

## LESSON PLAN: CASE STUDY 2

**What The? – Online Scams and Identity Theft**

**Duration:** 60 mins

**Aims:**

1. Students will identify potential issues related to online scams and identity theft.
2. Students will explore a range of strategies for avoiding online scams and identity theft.
3. Students will reflect on their current online safety in relation to identity theft and online scams and plan and implement a personal online security action plan.

**Outcomes:**

On the completion of this activity students will be able to:

1. identify potential issues related to online scams and identity theft and the likely consequences.
2. complete a personal online safety audit and then develop an online security action plan.
3. apply a range of strategies for avoiding online scams and identity theft.

**Resources needed:**

- *Wise Up to IT DVD: — What the? - Online Scams and Identity Theft*
- DVD player or DVD compatible computer drive
- student handout

**Overview:**

The focus of this lesson is protecting yourself from online scams and identity theft using a 'real life' case study.

'Brian' becomes the victim of identity theft after downloading some free software, which included a spyware program. The spyware program monitored his online behaviour and included a 'keylogger', which reported all his keystrokes to scammers. The first symptoms were a slower than normal system and a bombardment of on-screen pop-ups.

The lesson also provides advice about not responding to spam, which might be 'phishing' emails (lottery scams, money transfer schemes) that seek personal details or financial information such as bank account numbers.

**Teacher note:** Use the lesson plan as a guide and adapt it to suit your class.

## LESSON PLAN: CASE STUDY 2

**Introduction:** (10 minutes)

Introduce the topic by asking the students if they know what identity theft is. Also ask them if they are familiar with the term 'phishing'.

Some questions you may wish to use are:

- Have you seen any emails or SMS messages that ask for personal details such as your name and address or bank account details?
- Can you describe what the message was?
- Have you seen any emails or SMS messages that ask you to send money to someone?
- Have you had emails claiming to be job offers or notifications that you've won the lottery?
- Have you had requests to chat with people you do not know sent to your email address?

**Viewing:** (3.22 minutes)**What the?****Debriefing:** (15 minutes)

**Teacher note:** Conduct a debriefing session with the students. Use some of the following prompts to generate discussion:

- How did Brian's problems start?
- What sort of free software have you downloaded? How can you check if the free software is legitimate?

**Teacher note:** There are many types of so-called 'free' software:

- 'Freeware' is software that can be downloaded at no charge. This type of software may have a price attached in the form of advertising or spyware – it is important to only download this software from trusted sources (e.g. large, well-known software download sites like SourceForge or Tucows). Read the licence carefully! Some freeware is offered by pop-ups—this type of software should be viewed as particularly suspect.
- Improperly licensed or pirated software (known as 'warez') appears to be free because users don't have to pay for it. Apart from the possibility of significant fines associated with the use of pirated software, it is very often infected with adware and should be considered high risk.
- Some so-called free software is licensed in such a way that enables free use of the software—in this case, free refers to freedom of use and not price. This freedom includes being able to read the source code or 'recipe' for the software. Every line of code that goes into making this software can be read so it can be checked for spyware or adware. This software is alternatively known as GPL (General Public Licence) software, free/libre software (FLOSS) or open source software (OSS).

## LESSON PLAN: CASE STUDY 2



- Identity theft—what sort of fraudulent activities can someone carry out with your personal details (e.g. name, birth date, bank account details, passwords)?

**Teacher note:** Make sure the following issues are covered:

- accessing a bank account or credit card to steal funds
- pretending to be someone else online and ordering goods without their knowledge; locking a person out of their site and sending false email or text messages.
- How can you keep personal details safe?

**Teacher note:** Make sure the following issues are covered:

- never reveal your personal details to anyone online
- when submitting information make sure it is a secure website
- don't reply to email scams
- keep your passwords private and make sure that they are not easy to guess
- store personal information such as passwords in a protected place
- cut and paste passwords rather than keying them in
- use a private setting in sites such as MySpace and Facebook
- don't install peer-to-peer (P2P) networking in the same folder that personal information is stored in, and
- install security software such as anti-virus, anti-spam, pop-up stoppers and firewalls.
- Brian complains that his virus protection doesn't work—what do you think has gone wrong here?

**Teacher note:** Malicious software disables security software preventing anti-virus software from functioning properly. Antivirus software must be kept up-to-date (it is recommended that it should be updated hourly on a broadband connection and on-connect for dial-up). Anti-virus software is like a 'flu shot—it won't protect you entirely from the 'flu, especially against a new strain, and needs to be boosted regularly.

**Activity:** (15 minutes)

### Online safety quiz

See student handout.

**Teacher note:** Ask students to complete the quiz. The quiz will help them to identify where they might need to apply strategies to protect themselves from identity theft or scams. The quiz will inform their action plan, which is the next activity.

## LESSON PLAN: CASE STUDY 2



**Activity:** (15 minutes)

**Online security action plan.**

See student handout.

**Additional resources:**

**Websites**

ACMA provides information and advice on different aspects of cybersafety.

<http://www.acma.gov.au>

Kids Help Line provides free, confidential and anonymous telephone and online counselling.

<http://www.kidshelp.com.au>

SCAMwatch is hosted by the Australian Competition and Consumer Commission.

<http://www.scamwatch.gov.au>

Anti-virus vendor sites also have excellent information on the latest viruses, trojans, phishing scams and spyware.

**Extension activity:**

**Teacher note:** *If you wish to explore issues of identity theft and scamming over more than one lesson, consider the following extension activity.*

Ask the students in groups of two or three to research one of the following:

- safe peer-to-peer file sharing
- free software—what can be downloaded and how to do it safely
- common internet scams
- identity theft and how to protect yourself
- adware/spyware programs and how to protect your computer

Students will need to research the issue, list strategies for protecting themselves/their computers and report their findings to the class. This could take the form of a brief presentation of two to three minutes, which includes a handout for the other students. The handout should refer to information sources.