

JOINT ADVISORY BY THE CYBER SECURITY AGENCY OF SINGAPORE AND SINGAPORE POLICE FORCE

PROTECTING YOURSELF FROM COMPROMISED PAYPAL ACCOUNTS

The Police and CSA have observed a recent spate of cases involving cybercriminals using compromised PayPal accounts for transactions. From 1 Jan to 9 Feb 2024, a total of 27 cases were reported to the Police.

In these cases, victims would receive automated notifications from PayPal either in the form of emails or PayPal's inbox messages, informing them of various activities such as profile changes and receipts for transactions on their account. Upon checking their PayPal accounts, some victims discovered that funds from unknown sources were deposited, or that funds were being transferred to unfamiliar bank accounts added by the cybercriminals. Subsequently, the cybercriminals would initiate a chargeback request. The victims would then receive an automated notification, and funds were recovered from their accounts, resulting in a deficit balance.

The compromise of online credentials and passwords could be due to several reasons which include:

- a. Using weak passwords.
- b. Visiting phishing websites that ask for your online credentials and/or passwords, and downloading unverified apps sent via emails, SMSes, text messages or messages from social media platforms.
- c. Visiting websites or downloading files that are infected with malware designed to steal victims' credentials.
- d. Re-using the same password for multiple online accounts (When online services or platforms are involved in data breach incidents, it may cause your reused online credentials and passwords to be compromised).

The safe use of online payment platforms must be accompanied by strong cyber hygiene practices by the users to ensure that their online credentials and passwords are secured. Members of the public are advised to adopt the following precautionary measures and cyber hygiene tips:

- a. **ADD** security features to your PayPal account by enabling passkeys and two-step verification (2FA). Passkeys are a secure login standard allowing you to log in to PayPal using the same biometrics or device password you use to unlock your device. This can be done by logging in to PayPal from your mobile device using either Safari or Chrome browsers. Upon login, you will be presented with the option to create a passkey. Follow the steps on the screen.

2FA can also be enabled through PayPal's website as an extra precaution. Do note that you can do so by logging into your PayPal account through the web browser and not through the PayPal App. Go to 'Settings' ◇ 'Security' ◇ 'Set Up' ◇ select 'Use an authenticator app' ◇ click 'Set it Up' and following the steps on the screen.

Enable transaction alerts and review all transactions regularly for any suspicious activities. You are also strongly encouraged to install anti-virus apps on your devices that can detect malware and block access to phishing links. Please refer to Annex A on how to add these security features to PayPal accounts. CSA has also put together a list of recommended apps available at <https://www.csa.gov.sg/Tips-Resource/Resources/recommended-security-apps-list>;

- b. **CHECK** that you are using a strong password for your PayPal account. A strong password should consist of at least 12 characters with uppercase and lowercase letters, numbers or symbols. Use different passwords for each of your online accounts. Even if your PayPal account is inactive, you should still change your passwords from time to time as a best practice.

Remove any devices that you no longer use or do not recognise in your PayPal account's "trusted device" list by reviewing and turn off "auto-login" for your PayPal account. Turn on and monitor automated transaction notifications in your PayPal account. Be wary of unusual requests received that ask for your personal information, banking details and OTPs. You should not share your personal information with anyone. Do not click on any suspicious links, download unknown attachments or apps received via emails, SMSes, text messages or messages through social media platforms. They may contain phishing links or malicious programmes / apps used to steal data from your devices;

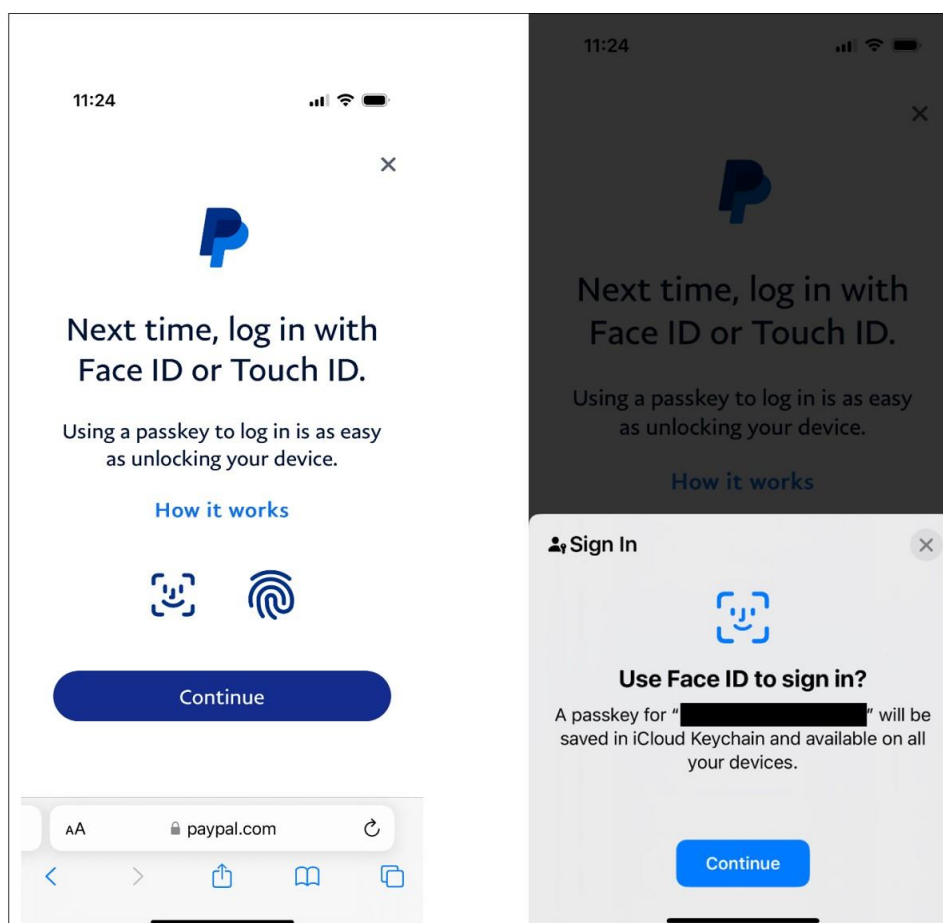
- c. **TELL** authorities, family, and friends about scams. Report any fraudulent transactions to PayPal at spoof@paypal.com or your bank immediately.

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!

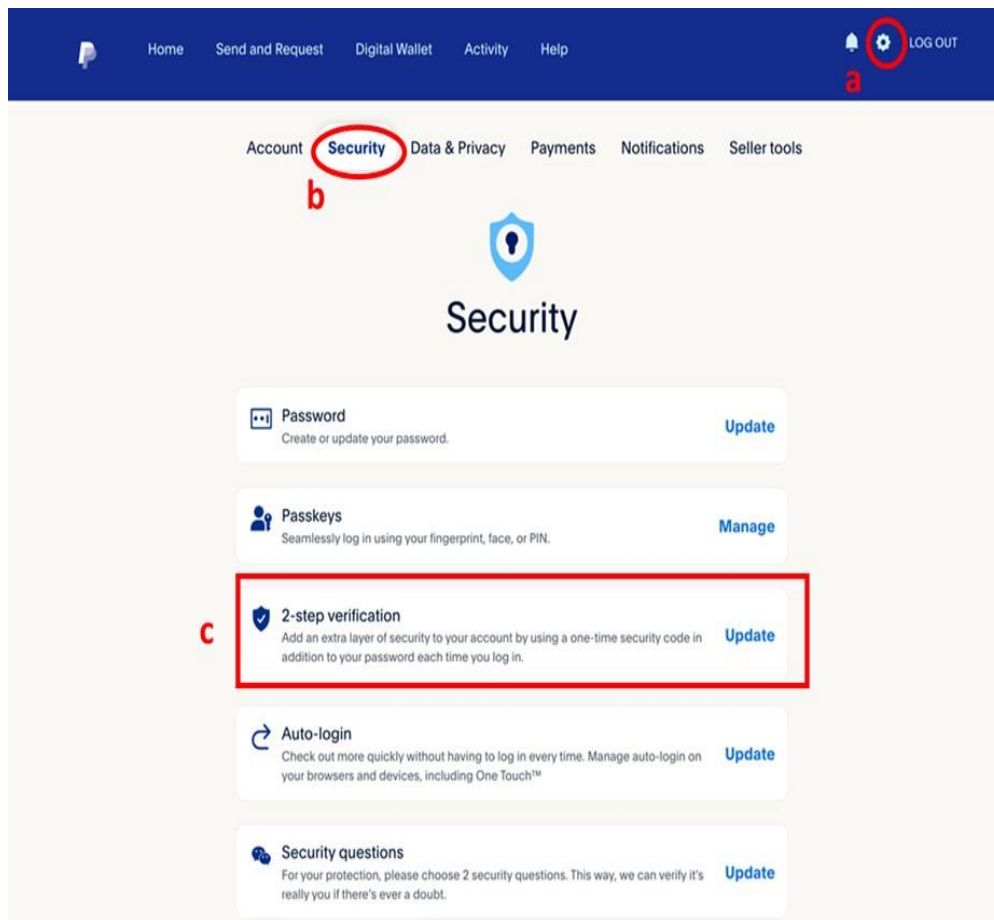
Annex A

Setting up a passkey for PayPal accounts ▼



Setting up 2FA for PayPal accounts ▼

1. Log in to your PayPal account through your web browser (and not the PayPal app).
2. Click the 'Settings' icon (a).
3. Click 'Security' near the top of the page (b).
4. Click 'Set Up' / 'Update' to the right of '2-step verification' (c).
5. Select 'Use an authenticator app', click 'Set it Up' and follow the steps on the screen.



Review and turn off auto-login in PayPal ▼

Manage auto-login, including One Touch™

You can turn off auto-login from any browser or device you no longer use or recognise.

You're logged in on the following devices:

Desktop Edge Windows	Turn off
Phone Chrome Mobile Android 9	Turn off
Phone Chrome Mobile Android 9	Turn off

[Log out of all devices](#)

Done



Switch on automated notifications (for PayPal business accounts) ▼

1. Log in to your PayPal business account through your web browser (and not the PayPal app).
2. At the top right corner, click your business name and select 'Account settings' (a).
3. On the left sidebar, click 'Notifications' (b).
4. On the right, next to "Notifications", click 'Update' (c).
5. Select the relevant alerts you wish to receive (d).

Account Settings

ACCOUNT & SECURITY

- Account access
- Account preferences
- Payment preferences

BUSINESS PROFILE

- Business information
- Account owner information
- Money, banks and cards

Notifications

Notifications

Notifications

Manage alerts sent when you change account information, or when you have discounts or special offers.

[Update](#)

Instant payment notifications

Integrate PayPal payment notifications with your website.

[Update](#)

Alerts about activities in your account

You can choose whether or not you want to receive notifications for the following.

- Request money
- Receive a payment

We'll always send you notifications when you Send money

We'll send you notifications when a secondary user in your account

- Change business information
- Change account owner password or an answer to a security question.
- Add or remove a credit card
- Add or remove a street address
- Add or remove a bank account

 We've saved your preference.