SENIORS ONLINE SECURITY

Internet Banking

5 of 5 training guides available

Carindale PCYC
Improving Communities Through Youth Development

Government of Western Australia
Department of Commerce
Consumer Protection

An Australian Government Initiative

Internet banking
A training guide for seniors

#5 out of 5 training guides available

This training guide provides Australian Seniors with information about how to safely and confidently use internet banking services.

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

A new way to manage your affairs

The internet has changed the way that people do business. There was a time when to pay a bill or do any banking, you needed to visit your local branch, stand in line and wait to be served by a cashier. This is no longer the case. The internet has increased our ability to do many things, including banking. The majority of banks and financial institutions now have virtual banks, where you can log into a website and access your accounts. While you can't physically withdraw money from your computer, there are a range of other transactions which can be done from the convenience of your own home. Internet banking is a new concept for many and may seem a little scary. However, by taking some simple steps to secure your computer, you can enjoy the benefits of internet banking and reduce the chances that you become a victim of fraud.

Overview of this module

This module looks at different topics related to internet banking. The purpose of this module is to provide information about internet banking that will improve the confidence of computer users to safely use internet banking.

By the end of this module, you will be able to:

- → Understand the benefits that internet banking provides;
- → Name the different dangers to look out for relating to internet banking;
- → Understand what is meant by the term phishing;
- → Understand how other people can get your details to access your bank accounts;
- → Know what you can do to protect your bank accounts and money; and
- → Know who to contact if you think you have become a victim.

This module will give you details about some simple strategies which will allow you to confidently use internet banking in a safe manner.

What is internet banking?

Internet (also known as online) banking allows customers of banks and other financial institutions to conduct their business through the computer. While customers cannot physically withdraw money from their computers, they can do a large range of other transactions. This includes transferring money between accounts, paying bills, paying other people, viewing account statements and accessing account balances. The biggest advantage to internet banking is that it is available to users 24 hours a day, 7 days a week, 365 days per year. The need to visit a local branch to do business is not required. Internet banking gives customers flexibility and freedom to do their banking when they want, compared to the restricted hours that most branches have.

Many people have embraced the use of internet banking. It can be a great way to save time and effort in doing tasks such as paying bills. It is much easier to log into your computer at home than it is to go into the bank during business hours, and wait in a queue to be served. However, there are a few things to be aware of when using internet banking.

What you need to know about internet banking

Internet banking is an easy way of conducting financial transactions at a time which is convenient to you, the customer. However, it is not surprising that some people target online banking websites and customers. They try to trick people into giving over their personal account information to access their money. There are many ways that strangers can target consumers. The following presents two of the most prevalent threats to the security of banking over the internet.

PHISHING EMAILS

The term “phishing” looks a bit 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 while another person sits back and waits for a “bite”, in that they wait for you 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. 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 it 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 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 other people free access to your bank accounts. They can then transfer all of your money.

The second way that other people will try to get your details is to provide a link in the email, and ask you to click on this. 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 is fake and is designed to record 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 accounts and access your money. 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 the your name.

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. 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 on a computer. 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.

Revision questions

The following questions are designed to see how well you have understood fraudulent emails and malware.

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.

1) How would you define a "phishing email"?

a) An email which offers a great deal on fishing equipment
b) An email which asks you for money
c) An email which asks for personal details
d) An email which offers you a prize

2) What is a phishing email likely to do?

a) Ask you to provide your personal details in a reply email
b) Ask you to click on a link to a website to enter your personal details
c) Neither a) nor b)
d) Both a) and b)

3) What type of details are safe to send over email?

a) You should never send any personal details to someone over email
b) Name, address and phone number
c) Mother's maiden name
d) The name of your pet

4) What does the term "malware" mean?

a) A new computer program
b) A computer accessory
c) A type of malicious software
d) A popular website

Protecting yourself when doing internet banking

Internet banking provides a greater amount of flexibility and freedom compared to having to go into a branch to pay bills and do other business. The first part of this booklet has described how internet banking works and the advantages of being able to do your financial transactions online. It has also looked at what you need to be aware of when using internet banking. The next section looks at simple ways in which you can try to protect yourself, so that you can safely use internet banking with confidence.

THE IMPORTANCE OF ANTI-VIRUS SOFTWARE AND AN ACTIVE FIREWALL

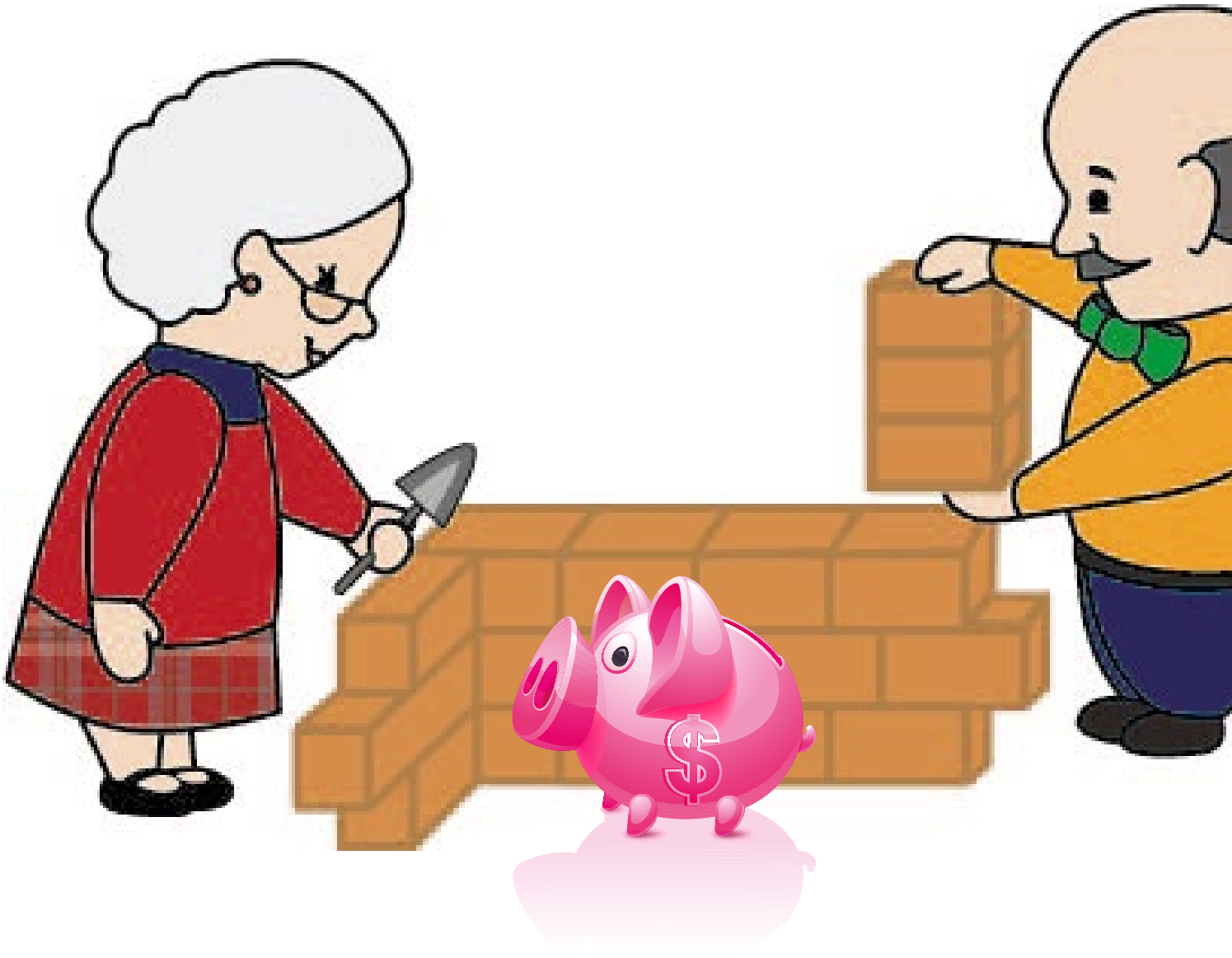
It is essential that your home computer has anti-virus software installed. It is even more important to make sure that this is updated on a regular (such as daily) basis. Anti-virus software can be installed and used to protect your computer from unwanted malware. It will scan your computer on a regular 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 by installing more than one anti-virus program, it 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 so that it stays up to date with the latest threats.

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.

The same goes for doing banking through your phone. A lot of new phones have the ability for you to use an application or the internet to do your banking literally anytime, and anywhere you go. Some of the new phones are more powerful than the computer that you have at home, even though they are much smaller. You should treat these phones like a computer and install anti-virus on your phone. As with your own computer, you should only use your phone to do online banking if it is protected.

In terms of internet banking, some banks also have policies around the need to have anti-virus software on your computer. If you do not have this, and your computer is infected with malware, the banks may not be obligated to reimburse any money you lose if your accounts are compromised. Check with your own bank to see what their policy is and make sure that you meet their criteria.



AVOID USING PUBLIC COMPUTERS

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 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.

While public computers are great when travelling to send an email to family and friends at home, you should think twice before using a public computer to do your internet banking. 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 and 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 to do your internet banking, you are at a greater risk of compromising your details, through a keylogger or spyware

being installed on the computer without your knowledge.

Again, your bank may have a specific policy about using public computers to do internet banking. Banks sometimes have computers available for you to use inside their branches, and these should be much safer to use than public computers in other places. However, in all circumstances, you should only use the internet for your banking on computers that you trust and can be confident in their level of protection. If you are unsure, it may be safer to wait until you can use a computer that you are confident about.

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, and they can be used 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 someone will try to get your personal details. **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 just because the email looks legitimate, it is.

NEVER PROVIDE YOUR PERSONAL DETAILS THROUGH AN EMAIL LINK

In the same way that you should never send your personal details via email, you should never click a link in an email to fill out your personal details. The website may look genuine, and may have the same logos and the same layout to your usual bank website, but it is very likely to be false. By typing your personal details into this type of website, you are giving another person access to your current accounts as well as giving them enough information to open up new credit accounts or loans.

As stated in the previous point, if you receive an email asking you to provide your personal details in a website, take the same precautions. Give your bank or financial institution a call and ask if they really sent you the email and if they really need your details. They are very likely to tell you it is fraudulent. It doesn't matter what story is given in the email and what reason they have given for clicking on the link, the end result is the same. They want your personal details for their own benefit. Remember, **you should never be asked for personal details in an email**, no matter what the reason or no matter how urgent it is supposed to be.

USING STRONG PASSWORDS

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 on the internet, for example, on your social networking 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 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.

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 on a credit card statement and not look at the entire bill or file away bank statements 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. 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. This means that you are in a much better position to take action which will limit any losses and allow you to take steps which will help you prevent it from reoccurring in the future.

TAKE ADVANTAGE OF EXTRA PROTECTION FOR YOUR ACCOUNTS

To increase the security of your accounts when doing business online, many banks are now offering extra levels of protection. This is to make sure that the person doing the transaction is you and not someone who has gained your details without your knowledge. Added measures include sending a text message to your mobile phone with a one time password to enter as well as the use of tokens which also generate a one time password. These extra security measures can help you protect your accounts from unauthorised use. If you are interested in these, contact your bank to see what they offer and if it is suitable for you to use.

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 depend on 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 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. However, if you follow the steps outlined earlier in this booklet, you are reducing the opportunities for this to happen to you.

Conclusion

Using the internet to do banking is a very easy and convenient way to manage your financial affairs. It gives you the flexibility and freedom to do business from anywhere at anytime of day. Although there are things to be aware of when using internet banking, if you take all the necessary precautions, it is a very safe way to do business.

Phishing emails and malware are the biggest things which you need to be aware of when using internet banking. These will both try to get your personal details so that other people can access your accounts and take your money. While there is no guarantee it won't ever happen, there are many simple steps you can take to protect yourself and your bank accounts.

It is essential that you install anti-virus software on your computer and update this on a regular (if not daily) basis. It is also important that you only use computers that you know and trust when doing internet banking. If you are unsure of the security of any computer, avoid using it for banking. You don't want to risk the security of your bank accounts. As with all of your accounts you should use strong passwords to prevent people from accessing them. There are also options to use extra security features for online banking, such as text message and token passwords. These are things which you should talk to your bank or financial institution about, to see if they will work for you.

Above all, do not respond to any email request for personal details, such as your bank account numbers and pin or passwords. You should never have to provide this type of information to anyone over email, regardless of who it comes from and why they say they need it. Just because an email looks to be true, it doesn't mean that it is.

This module has looked at internet banking and the ways that you can protect yourself so that you can use internet banking with confidence. It has also given advice on what you can do if you realise that you may be a victim of fraud. Internet banking is a great way to do business and by taking some simple precautions as outlined in this booklet, you should feel safe to use it with confidence.

Revision scenario

Beryl has just signed up for internet banking. She is looking forward to paying her bills online as she struggles to make it to the post office every month. Beryl has a fairly new computer, but is unsure about what programs she currently has installed. She remembers the salesman installing anti-virus software when she bought the computer, but hasn't done anything about it since that time.

1) What steps should Beryl take to ensure that her computer is secure for internet banking?

Beryl has secured her computer and has been using internet banking for a few months. She now relies heavily on her online banking to pay all of her bills, to transfer money between her accounts and to pay her mortgage. One day, Beryl receives an email from her bank, stating that they have noticed some suspicious activity on her account, therefore her accounts have been suspended until the matter can be investigated further. The email asks her to log into her account via a link in the email, to reactivate her accounts and ensure that she is the only one authorising any transactions.

2) What action, if any, should Beryl take about this email?

Beryl tried calling her bank, but after spending over an hour on hold, hung up without talking to them. She knew that she had a bill due and some other transfers organised the next day, which she didn't want disrupted. Beryl decided she had better clear the matter up as soon as possible. She clicked on the link in the email, which took her to the sign in page of her bank. She entered her details as requested and felt relieved that the matter was now over.

3) What are the consequences of Beryl's action? What should she do to prevent further damage?

Answers to revision questions

1) How would you define a “phishing email”?

a) An email which offers a great deal on fishing equipment
b) An email which asks you for money
c) **An email which asks for personal details**
d) An email which offers you a prize

The purpose of a phishing email is to try and trick you into giving over personal information, such as bank account details or usernames and passwords. It doesn’t matter how legitimate the email looks, or why the email says it needs your personal details, **you should never send personal information in response to an email**.

2) What is a phishing email likely to do?

a) Ask you to provide your personal details in a reply email
b) Ask you to click on a link to a website to enter your personal details
c) Neither a) nor b)
d) **Both a) and b)**

The purpose of a phishing email is to try and trick you into giving over personal information. This usually happens in one of two ways. The first is that the email will simply ask you to reply to the email you have received, answering all the questions. The second is that the email will contain a link to a website and will ask you to click on this link. Once you click on the link, you will be prompted to enter all of your personal details on a website. No matter how genuine the website looks, it will be false and by entering your personal details, you are giving criminals unauthorised access to your accounts and your identity.

3) What type of details are safe to send over email?

a) **You should never send any personal details to someone over email**
b) Name, address and phone number
c) Mother's maiden name
d) The name of your pet

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, it may not be. Your name, address and phone number are details which you should only share with people you know in person and are comfortable with. You generally wouldn't want a complete stranger knowing where you live and how to contact you. Also, your mother's maiden name is one of the most common security questions used by companies to verify a person's identity. In the same way, many people create their own security questions which might be the name of their pet. By sending this type of information, you are increasing the chances that someone can access your accounts.

4) What does the term "malware" mean?

a) A new computer program
b) A computer accessory
c) **A type of malicious software**
d) A popular website

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.

Answers to revision scenario

1) What steps should Beryl take to ensure that her computer is secure for internet banking?

There are a few steps that Beryl should take to ensure that she can use her computer safely. The first is to make sure that she has anti-virus protection and that it has been updated. If Beryl is unlikely to do this on a regular basis, she should arrange for her computer to automatically update the anti-virus protection every time she turns the computer on.

Second, Beryl should scan her computer to make sure that she has no malware on her computer. If she has been using the internet without adequate anti-virus protection, she may have unknowingly downloaded malware onto her computer. If she starts to use internet banking with malware on her computer, she risks her personal details being stolen by a criminal. If a scan of her computer reveals that there is malware installed, then she should remove this. If she is unsure of how to do this, Beryl should take her computer to a local IT professional or have one visit her house to make sure that her computer is malware free.

Third, Beryl should check with her bank to see what policies they have about internet banking. There might be certain requirements that she has to be aware of, which ensure that if her account is compromised, she is covered for any losses.

2) What action, if any, should Beryl take about this email?

The email that Beryl has received is very likely to be a phishing email, which is trying to trick her into giving over her banking details. No bank should ever ask their customers to send personal banking details over the internet, in response to an email. Beryl should just delete this email.

If Beryl is unsure about the email, she should give her bank a call to check if they really did send it. It is very likely that the bank will let her know that it is fraudulent and that they haven't sent her that email. Beryl can then delete the email without thinking about it again.

3) What are the consequences of Beryl's action? What should she do to prevent further damage?

Beryl has become a victim of a phishing email. The email has successfully tricked Beryl into giving over her banking information. It has done this through the threat of suspending her accounts and not allowing her to access her money until the matter is sorted. While the link provided in the email looked legitimate, it is very likely to have been a fraudulent website, made to look genuine. When Beryl entered all of her account details and passwords into the website, these would have been sent to a criminal, who can now access Beryl's accounts. Beryl is likely to lose the money in her accounts and may have new credit cards or loans taken out in her name as a result of this action.

To limit further damage, Beryl should contact her bank as soon as possible, so that her accounts and credit cards can be shut down and cancelled. The bank will reissue her passwords and credit cards as necessary. They will also be able to tell her what damage has been done. If Beryl is unsure of what else her details have been used for, she should get a credit report. This will give her the details of all credit and loans that have been taken out in her name. If anything is suspicious on this report, she can contact the bank or lender to sort the matter out 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.