



## **POLICE NEWS RELEASE**

---

### **POLICE ADVISORY ON SCAM TARGETING STEAM ACCOUNT USERS**

The Police have observed a trend where scammers would target users of the digital platform, Steam. Steam is a digital distribution platform for video games, and consists of a gaming community where players and game developers can buy and sell video games online. The scammers leverage compromised Steam accounts to convince the victims to make payment to unlock their accounts, which the scammers claimed had been accidentally reported for fraudulent activity.

2 In these cases, scammers would approach the victims through compromised Steam accounts and would claim that they had accidentally reported the victims' Steam accounts while trying to report another Steam user. Thereafter, under the pretext of rectifying the wrongful reporting, the scammers would request for the victims to contact a specific user who was purportedly a platform administrator through the platform's chat function or external chat platforms, to verify and unblock their accounts. The fake administrator would then instruct the victims to log out of their Steam accounts and provide their account login details, including their One-Time Password (OTP), to verify their account. Thereafter, victims would be required to make game-related transactions or make purchases on third party websites as part of the verification review. In some cases, the victims were asked to purchase Steam cards and hand over the redemption code to the fake administrator to unblock their accounts. The fake administrator would claim that the victims would receive a refund after their accounts had been verified. Victims would later realise that they had been scammed when they discovered that they were subsequently unable to log in to their Steam accounts and no refund was received.

3 Members of the public are advised to adopt the following crime prevention measures:

- a. Never give out your account login details and OTP to anyone, including family and friends;
- b. Always verify the authenticity of the information received with official sources;
- c. Report any fraudulent credit/debit card charges to your bank and cancel your card immediately.

4 If you have information related to such crimes or if you are in doubt, please call the Police hotline at [1800-255-0000](tel:1800-255-0000), or submit it online at [www.police.gov.sg/iwitness](http://www.police.gov.sg/iwitness). Please dial '999' if you require urgent Police assistance.

5 For more information on scams, members of the public can visit [www.scamalert.sg](http://www.scamalert.sg) or call the Anti-Scam Hotline at [1800-722-6688](tel:1800-722-6688). Join the 'Spot the Signs. Stop the Crimes' campaign at [www.scamalert.sg/fight](http://www.scamalert.sg/fight) by signing up as an advocate to receive up-to-date messages and share them with your family and friends. Together, we can help stop scams and prevent our loved ones from becoming the next victim.

**PUBLIC AFFAIRS DEPARTMENT  
SINGAPORE POLICE FORCE  
9 MAY 2021 @ 10.00am**

## Messages exchanged between scammer and victim



Members of the public are advised to verify the claim through other official means.  
Never reveal your account login details or OTP to anyone.