Lesson plan 1: Online financial transactions

Online financial transactions — be savvy and safe

Year level: Year 9 and 10

Duration: 60 minutes (lesson 1 of 2 connecting lessons)

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. The lesson concludes with the opportunity for students to apply their knowledge and skills in the interactive MoneySmart Teaching ‘Online shopping and banking’ practice conversation.

Enduring 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.

* Please note that this lesson plan has been aligned with the draft Economics and business curriculum. This mapping will be confirmed when the curriculum is endorsed.
**Activity 1: 'Too good to be true' video (10 minutes)**

**Task 1: Video**

Watch the MoneySmart Rookie 'Too good to be true' video. (Duration 5 minutes)

**Task 2: 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.

**Activity 2: Website security checklist (10 minutes)**

**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 Handout 1: Secure websites. 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://
Lesson plan 1: Online financial transactions

Teacher tips:
Copy Handout 1 into a PowerPoint slide and display to the class for comment.

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, using the internet, 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.

**Activity 3: Identity theft (10 minutes)**

**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 definitely 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:
Lesson plan 1: Online financial transactions

The ACMA’s Netbasics video Episode 3 at www.cybersmart.gov.au (45 seconds) which shows Neville being tempted to click on a range of suspicious offers and links. Episode 6 could also be used.

Consumer Affairs Victoria has a set of ‘Stevie’s Scam School’ videos (approximately 2 minutes each) at www.consumer.vic.gov.au 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.

**Activity 4: Scambusters (15 minutes)**

**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.
Lesson plan 1: Online financial transactions

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 http://www.scamwatch.gov.au to present ‘recent scam victim stories’ to see how sophisticated scams have become.

Activity 5: Online financial safety 101 (10 minutes)

Task 1: Online financial safety 101 worksheet

Distribute 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:

- Under 25s section of the MoneySmart website www.moneysmart.gov.au/
- Consumers section of the ACCC website www.accc.gov.au/consumers
- ACCC SCAMwatch website http://www.scamwatch.gov.au
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 Activity: ‘Online shopping and banking’ practice conversation (10 minutes)
- This activity is described in Lesson plan 2. However, it may be helpful for some students to do this activity in Lesson 1 as well — so that their participation in Lesson 2 becomes a strengthening of the development of their practical skills in this type of conversation.
Lesson plan 1: Online financial transactions

Resources
1. MoneySmart Rookie ‘Too good to be true’ video
2. Data projector/TV & DVD player or computer
3. ‘Online Shopping and banking’ practice conversation
4. Online financial safety 101 worksheet
5. Computers with internet access
6. Newspaper access
7. ASICs MoneySmart and MoneySmart Teaching websites

Additional resources
This lesson plan is part of the MoneySmart Rookie suite of resources for educators which can be accessed at: http://teaching.moneysmart.gov.au/resource-centre/moneysmart-rookie-for-educators.

Other topics include:
- Credit and debt
- First car
- First job
- Mobile phone ownership
- Moving out of home

The Under 25s section of the MoneySmart website has additional MoneySmart Rookie materials for young people including case studies, videos, tips and tools and calculators. These can be accessed at: https://www.moneysmart.gov.au/life-events-and-you/under-25s

The Australian Communications and Media Authority's (ACMA) Cybersmart program provides ‘Netbasics’ a series of videos designed to show how user's computer activities can expose them to a number of security vulnerabilities and positive steps they can take to protect their computers and data. Topics include online shopping, scams and identity theft.

Consumer Affairs Victoria has a set of 'Stevie's Scam School' videos which highlight some key consumer scams to watch out for. These can be accessed at: http://www.consumer.vic.gov.au/resources-and-education/scams/consumer-scams

The MoneySmart Teaching secondary package has a number of units of work for Year 9 and 10 students. The package can be downloaded for free at: http://teaching.moneysmart.gov.au/professional-learning/moneysmart-teaching-packages

English Year 9: Could I live smaller?
- Online transactions, consumerism, shopping online

English Year 10: Teens talk money
- Financial planning, online payments, budgeting

Mathematics Year 9: How can we obtain more money?
- Earning, managing and growing money, achieving goals, data analysis, statistics and samples.

Mathematics Year 10: Reaching goals: What's involved?
- Setting goals and planning, compound interest in a range of financial contexts; risks and rewards of borrowing money.
Worksheet 1: Online financial safety 101

NAME: ___________________________________________

Answer the following questions on the worksheet using these websites:

- Under 25s section of the MoneySmart website
- 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?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________
Handout 1 – Secure websites
Spot the difference between these websites.

![Secure website](https://www.shoppingonline.com.au)

Welcome to Online Shopping!

Start by clicking here

If you are having problems, please contact us at:
info@shoppingonline.com.au
02 9123 4567

![Non-secure website](http://www.shoppingonline.com.au)

Welcome to Online Shopping!

Start by clicking here

Congratulations you are our 1,000,000 visitor!
You have won an iPad!
Click here to claim!
Lesson plan 1: Online financial transactions

Links to the Australian Curriculum and National Consumer and Financial Literacy Framework

Australian Curriculum content

English

Understand how language use can have inclusive and exclusive social effects, and can empower or disempower people (ACELA1564) (Language/Language for interaction).

- Analyse and explain how text structures, language features and visual features of texts and the context in which texts are experienced may influence audience response (ACELT1641) (Literature/Responding to literature).

Mathematics

- Evaluate statistical reports in the media and other places by linking claims to displays, statistics and representative data (ACMSP253) (Statistics and Probability/Data representation and interpretation).

Economics and business

Year 9

- Ways of managing consumer and financial risks to individuals and the community.

Year 10

- The range of factors influencing consumer choice including marketing by financial institutions.

National Consumer and Financial Literacy student learnings

- Identify and take precautions to prevent identity theft and explain what to do if this happens to them.
- Explain the procedures for resolving consumer disputes relating to a range of goods and services.

ASIC’s MoneySmart Teaching initiative builds the consumer and financial literacy capabilities of Australian school students by developing students’ knowledge, skills, values and behaviours to enable them to make confident, informed consumer choices and responsible financial decisions that are essential to their future financial wellbeing. To view the MoneySmart Teaching Primary and Secondary packages and all the online and digital resources visit www.teaching.moneysmart.gov.au