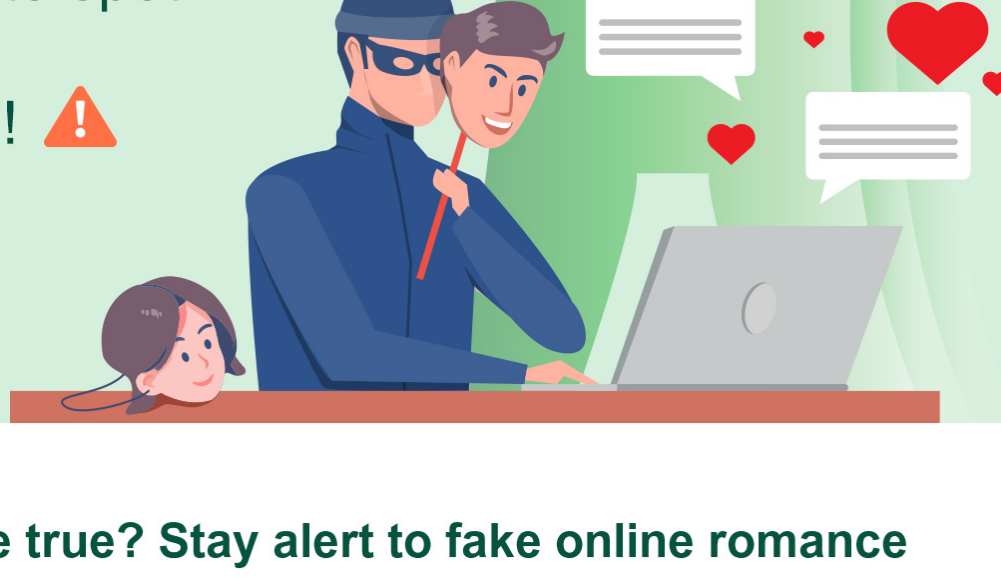


Check out how to spot "fakelovers, real scammers"!



Too perfect to be true? Stay alert to fake online romance

Fraudsters don't just target dating apps anymore - they're now preying on social media and instant messaging platforms, often starting with a random message to strike up a conversation. They'll patiently build a friendship with you, playing the long game to lure you into their trap.

Fake persona to win your heart

Scammers often create an appealing profile, pretending to be professionals, wealthy heirs or foreigners. They're also attentive and caring, always checking in and showering you with sweet talk to get you emotionally invested.



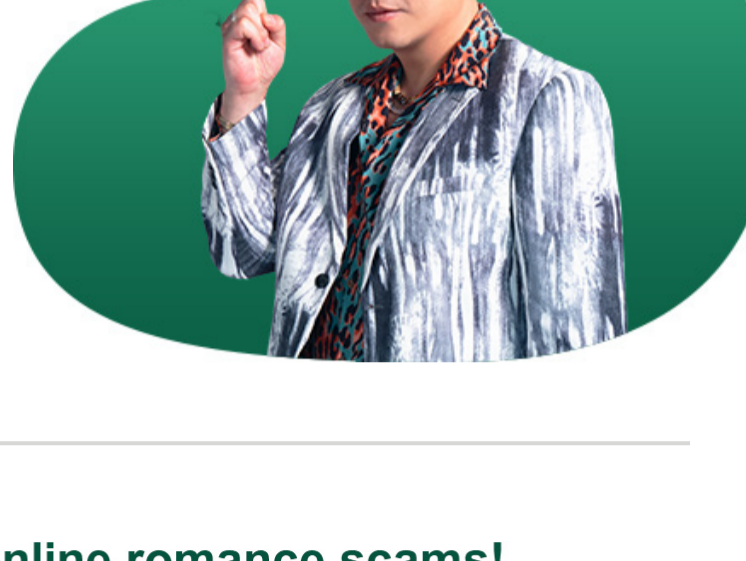
Fake excuses to request for money urgently

Once they've gained your trust, scammers create various scenarios to ask for money, such as business needs, car accidents, medical expenses or customs fees for gifts from overseas.



Fake promises to lure you into investments

The sweet talks and care of scammers will gradually make you fall for them. They'll use "let's plan for our future" as an excuse to lure you into investing or even hand over your bank account details and passwords.



It's not hard to spot online romance scams! Just remember these few tips:



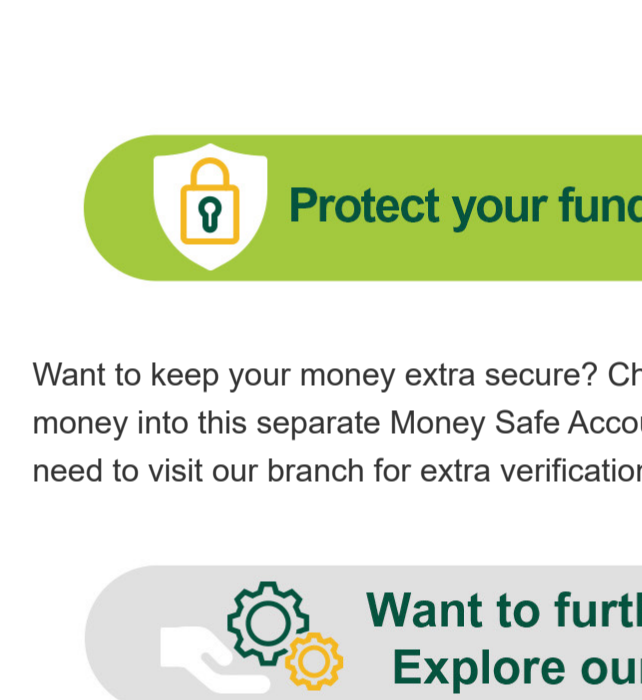
Beware the "perfect match"

Stay alert if they seem too good to be true, insist on only texting or calling and always make excuses not to meet up. Even if you've video called them, the video could be an AI deepfake and the person you see might not even be real.



Guard your privacy online

Never share sensitive personal or financial details with someone you've only met online, let alone sending intimate photos or engage in explicit video chats - these can be used for blackmail by scammers.









Don't rush to "give your heart and wallet"

If the conversation shifts from romance to requests for financial support, investment tips or account operations, take a step back and think critically. Don't lend money or follow so-called tips to invest or buy cryptocurrency.

Protect your funds with "Money Safe Account"

Want to keep your money extra secure? Check out Money Safe introduced by HKMA! Putting money into this separate Money Safe Account is just like locking money into a "safe", you'll need to visit our branch for extra verification to unlock it.

Want to further protect your account? Explore our other security features!

-  **What to do if you lose your credit or debit card when travelling?**
Block your card instantly using Hang Seng Mobile App to prevent losses! Report it and request a replacement card if confirmed lost. If the credit card is accidentally damaged during the trip, you can easily apply for a replacement card via the App.
-  **Report unauthorised transaction**
Protect yourself from scams! Please report any unauthorised or suspicious transaction to us immediately via Hang Seng Mobile App "Settings & Security."
-  **Identify credit card transactions quickly with additional info**
Want to check your card transactions? You can now easily find more info like merchant names, foreign exchange rates and post dates via "My Credit Card" page, helping you manage transactions more effectively and spot unauthorised ones sooner!
-  **Track your multicurrency debit card transactions easily**
We've gathered debit card transactions – pending and posted – into one handy place on the "My Debit / ATM Card" page of Hang Seng Mobile App! Primary debit cardholders can see debit card transaction record at a glance, keeping a clear eye on both primary and supplementary cards, making it easier to spot any suspicious transactions!
-  **A safer way to verify your identity**
When registering Personal e-Banking or binding Hang Seng Mobile App with a new device, you'll need to take a photo of your valid HKID or Exit-Entry Permit for Travelling to and from Hong Kong and Macao and a selfie to verify your identity. Make sure there's sufficient lighting and keep the device steady.
To protect your account security, you'll need to verify your identity via the App for high-risk transactions (such as password reset) after binding.
-  **Bind your device via ATM 24/7**
If you're unable to verify identity via Hang Seng Mobile App, you can now bind your device at any Hang Seng or HSBC ATMs anytime. Simply set up via App first and bring your Hang Seng Credit Card, debit card or ATM card to the ATM. You can then follow a few steps to finish binding (only applicable if you used HKID to open account).

An Anti-scam (Scameter) alert helps you to stay vigilant against scams

When sending money via Hang Seng Mobile App or Personal e-Banking and receiving a Scameter alert, it means the payee is reported as a fraudster, don't transfer money to them.

Ensure your contact details are up-to-date

To keep your account safe, remember to regularly check if your contact info (e.g. mobile number, email and correspondence addresses, etc.) is correct and up-to-date! You can always update it via Hang Seng Mobile App.

Coming soon

The Hong Kong Monetary Authority (HKMA) is rolling out a new interactive game this Mar to keep you ahead of scammers! It allows you to experience firsthand how to spot scams and protect your sensitive info. Keep an eye on Hang Seng Bank Website for more details and ready to level-up your fraud-busting skills!

Protect yourself from scams. Never click suspicious links or share sensitive personal info. Safeguard your physical cards, account details and passwords. Pay attention to our transaction reminders sent via Push Notification or SMS to prevent losses due to unauthorised transactions and negligence. For more antifraud info and ways to report scams, visit "Security Information Centre" on Hang Seng Bank website.

Hang Seng Bank
恒生銀行

This is a computer generated email by Hang Seng Bank.
這是由電腦編印的恒生銀行電郵。

Please don't reply to this email. The English version of this email shall prevail whenever there's a discrepancy between the English and Chinese versions.
請勿回覆這封電郵。如電郵中英文內容有異，請以英文版本為準。

If there are any changes in your contact information, please update it by logging on to Hang Seng Personal e-Banking or Hang Seng Mobile App. You can also download the Update of Customer's Information Form from hangseng.com and return the completed form to any of our branches or mail to: Hang Seng Bank Ltd, GPO Box 3013, Hong Kong.
如你的聯絡資料有所變更，請登入恒生個人e-Banking或恒生Mobile App更新，或於hangseng.com下載更改客戶資料表格，填妥表格後交回我們任何一間分行或郵寄到香港郵政信箱3013號恒生銀行有限公司。

To learn about our Online Important Notices, please refer to hangseng.com > Important Notices > Online Important Notices section for details.
如想了解我們的網上重要通告，你亦可瀏覽hangseng.com > 重要通告 > 網上重要通告了解詳情。

Security Reminder 保安提示
We maintain strict security standards and procedures to prevent unauthorized access to your personal information. We'll not ask you for sensitive personal information such as logon password or one-time passwords; and we'll never ask you to validate your user ID, account number, or click on a hyperlink to log on to Hang Seng Personal e-Banking or to update your information by email. If you receive such request, please contact us on **(852) 2822 0228**.

我們堅守高度安全標準及程序，防止未經你授權的個人資料外洩。我們不會主動向你查詢登入密碼或一次性密碼等個人資料；亦不會透過電郵要求你核實使用者名稱、戶口號碼、透過連結登入個人e-Banking或更新你的資料。如你收到這類要求，可致電**(852) 2822 0228** 聯絡我們。