



Case study: What the?—Online scams and identity theft

Theme

The internet and mobile technologies are a source of scams and identity theft.

Key learning/subject areas

Cross curricula.

Duration

One to two periods.

Objectives

On completion of this activity students will be able to:

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

The outputs will be:

- students to reflect on their current use of online and mobile technologies
- students to develop an action plan to change any risky behaviour identified
- a list of strategies for students to protect themselves/their computers from scams.



Resources/links/materials required

CyberNetrix CD-ROM

Object in the room	Activity
TV	What the?
Magazine	Buzz on identity theft
Mobile phone	Ring tone activity Glossary
Laptop	Chatting smart Chat smart information Glossary
Phone	Who're you going to call?
Stereo	Internet banking

Materials required at school

- Case study activity handout.
- Case study transcript handout.
- If desired, computers with internet access to view selected websites and video clips.

Additional resources

Websites

- ACMA provides information and advice on different aspects of cybersafety.
www.netalert.gov.au
- Kids Help Line provides free, confidential and anonymous telephone and online counselling.
www.kidshelp.com.au
- SCAMwatch is hosted by the Australian Competition and Consumer Commission.
www.scamwatch.gov.au
- Anti-virus vendor sites also have excellent information on the latest viruses, trojans, phishing scams and spyware.



Introduction

The focus of this case study is how to protect yourself from online scams and identity theft. Students can undertake this activity by reading the handout and case study transcript, or in conjunction with viewing the video on the CyberNetrix CD-ROM.

Prior learning

Students need to have knowledge of online and mobile technologies and scams. They also need to be familiar with possible responses to potentially dangerous situations when using the internet and mobile technologies.



Activity description

1. Whole class activity

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'.

As a class, students can discuss the following:

- 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?

Students can view or read 'What the?—Online scams and identity theft' case study.



Some of the following prompts can be used to generate student discussion:

Question	Possible answer
1. How did Brian's problems start?	Brian downloaded lots of online programs and games one of which had spy program hidden inside it.
2. What sort of free software have you downloaded? How can you check if the free software is legitimate?	<p>The following are three examples of 'free' software:</p> <ul style="list-style-type: none"> • 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 popups—this type of software should be viewed as particularly suspect. • Warez is improperly licensed or pirated software which 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).

continued...



Question	Possible answer
<p>3. Identify theft—what sort of fraudulent activities can someone carry out with your personal details (e.g. name, birth date, bank account details, passwords)?</p>	<ul style="list-style-type: none"> • 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 emails or text messages.
<p>4. How can you keep personal details safe?</p>	<ul style="list-style-type: none"> • 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 passwords private and make sure 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 in which personal information is stored. • Install security software such as anti-virus, anti-spam, popup stoppers and firewalls.
<p>5. Brian complains that his virus protection doesn't work. What do you think has gone wrong?</p>	<ul style="list-style-type: none"> • Malicious software disables security software preventing anti-virus software from functioning properly. Anti-virus software must be kept up-to-date. It is recommended that it should be updated hourly on a broadband connection and on-connection for dial-up. Anti-virus software is like a flu shot—it won't protect you entirely from the flu, especially a new strain, and needs to be boosted regularly.



2. Individual activity

Students complete the online safety 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.

3. Individual activity

Students develop an action plan on how they can change their risky online behaviour.

Extension activity

1. Small group/whole class activity

Students form groups of two or three to research one of the following:

- safe peer-to-peer (P2P) 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 – three minutes, which includes a handout for the other students. The handout should refer to information sources.



Teacher notes

This lesson provides advice about not responding to spam, which might be ‘phishing’ emails including lottery scams and money transfer schemes that seek personal details or financial information such as bank account numbers.

It might be useful to contact the school’s welfare coordinator before beginning the activity if you believe the case study is too close to home for some students. After the class has reviewed the case study, you may choose to debrief them and discuss who they can contact if they feel concerned, threatened or exploited.



Handout

Case study: What the?—Online scams and identity theft

Online safety quiz:

Find out how safe you and your computer really are by doing this quiz. Circle the answers that best describe what you do online. You may find in some sections that you will want to circle more than one answer—that's okay, but only select the ones that best apply to you. Be honest!

At the end of the quiz, add up your total score and see what your personal security profile is.

Email	Scores	Your score
A. I read every email I get, even if it's not addressed to me.	A=4	
B. Whenever I get mail that I don't want, I try to unsubscribe. If I can't, I send an email telling the sender to take me off their list.	B=5	
C. I only read emails addressed to me.	C=1	
D. I only ever read emails addressed to me from people I know.	D=0	
Total score		

Email attachments	Scores	Your score
A. I like getting funny email attachments and I always check them out.	A = 5	
B. I only open email attachments addressed to me from people I know.	B = 1	
C. I never open email attachments, unless I know exactly what they are.	C = 0	
Total score		



P2P	Scores	Your score
A. I use P2P to download software.	A = 5	
B. I use P2P to download movies/music.	B = 4	
C. I only use P2P to download software/movies/music from trusted sites that have links to their own content.	C = 0	
D. I have adjusted my router settings to make P2P run faster.	D = 1	
Total score		

Web surfing	Scores	Your score
A. I like to surf around following links to other sites.	A = 3	
B. I use a search engine to find what I'm looking for.	B = 0	
C. I like to download software from the internet.	C = 3	
D. I like to go to sites where I can download movies, MP3s and software.	D = 5	
E. I only go to sites I know and trust.	E = 0	
F. I like to enter competitions on the web.	F = 3	
G. I never read the privacy policy or terms and conditions on websites.	G = 1	
H. When I get pop-ups I like to check out the sites in the popup.	H = 5	
Total score		



Internet banking/shopping	Scores	Your score
A. I use the same password for my internet banking that I do for most other online activities.	A = 5	
B. My internet banking password is a real word.	B = 5	
C. My internet banking password has only letters in it.	C = 4	
D. I shop online using a credit card.	D = 3	
E. I shop online using a debit card.	E = 2	
F. I only shop online with businesses I know have retail stores.	F = 0	
G. I use eBay.	G = 1	
H. I don't pay much attention to eBay seller feedback.	H = 4	
I. I shop online at overseas businesses.	I = 3	
J. I buy things from offers in emails.	J = 5	
K. I update my bank account when emails are sent to me.	K = 5	
Total score		

Personal security profile:

If you scored more than 16

High risk! You are placing yourself at high risk of having your personal identity stolen or being scammed. Think about changing your online behaviour to better protect yourself and your computer.

A score of 6 to 15

Average effort. You need to change some of your online behaviour. Look back at the quiz and work out where you need to make changes.

A score of 0 to 5

Good effort! You are doing everything right—or at least nearly everything. Check to see where you have scored higher than 2 and work on changing that behaviour.



Handout

Case study: What the?—Online scams and identity theft

Security action plan

Look at your quiz results. Select one of your answers with a score of 3 or above. Copy it into the table below and decide how you are going to deal with the issue. If you are in the high risk category you might need to think about several of your answers.

Activity	Issue	Action
<i>Example</i>	<i>I use P2P to download movies/music</i>	<i>I will find out about trusted P2P files</i>
Email and email attachments		
P2P		
Web surfing		
Internet banking/shopping		



Handout

Case study: What the?—Online scams and identity theft

Transcript

'Well, I downloaded a lot of stuff to my computer—heaps of stuff actually: music, programs, games. I guess in the back of my mind I've always been worried about security but I didn't think I could do anything about it, or anything that bad could happen to me. I guess when you're connected and doing frequent downloads you never know what's coming down your phone line.

One day I downloaded this particular program, and after that my computer seemed to be a lot slower. It was taking forever for pages to load and even normal things like writing an email or writing a Word document would take a long time. I didn't think too much of it 'cos my computer was getting pretty old and I had heaps of stuff on it. But then my home page got changed to some free download site and when I checked my internet settings I found that they'd all been changed. But things kept on getting worse. Whenever I went online to the internet I got bombarded with pop-ups and, like, my computer would just crash and I would have to manually reset it.

Then things got really serious. I couldn't log-in to my email account and I discovered that someone was using my internet banking. I had anti-virus software installed onto my computer but it just wasn't picking up anything.

What I didn't realise at the time was that when I'd downloaded this free program a couple of months ago, a smaller program downloaded and installed itself onto my computer. But, I had no idea.

This spyware program monitored all my internet activity and the keylogger recorded all the keystrokes I made on the computer such as my log-in, my passwords and all the emails I sent to my mates. It then sent all this information to the software developer.

I ended up taking my machine to a computer specialist who was able to find and remove all the spyware. I had to contact my bank and my ISP to change my account details.

You know, even free stuff comes at a cost nowadays and I know it sounds corny, but if it's too good to be true then it probably is. Before I download anything now I make sure there's no adware or spyware associated with it and I read the user agreement statement. There are websites online that, sort of, help you out with this and can offer great reviews and advice on the program and company that you're downloading from.

If it's free, there's usually a catch. I guess I learnt the hard way.'