

## Stay Alert to Frauds

—Beware of suspicious links, unofficial apps, screen sharing, virtual inspection and etc

Dear Customer,

To help protect your financial safety, please stay alert to the following common scams:

1. Fake “closure of direct debit service”: Fraudsters may pose as customer service agents, claiming you've activated a direct debit service (such as membership auto-renewal). They may ask for your card details or screen sharing, claiming that they can help you close the service.
2. Credit repair scams: Scammers may promise to “remove negative credit records” or “boost your credit score” in exchange for high fees, but these services are falsified and meant to deceive.
3. Fake investment platforms or apps: Fraudulent apps or websites may be promoted through unofficial sources. They often contain malware that can steal your financial information or directly steal funds.
4. “Virtual inspection” scam: Criminals may claim your account is under inspection and ask you to stay on video calls or avoid contact with others, creating fear and pushing you to transfer money.

Please remember the following security tips:

- Don't click unknown links in emails or texts to avoid phishing traps.
- Only use official sources to download apps or access services.
- Don't share your screen with strangers.
- Be skeptical of remote “inspection” involving sensitive info or money transfers.
- Verify identities of anyone claiming to be from banks or authorities.
- Protect your personal data, especially on unfamiliar websites or apps.
- Report suspicious activity immediately by calling 110.

If you're uncertain or have doubt, please contact our customer service at 95366/+86 (21) 95366. Your vigilance is your first line of defense.

HSBC Bank (China) Company Limited

2025/6/20