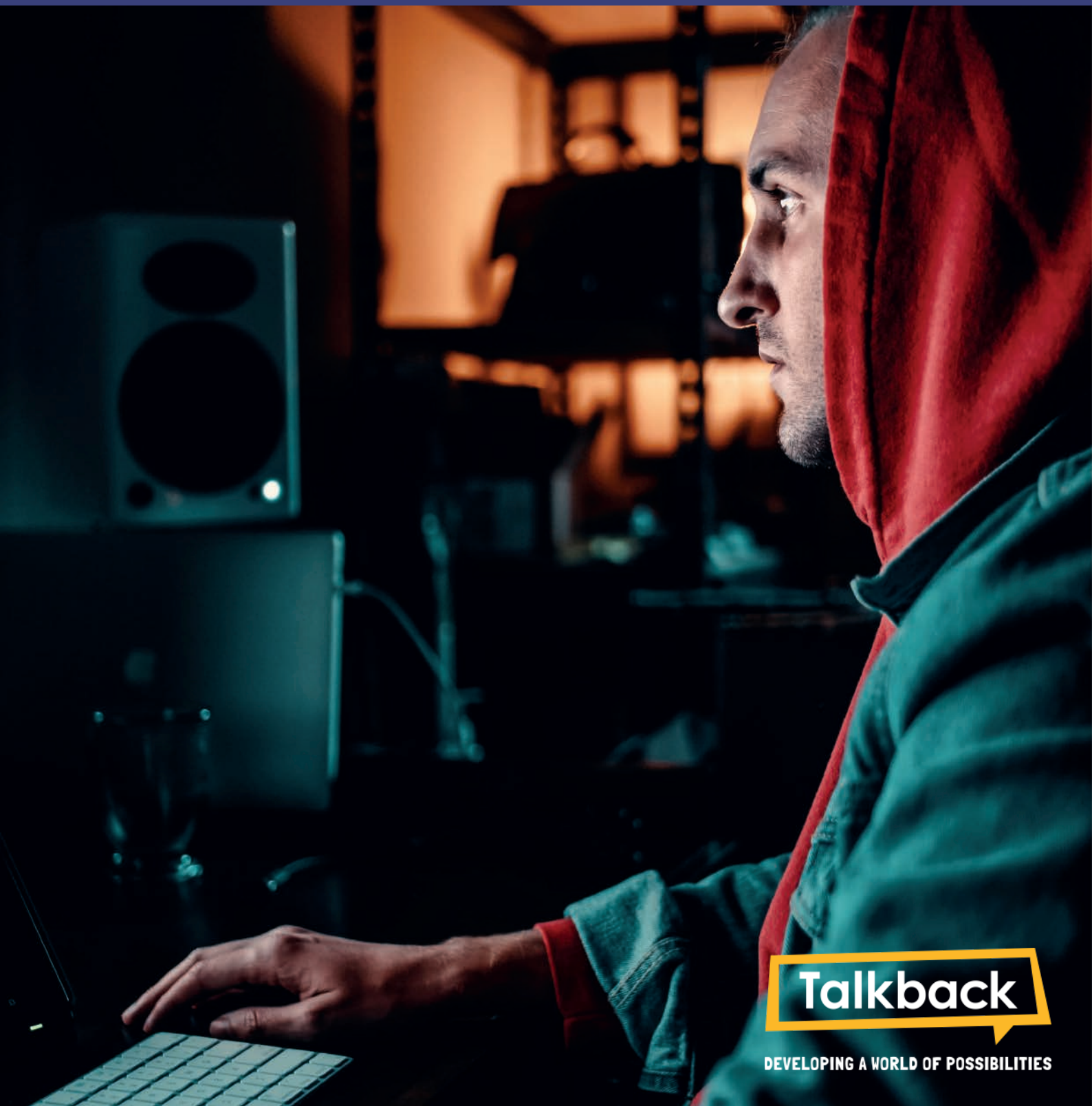
Cyber Fraud
Training Booklet

This workbook is to be used alongside the community safety film on Cyber Fraud.



Talkback

DEVELOPING A WORLD OF POSSIBILITIES

Welcome to the Talkback
Cyber Fraud Training

This guide has been produced to accompany the cyber fraud video. Please follow the steps outlined carefully. We have produced this document with helpful training tips, that are highighted in the yellow boxes.

Learning Objectives

- To understand what is meant by the term 'Fraud' and how fraud can be committed.
- To understand steps that can be taken by individuals to keep their money safe.
- For an individual to know what to do if they suspect they may have been a victim of fraud.

What's in the video?

In this video, you will see two parts of a story. The first part of the story shows what can happen when someone tricks you so that they can steal your money. The second part of the story shows what you can do to keep your money safe.

Glossary: Key Terms

What does Fraud mean?
Fraud is when someone tricks you so that they can steal your money.

Trainer tips

After you've talked through the learning objectives and key terms, show the member the film in full. Then, using the narration of events below, read through the story making use of the timestamps if necessary to rewatch the relevant parts of the film.

Use the trainer tips as discussion points to pause and reflect on what is happening.

Part 1 of the story shows what can happen when someone tricks you so they can steal your money.

00:00:39 George gets a call on his phone from a number he hasn't seen before.

00:00:52 The person on the phone says that he's from the Fraud Team at George's bank. The person on the phone tells George that there's been some unusual activity on his account and that large payments are being sent to a marketing agency called Fox Marketing.

Trainer tips

Check with the member that they are clear who the characters are in the story so far. Make sure the member understands that a Fraud Team at a bank are the people who deal with fraud problems, including money being stolen from a bank account.

00:01:04 The person on the phone offers to block the payments for George and move George's money to another account to keep it safe. The person on the phone sounds like he wants to help George.

George isn't sure what to do, but the person on the phone is very pushy.

Trainer tips

Ask the member whether they think the person on the phone actually wants to help George or if he might be tricking him.

00:01:12 The person on the phone asks George to give him his banking login username and George tells him what it is.

00:01:20 The person tells George he will receive an access code to his phone. The person on the phone asks George to read the code out to him and George reads it out.

Trainer tips

Check the member understands what is happening.

00:01:56 George gets an alert from his bank saying that he has been a victim of fraud. George is confused. George realises the person on the phone wasn't who he said he was and that he has now been a victim of fraud.

Trainer tips

Discuss the storyline so far and check understanding of what's happened to George.

Part 2 of the story shows what you can do to keep your money safe.

00:02:11 George gets a call that he's not expecting from a number he hasn't seen before. The person on the phone says that there's been some unusual activity on George's bank account. He says that large payments are being sent to a marketing agency.

00:02:31 The person on the phone offers to block the payments and move his money to another account to keep it safe. He sounds like he wants to help George.

Trainer tips

Emphasise to the member that 'fraudsters' can be very clever and sound like they want to help, but what they really want is personal information so they can steal your money.

Discuss with the member what help is available to them from their own bank. This may be contained in the bank's security or fraud section on an app or website. They can also call their bank's customer service number to find out this information.

00:02:37 George says he doesn't think he should be giving out these details. The person on the phone tries to persuade George to give them to him.

00:02:45 George says he will check with his trusted person first and then speak to his bank later on. Then George hangs up the phone.

Trainer tips

Reiterate that George has done the right thing here by ending the call and asking the advice of his trusted person

00:02:59 The person on the phone is annoyed because he hasn't succeeded in tricking George to steal his money. George has avoided being a victim of fraud.

Trainer tips

Discuss with the member the term 'victim of fraud' and what this means, i.e., when someone has stolen your money by using your personal details.

Quick Quiz

Work with the member to complete this quiz to gauge their understanding of what they've learnt.

Fill in the gaps to complete these sentences about keeping your information safe online.

1. Fraud is when someone _____ you, so they can steal your money.
2. You shouldn't give out your online banking details such as _____ to anyone.
3. If you are confused about a phone call you have received about your money, you should always talk to _____.
4. If you want to know how your bank can help you with fraud, you can find this information on _____ or call _____.

Answers

1. Tricks
2. Account number, sort code, password, username.
3. Your trusted adult.
4. Fraud section of website or app / customer service.

Trainer tips: Final scenario check

Present this scenario to the member to see if they can apply the knowledge they have learnt.

Richard receives a text message that looks like it is from his bank. It says that he needs to change his password and gives a link for him to follow so he can do that. What should Richard do?

Answer

Before clicking on the link, Richard should ask the advice of his trusted person. He should also call his bank and ask them whether it was them who sent him this text message.