25–30 mins.

Senior Secondary (9–12)

How to spot a scam

This lesson explores scams and how to avoid them.

Outcomes

Students:

- recognise a scam
- understand the personal and community impacts
- know where to go for trusted information
- know where to find support

Curriculum links v9.0

Mathematics

AC9M9ST04

AC9M10ST02

HASS

AC9HE9K05

Technologies

AC9TDI10P13

AC9TDI10P14

General Capabilities

Digital Literacy

Managing online safety Level 6

Managing digital privacy and identity Level 6

Locate information Level 6

Literacy

Understanding texts Levels 10 and 11

Numeracy

Interpreting and representing data Level 5 and 6

Understanding Money Level 7–10

Getting started (10 mins)

Open a conversation together on scams:

- What is your experience with scams? Share some stories.
- What types of scams do you know about (e.g. investment scams, romance, phishing)?

Discovery (15–20 mins)

1. Do you know how to spot a scam? It can be hard to tell if something is legitimate, but there are things you can do to protect yourself. Have your students watch the video. Then they can spend 10 mins reading one or scanning all of the following material, marking one or two facts to share with the class.
   a. Watch this short video: Avoid scams (1.22)
   b. Read: Types of scams | Scamwatch
   c. Read: Scam statistics | Scamwatch
   d. Read: Protect yourself from scams | Scamwatch
   e. Read: Banking and credit scams - Moneysmart.gov.au

   For example:

   a. Did you know that up until November 2022 (in only 11 months) Australians lost over $51,741,000 to scams?
   b. Did you know that the greatest amount lost was through investment scams?
   c. Did you know that scammers don't usually work alone and are often organised businesses with thousands of employees?
2. Have your class share and compare tips on how to protect yourself from scams. Some examples:
   a. Do your research before signing up for offers to make easy money
   b. Use trusted sites when shopping online
   c. Keep your personal information safe
3. Ask your class what might be some of the things they should do if they have been scammed. Then read the What to do if you've been scammed - Moneysmart.gov.au webpage to affirm or discover more.

moneysmart.gov.au

How to spot a scam

Other resources

Webpages

Crypto scams - Moneysmart.gov.au

Quizzes

Spot the scam quiz - Scamwatch

Videos

Avoid scams (1.22)

Get Moneysmart (1.05)

Making money decisions (1.11)

Keeping track of spending (0.54)

Choosing a bank account (1.14)

Maximise your savings (1.11)

Getting paid (1.04)

Understanding superannuation (1.12)

Budget for irregular income (1.10)

Manage spending and debt (1.21)

Talking about money (0.58)

Know your consumer rights (1.04)

Know where to get help (1.12)

Understand credit and loans (0.52)

Plan for the future (1.20)

Set savings goals (1.02)

Understand your financial future (1.27)

Planning for big purchases (1.09)

Make an investment plan (1.18)

Extension (10mins)

Can you spot a scam? Take the quiz to find out.

1. You receive a call from Marina from *Out of the Blue* investments. Marina explains that she has a great investment opportunity for you. She says the investment offers high and fast returns, with low risk. She explains that this is 'inside information' and this is an opportunity to invest before the offer is made to the public.

Should you take up the offer?

- Yes – it seems like a great opportunity to make easy money quickly
- No - it might be a scam

2. When you shop online, what are some of the signs that the website you are using is secure?
   - The web address shows a closed padlock or key
   - The web address starts with 'https://'
   - The company has complete contact details, including a street address, phone number and email
   - All of the above
3. How can you protect yourself from identity theft?
   - Use public computers with caution
   - Be aware of what you post on social media
   - Use virus protection software on your computer
   - Monitor your bank transactions
   - All of the above
4. You receive an email from your internet provider advising there is a problem with your account. The email contains a link asking you to update your personal details and requesting immediate payment on the account. The email doesn't match the company name and contains spelling mistakes. What do you do?
   - Click on the links, follow the prompts and enter your personal and payment details
   - Click on the link to check if its legitimate
   - Don't click on the link and delete the email straight away
5. Cryptocurrency scams are increasing. Scammers try to trick people into investing in fake opportunities to buy crypto. What are some of the common tactics?
   - False promises of high returns
   - Fake endorsement from celebrities or government agencies
   - Being contacted through social media or text messages
   - Using dating apps to create a romantic connection and gain trust
   - All of the above

How to spot a scam

Remember:

Remind your students it can be really hard to identify a scam. Scammers are very clever at tricking you out of your money and scams may look real.

Protect your personal information and don't be pressured into making quick financial decisions. **If something sounds to good to be true, then it probably is.**

Solutions.

Question 1

YES - Incorrect. You've just been scammed! This is a common investment scam. Scammers get you to hand over your money by offering high and quick returns, low or no risk opportunities and inside information, like an opportunity to invest before public floats or discounts for early bird investors.

NO - Correct! Good choice. This is a common investment scam. Scammers get you to hand over your money by offering high and quick returns, low or no risk opportunities and inside information, like an opportunity to invest before public floats or discounts for early bird investors.

Reference: Investment scams - Moneysmart.gov.au

Question 2

ALL OF THE ABOVE: That's right! These are all signs of a secure website.

ALL OTHER ANSWERS: Incorrect. That's not quite right, the correct answer is 'all the above'.

Reference: Online shopping - Moneysmart.gov.au

Question 3

ALL OF THE ABOVE: That's right! These are all simple steps to avoid identity theft.

ALL OTHER ANSWERS: That's not quite right. The correct answer is 'all of the above'.

Reference: Identity theft - Moneysmart.gov.au

Question 4

DON'T CLICK: Correct! That's right. This is a phishing scam. Phishing is when a scammer tries to steal your personal information.

ALL OTHER ANSWERS: Incorrect. Be careful, you may be providing your details to scammers. These types of scams are phishing scams. Phishing is when a scammer tries to steal your personal information. The scammer pretends to be a company you know, like a bank or an internet provider. The scammer may contact you by email, phone or text, or on social media.

Reference: Remote access scams - Scamwatch

Question 5

ALL OF THE ABOVE: That's right! These are all common cryptocurrency scam tactics.

ALL OTHER ANSWERS: That's not quite right. The correct answer is 'all of the above'.

Reference: Crypto scams - Moneysmart.gov.au