Topic 5: Online financial transactions

Moneysmart Rookie - Educator guide

Financial literacy for young people

Australian Government

moneysmart.gov.au

Copyright information

Website: moneysmart.gov.au

ISBN: 978 0 9805533 9 0.

Creative Commons

This Educator guide is available under the Creative Commons license (BY - NC - SA). Under this license, the material is available for free use and adaption so that educators can use, adapt and re-publish material from the resource without seeking the permission of ASIC.

Copyright notice

CAL exemption

March 2021

Table of contents

Introduction to ‘Online financial transactions’

Moneysmart’s Rookie series helps people aged 16-25 avoid expensive mistakes or ‘rookie errors’ when they make their first financial decisions.

This topic is about what to be careful of when banking or shopping on the internet – especially protecting your money and your personal information. There is also information about what a person can do if they have problems banking or shopping online.

Some of the aspects covered in the topic are:

- How to check the security and privacy of a website
- Checking for scams, fake products and fake emails
- Keeping your computer and mobile phone secure
- The importance of keeping records (e.g. receipts)
- Keeping your passwords and personal information safe
- Solving problems with online banking and shopping.

Overview

- **Year level:** 9-12
- **Duration:** 4.5 hours (Educator guide - approx. 1.5 hours + Additional lessons – 3 hours)
- **Learning areas:** Economics and Business, English
- **Audience:** Youth and community workers, student advisers, mentors.

Topics

The Moneysmart Rookie education initiative covers six topics:

1. Car ownership
2. Credit and debt
3. Mobile phone ownership
4. Moving out of home
5. **Online financial transactions**
6. First job

Rookie resources

This Educator Guide for **Topic 5: Online financial transactions** will be used in combination with the following resources which have been designed to suit the various levels of knowledge and understanding of students.

Required Moneysmart resources	Optional Moneysmart resources
Video: Too good to be true (5:11 mins) **Optional video:** Kate gets scammed (1:33 mins) **Optional video:** To buy or not to buy (0:50 sec)	• Rookie: Online financial transactions – Teaching resource page includes Curriculum alignment • Student life and money section on Moneysmart, see 'Online Shopping' • Teaching resources (filter by year) on Moneysmart • Australian Competition and Consumer Commission (ACCC), and Scamwatch

Knowledge levels

What content will suit your students? The level of information you use will depend on how much understanding your students have of a topic. The following describes the content that best suits different levels of understanding (1, 2, and 3):

Your audience has this level of knowledge	Description
Level 1: No or limited understanding	If your students cannot answer any of your questions or can only answer them a bit, they have no or a limited understanding. You can help them to understand more by showing the *Moneysmart Rookie* videos for the topic. You can also go through the Level 1 activities in the guide. After watching the video, see if your students have developed some understanding of the topic by asking them to answer the questions again.
Level 2: Some level of understanding	If your students answer one or more of your questions, they have some level of understanding. You can show them the *Moneysmart Rookie* videos to review the topic. You may wish to pause the video in sections and discuss key issues shown. You can also go through the Level 2 activities and stories in the guide, as these are for students with some level of understanding.
Level 3: Good level of understanding	If your students are able to answer all of your questions, they have a good level of understanding. You can show them the *Moneysmart Rookie* videos to review the topic. You can also go through the Level 2 and 3 activities in the guide, as these are for students with a good level of understanding.

Note: Educators can use these levels as progressions, starting points and extensions to suit students' needs.

Reflection questions

At the end of each session, educators can use the following questions to reflect on the effectiveness of the session:

- What worked well? What did not work well?
- Did the students understand the key messages?
- Did the activity engage the students? How could the activity have been more effective?
- What questions unexpectedly emerged and how did you handle them?
- What might you do differently next time?

Sub-topic: Secure payment options

Key messages

- Protect your money when shopping online
- Use secure options when shopping online
- Transact through trusted websites.

Notes for the educator

Make sure that a company's website is secure and safe before you enter any personal information or buy online.

Check three things:

1. The safety and security of a website can be checked by making sure the address at the top of the page starts with https:// and not just http://. It's the 's' in https:// that tells you the website is secure.
2. Does your web browser show a closed padlock like this  If it does, the website is secure.
3. Does the company have complete contact details, including a street address? If you don't know and trust the company, don't buy from them and don't enter personal details.

Some of the dangers of not sticking to these rules are:

- You could lose your money because you don't receive what you bought online.
- Your bank account details could be stolen, and money could be stolen from your account
- Your personal information (name and contact details) could be used to steal your identity and then steal money from you or people you know. This is called identity theft (or identity fraud).

Your best protection is to find out more about how scams work so you'll have a better chance of spotting one. Visit the Australian Competition and Consumer Commission (ACCC).

Activity 5.1: What does https:// tell you?

Level	Duration	Resources needed
1	10 mins	• Too good to be true (5:11 mins)

This activity is based on the *Moneysmart Rookie: Too good to be true* video. It will help the students to start thinking about ways they can tell whether a website is secure for online purchasing or not.

Step one

Ask them to watch the video from start to finish and look out for clues that tell people a website is more secure. Point out that one clue appears just for a moment.

Step two

Ask the students the following question:

What clues were in the video that tell you whether a website is secure enough to buy stuff from?

Educator note: This requires simple attention and observation on the part of the student.

Suggested answer

The letters https:// appear briefly.
Announcements about winning prizes etc. mean a website should be treated with suspicion (it may not be secure).

Note: Most website addresses start with http://. However, a website that is secure for online purchases begins with https:// (NOTE the 's').

Activity 5.2: Secure websites – spot the difference

Level	Duration	Resources needed
1	10 mins	Worksheet 5.2

Note: Students with a Level 1 of understanding will be able to answer the questions in the activity. However, the questions relate to important security information and students at all levels should do this activity, so they have the opportunity to learn the information.

Step one

Introduce the worksheet to students and explain that these are two websites with products you can buy online. However, only one of them is safe to buy from.

Step two

Ask the students the following questions:

1. Can you spot anything that looks suspicious about one of these websites?
2. Can you spot anything on either page that gives you confidence that the page is secure for online payments?
3. Which website looks like it is safer for making payments online?

Suggested answers

1 The website on the right looks suspicious because:

- a it does not have https:// in its web address at the top
- b there is a ‘You’ve won!’ box that could be a scam
- c there are no contact details for the company

2 The website on the left looks more secure because

- a It has a padlock symbol
- b It has the company name, address and phone number

3 The website on the left (because of the answers to questions 1 & 2)

Activity 5.3: Non-secure websites – what can happen?

Level	Duration	Resources needed
2	10 mins	This activity builds on Activity 5.2. Too good to be true (5:11 mins)

It helps the students to understand the dangers of buying from an unsecure website.

Ask the students the following questions:

1. What could happen if you buy from the suspicious website?
2. What is identity theft?

Suggested answers

1. You could lose your money because they don't send you the product.
   Your bank account details could be stolen, and money could be stolen from your account.
   Your personal information (name and contact details) could be used to steal your identity.
2. Identity theft is when someone else uses your personal details in order to steal money or gain other benefits by pretending to be you.

Note: Identity theft is explained effectively in the *Moneysmart Rookie: Too good to be true* video. If you think the student needs a clearer idea of what identity theft is, you could show them the *Moneysmart Rookie: Too good to be true* video again.

Check for understanding

After completing the activities, you can check the students' level of understanding and knowledge by asking questions such as:

- Tell me one thing that means a website is more secure.

A:
a https://
b Padlock
c Company contact details

- How can you lose money if you buy from a website that is not secure?

A:
a You could lose your money because they don't send you the product.
b Your bank account details could be stolen and money could be stolen from your account.
c Your personal information (name and contact details) could be used to steal your identity.

Sub-topic: My rights when shopping and banking online

Key messages

- You have rights as a consumer
- There are things you can do to resolve disputes when buying online
- Talk to someone who can help you resolve your dispute.

Notes for the educator

Knowing your rights can help you if you have a problem with an online purchase. You can find out your rights from the Australian Competition and Consumer Commission (ACCC) or your state or territory consumer protection or fair trading organisation.

If you don't receive what you pay for in good condition, there are steps you can take to try to fix the problem.

- Check the seller's website to see if they tell you how to make a complaint to them. If they don't seem to have a special way to make a complaint, phone them or email them.
- Contact your bank or other financial institution about any protection they may have for you such as chargeback. A chargeback is a return of funds from a retailer or service provider to a consumer's bank account, often initiated by the consumer's bank.
- Contact the ACCC or your consumer protection or fair trading organisation in your state or territory. They may be able to help you sort things out with the seller. The main responsibility of the ACCC is to make sure that businesses and individuals comply with Australian competition, fair trading, and consumer protection laws – in particular the Competition and Consumer Act 2010.

Activity 5.4: Deng gets tricked by a fake

Level	Duration	Resources needed
2	10 mins	Worksheet 5.4

This activity uses **Deng's story** as an example for the students to think about how to deal with problems to do with online purchasing.

Educator note: Students with a Level 2 of understanding will be more likely to be able to answer the questions in the activity. However, it is important security information and students at all levels should do this activity, so they have the opportunity to learn the information.

Step one

Read out the first part of Deng's story and ask students the following question:

1. What should Deng do to solve the problem?

Suggested answer

1. Check the seller's website to see if they tell you how to make a complaint to them. If they don't seem to have a special way to make a complaint, look for their contact details on the website, then phone them or email them. Tell them about the problem and ask the seller what they will do to fix the problem. – You have a right to receive what you paid for or a refund in full.

Step two

Read out the second part of the story and ask students the following question:

1. Where can Deng go for help getting his order or his money back?

Suggested answer

1. Deng can contact the ACCC or the consumer protection or fair trading organisation in his state or territory. He should also ask his bank or financial institution if he has any protection to get the payment reversed because of the fraud.

Notes:

- How to get help is explained near the end of the *Moneysmart Rookie: Too good to be true* video. If you think the student would benefit from seeing the video, you could show them the video again.
- To contact the ACCC, people can visit the ACCC website and click 'Contact us'.

Check for understanding

After completing the activities, you can check the students' level of understanding and knowledge by asking questions such as:

- **If you buy something online and you don't receive it, what's the first thing to do to solve the problem?**
  A: Contact the company you bought from.
- **If you can't contact the company, what do you do next to solve the problem?**
  A: Contact the ACCC or the consumer protection or fair trading organisation in your state.
- **What is the ACCC?**
  A: The Australian Competition and Consumer Commission. The main responsibility of the ACCC is to make sure that businesses and individuals comply with Australian competition, fair trading, and consumer protection laws – in particular the Competition and Consumer Act 2010.

Sub-topic: Recognising scams

Key messages

- Scammers use tricks
- Use safe online practices to avoid being scammed
- If you think you have been scammed you can get help.

Notes for the educator

Phishing scams are a way of stealing your financial and personal details. Scammers send fake emails or texts, or they call people and pretend to be from a bank or other financial institution. A scammer's email may include a link to a fake website. Everything seems very real but it's actually a very clever fake.

What should you do? DON'T click on links and DON'T give them any information.

If you think money has been taken from bank account, tell your bank immediately.

Learn how to recognise scams and get other tips about this by searching 'banking and credit scams' on Moneysmart.

Your best protection is to find out more about how scams work so you'll have a better chance of spotting one.

If you get scammed, contact the ACCC who can use your information to:

- help catch the scammer
- help other people avoid the scam
- prosecute the scammer in court (you may even get some financial compensation!)

To contact the ACCC, people can visit the ACCC website and click 'Contact us'.

Activity 5.5: Effy gets scammed

Level	Duration	Resources needed
1	15 mins	Too good to be true (5:11 mins)

This activity is based on the *Moneysmart Rookie: Too good to be true* video. It will help the students to avoid rookie errors.

It will also help people to think about how to avoid getting caught by a scam.

Step one

Before watching the video, ask the students the following question:

1. What do you think is meant by the word 'scam'?

Step two

Watch the video and then ask the student the question again:

1. Now, after watching this video what do you think is meant by the word 'scam'?

Answer

A trick designed to cheat you of your money. If the scam operates using the internet, it's called an 'online scam'.

Step four

Ask the students to watch the video from start to finish and look out for anything about scams.

Step five

Ask the students the following questions:

1. How did Effy get scammed?
2. How could you spot or avoid getting caught by similar scams?
3. What other online scams have you heard of?
4. How could you avoid getting into financial trouble through these scams?

Suggested answers

1. Effy was waiting for her first credit card to arrive and someone called her pretending to be from her bank. She gave them her personal details and the scammer then used her details to get money off her credit card and she lost $10,000.
2. Before you give your personal details away, ask questions to make sure the person is definitely who they say they are. To be even more certain that it's not a scam, tell the person you will hang up and then ring the bank to check the person calling is from the bank. (Students may have other good suggestions.)
3. There could be many responses, but if no scams are mentioned then you could discuss the scam mentioned in one of the comments from people in the video (e.g. an email from someone pretending to be a relative and asking for money).
4. There could be many responses, but if no scams are mentioned then you could discuss the scam mentioned in the comment about the email (above) and suggest:
    - not responding to the email, and/or
    - blocking the sender, and/or
    - reporting the sender to the police, ACCC or similar law-enforcement agencies.

Note: One of the students may mention the word 'phishing' or you may wish to introduce the word yourself. It means: 'sending emails or text messages that attempt to trick you into giving out your personal information such as usernames, passwords or banking details'.

Activity 5.6: Getting help if you get scammed

Level	Duration	Resources needed
2	10 mins	This activity builds on Activity 5.5 Optional links: • ACCC • Scamwatch

Step one

Ask the students the following questions:

1. If you discover there's money that's been withdrawn from one of your bank accounts, what should you do immediately?
2. If you discover that a purchase has been made using your credit card what should you do immediately?

Suggested answers

1. Contact your bank and tell them what the problem is.
2. Contact your bank (or other financial institution) and tell them what the problem is.

Step two

Ask the students the following question:

1. Why is it also a good idea to contact the ACCC (Australian Competition and Consumer Commission) or the consumer protection or fair trading organisation in your state?

Suggested answer

2. The ACCC can use your information to:
    - help catch the scammer
    - help other people avoid the scam
    - prosecute the scammer in court (you may even get some financial compensation!)

Note: To contact the ACCC, people can visit the ACCC website and click 'Contact us'.

Check for understanding

After completing the activities, you can check the students' level of understanding and knowledge by asking questions such as:

- What's meant by the word 'scam'?
  A: A trick designed to cheat you of your money. If the scam operates using the internet, it's called an 'online scam'.
- How could you spot or avoid getting caught by scams?
  A: Before you give your personal details away, ask questions to make sure the person is who they say they are. To be even more certain that it's not a scam, tell the person you will

hang up and then ring the bank to check the person calling is from the bank. (Students may have other good answers.)

- How can the ACCC help you?
  A: i The ACCC has great information about scams and how to avoid getting tricked by them.
  ii The ACCC can catch people who carry out scams (including a scam that you get caught by).

Sub-topic: Protecting yourself online

Key messages

- Identity theft can be achieved through small pieces of personal information
- Protect your identity when using social media
- Identity theft can impact on finances.

Notes for the educator

People use scams to steal your money, your credit card or bank details, or your identity. This can have a big impact on your finances.

People can steal your personal and financial information piece by piece in different ways (by reading your social media page, using a fake email or phone call, creating a fake website, or sending you a fake letter). This is called identity theft (or identity fraud).

It can be difficult to tell whether a website, email or phone call is real or fake.

How can you protect yourself?

- BE CAREFUL about the personal details you put on your social media page, think about making your profile private so only friends can see it.
- DON'T click on links that look suspicious or come from email addresses you do not recognise
- DON'T give out information online unless you trust the website you are providing information to.

If someone phones you, ask questions to make sure the person is definitely who they say they are. To be even more certain that it's not a scam, tell the person you will hang up and then ring the bank to check the person calling is definitely from the bank.

Your best protection is to find out more about how scams work so you'll have a better chance of spotting one. For more information visit the Australian Competition and Consumer Commission (ACCC).

Activity 5.7: Johnny's social media page

Level	Duration	Resources needed
2	20 mins	Worksheet 5.7

This activity uses **Johnny's social media page** to show the student how simple personal details can be used for identity theft.

Note: Students with a Level 2 of understanding will be more likely to be able to answer the questions in the activity. However, it is important security information and students at all levels should do this activity, so they have the opportunity to learn the information.

Step one

Show students the worksheet and ask the following questions:

1 What personal information has Johnny put on his social network page that could be used by another person pretending to be Johnny?

2 What is the name given to this sort of thing when someone steals another person's personal details and pretends to be them?

3 Why are those three pieces of information valuable to an identity thief?

Suggested answer

1 All of that information could be used by someone pretending to be Johnny. Probably the most valuable ones are the following:

a) his name

b) his complete address

c) his date of birth (17 January 1998).

2 Identity theft - Note: For more information on identity theft, visit ACCC's Scamwatch

3 Those three pieces of information are often asked for by banks and other financial institutions for identification purposes (e.g. when you phone them).

Activity 5.8: Johnny reveals his secret details

Level	Duration	Resources needed
3	20 mins	• This activity builds on Activity 5.7. • Worksheet 5.7 and 5.8

The activity uses **Johnny's story** about a fake email he got about his social media page to show the students how their identity can be stolen and used to trick other people they know.

Note: Students with a Level 2 of understanding will be more likely to be able to answer the questions in the activity. However, it is important security information and students at all levels should do this activity, so they have the opportunity to learn the information.

Steps

Ask students the following question:

1 What advice would you have given Johnny about the email he received?

2 Does anyone know the word that's used for 'sending emails or text messages that try to trick people into giving out their personal information such as usernames, passwords or banking details'?

3 Does anyone know a website where you can get more information about what phishing is and news about identity theft by phishing'?
Note: If no-one can answer, try the next question.

4 Does anyone know which organisation runs the Scamwatch website'?

Suggested answer

1 Never send your social network account details through a link in an email and think carefully before you give away any personal or financial information.

2 Phishing.

3 a) Australian Competition and Consumer Commission (ACCC)

b) Scamwatch

4 a) Australian Competition and Consumer Commission (ACCC)

Extension

Ask students for examples of information they share on a variety of platforms & the information they could inadvertently share through images and sharing of geo-location.

Visit Scamwatch website to see statistics on all types of scams in Australia.

Johnny's identity theft story – Part 2:

Read part 2 of Johnny's story.

Steps

Ask students the following questions:

1 What advice would you have given Johnny's sister about the email she received?

2 Where else could a person go on the internet to steal your personal details?

3 What should you do if someone steals your identity and pretends to be you?

Suggested answer

1 Never send your bank account details through email and think carefully before you give away any personal or financial information.

2 A person goes on the internet to steal your personal details from:

a) Other social network sites you use (including sites where you send messages to subscribers)

b) Your blog

c) The website of any organisation where you have given your personal details

Note: If the student has already done the activity about secure and non-secure websites, you could remind the student that they should check any organisation's website for security clues before they give their personal details to the organisation.

3 If your bank account details have been stolen, immediately tell your bank.
Report identity theft and other to the ACCC Infocentre on 1300 302 502. This can help the ACCC to warn other people and can even help you to get compensation.

Check for understanding

After completing the activities, you can check the students' level of understanding and knowledge by asking questions such as:

What is meant by 'identity theft'?
A: Using someone else's personal details in order to steal money or gain other benefits by pretending to be that person.

What are some of the ways people get your personal information?

A:

- From your social media page
- By sending you a fake email
- By phoning you and asking you questions
- By tricking you with a fake website
- By sending you a letter through the post

Worksheets: Online financial transactions

Worksheet 5.2: Secure websites – spot the difference

Worksheet 5.4: Deng gets tricked by a fake website

Deng's story

Deng is really into computers and ordered some special equipment online from a company he found who offered free express shipping by air to Australia. He ordered the equipment and paid on his debit card. He got an email from the company confirming his order and saying the goods should get to him within 10 days. However, it's now been one month since he ordered the equipment.

Question

1 What should Deng do to solve the problem?

Part two

Deng tried to email the company, but his email bounced back and when he tried to check the contact details on their website again, the website was no longer there, it has been taken down. He kept the email from the company confirming his order but he's not sure what to do next.

Question

1 Where can Deng go for help getting his order or his money back?

Worksheet 5.7: Johnny's social media page

Johnny Bloggs

PUBLIC PROFILE

Work and Education

ABC123 Workplace
Sydney, NSW
Sep 2017 to present

Example Highschool
Sydney, NSW
Feb 2011 to Nov 2015

Living

Current
123 Sample St, Sampletown
NSW, 2000

Hometown
Darwin, NT

Family

Buster Bloggs
My dog

Basic Information

Birthday: January 17, 1998
Status: Single

Johnny Bloggs

I'm actually earning decent money for a change!

Like · Comment · Share

Worksheet 5.8: Johnny reveals his secret details

Johnny's story

Johnny got an email that looked like a genuine email from Instagram. The email said that there had been a security issue with the network and asked him to click a link in the email. When he clicked the link, he was taken to a webpage which looked like an official request for him to confirm his username and password. The next day he discovered that he could not access his own social network home page. Someone had logged in to his account and changed his password.

Questions

1. What advice would you have given Johnny about the email he received?

2. Does anyone know the word that's used for 'sending emails or text messages that try to trick people into giving out their personal information such as usernames, passwords or banking details?

3. Does anyone know a website where you can get more information about what phishing is and news about identity theft by phishing?

OR

Does anyone know which organisation runs the Scamwatch website?

Johnny's story – Part two

Johnny's sister got an email that looked like it was from Johnny. The email said that Johnny wanted to send her some money and it asked her for her bank account details. Johnny's sister replied to the email by clicking Reply and sent all the details. Then she discovered that someone had withdrawn money from her account. She phone Johnny and he told her that he had not sent the email to her. They realised that someone was using Johnny's identity to pretend to be him.

Questions

1. What advice would you have given Johnny's sister about the email she received?

2. Where else could a person go on the internet to steal your personal details?

3. What should you do if someone steals your identity and pretends to be you?

Additional lesson 1: Online financial transactions — be savvy and safe

- **Year level:** Year 9 and 10
- **Duration:** 2 hours
- **Key learning area:** English, Mathematics, Economics and business

Lesson description

Students explore and investigate the diversity of consumer rookie errors associated with making an online financial transaction to purchase goods and services. Learning begins with watching the Moneysmart *'Too good to be true'* video. Students then discuss and reflect on the key financial positives and negatives of making an online financial transaction to purchase goods and services, including the investigation of online scams, scam protection techniques, and online consumer purchase rights.

In the second part of the lesson students complete an activity worksheet to investigate the necessary precautions and knowledge required to avoid making rookie errors when making an online financial transaction consumer purchase.

Long-term understanding/deep learnings:

- Making informed responsible choices around online financial transaction to purchase goods and services can protect your money.
- You can protect your money and avoid common issues or 'rookie errors' if you use safety methods for online financial transactions services including protection against scams, viruses, identity theft, and password corruption.
- In Australia you have the same consumer rights when shopping online as when shopping at a physical retail store but this may not be the case for online stores based offshore.
- You can access help from places or organisations such as Scamwatch, the police, your bank or financial institution when online financial transaction safety or consumer issues arise.

Additional activity 1(a): 'Too good to be true' video

Level	Duration	Resources needed
N/A	15 mins	Too good to be true (5:11 mins)

Discussion

Facilitate a class discussion of some of the video's key messages. Ask the class, 'What were the main messages of the *Too good to be true* video?'

Write responses on the board - responses should focus around:

- Protecting yourself when you are online (using strong passwords, only visiting safe websites).
- Keeping your antivirus software up to date.
- Avoiding scams or knowing what to do if you have been scammed.
- Taking precautions to prevent identity theft.
- Knowing what to do if you don't get what you ordered online.

Additional activity 1(b): Website security checklist

Level	Duration	Resources needed
N/A	20 mins	Additional worksheet 1(b) - Secure websites

Task 1: Discussion

Ask the students: What three standard website security checks you need to undertake to ensure a website is secure before you enter any personal information or buy online?

- Make sure the address at the top of the page starts with https://. Emphasise that it is the 's' in https:// that informs you the website is secure.
- Make sure your web browser shows a closed padlock icon, which indicates it is secure.
- Make sure the company has complete contact details including a street address.

Ask the students: What could happen if you don't conduct the three standard website security checks before you enter any personal information or buy online?

Answers should focus around:

- You could lose your money and not receive the product you bought online.
- Your bank account details could be stolen and money stolen from your account.
- Your personal details could be used to steal your identity and then used to steal money from you or people you know.

Task 2: Website security practice task

Distribute additional worksheet 1(b) and ask the class: 'Which website is safe to buy from? Why?'

Suggested Answers

- The website on the right looks suspicious because:
    - It does not have https:// or padlock in its web address at the top.
    - There is a 'You have won an iPad!' box that could be a scam.
    - There are no contact details for the company.
- The website on the left looks more secure because:
    - It has a padlock symbol.
    - It has the company name, address and phone number.
    - It has an 's' in its website address: https://

Teacher tips:

Emphasise that people need to double check all website details by cross referencing them with other sources of information such as online yellow pages. They should also carefully check details such as the website address to make sure it is correctly spelt.

Task 3: Internet website security check

Ask the students to select one banking website (e.g. ANZ, NAB), one sporting website (e.g. AFL/NRL/A-League) and one online sales website (e.g. Myer, eBay, Gumtree), and check to see if your selected website has the three basic website security safety standard checks.

Additional activity 1(c): Identity theft

Level	Duration	Resources needed
N/A	30 mins	Optional links: • Protecting your personal information on the eSafety website • Stevie's scam school videos (2 mins each) on the Consumer Affairs (Victoria) website.

Task 1: Discussion

Focus statement: Identity theft is a specific type of fraud, which involves stealing money or gaining other benefits by pretending to be someone else.

Ask students the following questions to prompt discussion:

- What personal information might a fraudster/scammer find useful? (full name, address, birth date, bank account or other financial information, passport number).
- Where might a fraudster gain access to this type of information? (social networking profiles, malicious software used to gain access to computer data, scams requesting personal information).
- What would a fraudster potentially gain from stealing someone's identity? (access to bank account, credit card, personal loan set up in some else's name, conducting illegal business).

Ask the students for ideas on how they can protect themselves from identity theft.

Answers should focus around:

- Limit the personal details you place on social media pages.
- Don't click on links that come from email addresses you don't recognise.
- Don't give out information online unless you trust the website.
- If someone phones you seeking personal information, ask questions to confirm the person's identity, or hang up, ring the bank to check the person calling you is from the bank.
- Keep your passwords secure, secret, and difficult for scammers to guess.

***Teacher tip:** if you have time introduce this activity with either of the following resources:

- Consumer Affairs Victoria has a set of 'Stevie's Scam School' videos which highlight some key consumer scams to watch out for.

Task 2: Creating a secure password

Whilst there is no such thing as an unbreakable password, steps can be taken to make your password secure and easily remembered by you, but not others.

- Try to create a complex password, with at least seven characters. A complex password is more difficult to guess than a simple password and offers better protection.
- Your password could include at least one character from at least three of the following sets:
- uppercase letters (A-Z)
- lowercase letters (a-z)
- numerals (0-9)
- special characters such as ()~`#$*&@^
- Instead of using a simple password that says '**blues**', you could enhance your password security by turning it into **Blues#5?!,** which now includes an uppercase letter **'B**', lower case letters, '**lues**', a number, '**5',** and special characters, # ? !
- Rather than use a password that can be easily guessed eg, *current pet's name or current street name*, use the name of the first pet you owned, or a previous street address. That way your password will be still easy to remember, but not as easily guessed, providing you don't share your password with anyone.
- Using the above guidelines create two secure passwords, but don't reveal them to your friends or classmates as you will have an opportunity to test the security of your password when you test it on '*The Password Meter'* in the next lesson.

Additional activity 1(d): Scambusters

Level	Duration	Resources needed
N/A	20 mins	Scamwatch website

Task 1: Discussion

Ask the class the following questions:

What are the basic ingredients of a scam?

Answers should focus around a scam:

- wanting money or access to bank accounts
- trying to entice you with a free offer or prize
- having a time limit on it (e.g. register now).

How do you spot a scam?

Answers should focus around:

- If a scam appears too good to be true – it is!
- If a scam sounds or reads as dodgy – it is!
- Many scams have several simple grammar or spelling errors.
- Most scams come via an indirect and/or impersonal source (e.g. internet, email, letter etc).
- Most scams are a variation of an old or well-known scam from history.

Present the following classic scams to the class:

- 'Distant Relative Inheritance Scam': You have inherited a large sum of money from a distant relative overseas. Just send us your bank account and we'll send you the money within 24 hours.
- 'Lost Gold Mine Scam': I have discovered an ancient African/Australian/South American gold mine worth millions, but you need to send me a mere $10,000 to help secure the land title. In return you'll receive a big percentage of the profits.
- You have won a $1 million jackpot! Just transfer $100 into my bank account to cover fees and I'll post you your prize money by cheque.

Ask the class to describe any scams they have come across.

***Teacher tips:** Put the classic scams into a PowerPoint to present to the class.

Use the Scamwatch website to present 'recent scam victim stories' to see how sophisticated scams have become.

Additional activity 1(e): Online financial safety 101

Level	Duration	Resources needed
N/A	20 mins	Additional worksheet 1(e)

Task 1: Online financial safety 101 worksheet

Distribute additional worksheet 1€: 'Online financial safety 101'. Ask students to answer the following questions on the worksheet provided:

1 Describe three methods for protecting ourselves from scams.

2 What should you do if you believe you have been scammed?

3 What consumer rights do you have when buying products online?

4 Who can you contact?

5 Using the internet/newspapers, research a scam news story, and answer the following questions:

- What was the scam?
- How did the scam work?
- Who was the scam targeting?
- How much money was taken by the scammers?
- How was the scam uncovered?
- How could the scam have been prevented?

***Teacher tip:** This exercise could be completed by individual students, or in pairs, as a class response or summative assessment task. Ask students to use the following websites:

- Online shopping on the 'Student life and money' section on Moneysmart
- Consumers section of the ACCC website
- ACCC Scamwatch website

Extension or homework activity

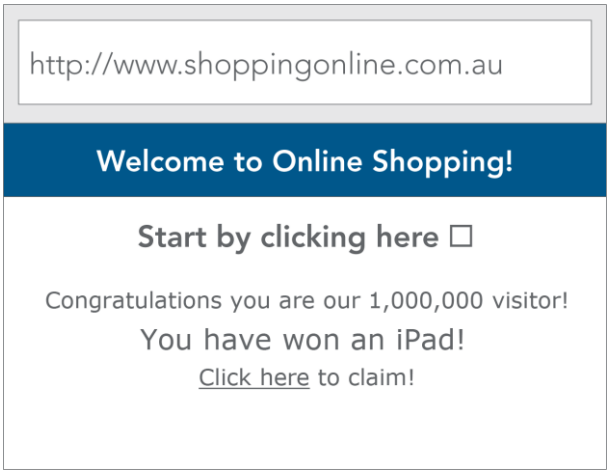
Investigate the history and scam mechanisms used in a 'PONZI' scam which is still used on a regular basis today to successfully rip off billions of dollars from unsuspecting people.

Reflective/summative assessment (5 minutes)

- List three new things that you learned today about online financial transactions.
- In your opinion, which of these components is the most important to you?
- What else did you learn about online financial transactions today?

Additional worksheet 1(b) – Secure websites

Spot the difference between these websites.



Additional worksheet 1(e): Online financial safety 101

NAME:

Answer the following questions on the worksheet using these websites:

- Online shopping on the 'Student life and money' section on Moneysmart
- Consumers section of the ACCC website
- ACCC Scamwatch website

1. Describe three methods for protecting ourselves from scams.

2. What should you do if you believe you have been scammed?

3. What consumer rights do you have when buying products online?

4. Who can you contact about your online consumer rights?

5. Using the internet or newspapers, research a ‘scam’ news story and answer the following questions:

a. What was the scam?

b. How did the scam work?

c. Who was the scam targeting?

d. How much money was embezzled by the scammers?

e. How was the scam uncovered?

f. How could the scam have been prevented?

Additional lesson 2: Online financial transactions — the fine print

- **Year level:** Year 9 and 10
- **Duration:** 90 minutes
- **Key learning area:** English, Mathematics, Economics and business

Lesson description

Students will continue to explore and further investigate the previously identified range of consumer rookie errors associated with making an online financial transaction to purchase goods and services by revising their learnings from the previous lesson on online financial transactions.

In the second part of the lesson students inquire more deeply into the underlying complexities of common rookie errors and financial pitfalls of online scams, scam protection techniques and online consumer purchase rights by designing and producing a poster, PowerPoint or brochure. The lesson concludes with students applying their richer knowledge of online financial transaction rookie errors to complete the related Moneysmart Teaching *'Online Shopping and banking'* practice conversation.

Long-term understanding/deep learnings:

- You can protect your identity and your money when online by using safe practices online, secure options and making transactions through trusted websites.
- You can protect your money and avoid common issues or 'rookie errors' if you use safety methods for online financial transactions services including protection against scams, viruses, identity theft, and password corruption.
- You can access help from places or organisations such as Scamwatch, the police, your bank or financial institution when online financial transaction safety or consumer issues arise

Additional activity 2(a): Revision

Level	Duration	Resources needed
N/A	10 mins	N/A

Task 1: Revision competition

Divide the class into two teams. Take turns to ask each team the following questions. Tell students that they can consult each other before answering the question.

- What can you do to protect yourself online?
- Identify a method for protecting yourself from scams.
- How can you prevent identity theft?
- What can you do to resolve an online dispute?
- Identify one right that you have when making online purchases.
- How can you avoid being scammed?
- How can you tell that a website is secure?
- How can you keep your computer or mobile phone secure?
- What are the key characteristics of a secure password?
- What is the value of keeping an electronic or paper receipt?

Give each team a point for a correct answer. The winner is the team with the most points. Alternatively, the questions are open-ended enough to allow for each group to give correct answers so that the competition might result in a draw.

***Teacher Tip:** Put the questions into a PowerPoint and show them on the projector or TV screen.

Additional activity 2(b): Password meter

Level	Duration	Resources needed
N/A	10 mins	Password meter website (http://www.passwordmeter.com/).

Task 1: Test your password

Ask students to go to the password meter website. Ask students to enter the password or passwords from the previous lesson to test out the security of their password or passwords. Discuss what types of passwords work best.

Additional activity 2(c): What to do if you have had your identity stolen

Level	Duration	Resources needed
N/A	10 mins	Identity theft page on Moneysmart

Task 1: Identity theft actions

Show the class the information on scams and identity fraud on the Moneysmart website. Ask students to list four actions to take if their identity is stolen.

Expected responses include:

- Report it to the police immediately
- Contact your bank or financial institution
- Inform the relevant government agency or business

Reflective/summative assessment

Students could be assessed on their final presentations. Worksheet 1 includes criterion for assessing the poster, PowerPoint or poster.

Additional activity 2(d): Poster, PowerPoint or Brochure

Level	Duration	Resources needed
N/A	45 mins	Worksheet 2(d)

Task 1: Design a promotional tool

***Teacher tip**: This task is designed to go over a number of class sessions with its introduction taking 30 minutes.

Have the class design and produce a poster, PowerPoint or a brochure highlighting the positives and negatives of conducting finances online. Prompt students to think about their audience (who will see or read the poster or brochure) and what students want their audience to think when they see the poster, PowerPoint or brochure.

Brainstorm with students who their audience might be. It would be helpful to consider who in the community might benefit in terms of time and convenience by conducting finances online contrasted to those who might be most vulnerable to online rookie errors. For example, many older people know less about the internet than young people do. The class might need to discuss how you would aim a promotional tool at older people.

Distribute the worksheet: Poster, PowerPoint or brochure which asks students to cover the following:

- an explanation of why strong passwords are important
- a description of why it is important to only visit safe websites
- an outline of why it is important to keep your antivirus software up to date
- an explanation of how to avoid scams
- an outline of what to do if you have been scammed
- an explanation of the precautions that can be taken to prevent identity theft
- a description of how to resolve disputes when making online purchases
- five positive factors about conducting finances online, including convenience, ability to check or monitor financial status, time, portability, ability to keep electronic records

Remind students that they should include colour and pictures in their tool. A good strategy to follow would be to keep it short (to the point) and simple.

You may wish to ask groups to present their promotional tool to the class. In their presentation they could identify their target audience and how they have delivered the key points to suit this audience.

Additional worksheet 2(d): Poster, PowerPoint or brochure

NAME:

Design and produce a poster, PowerPoint or a brochure highlighting the positives and negatives of conducting finances online.

Use Moneysmart and the internet to research the content for your product. Cover the following in your final presentation:

- an explanation of why strong passwords are important
- a description of why it is important to only visit safe websites
- an outline of why it is important to keep your antivirus software up to date
- an explanation of how to avoid scams
- an outline of what to do if you have been scammed
- an explanation of the precautions that can be taken to prevent identity theft
- a description of how to resolve disputes when making online purchases
- five positive factors about conducting finances online, including convenience, ability to check or monitor financial status, time, portability, ability to keep electronic records.

Remember to include colour and pictures in your presentation. A good strategy to follow would be to keep it short (to the point) and simple. Your work will be assessed using the following criteria:

Criteria	Mark
A detailed explanation of why strong passwords are important A concise and accurate description of why it is important to only visit safe websites A detailed outline of why it is important to keep your antivirus software up to date A detailed explanation of how to avoid scams A detailed outline of what to do if you have been scammed A detailed explanation of the precautions that can be taken to prevent identity theft A concise and accurate description of how to resolve disputes when making online purchases A detailed description of five positive factors about conducting finances online	10
A good explanation of why strong passwords are important A concise description of why it is important to only visit safe websites A good outline of why it is important to keep your antivirus software up to date A good explanation of how to avoid scams A good outline of what to do if you have been scammed A good explanation of the precautions that can be taken to prevent identity theft A concise description of how to resolve disputes when making online purchases A concise description of five positive factors about conducting finances online	7-9

An explanation of why strong passwords are important A description of why it is important to only visit safe websites An outline of why it is important to keep your antivirus software up to date An explanation of how to avoid scams An outline of what to do if you have been scammed An explanation of the precautions that can be taken to prevent identity theft A description of how to resolve disputes when making online purchases A description of five positive factors about conducting finances online	4-6
A poor explanation of why strong passwords are important A very brief description of why it is important to only visit safe websites A poor outline of why it is important to keep your antivirus software up to date A poor explanation of how to avoid scams A poor outline of what to do if you have been scammed A poor explanation of the precautions that can be taken to prevent identity theft A very brief description of how to resolve disputes when making online purchases A very brief description of five positive factors about conducting finances online	1-3
No explanation of why strong passwords are important No description of why it is important to only visit safe websites No outline of why it is important to keep your antivirus software up to date No explanation of how to avoid scams No outline of what to do if you have been scammed No explanation of the precautions that can be taken to prevent identity theft No description of how to resolve disputes when making online purchases No concise description of five positive factors about conducting finances online	0