TransUnion

Fraud Education Programme

Lesson Plan Slides

Fraudsters are clever – but you're smarter



TransUnion International UK Limited, registered in England and Wales with company number 3961870.
Registered office: One Park Lane, Leeds, West Yorkshire LS3 1EP. Authorised and regulated by the Financial Conduct Authority.

Part One: What is fraud?

Q. What is online fraud?

A. “Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person”. Source - Report Fraud

Q. Has anybody been a victim of fraud themselves or know anybody else who has e.g. a family member?

Q. Can you name different types of fraud that young people are most vulnerable to? and why?

A. 4 types of fraud, young people are most vulnerable to are:

1. Buying goods online and paying upfront
2. Banking Fraud and Money Mules
3. Scams, meeting people online – any fraud that happens online
4. Identity theft

Why? Because they are high online activity, risk takers, lack of awareness, use weak passwords, peer pressure, social inclusion, trusting by nature

Q. What are the consequences of committing fraud?

A. Many consequences which include:

- Prison - up to 10 years = a criminal record
- Fines
- Blocked from opening a bank account or getting a student loan
  Thrown out of college or university
- Unable to get a job due to a criminal record
- Emotional and psychological impact
- Lose friends or damage relationships

© 2025 TransUnion International UK Limited. All Rights Reserved.

Part two: Case studies

Small group or work in pairs

1. **Allocate and find the case studies in your Fraud Education Handbook.**
   - The case studies can be found on pages 7-20:
   - Case study one: Chloe's new friend, page 7
   - Case study two: Online shopping and scams – Olivia's bad purchase, page 10
   - Case study three: Money Mules – Jack's #EasyMoney, page 13
2. **Read through one case study which includes:**
   - The task
   - Meet the victim and fraudster
   - The story
   - Answer the questions, discuss in groups to present back to the class

The victim

Case study 1: Introducing Chloe

Meet Chloe, a 17 year old college student



Location: Urban UK

Education: Sixth form A-levels

Lifestyle: Active on Instagram, TikTok, and Snapchat using iPhone or her Chromebook. She's trying to build her following and has her profiles set to public.

Her content is focused on TikTok dances to the latest music, fashion and selfies. Lately she's been posting about her new car and passing her driving test.

Has a part-time job at a café to pay for her online shopping (fast fashion, tech and accessories). She got her own bank account so she can get paid and uses this to buy online items.

Personality:

- Friendly and outgoing – loves making new friends online and want to become a fashion influencer
- Trusting – tends to believe people who seem kind or share her interests
- Not very tech-savvy – doesn't fully understand privacy settings or data risks

Online Behaviour

- Uses public Wi-Fi often and reuses passwords across sites
- Uses hashtags like #OOTD, #UKTeens, #FashionInspo #FashionTok
- Accepts friend requests from people with mutual interests and sometimes shares personal info in DMs (e.g., birthday, school name)
- Has Find My Phone which her dad setup but she's never logged into it herself

Why She's a Target

- Her public profile makes it easy to gather personal info
- She's flattered by attention from older teens or young adults
- She's unaware of synthetic ID fraud or how her data could be misused
- She's less likely to report suspicious behaviour out of embarrassment

The fraudster

Case Study 1: Meet the Fraudster – The Friendly Faker

Fraudsters aren't always who we think they are, as in this example. Some fraudsters are opportunistic, while others operate within a crime gang, but all are perpetrators and committing a crime.



Alias: "Jay"

Age: "19"

Location: Unknown (possibly abroad or using VPNs) – frequently changing

Platforms: TikTok, Instagram, Snapchat, Discord, WhatsApp, Line

Goal:

- To collect personal information (like full name, date of birth, address, selfies, school name) to commit identity fraud or create synthetic identities.
- Poses as a peer or influencer
- Uses fake profiles with stolen photos
- Targets teens who are active online and appear independent

Tactics Used

- Pretends to be a young adult
- Uses fake photos (stolen from influencers or AI-generated)
- Builds trust slowly: Compliments, shares fake personal stories, pretends to have mutual interests and seems to follow teens across multiple platforms like you would a friend
- Creates urgency or emotional pressure: "I need your help with something personal" or "Can you send me a pic for a photo shoot?"
- Offers fake opportunities: Modelling gigs, giveaways, or exclusive invites via phishing links or malware
- Exploits shame and fear to silence victims
- May impersonate brands or use deepfake tech

The story

Case study 1: Story | Chloe's "new friend"

Chloe is contacted by someone who seems charming and shares her interests in fashion and music on Snapchat. He's a little bit older, so it's really flattering and he builds trust by taking an interest in her, asking questions about her school, subjects and her hometown. He lives not too far away but he can't meet her at the moment because he's busy with his new job. He regularly sends daily Snaps about his day and she has shared her TikTok, insta and discord handles where he also likes her stories…but he never has time to go on video because of his new job.

Jay thinks Chloe is so beautiful, and is always asking for selfies in her latest looks, though he prefers to just see her smiling face. He's just started working at a fashion brand PR company as an intern. He says his job is to find new talent to do collabs with Shein and Temu, and he thinks she'd be perfect since her following is growing across TikTok and insta. He sends her a link to a fake brand collab opportunity form. She clicks the link and is taken to the fake website which looks professional and features lots of photos of people wearing the latest Temu and Shein clothes. Chloe thinks Jay must be good at his job and is impressed. Jay say's to get started she needs to pay a small fee and asks her to move money to his bank account. Eagerly, Chloe does that, it's not much money only £50 and if this gives her the break she needs to get into the fashion industry then what's the harm. Jay asks her for photos of herself, including in her underwear, so that he can pass them onto Temu and Shein. He asks for more money as there are more fees to pay and said they needed to be paid today, as he was speaking with both companies later on. He begins to manipulate Chloe, by making more promises she's going to be a big hit with Temu and Shein, Chloe is brimming with confidence and can't believe her luck! Unbeknown to Chloe, Jay is not the person she thought he was.

Jay has used Chloe's personal information from the form and her photos, to create a false identity which he's used to open bank accounts in her name. Jay had also used Chloe's personal information to gain access to her bank account and emptied her savings accounts. It's not until Chloe couldn't access her social media platforms that she realised something was very wrong.

It all happened so quick. Chloe couldn't believe she had been so silly to think this give her the break she needed. Jay had been so nice and helpful. Chloe felt violated. Confused. Embarrassed. Angry. She didn't know who to tell. Would they blame her? Would they understand?

Why This Story Matters

Chloe's experience isn't rare. Young people are increasingly targeted by online fraudsters who want to steal your personal information and banking information. It isn't personal. Fraudsters look for vulnerable people who they can befriend, manipulate and trick. The emotional toll can be devastating—shame, isolation, anxiety—and the financial impact can be life-altering where large sums of money have been stolen.

© 2025 TransUnion International UK Limited. All Rights Reserved.

Answer these questions

The task is to answer these questions

- What are the warning signs that something isn't right?
- What emotions did your victim feel?
- What things, could your victim have done better, to help protect themself?
- Who could have helped her?

The questions are in The Transunion Fraud Education Handbook, see pages 7, 10 and 13

© 2025 TransUnion International UK Limited. All Rights Reserved.

Part three: Support from organisations

You're not alone should you be a victim of fraud

Lots of people and organisations can help you:

- Family, friends, teachers, a neighbour – anybody you trust
- Charities like Victim Support, Childline, NSPCC
- Your bank
- Your mobile phone company
- Report it to the police (call 101 or Report Fraud), social media platforms
- Share your story to make others away of what happened.



© 2025 TransUnion International UK Limited. All Rights Reserved.

Part three: Support from organisations

STOP

S Slow down - Don’t reply or click.

T Think it through

O Overcheck the ad / message - screenshot and report it.

P Pass it by someone you trust



- Talk to a parent, teacher, or trusted adult.
- Report any money losses to your bank
- Report it to the police via Action Fraud
- There are lots of organisations out there who can help you
- See your Fraud Education Programme Handbook for lists of organisations and ways to protect your yourselves online

© 2025 TransUnion International UK Limited. All Rights Reserved.

Part four: Action plan

Complete the action plan

Keep this plan safe.

Check out The Transunion Fraud Education Handbook for:

- Tips for protecting your personal information online (page 20)
- Organisations who can help and what to do if you are a victim of fraud (page 23)

Answer these questions:

- What three things will you do to stay safe online
- Which one trusted adult would you tell
- What is the first thing you would do immediately, after realising you have been a victim of fraud

© 2025 TransUnion International UK Limited. All Rights Reserved.

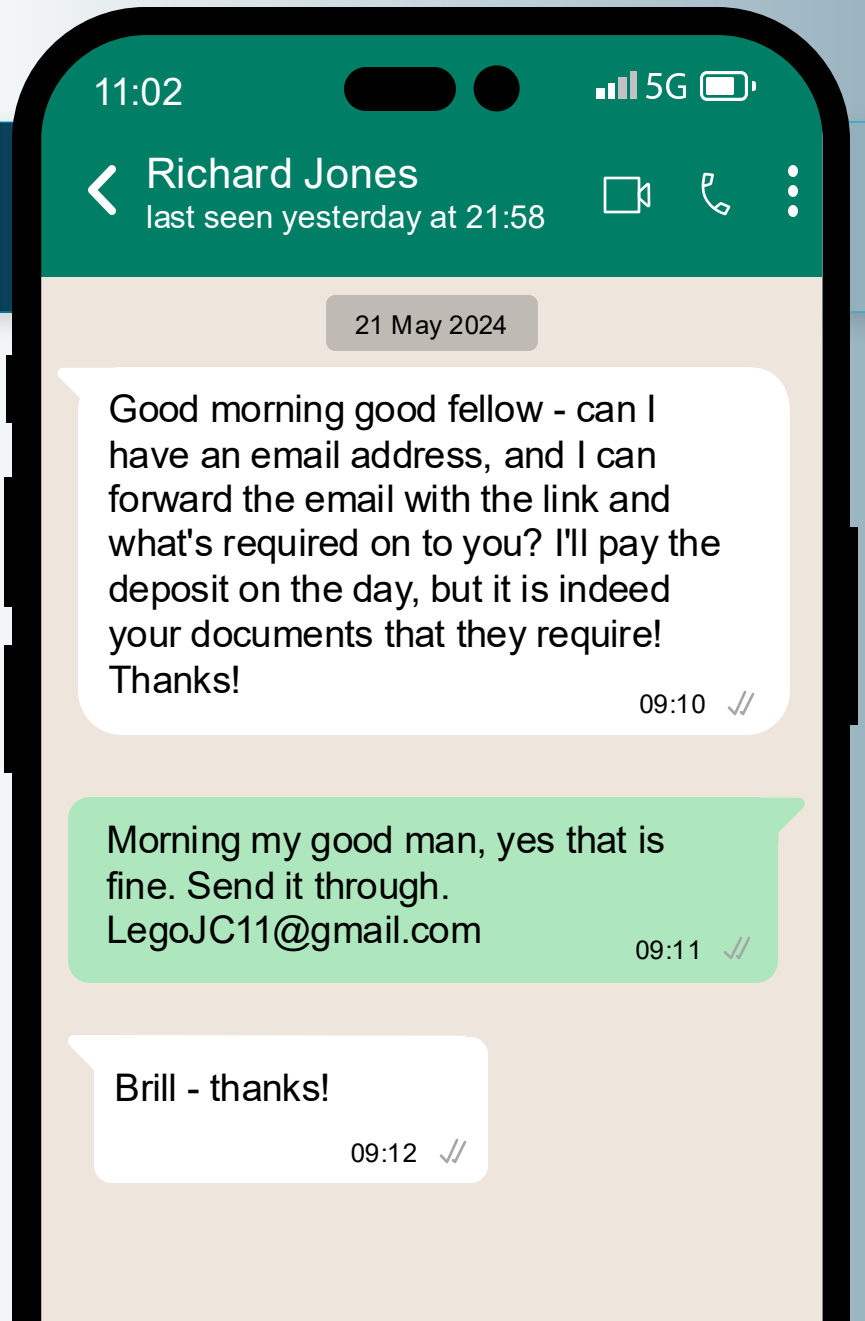
Part five: Quiz

- Test your knowledge
- Beat the fraudsters who scam



© 2025 TransUnion International UK Limited. All Rights Reserved.

A message exchange between two friends.



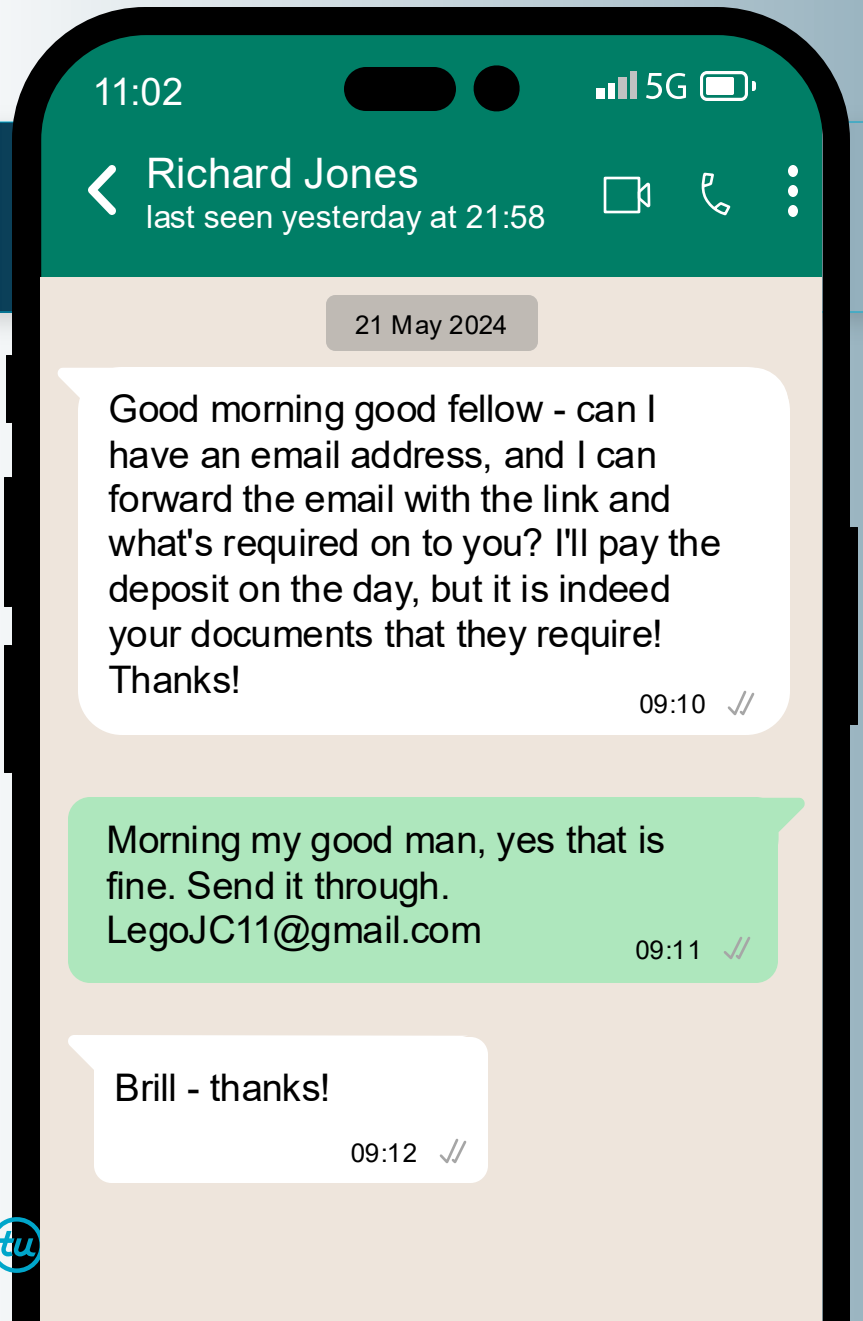
Is this What's App message exchange suspicious?



A Yes

B No

© 2025 TransUnion International UK Limited. All Rights Reserved.

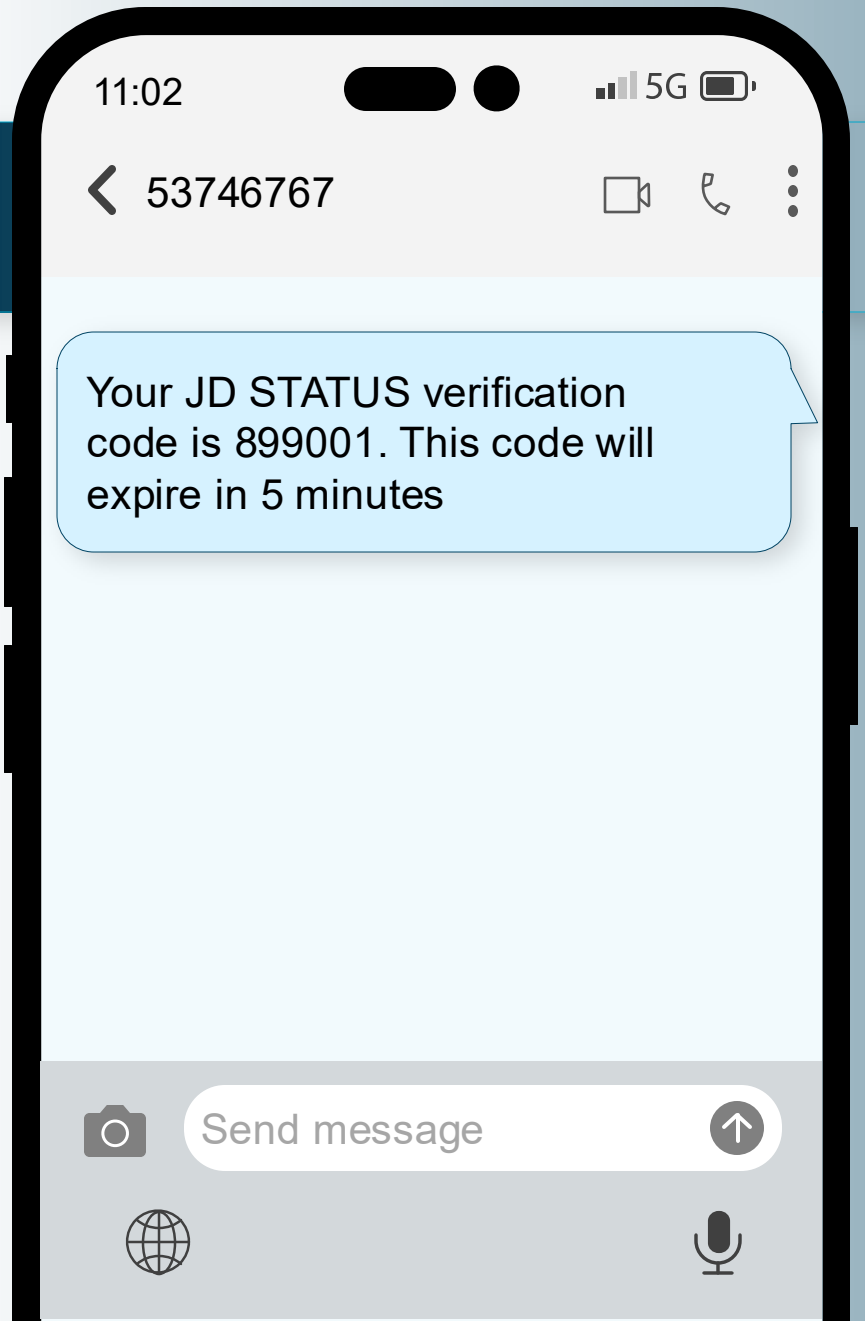


Answer is **No**



- It’s a genuine conversation between two friends
- The sender is known to the recipient
- The ask for the email address was expected
- The reason for the ask was known.

© 2025 TransUnion International UK Limited. All Rights Reserved.



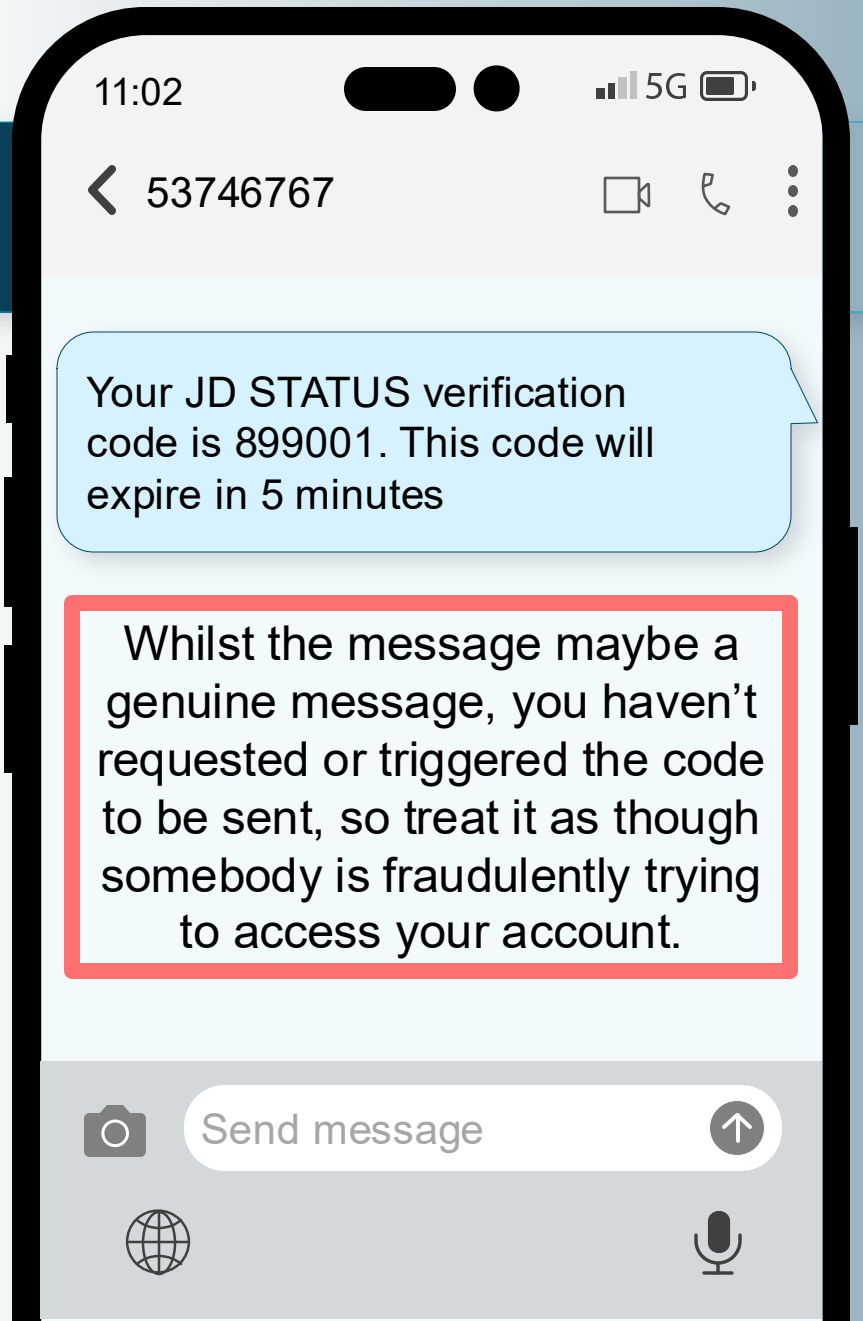
You receive this message, with a new verification code to access your account. It's not expected.

What should you do?



- **A** Ignore it
- **B** Log into your account to change the password
- **C** Contact the company to query the message
- **D** Do B and C

© 2025 TransUnion International UK Limited. All Rights Reserved.

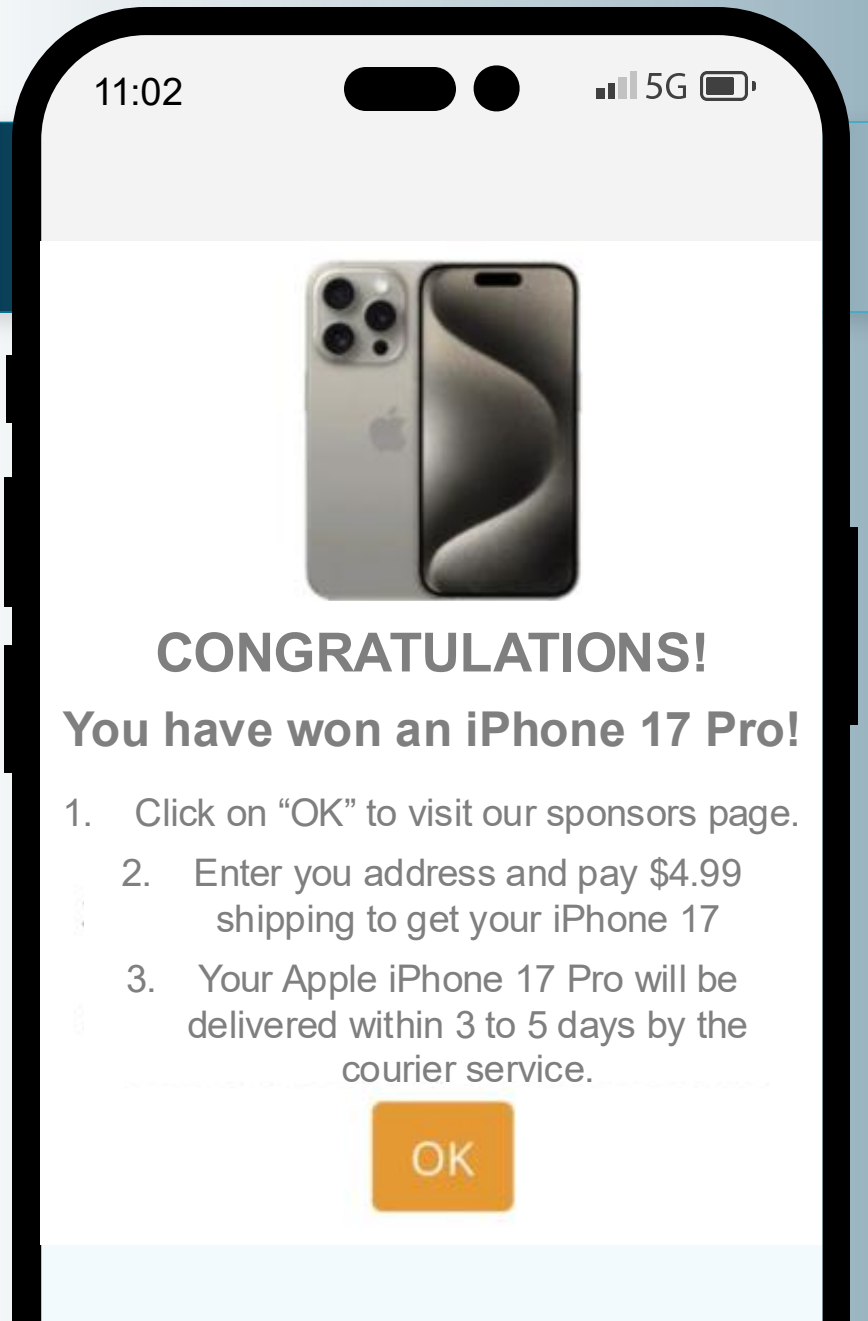


Answer is **D**



- Log into your account to change the password
- Contact the company to query the message

© 2025 TransUnion International UK Limited. All Rights Reserved.



You received an email offering you the chance to win an iPhone.

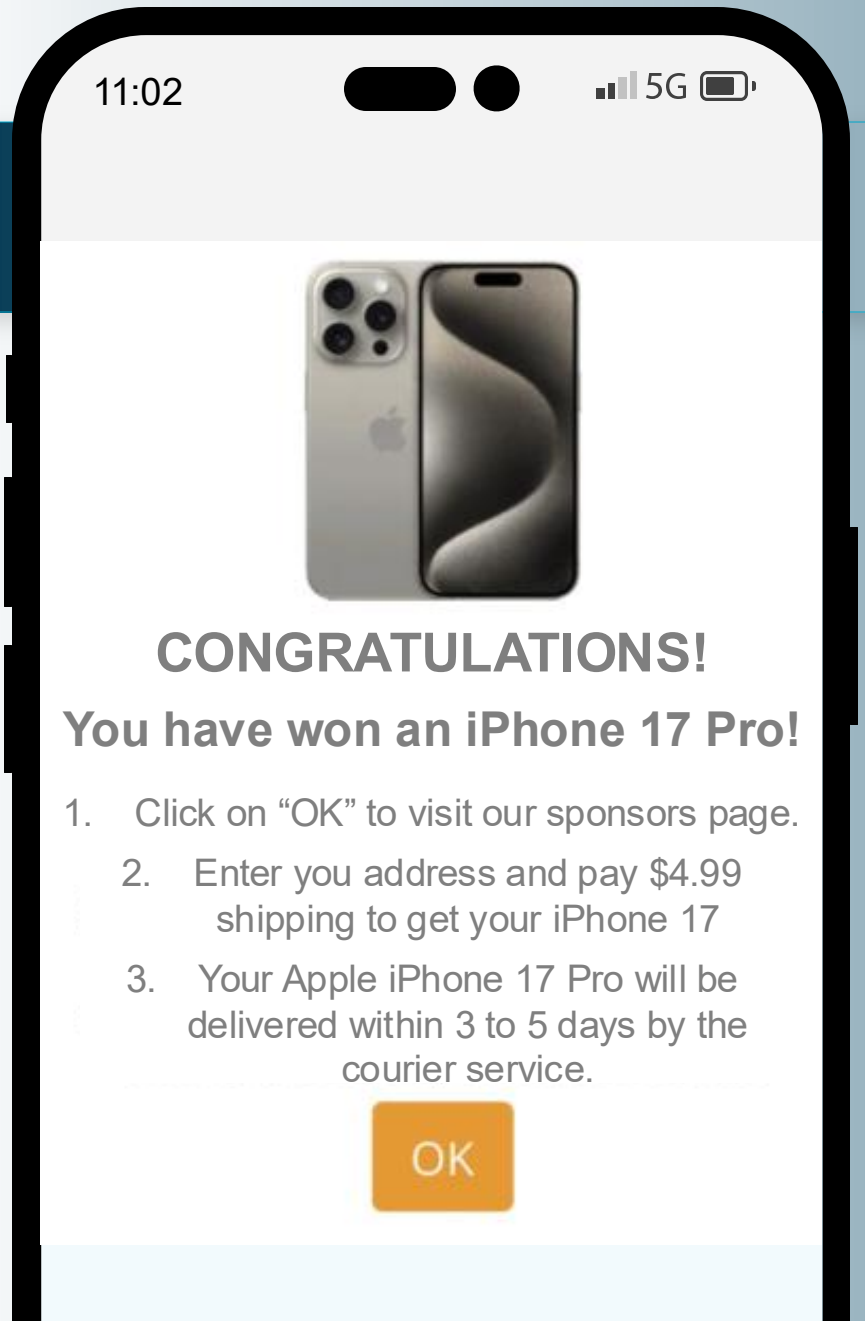
What do you do?

A Sign up immediately

B Ignore it



© 2025 TransUnion International UK Limited. All Rights Reserved.



Answer is **B Ignore it**



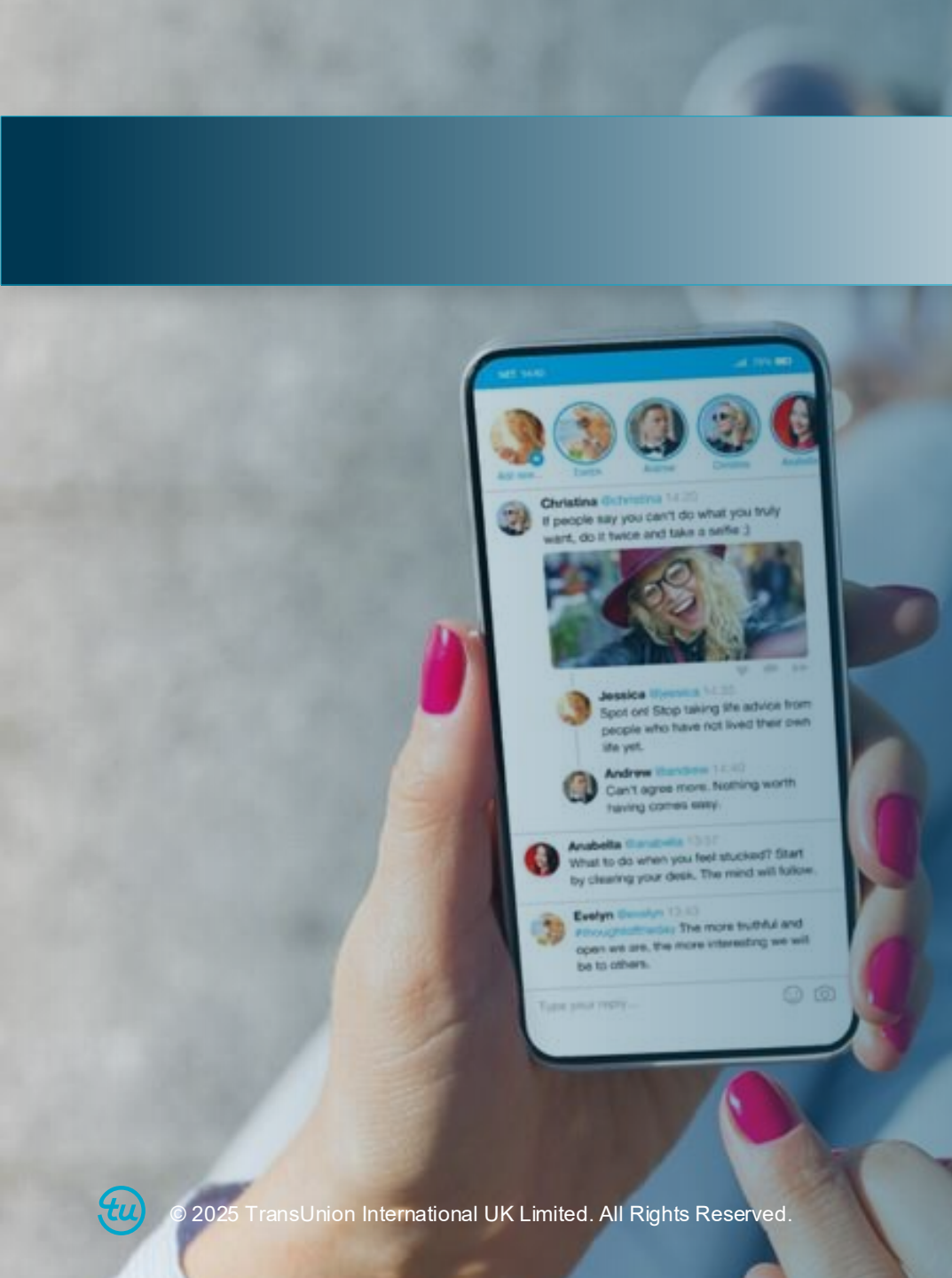
Why? Ignore it because

- You wouldn’t normally pay for shipping if you had won something
- The link says it will take you to their sponsors page which is unusual
- US Dollars not UK £

Source: UK University

© 2025 TransUnion International UK Limited. All Rights Reserved.

As you scroll through your messages, you receive a suspicious email or message, what should you do?



A

A: STOP

- Speed up
- Tell a friend you've won the competition!
- Obviously, do as the request asks and share your details
- Promptly act, because the offer is only available for a short amount of time

B

B: STOP

- Slow down
- Think it through
- Over check
- Pass it by someone you know

© 2025 TransUnion International UK Limited. All Rights Reserved.

The answer is B

STOP

- **S** Slow down - Don’t reply or click.
- **T** Think it through
- **O** Overcheck the ad / message - screenshot and report it.
- **P** Pass it by someone you trust

Talk to a parent, teacher, or trusted adult
Report any money losses to your bank
Report it to the Police via Action Fraud

© 2025 TransUnion International UK Limited. All Rights Reserved.

[PayPal] ……..



Dear PayPal customer,

Your PayPal account is limited. You have 24 hours to solve the problem, or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing and sending and receiving money.

Why is my PayPal account limited?

We believe that your account is in danger from unauthorised users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

You receive this message from PayPal, advising of a problem with your account.

What should you do?

- **A** Ignore it
- **B** Respond straight away by clicking the button
- **C** Do not select the button 'confirm your information' instead log into your account to check everything is ok
- **D** Contact PayPal's customer service team to check if the email is genuine
- **E** Do C and D

© 2025 TransUnion International UK Limited. All Rights Reserved.

[PayPal] ……..

PayPal

Dear PayPal customer,

Your PayPal account is limited. You have 24 hours to solve the problem, or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing and sending and receiving money.

Why is my PayPal account limited?

We believe that your account is in danger from unauthorised users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information



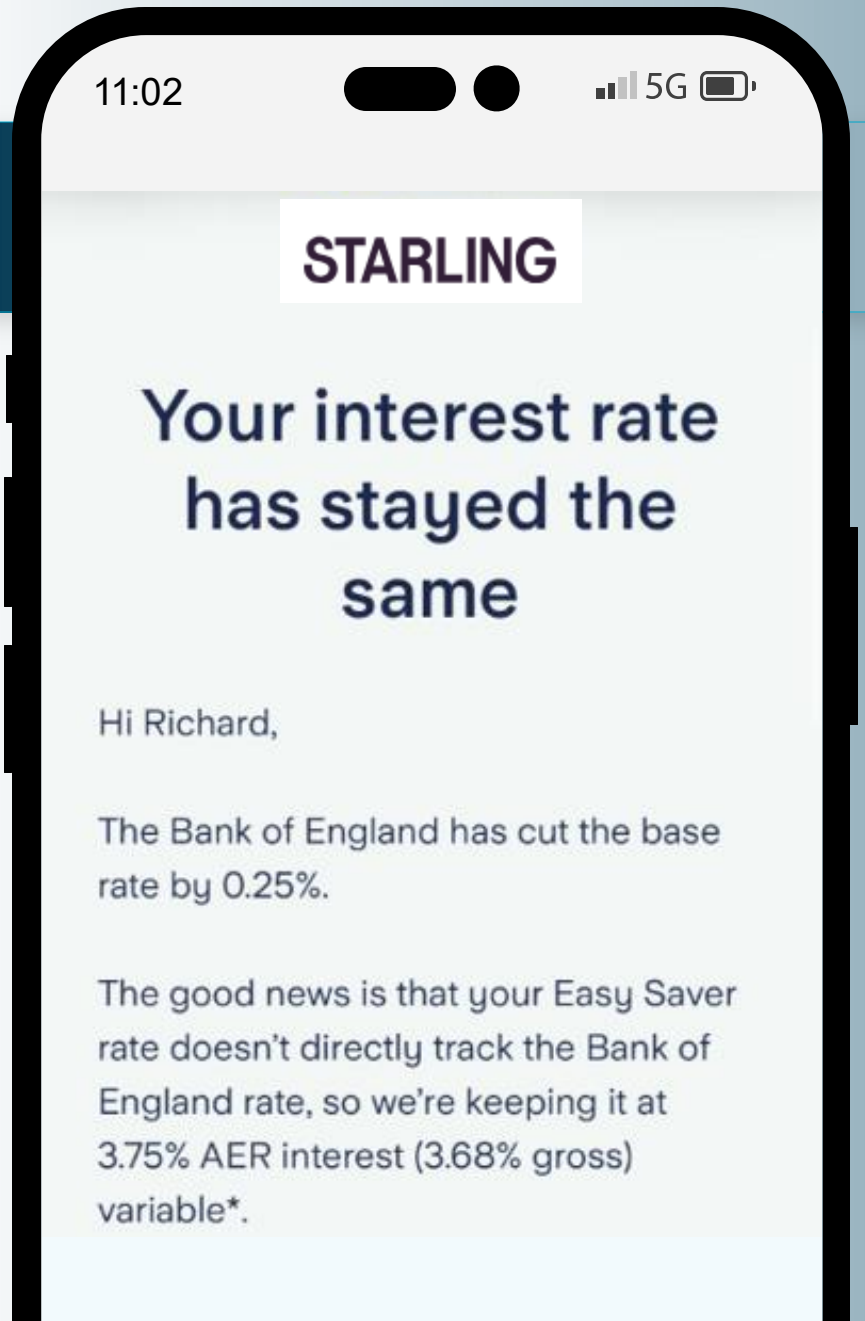
Answer is **E**

Yes, this email is spam because:

- The email is unexpected
- Call to action is 'Act Now!'
- Pressure to act within 24 hours
- Talks about a non-specific problem
- Uses the words 'secure server' which a genuine message wouldn't
- The wording and phrases used don't read as though a genuine company has written them
- Uses alarming language such as 'in danger from unauthorised users' to get your adrenalin going which induces stress, anxiety, all prompting you to act quickly

Source: Chat forum on Reddit discussing

© 2025 TransUnion International UK Limited. All Rights Reserved.



You are a Starling Bank customer, and you receive this email from the bank.

Is it a genuine email?

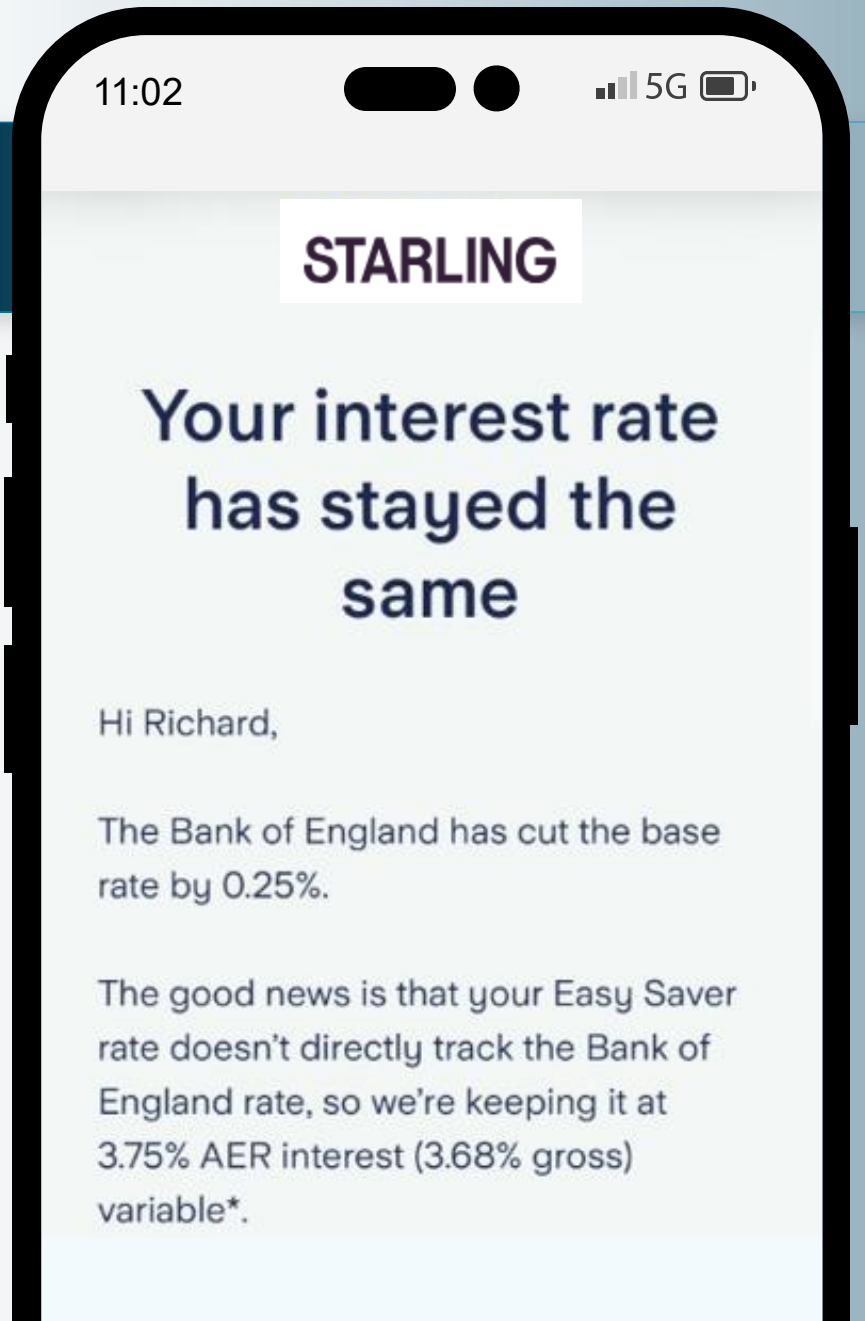


A Yes

B No

Source: Reddit

© 2025 TransUnion International UK Limited. All Rights Reserved.



Answer is **Yes, it's a genuine email**

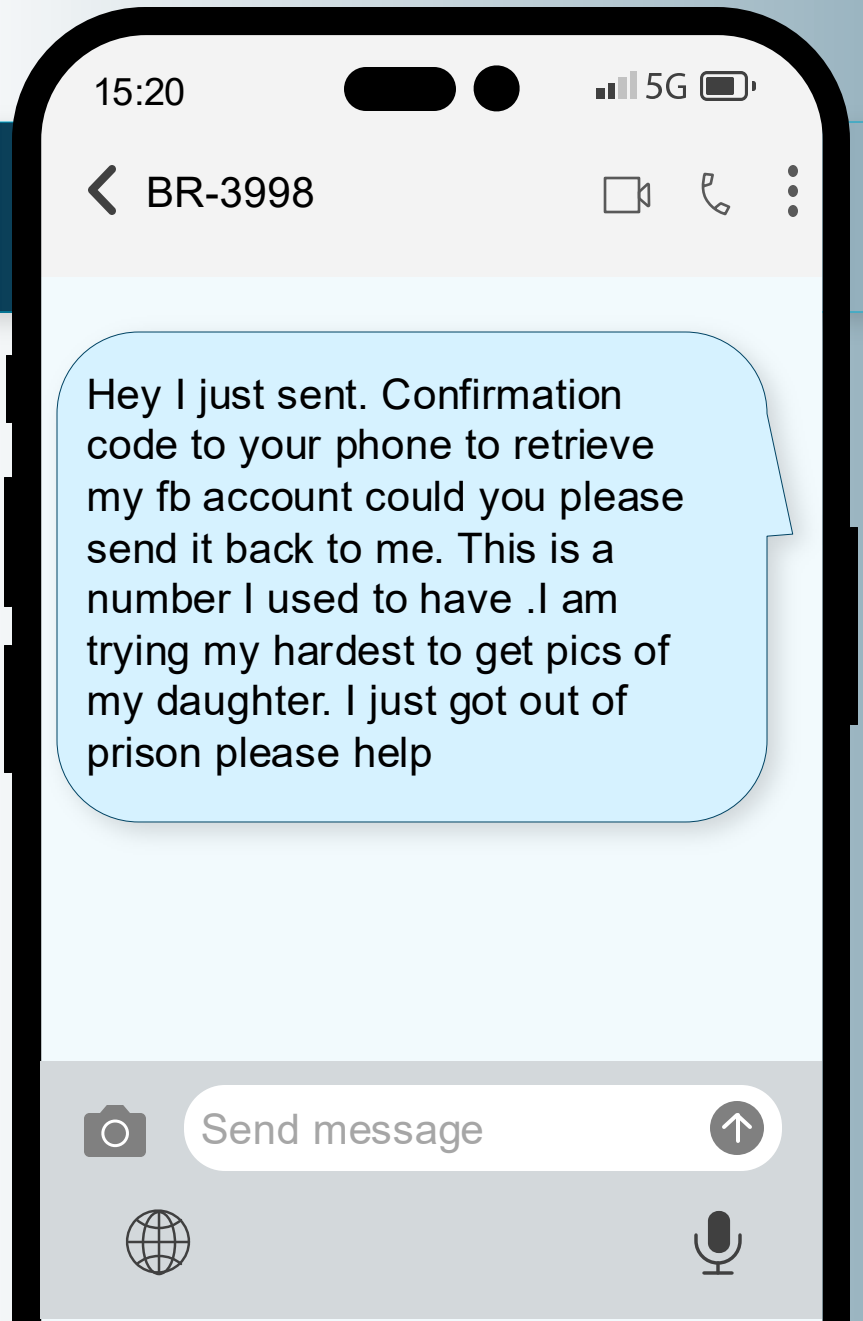


Why? The email is:

- Well worded
- Uses the correct logo
- An 'Information' email i.e., not asking you to do something
- Very unlikely to be fraudulent because fraudsters don't waste their time telling you things!

Source: Reddit

© 2025 TransUnion International UK Limited. All Rights Reserved.



You receive this text message which is unexpected.

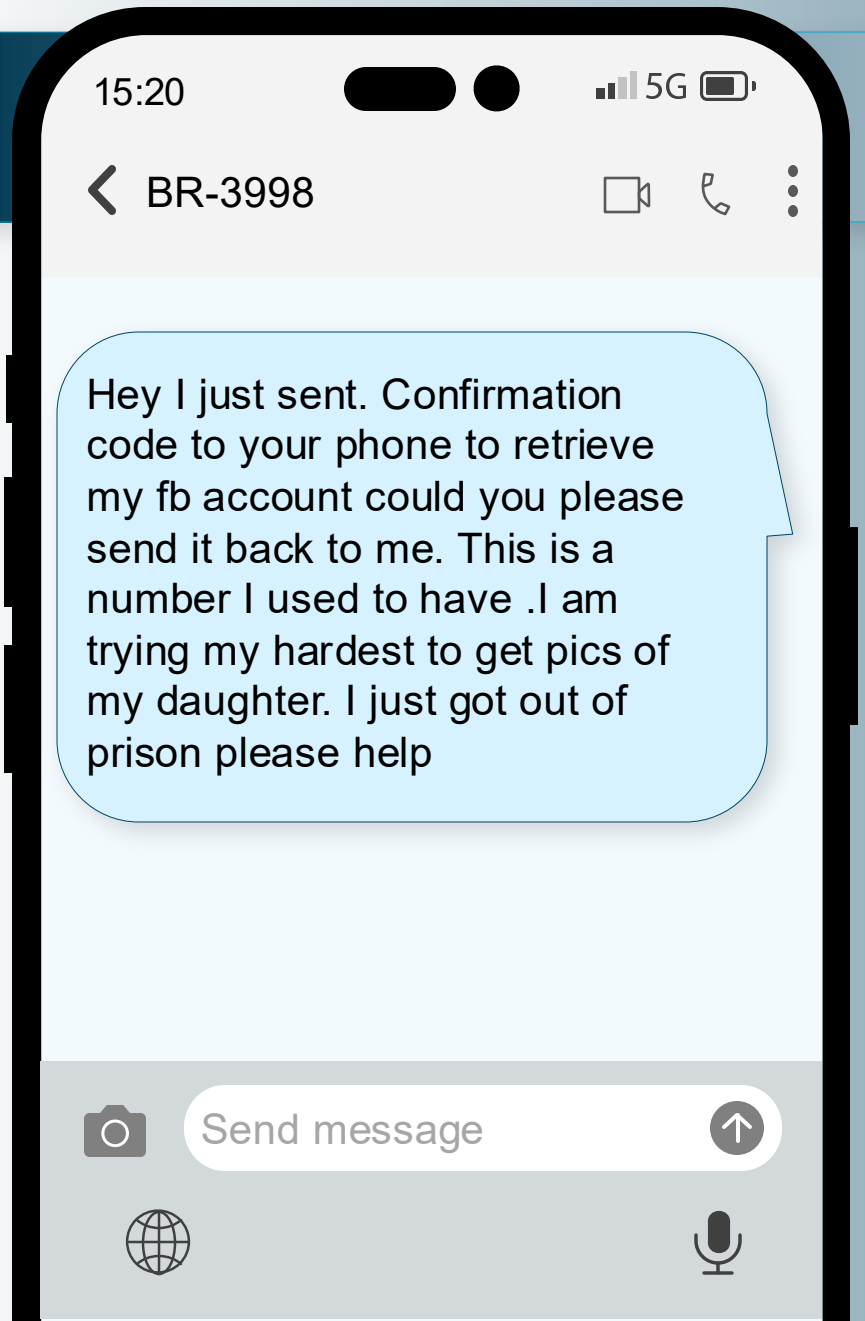
Is this message suspicious?

A Yes

B No



© 2025 TransUnion International UK Limited. All Rights Reserved.



Answer is **A**



Why? It's suspicious because

- It's unexpected
- It's from an unknown phone number
- You may not know anybody who has been in prison
- It's badly worded
- It has poor use of grammar
- It's guilting you about photos of his daughter, aiming to trigger your hormones and a reaction to respond.

© 2025 TransUnion International UK Limited. All Rights Reserved.

Remember, fraudsters are clever, but you are smarter!

© 2025 TransUnion International UK Limited. All Rights Reserved.



Additional slides for 100 mins - 2 full lessons and 150 mins – 3 full lessons

Part One: What is fraud?

Q. What is online fraud?

A. “Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person”. Source - Report Fraud

Q. Has anybody been a victim of fraud themselves or know anybody else who has e.g. a family member?

Q. Can you name different types of fraud that young people are most vulnerable to? and why?

A. 4 types of fraud, young people are most vulnerable to are:

1. Buying goods online and paying upfront
2. Banking Fraud and Money Mules
3. Scams, meeting people online – any fraud that happens online
4. Identity theft

Why? Because they are high online activity, risk takers, lack of awareness, use weak passwords, peer pressure, social inclusion, trusting by nature

Q. What are the consequences of committing fraud?

A. Many consequences which include:

- Prison - up to 10 years = a criminal record
- Fines
- Blocked from opening a bank account or getting a student loan
  Thrown out of college or university
- Unable to get a job due to a criminal record
- Emotional and psychological impact
- Lose friends or damage relationships

© 2025 TransUnion International UK Limited. All Rights Reserved.

Part One: What is fraud?

Q. What is online fraud?

A. “Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person”. Action Fraud

Q. What are the consequences of committing fraud?

A. Prison, up to 10 years = a criminal record

Fines, blocked from opening a bank account or getting a student loan, thrown out of college or university, unable to get a job due to a criminal record, emotional and psychological impact, lose friends or damage relationships

© 2025 TransUnion International UK Limited. All Rights Reserved.



Recap

What is fraud?

Who could be a victim of fraud?

© 2025 TransUnion International UK Limited. All Rights Reserved.



Additional slides for 150 mins - 3 full lessons only



Recap

What have I learnt that I want to pass on to my family and friends?

What surprised me?

© 2025 TransUnion International UK Limited. All Rights Reserved.