**Safer Internet Day 2025**  
**Resources for use with 14 to 18 year olds**

*Too good to be true? Protecting yourself and others from scams online*

**Quiz: Protecting yourself and others from scams online**

The quiz can also be found online at: [saferinternet.org.uk/sid-quiz](http://saferinternet.org.uk/sid-quiz)

1. Ola’s favourite independent jewellery designer is doing a giveaway because they’ve just hit 10,000 followers. To enter the giveaway, people have to like a post on the designer’s profile, share it on their story and tag three friends in the comments. The post states that the winner will be selected at random in a week’s time. Ola enters the giveaway and a few days later receives a DM from an account that looks similar to the designer’s saying she has won. Ola notices the username is slightly different.

Which of these is the best response?

1. Ola should check the official account to see if there’s anything about the competition results. Once she’s confirmed it’s fake, she should screenshot the message and profile of the fake account. Ola should share the screenshot with the designer’s official account so they can warn their other followers. Ola should also block and report the fake account.
2. Ola should check the official account to see if there’s anything about the competition results. Once she’s confirmed it’s fake, she should report the message to the platform and comment on the original post warning others about the scam. Ola should also reply to the fake account to troll them and keep them occupied so they’re not able to scam anyone else.
3. Ola should check the official account to see if there’s anything about the competition results. Once she’s confirmed it’s fake, she should screenshot the message and profile of the fake account. Ola should share the screenshot with the designer’s official account so they can warn their other followers and comment on the original post warning others about the scam. Ola should reply to the message and inform them that she knows they’re a fake.

**Correct answer: a**

Giveaways are frequently used by criminals as an opportunity to try and trick people into giving away personal details, often including their banking information. Although it can be exciting if it seems you have won a competition, it’s always important to check that it is the account you are expecting to contact you. Ola can check the official account to see if there’s anything about the results and confirm it is fake. She could also screenshot the message and the fake account to show to the designer’s official account so that they can warn others about what is happening. It’s also important for Ola to block and report the account, so the platform can take action too.

1. Simeon is in his first year at university and struggling financially. He hears about a money-making opportunity via social media. When he messages them for more information, he finds out it involves receiving large sums of money into his bank account and holding it for a period of time before transferring it to someone else. In return, he keeps a certain percentage of the money. Simeon realises that this is probably not legal, but it means that he can afford better nights out and the brands he wants to buy.

When considering his decision, which consequences are most important for Simeon to think about?

1. Simeon would make money which could fundamentally change his university experience. He may also be able to offer opportunities for his friends and flatmates to benefit too.
2. Simeon could be prosecuted for money laundering and is also at risk because of his involvement with organised crime.
3. Simeon could get kicked out of university for his participation in the scheme and his friends may be suspicious and jealous of his newfound wealth.

**Correct answer: b**  
  
With the cost of rent and basic necessities high, university can be an expensive time, so the promise of more comfortable living could be very tempting for Simeon. However, the most important consequence for Simeon to consider when thinking about his decision is the fact that he could be prosecuted and would be involved in organised crime. This money-making opportunity that Simeon has discovered is known as money muling and is a type of money laundering, which is illegal. If Simeon gets caught taking part in this, he could face negative consequences that could greatly impact his future.

1. Jo subscribes to an online programme promoted by an influencer they follow. The programme is designed to give them skills in selling and social media marketing, but also involves investing in the company to access the resources. Jo can increase their earnings by recruiting new participants. Jo is impressed with the initial materials and starts telling their friends in the hopes of making more progress. One of Jo’s friends accuses them of being part of a pyramid scheme.

How should Jo respond?

1. Jo should research pyramid schemes and the programme they have subscribed to. If Jo finds that their friend is right, Jo should report the programme to Action Fraud, or if in Scotland the police by calling 101.
2. Jo should research pyramid schemes and the programme they have subscribed to. If Jo finds that their friend is right, Jo should apologise and acknowledge that they were to blame. Jo should then cut all contact with the programme and accept they’ve lost any investments made so far.
3. Jo should research pyramid schemes and the programme they have subscribed to. If Jo finds that their friend is right, Jo should work to recruit as many other people as possible to try and make their initial investment back before leaving the programme.

**Correct answer: a**

This is a pyramid scheme designed to make money out of people but Jo is not to blame. Jo should gather any evidence they have and report it. If Jo lives in Scotland they should contact the police on 101. For all other parts of the UK they should contact Action Fraud. Jo could also report the scheme on any platforms they see it on in future.

1. Steffan receives a message on social media from someone who claims they have nude images of him. They threaten to share the photos with his friends and family if he doesn’t send them £100. They have screenshots of the friends he follows on social media to show who they will message.

Which of these is the best response?

1. Steffan does everything he can to prevent the images being shared. First, he uses a website he heard about in school to help remove images that may be online, then he deletes the images from his device. He also transfers the blackmailer £100, reasoning that this is worth it to stop the photos getting out. Then he shuts down his social media accounts.
2. Steffan uses a website he heard about in school to help remove the images. The website also puts him through to a counsellor who helps him decide to tell his parents. Together they also report it to the police.
3. Steffan has heard about these types of scams and figures they probably don’t even have the images. He ignores the message and blocks and reports the sender.

**Correct answer: b**

Being targeted with sextortion can be a scary and difficult experience to talk about, but talking to a trusted adult about what is happening is the best way for Steffan to get support. Together, they can report the messages to the police and to the platform they were received on. Steffan should use [Take It Down](https://takeitdown.ncmec.org/) or [Report Remove](https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/) to help remove the images from the internet.

It is always safest not to respond to a blackmailer, and to save screenshots of the messages as evidence of what has happened. There is lots of support out there for those targeted by sextortion. Sextortion can be reported to the police using 101, or to [CEOP](https://www.ceop.police.uk/Safety-Centre/) by visiting their website.

1. Molly gets a Snapchat message from her friend saying her Insta account is posting weird offers and cryptocurrency advice. Molly tries to open the app on her phone, but she has been signed out and her password no longer seems to work. She tries to reset her password using the ‘Forgot password?’ button but doesn’t receive any emails. Molly realises her account has been hacked and she can no longer access it.

Where should Molly report this?

1. To Instagram and to her friends and family, so they can do the same, then to Action Fraud (or in Scotland to the police by calling 101).
2. To Instagram only. This isn’t a matter for the police.
3. To Instagram and to her friends and family, so they can do the same.

**Correct answer: a**

Criminals may take over accounts on social media, but also on other apps and services including banks, by using stolen data or because the owner of the account has been targeted by another scam such as phishing. To regain access to her account Molly should report this incident to Instagram and encourage her friends and family to do the same. Additionally, account takeovers can be reported to the police as a form of cybercrime. In England, Wales and Northern Ireland, this can be reported online to Action Fraud or by calling 0300 123 2040. In Scotland, this can be reported to the police by calling 101.