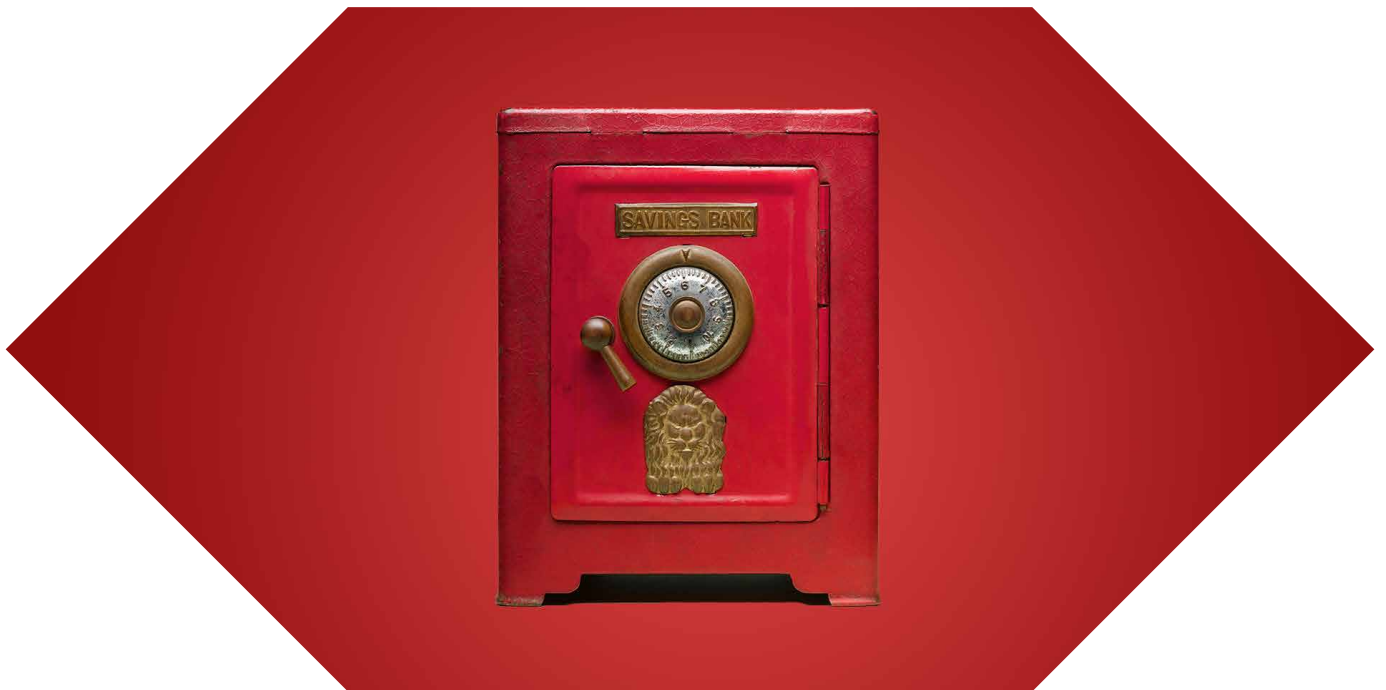


Financial education for pre-teens

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	05
 Protecting your money	06
 How to bank and make payments safely online?	07
 How to spot phishing	09

Guarding against fraud

We all think fraud (a crime in which someone tricks or lies to somebody else to get unfair or unlawful gain) 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're less likely to be fooled.

► Types of fraud to be aware of



Email scams (phishing)

Phishing is a way criminals try to get sensitive information, like usernames and passwords via 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. It's also likely to have a generic opening (they probably won't address you by name), and incorrect spelling and grammar.



How to avoid:

Always check the sender's email address. Don't click on any links, and don't open any attachments. 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.



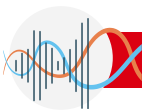
What to look out for:

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



How to avoid:

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



Voice scams (vishing)

You may receive an unexpected call, claiming to be from someone you'd normally trust, like your bank or the police, but in fact it's a criminal trying to scam you or get information from you so they can scam you in the 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, or even your account passwords, PIN or secure key codes.



How to avoid:

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 back on a number you know and trust. In the case of your bank, it would be the number on the back of your card.



Identity theft

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



What to look out for:

Online quizzes that tell you (for example) your personality type, may seem harmless, but they may get you to reveal personal details about yourself. The terms and conditions of these quizzes often allow the data you enter to be sold to third parties.



How to avoid:

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



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 fraudster tricks you for their own financial gain.

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

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

Ask yourself the following questions when you spot something suspicious:




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

Protecting your money

Great news! You're finally building up a healthy-looking bank balance. Now you have to keep your money safe.

There are small steps you can take each day to protect your money, such as checking your bank statements for any unusual transactions, and bigger steps such as checking the person or company you're paying is genuine before making payments.

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

Scenario	ANSWER
<p>1 One of your friends has messaged you via 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. Always check with the person by calling or messaging them to make sure they actually asked for the money. Don't contact them on social media. Your friend may have been hacked or someone may be impersonating their social media accounts, and you could be the victim of an attempted scam.</p>
<p>2 You're out shopping and have connected your phone to the shopping centre's public WiFi. You see the perfect pair of shoes but 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 is not secure and 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 While you are shopping, you realize you don't have cash for payment. Your friend offers to help you get cash from an ATM nearby. They ask for your ATM card and PIN.</p> <p>What would you do, and why?</p> 	<p>Don't leave your card in someone else's possession, and never share your PIN with anyone, not even your best friend, and especially not in public where someone could overhear. 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 mobile apps 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 your operating systems up to date.

You can set laptops and desktops to install software updates automatically 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 benefit from any security enhancements, which are designed to make it difficult for hackers to gain access.

You should also install anti-virus software from a well-known, reputable and trusted company to protect your device from any malicious activity. You can 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 protecting your personal information.

When it comes to passwords, longer equals stronger. Using a mix of upper case, lower case, numbers and symbols also makes them harder to crack. Another way to strengthen a password is to combine unrelated words.

If you're banking online or using a mobile app, there are further security measures you can put in place. 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're making online payments.



Look for secure connections

Look for a padlock in the address bar to confirm your web connection is secure. But remember, the padlock doesn't guarantee an authentic site.

For example, if you're on hsbc.com.hk and see a green padlock, you know you're securely interacting with HSBC. But if you're on hs8c.com.hk, you could 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, additional words / 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, debit card, PayPal or a payment option that offers some protection against fraud.

If there's suspicious activity on your account, contact us immediately on +852 2233 3000.



Avoid scams

Even after you've put these security measures in place, you need to be mindful of common scams. Here are some tips on what 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 out of the blue.

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

How to spot phishing

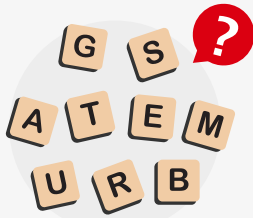
Criminals use fake emails and fake websites.

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"



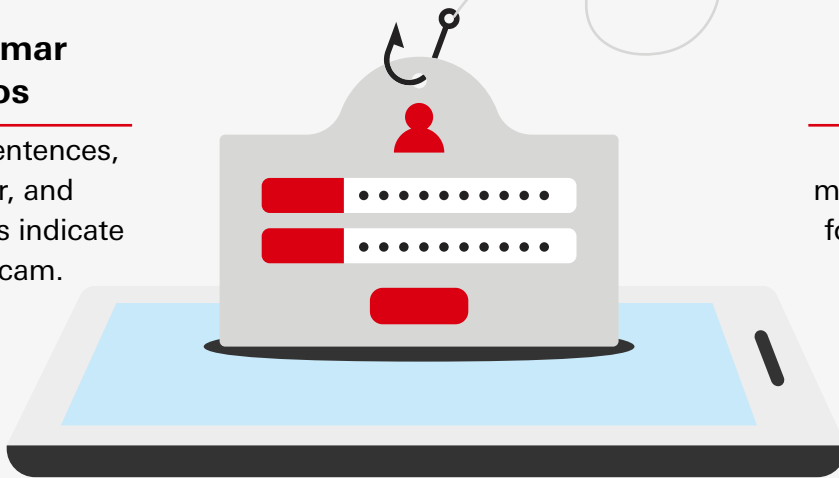
Bad grammar and typos

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.

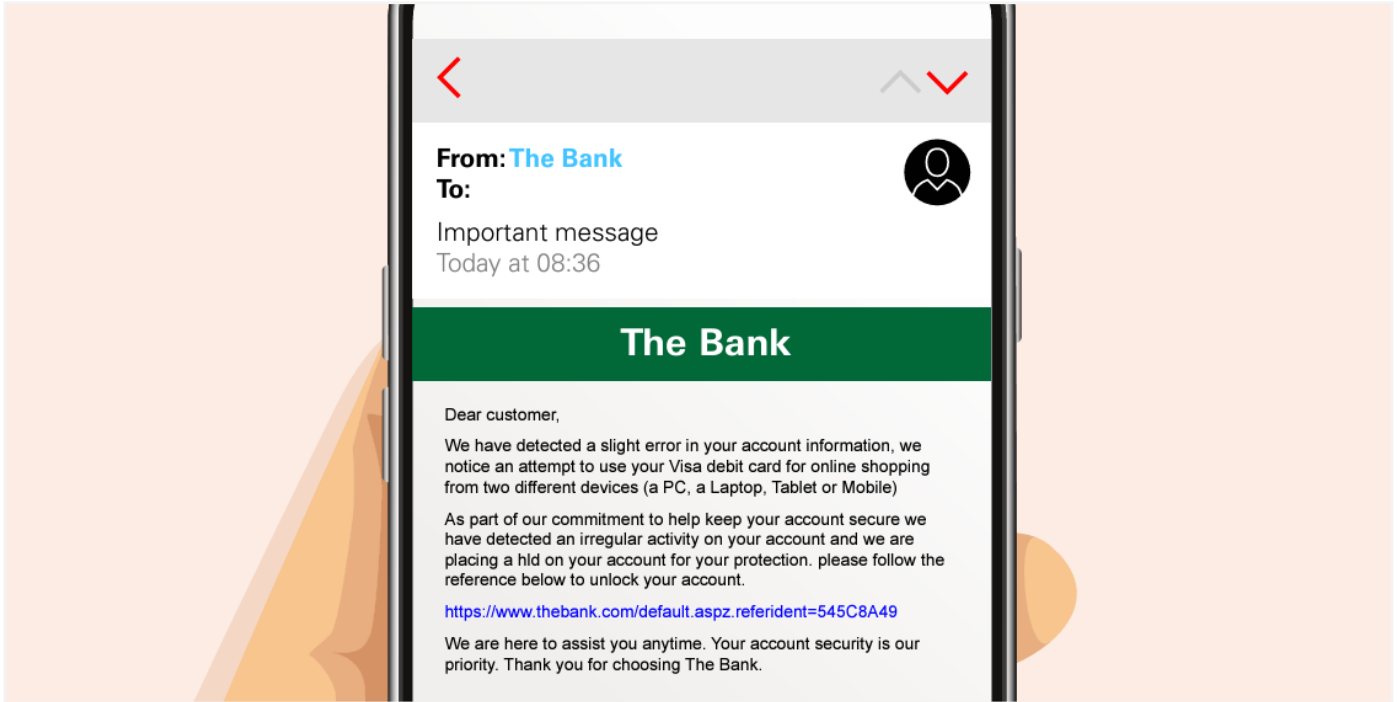


Logos or signatures

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:

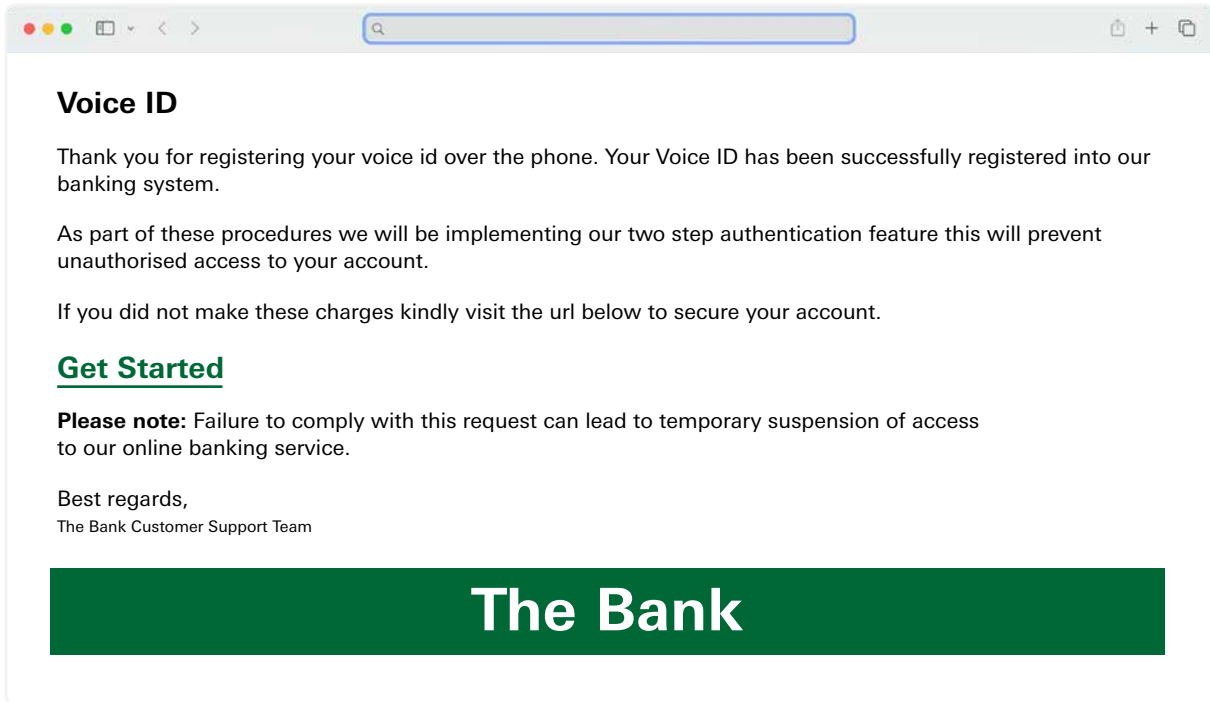
Check grammar and spelling mistakes. Your bank is unlikely to say 'slight error' – either there has been an error or there hasn't.

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:

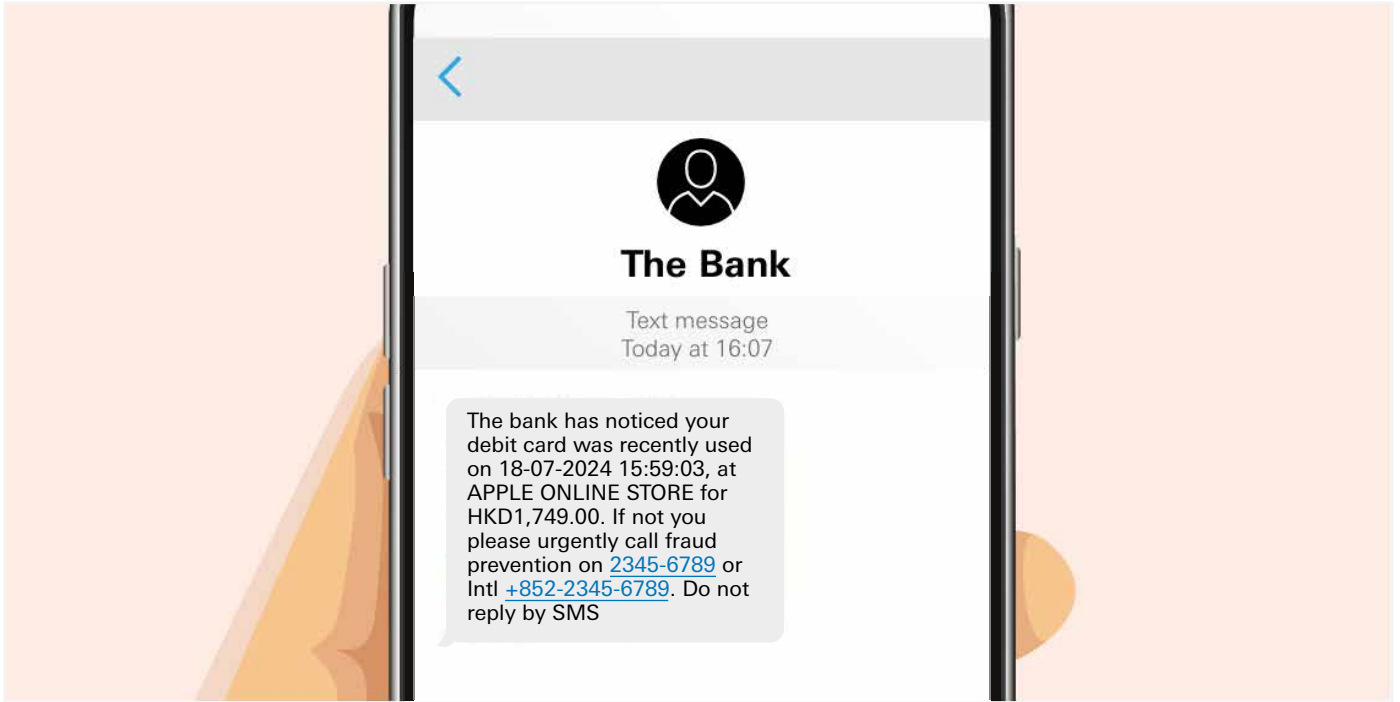
No customer name included again.

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?



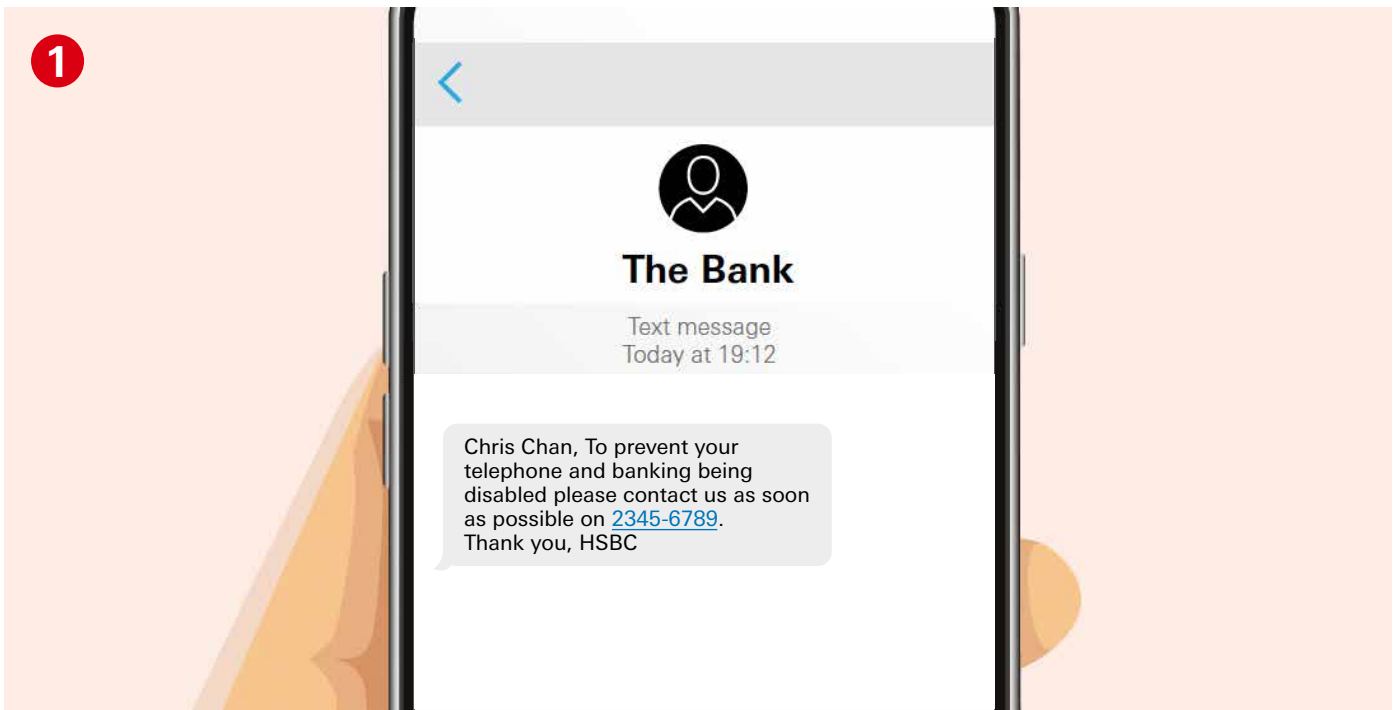
Stop and think.

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

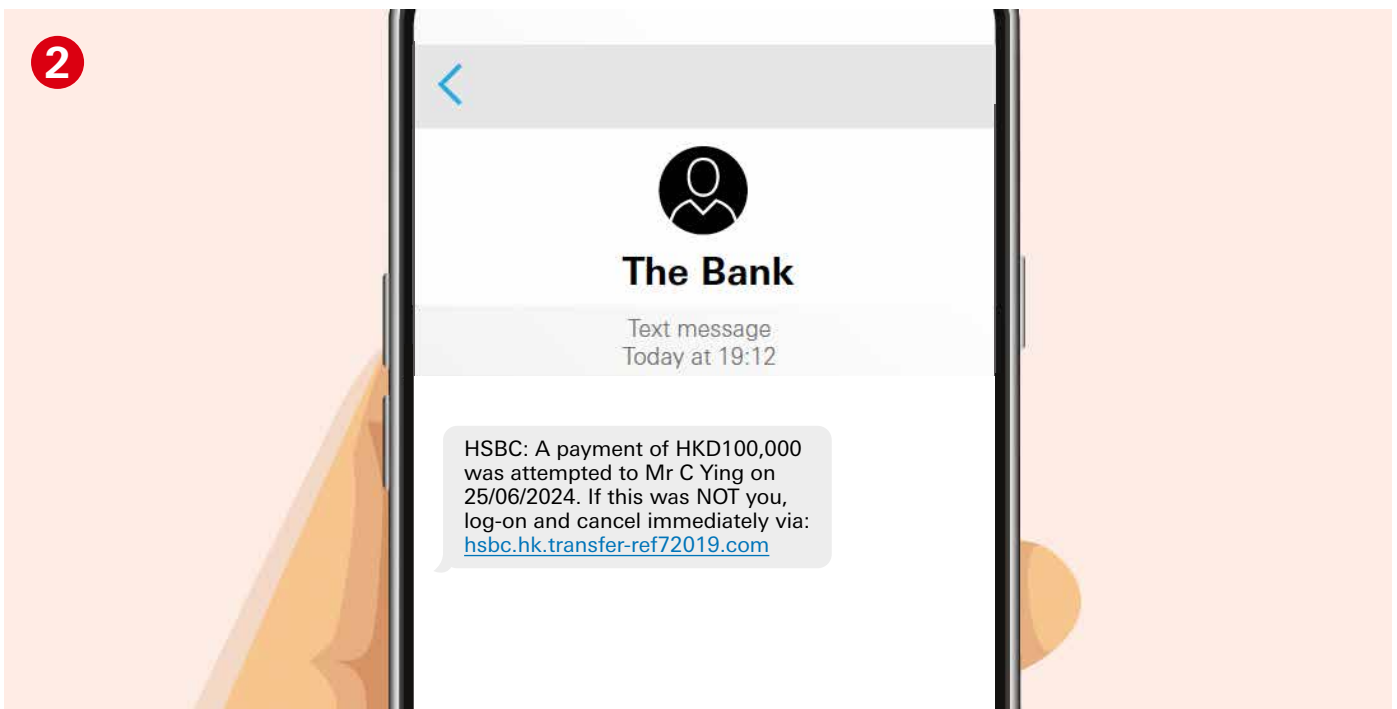
Answers:

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

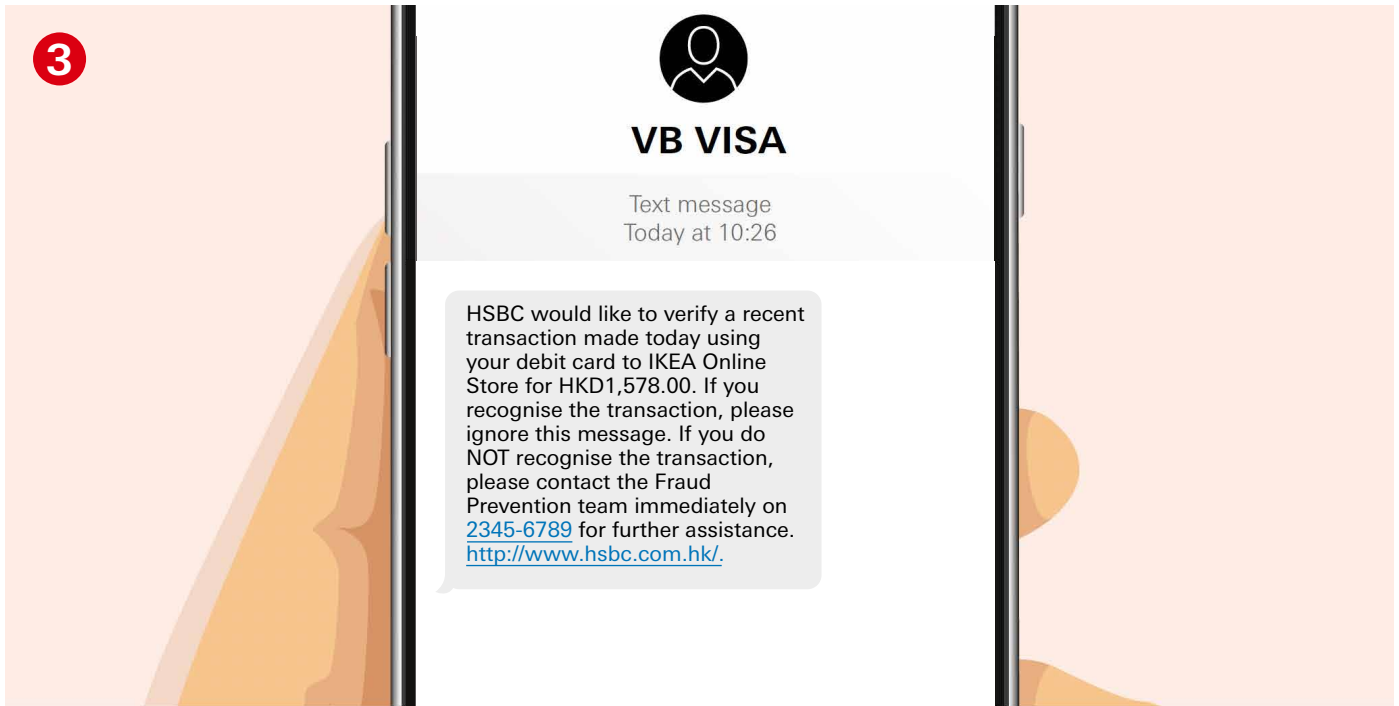


Legitimate Fraud

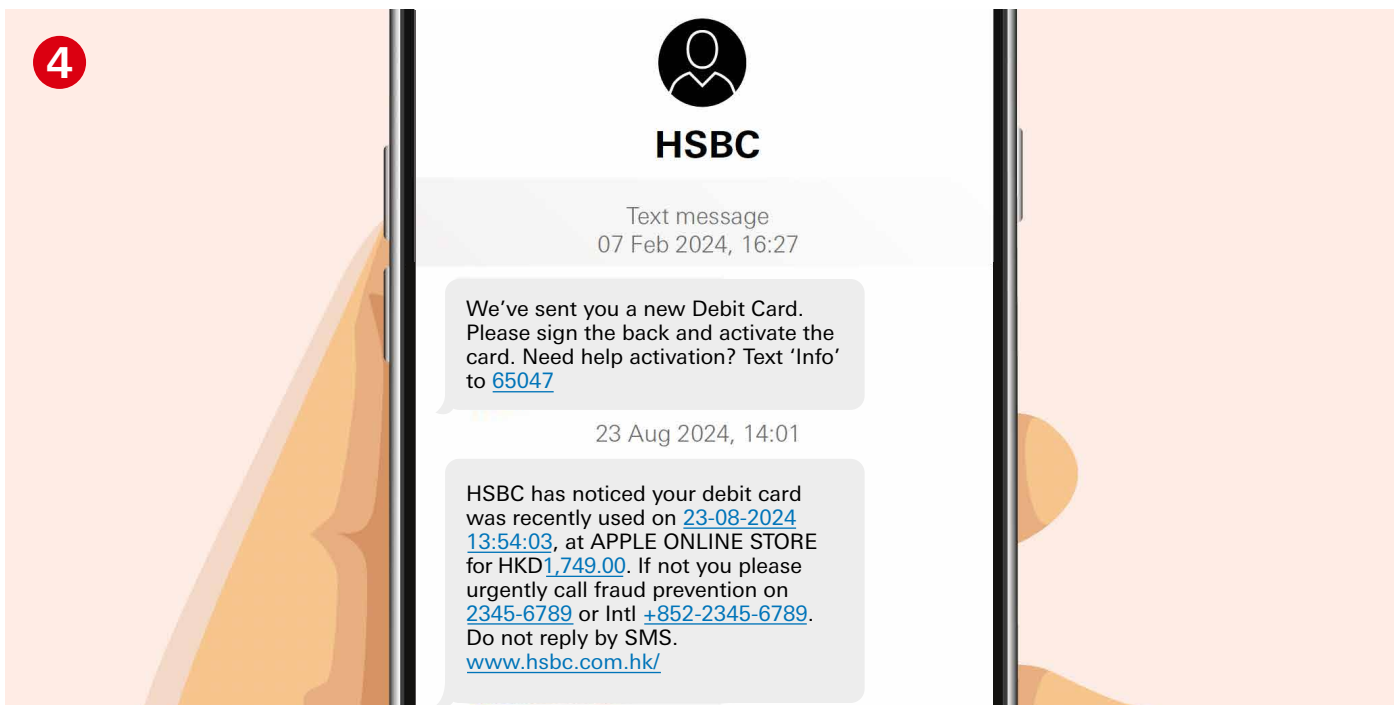
1. Fraud 2. Fraud

Answers:

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: