TRENDING SCAMS | IN THE PAST WEEK

Issue no. 21
11 Aug 2023

Scams to look out for

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 takes on the name you guessed. 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 with an emergency, such as a family member hospitalized.

CHECK with your real friend through other means or by calling their original number to verify if they had indeed called you earlier.

Job Scam

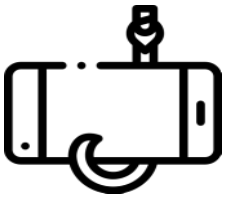
You receive a job offer promising high salary with little effort.

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

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.



Phishing Scam (Calls Impersonating Govt Agencies)

You receive a call from a "government official". You are then asked to provide your banking credentials, OTPs and/or personal details.

ADD ScamShield app only from the official app stores on your mobile phone. ScamShield blocks scam calls and detects scam SMSes from known blacklisted numbers. Do not provide your credentials and OTPs to unknown persons.

Social Media Impersonation Scam *

You receive a message from social media or other communication platforms claiming to be your friend/relative, asking for your assistance for various reasons like joining or voting for campaigns, to verify Telegram accounts, etc. You are then asked to enter details on a site or click on a malicious link.

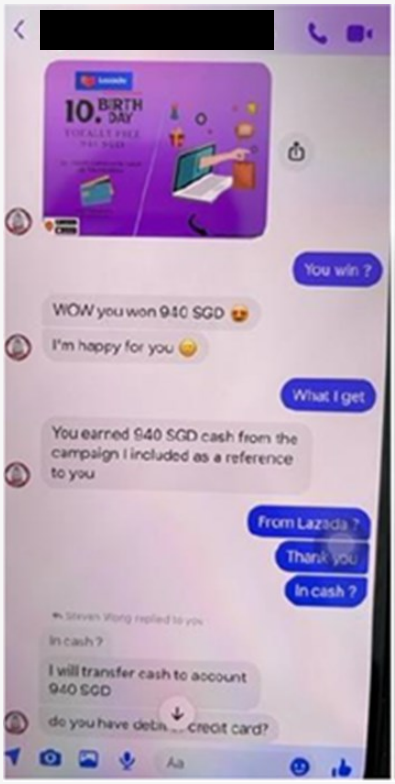
See the next page for more details on this scam type.

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

Asked to participate in a campaign to win prizes?

Scam Tactics

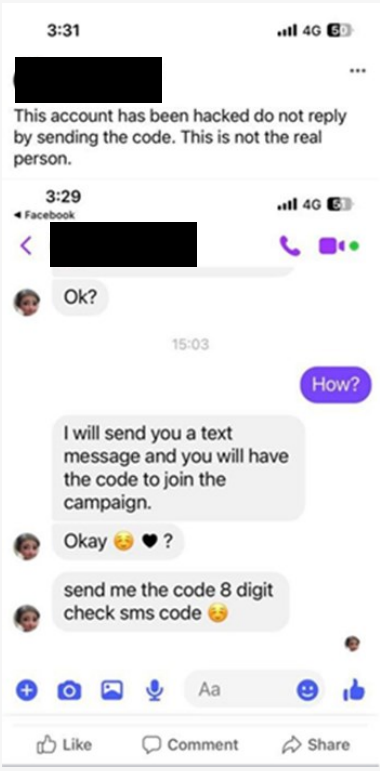
- Victims are approached on social media platforms to join or vote for "fake" campaigns by local brands (e.g., Lazada, Grab, Shopee). Unknown to victims, these social media accounts have either been taken over or spoofed by the culprits impersonating as the victims' relatives or friends.
- Scammers would ask victims for the phone numbers and/or OTPs sent from various platforms (e.g., Microsoft, Grab, Google) to receive gift vouchers or monies "won" from these "fake" campaigns.
- The OTPs would then be used by scammers to approve transactions from victims' linked bank accounts/cards to their e-wallets (e.g., Grab Activation Code). Victims may also lose access to their social media accounts after giving away their OTPs that were meant to reset their account passwords.
- In another variant, victims would receive a link to a website fraudulently bearing a bank logo which would be used to phish for their banking credentials. Victims would later discover unauthorised transactions made to their banking accounts and/or unauthorised charges made to their mobile phone bills, after providing the banking information within the link.



[Example of a fake Lazada Campaign with phishing link provided]

Some precautionary measures:

- **ADD** - ScamShield App and set security features (e.g., enable 2FA for banks, social media, Singpass accounts; set transaction limits on internet banking transactions, including PayNow/PayLah).
- **CHECK** – for scam signs with official sources (www.scamalert.sg, call the Anti-Scam Helpline at 1800-722-6688 or check with the platforms directly on whether the campaigns are real).
- Be wary of unexpected requests or offers from social media contacts, especially relating to campaigns or contests. Never disclose your personal details, banking credentials and OTPs to anyone.
- **TELL** – authorities, family and friends about scams. Report any fraudulent transactions to your bank and telecommunications company immediately.
- If your social media account has been compromised, report immediately to the platform and inform your friends too so that they do not fall prey to scammers.



[Example of a Facebook Password Reset Code Given by Victim to Participate in the "Campaign"]

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

21 号刊
2023年8月11日

当心骗局

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。

求职诈骗

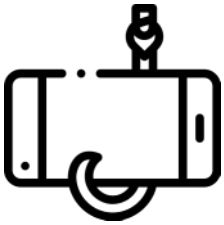
您收到一份承诺只需付出很少努力就能获得高薪的工作机会。

查看官方消息，如公司的官方网站，以核实该工作机会。

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。



钓鱼骗局（冒充政府部门来电）

您会接到来自“政府官员” 的电话。您被要求提供您的银行凭证、一次性密码和/或个人资料。

只从官方应用程序商店**下载**ScamShield 应用程序，拦截诈骗电话和过滤诈骗短信。切勿向身份不明人士提供您的凭证以及一次性密码。

社交媒体冒充他人骗局 *

您在社交媒体或其他沟通平台收到自称是您的朋友/亲戚发来的信息，要求您给予协助，理由包括参与或在宣传活动投票、核实Telegram账户等。您过后被要求在网站上输入详情或点击恶意链接。

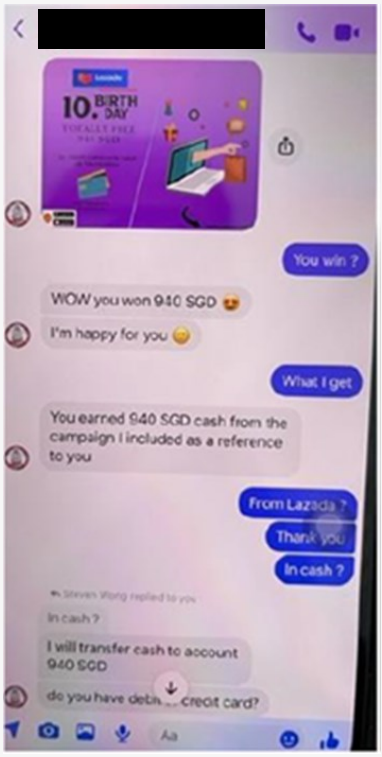
请参阅下一页以便了解更多这类诈骗的详情。

*本周新加入前五名的诈骗手法。

⚠ 参加宣传活动赢取奖品吗？

诈骗手法

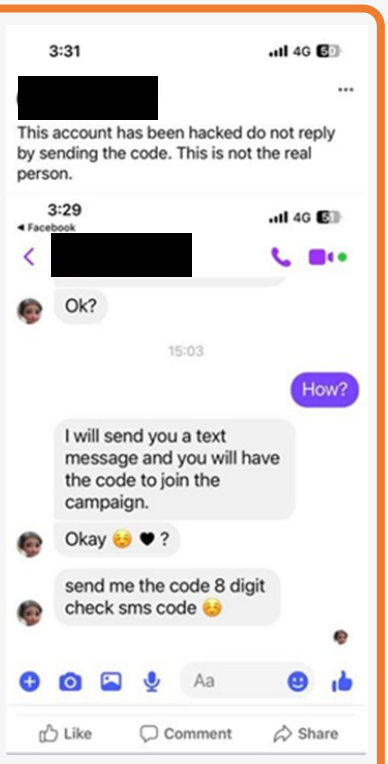
- 在受害者亲友的社交媒体账户被骗子接管或骗子冒充受害者亲友的情况下，受害者亲友在社交平台邀请不知情的受害者参加或投选本地品牌（如Lazada、Grab、Shopee）的"假"宣传活动。
- 骗子会利用各种平台（如微软、Grab、Google）向受害者索取电话号码和/或一次性密码，以领取这些从"假"宣传活动"赢取"的钱或礼券。
- 骗子会利用一次性密码批准从受害者绑定的银行账户/卡到电子钱包的交易（例如：Grab激活码）。受害者在提供了用于重置账户密码的一次性密码后也可能无法进入他们的社交媒体账户。
- 在另一种手法中，受害者会收到一个链接。该链接会引导受害者至一个带有银行标志的假网站。骗子利用钓鱼手法在网站索取受害者的银行凭证。在网站提供银行信息后，受害者发现他们的银行账户有未经授权的交易和/或手机账单有未经授权的收费。



[虚假的Lazada宣传活动和钓鱼链接的例子]

一些预防措施：

- **下载** – ScamShield应用程序并设置安全功能（如在银行,社交媒体，Singpass账户启用双重认证；设置银行交易限额，包括 PayNow/ PayLah）。
- **查看** – 官方消息并注意诈骗迹象(www.scamalert.sg, 拨打反诈骗热线 1800-722-6688 或者直接向平台查询宣传活动的真实性)。
- 提防社交媒体好友，尤其是与宣传活动或比赛有关，的突兀要求或优惠。切勿向任何人透露您的个人资料，银行凭证和一次性密码。
- **告知** – 当局、家人和朋友诈骗案件趋势。立即向银行和电信公司举报任何欺诈性的交易。
- 如果您的社交媒体账号被盗用，请立即向平台举报，并通知您的朋友，以免他们成为诈骗子的受害者。



[受害者提供脸书的密码重设码，以便参与"宣传活动"的例子]

⚠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. 21

11 Ogos 2023

SEPANJANG MINGGU LEPAS

Penipuan yang harus diawasi

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 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 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 (Panggilan Menyamar Sebagai Agensi Pemerintah)

Anda menerima satu panggilan daripada seorang "pegawai pemerintah". Anda diminta supaya memberikan butiran perbankan, OTP dan/atau butir-butir peribadi anda.

MASUKKAN aplikasi ScamShield hanya daripada gedung aplikasi rasmi ke telefon bimbit anda untuk menyekat panggilan penipuan dan mengesan SMS penipuan daripada nombor-nombor yang diketahui telah disenaraihitamkan. Jangan berikan butiran dan OTP anda kepada orang-orang yang tidak dikenali.

Penipuan Penyamaran di Media Sosial *

Anda menerima mesej daripada platform media sosial atau daripada platform komunikasi yang lain yang mendakwa dia seorang kawan/saudara mara anda, dan meminta bantuan anda atas pelbagai sebab seperti menyertai atau mengundi untuk kempen, untuk mengesahkan akaun Telegram, dsb. Anda kemudian diminta untuk memasukkan butiran ke sebuah laman web atau klik pada pautan berniat jahat.

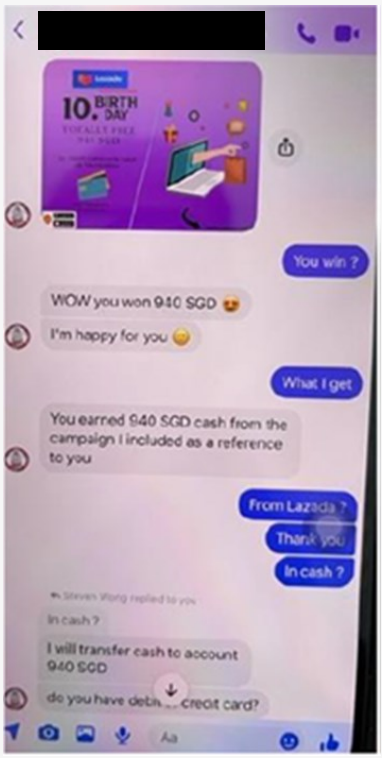
Lihat halaman seterusnya untuk butir-butir lanjut bagi jenis penipuan sebegini.

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

Diminta menyertai kempen untuk me-menangi hadiah?

Taktik Penipuan

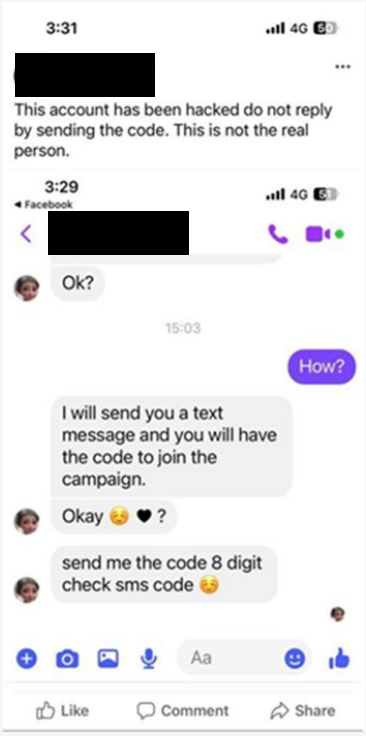
- Mangsa didekati di platform media sosial untuk menyertai atau mengundi untuk kempen "palsu" oleh jenama tempatan (misalnya, Lazada, Grab, Shopee). Tanpa diketahui mangsa, akaun media sosial ini telah, sama ada diambil alih atau ditiru oleh pesalah yang menyamar sebagai saudara mara atau kawan mangsa.
- Penipu akan meminta mangsa nombor telefon dan/atau OTP yang dihantar daripada pelbagai platform (misalnya, Microsoft, Grab, Google) untuk menerima baucar hadiah atau wang yang "dimenangi" daripada kempen "palsu" ini.
- Penipu akan kemudian menggunakan OTP tersebut untuk meluluskan transaksi daripada akaun/kad bank mangsa yang dipautkan kepada e-dompet mereka (misalnya, Kod Pengaktifan Grab). Mangsa juga mungkin kehilangan akses kepada akaun media sosial mereka selepas memberikan OTP mereka yang bertujuan untuk menetapkan semula kata laluan akaun mereka.
- Dalam versi yang lain, mangsa akan menerima pautan yang akan membawanya ke laman web palsu yang mengandungi logo bank. Pautan ini akan digunakan untuk memancing data butiran perbankan mereka. Selepas memberikan maklumat perbankan dalam pautan, mangsa akan kemudian menemui transaksi tanpa kebenaran daripada akaun bank mereka dan/atau caj tanpa kebenaran yang dibuat pada bil telefon mudah alih mereka.



[Contoh sebuah Kempen Lazada palsu dengan Pautan Pancingan Data yang disediakan]

Beberapa langkah berjaga-jaga:

- **MASUKKAN** – Aplikasi ScamShield dan pasangkan ciri-ciri keselamatan (misalnya, dayakan dua-faktor (2FA) untuk bank-bank, media sosial, akaun Singpass; tetapkan had transaksi untuk transaksi perbankan internet, termasuklah PayNow /PayLah).
- **PERIKSA** – Untuk tanda-tanda penipuan dan dengan sumber-sumber rasmi (www.scamalert.sg, telefon Talian Bantuan Antipenipuan di 1800-722-6688 atau periksa dengan platform-platform tersebut sama ada kempen itu benar atau tidak secara langsung).
- Berwaspada terhadap permintaan atau tawaran yang tidak dijangka daripada kenalan di media sosial, terutamanya yang berkaitan dengan kempen atau peraduan. Jangan sesekali mendedahkan butir-butir peribadi, butiran perbankan dan OTP anda kepada sesiapa.
- **BERITAHU** - Pihak berkuasa, keluarga dan kawan-kawan tentang penipuan. Laporkan sebarang transaksi menipu kepada bank dan syarikat telekomunikasi anda dengan segera.
- Jika akaun media sosial anda telah terjejas, laporkan kepada platform dengan segera dan juga beritahu kawan anda supaya mereka tidak menjadi mangsa penipu.



[Contoh sebuah Kod Tetapan Semula Kata Laluan Facebook Diberikan oleh Mangsa untuk Menyertai "Kempen"]

⚠ 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 Antipenipuan 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. 21

11 ஆகஸ்ட் 2023

எச்சரிக்கையாக இருக்க வேண்டிய மோசடிகள்

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**.

வேலை மோசடி

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

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

தகவல் திருட்டு மோசடி (அரசாங்க அமைப்புகளைப் போல ஆள்மாறாட்டம் செய்யும் அழைப்புகள்)

“அரசாங்க அதிகாரி” ஒருவரிடமிருந்து உங்களுக்கு அழைப்பு வருகிறது. உங்கள் வங்கி விவரங்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) மற்றும்/அல்லது தனிப்பட்ட விவரங்களை வழங்குமாறு நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்கள்.

மோசடி அழைப்புகளைத் தடுக்கவும், கறுப்புப் பட்டியலிடப்பட்ட எண்களிலிருந்து மோசடி குறுஞ்செய்திகளைக் கண்டறியவும், உங்கள் கைபேசியில் உள்ள அதிகாரப்பூர்வ செயலி விநியோக நிறுவனங்களில் இருந்து மட்டுமே ஸ்கேம்ஷீல்ட் செயலியைச் **சேர்க்கவும்**. தெரியாத நபர்களுக்கு உங்கள் விவரங்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லையும் (OTP) வழங்காதீர்கள்.

சமூக ஊடக ஆள்மாறாட்ட மோசடி *

நீங்கள் உங்கள் நண்பர் / உறவினர் என்று கூறிக்கொள்ளும் ஒருவரிடமிருந்து சமூக ஊடகம் அல்லது பிற தகவல்தொடர்பு தளங்களிலிருந்து ஒரு செய்தியைப் பெறுகிறீர்கள். பிரச்சாரங்களில் சேருவது அல்லது வாக்களிப்பது, டெலிகிராம் கணக்குகளைச் சரிபார்ப்பது போன்ற பல்வேறு காரணங்களுக்காக உங்கள் உதவியை அவர் கேட்கிறார். பின்னர் நீங்கள் ஒரு தளத்தில் விவரங்களை உள்ளிடவும் அல்லது தீங்கிழைக்கும் இணைப்பை கிளிக் செய்யவும் கேட்டுக்கொள்ளப்படுகிறீர்கள்.

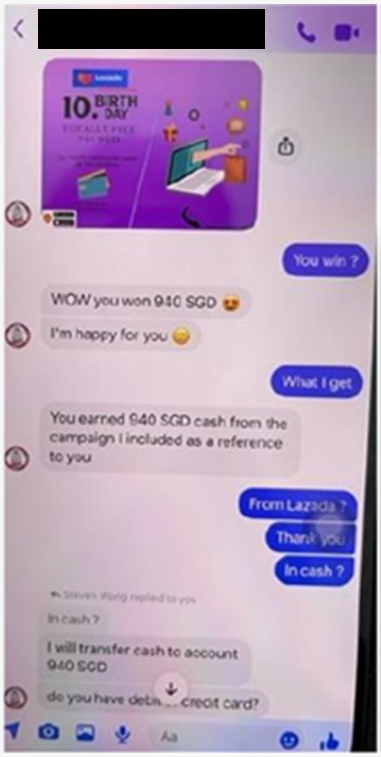
இந்த மோசடி வகை பற்றிய மேல் விவரங்களுக்கு, அடுத்த பக்கத்தைப் பார்க்கவும்.

*முந்தைய வாரத்துடன் ஒப்பிடும்போது இந்த மோசடி முதல் 5 இடங்களுக்குப் புதியது.

பரிசுகளை வெல்வதற்காக பிரச்சாரத்தில் பங்கேற்குமாறு நீங்கள் கேட்டுக்கொள்ளப்படுகிறீர்களா?

மோசடி உத்திகள்

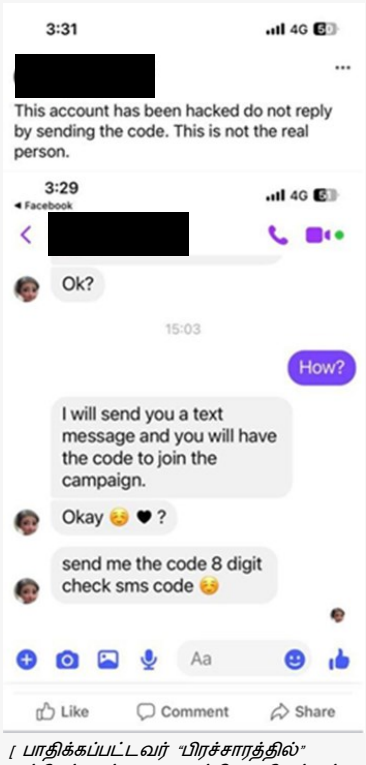
- உள்ளூர் பிராண்டுகளின் (எ. கா., Lazada, Grab, Shopee) "போலி" பிரச்சாரங்களில் சேர அல்லது வாக்களிக்க பாதிக்கப்பட்டவர்கள் சமூக ஊடகத் தளங்களில் அணுகப்படுகிறார்கள். இந்த சமூக ஊடகக் கணக்குகள் குற்றவாளிகளால் எடுத்துக் கொள்ளப்பட்டவை அல்லது பாதிக்கப்பட்டவர்களின் உறவினர்கள் அல்லது நண்பர்கள் போல ஆள்மாறாட்டம் செய்யும் போலி கணக்குகள் என்பது பாதிக்கப்பட்டவர்களுக்குத் தெரியாது.
- மோசடிக்காரர்கள் பாதிக்கப்பட்டவர்களிடம் இந்த "போலி" பிரச்சாரங்களிலிருந்து "வென்ற" பரிசு பற்றுச்சீட்டுகள் அல்லது பணம் ஆகியவற்றை பெறுவதற்கு பல்வேறு தளங்களிலிருந்து (எ. கா., Microsoft, Grab, Google) அனுப்பப்பட்ட தொலைபேசி எண்கள் மற்றும் / அல்லது ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) ஆகியவற்றை கேட்பார்கள்.
- பாதிக்கப்பட்டவர்களின் இணைக்கப்பட்ட வங்கிக் கணக்குகள் / அட்டைகளிலிருந்து அவர்களின் மின் பணப்பைகளுக்கான (எ. கா., Grab Activation Code) பரிவர்த்தனைகளை அங்கீகரிக்க மோசடிக்காரர்களால் ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) பயன்படுத்தப்படும். பாதிக்கப்பட்டவர்கள் தமது கணக்கிற்கான கடவுச்சொற்களை மீட்டமைப்பதற்காக தமது ஒருமுறை பயன்படுத்தும் கடவுச்சொற்களை (OTPs) வழங்கிய பின்னர் தங்கள் சமூக ஊடகக் கணக்குகளுக்கான அணுகலை இழக்க நேரிடலாம்.
- மற்றொரு வகையில், பாதிக்கப்பட்டவர்கள் வங்கி சின்னத்தைக் கொண்ட ஒரு வலைத்தளத்தின் இணைப்பைப் பெறுவார்கள். பின்னர், அது அவர்களின் வங்கிச் சான்றுகளை திருடுவதற்கு பயன்படுத்தப்படும். பாதிக்கப்பட்டவர்கள் தங்கள் வங்கிக் கணக்குகளில் செய்யப்பட்ட அங்கீகரிக்கப்படாத பரிவர்த்தனைகள் மற்றும் / அல்லது அங்கீகரிக்கப்படாத கைப்பேசி கட்டணங்கள் ஆகியவற்றை இணைப்புக்குள் வங்கித் தகவல்களை வழங்கிய பின்னரே கண்டுபிடிப்பார்கள்.



[போலி Lazada பிரச்சாரத்தில் உள்ள ஒரு தகவல் திருட்டு இணைப்பின் உதாரணம்]

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

- **சேர்க்க** - ஸ்கேம்ஷீல்ட் செயலியைச் சேர்த்து, பாதுகாப்பு அம்சங்களை அமைக்கவும் (எ. கா., வங்கிகள், சமூக ஊடகம், Singpass கணக்குகளுக்கு 2FA முறையைச் செயல்படுத்தவும்; PayNow/PayLah உள்ளிட்ட இணைய வங்கிச் சேவை பரிவர்த்தனைகளின் மீது பரிவர்த்தனை வரம்புகளை அமைக்கவும்).
- **சரிபார்க்கவும்** - மோசடிக்கான அறிகுறிகளைக் கண்டறிந்து, அதிகாரப்பூர்வ ஆதாரங்களுடன் சரிபார்க்கவும். (www.scamalert.sg, 1800-722-6688 என்ற மோசடி எதிர்ப்பு உதவி எண்ணை அழைக்கவும் அல்லது பிரச்சாரங்கள் உண்மையானவையா என்பதை நேரடியாக தளங்களுடன் சரிபார்க்கவும்).
- சமூக ஊடகத் தொடர்புகளிடமிருந்து, குறிப்பாக பிரச்சாரங்கள் அல்லது போட்டிகள் தொடர்பான எதிர்பாராத கோரிக்கைகள் அல்லது சலுகைகள் குறித்து எச்சரிக்கையாக இருங்கள். உங்கள் தனிப்பட்ட விவரங்கள், வங்கி சான்றுகள் மற்றும் ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) ஆகியவற்றை யாரிடமும் ஒருபோதும் வெளியிடாதீர்கள்.
- **சொல்ல** - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். எந்தவொரு மோசடி பரிவர்த்தனைகளையும் உங்கள் வங்கி மற்றும் தொலைத்தொடர்பு நிறுவனத்திடம் உடனடியாக தெரிவிக்கவும்.
- உங்கள் சமூக ஊடகக் கணக்கு பாதிக்கப்பட்டிருந்தால், உடனடியாக அந்த தளத்திற்கு தெரிவிக்கவும். மோசடிக்காரர்களுக்கு இரையாகாமல் இருக்க உங்கள் நண்பர்களுக்கும் தெரியப்படுத்துங்கள்.



[பாதிக்கப்பட்டவர் "பிரச்சாரத்தில்" பங்கேற்பதற்காக வழங்கிய .:பேஸ்புக் கடவுச்சொல் மீட்டமைப்பு எண்ணின் எடுத்துக்காட்டு]

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