SENIORS ONLINE SECURITY

Identity Crime

2 of 5 training guides available

PCYC
Carindale PCYC
Improving Communities Through Youth Development

WA POLICE

Government of Western Australia
Department of Commerce
Consumer Protection

An Australian Government Initiative

Identity crime
A training guide for seniors

#2 out of 5 training guides available

This training guide provides Australian Seniors with information about identity crime as well as simple strategies to better protect their personal information.

Meet Beryl and Alan

© Carindale Police Citizens Youth Club 2014 (2nd edition)

This training booklet is licensed by the Carindale Police Citizens Youth Club under a Creative Commons Attribution-NonCommercial (CC BY NC) 3.0 Australia Licence.

In essence, you are free to copy, communicate and adapt this training booklet, as long as you attribute the work to the Carindale Police Citizens Youth Club and do not gain any commercial profit.

To view a copy of this licence, visit
http://creativecommons.org/licenses/by-nc/3.0/

Author: Dr Cassandra Cross
Graphic Design: Nejien Creative
Beryl and Alan characters: Kitsch Design and Illustration

The Carindale Police Citizens Youth Club gratefully acknowledges the funding received from the Australian Government to develop the Seniors Online Security training package.

To Dr Cassandra Cross (Cass),

On behalf of the Carindale PCYC and the Australian community, thank you sincerely for your vision and leadership in developing the SOS project. I know firsthand the enormous time and effort that you have put into developing this great training package. I am very confident that because of your efforts and tireless commitment, our community and in particular, our beloved seniors citizens, will benefit greatly from what you have developed. Congratulations on a job well done.

Sergeant David Beard
Manager, Carindale PCYC

cc BY NC

Table of Contents

Introduction

The development of the internet has had a huge impact on our everyday lives. The way we do things such as communicate, do business, find out information and shop, has all changed. People are using the internet for an increasing number of things. This has great benefits in terms of the ease at which we can now do things online, anywhere at anytime. One of the consequences of the increased popularity of the internet is the vast amount of personal information that is stored in cyberspace. The internet has allowed society to store and transfer large amounts of information with ease and with speed.

While there are many benefits of being able to store and transmit information through the internet, there are also consequences. The ability to communicate through the internet as well as store large amounts of information on it means that as individuals, we conduct a large part of our lives online and store sizeable portions of our lives in cyberspace. Personal and private details about ourselves are now posted on social networking profiles for the whole world to see. Conversations which used to happen over the telephone or in person now occur in chatrooms or are posted on a person's profile. We are increasingly publicising aspects of our lives and our relationships. However, we may not always do this deliberately. We may think that our details are private and protected, but this is not necessarily the case.

One negative consequence of this increasing level of openness is identity crime. There are people who use the internet to seek personal details about others to gain unauthorised access to their accounts or use their identity. Identity crime is one of the fastest growing crimes in Australia and is the most frequent crime type reported in the United States of America. It is also unlikely that identity crime will decrease anytime in the future, as society continues to communicate and conduct business in the virtual world.

There are many simple steps which can be taken to reduce the likelihood that another person can use your identity. This module will help you learn how to better protect your identity when using the internet.

Overview of this module

This module looks at identity crime. The purpose of this module is to give you an understanding of how you can protect your identity. By the end of this module, you will be able to:

- Understand what is meant by identity crime;
- Name the different types of identity crime;
- Understand the public nature of the internet;
- Understand the different ways a person's identity can be stolen;
- Know what strategies will help protect your identity; and
- Know who to contact if you think you have become a victim.

This module will help you understand the ways that a person's identity can be easily pieced together. It will also help you to take steps to reduce the chances that you find yourself a victim of identity crime. The internet has great benefits in terms of sharing information, and there are many ways in which you can do this safely.

What is identity crime?

A person's identity is unique to the individual. There is no universal definition of identity crime. Sometimes, it is used interchangeably with other terms such as identity theft and identity fraud. While they all have similar characteristics, they can be defined as follows:

> **Identity crime** is a generic term to describe crimes which are committed through the use of a stolen or false identity.

> **Identity fraud** refers to when a person obtains money, goods, services or other benefits by using a false identity. This can be through the use of a completely made up identity or through the use of an existing identity. A common type of identity fraud is the misuse of a person's credit card details.

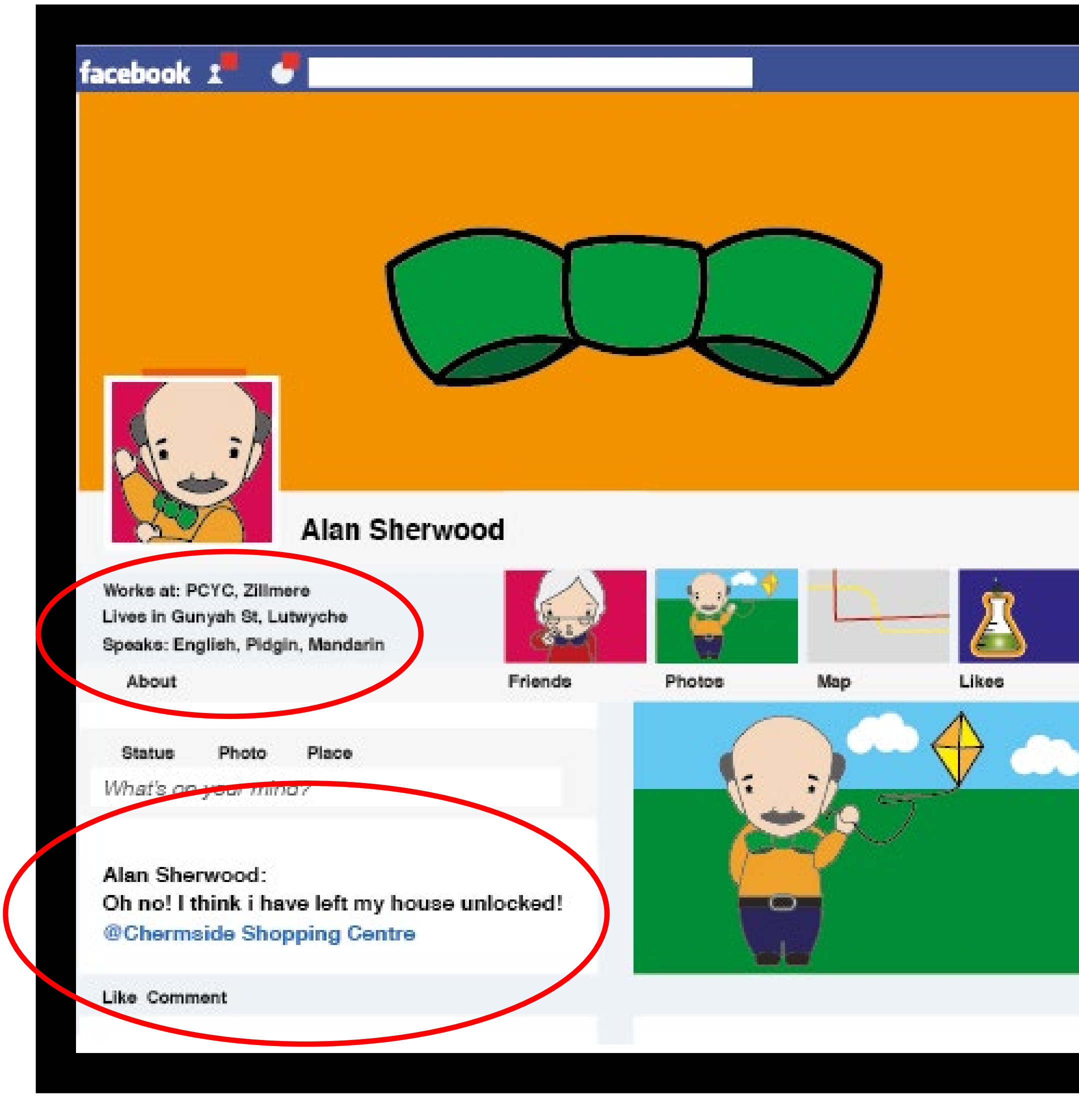
> **Identity theft** refers to when a person steals another's person's details or information in order to gain money, goods, services or other benefits. It includes the unauthorised use of a person's identity, living or dead. One of the most common consequences of identity theft is the loss of money from a victim's bank account or the establishment of new accounts.

Identity crime is the term which refers to any act that falsely uses a person's identity without their consent. Identity fraud and identity theft are specific ways of committing these types of crimes. Identity crime can have devastating effects on its victims. In many cases, people don't realise they have become victims of identity crime until they are rejected for a loan, or receive a bill in the mail for something they haven't purchased. The following section looks at some of the ways in which you can lose control over your identity.

Losing control of your identity

POSTING TOO MUCH INFORMATION ON THE INTERNET

One of the biggest threats to the security of our identity is not about others, but about our own need to post so much information on the internet. Many people have multiple profiles across a number of social networking sites and they might also have accounts with a number of other websites which store and display personal information.



Works at: PCYC, Zillmere
Lives in Gunyah St, Lutwyche
Speaks: English, Pidgin, Mandarin

Alan Sherwood:
Oh no! I think i have left my house unlocked!
@Chermside Shopping Centre

It is easy to forget that the internet is not private. It is easy to think that the information we post on the internet is only being read and accessed by those we know and trust. However this is not the case. No matter how private you think the internet is, once you put information about yourself on the internet, there is no guarantee that it will only be seen by those you select. Once you put something on the internet, you have lost control over it. You cannot possibly know all the people who have read it, downloaded it or forwarded it onto another person.

A lot of people put a lot of information on the internet. They have profiles which tell people every possible fact about themselves. They post every thought they have and tell people everything that is happening in their day, every place they intend to go and when they will be there. For example, a growing number of people are interested in tracing their family trees. There are websites established where you can search for members of your family as well as posting details of your own family. Without the proper security settings, it is very easy to view another person's family tree. Think about what is one of the most common security questions: what is your mother's maiden name? It is very easy in this instance to be able to answer that question with minimal effort. In relation to security questions, it is important to try and have unusual questions on topics which aren't plastered all over your social profiles. There is no point having your pet's name as a security question, if you have dozens of photos of your dog Rover on your profile. It may seem trivial, but it is important to think carefully about the amount of information and the type of information you post online, as well as the potential consequences it might have.

Others can take advantage of the high level of openness that we have on the internet. We might think that we are only communicating with a small group of our family and friends, when in reality we are broadcasting our personal details to the entire world. We might think that nobody really cares about our personal details, but there are people out there who can take all of our personal details and use them for their own benefit and we won't know it until it is too late.

FRAUDULENT EMAILS

Similar to social networking sites, fraudulent emails can be used to commit identity crime. The types of fraudulent emails that can appear in your inbox asking for personal information are infinite. These are called "phishing" emails. It might look strange, but the concept is simple. Much like the word "fishing", these emails will ask you to send through personal information and account details. The purpose of a phishing email is to "fish" for your details. The email is the bait and the other person sits back and waits for a "bite", in that they wait for someone to respond and provide them with the personal details they are after.

Phishing emails may look legitimate. They might have the company logo and all the information you would expect from that company. They might appear to come from your bank or financial institution. They might claim that there has been a problem with your account, and that your account has been suspended and you currently have no access to your money. They might claim that they have lost your details and need you to reconfirm them. It doesn't matter what story is used, the end result is always the same. **They want you to provide your personal details to them.**

Phishing emails will try to get your personal details in one of two ways. The first is to ask you to reply to the email you received. In these instances, the email will ask you to type things like your name, your username and your password. By sending these details, you are giving another person free access to your internet banking accounts, and they are likely to take all the money from your account/s.

The second way that another person will try to get your details is to include a link in the email, and ask you to click on this link. If you click on this link, it is likely to take you to a website which appears to be the home page of your bank or financial institution. As with the emails, these websites will look genuine and will use the company logo and similar formatting to the legitimate site. However, the website may be fake and is designed to steal your account login details. The website is likely to prompt you to enter a range of personal details, such as name, address birth date, mother's maiden name, account number, username and password. Once you have entered this data into the site, another person can then log into your account and access your money and accounts. In addition, with the level of information provided (such as name, mother's maiden name etc), they are likely to try and get new lines of credit or loans in your name.

There are other types of fraudulent emails which will also try to get your personal details. These may come in the form of job opportunities, lottery notifications, or inheritance notifications. There are literally thousands of other possible scenarios such as these, which try to trick you into giving over personal information.

MALWARE

Malware is a shortened term for "malicious software". It is designed to do any number of things to your computer, such as disrupt its use, disable your programs or anti-virus software, gain access to your files, or gather information from your computer. It is not always easy to detect malware and sometimes you might not even know it is on your computer.

Some types of malware are specifically designed to gather personal information such as account login details. For example, spyware is a type of malware which is installed on a person's computer without their knowledge and collects information about their computer usage, including internet banking habits, usernames and passwords, and sends this information to another computer. Your banking details can then be used by another person to log into your bank account.

Revision questions

With people increasingly storing and displaying personal details on the internet, it is no surprise that others are taking advantage of this to use a person's identity without permission. The posting of too much information on the internet, fraudulent emails and malware are all ways in which a person can lose control over their identity.

Before we look at ways to protect yourself from becoming a victim of identity crime, the following questions are designed to test how well you understand the threats to your identity. Each question has multiple options but there is only **one** correct answer. Answers to these questions can be found at the back of this booklet.

Question 1

What is identity crime?

a) Crimes committed by famous people
b) Crimes committed through the use of a stolen of false identity
c) Crimes committed by people in costumes
d) Crimes committed by animals

Question 2

When will a person know they have been a victim of identity crime?

a) The day that it happens
b) The day that the criminal calls to tell them
c) They may never find out until they receive unknown bills or accounts
d) On their birthday

Question 3

What type of personal information is safe to put on the internet?

a) Name and birth date
b) Bank account details
c) Mother's maiden name
d) None of the above

Question 4

What is malware?

a) A type of illness
b) A type of malicious software
c) A new computer game
d) A computer accessory

Question 5

If you receive an email from your bank asking for personal information what should you do?

a) Delete the email
b) Reply to the email to tell them you won’t respond
c) Reply to the email with all of your personal details
d) Print the email and decorate your walls with it

Question 6

What is a common type of identity fraud?

a) Stealing your car
b) Breaking into your house
c) Stealing of credit card details for unauthorised purchases
d) Driving over the speed limit

Question 7

To secure your personal details, what should you do?

a) Use strong passwords
b) Don’t put answers to security questions on the internet
c) Limit the amount of information you post on the internet
d) All of the above

How to protect your identity

The first part of this booklet has outlined some of the ways in which a person can lose control of their identity. The internet is a great communication tool and there are many simple steps that you can take to protect yourself and your identity. These are outlined in the following section.

LIMIT THE AMOUNT OF INFORMATION YOU PUT ON THE INTERNET

It is very important to think about the level and type of information that you post on the internet about yourself. If you are creating yourself a profile on the internet (for example, on a social networking site), think about what information people really need to know. If you met a stranger in the street, would you tell them everything about yourself in the first few minutes of conversation? In the same way, you should think through what details you want to put on your profile. Only you can control the amount of information you post on the internet about yourself.

It is also important to think about the type of information that you put on your profiles. Think about the security questions that you have with your bank and other agencies. If the answers to all of these questions are easily discovered on your profile page, then your accounts are not very secure.

In the same way that you should limit the amount of information you put on the internet about yourself, you should also think about the level of information you put up about other people, including family and friends. They might not like the fact that you keep putting up photos of them on your profile. If you are not sure, ask the person before putting pictures of them on the internet or writing details about them. If you wouldn't like someone to do it to you, then it is likely that they will feel the same. If someone else is posting information about you on the internet that you are not comfortable with, don't be afraid to ask them to remove it. Tell your family and friends that you don't want excessive information posted about yourself on the internet and ask them to respect this.

By limiting the amount of information you put on the internet, you are reducing the likelihood that a stranger can take your identity. By limiting the amount of information you post about other people and asking them to do the same, you are also reducing the chances that other identities can be stolen. By thinking through the type of information that you post on the internet, you are reducing the likelihood that your accounts can be compromised. It is important to remember that the internet isn't as private as you might think. However, by taking just a few moments to think through what you post about yourself and your contacts, you can protect yourself.

NEVER REPLY TO AN EMAIL WITH PERSONAL DETAILS

If you receive an email asking for personal details, it is very likely to be fraudulent. You should never have to send your personal details over email to any person or company. It may seem harmless to send information about you to a person, but it is the same as sending money to a stranger. Personal details are very valuable and other people will try and trick you into giving personal information so that they can use your identity.

If the email is from a person or a company that you do business with, and they are asking you for personal details, don't be afraid to give them a call. Ring the person or the company and tell them you have just received an email from them. However, don't call them on any numbers which are contained in the email you have received. Use a number you already have or look it up in the phone book. Ask them if they sent the email and if they really need those details. In most circumstances, they will tell you that they haven't sent the email, and it is fraudulent. If they did send you the email, then you can be satisfied that it is true, and it is up to you whether you provide what they want. It is much better to make a phone call before sending through any personal details, than it is to reply to the email and discover it is not true.

It doesn't matter what an email looks like, or the reason why the email says it needs your personal details. There are many different ways that other people will try to get your personal details and they are always coming up with new ways of approaching people. **The important**

thing to remember is that no one should send you an email asking for personal details. If an email asks for this, you have a right to be suspicious. You have the right to delete the email, and if unsure, you have the right to call the person or company to find out if it is true. Don't think that you have to reply just because the email was sent to you. The security of your personal details is paramount, so you have every right to protect this from being compromised.

KNOWING AND USING SECURITY SETTINGS

With most of your online accounts and profiles, there should be the option to use security settings. Security settings can be a great way to protect you personal details from unwanted attention and potential risks. However these settings are only good if you use them properly.

You should never rely on the default option that a site provides when you first sign up. This is usually not very strict and will not limit the number of people who can view your profile. Instead, you should set your security settings to make sure that only the people you want to view your information can do this. If you want to restrict your profile to known contacts, then do this. If you want your profile to be viewed by a wider group of people, then do this. You may be able to limit the types of people who can view certain parts of your profile. For example, only contacts can view your entire profile, but anyone can view your username and profile picture. You need to experiment with the settings available until you get to a point where you are comfortable. Also don't be afraid to change them, if you find you are not happy with the way they are working out. By restricting the number of people who can view your personal details, you are reducing the chances that a stranger will view your profile and try to take over your identity.

USING STRONG PASSWORDS

As with all accounts, you should use a strong password. This should not be easily guessed by another person. You should avoid using your name, your birth date and other significant names or dates. You should also avoid using something which is easily accessible from information on your profile. Although it is difficult to remember so many different usernames and passwords, try not to have the same password across all of your accounts, and never write these passwords down on a piece of paper next to your computer. The password should contain at least eight letters and numbers and include one symbol (such as !@#$%)

You should also think about the security questions that you have to retrieve your password on accounts. Try to avoid having the standard questions. These can be quite easy to guess from information about you that is available on the internet. Try to make up your own questions where the answers are not readily available on your profile.

Just as you would use a good quality lock on your front door to secure your house, you should use a strong password and strong security questions to protect your accounts and profiles. It is the only thing that guards your personal details from being accessed by other people and an important way to protect yourself from identity crime.

THE IMPORTANCE OF ANTI-VIRUS SOFTWARE AND AN ACTIVE FIREWALL

It is essential that your home computer has anti-virus software installed. It is even more important to make sure that this is updated on a regular (such as daily) basis. Anti-virus software can be installed on your computer and is used to protect it from unwanted malware. It will scan your computer on a regular basis to make sure that there is no malware detected. It will alert you if malware is present and will give you the ability to remove it.

It is advisable to have only one good anti-virus program on your computer. There are free anti-virus programs available. Some people think that installing more than one anti-virus program will increase the security of the computer. However, this is not the case. More than one program is likely to make your computer run very slowly. In some cases, one anti-virus program will detect another anti-virus program as malware and try to remove it. One good anti-virus program is sufficient.

It is also essential that you update your anti-virus program so that it stays up to date with the latest threats to your computer. If you can, set up your program to conduct automatic updates, so that you don't have to remember to do it. This will ensure that you always have the best and latest protection.

A firewall is a program which prevents unauthorised access to your computer and also stops programs on your computer talking to other computers on the internet without your permission.

While anti-virus software and firewalls are not perfect, it is really important to have them both on your computer. Although they cannot guarantee that you will never get malware on your computer, it will reduce the chances of this happening. If you are not sure about what anti-virus software or firewall to install on your computer or how to do it, contact your local IT professional who can advise you on what is best for you.

AVOID USING PUBLIC COMPUTERS

At home, you know how secure your computer is. You know what anti-virus you have installed and when it was last updated. You also know who has been using your computer and what they have been doing on it. If you use a public computer, such as one in an internet café, then you don't have that same level of information. You cannot assume that public computers have the same level of security as your own computer and that they are maintained to your same standards. You have no control over whether they have been updated recently with anti-virus protection or whether or not they have malware installed.

Public computers are useful when travelling and you don't have your own computer with you. However, criminals target public computers as they are not maintained as well as personal computers. With so many people using them, it is hard to track what people have been doing on them, what websites they have visited or what attachments they have opened. Public computers are much more likely to have malware installed. If you use a public computer for important business, you are at a greater risk of compromising your details, through malware being installed on the computer without your knowledge.

CAREFULLY SELECT THE WEBSITES YOU USE

This is particularly important if you decide to sign up for something or use the internet for shopping. Only use reputable sites which offer some degree of security on them. When shopping online, a bargain might not turn out to be so great if your credit card details are compromised and used to purchase unauthorised goods. Be careful about the sites that you sign up to and the level of personal information you provide. Also look for the privacy policies of the accounts and websites that you sign up for. Does the company have a policy on how they will store your information or a policy about selling your details to third parties? Just remember, once you have given over your personal details, you have lost control over them, so it is important that you consider the consequences before doing this.

MONITOR YOUR ACCOUNTS AND STATEMENTS

It is important to regularly monitor your accounts and statements. It is very easy every month to only look at the amount payable and not look at the entire bill. It is also easy when you receive statements, to just file them away without looking at them. It is important that you take the time to read through all of your bills and statements. In doing this, you give yourself the chance to identify any irregularities with your account sooner rather than later. If your account has been compromised, the sooner you realise it, the more effective any action is likely to be. It is hard to track things down months after they have occurred. Don't be afraid to question something that you are unsure of. By checking all of your bills and statements and keeping an awareness of your financial position, you are more likely to pick up any problems within a short time.

DESTROY YOUR PERSONAL INFORMATION APPROPRIATELY

One of the simplest ways to protect your identity has nothing to do with your computer. It is about the paperwork that you have around lying around the house. It is vital that you keep important documents in a secure place in your house. Security is even more important when destroying documents with your personal details on them.

You should always shred them before you put them in the rubbish. Never throw out any document with any of your personal details on it, without first shredding it. Otherwise, it is very easy for another person to go through your rubbish and piece together your identity. If you throw out a bank statement or a credit card bill, you are giving out your name, address, account number, and other details about your finances. This makes it very simple for another person to access the account on your behalf or open a new account. Shredding your documents is so simple, but can be very effective in protecting yourself from identity crime.

What to do if you think you have been a victim of fraud

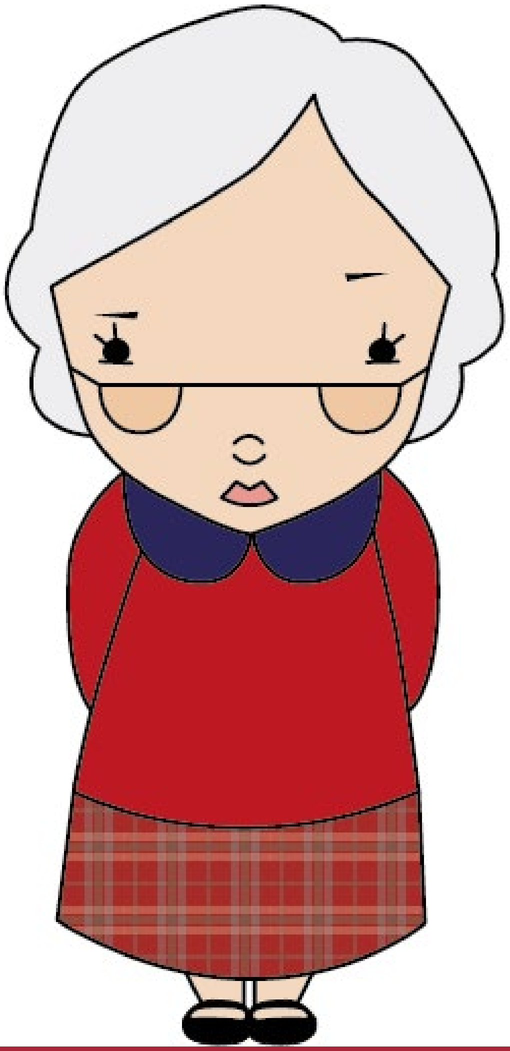
IF YOU HAVE SENT PERSONAL DETAILS...

If you have responded to a phishing email which asked you for personal details, there are a few things you should do straight away. Depending on the type of information you sent, will determine what you need to do.

If you have sent information about your bank accounts, then you should contact your bank immediately. Tell them what has happened and they will be able to change your passwords and close the accounts if necessary. They will also be able to reissue new credit cards to you, if necessary. In addition, banks can put a note on your account in case there is any suspicious activity in the future. If there has been unauthorised activity on your account, you can then talk to the bank to resolve the matter.

If you have sent information about another type of account (such as telephone or internet or a payment service) then you should contact them immediately. As with the bank, tell them what has happened and they can help you change passwords and close accounts if necessary. They can also put a note on your account for future reference. If there has been unauthorised activity on your account, as with the bank, you can talk to the company to resolve the issue.

If you have sent personal details, such as name, address, birth date and phone number, unfortunately there is not much you can do. If you have sent information such as your mother's maiden name or other answers to possible security questions, then you might want to consider changing these as soon as possible.



IF YOU HAVE NOTICED SUSPICIOUS/ UNAUTHORISED ACTIVITY ON YOUR ACCOUNT

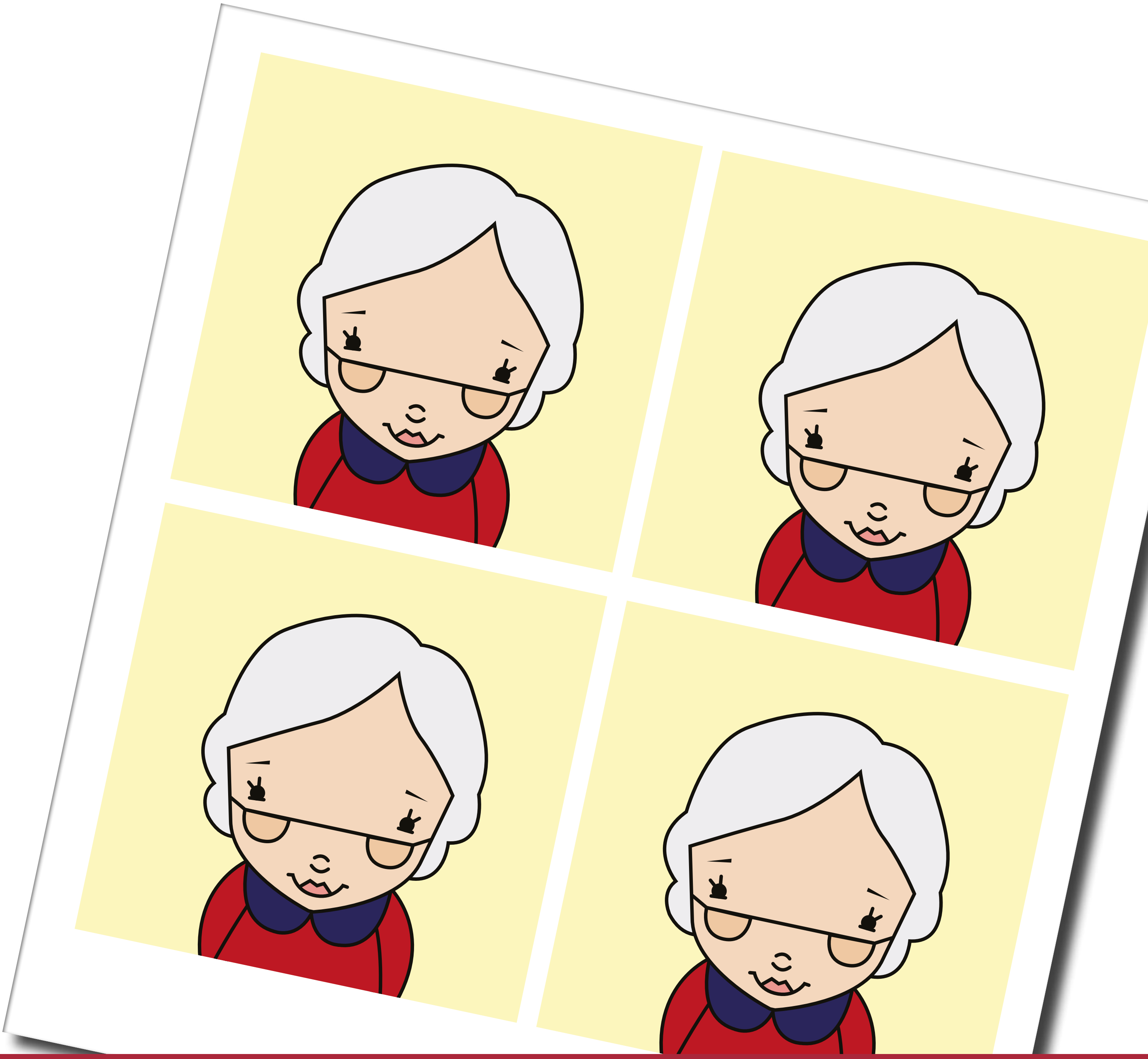
If you have noticed any unusual or suspicious transactions in your accounts or on your credit card statements, contact your bank or financial institution immediately. They will be able to help you determine if they are legitimate or not. If you discover that your account details or credit card has been compromised, you need to contact your bank straight away so that they can close your accounts and cancel your credit cards. The sooner you are able to do this, the sooner you are able to limit any losses to your account. You will then need to discuss with your bank or financial institution about any losses. They may or may not reimburse you for your losses, depending on the way the details were compromised and their own policies. Sometimes you may not ever know how your details were compromised.

IF YOU RECEIVE BILLS OR STATEMENTS WHICH ARE NOT YOURS

In many instances, the first time a person realises they have become a victim of identity crime is when they receive a bill or statement in the mail for an account or purchase they don’t recognise. If this occurs, contact the company to find out further details about the statement or purchase. Establish if it really is unauthorised and if this is the case, explain your situation to the company. At this point, you should contact the police to report the crime. You should also contact your bank to make sure that there has been no other unauthorised activity on your accounts. It would also be beneficial to obtain a credit report. This will give you a summary of all credit and loans which are in your name and may alert you to other accounts or loans which you have no knowledge about.

Conclusion

The internet has opened up many opportunities for sharing and storing personal data. However, this has also seen an increase in the theft of personal data by other people to commit various forms of identity crime. There are many ways you can lose control over your identity, such as the posting of too much information on the internet, responding to fraudulent emails and downloading malware. However, there are a number of simple steps you can take, which will dramatically reduce the chances of becoming a victim of identity crime. While there is no guarantee this won't occur, this booklet has outlined several strategies which are easy to put into practice and can help protect the security of your identity.



Revision scenario

Beryl loves her computer. Although she has been using it for years, she is continually surprised by the way that the technology has made her life easier. Beryl uses internet banking to pay all of her bills, she uses many social networking sites to meet new people, she uses a genealogy website to research her family history and she uses email to keep in touch with her family and friends. She can't remember what life used to be like before her computer.

One day Beryl receives an email from her friend, Annie. She hasn't heard from Annie in a while and knows that she has been travelling overseas with her husband. She opens the email and is a bit surprised not to find much in the email. There is no actual message, instead there is just an attachment, with a sentence saying, "check out this photo". Beryl assumes that Annie has sent her a photo of her trip and opens the attachment. The photo isn't of Annie and Beryl can't really make out what is in the photo. She thinks it is very strange and replies to Annie to find out what the photo is.

1) How have Beryl's actions compromised the security of her computer? Is there anything suspicious about the email from Annie?

Over the next few days, Beryl forgets about the email from Annie and continues with business. She pays her credit card and telephone bills. She continually checks her emails. She has a few spare hours and browses the genealogy website to find out more about her family.

A few weeks later, when Beryl gets her bank statement, she is horrified to see that her account is missing thousands of dollars. She immediately rings the bank, who confirm that her account is low, based on the recent transfers she has been making. She also learns that her credit cards have had their limit extended and have made several large purchases.

2) What do you think has happened to Beryl? What actions should she take to prevent further damage?

Having sorted out all of her bank dramas, Beryl continues business as usual. A few months later, she receives a letter from a debt collection agency, stating that she is behind on her car loan repayments and that unless she pays immediately, the car will be repossessed. Beryl is puzzled by this, as she has not bought a new car in over a decade.

3) How do you think this has happened to Beryl? What action should she take to prevent further damage?

Answers to Revision Questions

Question 1

What is identity crime?

b) Crimes committed through the use of a stolen or false identity

Identity crime is a generic term for crimes committed through the use of a stolen or false identity. It can come in many forms, such as stealing your credit card details, or by using your information to open new credit cards and loan accounts.

Question 2

When will a person know they have been a victim of identity crime?

c) They may never find out until they receive unknown bills or accounts

A person may not know straight away that they have become a victim of identity crime. Often, it is not until they notice strange activity on their bank account or receive a bill or statement to an unknown account that they start to ask questions. If you think your identity has been compromised, it may be worthwhile purchasing a credit report. This will summarise all the loans and credit cards taken out in your name. If you do not believe it to be accurate, you can then contact the agency involved as well as the police to record what has happened.

Question 3

What type of personal information is safe to post on the internet?

d) None of the above

You should think very carefully about what type of personal information you post on the internet. While you may think that it is harmless, you may be giving another person what they need to use your identity without your permission. Personal details are as valuable as money and should be protected in the same way.

Question 4

What is malware?

b) A type of malicious software

Malware is a type of malicious software which can infect your computer. There are many types of malware which have different purposes, from doing damage to your computer, spreading to other computers and stealing information from your computer. The severity of impact from malware can be anything from just annoying to severely damaging your files and computer system.

Question 5

If you receive an email from your bank asking for personal information what should you do?

a) Delete the email

No bank should ever send you an email asking you to reply with personal details, such as your username and password. If you receive an email asking for this, it is very likely to be fraudulent. You should not respond in any way. You should just delete the email and not think about it again.

Question 6

What is a common type of identity fraud?

c) Stealing of credit card details for unauthorised purchases

There are many types of identity fraud, however the stealing of a person's credit card details is one of the most popular. Stolen credit card details are then used to purchase goods and spend up to the credit limit of each card.

Question 7

To secure your personal details, what should you do?

d) All of the above

Your personal details are as valuable as the money you have in your bank accounts and you should take steps to protect these from being accessed by other people. You should use strong passwords on all of your accounts. Avoid using the same password for all accounts and try to make it something that is not easily guessed by others. When throwing out documents with your details on them, you should always shred these before putting them in the bin. You should also think about the amount and type of information you post about yourself on the internet. These steps will reduce the chances that you lose control of your identity.

Answers to revision scenario

1) How have Beryl's actions compromised the security of her computer? Is there anything suspicious about the email from Annie?

It is very likely that Beryl has downloaded some type of malware onto her computer, by opening the attachment in Annie's email. With Annie being overseas on holidays, it is likely that Annie is using public computers to email her family and friends. Public computers are more likely than personal computers to have malware installed on them, and it is likely that the computer Annie used has malware on it. It is likely that all of the contacts in Annie's email account received the same email that Beryl did. The attached photo is likely to be another type of malware, which when Beryl opened the file, has installed on her computer. Although the email came from someone that Beryl knew, she still has to be careful when opening attachments to emails, particularly when the email itself was out of character and instead of giving details about the holiday, just had a sentence asking recipients to open the attachment.

2) What do you think has happened to Beryl? What actions should she take to prevent further damage?

It is very likely that when Beryl opened the photo attachment to Annie's email, she downloaded malware onto her computer, probably in the form of spyware or a keylogger. This has enabled a third person to know what websites Beryl visits, her usernames and her passwords to her accounts, including her online banking. With this information, another person has been able to access Beryl's bank accounts and transfer the money out. They have also been able to increase the credit limit on her credit card and use this to obtain fraudulent purchases.

Beryl needs to talk to her bank about what has happened. She needs to immediately cancel her credit cards and discuss with the bank any options to recover her lost funds. She then needs to reduce the limit on her credit card back to its original amount and discuss options to recover the fraudulent transactions.

Beryl should also make sure that her anti-virus software is running and up to date. She should scan her computer to find the malware and remove it. If she cannot do this herself, she needs to contact a local IT professional to do this for her.

Beryl should also consider contacting all other agencies that she does business with. It is likely that if her bank accounts have been compromised, that other accounts could have been compromised as well. She should change the passwords and security questions to her accounts to make sure that no one is able to further access her accounts without her authorisation.

3) How do you think this has happened to Beryl? What action should she take to prevent further damage?

It is likely that when Beryl's bank accounts were compromised, the offenders also used her details to open a new loan in her name. Through having access to Beryl's bank accounts and all of her other personal details, the offenders were able to use those details to borrow a large amount of money to purchase a car. Once the loan was approved and the car was purchased, the offenders have not met the repayments as necessary. As a result, the matter has been referred to a debt collection agency, which is when Beryl is first notified. Beryl needs to contact the debt collection agency as well as the police, to report what has happened. It would also be in her interest to purchase a credit report, which will summarise all of the loans and credit currently in her name, which may alert her to any other loans she is unaware of.

This module is one of five available in this series:

#1 Computer security
#2 Identity Crime
#3 Social Networking
#4 Fraudulent Emails
#5 Internet Banking

If you are interested in accessing any of the other training modules, they are all available for download on the following website:

www.scamnet.wa.gov.au/projectsunbird

If you are interested in other resources on protecting yourself and your computer, the following two websites may be of interest:

www.scamwatch.gov.au

www.cybersmart.gov.au

If you are interested in learning more about computers and technology, the Australian Seniors Computer Club Association may be able to assist:

www.ascca.org.au

The Carindale PCYC expresses its sincere gratitude to the many people who have been involved in the *Seniors Online Security (SOS)* project and have helped with the development of these training materials.