SENIORS ONLINE SECURITY

Computer Security

1 of 5 training guides available

PCYC
Carindale PCYC
Improving Communities Through Youth Development

WA
POLICE

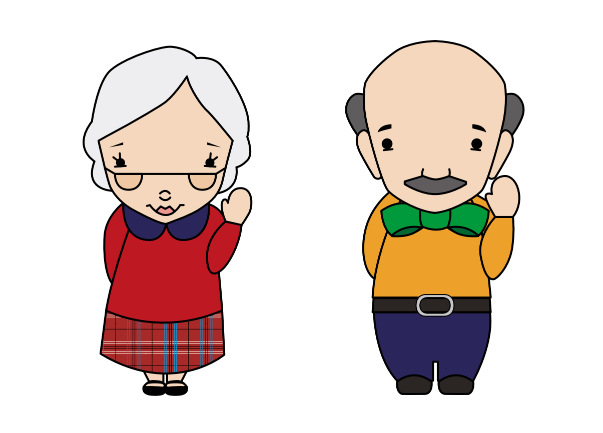
Government of Western Australia
Department of Commerce
Consumer Protection

An Australian Government Initiative

Computer security
A training guide for seniors

#1 out of 5 training guides available

This training guide provides Australian Seniors with information about ways in which the security of their computer can be reduced, but more importantly, outlines strategies to protect and strengthen their computer security.



Meet Beryl and Alan

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

Table of Contents

Introduction

Computers have changed the way we live. For many people, the first thing they do when they get out of bed in the morning is turn on their computer and check their email. Society is increasingly using computers and the internet across all aspects of life. Computers are central to our communication, our business and our social lives. While this has many benefits, there are also many things that can reduce the security of our computers and the personal information that we store on them. Just as it is important to secure your home, it is important to secure your computer. This module looks at several simple strategies that you can use to protect and strengthen the security of your computer.

Overview of this training module

This module looks at the various ways that the security of your computer can be threatened. By the end of this module, you will be able to:

- → Understand why computer security is important;
- → Name the different threats to computer security;
- → Understand the consequences of not have a secure computer;
- → Know what to do to secure your computer and its contents;
- → Know who to contact if you think the security of your computer has been breached.

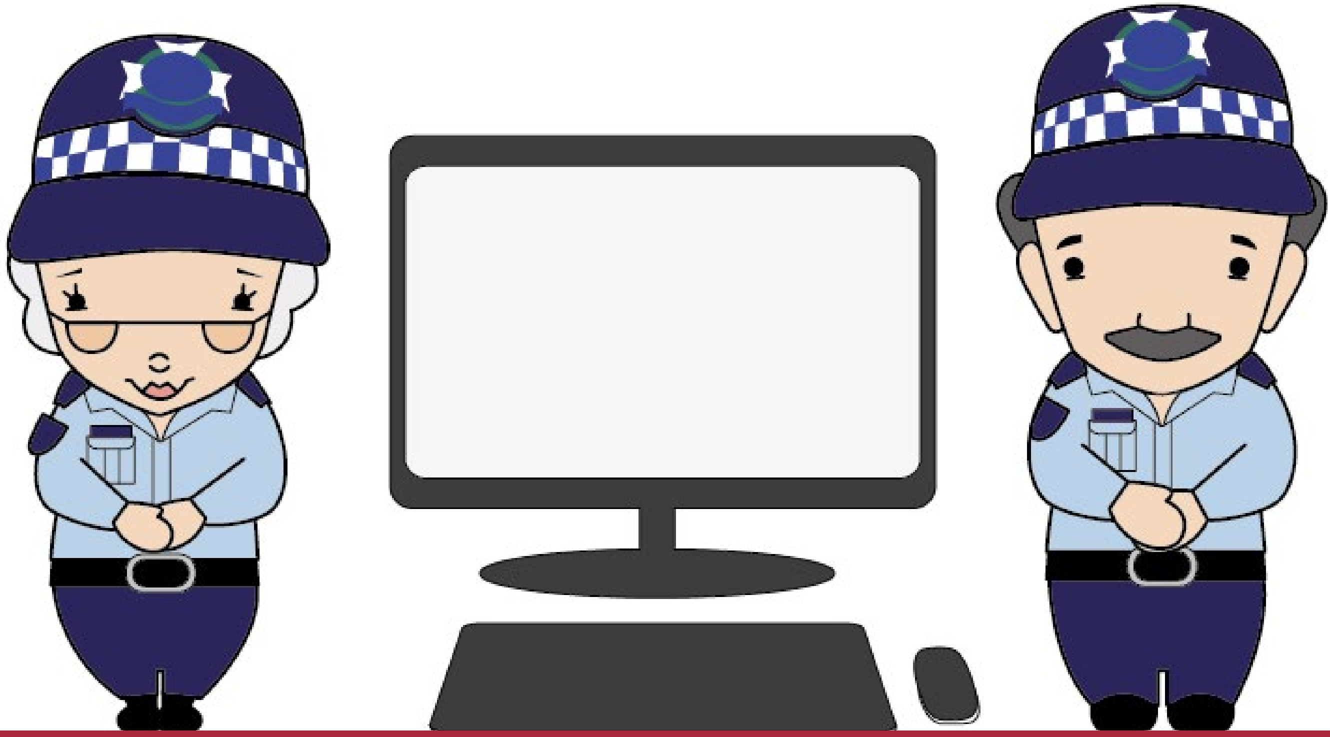
This module will give you information about how to keep your computer and all of its content safe and secure.

Why is computer security important?

Just as most people take steps to ensure that their property is safe (such as locking doors and windows when you leave the house), it is just as important to make sure that your computer is secure. Computers are used for an increasing number of activities in daily lives, such as banking, shopping and email. They are also being used to store large amounts of personal data. For many people, their computer is a central part of their lives. Computers are a great asset to many people in allowing them to communicate and conduct business from the comfort of their own home. This has many benefits and by being aware of how to minimise the risks associated with your computer, you can continue to enjoy using it in a safe environment.

Things to be aware of regarding the security of your computer

There are many different ways that the security of your computer can be broken. The following details some of the most common ways that this can occur. Remember though, that while the next section outlines the ways in which your computer security can be harmed, there are many simple steps that you can take to protect yourself, which will be outlined in the second part of this book.



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. Malware can come in many different forms. It is not always easy to detect malware and sometimes you might not even know it is on your computer.

Different types of malware are designed to do different things. Some types of malware are specifically designed to gather personal information such as account login details. Other types of malware can monitor every keystroke made by any user. Therefore, this type of software can record you typing your online banking website into the browser, then typing in your username and then typing in your password.

There are a lot of different types of malware. While the way that they operate and their impact can vary quite dramatically, all malware can have negative consequences to the computer and its user.

IDENTITY CRIME

Identity crime can be defined as the unauthorised use of your personal details, with the purpose of committing fraud or other crimes. For example, you may have your credit card details stolen and used to purchase goods which you didn’t buy. You might have your account details stolen and the money taken from your account. You might also have personal information about you taken so that a new credit card or loan is opened up in your name.

Identity crime is a huge problem. It is believed to be the fastest growing crime type in Australia and is already the most prevalent type of crime in America. Victims are increasingly having their identities stolen by criminals who are taking their details and using them for their own purposes.

A lack of security on your personal computer can increase the chances that you become a victim of identity crime.

FRAUDULENT EMAILS

Similar to identity crime, fraudulent emails are a big problem. Fraudulent emails will always try to get your personal information or money. Even if they don't ask for this in the first email, they will at some point down the track. Some fraudulent emails might contain attachments and ask you to open them. For example, you might receive an email from a postal service or courier about a parcel which is being delivered to you. The email will ask you to open the attached file, to either follow its instructions or as a receipt. If you open the file as requested, it is very likely to contain malware which will download and install itself onto your computer.

UNSECURED NETWORKS

Using an unsecured network poses a significant risk to the security of your computer. Many people have a wireless network in their homes to allow more than one computer user to connect to the internet at the same time. However, in the same way that people generally lock their homes when they leave and fence their property to keep unwanted persons out, there is a need to secure the wireless network so that only authorised people can access your internet connection. Without securing the network, anyone can use your internet at anytime. There are a number of dangers from having an unsecured network. Apart from the obvious fact that strangers can use all of your download allowance, you cannot control what other computers access your network and this opens up the possibility for malware to infect your own system. There is also the chance that any personal information that you have stored on your computer can be accessed by others using your internet connection.

As well as securing your home network, it is also important to avoid connecting to unsecured networks where possible. Public wireless hot-spots are great when travelling and you need to check your email or locate a restaurant or phone number. However, there are risks when using unsecured networks. Just as you cannot control who connects to your personal unsecured network and what they do, you have no knowledge about the network you have connected to. You don't know the type of security (if any) that the network has. You don't know who else is using the network and what they are using it for. You don't know if another user has malware on their computer which can download itself onto your system. Unsecured networks generally allow all users to view what each other is doing. This means that your private details may be on view to more people than you think. While public wireless hot-spots are convenient and easy to use, they can also increase the chances that your computer is infected with malware and your personal details (such as account logins and passwords) are taken by an authorised person.

Revision questions

The first part of this booklet has looked at the importance of computer security to protect yourself and your personal information. The following questions will see how well you understand the ways in which the security of your computer and personal details can be reduced.

Please select either true or false for each of the following questions:

1) Malware is a type of software designed to corrupt your computer.

True False

2) You may not know if malware is installed on your computer.

True False

3) Information posted on the internet is private.

True False

4) You will not know if someone has accessed your accounts.

True False

5) All fraudulent emails are obvious.

True False

6) Public wireless hotspots are just as safe as personal wireless networks.

True False

7) You should always be careful when opening attachments on emails.

True False

8) Identity crime can never happen to me.

True False

9) It is safe to send personal details in response to an email.

True False

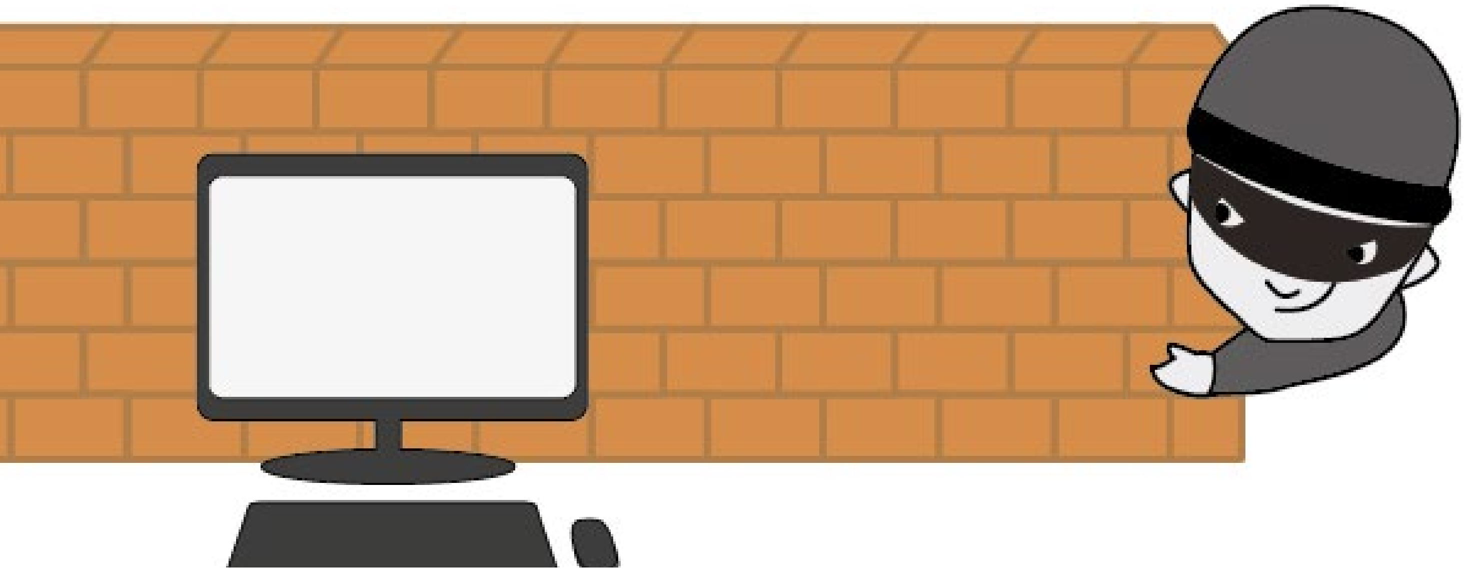
How to protect your computer

While the first part of this booklet has outlined the many ways in which the security of your computer and personal information can be threatened, this should not deter you from using your computer and the internet. While there are risks in cyberspace, there are also a number of simple steps which will dramatically reduce the chances that the security of your computer is compromised. Several of these are outlined below.

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 is used to protect your computer 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 on your computer and will give you the ability to remove it. 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.

It is advisable to have only one good anti-virus program on your computer. 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 to secure your computer. 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. Your computer may provide alerts which notify you that an update is available. It is important that you accept these updates to make sure your computer is fully protected. 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. While anti-virus software is not perfect, it is really important to have it on your computer. Although it cannot guarantee that you will never get malware on your computer, it will reduce the chances of this happening.

UPDATING SOFTWARE

In the same way that you should update your anti-virus software on a regular basis, you should also look for updates to your software and operating systems. These are released on a regular basis by companies and will fix identified weaknesses and vulnerabilities in your system. As with anti-virus software, it is important that if you are notified of an available update, you accept it. By having an up to date system in place, this helps to reduce the ways in which your computer can be compromised.

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 as valuable to you as the cash you have in your bank accounts. Criminals will use them in the same way, to get your money or to open up new accounts, credit cards or loans in your name.

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 fake.

It doesn't matter what an email looks like, or the reason why the email says it needs your personal details. There are so many different ways that offenders 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.

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 down on a piece of paper next to your computer. The password should not be a word found in a dictionary and should contain at least eight letters and numbers and include one symbol (such as !@#$%)

Consider using a password safe, which can safely store all of your passwords in the same way that a conventional safe can store your personal valuables. Never give your password to other people either, even close family and friends. This can void the security policy of your bank, if something were to happen to your accounts.

Just as you would use a good quality lock on your front door to secure your house, you should use a strong password to protect your bank accounts. It is the only thing that is protecting your personal details and money from being accessed by other people.

USE AN EMAIL FILTER

Email filters are a good way of stopping some fraudulent emails from coming into your inbox in the first place. Email filters are able to identify a lot of fraudulent emails and send them straight to a junk mail folder. This means that you don't have to deal with them, and you can delete the emails in your junk mail folder on a regular basis.

If you use an email filter, it is important to know that it is not foolproof. Email filters are not perfect and just like people, they will sometimes let fraudulent emails into your inbox. Just because it is in your inbox, does not mean it is legitimate. You still have to make that decision yourself. If you are not sure, talk to a trusted family member or friend about the email.

AVOID CLICKING ON LINKS IN EMAILS

It may seem silly, but clicking on links in emails can be very harmful to your computer. If you receive an email from someone you don't know asking you to check out a funny photo or an interesting story, think twice before you click on it. While it may really take you to a funny photo or interesting story, it may also take you to a website which has been compromised with malware, and by clicking on the link and visiting that page, you may accidentally download malware onto your own computer.

AVOID OPENING EMAIL ATTACHMENTS

In the same way that clicking on links in emails can be harmful, opening attachments in emails can also pose a threat. Opening an attachment which is infected with malware can download and install unwanted malware on your computer. If you receive an attachment from an unknown person, you should always delete it. If you receive an attachment from a contact, it is up to you to decide whether or not you think it is safe to open the attachment. If you choose to open the attachment, you should scan the attachment for malware before you open it, to make sure that it will not harm your computer. Most email packages will provide an option for you to do this, however if you are unsure, contact a local IT professional who can show you how to do this.

SECURE YOUR OWN NETWORK AND USE A FIREWALL

Just as you would install locks on your doors and windows in your home, you need to secure your wireless network. This will ensure that only those users you authorise can access your internet connection. It will also ensure that the personal information stored on your computer stays private and cannot be as easily accessed by others. There are different ways in which you can secure your home network, and most require a password or passphrase. 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. If you are unsure how to do it, contact a local IT professional for advice on what is best for you.

AVOID USING PUBLIC UNSECURED NETWORKS

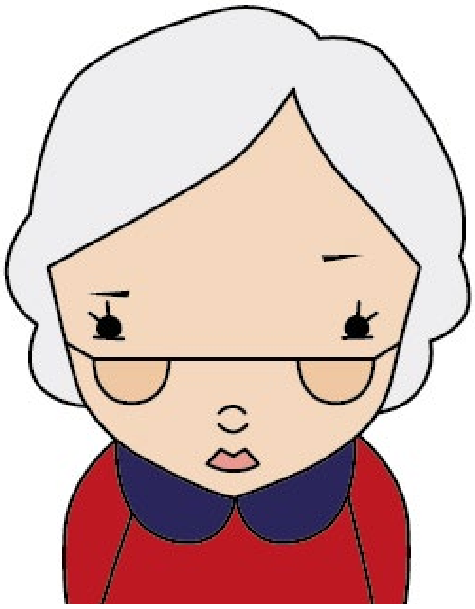
At home, you know how secure your computer is. You know what anti-virus software you have installed and when it was last updated. You also know who has been using your computer and what they have been doing on it. If you connect to a public wireless network, you do not have the same level of information about the security of the network or the same level of control about who is using it and what they are using it for.

While public networks are great when travelling or when you are out and about, they are not as secure as your own personal network. If you must use an unsecured network, make sure you have anti-virus protection on your computer and that it is up to date. Also, try to restrict the type of business that you do. Try to avoid doing banking or anything that uses your personal information. Public networks are much more likely to have malware present or have other users with malware on their computers, which makes your computer vulnerable. In addition, always remember to log off and shut down any browser when leaving a public network.

SURF SAFELY

The internet is a great tool for finding out information, communicating with people and for doing business. There is a wealth of facts and figures at our fingertips. However, there are also many hidden dangers. When browsing the internet, you should always be careful of what sites you choose to visit. Try to stick to reputable websites, particularly if you are giving over personal information (such as credit card details for online shopping). Avoid the temptation to click on pop ups which may appear or download software or attachments which you are unsure of. Also be careful of links on websites which may take you to a less reputable or file sharing website. These may allow malware to download and install on your computer without your knowledge. Surfing the internet can be lots of fun and very informative, but you need to be careful with your actions.

What to do if you think your computer is not secure



There are many strategies that you can put into place to keep your computer and your personal details safe. However, there may be times when you think the security of your computer has been compromised. The following section looks at what you can do if this happens to you.

IF YOU THINK YOU HAVE MALWARE ON YOUR COMPUTER

If you suspect that your computer is infected with malware (for example its behaviour becomes erratic, the hard disc or internet connection always seems busy when you are doing nothing or it starts to run very slowly), there are a number of things you can do. Firstly, you can scan your computer with anti-virus software. This should be able to detect any malware which has installed itself on your computer. If detected, it should also provide you an option to remove this. However, some malware can be very tricky to remove and you may be unsure of the damage done to your computer. In these cases, it may be beneficial to take your computer to a local IT professional. If you don't want to take your computer to someone, there are also mobile repair technicians who will come to your house to look at and fix your computer, but this may come at a higher cost.

IF YOU THINK YOUR PERSONAL DETAILS HAVE BEEN COMPROMISED

If you think that your personal information has been accessed from your computer, there are a few things you should do straight away. The type of information you think is compromised will determine what you need to do.

If the information is about 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 the information is about another type of account (such as telephone or internet or a payment service) then you should contact the provider 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 it is about passwords to any of your accounts, you should change these as soon as possible. As with all accounts that you have, 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. 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 down on a piece of paper next to your computer. The best solution is to use a password safe. Never give your password to other people either, even close family and friends.

If it is about personal details, such as name, address, birth date and phone number, unfortunately there is not much you can do. If this information concerns your mother's maiden name or other answers to possible security questions, then you might want to consider changing these security questions as soon as possible. While you can't control what happens to your personal details, you can purchase a credit report, which will tell you what credit cards and loans have been taken out in your name. These can be purchased from a number of different companies and will alert you to any credit cards or loans which you didn't know about. Once you have this information, you can then approach the institution and try to sort the matter out.

If you think your personal information has been accessed by someone you have not authorised, it is important that you take action as soon as possible. There is no point pretending that it didn't happen or won't have any consequences. While nothing may come of it, you are still safer to check and pick up any problems early. It will be easier to resolve any issues with the bank or other organisation sooner rather than later.

Conclusion

Using your own computer at home to browse the internet has great benefits. It allows you to communicate with family and friends, find all sorts of information and do business such as banking and shopping. However, just as it is important to secure your physical property, it is very important to secure both your computer and your network. Even though there are many things which can reduce the security of your computer, you should not be afraid to use it. While there is no guarantee that you won't download malware at some point in time, this booklet has outlined many simple steps you can take which will strengthen and protect your computer.

Revision scenario

Beryl has just moved into a unit in the middle of town. She uses both a personal computer as well as a laptop to access the internet. She has organised a wireless network to be installed in her unit, so that she can access the internet with both devices at the same time. Beryl has set up regular anti-virus updates to her laptop as she uses it on many networks. However, she has not done the same with her personal computer. She also hasn't secured her wireless network, because she doesn't know how to do it.

1) What are some of the risks that Beryl faces by only protecting her laptop?

One afternoon, Beryl is at home in her unit. She turns on her computer to check her email, but it won't connect to the internet. She calls her internet service provider to report this fault. They tell her there is no fault and that she has already used all of her data allowance for the month. Beryl is puzzled as she hasn't been using her computer that often and she certainly hasn't been downloading any large files.

2) What do you think can explain Beryl's situation? What action should she take to prevent this from happening in the future?

With her wireless connection secured, Beryl continues to do business as usual on her computer. A few months later, she receives a bill in the mail for goods purchased from a computer store. The bill is for several thousand dollars. Beryl calls the store to let them know that she has mistakenly received someone else's bill, as she has not purchased any goods from that company. The store manager tells her that during the previous week her credit card was used to buy several laptops and software.

3) What do you think has happened to Beryl? How could she have prevented this from occurring? What action should she take to prevent any further consequences?

Answers to Revision Questions

1) Malware is a type of software designed to corrupt your computer.

True False

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.

2) You may not know if malware is installed on your computer.

True False

You can accidentally download malware onto your computer without knowing it. While obvious ways include the opening of attachments, sometimes a website you visit may be infected. There is not necessarily a warning sign that you have malware on your computer. That is why it is extremely important to have up to date anti-virus protection on your computer and to conduct regular scans, to make sure that your computer is clean.

3) Information posted on the internet is private.

True **False**

Many people think that information they post on the internet will only be read by their family and friends. However, this is not necessarily the case. The internet is not as private as people think. Once you post information on the internet, you have no way of knowing exactly who has seen it, downloaded it or forwarded it to someone else. This is particularly the case if you don't use a secure network. An unsecured network means that anyone can access your computer and personal information.

4) You will not know if someone has accessed your accounts.

True False

You may not know that someone has accessed your accounts. In the same way that you may not know you have malware on your computer, there are not necessarily signs which indicate that someone has accessed your accounts. If you don't have strong passwords and security settings or a secure network, you are at greater risk of another person being able to access your accounts. It is very important to make sure that you take action to protect your computer, your accounts and your personal information.

5) All fraudulent emails are obvious.

True **False**

Not all fraudulent emails are obvious to the recipient. While some may have terrible spelling and grammar, others will have no mistakes at all. Fraudulent emails may look very real to the person who receives them. However, you should never respond to an email asking for personal details or money, no matter how real it looks, who it is from or why they want the money or details.

6) Public wireless hotspots are just as safe as personal wireless networks.

True **False**

Public wireless hotspots are not as safe as your own network. You have control over your own network, and know what security settings you have in place. If you have a secure network, you should have a good idea of who is using your network and what they are using it for. When you use public networks, these are often unsecured. Therefore you have no control over who uses them and what type of websites they access. Public networks are attractive targets to criminals because of the lower level of security, particularly around malware. Sometimes using public networks is unavoidable, but you should not do important business (such as online banking) on these networks, and always ensure that your anti-virus protection is up to date.

7) You should always be careful when opening attachments on emails.

True False

Attachments may seem harmless but they can also contain malware. If you open an attachment that has malware in it, it will download and install itself on your computer. You may not even know this has happened. You should never open attachments from people you don't know. Even with people you do know, you should always think carefully before opening any attachment. If you do open an attachment, always scan it with your anti-virus software before you open it. This will reduce the chances that you open something more than what you bargained for.

8) Identity crime can never happen to me.

True **False**

Unfortunately identity crime can happen to all computer users. However this shouldn't scare you away from using your computer. There are many strategies you can put in place to protect your personal details. By limiting the amount of personal information you put on the internet, by using security settings on your account, by having strong passwords and by not responding to emails with personal details, you can reduce the chances that identity crime happens to you.

9) It is safe to send personal details in response to an email.

True [✓ **False**]

Although you may not realise this, your personal information is just as valuable as the money in your bank accounts. Personal information can be traded in the same way as cash, and can be used to access your existing accounts or to open up new accounts or lines of credit in your name. If you receive an email asking for personal details, you should never send any personal details. Even if it seems harmless, this information can be used against you. By sending personal information, you are increasing the chances that someone can access your accounts.

Answers to revision scenario

1) What are some of the risks that Beryl faces by only protecting her laptop?

Beryl faces several threats to the security of her computer and personal information. The first threat comes from not having anti-virus software on her personal computer. Even if she only uses her personal computer at home, it is essential that she has anti-virus software on it and that it is updated regularly. It is just as important for her personal computer as it is for her laptop. Beryl has done this on her laptop, but she needs to do this for her personal computer as well.

The second threat comes from having an unsecured network. Beryl is not able to control who connects to her network and what they do while they are connected to her network. This leaves her vulnerable to malware and compromises the security of any personal information she keeps on her personal computer. The fact that she has no virus protection as well as an unsecure network increases the chances that her computer and network will be targeted. Beryl needs to secure her network so that only authorised persons can access her connection.

2) What do you think can explain Beryl’s situation? What action should she take to prevent this from happening in the future?

It is very likely that someone has been connecting to Beryl’s network and using all of her download allowance. Without a secure connection, anyone can connect to her network. It is likely that one of her neighbours has realised this and has been taking advantage of this weakness. Beryl needs to secure her network so that other people cannot connect and use all of her download allowance.

3) What do you think has happened to Beryl? How could she have prevented this from occurring? What action should she take to prevent any further consequences?

Beryl’s personal information has been compromised. This may have occurred through someone accessing her computer when her network was not secure. She may also have downloaded malware onto her personal computer. No matter how this happened, Beryl now has to deal with the fact her identity has been stolen and she has become a victim of identity crime. Beryl needs to contact the police to report this incident. She also needs to talk with the store to sort out what will happen with the losses incurred from the bill she received.

To prevent this from happening in the future, Beryl needs to make sure that her network is always secure and that she always has up to date virus protection on all of her devices. She should also scan both her laptop and personal computer to make sure that there is no malware currently on her system. Beryl should also contact her bank and other agencies to check that nothing suspicious has occurred and to let them know she has been a victim of identity crime. She should also change her passwords and security questions, to make sure that no one can have further access to her accounts. Beryl should also consider purchasing a credit report, which will tell her of all the loans and credit currently in her name. This may alert her to any other issues that she is not aware of and allow her to deal with them as soon as possible.

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.