

Beware of Scams



Beware of fake fire victims' registration forms and fraudulent fundraising

If you wish to support the residents affected by the Tai Po fire, please donate through official and reliable channels. Please stay alert and verify the background of any entity before making a donation, ensuring the recipient is a legitimate entity or charity. Don't click on unknown links or scan QR codes and avoid transferring money to accounts of unknown origin.

Please note: bank staff, government departments, charities and social welfare groups won't ask for sensitive information such as your name, ID number, bank account number, passwords or verification codes.

It has come to our attention recently that unidentified individuals are spreading false information. If you receive calls claiming to be from bank staff or other institutions, please contact the relevant organisation to verify. If you suspect fraud, call the "Anti-Deception 18222" hotline for inquiries or seek assistance from the police.

Enhance Fraud Awareness



Remember 3 tips to avoid financial loss.



Check your bank records carefully

Scammers may use fake cheques or deposit slips to make transactions. When receiving payment, verify the available balance against the account records to ensure the funds have been received and don't purely rely on the message images. Now, you can also check both pending and posted transactions via the app. Primary debit cardholders can see transaction records of both primary and supplementary cards at a glance, making it easier to spot any suspicious transactions.



Never share your account details

When dealing with suspicious bank staff / organisations / individuals, don't disclose your account details or password. Also, avoid logging on to online banking with untrusted or public devices. If in doubt, remember to verify via the official channels.



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, correspondence addresses, etc.) is correct and up-to-date. You can always update it via Hang Seng Mobile App.



Want to further protect your account? There're even more features!



Protect your funds with "Money Safe"

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.



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

When sending money to other organisations / individuals via Hang Seng Mobile App or Personal e-Banking and an Anti-scam (Scameter) alert will give you 10 seconds to reconsider before proceeding. Do not transfer money to a payee that is in the list of suspicious scammers.



Safer way to verify your identity

We'll gradually upgrade our security measures to protect your account. From Nov 2025, if you've opened an account with HKID (applicable to customer who are aged 18 or above), you can quickly and safely register e-Banking or bind your device to Hang Seng Mobile App by capturing your HKID and taking a selfie.

Later we may verify your identity again to make sure it's you using the device. You can then have access to all services, including money transfer to new payees, payment to institutions and "card-not-present" transactions authentication.

Scammers may exploit the Hang Seng privatisation proposal to deceive or mislead you into transferring or withdrawing deposits. For details of the proposal, please refer to the joint announcement issued by Hang Seng and HSBC and information on Hang Seng's official website. Don't trust or forward your personal information to, or transact with, unverified sources.

Be vigilant against scams! You can visit the "Security Information Centre" on Hang Seng Bank Website to learn more about anti-fraud information.

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。