Fraud and scams

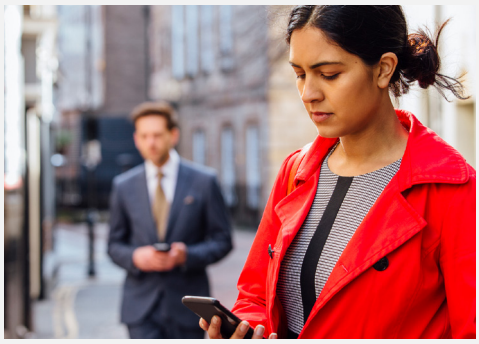
LifeSkills
Created with BARCLAYS

Worksheet 1

Do you know your phishing from your smishing? The various types of fraud can have some strange names. Learning these names is one thing, but understanding when you're being targeted – and how to avoid being duped – is another. Read through the different terms and their explanations here: barclayslifeskills.com/i-want-to-get-to-grips-with-money-and-my-payslip/school/what-is-phishing-and-online-fraud

Now you have learnt about some of the ways that fraudsters work, read through each of the scenarios and answer the questions. You can type your answers into the boxes.

Case study 1 – Deets and squares



Priya had been looking for a 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.

What type of fraud or practice is this?

What signs could the individual have spotted to stay safe?

What could they do differently next time?

LifeSkills
Created with BARCLAYS

Case study 2 – Online fraud

Jake was keen to get tickets for a football match which had sold out. He found some advertised online cheaper than the original price, and paid for them using his debit card. Jake was sent a confirmation email straight away to say that the tickets would arrive within 10 days. Unfortunately, the tickets never arrived and when he made calls to the company they were ignored.

What type of fraud or practice is this?

What signs could the individual have spotted to stay safe?

What could they do differently next time?

LifeSkills
Created with BARCLAYS

Case study 3 – Vishing

Tom got a text message from his mobile phone contract provider to say that his account had been used by someone else to download lots of apps. To get a refund, Tom was asked to click on a link and enter his bank details and the three-digital security code on his debit card into a form online; he was told that this refund would appear in his account within 5-10 days. The following day, when Tom checked his bank balance using his mobile banking app, he saw that a large sum of money had been withdrawn from his account.

What type of fraud or practice is this?

What signs could the individual have spotted to stay safe?

What could they do differently next time?

Which of the three scenarios poses the highest financial consequences?