

Social Engineering

Key Stage 4 | Lesson 2



QUALITY
ASSURED
RESOURCE
PSHE ASSOCIATION

Ground Rules

- Everyone has the right to be heard and respected
- We will use language that won't offend or upset other people
- We will use the correct terms, and if we don't know them, we'll ask the teacher
- We will comment on what was said, not the person who said it
- We won't share our own, or our friends', personal experiences
- We won't put anyone on the spot, and we have the right to pass
- We won't judge or make assumptions about anyone

Baseline: Key Questions

What do social engineering and cybercrime mean?

What is identity fraud?

How might someone use technology to carry out identity fraud?

What should someone do if they are a target of identity fraud?

How can someone protect their online information at home and at work?





Learning Objective and Outcomes

To learn about the risks of social engineering, how to recognise and challenge it, and sources of support available.

Students will be able to:

- explain what social engineering is and how to recognise its different forms
- explain the risks involved in revealing personal information and how to respond to social engineering attempts
- describe how and where someone can seek help if they are concerned about cybercrime

Key Terms

There are a range of complex terms used to describe different fraudulent techniques.

Being aware of these will help you to recognise if someone is trying to use them.

Work in pairs to match each term with its definition.

Resource 1: Key Term Card Sort

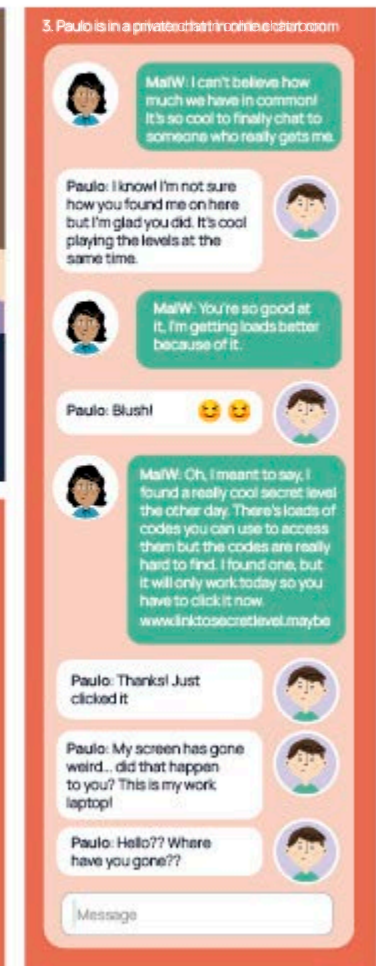
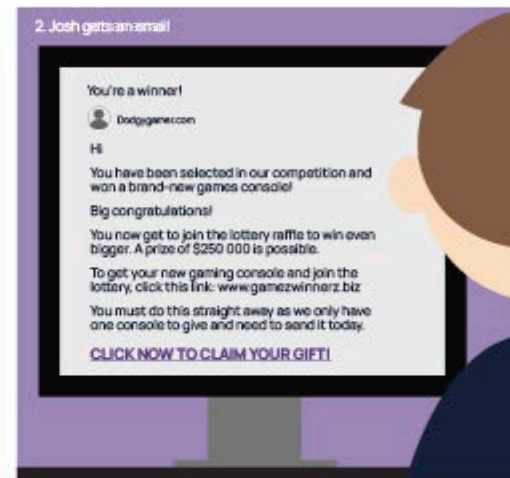
Match the words to the descriptions



Social Engineering	A type of crime that is committed using information technologies such as a computer and a network.
Cybercrime	Software which is specifically designed to disrupt or damage a computer system.
Phishing	An attempt to gain personal information through the use of text message.
Smishing	An attempt to gain personal information through the use of email communications.
Vishing	Software which is specifically designed to disrupt or damage a computer system.
Malware	A fake or tampered QR code to direct someone to a fraudulent website designed to steal information or prompting malware downloads.
Quishing	A method of manipulating people to reveal personal information about themselves.

Social Engineering Scenarios

Read the five scenarios – which type of social engineering does each one show?



Social Engineering Scenarios

Paulo's private chat online and being sent a malicious link – this is an example of a **malware attack**.



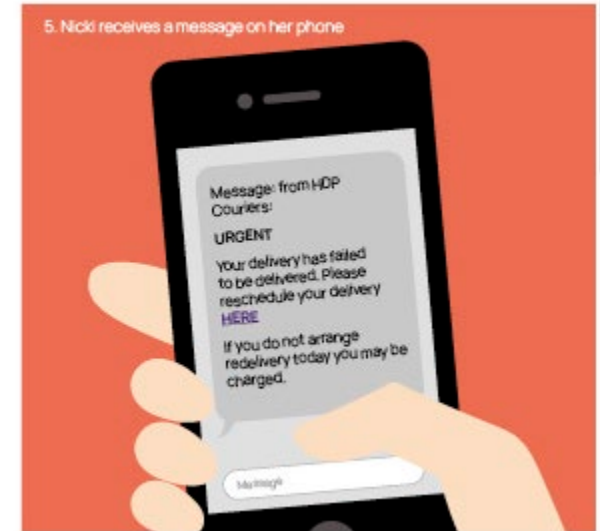
Carla's phone call claiming to be from a bank – this is an example of **vishing**.



Josh's email claiming he has won a games console and can join a lottery – this is an example of **phishing**.



Nicki's instant message about parcel delivery – this is an example of **smishing**.

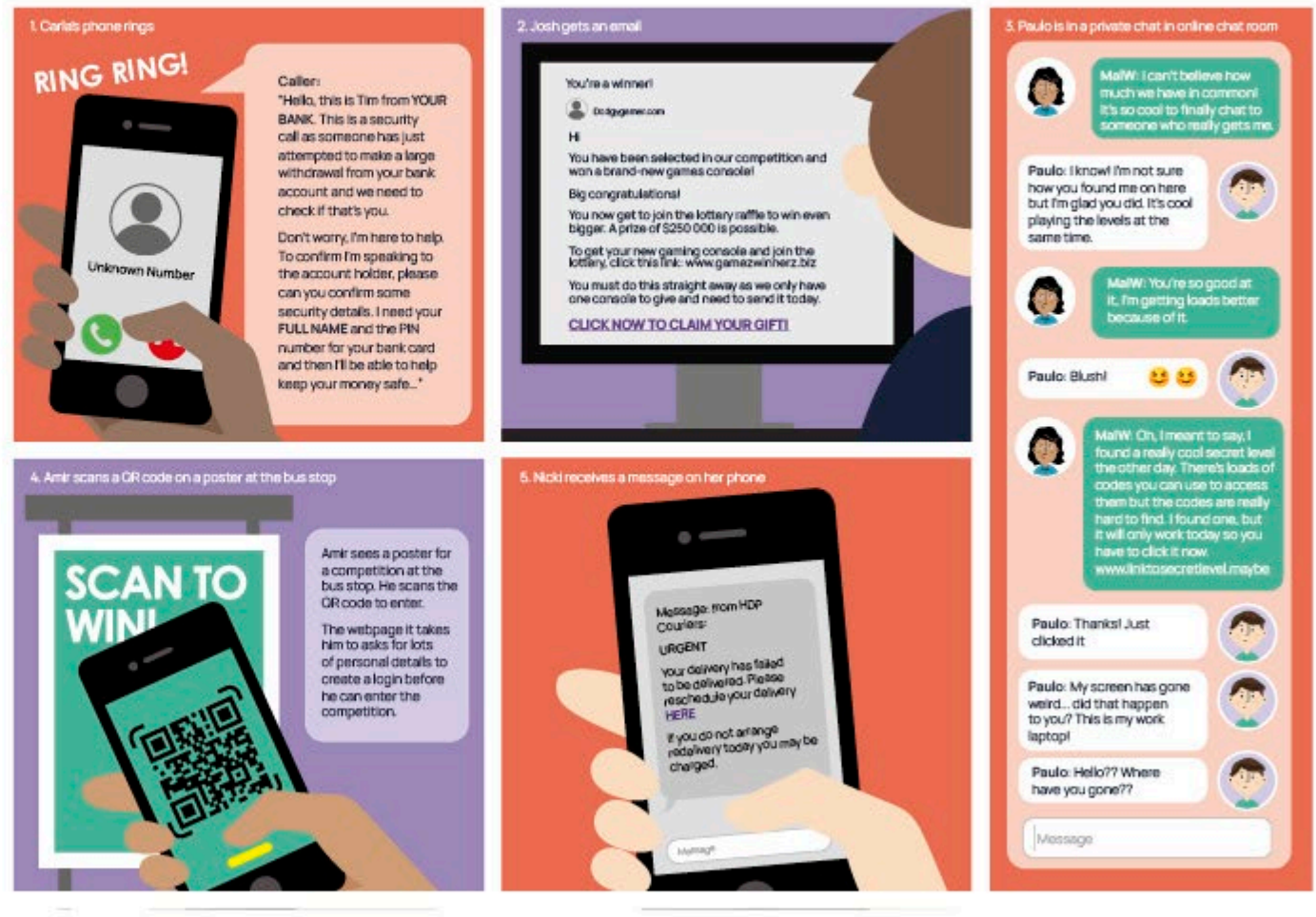


Amir scans a QR code on a poster that takes him to a fake login page – this is an example of **quishing**.



Social Engineering Scenarios

1. What might happen next to the characters in these scenarios?
2. What should they do now?
3. Where could they seek more help and advice?



Top Tips for Avoiding Social Engineering and Cybercrime



01

Get a second opinion if an offer, competition or giveaway is too unrealistic.

02

Avoid rushing or being pressured to act urgently, particularly if there is pressure to reply or give information in a short time period.

03

Think about the information being asked to handover; why might a legitimate company want or need this?

04

Trust instincts – if something doesn't seem right, don't be embarrassed to refuse to give over information or to leave the conversation.

05

Check who sent the email or verify the caller; if it's genuine, they won't mind if someone checks and uses the general email address or phone number.

Top Tips for Avoiding Social Engineering and Cybercrime



06

Check who the email is sent to and question where it came from.

07

Be aware of companies or contacts that are not familiar; use a search engine to check they are genuine.

08

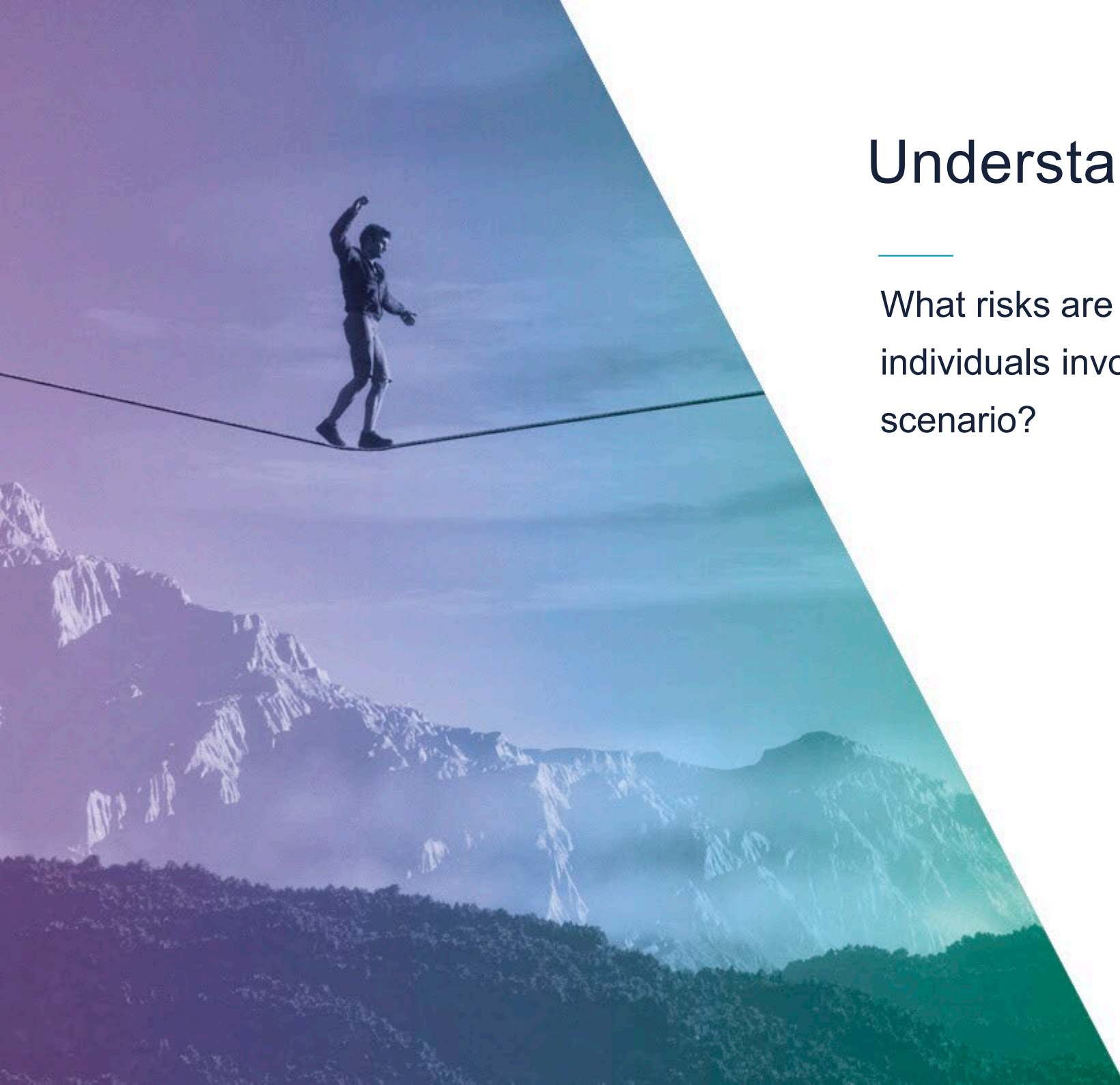
Do not click on any links or open any attachments without doing some research first.

09

Be cautious with social media, keeping privacy settings high, not over sharing personal information and being wary of clicking links.

10

Protect devices by making sure anti-virus software is installed and is regularly updated. Have strong and varied passwords for the different services used online.



Understanding Risk

What risks are there to the individuals involved in each scenario?

Giving Advice



Report Fraud is the place to tell the police about cyber crime and fraud. People can make a report online or by phoning 0300 123 2040.

It also provides a Report Fraud Victim Service, which offers dedicated and specialist help to victims of cyber crime and fraud.

www.reportfraud.police.uk

childline

ONLINE, ON THE PHONE, ANYTIME

Can be contacted about anything – they are there to support young people and help them find ways to cope.

www.childline.org.uk



An independent charity dedicated to supporting victims of crime in England and Wales. It provides help to support people to cope and move on to the point where they feel they are back on track with their lives.

www.victimsupport.org.uk



Take Five to Stop Fraud shares practical tips to spot scams and prevent fraud. It encourages everyone to Stop, Challenge and Protect against unexpected requests for your money or information.

www.takefive-stopfraud.org.uk



Family member or friend

Can listen to problems without judgement and knows the person well.



Teachers

Teachers/other staff members can help students to find appropriate further support.



Giving Advice

Choose one of the characters and write to them, explaining what the fraudsters might be trying to do, how they might recognise social engineering techniques and how they can seek help and support.

Signposting Support

If you are worried about fraud or want to find out more, you can speak to:

- a parent/carers or other trusted adult outside of school
- a tutor, pastoral lead or other trusted staff member in school

And/or visit:

Report Fraud: www.reportfraud.police.uk

Childline: www.childline.org.uk | 0800 1111

Victim Support: www.victimsupport.org.uk

UK Finance – Take 5 to Stop Fraud: www.takefive-stopfraud.org.uk

Stop! Think Fraud: www.stopthinkfraud.campaign.gov.uk





Endpoint: Key Questions

Return to the questions you answered at the start of the lesson. Using a different colour pen, add to, change or edit your original answers.

Finally, think about this learning on your own:

- Consider three ways you could spot social engineering
- Two things you could do to if you ever receive what you think might be a fraudulent email or message
- One source of support you could access for help

Extension Activity

Return to the list of tips for protecting against social engineering and cybercrime.

Design a logo, diagram or image to represent each of the ten top tips.

Resource 3:
Top Tips for Avoiding Social Engineering and Cybercrime



01	Get a second opinion if an offer, competition or giveaway is too unrealistic.
02	Avoid rushing or being pressured to act urgently, particularly if there is pressure to reply or give information in a short time period.
03	Think about the information being asked to handover; why might a legitimate company want or need this?
04	Trust instincts – if something doesn't seem right, don't be embarrassed to refuse to give over information or to leave the conversation.
05	Check who sent the email or verify the caller; if it's genuine, they won't mind if someone checks and uses the general email address or phone number.
06	Check who the email is sent to and question where it came from.
07	Be aware of companies or contacts that are not familiar; use a search engine to check they are genuine.
08	Do not click on any links or open any attachments without doing some research first.
09	Be cautious with social media, keeping privacy settings high, not over sharing personal information and being wary of clicking links.
10	Protect devices by making sure anti-virus software is installed and is regularly updated. Have strong and varied passwords for the different services used online.