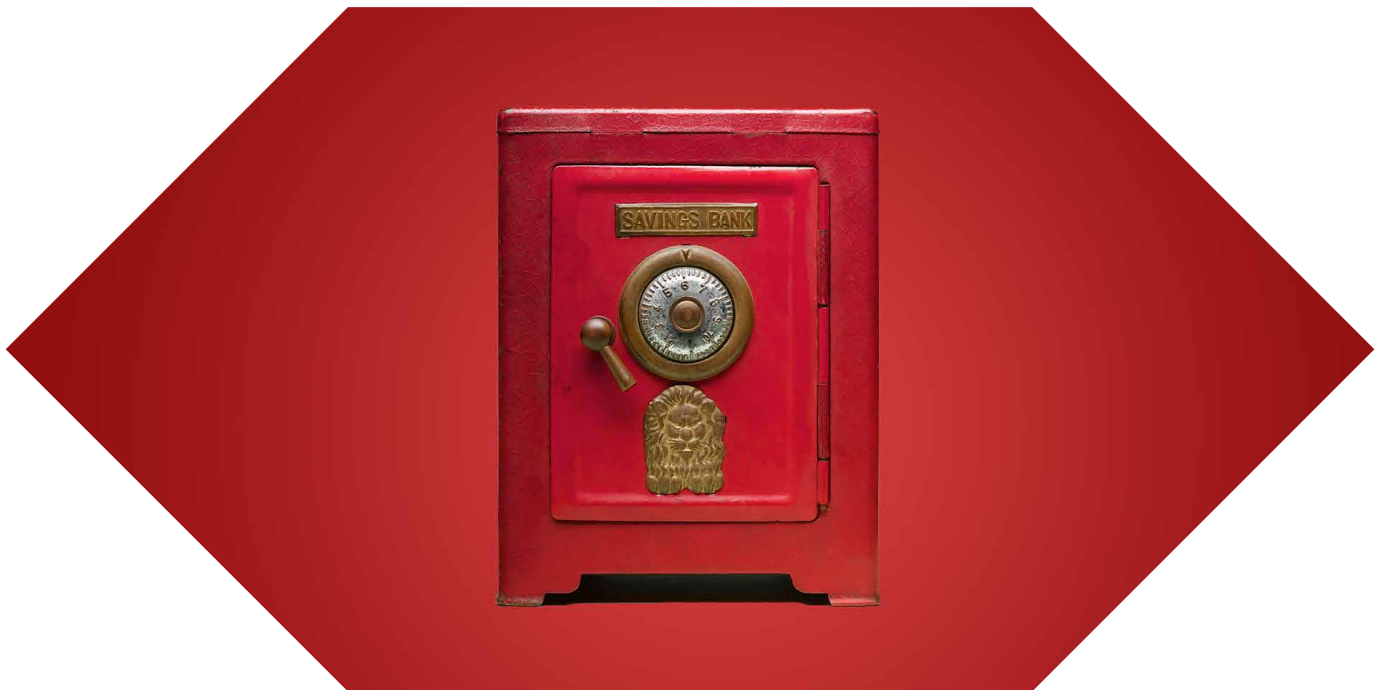


Financial education for young adults

Banking safely and securely









HSBC

| Opening up a world of opportunity

Contents

 Click to navigate to each section

 Guarding against fraud	03
 Fraud: Get protected	07
 Protecting your money	08
 How to bank and make payments safely online?	09
 Is digital banking secure?	11
 How to spot phishing	12

Guarding against fraud

We all think fraud is something that happens to other people, until it happens to us.

Understanding fraud is like understanding magic – confusing if you don't know the trick, but easy to spot once you know how it's done. If we all learn the tricks, we'll be less likely to be fooled.

► Types of fraud



Email scams (phishing)



Phishing is a way in which criminals try to get sensitive information, like usernames and passwords, by email. These messages look like they've come from someone you trust, such as your bank.



What to look out for:

The email will ask you for personal information, or direct you to a website (which might even look like a trusted website) asking you to share information. The email is also likely to have a generic opening (they probably won't use your name), and incorrect spelling and grammar.



How to avoid them:

Always check the sender's email address. Don't click on any links, and don't open any attachments. Never give out your sensitive information. If you're an HSBC customer, you can forward the email to phishing@hsbc.com and it'll be investigated.



► Quiz: How to spot phishing



SMS scams (smishing)



Criminals may send you fake text messages that look like they've come from someone you trust, such as your bank or mobile service provider.



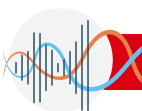
What to look out for:

They'll try to get you to click on a link or reply to the message with personal or financial information.



How to avoid them:

If you're not sure, don't click on any links and don't reply. Check to see what regular text messages from that organisation look like.



Voice scams (vishing)



Criminals may call you and claim to be someone you'd normally trust (like your bank or the police), while actually trying to scam you – or get information from you that they can use to scam you in future.



What to look out for:

They might try to persuade you to transfer or move your money to a 'safe place'. They might ask for personal information, such as your account passwords, PIN or security key codes.



How to avoid them:

Hang up the phone properly – wait 15 seconds until the line is fully disconnected. Wait another 15 seconds before beginning a new call. Ring the company they claim to be calling from, using a phone number you know and trust. In the case of your bank, that would be the number on the back of your card.



Authorised push payments



Authorised push payment (APP) scams happen when you're persuaded to send money to a criminal.



What to look out for:

Someone may try to persuade you to send money to a 'safe account' or an account you believe to be trustworthy, or they may try to trick you into sending money to buy goods that don't exist.



How to avoid them:

If anyone asks you to divert a payment or move your savings – question it. Make sure you phone the bank or company directly and check with them about any changes to payment details.



Payment diversion



Criminals may monitor email traffic and, when payments are due, send their own email that looks and feels like a genuine message from a company.



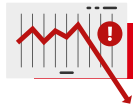
What to look out for:

The email will tell you that the bank details for your payment have changed and give you new details to send your money to.



How to avoid them:

Always check with the company you're paying by calling their official phone number – not the phone number on the email – before making a payment using new bank details.



Investment scams



A fraudster may claim to have an attractive investment opportunity, and back their claim up with (false) testimonials or marketing materials to make it seem more convincing.



What to look out for:

They'll often use false testimonials, fake celebrity endorsements, spoof websites and fake companies with names similar to those of genuine investment organisations.



How to avoid them:

Look up public records (e.g. on the Hong Kong Companies Registry) to confirm that the company is authorised. If it seems too good to be true, it probably is.



Money mules



Job adverts and offers from acquaintances that offer quick and easy ways to get money might seem harmless, but they're often run by organised crime groups. They try to get you to transfer money through your bank account in exchange for payment, making you a 'money mule'.



What to look out for:

You'll be asked to provide your bank details, receive a payment into your account, and then either withdraw it in cash or transfer it to another account. This can get you into serious trouble.



How to avoid them:

Never allow money to be transferred through your bank account in exchange for payment.



Identity theft



Criminals may try to get important pieces of personal information that would allow them to open new accounts in your name or take over your account.



What to look out for:

Online quizzes that tell you (for example) your personality type may seem harmless, but they might get you to reveal personal details that identity thieves can use. The terms and conditions of these quizzes often allow the data you enter to be sold to others.



How to avoid them:

Avoid any short, fun quizzes that pop up on social media, and keep your profile private. Make sure you destroy your bank statements and similar documents safely.



Romance scams



This type of fraud begins with a fast-moving online relationship. Criminals try to lower your guard by appealing to your compassionate or romantic side, and then they ask you for money.



What to look out for:

They'll go to great lengths to build rapport and form a strong emotional bond.



How to avoid them:

Never send money to someone you've only met online. And never agree to accept money from them to send somewhere else on their behalf.



Holiday scams



Many adverts promising great holidays turn out to be fake. Either the holiday doesn't exist, or it does exist but won't be what you think it is when you get there.



What to look out for:

Check the website you're booking the holiday through is legitimate, by looking for online reviews and recommendations. Look out for incorrect spelling and grammar.



How to avoid them:

Be wary of unusually cheap holidays, and always check the terms and conditions.



Purchase scams



Shopping for second-hand items or cheap deals on social media is often a good way to get a bargain. But beware of the many fake profiles and fraudsters that are waiting to trick you.



What to look out for:

Warning signs include accounts that have been created only recently and appear to be selling large numbers of products or use generic pictures of goods.



How to avoid them:

Be wary of sellers who ask for a deposit or ask you to send money to an apparently unrelated account or business.

It's really important to know how to avoid these types of fraud, because you won't usually be able to get compensation for money you lose if you become a victim.

Fraud: Get protected

Fraud and scams are where a criminal tricks you for their own financial gain.

Fraud can happen without you even realising, but a scam takes place when someone persuades you to complete an action on their behalf.

We all think fraud and scams are things that happen to other people, but the truth is that we're all equally vulnerable. Criminals know how to pressure us into situations that put us at risk.

When you spot something suspicious, ask yourself the following questions:




- Does it encourage me to take urgent action, or threaten me with account closure if I don't act quickly?
- Does it tell me that I'm owed money that I wasn't aware of?
- Does it encourage me to click on a website link in an SMS or email from an unknown sender?
- Does it ask me for personal, confidential or security information?
- Does it ask me to reply or to verify my account?
- Does it have poor spelling, formatting or grammar?
- Does it ask me to verify new payees, transactions or devices?
- Does it appear to be genuine, but when I look closer something's not quite right?
- Does it ask me to transfer money to a 'safe account' or withdraw cash and hand it to the 'police' for investigation?
- Does it contain an offer that seems too good to be true?
- Does it use different reasons to convince me to change my payment details?

Protecting your money

You're finally building up a healthy-looking bank balance – that's great! Now you have to keep your money safe.

You can take small steps each day to protect your money, such as checking your bank statements for any unusual transactions. You can also take bigger steps, such as checking the person or company you're paying is genuine before you make a payment.

You can test your fraud-spotting skills using the scenarios below.

Scenario	ANSWER
<p>1 One of your friends has messaged you on social media saying that they need cash to help with an emergency.</p> <p>What would you do, and why?</p> 	<p>Don't send them the cash. Check your friend really is asking for the money by calling or messaging them. Don't contact them on social media – if your friend's account has been hacked or someone is impersonating their social media accounts, you could become the victim of a scam.</p>
<p>2 You're out shopping and you've connected your phone to the shopping centre's public Wi-Fi. You see the perfect pair of shoes, but you need to check your balance to see if you can afford them.</p> <p>What would you do, and why?</p> 	<p>Don't check your balance when connected to public WiFi. Public WiFi isn't secure, so it could allow fraudsters to gain access to your financial details. It would be better to use your normal mobile data to connect to the internet, or go to an ATM to check your balance.</p>
<p>3 You're out with a friend for lunch. You give them your card to pay while you go to the toilet, and they ask for your PIN in case contactless doesn't work.</p> <p>What would you do, and why?</p> 	<p>Don't leave your card with someone else, and never share your PIN with anyone – not even your best friend, and especially not in public where someone could overhear you. The only person who should ever know your PIN and use your card is you.</p>

How to bank and make payments safely online

Shopping and banking online or in a mobile app can be fast and convenient.

But it's important to protect yourself against the risks, just as you would when spending or managing your money in any other way. Here are some tips to help you stay safe:



Keep your devices secure

Make sure your phone, tablet or computer is secure by keeping its operating systems up to date.

You can set laptops and desktops to automatically install software updates as soon as they become available. The same goes for app updates on your devices. Choose to install them whenever you're connected to Wi-Fi and a new update is available, or at night when your device is plugged in. This way you'll benefit from any security enhancements, which are designed to make it difficult for hackers to get in.

You should also install anti-virus software from a well-known, reputable and trusted company to protect your device from any malicious activity. Find out more by [visiting our cyber security and fraud hub](#).



TurfChainPasta4!

Create strong passwords

Complex online passwords might feel like a hassle, but they do an important job in protecting your personal information.

When it comes to passwords, longer equals stronger. Use a combination of upper case letters, lower case letters, numbers and symbols to make your passwords harder to crack. Another way to strengthen a password is to string together unrelated words.

If you're banking online or using a mobile app, you can put in place some other security measures too. For example, you can use fingerprint or face recognition to add biometric security to your banking app. This is known as two-factor authentication. At HSBC, we're also now using behavioural biometrics as an extra check when you make online payments.



Look for secure connections

To check that your web connection is secure, look for a padlock icon in the address bar. But remember, the padlock doesn't guarantee that a website is genuine.

For example, if you're on hsbc.com.hk and you see a green padlock, you know you're securely interacting with HSBC. But if you're on hs8c.com.hk, you might still see a green padlock, indicating a secure connection – but you wouldn't be interacting with HSBC. You might be on a site that's been set up to trick you into thinking that's what you're doing.

So always make sure a website is genuine by checking the address for subtle misspellings, extra words, extra characters or other irregularities. Sites like CyberDefender can help you work out if a site is legitimate.



Shopping and bank transfers

When shopping, check again for the padlock in the address bar before entering your personal or payment details, and don't give more information than is needed for the transaction. For example, only fill in the mandatory fields.

You can usually buy things without having to create an account – so don't create one if you don't have to. And, where possible, don't allow the retailer to save your payment details.

Never pay for something by bank transfer if you don't know the seller. Always use a credit card, a debit card, PayPal or a payment option that offers some protection against fraud.

If you notice any suspicious activity on your account, call us immediately on +852 2233 3000.



Avoid scams

Even after you've put these security measures in place, you still need to be mindful of common scams. Here are two warning signs to look out for.

Requests to move money: Genuine banks won't ask you to move money to another account and won't ask for your PIN, password or other personal details when you aren't expecting it.

Unknown senders: Never click on links or attachments from unknown sources.

Is digital banking secure?

When it comes to banking digitally, either on your computer or on your mobile phone, one of the first things you may be concerned about is security.

Banks do a range of things to make sure your money is safe, and understanding what checks are in place can give you some peace of mind. Here are a few features that make digital banking with us secure.



Safe ways to log on

Security key gives you extra protection against fraud. You must never share a security key or one time password with anyone to make sure only you can access your accounts on the HSBC HK Mobile Banking app and online.

For mobile banking, you can also use fingerprint or face recognition to log on quickly and securely, depending on what device you have.



Freeze and unfreeze your credit card

If you're worried that you've lost your credit card or that something suspicious is happening with it, you can put a temporary freeze on it. You can do this at any time on our mobile app or through online banking. Then if the card turns up or there was nothing to be suspicious about, you can unfreeze it instantly.

You can also report your card as lost or stolen. This allows you to quickly to stop your card from being used and order a replacement straight away.



Check payment details

When initiating a payment, double check the payment details before you confirm it. Check the account number, payee name and amount to be paid.

How to spot phishing

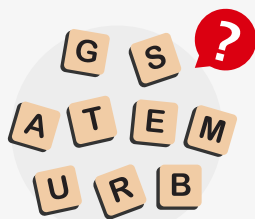
Criminals use fake emails and fake websites.

They set them up to con people into giving away passwords and bank details. The technical word for this is 'phishing'. They are good at making their emails and websites look realistic. But you can often spot the fake ones:



Disguised or modified links

Hovering over the link shows the actual URL you are being directed to e.g. "H5BC.com"



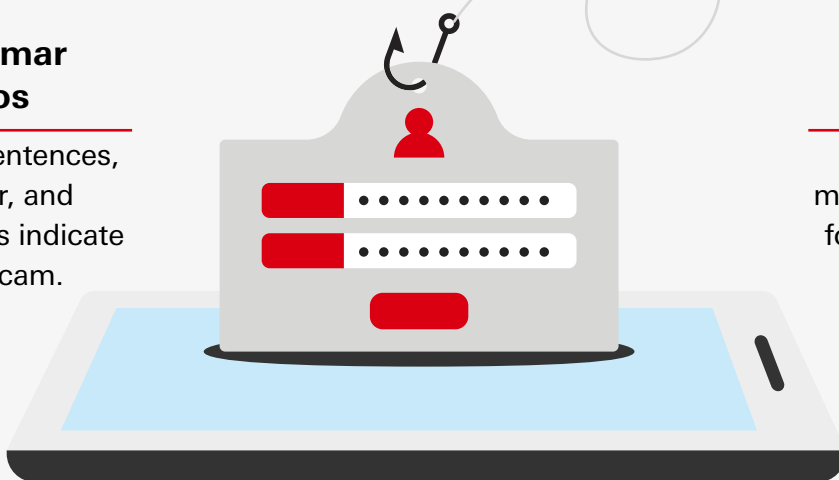
Bad grammar and typos

Poorly written sentences, bad grammar, and misspelled words indicate a phishing scam.



Personal information

Be wary of messages that ask for your personal information.



Urgency and account threat

Warning a sudden change to an account, asking to act immediately to verify.

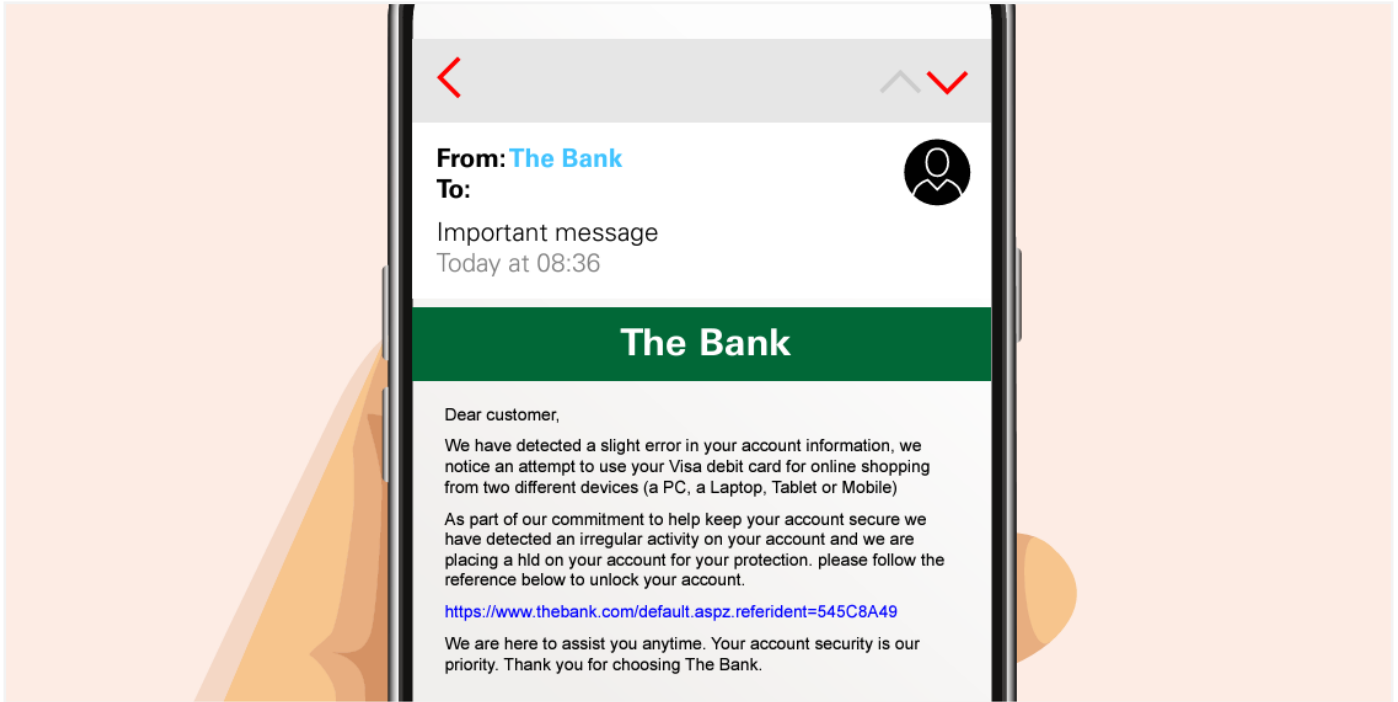


Logos or signatures

Don't assume an email is legitimate because it includes official looking graphics.

Email challenge 1: Spot the signs of fraud

Fraudsters send emails to people as part of scams to encourage them to give access to their bank accounts and money. It's hard to tell the difference but there are some clues – can you spot them?



Answers:

Warning #1:

'Dear customer': Your bank will know your name and include it when it writes to you.

Warning #2: Hover over the sender's email address – this usually reveals the actual sender's email

address which can reveal a suspicious looking address.

Warning #3:

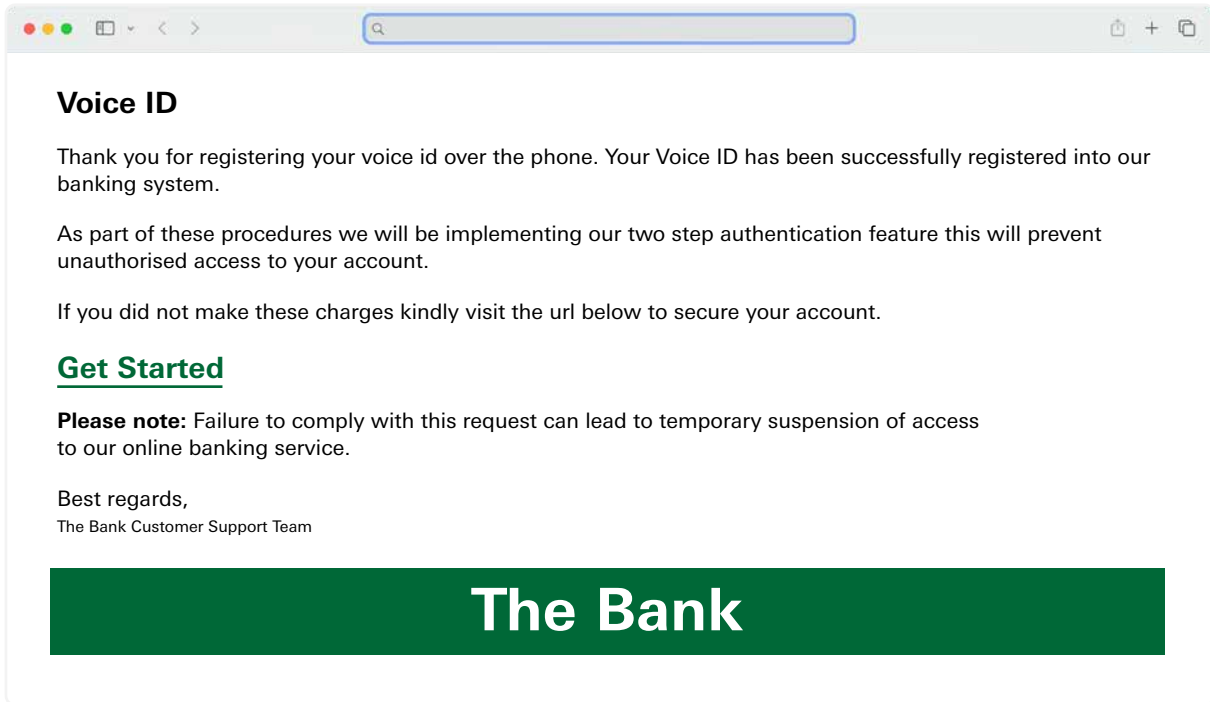
Check grammar and spelling mistakes. Your bank is unlikely to say 'slight error' – either there has been an error or there hasn't.

Warning #4:

Do you recognise the web link? Don't click on any web links that you don't recognise.

Email challenge 2: Spot the signs of fraud

Sometimes emails can sound very official to make you think that they are legitimate. But the signs are still there – can you spot them?



Answers:

Warning #1:

Selecting the link could be a risk – for example it could direct you to a fraudulent web site or allow access for a fraudster to information held on your computer. Hover over the link to see where it goes before you click.

Warning #2:

Poor quality of the message with different font sizes and colours should raise suspicions.

Warning #3:

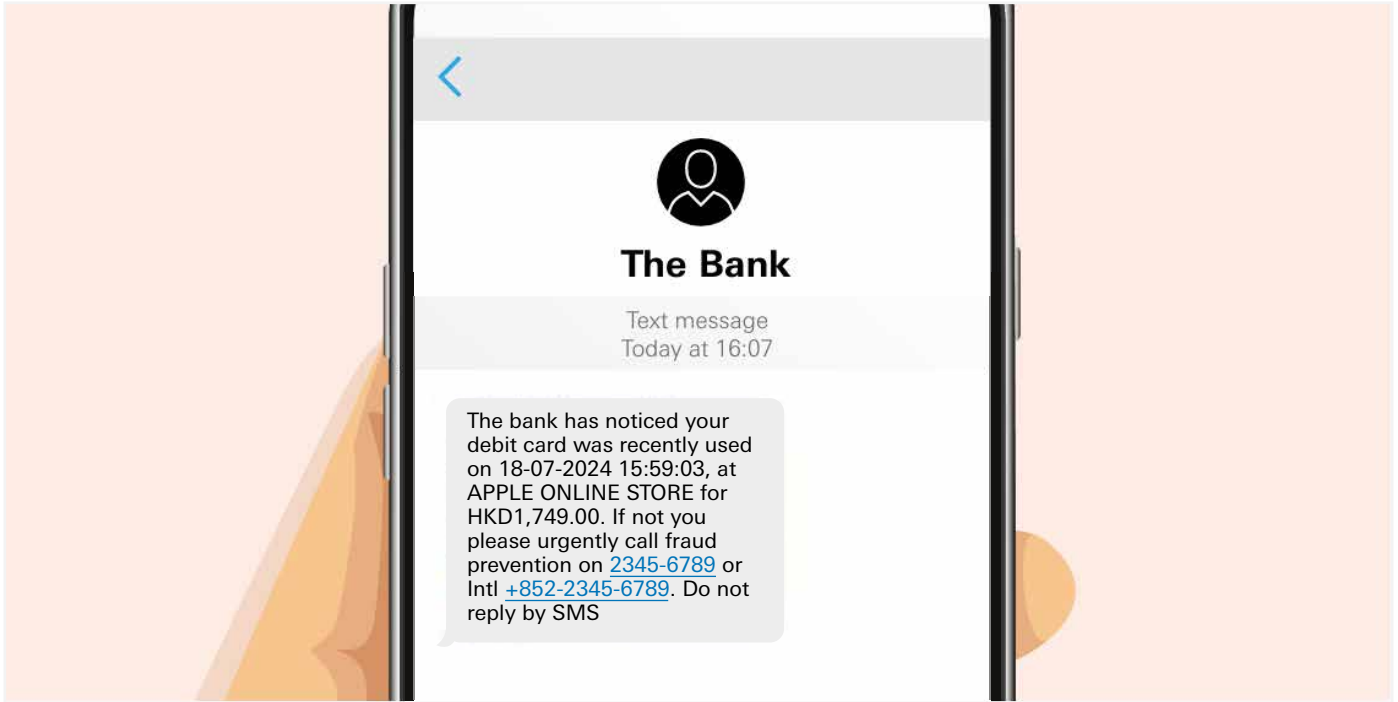
No customer name included again.

Warning #4: Have you registered for voice ID? The person who received this email had not.

Always think about if the purpose of the message makes sense to you.

SMS challenge 1: Spotting a fraudulent text

What about text messages, can you spot the signs that this is a fraudulent SMS?



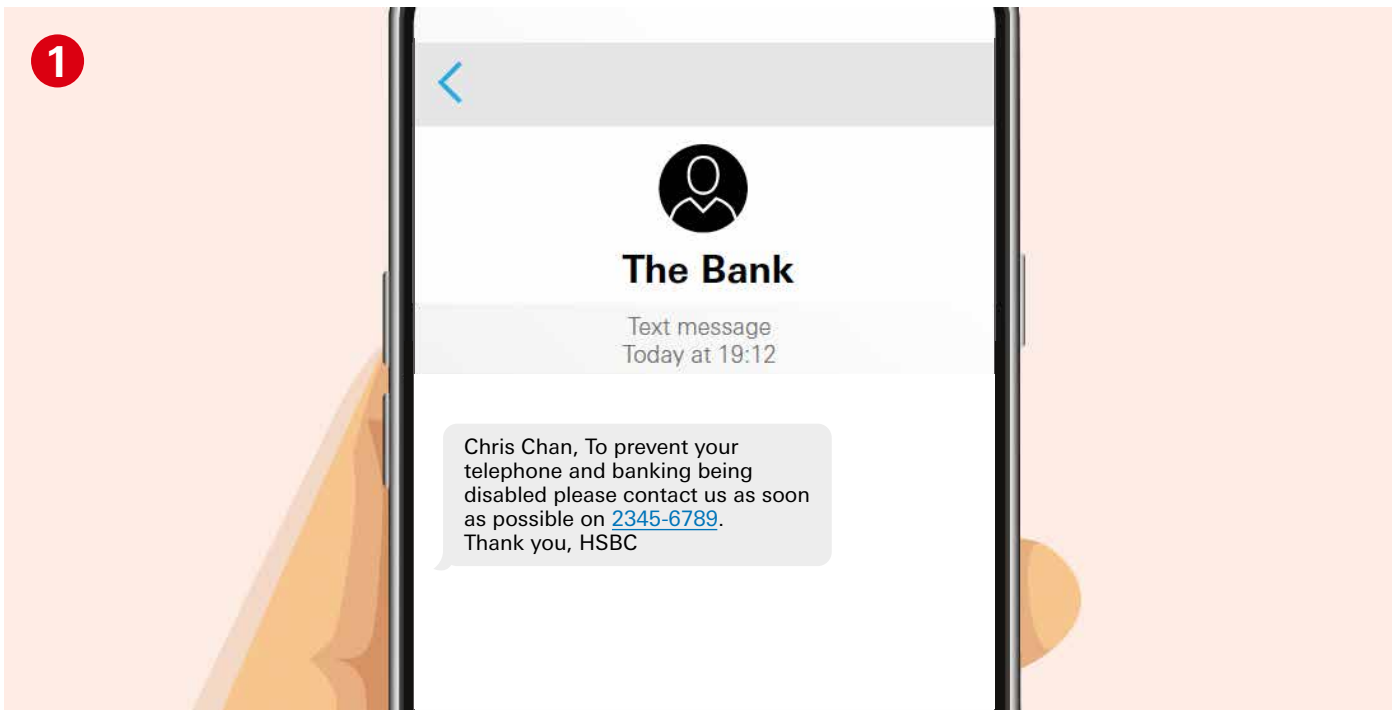
Stop and think.

It's even harder to tell if a text message is real or attempted fraud.

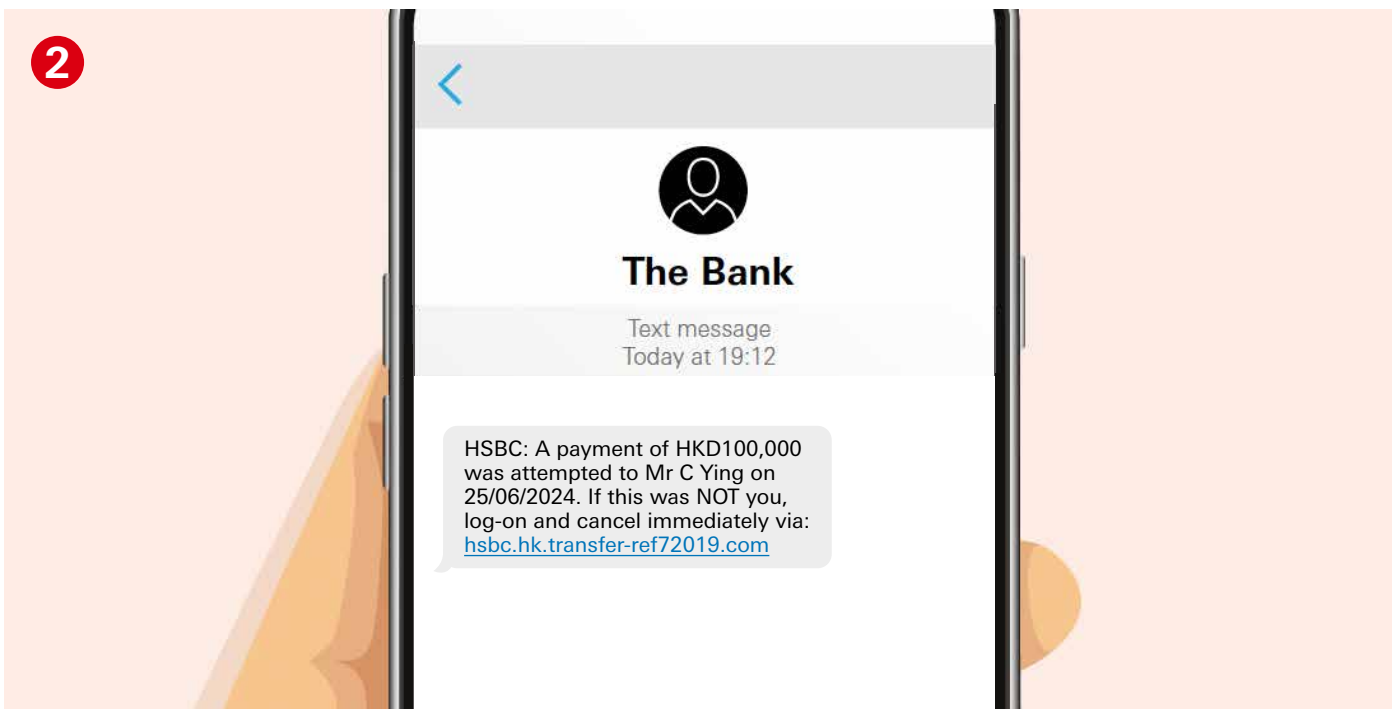
Answers:

Do you remember buying what's described? Don't call the number in the text message. This type of fraud is growing quickly. Call the bank's usual phone number (such as the number on the back of your card) not the number in the message.

SMS challenge 2: Spotting a fraudulent text



Legitimate Fraud

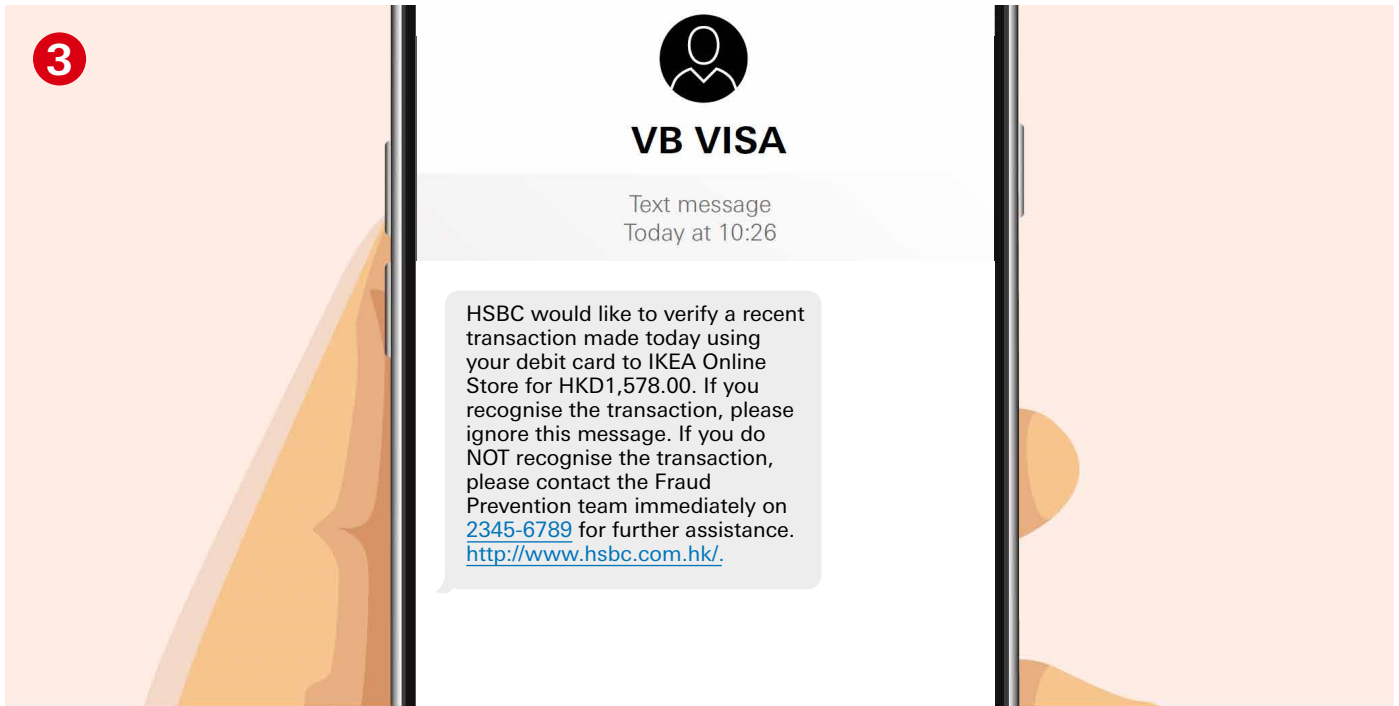


Legitimate Fraud

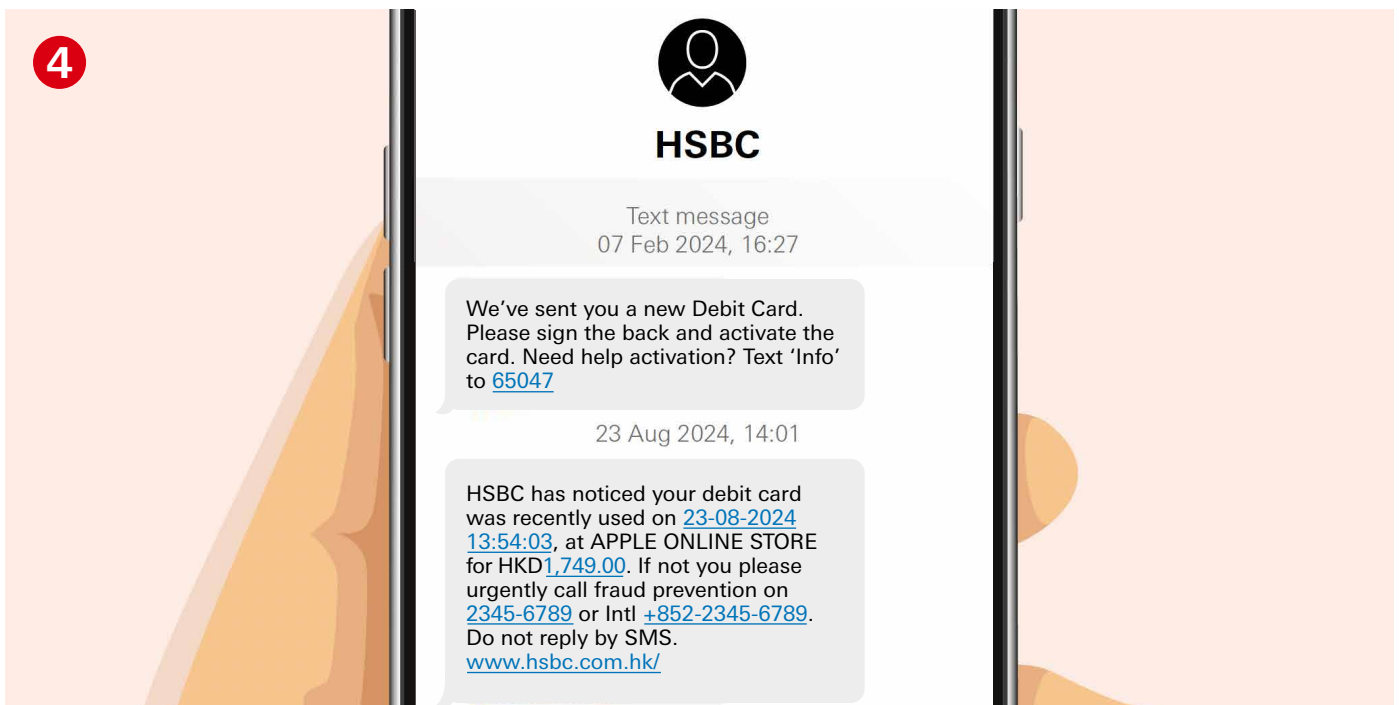
Answers:

1. Fraud 2. Fraud

SMS challenge 3: Spotting a fraudulent text



Legitimate Fraud



Legitimate Fraud

3. Fraud 4. Fraud

Answers:

Quick round: Final check



1 A friend at school asked you to tell them your pin number.

Do you give it to them?

A. Yes / B. No

2 You see a social media message offering to pay you for keeping some money safe for somebody in your account.

Do you accept?

A. Yes / B. No

3 You receive a social media friend request from somebody you didn't recognise.

Do you accept?

A. Yes / B. No

4 You receive a social media request (What's App, Facebook, Instagram, Snapchat) from a friend asking for money.

Would you send it?

A. Yes / B. No

5 Someone tries to distract you when you are using an ATM machine.

Do you turn around and be distracted?

A. Yes / B. No

6 You have lost your bank card.

What do you do next?

A. Nothing / B. Report it to the bank as soon as possible

- 1.B - Never tell anyone your PIN.
2.B - This is known as being a Money Mule and is illegal in the HK.
3.B - This may leave you open to criminals seeing personal information about you.
4.B - It may not be your friend - check with them in person first.
5.B - Make sure you keep your PIN covered or if you feel uncomfortable then simply remove your card and move away from the ATM. There are ATMs inside bank branches which may be better for you to use.
6.B - Make sure you have the lost/stolen number from the back of your card recorded in your mobile.

Answers: