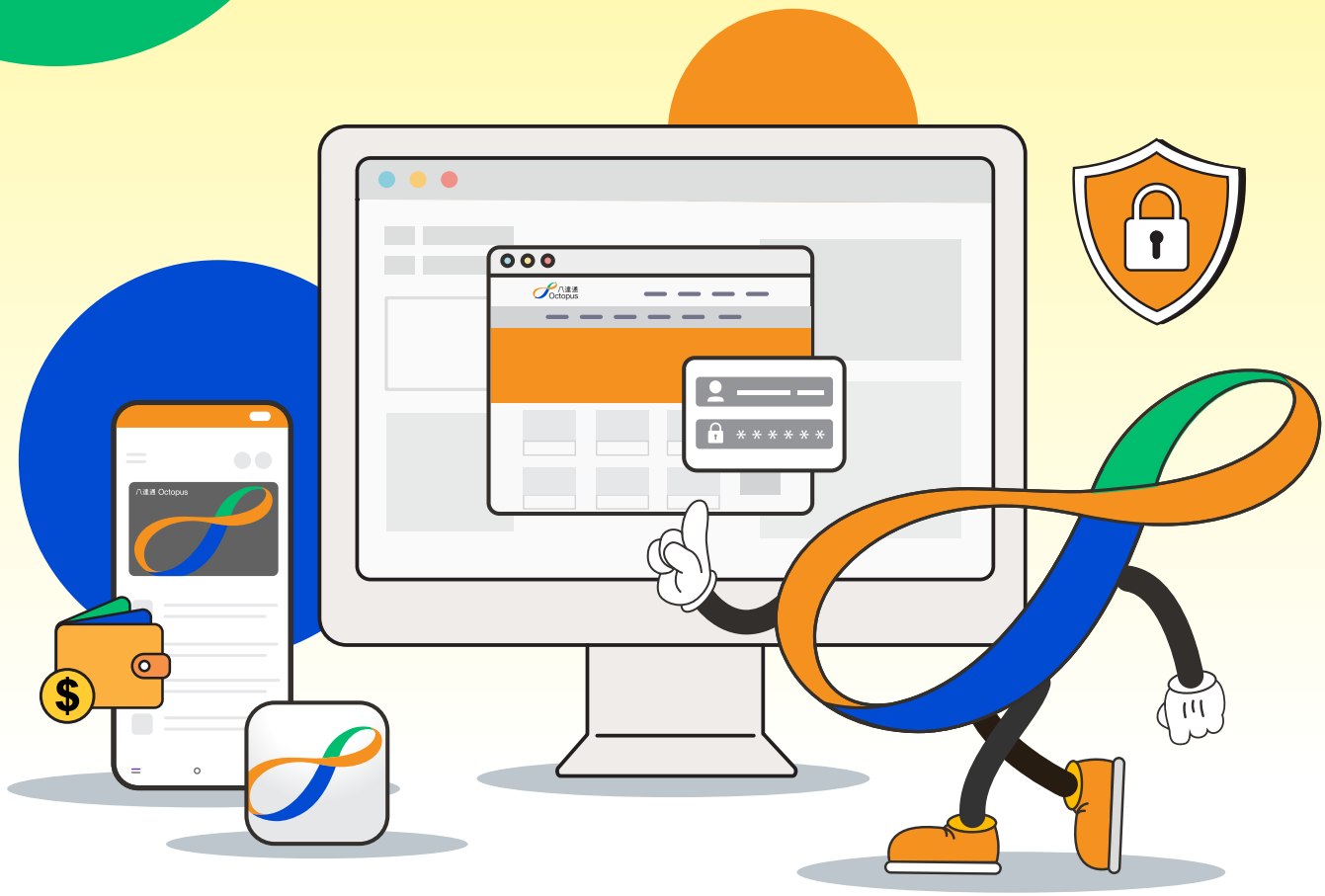


Octopus Online Service Safety Tips

Next page

八達通 Octopus

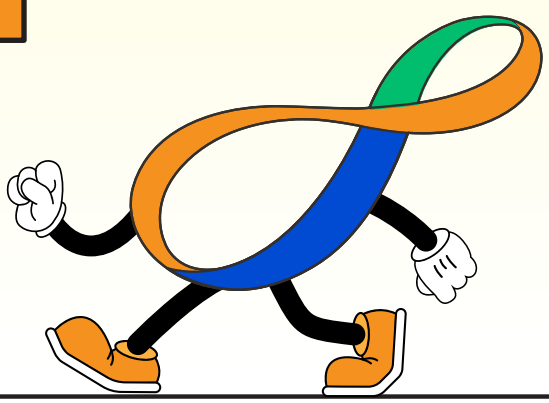
Octopus Service Hotline 2266 2222
www.octopus.com.hk/en

License number：**SVF0001**

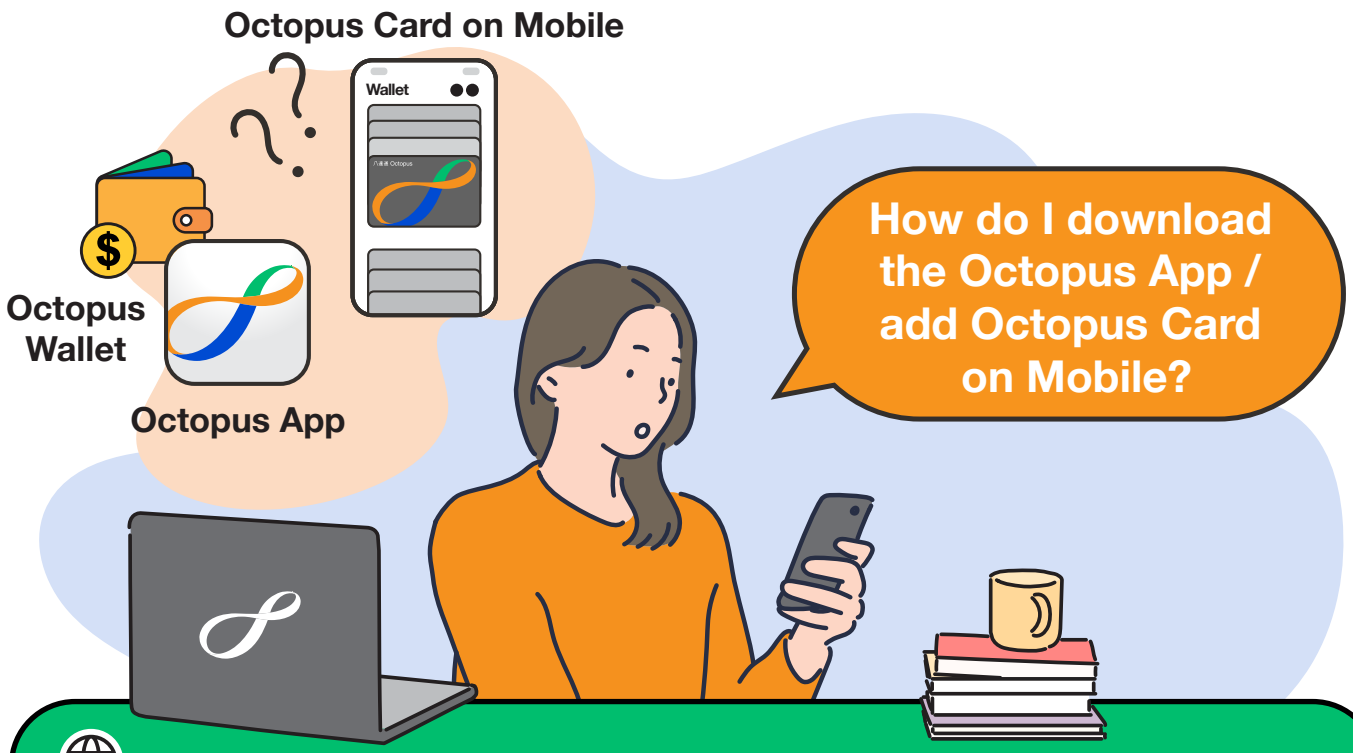
Stay smart online! Discover security tips and reminders for using the online and mobile services of Octopus Cards Limited (OCL).

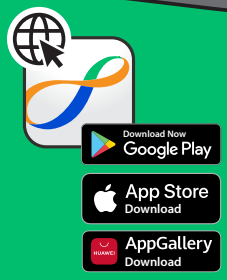
Contents

Next page



Download the Octopus App or add Octopus Card on Mobile

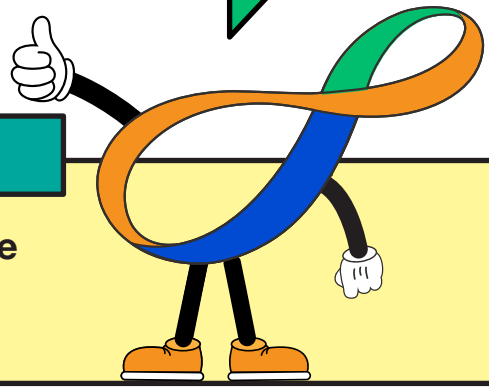




1 You can **download the Octopus App or Octopus App for Tourists** from the OCL website at www.octopus.com.hk/en or **authorised app stores** (such as Google Play Store, Apple App Store or HUAWEI AppGallery).

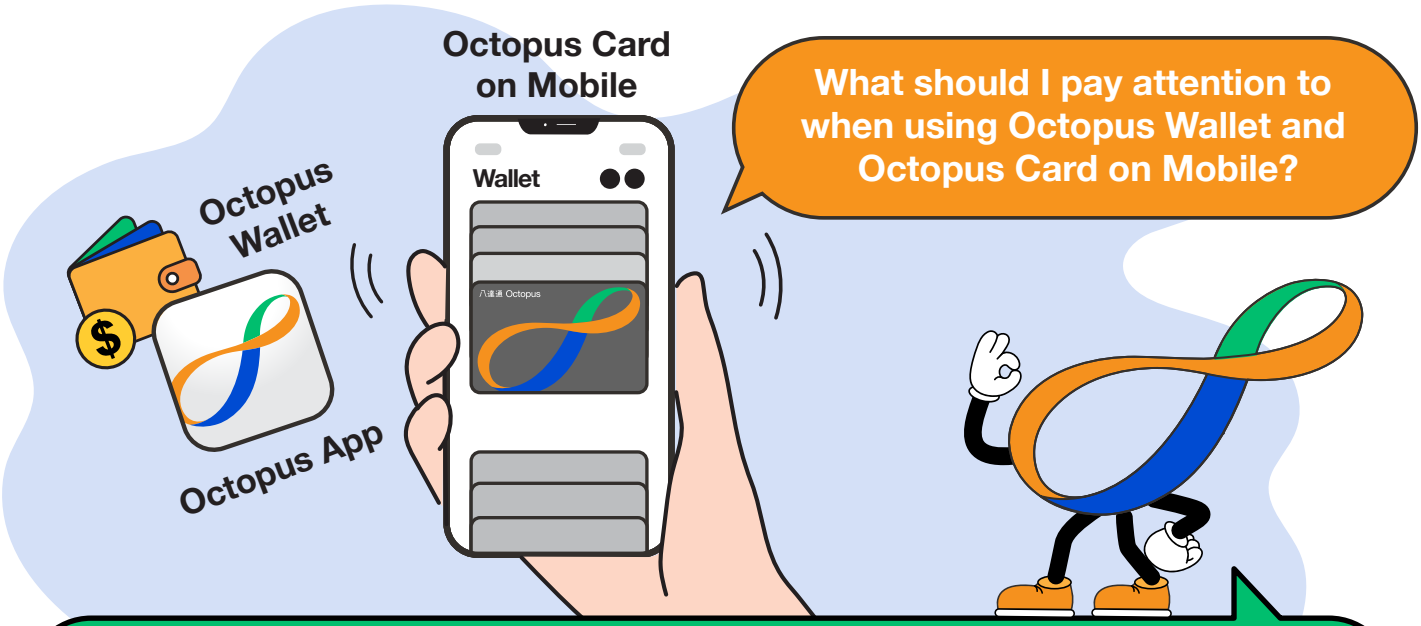
2 To use **Octopus Card on Mobile** (including Octopus on iPhone or Apple Watch, Octopus on Android, Huawei Pay Octopus or Smart Octopus in Samsung Pay), **you should download an authorised mobile payment app from an authorised app store and add Octopus as a mobile payment.**

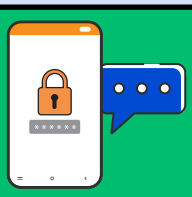
DOWNLOAD TIPS from Octoboy



To apply for an Octopus Wallet, please ensure that you apply it through the official Octopus App.

Tips for using Octopus Wallet and Octopus Card on Mobile





1 You should create a **strong account password** and keep both this password and your **one-time password (OTP)** safe. Do not write them down, and **remember to change your account password on a regular basis.**

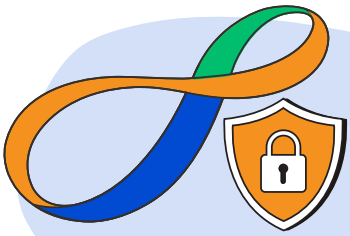
2 You can use fingerprint, face recognition or other biometric authentication on your mobile device to conduct transactions or access other Octopus App functions. Biometric data is solely stored on your mobile device and is never collected by OCL.

3 When other users invite you as a friend in Octopus Wallet, their mobile phone number will be displayed on the screen. **Please verify that the user is someone you know before accepting their request.**

4 **Notifications such as payment requests and payment reminders from Octopus Wallet will only be sent and received directly in the Octopus App. They are never sent via email or SMS.**

5 Before accepting a payment request or sending a P2P payment with Octopus Wallet, **review the payment details carefully – including the recipient and the payment amount.** All payment transactions in Octopus Wallet are irreversible upon confirmation of the payment instruction.

Security measures to protect Octopus customers



How does Octopus protect the security of my account?

1. After five invalid inputs, the Octopus App will be suspended for 24 hours.

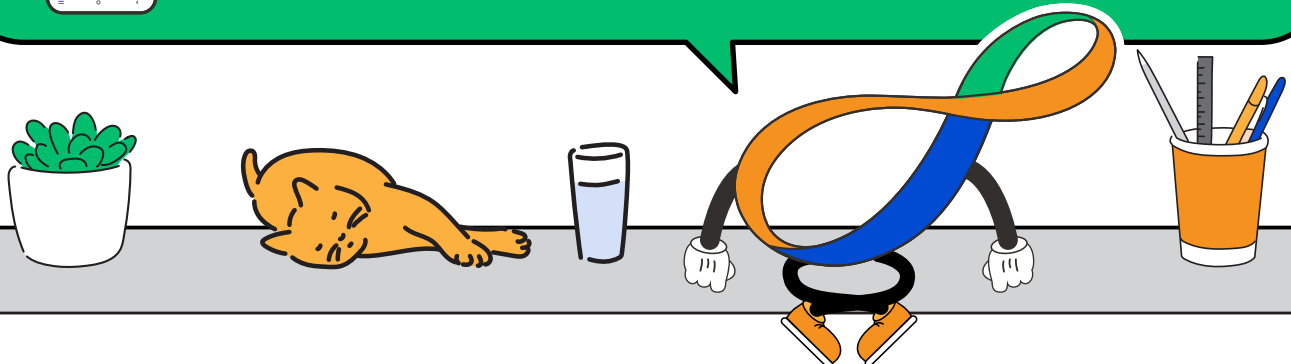
2. If your mobile device is detected to be “rooted” or “jail-broken”, the Octopus App will be suspended.

3. OCL will never ask you to validate your personal and/or account related information (such as registered email address or login password) through emails or SMS, or any hyperlinks embedded in emails or SMS.

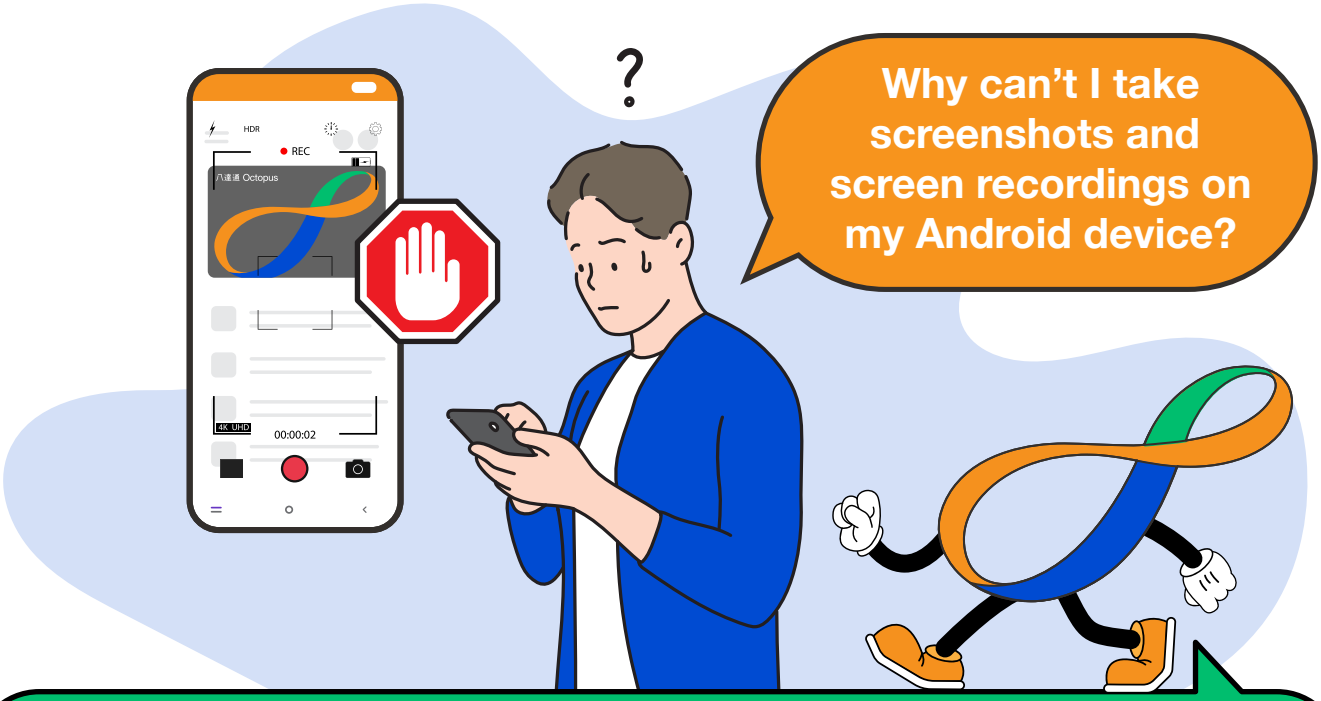
4. When you login the Octopus Wallet from a new mobile device, or when you increase your daily transaction limit, or when you make high risk transactions, a verification code and the purpose of the verification code will be sent to your registered mobile number via SMS. Please review the content of the SMS before entering the verification code in the Octopus App.

5. After each transaction completed with Octopus on Mobile, a push notification with transaction information will be sent to you. You can check your transaction records via your device’s Octopus App, Octopus App for Tourists, or authorised mobile payment app regularly.

6. To help you identify Octopus SMS instantly, we have joined the “SMS Sender Registration Scheme”, using registered sender IDs #Octopus and #OctopusOTP when sending SMS to local mobile users. If you receive SMS claiming to be from "Octopus" and the sender ID doesn’t start with "#", please be vigilant.

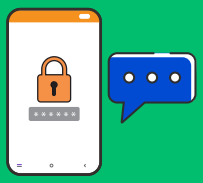


REC



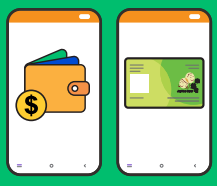
To protect the security of your account, the screen mirroring, capturing and recording features of Octopus App on Android devices are suspended in the following three scenarios:

- The input of any login credentials, including but not limited to user ID, password and OTP.



- Display of direct payment information, including but not limited to Octopus MasterCard number, Octopus UnionPay QR code and eLaisee QR code.

- Screens showing or involving the input of sensitive customer information, including but not limited to the application of services such as JoyYou Card and Octopus Wallet Upgrade via electronic Know-Your-Customer (eKYC).



What safeguard measures should I take?

1. **Never share with anyone your verification codes and OTP received via SMS or Push Notification.**

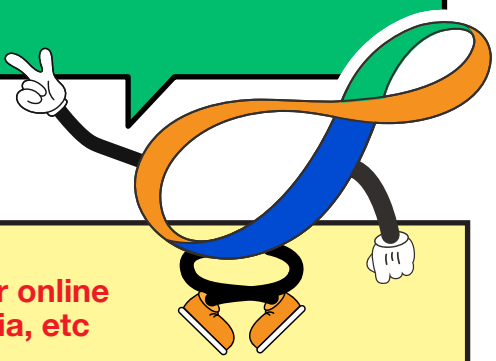
2. **Do not open any emails or SMS with a link requesting you to make a payment transaction or provide your personal data. OCL does not embed links in emails or SMS for these purposes and will never ask you to provide your credit card information.**

3. **Do not "jailbreak", "root" or "modify" the operating systems of your device. These actions will make your device vulnerable to computer viruses and spyware attacks that might cause harm or the theft of your personal information.**

4. **Always enable the screen lock function to prevent others accessing your personal information.**

5. **Regularly update your operating system and Internet browser. Use the latest versions of operating systems and mobile apps. Download and apply security patches for prompt protection against known security vulnerabilities.**

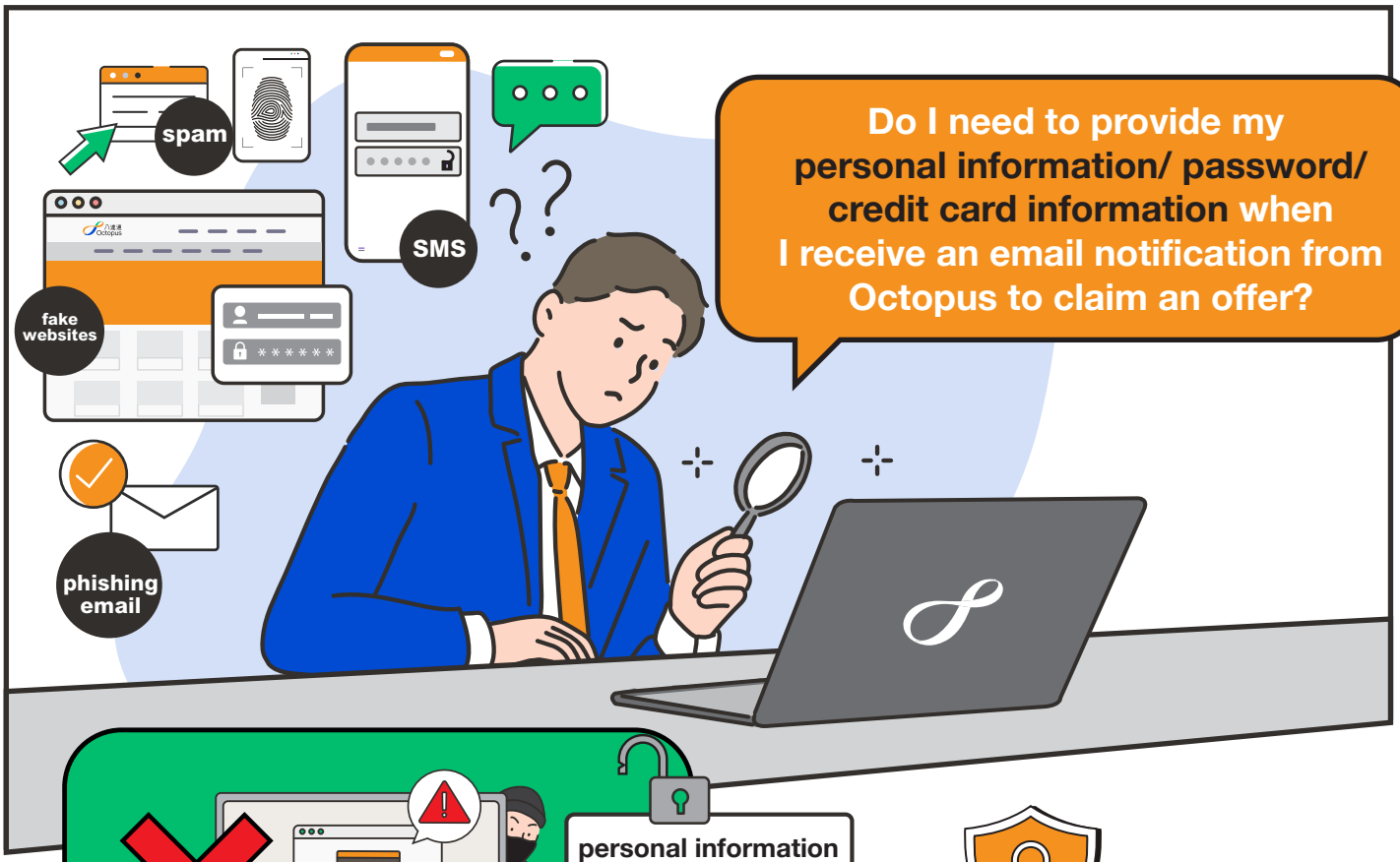
6. **If you have any questions or notice any suspicious activities when using Octopus Online Services, please call the Octopus Customer Service Hotline at 2266 2222 immediately. Please note that OCL will never ask you for your password.**

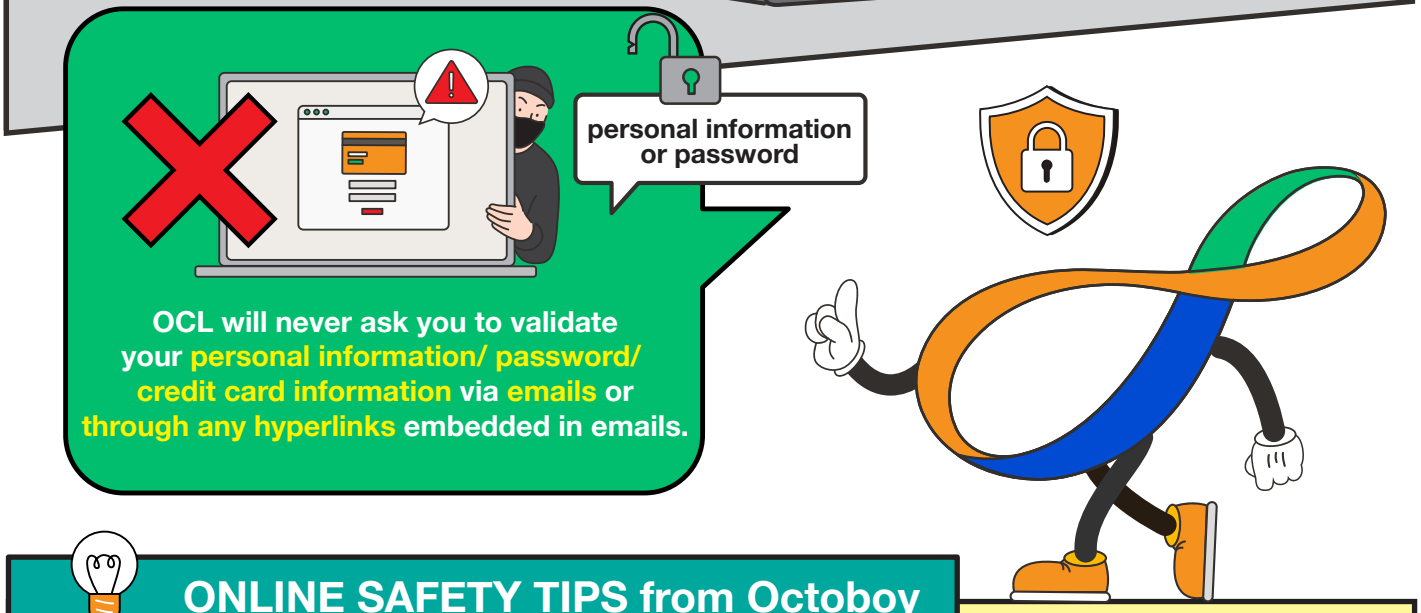


PASSWORD TIPS from Octoboy

- ✗ **Avoid using the same password for accessing other online services, such as online banking, email, social media, etc**
- ✗ **Do not create your password with personal information (e.g., your contact numbers, date of birth, HKID card number).**
- ✗ **Do not write down your password or store your password on any computer or mobile device.**
- ✓ Change your password regularly.

Beware of fake/ phishing emails, SMS, social media posts, spam emails, fraudulent websites and mobile apps





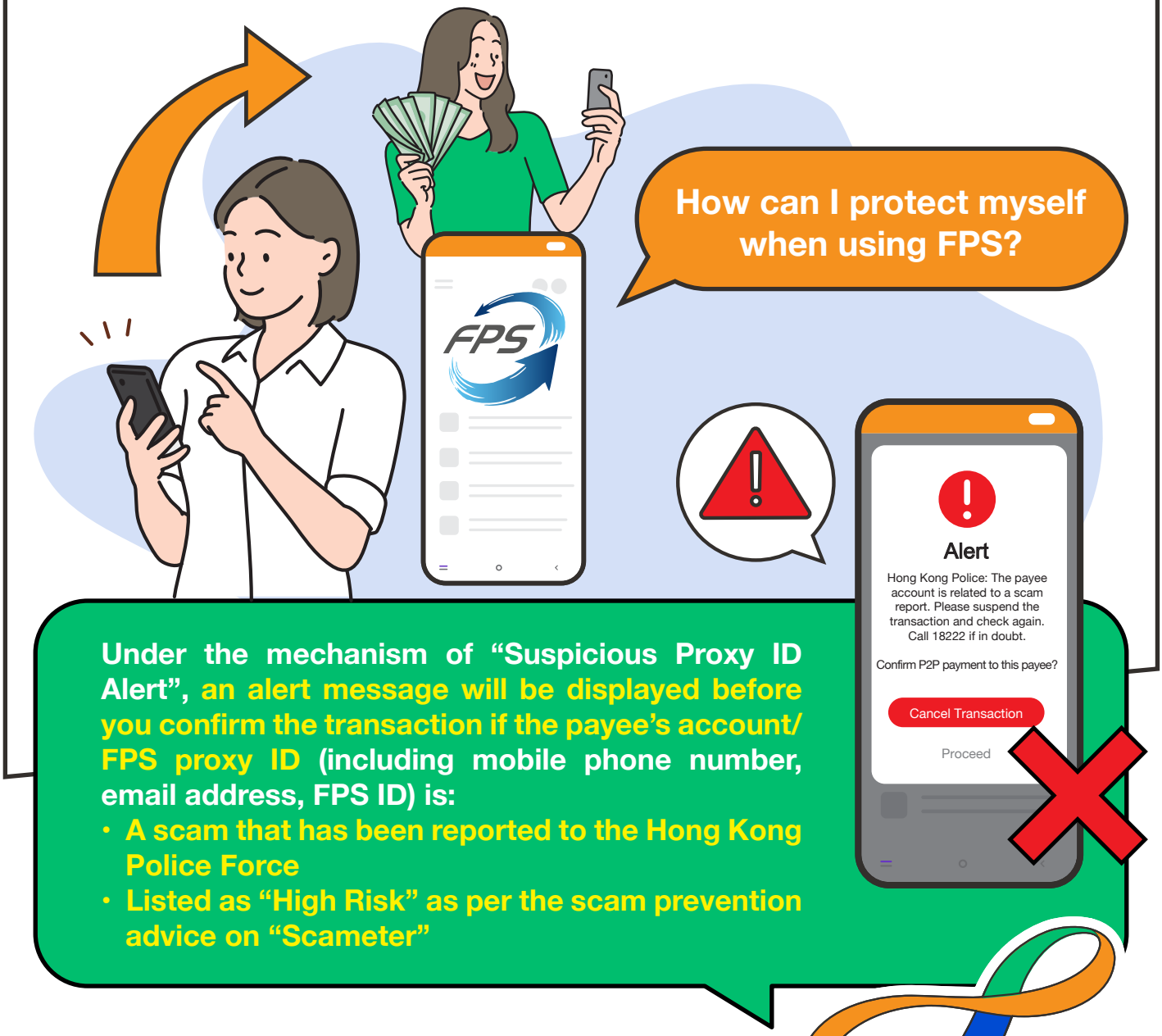
ONLINE SAFETY TIPS from Octoboy

Do not open, reply to or click on fraudulent emails or SMS.

To help you identify Octopus SMS instantly, we have joined the “SMS Sender Registration Scheme”, using registered sender IDs #Octopus and #OctopusOTP when sending SMS to local mobile users. If you receive SMS claiming to be from "Octopus" and the sender ID doesn’t start with "#", please be vigilant.

Always turn on the spam filtering function of your email software or use the related function provided by your webmail service provider, and always make sure that you are visiting the official OCL website.

Be cautious of the "Faster Payment System (FPS) Suspicious Proxy ID Alert"



Under the mechanism of "Suspicious Proxy ID Alert", **an alert message will be displayed before you confirm the transaction if the payee's account/ FPS proxy ID** (including mobile phone number, email address, FPS ID) is:

- **A scam that has been reported to the Hong Kong Police Force**
- **Listed as "High Risk" as per the scam prevention advice on "Scameter"**

FPS SAFETY TIPS from Octoboy

- ✓ Whenever you use the Faster Payment System (FPS), carefully verify the payment details and whether the payee identity is trustworthy before confirming the transaction.
- ✓ Use the most updated version of Octopus App containing the "FPS Suspicious Proxy ID Alert" feature.
- ✗ **If you receive an alert before confirming a transaction, you should consider it carefully before deciding whether to proceed with the transaction. If in any doubt, cancel the transaction immediately to avoid potential losses.**

To know more detailed security information about Octopus Online Services, please refer to the full version of the "Octopus Online Service Safety Guide" on the Octopus Cards Limited website, or click hyperlink below.

https://www.octopus.com.hk/en/document/online_safety.pdf