



Introduction to fraud and scams

Age range: 11-14



Sam's story

2

"Sam is 20 years old. He left school two years ago and has been working at a call centre, earning £22,000 per year. Pay day is the last Friday of the month and that night is always a celebration. Sam will take £100 from the cash machine when he leaves work and meets his friends, and usually has around £10 left on Saturday morning."

Sam's story

"Sometimes Sam will spend extra money that evening using his debit card, but doesn't keep his receipts or check his balance the next day to keep track of it. On the first Saturday after pay day Sam will make a trip to the shops and buy clothes on one of his credit cards without checking his statement to see how much money he already owes."



Sam's story

"Sam has given the same PIN to all of his debit and credit cards so it's easy to remember – 1234. He also uses this as his passcode for his mobile banking app, just adding 56 as it needs to be six digits long. Sam has a laugh at friends who forget their PIN and will regularly tell them to keep it simple and use a number like his. He has multiple social media accounts, and low privacy settings as he likes everyone to know when his birthday is and when he's going on holiday."



Sam's story

"Sam was putting his bank statements in the bin when they arrived in the post, but has switched to paperless banking so he doesn't have to worry about them stacking up anymore. At the end of the month, Sam will pay the minimum amount necessary on each credit card. On a couple of occasions this has been a problem because Sam did not have enough left in the bank and hadn't checked his bank account online to see what he had spent."

What could Sam do to improve his money management, and make sure he stays safe?



Sam's action plan: student sheet

What are Sam's bad habits?	What are his good habits?
What actions could Sam take to adjust his money management and stay safe online?	

Definition of fraud and scams

- **Fraud:** when your account or card has been accessed, stolen or used without your knowledge. It can also be when a fraudster opens an account using your identity.
- **Scams:** are a type of fraud. When you're duped into making a payment by bank transfer for something you thought was genuine, like goods or services, which turn out to be fake. This can lead to a loss of money or services.



Match the term to the definition

Term	Definition
Online purchase scams	A scam to access valuable personal details by using QR codes which ask you to download an attachment or follow a link to a website containing malware, which can collect secure information.
Social engineering	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Vishing	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Phishing	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Quishing	Fraudsters send emails that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, for example, due to an unauthorised payment.

Definition of terms: answers

Term	Definition
Online purchase scams	
Social engineering	
Vishing	
Phishing	
Quishing	

Definition of terms: answers

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	
Vishing	
Phishing	
Quishing	

Definition of terms: answers

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	
Phishing	
Quishing	

Definition of terms: answers

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing	
Quishing	

Definition of terms: answers

9

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing	Fraudsters send emails that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, for example, due to an unauthorised payment.
Quishing	

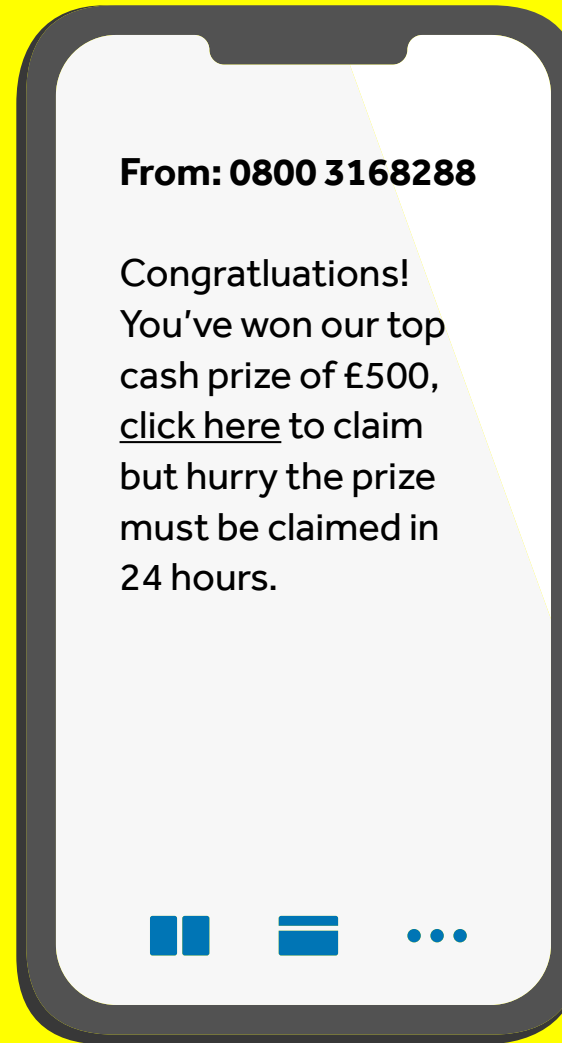
Definition of terms: answers

9

Term	Definition
Online purchase scams	Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.
Social engineering	Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.
Vishing	A phone call from a fraudster posing as an employee of a reputable company, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.
Phishing	Fraudsters send emails that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, for example, due to an unauthorised payment.
Quishing	A scam to access valuable personal details by using QR codes which ask you to download an attachment or follow a link to a website containing malware, which can collect secure information.

Spam text messages

10

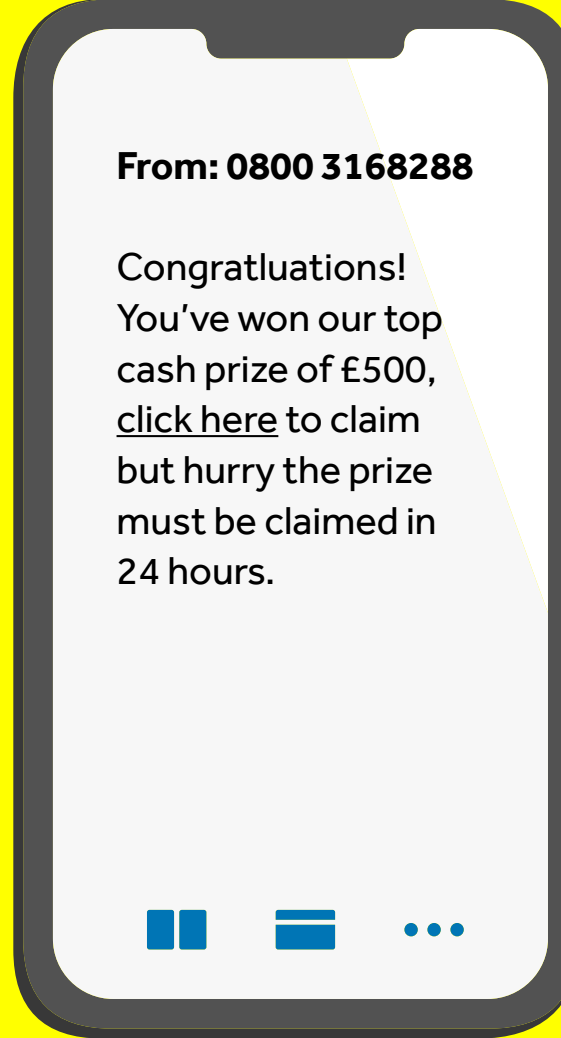


Spam text messages

11

Phone number

A number you might not recognise, but sometimes they are created to look similar to a number you might recognise. This is called number spoofing.

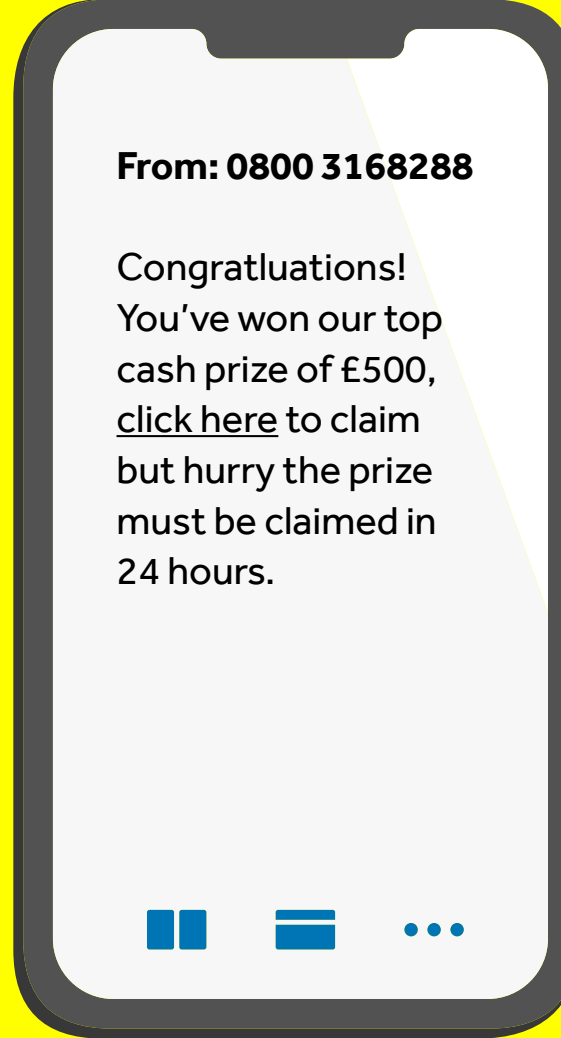


Spam text messages

12

Phone number

A number you might not recognise, but sometimes they are created to look similar to a number you might recognise. This is called number spoofing.



Spelling mistakes

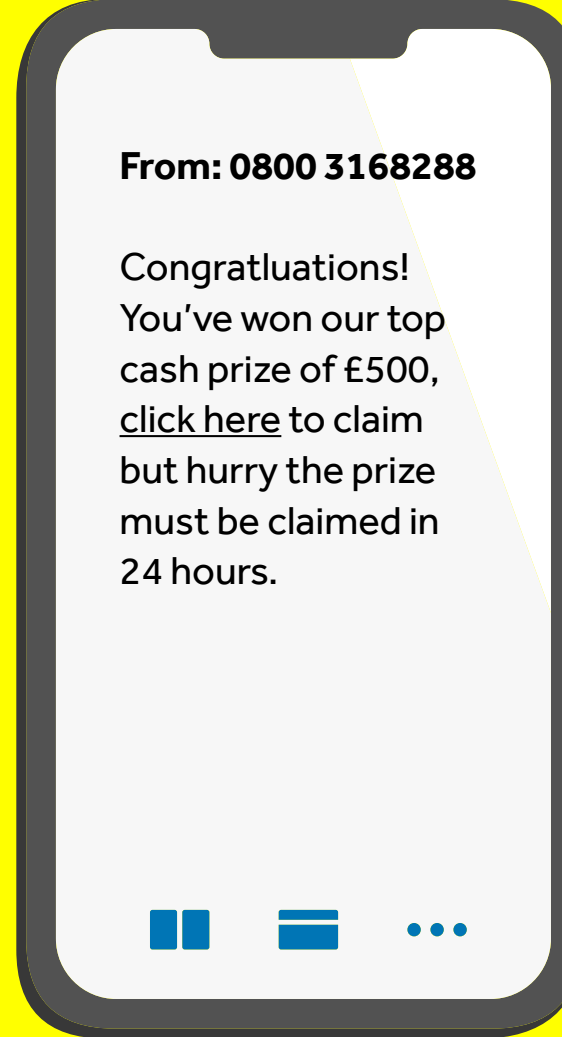
Spelling mistakes can be a sign it's not from a genuine sender.

Spam text messages

13

Phone number

A number you might not recognise, but sometimes they are created to look similar to a number you might recognise. This is called number spoofing.



Spelling mistakes

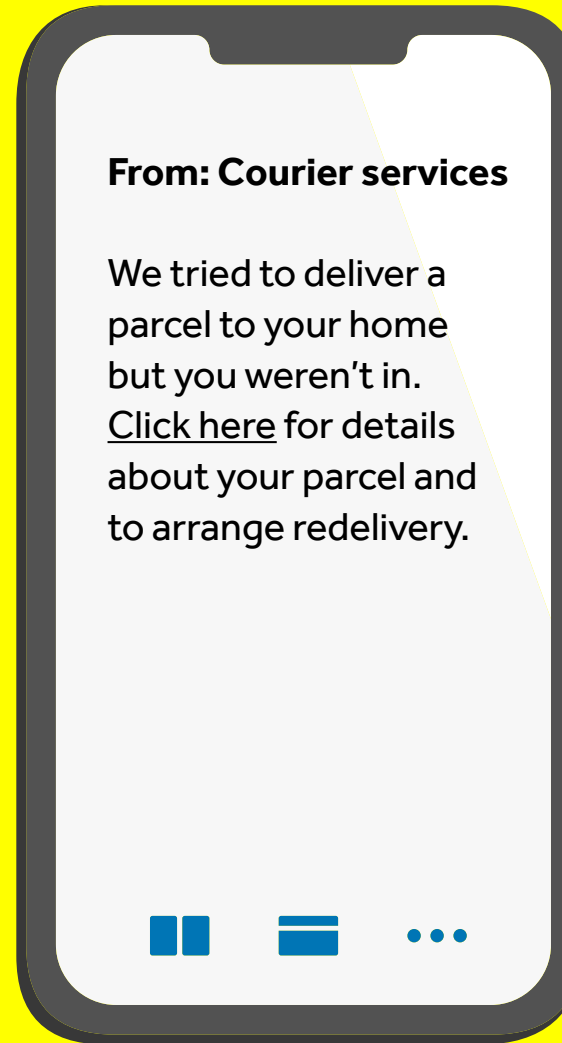
Spelling mistakes can be a sign it's not from a genuine sender.

Offering a prize or reward

Tries to entice people in and excite them without thinking, regarding a competition they have not entered.

Spam text messages

14

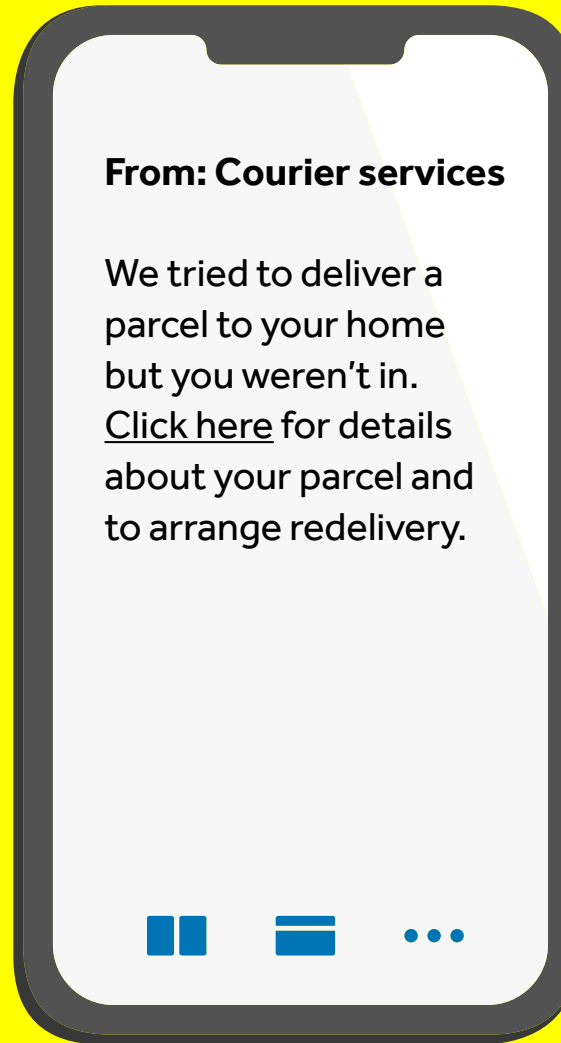


Spam text messages

15

From

Can appear to be from a professional company, even one you might recognise.



Spam text messages

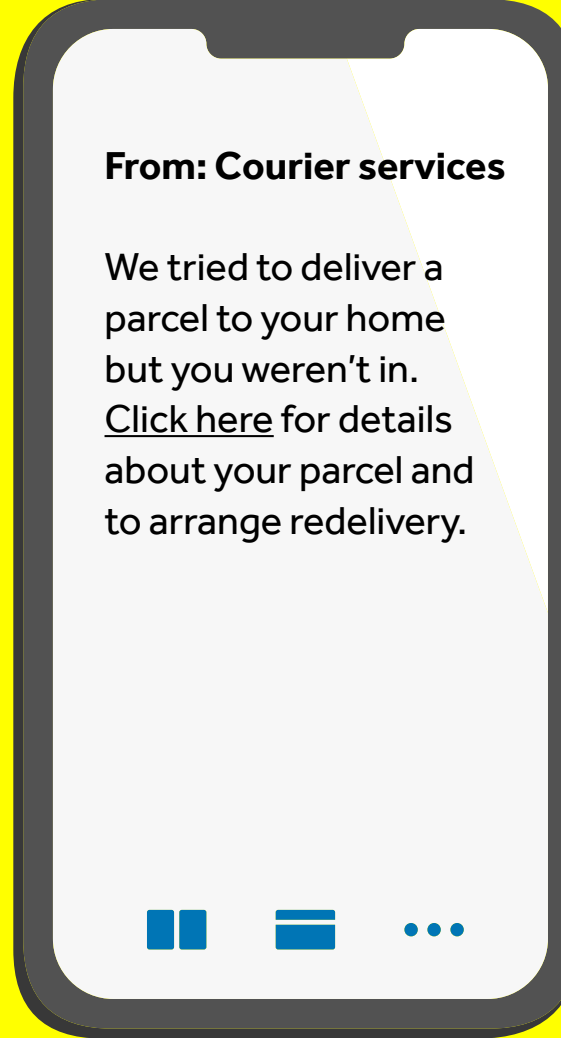
16

From

Can appear to be from a professional company, even one you might recognise.

Details about your parcel

This is designed to spark your curiosity to see what the package is.



Spam text messages

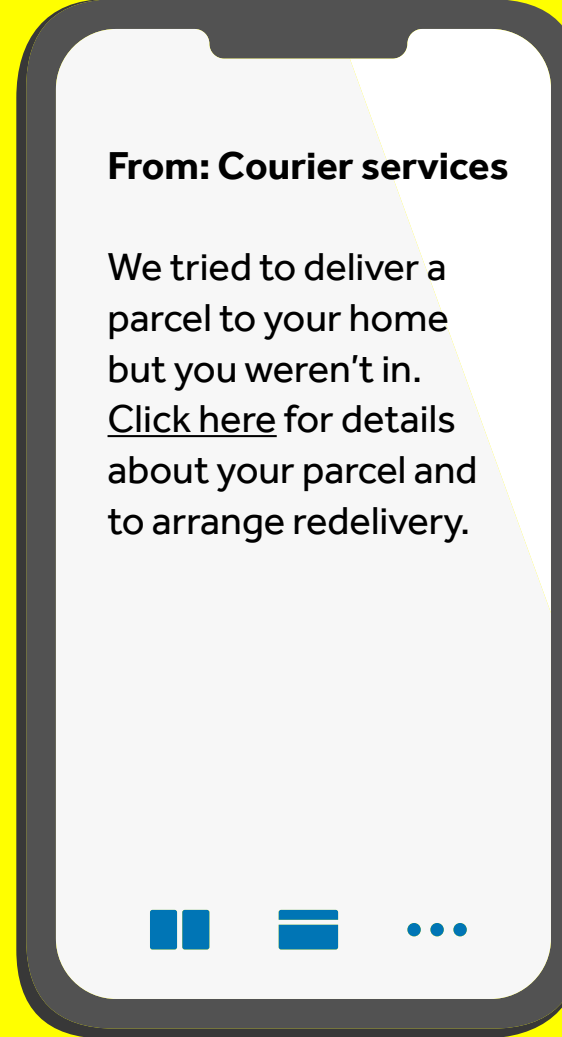
17

From

Can appear to be from a professional company, even one you might recognise.

Details about your parcel

This is designed to spark your curiosity to see what the package is.

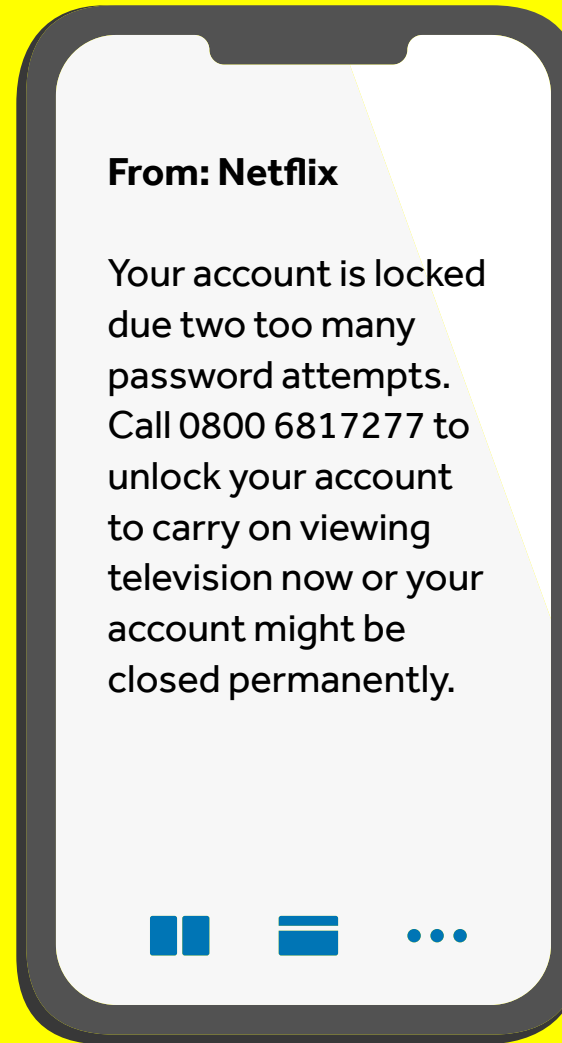


Click here

Be careful if you are asked to click on a link as you might be directed to a fake website where your login and personal details are requested and stolen, or your device could be infected by a virus.

Spam text messages

18

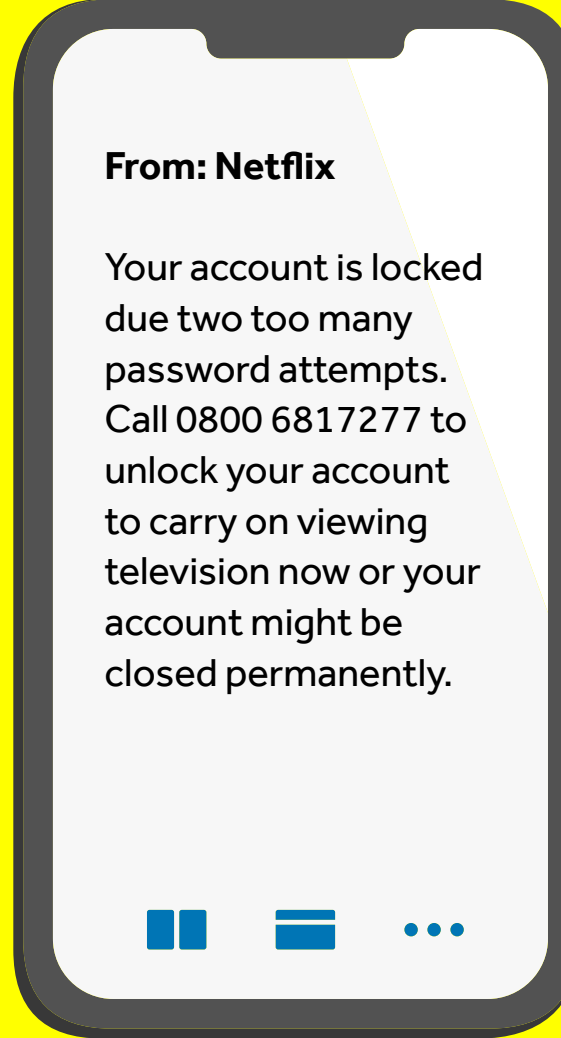


Spam text messages

19

Closed permanently

Fraudsters can make you panic in an attempt for you to respond quickly without thinking.



Spam text messages

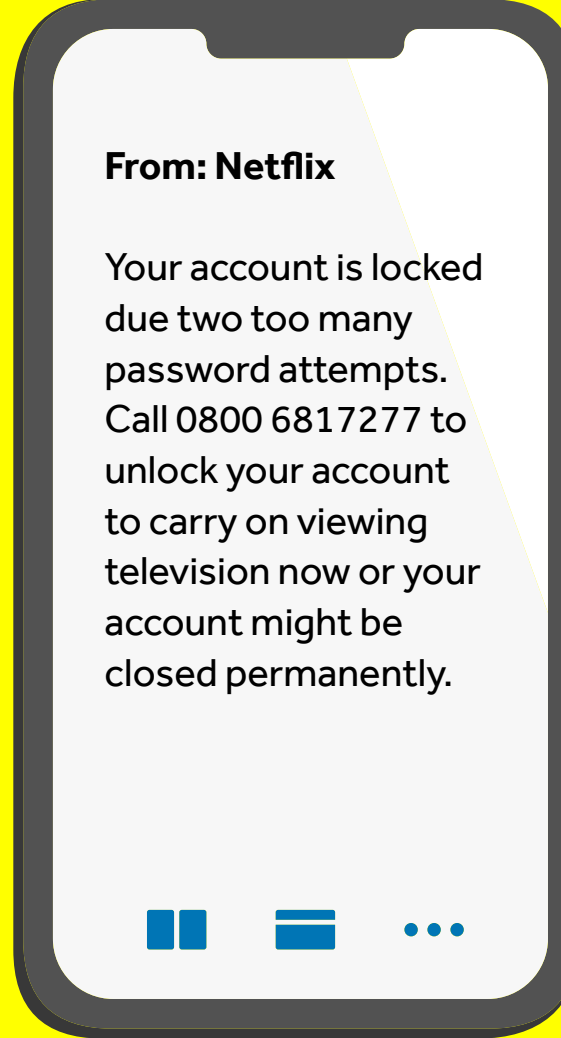
20

Closed permanently

Fraudsters can make you panic in an attempt for you to respond quickly without thinking.

Spelling/grammar mistakes

Spelling mistakes can be a sign it's not from a genuine sender.



Spam text messages

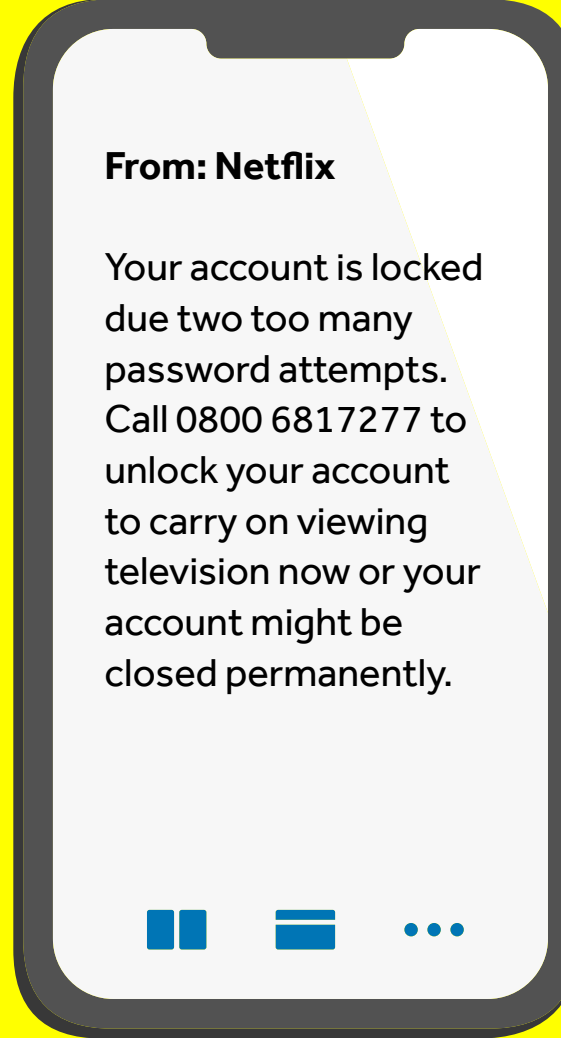
21

Closed permanently

Fraudsters can make you panic in an attempt for you to respond quickly without thinking.

Spelling/grammar mistakes

Spelling mistakes can be a sign it's not from a genuine sender.



From

Can seem like it's from a company you know and trust.

Spam text messages

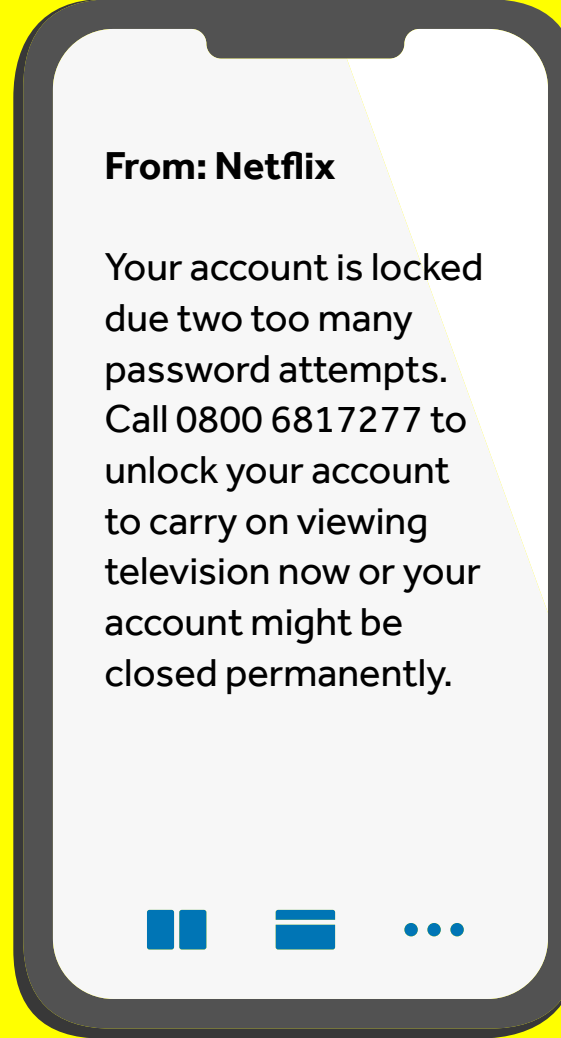
22

Closed permanently

Fraudsters can make you panic in an attempt for you to respond quickly without thinking.

Spelling/grammar mistakes

Spelling mistakes can be a sign it's not from a genuine sender.



From: Netflix

Your account is locked due two too many password attempts. Call 0800 6817277 to unlock your account to carry on viewing television now or your account might be closed permanently.

From

Can seem like it's from a company you know and trust.

Call 0800 6817277

Be careful if you are asked to call a number, you could potentially be directed to speak to the fraudsters who would try to get login or personal details in an attempt to steal money.

Money mules

A money mule is someone who is asked by someone, that could be a stranger or even a person known to them, to receive money into their bank account and transfer it onto another account, or allows a third party to take control of their account. The money being transferred is the proceeds of crime and as such a money mule is involved in money laundering.

This is a serious crime where the proceeds are often used to commit other serious offences such as drug dealing, people trafficking and terrorism.



Case study 1 – Priya

"Priya had been looking for a weekend job to earn some money, when she was approached outside her college by someone who offered her a way of making easy cash. They asked Priya to share her bank details so that money could be transferred into her account for a short period of time.

She agreed when they said that whilst £500 would be transferred in, only £450 would be taken out and she could keep the rest."

24



Case study 2 – Jack

"Jack is approached via social media by Lewis who goes to his school and is a few years older than him. Lewis asks how Jack is, then tells Jack that he will need his debit card and pin number as he needs to use his account."

Lewis tells Jack he will get £50 for agreeing and if he doesn't he will be in trouble. Jack is reluctant but agrees as Lewis is part of a gang and he is worried about the consequences of not agreeing, there is also a new game he could buy with the money."

Jack agrees to give Lewis his debit card and pin the next day at school."

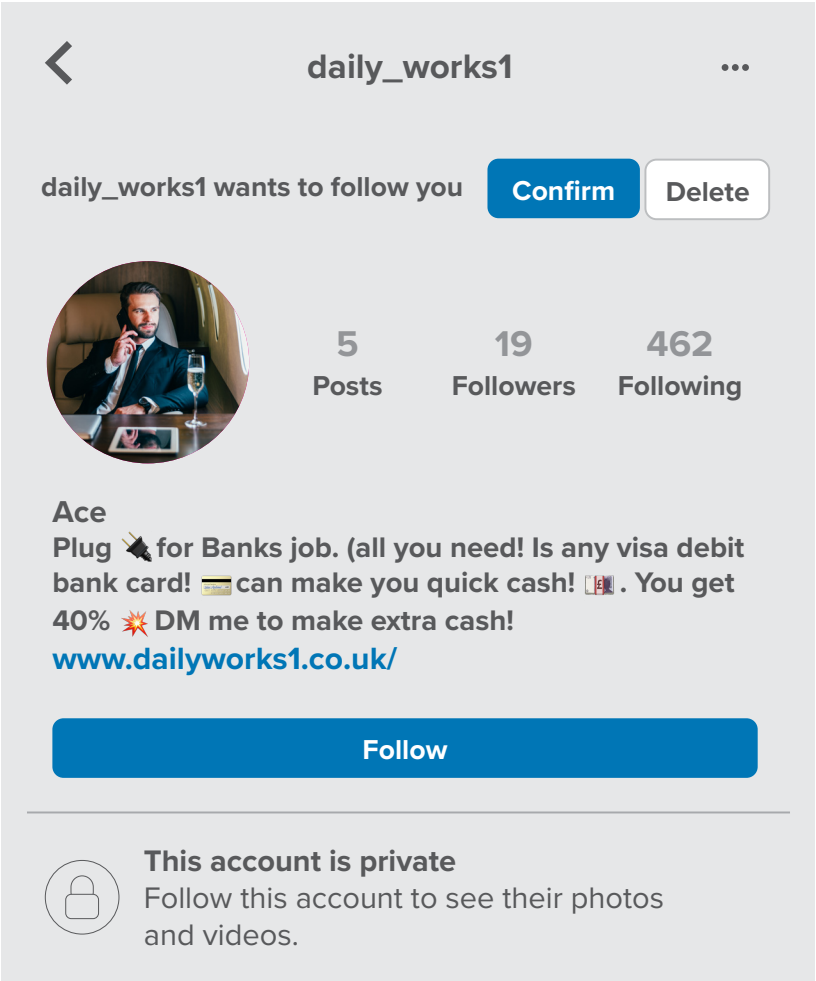


Being approached as a money mule

26



What might an approach look like on social media



Quick quiz

28

What is the most common way 12- 18 year olds are approached by scammers?

What is an attempt to get sensitive information by texts or SMS called?

What is fraud?

What is a scam?

Quick quiz

28

What is the most common way 12- 18 year olds are approached by scammers?

Social media.

What is an attempt to get sensitive information by texts or SMS called?

What is fraud?

What is a scam?

Quick quiz

28

What is the most common way 12- 18 year olds are approached by scammers?

Social media.

What is an attempt to get sensitive information by texts or SMS called?

'Smishing'.

What is fraud?

What is a scam?

Quick quiz

28

What is the most common way 12- 18 year olds are approached by scammers?

Social media.

What is an attempt to get sensitive information by texts or SMS called?

'Smishing'.

What is fraud?

Transactions carried out by a third party which are not authorised by the customer.

What is a scam?

Quick quiz

28

What is the most common way 12- 18 year olds are approached by scammers?

Social media.

What is an attempt to get sensitive information by texts or SMS called?

'Smishing'.

What is fraud?

Transactions carried out by a third party which are not authorised by the customer.

What is a scam?

Transactions in which the customer has been convinced or coerced to make the transaction.

Top tips for staying safe online

1. Check which personal information is public on your social media accounts, e.g. your birthday, hometown, pet names, holiday dates, job title. Fraudsters can use this information to steal your identity and apply for bank accounts or buy products in your name.
2. Be wary if you see encouragement to click on an unknown link – if you're not sure, visit the organisation's website directly.
3. Never share your PIN, bank details or passwords with anyone who contacts you through text, email, phone or in person, and don't write them down. Never let anyone else access your account.
4. Remember that letting someone else use your bank account is a potentially serious crime which could damage your financial future, so take time to think it through and talk to an adult you trust.
5. Phone organisations directly from the number listed on their website to verify who is contacting you.
6. Password protect your devices using random words and include symbols, numbers and capitals. Set passwords to be at least 10 characters long and don't use the same passwords for different accounts.
7. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping.
8. Hover over links before clicking on them to reveal the web address destination.
9. Install anti-virus software on your laptop and any other personal devices and keep it up to date.
10. If you have any concerns, share them with someone you trust, whether it's a parent, tutor or friend. Remember not to talk to strangers in person or online, even if they send follow up messages. Resist the urge to reply.