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.

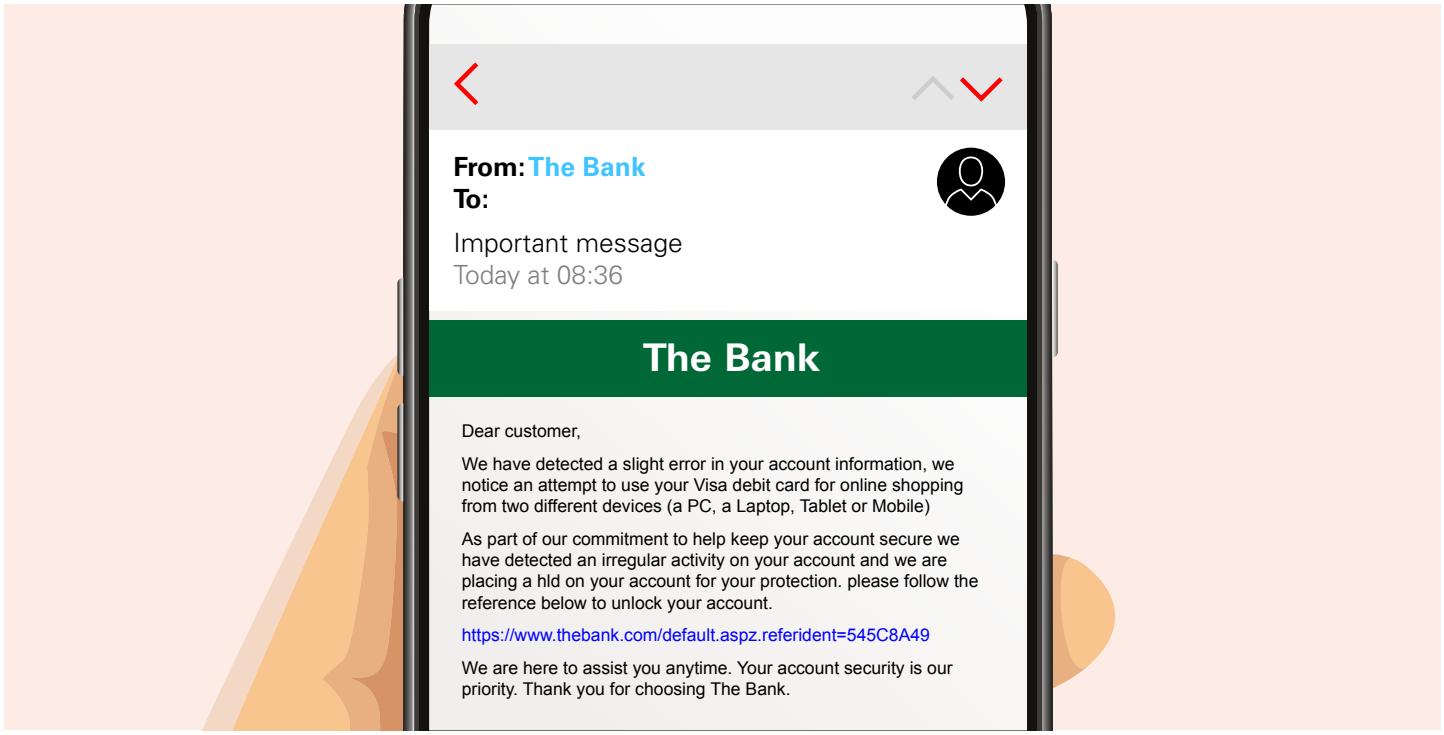
Personal information
Be wary of messages that ask for your personal information.

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?



.....

.....

.....

.....

.....

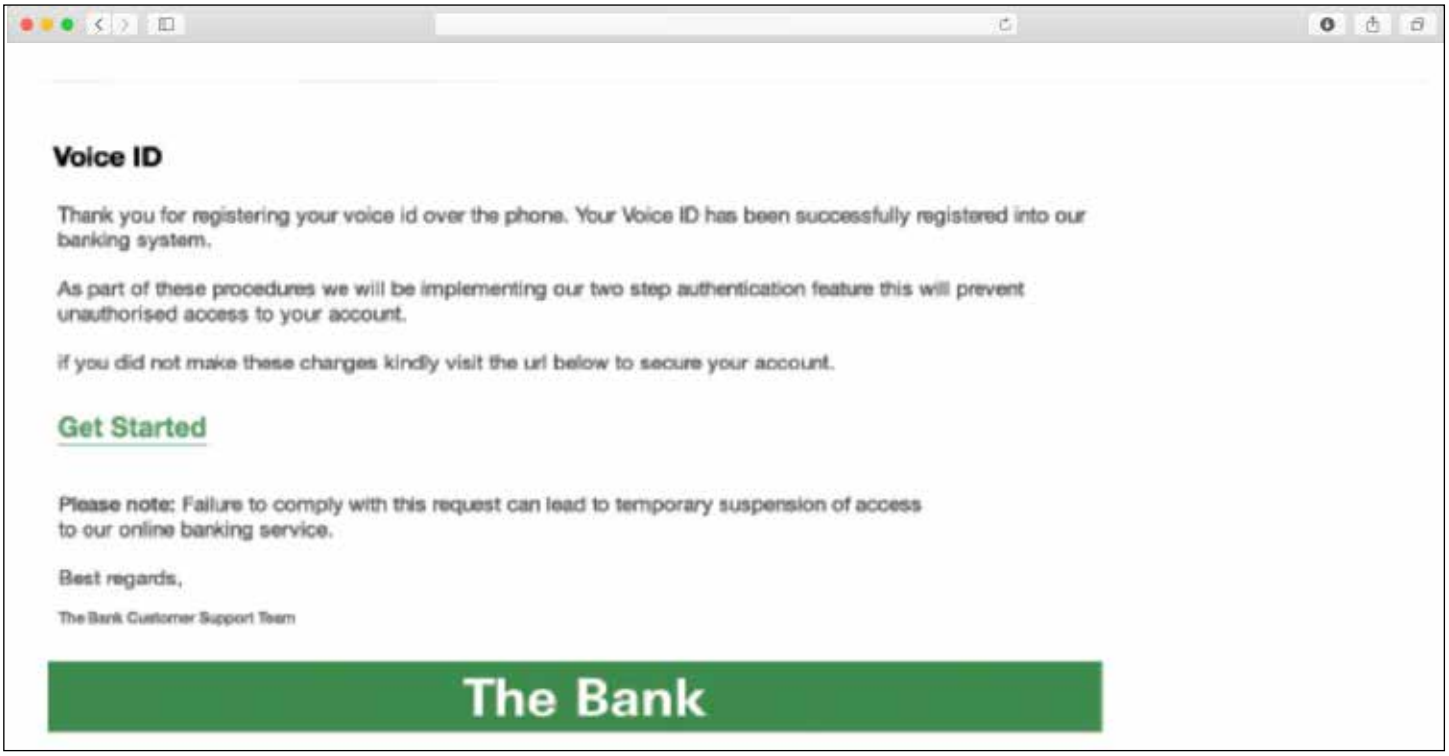
.....

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?



Voice ID

Thank you for registering your voice id over the phone. Your Voice ID has been successfully registered into our banking system.

As part of these procedures we will be implementing our two step authentication feature this will prevent unauthorised access to your account.

if you did not make these changes kindly visit the url below to secure your account.

Get Started

Please note: Failure to comply with this request can lead to temporary suspension of access to our online banking service.

Best regards,

The Bank Customer Support Team

The Bank

.....

.....

.....

.....

.....

.....

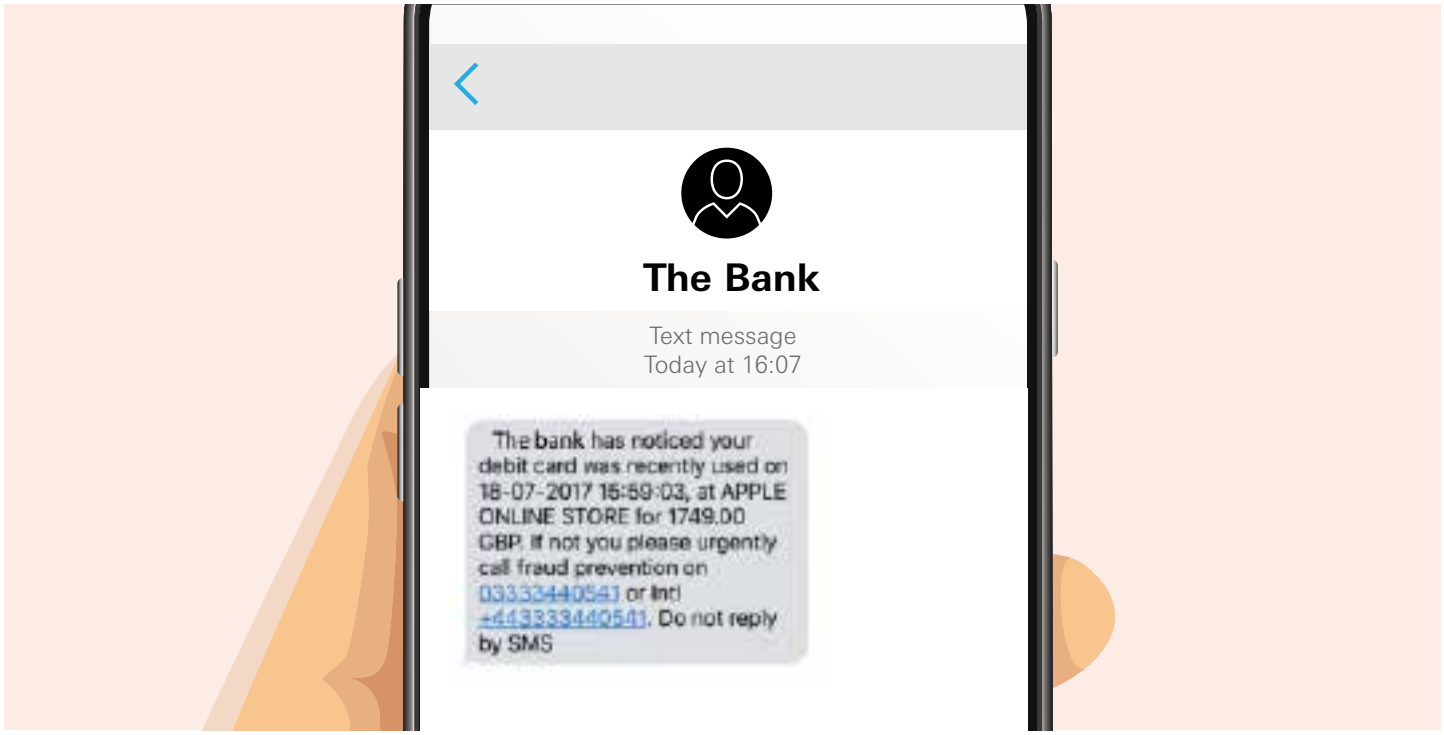
.....

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?



.....

.....

.....

.....

.....

.....

Answers:

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

Stop and think.

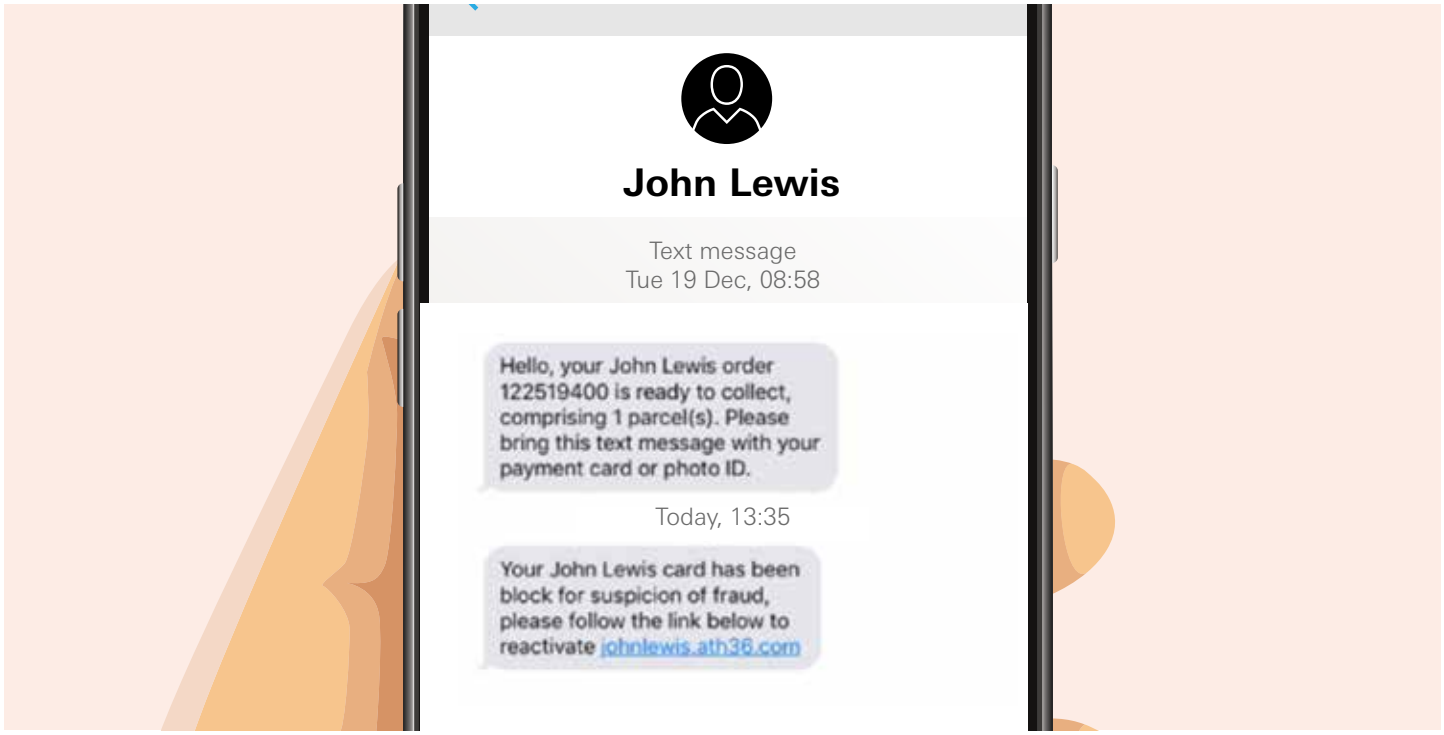
Do you remember buying what's described?

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

Some text message scams can appear to be from organisations that you trust. Why could this text message be fraudulent?



.....

.....

.....

.....

.....

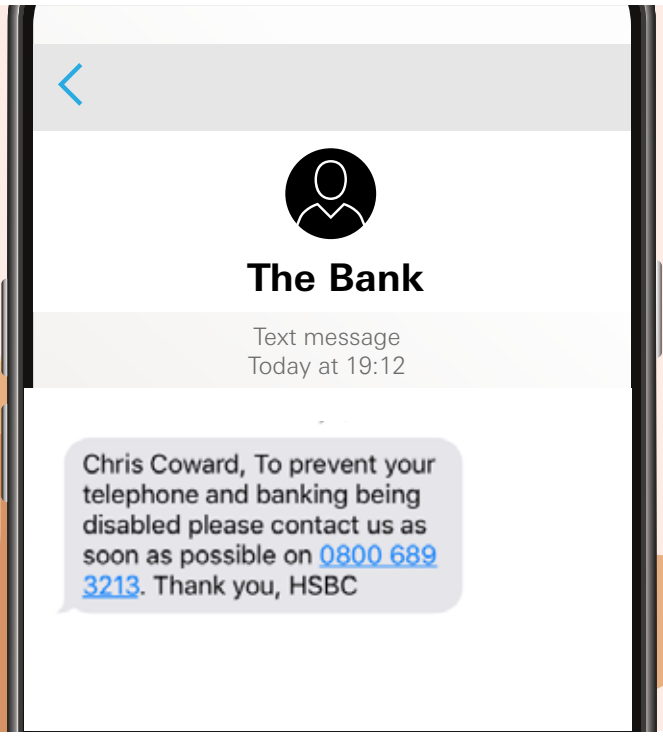
.....

Answers:
This was a tricky one! Here that the fraudulent message has appeared in a genuine SMS thread from HSBC. The first message in the thread was legitimately sent by the bank. Fraudsters can manipulate messages to appear that they were sent by HSBC.

Financial Education

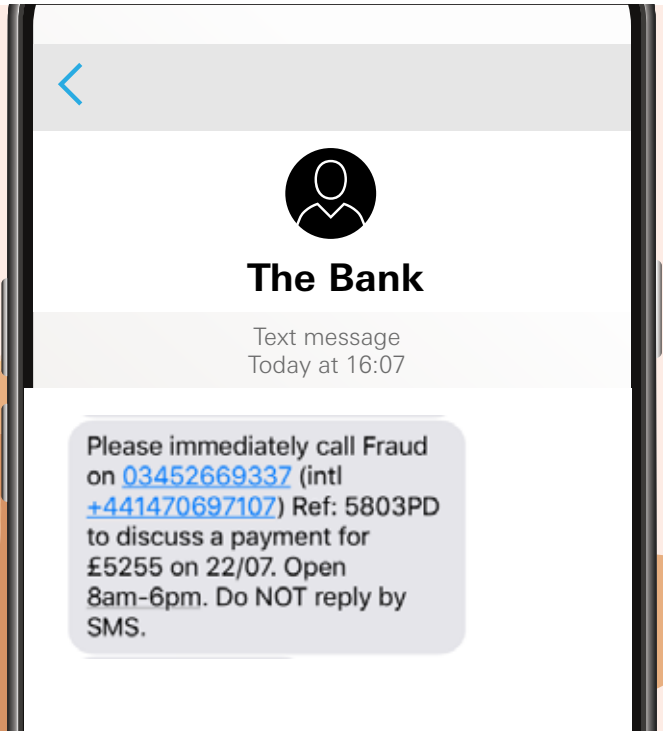
SMS Challenge 3: Spotting a fraudulent text

1.



☐ Legitimate ☐ Fraud

2.



☐ Legitimate ☐ Fraud

Answers: 1. Fraud 2. Legitimate

X3349

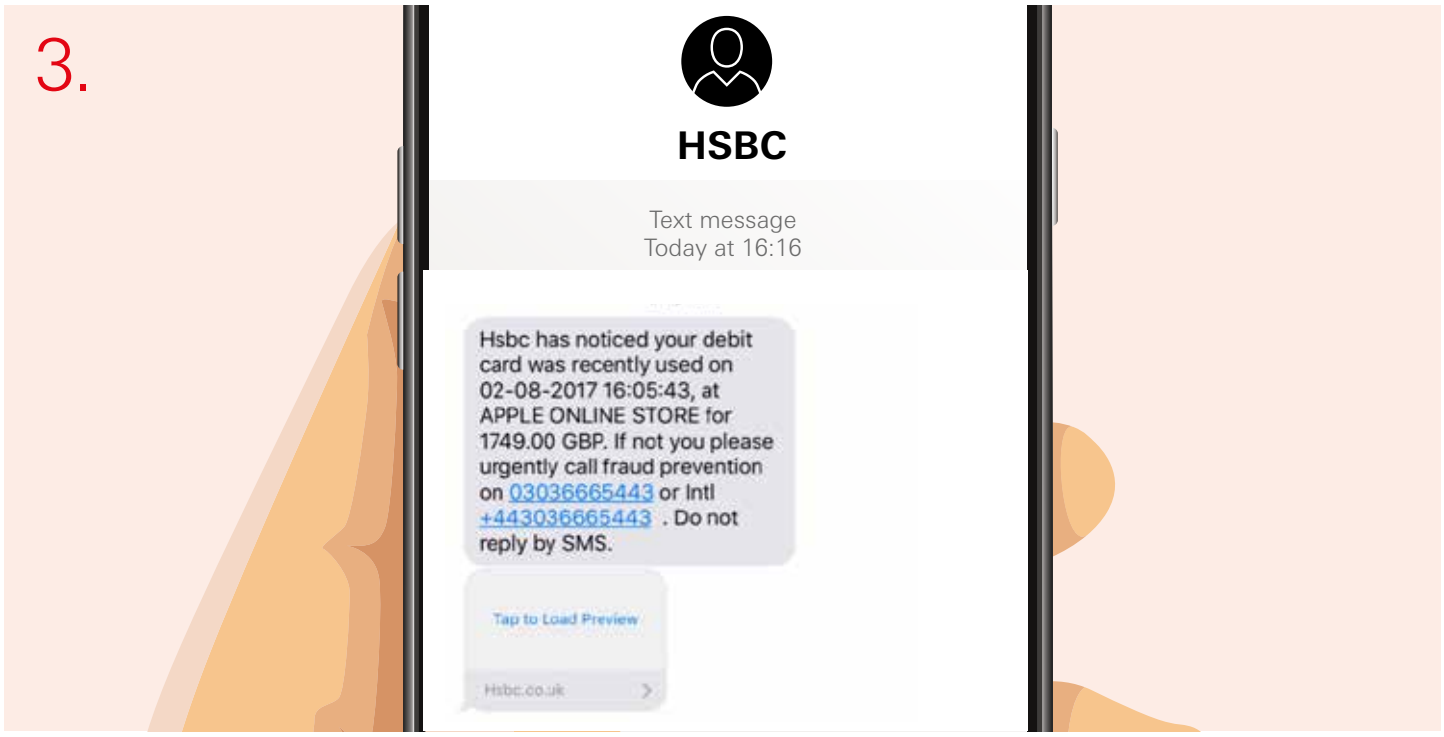
hsbc.co.uk/financial-education

HSBC UK

Name:

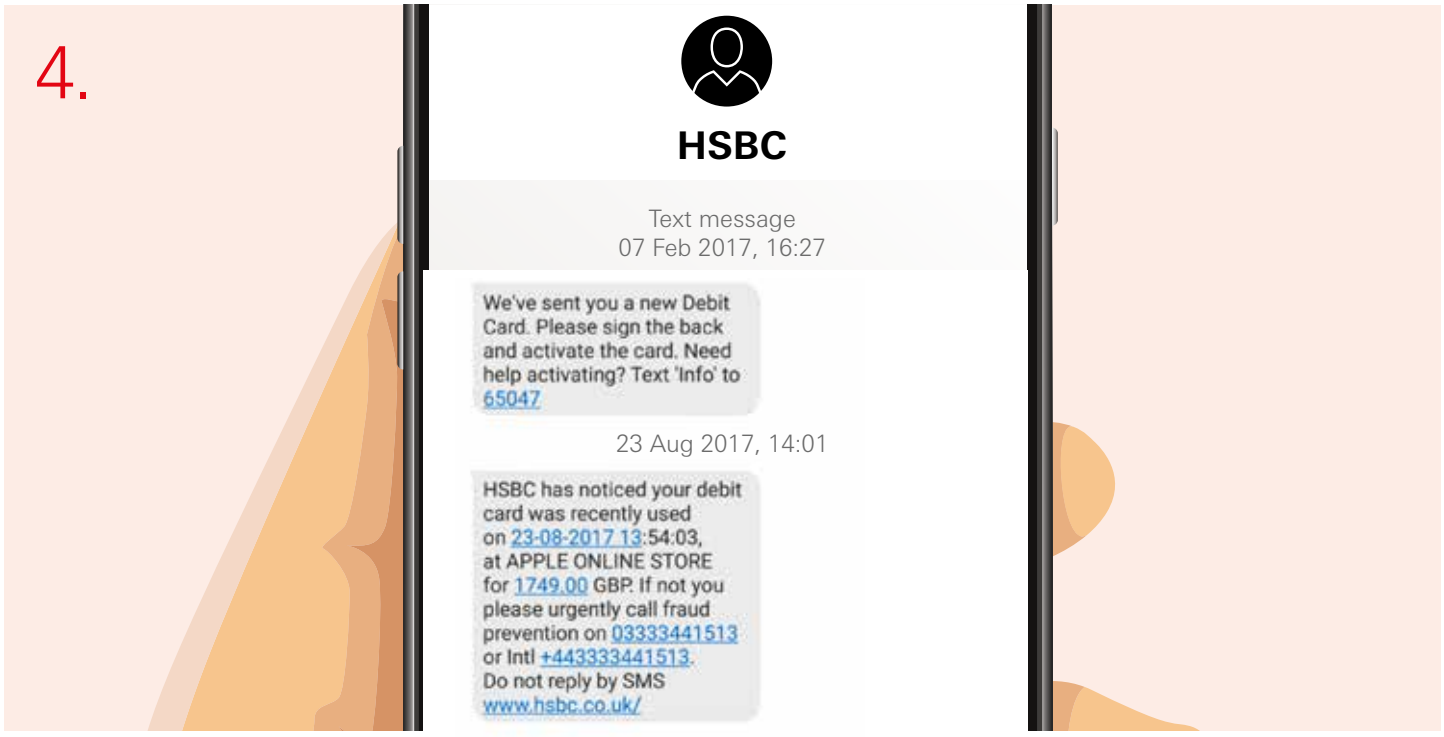
SMS Challenge 3: Spotting a fraudulent text

3.



☐ Legitimate ☐ Fraud

4.



☐ Legitimate ☐ Fraud

Answers: 3. Fraud 4. Fraud

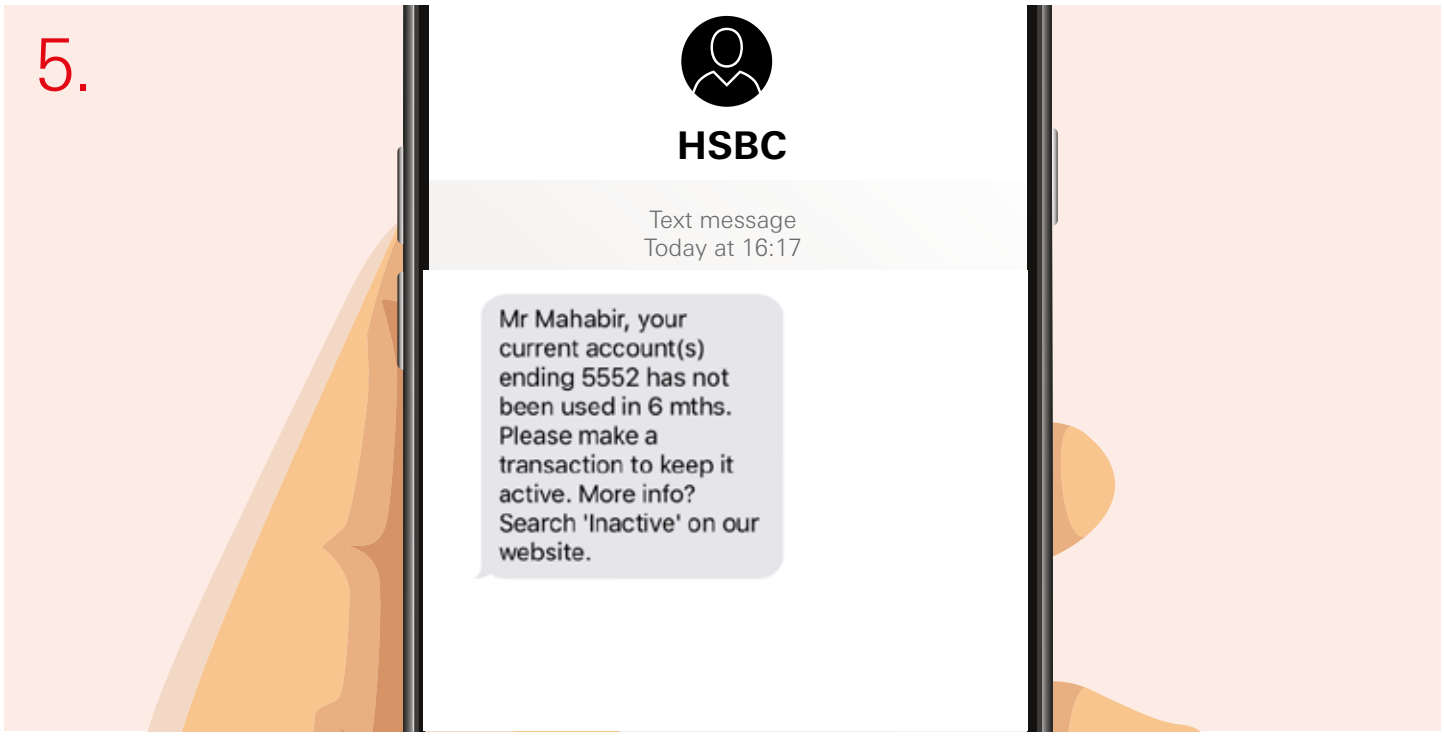
X3349

hsbc.co.uk/financial-education

Name:

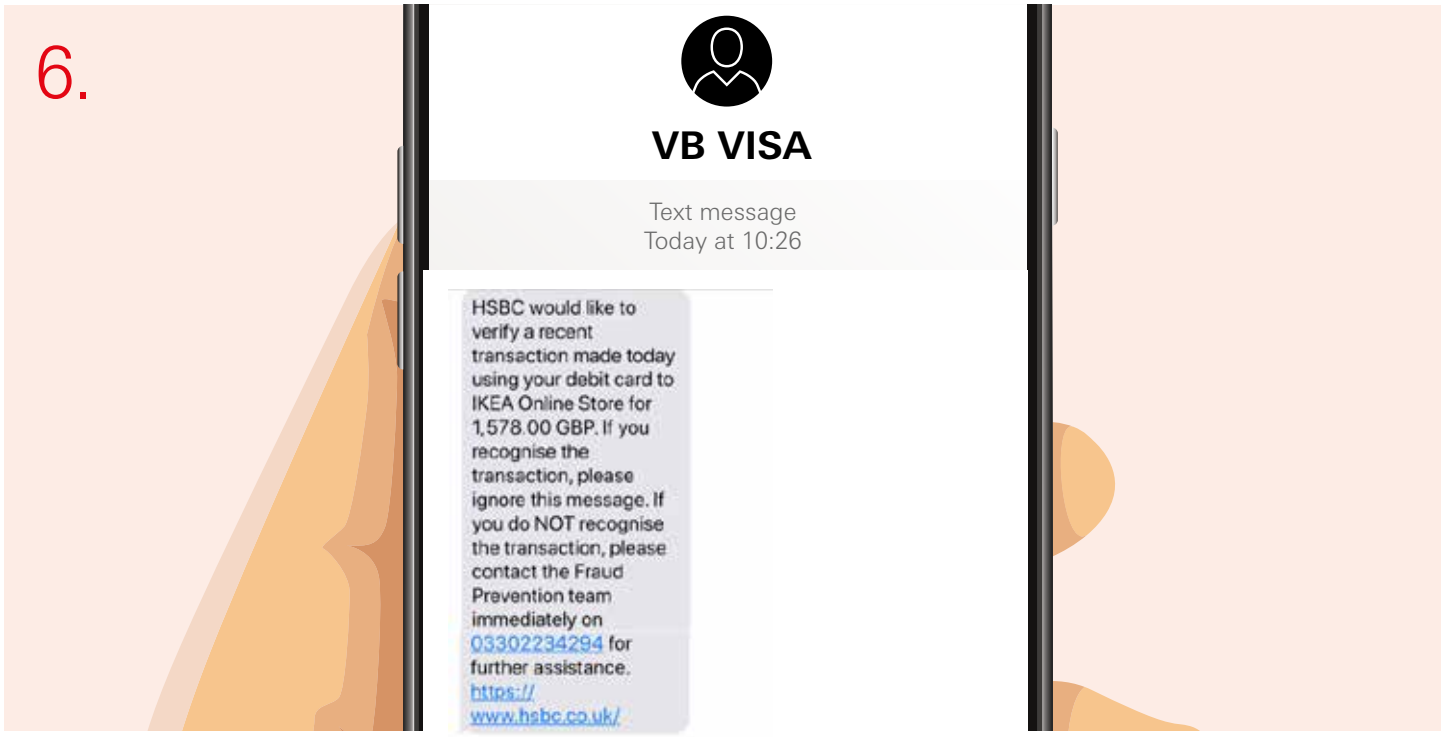
SMS Challenge 3: Spotting a fraudulent text

5.



☐ Legitimate ☐ Fraud

6.



☐ Legitimate ☐ Fraud

Answers: 5. Legitimate 6. Fraud

X3349

hsbc.co.uk/financial-education

Name:

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

Answers: 1B Never tell anyone your PIN; 2B This is known as being a Money Mule and is illegal in the UK; 3B This may leave you open to criminals seeing personal information about you; 4B It may not be your friend – check with them in person first; 5B 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; 6B Make sure you have the lost/stolen number from the back of your card recorded in your mobile.