2024 – Issue 10 8 Mar 2024

Weekly Scams Bulletin

Scammers impersonate legal or financial firms and target victims who have lost money to investments or scams. Scammers may reach victims via calls/messages/emails and use social media advertisements (e.g. Facebook) to promote their "fund recovery" services.

Scammers would instruct victims to make upfront payments via bank transfers, cryptocurrencies, or virtual credits, claiming these as "administrative procedures". Scammers may also access victims' mobile devices and bank accounts by requesting victims to:

a. Download software like AnyDesk; or
b. Share their banking credentials, debit/credit card details, or One-Time Passwords (OTPs)

Victims would realise they had been scammed when their funds are not recovered, scammers became uncontactable, or after checking with their banks or the Police.

Some Precautionary Measures:

ADD – Two-Factor or Multifactor Authentication for your banks and online accounts. Set transaction limits for internet banking transactions, including PayNow). Secure a portion of your bank savings with Money Lock.

CHECK – if the law firm is registered with the Legal Services Regulatory Authority (LSRA) using the LSRA directory at https://eservices.mlaw.gov.sg/lsra/search-lawyer-or-law-firm/. If the advertised law firm is not registered, it is likely to be a scam.

- 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 believe companies that claim to be able to recover the monies you have lost.
- Do not share your banking credentials, debit/credit card details, or One-Time Passwords (OTPs) with others.

TELL – the authorities, family, and friends about scams. Report any fake comments or postings to the online platform administrators.

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

诈骗周报

骗子冒充律师所或财务公司，以因投资或诈骗而蒙受损失的受害者为目标。骗子可能通过电话/短信/电邮接触受害者，并利用社交媒体广告（例如脸书）来推广他们的“资金追回”服务。

骗子会指示受害者通过银行转账、加密货币或虚拟信用等方式预付款项，声称这些是“行政程序”。骗子还可能通过要求受害者:

a. 下载如 AnyDesk 之类的软件；或

b. 分享他们的银行凭据、借记/信用卡信息或一次性密码 (OTP),

以进入受害者的移动设备和银行账户。

当受害者发现资金没有被追回、骗子失联、或者向银行或警方核实后，才意识到自己被骗了。

一些预防措施：

添加 – 为银行及网上账户设置双重或多重认证。为网络银行设置交易限额，包括 PayNow。使用 Money Lock 保护您银行存款的一部分。

查证 – 使用法律服务管制局 (LSRA) 注册名单 https://eservices.mlaw.gov.sg/lsra/search-lawyer-or-law-firm/ 查证律师所是否已在法律服务管制局注册。

- 如果所宣传的律师所未注册，那可能是那可能是骗局。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。
- 不要相信声称能够帮您找回失去资金的公司。
- 不要与他人分享您的银行凭据、借记/信用卡信息或一次性密码（OTP)。

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)

Buletin Penipuan Mingguan

Penipu menyamar sebagai firma guaman atau syarikat perkhidmatan kewangan dan menyasarkan mangsa yang telah kehilangan wang akibat pelaburan atau penipuan. Penipu mungkin menghubungi mangsa melalui panggilan, mesej atau e-mel dan menggunakan iklan media sosial (contohnya, Facebook) untuk mempromosikan perkhidmatan "pemulihan dana" mereka.

Penipu akan mengarahkan mangsa untuk membuat bayaran pendahuluan melalui pemindahan bank, mata wang kripto, atau kredit maya, dan mendakwa ia adalah sebahagian daripada "prosedur pentadbiran". Penipu juga mungkin mengakses peranti mudah alih dan akaun bank mangsa dengan meminta mangsa untuk:

a. Memuat turun perisian seperti AnyDesk; atau

b. Berkongsi butiran perbankan, butiran kad debit atau kredit, atau Kata Laluan Guna Sekali (OTP) mereka

Mangsa akan menyedari mereka telah ditipu apabila dana mereka tidak dikembalikan, penipu tidak dapat dihubungi lagi, atau selepas memeriksa dengan bank-bank mereka atau polis.

Beberapa langkah berjaga-jaga:

MASUKKAN – Pengesahan Dua-Faktor atau Pengesahan Pelbagai Faktor untuk bank dan akaun dalam talian anda. Tetapkan had transaksi untuk transaksi perbankan internet, termasuklah PayNow). "Kuncikan" sebahagian daripada wang simpanan dalam bank anda dengan Money Lock.

PERIKSA – sama ada firma guaman itu berdaftar dengan Penguatkuasaan Kawal Selia Perkhidmatan Perundangan (LSRA) melalui direktori LSRA di https://eservices.mlaw.gov.sg/lsra/search-lawyer-or-law-firm/. Jika firma guaman yang diiklankan tidak berdaftar, kemungkinan ianya merupakan penipuan.

- Hubungi talian bantuan Anti-Penipuan di 1800-722-6688 sekiranya anda tidak pasti jika situasi yang sedang anda hadapi ialah satu penipuan.
- Jangan percaya kepada syarikat-syarikat yang mendakwa boleh mendapatkan semula wang anda yang telah hilang.
- Jangan berkongsi butiran perbankan, butiran kad debit atau kredit, atau Kata Laluan Guna Sekali (OTP) anda dengan sesiapa.

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

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

வாராந்திர மோசடிகள்

மோசடிக்காரர்கள் சட்ட அல்லது நிதி நிறுவனத்தைப்போல் ஆள்மாறாட்டம் செய்து, முதலீடுகளில் அல்லது மோசடிகளில் பணத்தை இழந்தவர்களைக் குறி வைக்கின்றனர். இந்த மோசடிக்காரர்கள் தொலைபேசி அழைப்புகள் / குறுந்தகவல்கள் / மின்னஞ்சல்கள் மூலம் பாதிக்கப்பட்டவர்களை அணுகுகின்றனர். அதோடு, சமூக ஊடக விளம்பரங்களை (எ.கா. ∴பேஸ்புக்) பயன்படுத்தி தங்களது "நிதி மீட்புச்" சேவைகளை விளம்பரப்படுத்துகின்றனர்.

மோசடிக்காரர்கள் வங்கிப் பணமாற்று, க்ரிப்டோ நாணயம், அல்லது மெய்நிகர் பற்றுத்தொகை மூலம் முன்பணம் செலுத்தும்படி பாதிக்கப்பட்டவர்களிடம் சொல்வார்கள். இது "நிர்வாக நடைமுறை" என்று அவர்கள் கூறுவார்கள். பாதிக்கப்பட்டவர்களின் கைப்பேசிகளையும் வங்கிக் கணக்குகளையும் ஊடுருவ, அவர்களிடம் மோசடிக்காரர்கள்:

a. "AnyDesk" போன்ற மென்பொருளைப் பதிவிறக்கம் செய்யச் சொல்லலாம்; அல்லது

b. தங்களது வங்கிக்கணக்கு விவரங்கள், ரொக்கக்கழிவு / கடன் அட்டை விவரங்கள், அல்லது ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTPs) ஆகியவற்றைப் பகிரச் சொல்லலாம்

பாதிக்கப்பட்டவர்கள் ஏற்கனவே இழந்த நிதி மீட்டுக் கொடுக்கப்படாதபோது, மோசடிக்காரர்களுடன் தொடர்புகொள்ள முடியாமல் போகும்போது, அல்லது வங்கிகளிடமோ காவல்துறை அதிகாரிகளிடமோ விவரம் கேட்டறிந்த பிறகே தாங்கள் மோசடிக்கு உள்ளாகியிருப்பதை உணர்வார்கள்.

சில முன்னெச்சரிக்கை நடவடிக்கைகள்:

சேர்க்க - ஸ்கேம்ஷீல்டு செயலியைப் பதிவிறக்கம் செய்து, பாதுகாப்பு அம்சங்களை அமைத்திடுங்கள் (எ.கா. வங்கிகளுக்கு இரட்டை மறைச்சொல் முறையையும் (2FA) பன்முக உறுதிப்பாட்டையும் செயல்படுத்தலாம். PayNow உள்ளிட்ட இணைய வங்கிப் பரிவர்த்தனைகளுக்கு வரம்புகளை நிர்ணயிக்கலாம். உங்கள் வங்கிச் சேமிப்பின் ஒரு பகுதியை 'Money Lock' மூலம் ஒதுக்கி வைத்து பாதுகாக்கலாம்.

சரிபார்க்க - விளம்பரம் செய்த சட்ட நிறுவனம், சட்டச் சேவைகள் கட்டுப்பாட்டு ஆணையத்தில் (LSRA) பதிவு செய்துள்ள நிறுவனமா என்பதை https://eservices.mlaw.gov.sg/lsra/search-lawyer-or-law-firm/ இணையத்தளத்தில் கிடைக்கும் LSRA தகவல் தொகுப்பைப் பயன்படுத்தி சரிபார்க்கவும். விளம்பரப்படுத்தப்பட்ட சட்ட நிறுவனம் பதிவு செய்யப்படாவிட்டால் அது மோசடியாக இருக்கக்கூடும்.

- நீங்கள் எதிர்நோக்கும் சூழ்நிலை ஒரு மோசடியா என்பது உறுதியாகத் தெரியாவிட்டால், மோசடித்தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைத்து உறுதிப்படுத்திக் கொள்ளவும்.
- நீங்கள் இழந்த பணத்தைத் தங்களால் மீட்டுத் தரமுடியும் என்று சொல்லும் நிறுவனங்களை நம்பாதீர்கள்.
- உங்களது வங்கிக்கணக்கு விவரங்கள், ரொக்கக்கழிவு / கடன் அட்டை விவரங்கள், அல்லது ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTPs) எதனையும் மற்றவர்களுடன் பகிராதீர்கள்.

சொல்ல - மோசடிகளைப் பற்றி அதிகாரிகள், குடும்பத்தார், நண்பர்கள் ஆகியோரிடம் சொல்லுங்கள். பொய்யான கருத்துகள் அல்லது பதிவுகளைப் பற்றி இணையத்தள நிர்வாகிகளிடம் புகார் செய்யுங்கள்.

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