2024 - Issue 11 15 Mar 2024

Weekly Scams Bulletin



Victims encounter fake job offers online or on messaging platforms like Telegram or WhatsApp chatgroups.

After expressing interest, victims would be instructed to provide their Singpass password and screenshots of their NRIC. Under the pretext of a required job screening, victims would also be asked to:

- (1) Change their Singpass email address and/or mobile number to those provided by the scammer; or
- (2) Authorise the retrieval of their personal details through multiple Singpass login weblinks sent to the victims

Scammers would use the victims' Singpass accounts to register for bank accounts that would be used to facilitate criminal activities.

Some Precautionary Measures:

CHECK - Call the Anti-Scam Helpline at 1800-722-6688 to check when you are unsure if a situation you are facing is a scam.

- Do not click on Singpass login URL links sent to you via SMS or messaging platforms such as WhatsApp or Telegram. Should you need to access a digital service via Singpass, you should do so via the organisation's website.
- Your Singpass and banking credentials, debit/credit card details, or One-Time Passwords (OTPs) are strictly for personal use. Do not share them with others, as they could be used for criminal activities.

TELL - authorities, family, and friends about your scam encounters. Report any fake comments or postings to the online platform administrators.

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







2024-11号刊 2024年3月15日

诈骗周报

保护好您的 Singpass 资料! 别与他人分享。









您的Singpass及银行凭证、 借记/信用卡信息或一次性密码 (OTPs) 仅限个人使用。 切勿与他人分享,因这些信息或被用 于犯罪活动。

受害者会在网上或如Telegram或WhatsApp聊天群组的通讯平台上看见虚假的工作机会。

在表示感兴趣后,受害者将被要求提供他们的 Singpass 密码和身份证截图。以进行工作所需 筛选为由,受害者还会被要求:

- (1) 将Singpass 电邮及/或手机号码更改成骗子提供的电邮及/或手机号码;或
- (2) 通过发送给受害者的多个 Singpass 登录链接授权提取其个人资料 骗子会利用受害者的 Singpass 账号来开设银行户口,从而为犯罪活动提供便利。

一些预防措施:

查证 – 当您不确定所面临的情况是否是诈骗时,请拨打反诈骗热线 1800-722-6688 查询。

- 切勿点击通过短信或通讯平台(如 WhatsApp 或 Telegram)发送的 Singpass 登录链 接。若需使用 Singpass 数码服务,应通过该机构的网站进行。
- 您的 Singpass 及银行凭证、借记/信用卡信息或一次性密码 (OTPs) 仅限个人使用。 切勿与他人分享,因这些信息或被用于犯罪活动。

通报 – 当局、家人和朋友诈骗案件趋势。向线上平台管理员举报任何虚假评论或帖子。

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









2024 – Isu 11 15 Mac 2024

Buletin Penipuan Mingguan



Mangsa menerima tawaran pekerjaan palsu dalam talian atau di platform pesanan seperti kumpulan sembang Telegram atau WhatsApp.

Selepas menyatakan minat mereka, mangsa akan diarahkan supaya memberikan kata laluan Singpass dan tangkap layar kad pengenalan mereka.

Dengan alasan keperluan untuk sebuah pemeriksaan pekerjaan, mangsa akan diminta supaya:

- (1) Menukar alamat e-mel Singpass dan/atau nombor telefon bimbit mereka kepada seperti yang diberikan oleh penipu: atau
- (2) Memberi kebenaran untuk mendapatkan semula butir-butir peribadi mereka melalui pelbagai pautan web log masuk Singpass yang dihantar kepada mangsa

Penipu akan menggunakan akaun Singpass mangsa untuk mendaftar untuk akaun bank yang akan digunakan untuk memudahkan kegiatan jenayah.

Beberapa langkah berjaga-jaga:

PERIKSA – Hubungi talian bantuan Anti-Penipuan di 1800 - 722-6688 sekiranya anda tidak pasti jika situasi yang sedang anda hadapi ialah satu penipuan.

- Jangan klik di pautan URL log masuk Singpass yang dihantar kepada anda melalui SMS atau platform pesanan seperti WhatsApp atau Telegram. Sekiranya anda perlu mengakses khidmat digital melalui Singpass, anda harus melakukannya melalui laman web organisasi tersebut.
- Butiran Singpass dan perbankan, butir-butir kad debit/kredit, atau Kata Laluan Sekali Sahaja (OTP) anda adalah hanya untuk kegunaan peribadi.Jangan kongsikan ia dengan orang lain, kerana ia boleh digunakan untuk kegiatan jenayah.

BERITAHU – Beritahu pihak berkuasa, keluarga, dan kawan-kawan tentang penipuan. Laporkan sebarang komen atau hantaran palsu kepada pentadbir platform dalam talian.





TELL
Authorities, family and friends





2024 - வெளியீடு எண். 11 15 மார்ச் 2024

வாராந்திர மோசடிகள்



பாதிக்கப்பட்டவர்கள் இணையத்தில் அல்லது டெலிகிராம், வாட்ஸ்ஆப் செய்தி அனுப்பும் தளங்கள் போன்ற உரையாடல் தளங்களில் வேலை வாய்ப்புகளைப் பார்ப்பார்கள்.

ஆர்வத்தை வெளிப்படுத்திய பிறகு, பாதிக்கப்பட்டவர்கள் தங்கள் Singpass கடவுச் சொல்லையும் அவர்களின் அடையாள அட்டையின் திரைக்காட்சிகளையும் வழங்குமாறு கூறப்படுவார்கள்.

வேலைச் சோதனை என்ற சாக்குப்போக்கின் கீழ், பாதிக்கப்பட்டவர்கள் பின்வருவனவற்றைச் செய்யும்படி கேட்டுக்கொள்ளப்படுவார்கள்:

- மோசடிக்காரர் வழங்கிய Singpass மின்னஞ்சல் முகவரி மற்றும் / அல்லது கைபேசி எண்ணுக்கு மாற்றுதல்; (1) அல்லது
- பாதிக்கப்பட்டவர்களுக்கு அனுப்பப்பட்ட பல Singpass உள்நுழைவு இணைய இணைப்புகள் மூலம் அவர்களின் தனிப்பட்ட விவரங்களை மீட்டெடுக்க அனுமதி அளித்தல்

மோசடிக்காரர்கள், பாதிக்கப்பட்டவர்களின் கணக்குகளைப் பயன்படுத்தி, Singpass குற்ற நடவடிக்கைகளை எளிதாக்குவதற்கு வங்கிக் கணக்குகளுக்குப் பதிவு செய்வார்கள்.

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சரிபார்க்க - நீங்கள் எதிர்நோக்கும் தூழ்நிலை ஒரு மோசடியா என்பது உறுதியாகத் தெரியாவிட்டால், மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைத்து உறுதிப்படுத்திக் கொள்ளவும்.

- வாட்ஸ்ஆப், டெலிகிராம் போன்ற செய்தி அனுப்பும் தளங்கள் வழியாகவோ அல்லது குறுஞ்செய்தி மூலமாகவோ உங்களுக்கு அனுப்பப்படும் Singpass உள்நுழைவு இணையத்தள முகவரி இணைப்புகளைக் கிளிக் செய்ய வேண்டாம். நீங்கள் Singpass வழியாக மின்னிலக்கச் சேவையை அணுக வேண்டும் என்றால், அமைப்பின் இணையத்தளம் வழியாக அவ்வாறு செய்யுங்கள்.
- உங்கள் Singpass மற்றும் வங்கி விவரங்கள், பற்று / கடன்பற்று அட்டை விவரங்கள், ஒரு முறை கடவுச் சொற்கள் ஆகியவை உங்கள் தனிப்பட்ட பயன்பாட்டிற்கானது. அவை குற்ற நடவடிக்கைகளுக்குப் பயன்படுத்தப்படலாம் என்பதால், அவற்றை மற்றவர்களுடன் பகிர்ந்துகொள்ள வேண்டாம்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தார், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். பொய்யான கருத்துகள் அல்லது

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



ADD

CHECK

TELL Authorities, family and friends



