Financial literacy – Financial scams

Levels 9 and 10,
Economics and Business,
sample activities

Authorised and published by the Victorian Curriculum and Assessment Authority
Level 7, 2 Lonsdale Street
Melbourne VIC 3000

© Victorian Curriculum and Assessment Authority 2021

No part of this publication may be reproduced except as specified under the *Copyright Act 1968* or by permission from the VCAA. Excepting third-party elements, schools may use this resource in accordance with the [VCAA educational allowance](https://www.vcaa.vic.edu.au/Footer/Pages/Copyright.aspx). For more information go to <https://www.vcaa.vic.edu.au/Footer/Pages/Copyright.aspx>.

The VCAA provides the only official, up-to-date versions of VCAA publications. Details of updates can be found on the VCAA website at [www.vcaa.vic.edu.au](https://www.vcaa.vic.edu.au/Pages/HomePage.aspx).

This publication may contain copyright material belonging to a third party. Every effort has been made to contact all copyright owners. If you believe that material in this publication is an infringement of your copyright, please email the Copyright Officer vcaa.copyright@edumail.vic.gov.au

Copyright in materials appearing at any sites linked to this document rests with the copyright owner/s of those materials, subject to the Copyright Act. The VCAA recommends you refer to copyright statements at linked sites before using such materials.

The VCAA logo is a registered trademark of the Victorian Curriculum and Assessment Authority.

|  |
| --- |
| Contact us if you need this information in an accessible format - for example, large print or audio.Telephone (03) 9032 1635 or email vcaa.media.publications@edumail.vic.gov.au |

Contents

[Introduction 1](#_Toc68789565)

[Overview of the activities 1](#_Toc68789566)

[Key terms 2](#_Toc68789567)

[Activities 3](#_Toc68789568)

[Activity 1: Understanding scams 3](#_Toc68789569)

[Activity 2: Exploring the Scamwatch website 4](#_Toc68789570)

[Activity 3: Investigating different types of scams 4](#_Toc68789571)

[Activity 4: Presentation 5](#_Toc68789572)

[Activity 5: Reporting a scam 5](#_Toc68789573)

[Assessment 5](#_Toc68789574)

**Note:** Please see the accompanying Financial Literacy – Financial Scams resources document for supporting resources that can be distributed to students.

Introduction

These sample activities address the Economics and Business curriculum area of the Victorian Curriculum F–‍10 at Levels 9 and 10.

The prevalence and impact of financial fraud on Australian consumers is increasing annually. In 2019 Australians lost more than $634 million to scams alone, according to the *Targeting scams 2019* report (Australian Competition and Consumer Commission, 2020). It is therefore vitally important that Australians become aware of the existence of financial fraud, are able to recognise a fraudulent scam quickly and know what to do in order to avoid becoming a victim.

The following activities are designed to introduce students to the concept of financial scams, fraud and identity theft, and allow them to recognise the different forms these illegal activities may take. Students will become acquainted with types of financial fraud currently operating and learn to utilise the [Scamwatch](https://www.scamwatch.gov.au/) website as a means of identifying, learning about and reporting financial fraud.

This series of activities is designed to be completed in a sequence of lessons.

Overview of the activities

Timing

Approx. 60–90 minutes total

Links to the Victorian Curriculum F–10

Relevant Economics and Business Levels 9 and 10 achievement standard extract

Students explain the importance of managing consumer and business financial risks and rewards and analyse the different strategies that may be used when making decisions.

Relevant Economics and Business Levels 9 and 10 content description

Explain why and describe how people manage financial risks and rewards in the current Australian and global financial landscape [(VCEBC023)](https://victoriancurriculum.vcaa.vic.edu.au/Curriculum/ContentDescription/VCEBC023)

Learning intentions

Students will be able to:

* understand what a scam is
* identify different types of scams
* understand the financial impact of scams
* report a scam.

Teacher resources and preparation

* The following student worksheets have been provided in the accompanying Financial Literacy – Financial Scams resources document for use during the activities:
* Worksheet A: Scamwatch web search
* Worksheet B: Scams research
* Worksheet C: Reporting a scam
* Teachers should provide students with either hardcopy worksheets or access to worksheets online.
* Students will require internet access to complete the worksheets.
* Online resources:
* [*The Little Black Book of Scams: A pocket-sized guide so you can spot, avoid, and protect yourself against scams* (Australian Competition and Consumer Commission, 2016)](https://www.accc.gov.au/system/files/1557_Little%20Black%20Book%20of%20Scams%202019_FA%20WEB.pdf)
* [*Targeting scams 2019* (Australian Competition and Consumer Commission, 2020)](https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf)
* [Identity Crime, Australian Federal Police website](https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime)
* [Scamwatch website](https://www.scamwatch.gov.au/)

Student prior knowledge and skills required

* Are able to independently use and access technology

Key terms

**Fraud:** The crime of getting money by deceiving people.

**Identity theft:** The illegal use of someone else’s personal information (such as their tax file number or driver’s licence) to obtain money or credit.

**Malware:** Harmful software that a scammer puts onto a victim’s computer. Malware may collect personal information or damage the computer or computer files.

**Phishing:** Tricking people into handing over personal information such as bank account numbers, passwords, credit card numbers and superannuation details. Phishing can occur using email, text messages or websites, or over the phone.

**Ransomware:** A type of malware that causes a computer to freeze or lock or encrypts certain files. The scammer demands a payment to have the computer unlocked or the files decrypted.

**Scam:** A dishonest scheme; a fraud or swindle.

Activities

Activity 1: Understanding scams

1. Display the following words:

* scam
* fraud
* identity theft
* phishing
* malware
* ransomware.

2. Conduct a class discussion:

* What do all of these words have in common?
* What does each word mean?

3. Display definitions of each word as follows.

**Scam:** A dishonest scheme; a fraud or swindle.

**Fraud:** The crime of getting money by deceiving people.

**Identity theft:** The illegal use of someone else’s personal information (such as their tax file number or driver’s licence) to obtain money or credit.

**Phishing:** Tricking people into handing over personal information such as bank account numbers, passwords, credit card numbers and superannuation details. Phishing can occur using email, text messages or websites, or over the phone.

**Malware:** Harmful software that a scammer puts onto a victim’s computer. Malware may collect personal information or damage the computer or computer files.

**Ransomware:** A type of malware that causes a computer to freeze or lock or encrypts certain files. The scammer demands a payment to have the computer unlocked or the files decrypted.

4. Explain to students that these learning activities will introduce them to types of financial fraud and scams they may encounter, and teach them how to recognise scams and what to do when a scam is encountered.
Emphasise that it is important that we all know how to protect ourselves against financial fraud and scams

5. Explain to students that the [Scamwatch website](https://www.scamwatch.gov.au/) will be used as a point of reference during these learning activities.

Activity 2: Exploring the Scamwatch website

Instruct students to use their computer or device to complete **Worksheet A: Scamwatch web search**, a web navigation activity based around content on the [Scamwatch website](https://www.scamwatch.gov.au/).

Activity 3: Investigating different types of scams

For this activity students will use the Scamwatch website, in particular *The Little Black Book of Scams*, and other relevant websites to investigate, compile a fact sheet about and report back on a specific type of scam.

1. Working in pairs, students are allocated one of the following types of scams to investigate and report back on:

* identity theft scams
* buying or selling scams
* dating and romance scams
* fake charities
* investment scams
* jobs and employment scams
* unexpected money scams
* unexpected winnings scams
* phishing
* online shopping scams.

2. Each pair compiles information under the following headings, as per **Worksheet B: Scams research**.

* Name of scam type
* Brief description of how the scam works
* Specific examples of this scam
* Warning signs
* Advice (how to protect yourself against being scammed)
* Other interesting observations about this type of scam

3. Each pair also investigates scam statistics for their scam type and others, as per the worksheet.

Activity 4: Presentation

1. Students develop one of the following about the scam they investigated in Activity 3:

* a fact sheet, poster, pamphlet or multimedia presentation
* an oral presentation
* a short news report.

2. Each pair presents and shares their findings with the class.

Activity 5: Reporting a scam

1. Distribute **Worksheet C: Reporting a scam**. Students work through this in pairs.

2. Discuss each type of scam as a class.

Assessment

Activities 3 and 4 may be used as summative assessment.