Issue 06/25

6 June 2025

MONTHLY SCAMS BULLETIN

Phishing Scams on the Rise!

In a recent spate of phishing scam cases, victims would encounter the scam by clicking on links embedded in the following channels:

Fake emails

Fake POSB emails about expired mobile banking digital tokens, with embedded URL links urging immediate action.

Fake websites

Victims search for AXS website on search engines (e.g. Google) to pay bills and are redirected to fake websites mimicking AXS that appear as top search results.

Fake advertisements

Victims come across advertisements on social media platforms impersonating local companies offering enticing promotions.

Tips:

- Activate the Money Lock feature of your bank to "lock up" a portion of your money so that your money cannot be transferred out digitally even if your banking details are compromised.
- Set transaction limits and lower transaction notification thresholds so you will know if there is an unauthorised transaction.
- Alert the bank immediately of any suspicious activity in your bank account.

Preventive Measures

For emails

Always check the sender's email address.

Email Sender ID can be spoofed to make the email look legitimate.

For SMS messages

Legitimate organisations use consistent and official Sender IDs. Text messages from government agencies will be sent from 'gov.sg' sender ID.

If you are unsure, verify the message with official channels. For example, if the message appears to be from your bank, call them directly using the phone number listed on their official website to confirm whether it is legitimate.

For advertisements

Always check directly with the company offering the promotion on its legitimacy.

UNSURE IF IT'S A SCAM? CALL AND CHECK WITH THE 24/7 SCAMSHIELD HELPLINE AT 1799

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

诈骗月刊

钓鱼骗局日益剧增!

在最近接二连三的钓鱼骗局中，受害者往往通过点击以下渠道内的链接遭遇诈骗:

虚假电邮

虚假的 POSB (储蓄银行) 电邮，声称手机银行密码生成器已过期，并内含网站链接，敦促立即采取行动。

虚假网站

受害者通过搜索引擎（例如谷歌）搜索AXS网站以支付账单，却被转接至出现在搜索结果顶部，效仿AXS的虚假网站。

虚假广告

受害者在社交媒体平台上看到冒充本地公司提供诱人促销活动的广告。

贴士:

- 启动银行的 Money Lock 功能，将您部分资金“锁定”，这样即使您的银行信息被泄露，也无法以数码方式转出。
- 设置交易限额并降低交易通知限额，如果有未经授权的交易，您将收到通知。
- 如果银行账户中出现任何可疑活动，请立即通知银行。

防范措施:

电邮

务必检查发送人的电邮地址。

电邮发送人的身份可以是伪造的，目的就是让电邮显得有合法性。

短信

正当机构使用的是一致且官方的发送者身份。政府机构的短信都将以'gov.sg' 发送者身份寄出。

若不确定，可通过官方渠道核实短信。例如，如果短信看似来自银行，可直接拨打银行官方网站列出的电话号码以确认短信的真实性。

广告

务必直接和公司确认其促销的真实性。

不确定这是否是个骗局?请拨打24小时的SCAMSHIELD援助热线 1799 查询。

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

Isu 06/25

6 Jun 2025

BULETIN PENIPUAN BULANAN

Penipuan Pancingan Data semakin Berleluasa!

Dalam beberapa kes penipuan pancingan data baru-baru ini, mangsa diperdaya untuk klik pautan yang dihantar oleh penipu melalui saluran berikut:

E-mel palsu

E-mel daripada POSB yang palsu mengenai token digital perbankan mudah alih yang telah tamat tempoh, dengan pautan URL yang terdapat dalam e-mel itu menggesa tindakan segera.

Laman web palsu

Mangsa mencari laman web AXS melalui enjin carian (contohnya Google) untuk membayar bil, tetapi diarahkan ke laman web palsu yang meniru AXS dan muncul sebagai hasil carian teratas.

Iklan palsu

Mangsa menemui iklan di platform media sosial yang menyamar sebagai syarikat tempatan dan menawarkan promosi menarik.

Tip:

- Aktifkan ciri kunci wang bank untuk 'mengunci' sebahagian daripada wang anda supaya ia tidak boleh dipindahkan keluar secara digital walaupun butiran perbankan anda terjejas.
- Tetapkan had transaksi dan had pemberitahuan transaksi yang lebih rendah supaya anda dapat mengetahui jika terdapat transaksi tanpa kebenaran.
- Maklumkan kepada bank dengan segera tentang sebarang aktiviti yang mencurigakan dalam akaun bank anda.

Langkah pencegahan

Untuk e-mel

Sentiasa periksa alamat e-mel penghantar.

ID E-mel Penghantar boleh dipalsukan untuk membuat e-mel itu kelihatan sah.

Untuk mesej Khidmat Pesanan Ringkas (SMS)

Organisasi yang sah menggunakan ID Penghantar yang konsisten dan rasmi. Mesej teks daripada agensi Pemerintah akan menggunakan ID Penghantar 'gov.sg'. Jika anda tidak pasti, sahkan mesej tersebut melalui saluran rasmi. Sebagai contoh, jika maklumat yang dipaparkan dalam mesej teks menunjukkan penghantar adalah daripada pihak bank anda, hubungi mereka secara langsung menggunakan nombor telefon yang disenaraikan di laman web rasmi mereka untuk mengesahkan sama ada mesej teks itu sahih.

Untuk iklan

Sentiasa periksa secara langsung dengan syarikat yang menawarkan promosi itu untuk memastikan ia sahih.

TIDAK PASTI SEKIRANYA IA SATU PENIPUAN? TELEFON DAN PERIKSA DENGAN TALIAN BANTUAN SCAMSHIELD DI 1799

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources

வெளியீடு 06/25

மாதாந்திர மோசடிகள்

6 ஜூன் 2025

தகவல் திருட்டு மோசடிகள் அதிகரித்து வருகின்றன!

சமீபத்திய மோசடி சம்பவங்களில், பாதிக்கப்பட்டவர்கள் பின்வரும் வழிகள் மூலம் இணைக்கப்பட்ட இணைப்புகளைக் கிளிக் செய்து மோசடியை எதிர்கொண்டனர்:

போலி மின்னஞ்சல்கள்

காலாவதியான மொபைல் பேங்கிங் மின்னிலக்க டோக்கன்கள் தொடர்பாக உடனடி நடவடிக்கை எடுக்க வலியுறுத்தும் பதிக்கப்பட்ட இணையத்தள முகவரி (URL) இணைப்புகளைக் கொண்ட போலி பிஓஎஸ்பி (POSB) மின்னஞ்சல்கள்

போலி இணையத்தளங்கள்

பாதிக்கப்பட்டவர்கள் தங்கள் கட்டணங்களைச் செலுத்த இணையத்தில் (எ.கா. கூகிள்) ஏஎக்ஸ்எஸ் (AXS) இணையத்தளத்தைத் தேடியபோது, உண்மையான AXS இணையத்தளம் போல தோற்றமளிக்கும் போலி இணையத்தளங்கள் முதல் சில தேடல் முடிவுகளாகத் தோன்றின.

போலி விளம்பரங்கள்

கவர்ச்சிகரமான சலுகைகளை வழங்கும் உள்ளூர் நிறுவனங்களைப் போல தோற்றமளிக்கும் விளம்பரங்களை சமூக ஊடகத் தளங்களில் பாதிக்கப்பட்டவர்கள் காண்பார்கள்.

குறிப்புகள்:

- உங்கள் வங்கி விவரங்கள் மற்றவர்களால் அறியப்பட்டாலும் கூட, உங்கள் பணத்தை மின்னிலக்க முறையில் மாற்ற முடியாதபடி, உங்கள் பணத்தின் ஒரு பகுதியை ஒதுக்கி வைக்க உங்கள் வங்கியின் பண பூட்டு அம்சத்தை செயல்படுத்துங்கள்.
- பரிவர்த்தனை வரம்புகள், குறைந்த பரிவர்த்தனை வரம்பு அறிவிப்புகள் ஆகியவற்றை அமைக்கவும், இதனால் அங்கீகரிக்கப்படாத பரிவர்த்தனை நிகழும்போது உங்களுக்கு தெரிவிக்கப்படும்.
- உங்கள் வங்கி கணக்கில் சந்தேகத்திற்கிடமான நடவடிக்கைகள் ஏதேனும் இருந்தால் உடனடியாக வங்கிக்கு தெரியப்படுத்தவும்.

தடுப்பு நடவடிக்கைகள்

மின்னஞ்சல்களில்

அனுப்புநரின் மின்னஞ்சல்முகவரியை எப்போதும் சரிபாருங்கள்.

மின்னஞ்சலை நம்பக்கூடியதாகத் தோன்றச் செய்ய, போலி மின்னஞ்சல் முகவரியை பயன்படுத்தலாம்.

குறுஞ்செய்திகளில்:

சட்டபூர்வமான நிறுவனங்கள் ஒரே அதிகாரப்பூர்வ அனுப்புநர் அடையாளங்களைப் பயன்படுத்தும். அரசாங்க அமைப்புகளிடமிருந்து வரும் குறுஞ்செய்திகள் 'gov.sg' என்ற அனுப்புநர் அடையாளத்தில் அனுப்பப்படும். உங்களுக்கு உறுதியாகத் தெரியவில்லை என்றால், அதிகாரபூர்வ முறைகள் மூலம் குறுஞ்செய்தியை சரிபாருங்கள். உதாரணத்திற்கு, குறுஞ்செய்தி உங்கள் வங்கியிடமிருந்து வந்திருப்பதாகத் தோன்றினால், அது சட்டபூர்வமானதா என்பதை உறுதிப்படுத்த, வங்கியின் அதிகாரபூர்வ இணையத்தளத்தில் உள்ள தொலைபேசி எண்ணை நேரடியாக அழையுங்கள்.

விளம்பரங்களில்:

எப்போதும் சலுகைகளின் நம்பகத்தன்மையை நிறுவனத்துடன் நேரடியாக சரிபாருங்கள்.

இது ஒரு மோசடியா என்று உறுதியாக தெரியவில்லையா?

1799 24/7 'ஸ்கேம்ஷீல்டு' உதவி எண்ணை அழைத்து சரிபாருங்கள்.

I CAN ACT AGAINST SCAMS

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

Scan for SPF Scam Resources