Joint advisory on government official impersonation scam

The Singapore Police Force (SPF) and the Central Provident Fund Board (CPFB) would like to alert the public on a Government Official Impersonation Scam variant. In December 2023, there have been at least 120 victims reported falling prey to Government Officials Impersonation Scam (GOIS), with total losses amounting to at least $13.3 million. Of which, there were three cases involving about $488,000 in CPF withdrawals that were made from November to December 2023. The typical modus operandi of this scam variant is:

1. Victims would receive unsolicited calls from scammers impersonating bank officers and seeking validation of suspicious banking transactions that they allegedly conducted. When victims denied making such transactions or possessing such bank cards, the scammer would transfer the call to another scammer claiming to be a Government official (e.g., SPF, China official). This second scammer would accuse victims of being responsible for criminal activities (e.g., fraud, money laundering).

2. Under various pretexts (e.g., support investigations, prevent abuse of bank or CPF accounts), scammers would instruct victims to transfer their monies to “security accounts”, specified bank accounts supposedly designated by the “authorities”. They may also request for victims’ banking credentials, credit card details, or One-Time Passwords (OTPs). In the three cases involving CPF withdrawals, scammers instructed victims to withdraw CPF monies into victims’ bank accounts, and subsequently instructed victims to make further transfers or provide banking credentials.

3. Victims would realise that they had been scammed when the scammers become uncontactable or when they subsequently verify their situation with the banks or with SPF through official channels.

Government officials will never ask members of the public over the phone to (i) transfer monies to them; (ii) provide their banking credentials or CPF-related information such as CPF balances. Members of the public are advised to adopt the following precautionary measures:

ADD - ScamShield App to protect yourself from scam calls and SMSes. Set security features (e.g. set up transaction limits for internet banking transactions, enable Two-Factor Authentication (2FA), Multifactor Authentication for banks and e-wallets).

CHECK - For scam signs with official sources (e.g., ScamShield WhatsApp bot @ https://go.gov.sg/scamshield-bot, call the Anti-Scam Helpline on 1800-722-6688, or visit www.scamalert.sg). Never disclose your internet/mobile banking or credit card details such as bank account user ID, passwords, Personal Identification Numbers (PINs) or OTPs to anyone through phone, email or SMS/messaging applications. Do not allow anyone to access your bank account(s) or Singpass, and do not authorise any authentication request via digital token or OTP if you did not initiate any internet/mobile banking transaction.

TELL - Authorities, family, and friends about scams and do not be pressured by the caller to act impulsively. Report any fraudulent transactions to your bank immediately!

CPF Board has recently implemented a suite of security measures which include setting $2,000 as the default daily limit for online CPF withdrawals, with the option to disable online withdrawals completely by activating the CPF Withdrawal Lock. Increases to the daily withdrawal limit will be subject to Singpass Face Verification and a 12-hour cooling period. These measures create friction for scammers and help to reduce losses, but ultimately, it is important that members of the public stay alert against the latest scam tactics and avoid falling prey.

If you have any information relating to such crimes or if you are in doubt, please call the Police Hotline at 1800-255-0000, or submit it online at www.police.gov.sg/iwitness. All information will be kept strictly confidential. If you require urgent Police assistance, please dial ‘999’.

For more information on scams, members of the public can visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688. Fighting scams is a community effort. Together, we can ACT Against Scams to safeguard our community!
