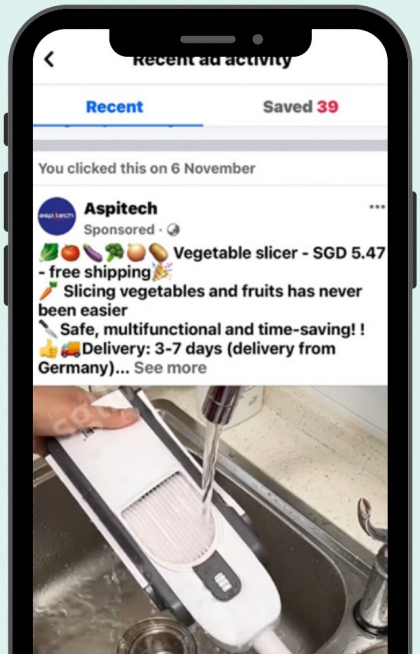
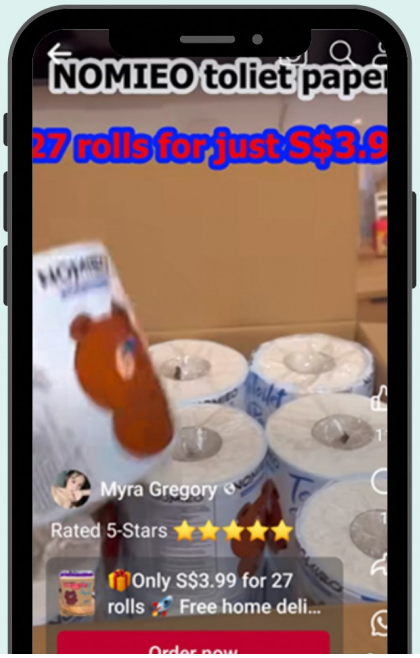
Weekly Scams Bulletin

Saw an attractive deal for an item that you want?

Since January 2024, at least 104 victims have fallen prey to such scams, with losses amounting to at least $63,000.

Screenshots of Fraudulent Social Media Advertisements





Shop on well-established e-commerce sites and check the e-commerce platform's Transaction Safety Rating at go.gov.sg/mhatsr

Victims would encounter advertisements/ posts on social media platforms (e.g. Instagram/Facebook/TikTok) offering promotions for electronics, food, and daily items with fantastic discounts.

As victims prepare to make purchase, they are directed to phishing websites that may mimic bank or e-commence sites, to key in their card details and One-Time Passwords (OTPs) to make payment.

Victims would discover unauthorized transfers or deductions from their bank accounts.

Some Precautionary Measures:

ADD – security features and set up transaction limits for internet banking transactions, enable Two-Factor Authentication (2FA), Multifactor Authentication for bank accounts. Consider Money Lock option for your bank accounts.

CHECK – for any spelling errors in the webpage link for tell-tale signs of a phishing website. Call the NCPC Anti-Scam Helpline at 1800-722-6688 if you are unsure if a situation you are facing is a scam.

- Be cautious of attractive deals that seem too good to be true.
- Shop on well-established e-commerce sites and check the e-commerce platform's Transaction Safety Rating at go.gov.sg/mhatsr.

TELL – the authorities by filing a police report and contact your bank immediately if you suspect that your account or credit card has been compromised.

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

诈骗周报

受害者会在社交媒体平台（如 Instagram/脸书/TikTok) 上看见电子商品、食品和日常用品正进行大促销的广告/帖子。

当受害者准备购买时，他们会被转接至貌似银行或电子商务网站的钓鱼网站，以输入信用卡信息和一次性密码 (OTPs) 来进行付款。

受害者会发现银行账户有未经授权的交易或款项遭扣除。

一些预防措施：

添加 – 安全功能并设置网络银行交易限额以及为银行账户启用双重或多重认证。考虑为银行账户设置 Money Lock。

查证 – 网页链接是否有任何拼写错误，以识别钓鱼网站迹象。当您不确定所面临的情况是否是诈骗时，请拨打全国罪案防范理事会反诈骗热线 1800-722-6688 查询。

- 若优惠好得难以置信，请小心谨慎。
- 务必在信誉良好的电子商务网站购物，并游览 go.gov.sg/mhatsr查看电子商务平台的交易安全评级。

通报 – 如果您怀疑您的账户或信用卡已被盗用，请立即向警方报案并联系您的银行。

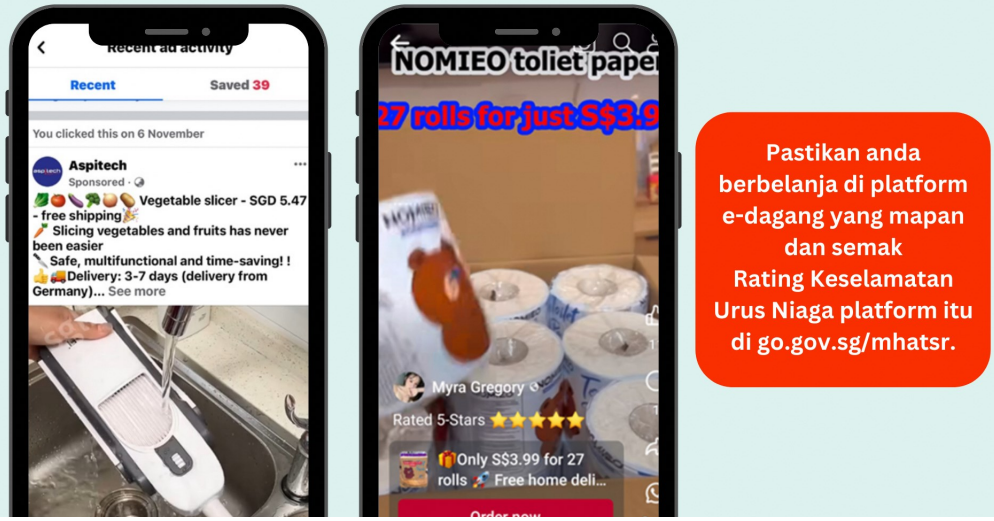
欲了解更多关于这个骗局的信息，请浏览 SPF | News (police.gov.sg)

Buletin Penipuan Mingguan

Ternampak tawaran yang menarik untuk barangan yang anda mahu?

Sekurang-kurangnya 104 orang telah menjadi mangsa penipuan sedemikian sejak Januari 2024, dengan kerugian berjumlah sekurang-kurangnya $63,000.

Tangkap layar iklan media sosial menipu



Pastikan anda berbelanja di platform e-dagang yang mapan dan semak Rating Keselamatan Urus Niaga platform itu di go.gov.sg/mhatsr.

Mangsa akan menerima iklan / hantaran di platform media sosial (contohnya Instagram / Facebook / TikTok) yang menawarkan promosi untuk peralatan elektronik, makanan, dan barangan keperluan harian dengan diskaun yang hebat.

Sedang mangsa bersedia untuk membuat pembelian, mereka diarahkan ke laman web pancingan data yang mungkin meniru laman web bank atau e-dagang, untuk memasukkan butiran kad dan Kata Laluan Sekali Guna (OTP) mereka untuk membuat pembayaran.

Mangsa akan mendapati adanya pemindahan atau potongan tanpa kebenaran daripada akaun bank mereka.

Beberapa langkah berjaga-jaga:

MASUKKAN – ciri-ciri keselamatan dan tetapkan had transaksi untuk transaksi perbankan internet, dayakan Pengesahan Dua-Faktor (2FA), Pengesahan Pelbagai Faktor untuk akaun bank. Pertimbangkan pilihan 'Kunci Wang' untuk akaun bank anda.

PERIKSA – sebarang kesilapan ejaan dalam pautan laman web untuk tanda-tanda ketara sesebuah laman web pancingan data. Hubungi Talian Bantuan Anti-Penipuan NCPC di 1800-722-6688 sekiranya anda tidak pasti jika situasi yang anda sedang hadapi ialah satu penipuan.

- Berhati-hati dengan tawaran menarik yang terlalu hebat untuk dipercayai.
- Pastikan anda berbelanja di platform e-dagang yang mapan dan semak Rating Keselamatan Urus Niaga platform itu di go.gov.sg/mhatsr.

BERITAHU – pihak berkuasa dengan menfailkan laporan polis dan hubungi bank anda dengan segera sekiranya anda syak bahawa akaun atau kad kredit anda telah dikompromi.

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

வாராந்திர மோசடிகள்

பாதிக்கப்பட்டவர்கள் மின்னணுவியல், உணவு, அன்றாடப் பொருட்கள் ஆகியவற்றுக்கு அருமையான தள்ளுபடிகளை வழங்கும் விளம்பரங்களை/பதிவுகளை சமூக ஊடகத் தளங்களில் (எ.கா. **Instagram/Facebook/TikTok**) பார்ப்பார்கள்.

பணம் செலுத்த, பாதிக்கப்பட்டவர்கள் வங்கி அல்லது மின்-வர்த்தக இணையத்தளம் போல தோற்றமளிக்கும் தகவல் திருட்டு இணையத்தளத்தில் தங்கள் அட்டை விவரங்கள், ஒரு முறை கடவுச் சொல் (**OTP**) ஆகியவற்றை உள்ளீட வேண்டியிருக்கும்.

அங்கீகரிக்கப்படாத பணப்பரிமாற்றங்கள் அல்லது கழிவுகள் அவர்களின் வங்கி கணக்கு மூலம் செய்யப்பட்டதை பாதிக்கப்பட்டவர்கள் கண்டுபிடிப்பார்கள்.

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - இணைய வங்கிப் பரிவர்த்தனைகளுக்குப் பாதுகாப்பு அம்சங்களையும் பரிவர்த்தனை வரம்புகளையும் அமைக்கவும். வங்கிக் கணக்குகளுக்கு இரட்டை மறைச்சொல் முறையையும் (2FA) பன்முக உறுதிப்பாட்டையும் செயல்படுத்தவும். உங்கள் வங்கிக் கணக்குகளுக்குப் பணப் பூட்டு (**Money Lock**) போடுவது பற்றி யோசித்துப் பார்க்கவும்.

சரிபார்க்க - இணையப்பக்க இணைப்பில் ஏதேனும் எழுத்துப் பிழைகள் இருக்கிறதா என்று சரிபார்க்கவும், அது ஒரு தகவல் திருட்டு இணையத்தளம் என்பதற்கான அறிகுறியாகும். நீங்கள் எதிர்நோக்கும் சூழ்நிலை ஒரு மோசடியா என்பது உறுதியாகத் தெரியாவிட்டால், மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைத்து உறுதிப்படுத்திக் கொள்ளவும்.

- உண்மையாக இருக்க முடியாது என்று தோன்றும் கவர்ச்சிகரமான ஒப்பந்தங்கள் குறித்து எச்சரிக்கையாக இருங்கள்.
- நன்கு நிறுவப்பட்ட மின்-வர்த்தக இணையத்தளத்தில் வாங்குவதுடன், go.gov.sg/mhatsr இல் மின்-வர்த்தகத் தளத்தின் பரிவர்த்தனை பாதுகாப்பு மதிப்பீட்டை சரிபார்க்கவும்.

சொல்ல - உங்கள் கணக்கு அல்லது கடன் அட்டை பாதிக்கப்பட்டிருப்பதாக நீங்கள் சந்தேகித்தால், காவல்துறையில் புகார் செய்து அதிகாரிகளிடம் தெரியப்படுத்துவதோடு, உங்கள் வங்கியுடனும் உடனடியாகத் தொடர்பு கொள்ளவும்.

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