்கும் மென்பொருள் மூலம் தகவல் திருட்டு மோசடி*

இணையத்தில் ஒரு நல்ல பொருளையோ சேவையையோ காண்கிறீர்கள். கட்டணம் செலுத்துவதை எளிதாக்க, நீங்கள் ஓர் இணைப்பை கிளிக் செய்து அறியப்படாத தளத்திலிருந்து ஒரு விண்ணப்பத்தைப் பதிவிறக்கம் செய்யும்படி கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகள் மற்றும் மோசடி குறுஞ்செய்திகளைத் தடுக்க கைபேசியில் ஸ்கேம்ஷீல்ட் செயலியைச் **சேர்க்கவும்**. செய்தி அனுப்பும் தளங்கள் அல்லது சமூக ஊடகத் தளங்கள் வழியாக தெரியாதவர்களால் அனுப்பப்படும் எந்தவொரு இணைப்புகளையும் கிளிக் செய்ய வேண்டாம். அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யவும்.

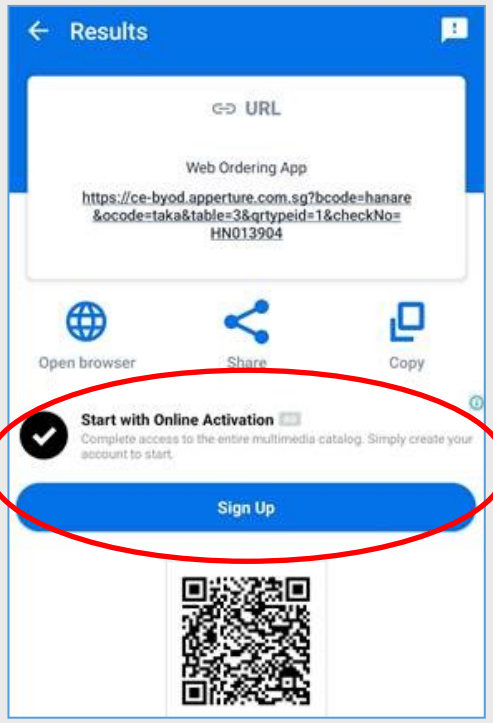
*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது.

வளர்ந்து வரும் மோசடிப் போக்கு

தீங்கிழைக்கும் விரைவுத் தகவல் (QR) குறியீடுகளிலிருந்து உங்களைப் பாதுகாத்துக்கொள்ளுங்கள்

விரைவுத் தகவல் (QR) குறியீடுகள், மின்னிலக்கக் கட்டணமுறைகளையும் சேவைகளையும் எளிதாக்க வர்த்தகங்களால் பயன்படுத்தப்படுகின்றன. அவை தீங்கு விளைவிக்கக்கூடியவை அல்ல, ஆனால் மோசடிக்காரர்கள் தீங்கிழைக்கும் விரைவுத் தகவல் (QR) குறியீடுகளைப் பயன்படுத்தி பாதிக்கப்பட்டவர்களை ஏமாற்றி அச்சுறுத்தல்களுக்கு ஆளாக்கலாம். விரைவுத் தகவல் (QR) குறியீடுகள் சம்பந்தப்பட்ட சில பொதுவான அச்சுறுத்தல்கள் இவை:

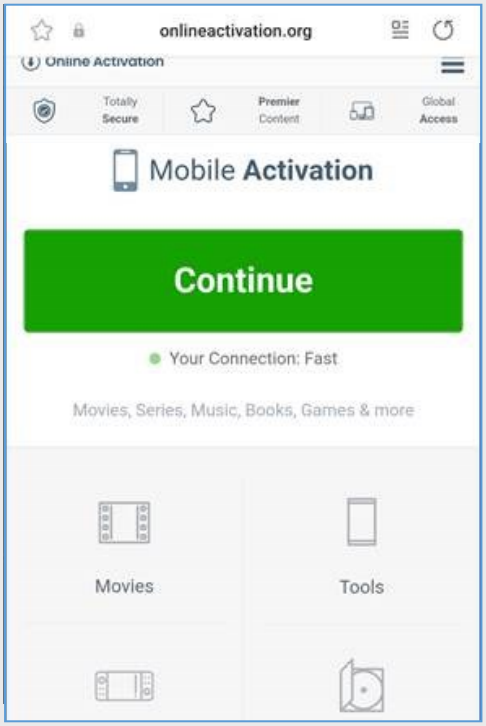
- தகவல் திருட்டு - தீங்கிழைக்கும் விரைவுத் தகவல் (QR) குறியீடுகள், முக்கியமான தகவல்களைத் திருடுவதற்காகச் சட்டபூர்வமானவையாகத் தோன்றும் தகவல் திருட்டு இணையத் தளங்களுக்கு பாதிக்கப்பட்டவர்களை கொண்டு செல்ல பயன்படுத்தப்படுகின்றன.
- விரைவுத் தகவல் (QR) குறியீட்டு மாற்றம் - வியாபாரங்களில் காட்டப்படும் சட்டபூர்வமான விரைவுத் தகவல் (QR) குறியீடுகள் பாதிக்கப்பட்டவர்களை ஏமாற்றுவதற்காக மாற்றப்படுகின்றன. இதனால் அவர்கள் திட்டமிட்ட பெறுநருக்கு பதிலாக மோசடிக்காரரின் வங்கிக் கணக்கிற்கு பணம் செலுத்துவார்கள்.
- தீங்கு விளைவிக்கும் மென்பொருள் தொற்று - தீங்கிழைக்கும் விரைவுத் தகவல் (QR) குறியீடுகளில் இணைப்புகள் பொருத்தப்பட்டிருந்தால், அவற்றை ஸ்கேன் செய்து அணுகும்போது, பாதிக்கப்பட்டவரின் சாதனத்தில் தீங்கு விளைவிக்கும் மென்பொருள் பதிவிறக்கம் செய்யப்பட்டு நிறுவப்படலாம். இது அனுமதிக்கப்படாத அணுகல் அல்லது தரவு மீறல்களுக்கு வழிவகுக்கிறது.



[பாதிக்கப்பட்டோரைக் கணக்கை உருவாக்கத் தூண்டும் விளம்பரம்]

தீங்கிழைக்கும் விரைவுத் தகவல் (QR) குறியீடுகளுக்கு எதிரான சில முன்னெச்சரிக்கை நடவடிக்கைக்கள்:

- விரைவுத் தகவல் (QR) குறியீடு எங்கிருந்து அனுப்பப்படுகிறது என்பதை சரிபார்க்கவும். சமூக ஊடகச் செய்தி அனுப்பும் தளங்கள் மற்றும்/அல்லது அறியப்படாத மூலங்களிலிருந்து பெறப்படும் குறியீடுகளை ஸ்கேன் செய்வதைத் தவிர்க்கவும்.
- விரைவுத் தகவல் (QR) குறியீடுகள் மாற்றப்பட்டதற்கான அறிகுறிகள் ஏதேனும் உள்ளனவா என்று ஆராயவும். அசல் குறியீட்டின் மீது ஒட்டப்பட்டிருப்பதாகத் தோன்றினால், அதை ஸ்கேன் செய்ய வேண்டாம். அந்த நிறுவனம்/கடையுடன் சரிபார்க்கவும்.
- எந்தவொரு விரைவுத் தகவல் (QR) குறியீடுகளையும் ஸ்கேன் செய்த பிறகு, அது சரியான இணையப்பக்க முகவரியா என்பதை உறுதிப்படுத்த எப்போதும் இணையப்பக்க முகவரியைச் சரிபார்க்கவும். எழுத்துப்பிழை உள்ள களங்கள் அல்லது அறிமுகமில்லாத முகவரிகள் உள்ளனவா என்பதைப் பார்க்கவும். உங்களுக்கு சந்தேகம் இருந்தால் இணையத்தளத்தை அணுக வேண்டாம்.
- பணம் செலுத்துவதை உறுதிப்படுத்துவதற்கு முன்பு காட்டப்படும் பரிவர்த்தனை விவரங்களைச் சரிபார்க்கவும். தொகை, பெறுநர் மற்றும் பிற தகவல்கள் துல்லியமாக இருக்கிறதா என்பதை சரிபார்க்கவும். உங்களுக்கு உறுதியாகத் தெரியவில்லை என்றால், நிறுவனம்/கடையுடன் சரிபார்க்கவும்.
- அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களிலிருந்து (அதாவது, ஆப்பிள் ஸ்டோர் அல்லது கூகிள் பிளே ஸ்டோர்) மட்டுமே செயலிகளை பதிவிறக்கம் செய்து நிறுவவும்.



[பாதிக்கப்பட்டவரின் கடன்பற்று அட்டை விவரங்களைக் கோரும் தகவல் திருட்டு இணையத்தளம்]

எப்படி உங்களைப் பாதுகாத்துக்கொள்வது

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.

ஸ்கேம்ஷீல்ட் செயலியை இலவசமாக பதிவிறக்கம் செய்யுங்கள்.
ஸ்கேம்ஷீல்ட் 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