How to protect yourself against scams

Could you become a victim of scams or fraud?

Anyone can become a target for scammers. According to the Hong Kong Police Force, elderly people are often the victims of street and telephone scams. Fraudsters are always looking for new ways to deceive you, so it’s worth being aware of how some of these scams work.

At HSBC, we’re committed to supporting elderly customers by promoting “age-friendliness” and helping you stay vigilant about financial crime to protect your financial wellbeing. Our industry-leading fraud detection systems are designed to protect our customers, but it’s also important to be aware of scams and how to avoid them.

This guide explains some types of scams to watch out for, differences between how banks and fraudsters might reach out to you, where to learn more and how to report suspicious behaviour. Please read it carefully.

What kinds of scams are out there?

Most scams are uninvited. They usually ask you for personal information or security details, and they often create a false sense of urgency.

Scammers hope to trick you into revealing key details about your account so they can steal your money. Here are some common types of scams.

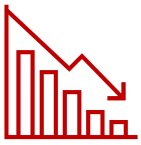
Phone scams | “Vishing”

A fraudster calls you or leaves a voicemail pretending to be someone from your bank, another well-known organisation, a government department or even the police from mainland China. They may already know some of your personal information.

They may try to convince you that they are genuine and scare you into doing something immediately, without giving you time to think.

	A fraudster might…	*A bank would…*
Example 1 You receive a phone call from someone claiming to be from your bank’s fraud team. They ask you to assist them in a fraud investigation.	…ask you to transfer funds to another account for safe keeping. They might also ask for your PIN or online banking passwords and your security details.	…explain that there has been some unusual activity on your account and check whether you made the payments. A bank may also ask you a few questions for identification and verification purposes.
Example 2 You receive a call from someone claiming to be from your bank. They invite you to apply for a personal loan or a credit card.	…push you to reveal personal information so you can sign up for credit products or services with low interest rates, such as personal loans or add-on mortgages. They will not share any information you can trace or verify.	…address you by your full name and share the caller’s full name, extension or direct line number and details of how they got your phone number and account information to prove who they are. If you have any suspicions, they will be happy for you to call them back using the bank’s official customer service hotline.

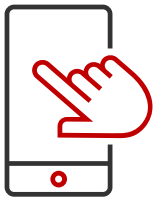
Investment scams



A fraudster claims to have an attractive investment opportunity and tries to convince you it is genuine by using false testimonials or marketing materials.

	A fraudster might…	*A bank would…*
Example You are contacted about an investment opportunity.	…claim to have a time-limited investment offer with high returns and low risk. They may try to pressure you into accepting quickly.	…behave professionally and share their credentials, which you can then verify using the bank's official customer service hotlines.

Social engineering scams



A combination of a phone and online social media scam, a fraudster contacts you pretending to be someone from a trusted organisation, a public official or a law enforcement officer but also knows a lot about your personal activity and life, e.g. purchases, travel history, family and friends' names. All of this information is being guessed or extracted from your social media posts. Then they try to convince or scare you into doing something that puts you at risk, e.g. providing banking credentials and sensitive personal information or transferring money.

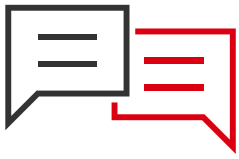
	A fraudster might…	*A trusted organization would…*
Example You receive a call from someone claiming to be a police inspector from mainland China. They tell you that you could be in serious legal trouble because your account has been hacked or because of tax evasion.	…ask you to give your bank details so they can "monitor suspicious activity" and tell you that there will be consequences if you hang up before you have given them personal data. They may also ask you about your travel between Hong Kong and mainland China, and they may be aware of personal information you have shared on social media.	…invite you to connect with them through an official customer channel. They would not pressure you to share sensitive information without giving you credentials that you can verify through official channels, such as a hotline.

Email scams | “Phishing”

A fraudster sends you an email encouraging you to share personal details, click on fake links or QR codes, or open file attachments so they can steal your information by installing bad software, also called malware, on your device.

	A fraudster might…	*A bank would…*
Example You receive an email that appears to be from your bank.	…ask for your account number, PIN, banking password (including for internet or phone banking apps), or ask you to transfer money.	…only email you to give you details about services that you might find useful or, in Hong Kong, ask you follow-up questions about your banking experience.

SMS/text scams | “Smishing”



A fraudster sends you an SMS or text message that appears to be from your bank or another trusted organisation.

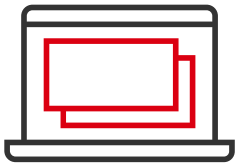
	A fraudster might…	*A bank would…*
Example 1 You receive a message asking you to call your bank urgently on a specific phone number.	…ask about a suspicious payment from your account and request you to provide login details, claiming that they are needed to stop the payment.	…stop the payment and suspend your card.
Example 2 You receive an message stating that a new payee has been added to your account. You need to click the link to confirm this is correct.	…direct you to a look alike website for your bank where you need to enter your login information and password.	…never send you a link which direct you to a page where you need to fill in login credentials.

Romance scams

Somebody you have never met in person contacts you to start a romantic relationship with you. They then make up a reason to ask you for money.

	A fraudster might…	*A bank would…*
Example 1 Someone who started a relationship with you online tells you that their sister is very ill and needs urgent help. They then ask you for money as a favour, promising to return it.	…tell you that they love you before saying that they or someone in their family needs a life-saving operation or is dealing with an emergency and that they need money urgently to pay a fee.	…never ask or contact you about personal matters; only professional ones.
Example 2 Your contact tells you they would like to visit you or that they have valuables, such as gems, to give you.	…ask you to pay for their travel expenses so they can visit you, or ask you to pay taxes or fees so they can give you the valuable items.	
Example 3 Your contact tells you they have inherited a large amount of money but they cannot access it without funds from you.	…ask you for money as a favour, promising to return it.	

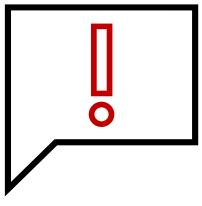
Online shopping scams



Fraudsters use fake shopping websites or pretend to sell goods in order to acquire your payment details.

	A fraudster might…	*A trusted organization would…*
Example You are shopping online and find an item you want to buy. You do not know who the seller is.	…have their scam site pose as a genuine one. They hope to convince you to buy something in order to obtain your personal information (if you need to create an account on the website) or payment details.	…advise you to check that there is a padlock icon on the top left of the website address bar.

Account takeover fraud



Fraudsters claiming to be your internet provider may contact you to tell you that there is a problem with your internet. They will try to obtain your banking details by persuading you to install software, internet banking or e-wallet mobile applications.

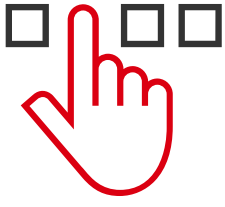
	A fraudster might…	*A trusted organization would…*
Example You receive a call from someone claiming to be your internet provider. They ask you to download software which will allow them to see your computer screen. They then convince you to log on to your bank account as a “test”.	…ask you to visit website URLs with similar names to those of official institutions, to open or download bad software or an app. Then, they ask you to give them complete access or “remote control” your computer to fix “problems”.	… only advise you to visit an official bank site or an official brand’s app store application to download any software or apps necessary to help you. They only ask you to share your screen if you initiated the call.

WhatsApp | Messaging app scams

Fraudsters may hack your close contacts' accounts to impersonate them. They then message you asking you to buy something, click on a photo, GIF or link, or download something. Their aim is to steal your personal information and sensitive data.

	A fraudster might…	*A genuine contact would…*
Example You receive a message from your sister or friend telling you to buy top-up cards for online games to resell at a higher price.	…ask you to click on a link or go somewhere to share your bank details and PIN. They may pressure you by messaging you again, and ask for images of sensitive information over WhatsApp or another messaging service.	…explain more about their suggestions over a call or in person.

ATM scams



Fraudsters may attach card readers and pinhole cameras to ATMs to record all of the account information associated with your card. They may even wait near the ATM and try to see your PIN, or approach you to say that you dropped some money or something personal.

	A fraudster might…	*An ordinary person would…*
Example Someone asks you to pick something up while you are using your ATM card.	…distract you from looking at the ATM machine so they can take your ATM or credit card and replace it with a dummy card.	…wait until you have completed your transaction and keep a respectful distance.

How can you protect yourself from scams?

To avoid becoming a victim, follow this important advice:

Be cautious

- If something sounds too good to be true (such as a generous service offer or prize) and you have to make a payment to receive it, it's probably a scam.
- Always be suspicious of someone who approaches you without you inviting them to, and refuse all offers of help from strangers when you are using an ATM.
- If you think you've been targeted by a scam, keep calm. Contact us or call the official phone number of the organisation in question to check if the calls or messages are genuine.

Build good habits

- Check your bank statements regularly and contact us immediately if you notice any unusual activity.
- Log in to your account regularly to remind yourself of your passwords and PINs and to update them.
- Use different PINs for different websites and banking channels (ATM, Phone Banking, Internet and Mobile Banking).
- Regularly update your mobile apps.

Share with care

- Never share personal information or images with someone whose identity you have not checked.
- Be cautious about what you share online, especially on social media.
- Shred important documents and papers that contain personal information before you throw them away.

Boost your security

- Register for and use biometric authentication, such as iOS Face ID, iOS Touch ID, Android™ Fingerprint ID and Voice ID[1].
- Strengthen your security settings by enabling 2-step verification on WhatsApp and your other messaging services.
- When using online or mobile banking services, use trusted Wi-Fi networks and service providers, and turn off Bluetooth when you aren't using it.
- Avoid clicking on pictures or links unless you trust the sender.
- Search for the sender in your contacts to verify their identity.

For more detailed information and guidance, visit www.hsbc.com.hk/help/online-and-banking-security.

Where can you find additional help and report suspicious activity or crime?

Hong Kong Police Force Anti-Deception Coordination Centre (ADCC)

The ADCC provides the latest scam alerts, videos and useful links to help you protect your finances and request assistance.

- Call the ADCC Anti-Scam Helpline at 18222 to report suspicious activity.
- Visit www.police.gov.hk/ppp_en/04_crime_matters/adcc.

Investor and Financial Education Council (IFEC)

The IFEC provides tips, guidance, articles, videos and useful links to help you prevent fraud.

- Visit www.ifec.org.hk/web/en/moneyessentials/scams/index.page.

[1] Touch ID and Face ID are trademarks of Apple Inc., registered in the U.S. and other countries and regions. iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple Inc. under license. Android is a trademark of Google LLC. Fingerprint authentication is available on compatible Android™ devices running Android™ OS version 8.0 or later. For more info, visit www.hsbc.com.hk/ways-to-bank/internet/security-key/#activation or www.hsbc.com.hk/help/cybersecurity-and-fraud/safeguard.

Contact us | We're here to help

To learn more about planning for a more secure financial future, visit www.hsbc.com.hk/age-friendly-banking.

To learn more about how to handle or report fraud, visit www.hsbc.com.hk/help/online-and-banking-security/how-to-report-fraud.

You can also get in touch with us in the following ways:

- **Visit our branches**

- **Call our customer service hotlines**

  - HSBC Premier Elite (852) 2233 3033
  - HSBC Premier (852) 2233 3322
  - All other customers (852) 2233 3000

- **Email us to report a problem csv@hsbc.com.hk**