SENIORS ONLINE SECURITY

Social Networking

3 of 5 training guides available

Carindale PCYC
PCYC
Improving Communities Through Youth Development

WA POLICE

Government of Western Australia
Department of Commerce
Consumer Protection

An Australian Government Initiative

Social networking
A training guide for seniors

#3 out of 5 training guides available

This training guide provides Australian Seniors with information about social networking as well as strategies to protect themselves when communicating online.

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

THE RISE OF SOCIAL NETWORKING 4

OVERVIEW OF THIS MODULE 5

WHAT IS SOCIAL NETWORKING? 5

HOW DOES SOCIAL NETWORKING OPERATE? 6

- Important facts about online communication 6

WHAT TO LOOK OUT FOR WHEN USING A SOCIAL NETWORKING WEBSITE 7

- Identity theft 7
- Fraudulent emails 8
- Malware 8

REVISION QUESTIONS 9

HOW TO PROTECT YOURSELF WHEN USING SOCIAL NETWORKING 10

- Limit the amount of information you put on the internet 10
- Knowing and using security settings 11
- Using strong passwords 11
- Avoid clicking on links in emails 12
- Never reply to an email with personal details 12
- Never send money in response to an email 13

THE CASE OF ONLINE DATING SITES 15

WHAT TO DO IF YOU THINK YOU HAVE BECOME A VICTIM OF FRAUD ON A SOCIAL NETWORKING SITE 17

- Contact the social networking site 17
- Using the delete key 17
- If you have sent money… 18
- Conclusion 20

REVISION SCENARIO 21

ANSWERS TO REVISION QUESTIONS 23

ANSWERS TO THE REVISION SCENARIO 25

The rise of social networking

In recent years, there has been a significant increase in the number of people using the internet to communicate with family and friends across the world. As a result, the number of social networking websites has increased as has the number of people using them.

There are great benefits in being able to use social networking to communicate with others. It allows family members to stay in touch with those living in different parts of the country and world. It allows people to stay in contact, or re-establish contact with friends and acquaintances they might have otherwise lost. It is a great tool to keep up to date with what is happening in people's lives, by posting messages, status updates, uploading photos and videos and viewing these immediately. A lot happens on these social networking sites, and they have become a critical way in which people communicate, stay informed about things and stay in contact. These benefits are great and cannot be underestimated.

However, it is not surprising that with so many people using social networking sites that criminals have also become attracted to these sites for criminal activities. This module looks at how this can occur and what you can do to prevent it from happening to you.

Overview of this module

The aim of this module is to provide an increased awareness around social networking and how to do it safely. By the end of this module you will be able to:

- → Identify the benefits of using social networking to communicate with family and friends;
- → Understand how social networking operates;
- → Understand the different ways in which criminals target people on social networking sites;
- → Know what level and type of information you should post online;
- → Know how to use security settings on your accounts and profiles;
- → Understand how communicating online is different to communicating face to face;
- → Know simple strategies which can reduce the likelihood that you become a victim; and
- → Know what to do if you think you have been a victim on a social networking site.

This module will give you information about how you can use social networking sites to meet and communicate with people in a safe manner. Overall, this aims to reduce the chances that you become a victim of a crime on a social networking site.

What is social networking?

Social networking is all about communicating with people. Social networking is a way of connecting people who wouldn't normally meet each other through their friends and other contacts. Social networking has grown in popularity through the internet, with hundreds of websites being specifically created to enable people to meet and talk to each other. Social networks can be based around many things such as a certain interest or hobby (Italian cooking or salsa dancing), or a certain group of people (new mothers). The internet allows people all over the world to talk to each other and share interests and experiences.

How does social networking operate?

Social networking normally operates through a person joining a chosen site and posting a personal profile. They can then view the profiles of other users and initiate discussions and contacts with those people. They can also be contacted by other people who have viewed their profile. It allows people to communicate who wouldn't usually be able to talk with each other.

IMPORTANT FACTS ABOUT ONLINE COMMUNICATION

Communicating over the internet is easy. Through email, or chat rooms or web cameras, there are many different ways that you can talk to people all over the world. However, there are a few facts about online communication which are very important to remember.

When you are talking face to face to another person, it is generally easy to know who you are talking to. You are able to see their gender, their approximate age, the colour of their hair, how tall they are and the colour of their skin. You know all of this about the person because they are standing in front of you and you can physically see it.

When you are talking to a person over the internet, the same level of trust is difficult to establish, because you can't physically see the person. Instead, you can only rely on what the person tells you about them. For example, the person might tell you they are a tall, muscular and blonde man. In real life, the same man is nothing like that.

Over the internet, it is harder to know if the information you are being given is true. The internet makes it more difficult to check the truth behind what people tell you.

It is also very important to know that **not everything that appears on the internet is true**. There is no filter which edits material posted on the internet. Anyone can write anything, true or false, and put it on a website. No matter how professional or legitimate the website looks, it may not be true. The same goes for people. There are people on the internet who will lie to trick people into giving them what they want.

You should not be scared or afraid to communicate with people on the internet. It is up to you to decide who you trust and how much information you give them. The rest of this booklet will look in more detail at some of the ways you can protect yourself and be confident to use social networking sites.

What to look out for when using a social networking website

As stated in the introduction to this booklet, social networking is a great way to stay in touch with family and friends and keep up to date with the lives of your friends, meet new people and re-establish friendships with people you have lost contact with. However, as in real life, socialising in the online world has some things you need to look out for. Some of these are listed below:

IDENTITY THEFT

One of the biggest issues around social networking relates to a person's identity. Identity theft 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 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.

It is very easy to forget that when you create your profile or type a message to a friend on a site, that people other than your friend can read it. You might think that what you have put on the internet is private, but the internet is not really private. You cannot assume that the conversation is just between you and your friend.

Some people put a lot of information on the internet. Others can take advantage of the high level of openness that occurs 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.

FRAUDULENT EMAILS

Similar to identity theft, fraudulent emails are a big problem on social networking sites. The types of fraudulent emails that can appear in your inbox from social networking sites are infinite. You might get an email from the social networking site itself, asking you to confirm your identity and account. You might get an email from a "friend" asking you to click on a link to a funny photo or story. You might get an email from someone you know, telling you they are in trouble and need money transferred to them immediately. In each of these situations, it could be fraud. An email asking you to confirm your identity will try to get your personal account information to in order to log into your account or to open a new account in your name. An email asking you to click on a link might take you to a website which contains malware and infects your computer. An email from someone you know asking for money may be from someone who is pretending to be your friend and trying to trick you into giving money to them. There are many other possible scenarios where a person could try to trick you into giving over personal information or money.

MALWARE

Malware is a shortened term for "malicious software". It is designed to do a variety 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 varieties and can do significant damage to your computer and the way you use it. It is not always easy to detect malware and sometimes you might not even know it is on your computer.

Revision Questions

So far we have looked at a number of different aspects of social networking. We have looked at the benefits of social networking, but we have also looked at some of the differences in internet communication and things that you need to be aware of. Before we look at specific ways to protect yourself, the following questions will test your knowledge to this point. Each question is either true or false. Circle the option that you think is correct with the following:

1) Social networking only occurs over the internet.

True False

2) Online communication is the same as face to face communication.

True False

3) Identity theft, fraudulent emails and malware are all things to look out for when using social networking.

True False

4) You should respond to every email that you receive.

True False

5) You may not know if your computer has malware installed on it.

True False

6) Information you post on the internet can only be seen by your friends.

True False

7) Social networking sites are attractive targets for criminals.

True False

8) People post too much information about themselves on the internet.

True False

9) Sending personal information over the internet is harmless.

True False

10) There is nothing you can do to prevent identity theft.

True False

How to protect yourself when using social networking

While there are things you need to look out for when using social networking sites, they are still a great way to communicate with family and friends. The following section looks at some simple strategies for you to protect yourself while using social networking sites.

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 about yourself on the internet. When creating a profile, 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.

Also think about the type of information you post on a regular basis. You might be going on an overseas holiday for six weeks and announce this as an update. You may think that you are just telling your friends about an exciting adventure you are about to go on. However, you are also telling complete strangers that your house will be empty for six weeks. If you have your home address as part of your profile, it won't be hard for someone to link the two together. Even if you don't have your address as part of your profile, it may still be easy enough to figure out where you live from other comments and posts.

Sometimes it is easy to forget that the internet isn't as private as you might think. Be very careful in posting any negative comments about people on your profile as you cannot be sure who will read them and what the potential consequences of doing this might be. Once you put something on the internet, you lose control over what happens to it. You don't know who sees it, who downloads it and who it is shared with. It is also very difficult to remove the information entirely, as it is likely that the social networking company keeps the information even if you delete it from public view. Think through very carefully what you write as you don't want it to come back to haunt you in the future.

By limiting the amount of information you put on the internet, you are helping to protect yourself and your family and friends. By thinking through the type of information that you post on the internet, you are reducing the likelihood that you will regret your actions in the future.

KNOWING AND USING SECURITY SETTINGS

On every social networking site that you sign up to, there should be the option to use security or privacy settings. Security settings can be a great way to protect yourself. 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 to you to 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.

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 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 contain at least eight letters and numbers and include one symbol (such as !@#$%). 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 accounts and profiles. It is the only thing that is protecting your personal details from being accessed by other people.

AVOID CLICKING ON LINKS IN EMAILS

It may seem innocent, 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 look at a funny photo or an interesting story, think twice before you click on it. It may take you to a website which has been compromised with malware, and by clicking on the link and visiting that page, you may unknowingly download malware onto your own computer. Even if you receive an email from a person you know asking you to click on a website, consider whether you think it is safe to do so.

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. They can be used 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, ring the person or the company and ask whether they have sent the email. 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. 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 people will try to get your personal details and they are always coming up with new ways. **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 they email was sent to you.

NEVER SEND MONEY IN RESPONSE TO AN EMAIL

If you receive an email asking you to send money, no matter how small the amount may seem, it is likely to be fraudulent. If an email asks you to send money, you should be suspicious about who is actually asking you to send money and what it is for.

There are many ways that other people will try to get money from you. The ways in which you might be asked to send money is not important, the fact that you have been asked to send money is what you need to focus on. **You should be very wary if a person asks you to send money.** If you were walking down the street and a stranger walked up to you and asked for money, it is unlikely you would give it to them. If a person you had met a few times in your street or in your office building came up and asked you for money, it is unlikely you would give it to them. Even if a close friend or family member came to you for money, you are likely to at least think about it. Under no circumstances do people generally just hand out money. So there is no reason why this should occur over the internet. Just because you have been asked to send money, doesn't mean you have to send it.

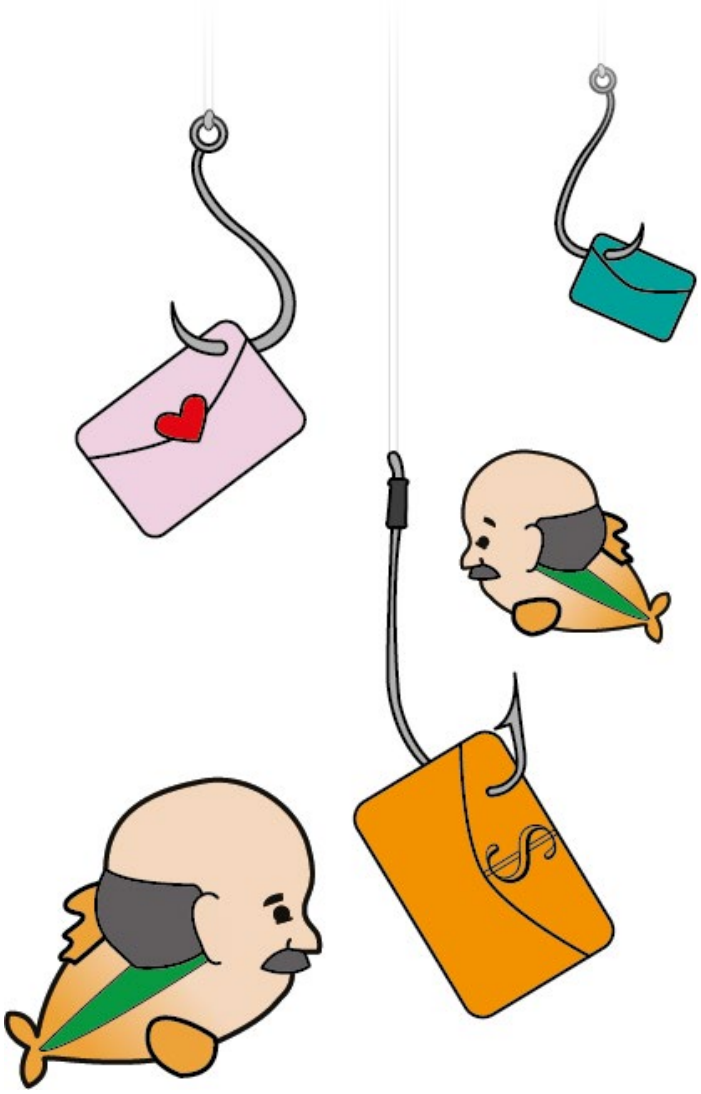
If the request comes from someone you know, as with your personal details, give the person a phone call and ask them if they sent you the email and if they really do need money. In many cases they will tell you that they haven't sent the email. In the remaining cases, if they have sent the email, you can then decide what to do.

If you have been asked to send money, think about where you have been asked to send it. If the email is asking you to send money overseas, you should be suspicious. If the email asks you to use a wire transfer company (such as Western Union or MoneyGram), then you should be suspicious. These companies are legitimate and are very good at what they do, but can be used by people to get your money.

If you decide to send money via one of

these companies, you need to realise that once you have transferred the money, it is gone. There is no way you can get it back. So, if down the track, you find that you have been defrauded, there is no way that you can get your money back. So if you decide to send money in response to an email, you need to be aware of the risk that you are taking and be prepared to never see the money again.

As previously stated, it doesn't matter who asks you for money or what the reason is. There are so many different stories that people might use to try and get your money. It is up to you to protect your money, and to stop and think when you are asked to send money. If you are unsure about the legitimacy of the request, take your time to do your research. Call the person who is asking for money on a phone number that you have found. Talk to your friends or family about the situation. If you are still unsure, contact your local crime prevention officer at the police station to see what they think. In most circumstances, it is likely to be fraud and you will be advised not to send the money. If you do decide to send the money, at least it will be your own choice. Be aware that you will not get it back regardless of what you discover at a later date. It is also beneficial to use a service such as PayPal, where you may be given a greater level of protection.



The case of online dating sites

Social networking on the internet has seen an increase in the number of people looking for relationships online. There are hundreds of dating websites which have been established. Online dating can be tricky. There are many genuine profiles. However, there are also many people who put up fake profiles to try and trick people into giving them money. Romance fraud is one of the fastest growing types of online fraud, and the number of victims and the amounts of money they lose are continually rising. It is also the most difficult to recognise and deal with, as it plays heavily on the emotions of real people, looking for real relationships.

One of the difficulties with online dating is that people offer a high level of detailed personal information, with the hope that it will allow them to meet someone with similar interests and that they are compatible with. By its very nature, online dating gives those without good intentions, an immediate way of introduction into who you are, what you like and what you are looking for. It is very easy to respond to people and give them exactly what they want. Therefore, it is very important when starting a relationship over the internet, to try and be objective about the situation. If you are asked for money, think very carefully before sending it. Some people have no issues in using love and relationships to get money out of unsuspecting victims. The consequences

of this can be devastating. The following example shows how this could occur.

Beryl was recently single and signed up to an online dating website. She was matched with a number of different men, but there was one man she felt a connection with. Beryl spent months talking to this man, and established what she believed to be a strong and legitimate relationship. They spent hours talking on the phone every day, and would send daily emails and photos. He had a daughter and Beryl had spent a lot of time with her on the phone as

well as receiving her emails and photos. Months down the track, Beryl received a phone call from this man, telling her that his daughter had been involved in an accident and was in hospital. She had sustained severe injuries and was in desperate need of surgery, but he couldn't afford it. He asked Beryl if she would pay for his daughter's surgery. The initial amount was just over $10,000 and while Beryl felt uneasy about it, she was given the phone number of the doctor and the hospital and spoke to both. She couldn't bear the thought of this little girl dying without medical care, so she sent the original amount over. Many requests came after that, and within a few months, Beryl had sent over $50,000. After a while, Beryl began to question the man about his daughter's medical costs. He became very abusive towards her and demanded further money. Beryl felt responsible but had no money left to send. Once she told him that she couldn't send over any money, he stopped calling her and only sent her offensive emails and blamed her for anything that would happen to his daughter. Beryl started to realise that he only wanted her money and started to question whether or not he actually had a daughter. However, the money she had sent was gone, and Beryl had lost all of her life savings.

Unfortunately Beryl is one of many who fall victim to romance fraud. Stories such as this one seek to exploit a victim's compassion and desire to help.

When confronted with a situation similar to Beryl's, it is hard not to send the money as requested.

There are many ways that people will use online dating websites to try and trick people into sending them money. If you are involved in a relationship online and you are asked to send any amount of money, you need to think twice. With regards to online relationships, it is wise to avoid giving the impression that you have money to spare. This may deter others from asking for it. Once you have sent money to another person, there is generally no way you can get it back.

Online dating sites are a great way to meet others. However, some people on these sites will use whatever means possible to get your money, and do not care if they hurt anyone in the process. When communicating with people online across all social networking sites, including dating sites, if you are asked for money, you have a right to be suspicious. Ask more questions and above all, don't be afraid to say no. If the relationship ends because you wouldn't send money, then it might not have been worth keeping in the first place. Whatever you do, make sure that you are comfortable with your actions, do not let anyone pressure you into making a decision (such as sending money) that you are not happy with.

What to do if you think you have become a victim of fraud on a social networking site

Despite the best intentions, things can happen. It can be hard to know what to do, if you find yourself in this situation. However, there are a few things you can do.

CONTACT THE SOCIAL NETWORKING SITE

Most social networking sites have a way that you can contact them to report any concerns or issues you may have. If you believe that someone is acting suspiciously or has asked you for money, you can report the person to the site. Depending on the complaints received, this may result in the person being blocked from the site and their profile removed.

USING THE DELETE KEY

Never be afraid to use the delete key. Delete people from your contact list who you do not want to have future contact with. Just because a person calls you or emails you, doesn't mean you have to respond. Without contact, they are likely to tire quickly and leave you alone.

IF YOU HAVE SENT MONEY...

If you have sent money, there are a few things which you should do straight away. Although it is likely that you will be upset about the situation, it is important to realise that people may not be able to help you in the way that you want.

If you have sent money via your bank, then it is worth contacting them straight away. They may be able to cancel the transaction, but this will only happen in limited circumstances. They may be able to recover the money for you, but again, this

may only happen in limited circumstances and it is not something you can expect to occur in every situation.

If you sent money via a wire transfer service (such as Western Union or MoneyGram), contact the branch immediately. Depending on the time between the transaction and when you contact them, they may be able to cancel the transaction. However, if the money has already been collected on the other end, then there is nothing which can be done. It is very unlikely that you are going to be able to recover the money, and you cannot expect the agency to be able to do this for you.

If you have lost money, it is important that you report it to your local police station. Keep the original copy of all the email correspondence you have with the person you sent the money to, as well as any receipts from transferring the money. When you report it to the police, explain what has happened and the amount of money you have lost. Be patient with the person you are reporting this to, as this type of fraud can be tricky and not everyone has a good understanding of how it happens and what can be done. Unfortunately, if you have sent money to an overseas jurisdiction, there is not much that police can do. They can take your report, but their ability to investigate your situation, arrest the offender and prosecute is very limited. If you have sent money within Australia, police are more likely to be able to investigate.

Even though you are unlikely to recover your money, it is still important that these types of crimes are reported. Many victims feel too ashamed and embarrassed about what has happened and do not feel they can come forward. While the police may not be able to do anything specifically about your situation, they can use your experience to educate others and help prevent other people from finding themselves in your situation.

CONCLUSION

This module has looked at social networking. It has detailed the great benefits of using social networking to keep in touch with family and friends as well as meeting new people. Online communication is easy, cost effective and growing in popularity every day. You should not be afraid to use social networking as a way of communicating with people.

However, there are a few things which you need to be aware of when communicating online. The ability to verify the information being presented to you is more difficult over the internet than it is face to face. It is also easy to forget that the internet isn't always as private as we think and that strangers may be able to see what is posted.

It is important to think through the type and amount of information that you put on the internet. You can control the information that you post about yourself on your profile. You can also control the people who see it, by using your security settings. Make sure that you don't put something up which you will regret in the future. Once you post something on the internet, it is there forever.

Social networking may also involve online dating. A growing number of people are turning to the internet to try and find friends and relationships. While many legitimate people use these sites to find serious relationships, others will target a person's desire to have a relationship and trick them into giving over large amounts of money. You should think very carefully before sending money to anyone as the result of an online request. You could lose the money and once it is gone, you cannot get it back.

Social networking is a great tool for communication. It is important not to be afraid of using it to keep in touch with people and make new friends. By following the strategies set out in this module, you can protect yourself while using social networking sites. By limiting the amount of information you post online, by using your security settings, by remembering the differences in online communication compared to communicating face to face and by not sending money to those you meet online, you are likely to enjoy the many benefits of social networking for many years to come.

Revision scenario

Alan had recently split from his girlfriend. His friends had told him about online dating and although he was a bit sceptical about it, he decided to give it a go. He signed up to a few different websites and posted an in-depth profile of himself as well as a photo on each of them.

1) What are some of the dangers that Alan needs to think about when using an online dating website?

Alan had received many different emails from girls all over the world. He was quite flattered at the interest his profile had sparked. While he wasn't interested in many of the people who had responded to him, there was one girl, Maya, that had sparked his interest. She lived in Africa and she had sent him a beautiful photo of herself. They had a lot in common and chatted on both the phone and internet everyday.

A few months down the track, Alan was talking to her one day when he noticed that she seemed upset. Although Maya said nothing was wrong, Alan didn't believe her and after a lot of coaxing, she told him that she had lost her job a few weeks ago and was unable to pay her bills. She said that she had been looking for another job, but it was tough and she was going to be evicted if she didn't pay up. Alan knew how upset she was. Having just received a promotion at work, he asked her how much she needed. At first, Maya refused to take his money, but Alan finally convinced her to borrow $5,000. She asked if he could send it her via Western Union, which he did that very same day.

2) What do you think about Alan's situation? Do you have any reason to suspect fraud?

After Alan sent the initial amount of money, things seemed to be good, although Maya had not yet been able to get a job. Then Maya contacted him to say that she was in a lot of trouble and needed his help. She told him that her father had been a heavy gambler and that he had suffered great losses. He had died the previous year, but she had just been visited by debt collectors who said that it was now her responsibility to pay his debt. She told Alan how these men had visited her house with guns and threatened her and the rest of the family unless they paid what he owed. She said they had given her a week to come up with the money. Alan asked her how much her father owed. She was silent for a moment, before she told him $50,000. Alan was shocked. He didn't have that type of money available to him. Maya was distraught and asked him to send whatever he could.

3) What should Alan do in this circumstance?

After a lot of thought, Alan was able to get $20,000 together for Maya. He wanted to transfer it into her bank account but she insisted that he transfer it via Western Union so that the debt collectors couldn't trace it. Maya said she had been able to pull together $10,000 and with Alan's money, the debt collectors should be happy with that. A few days later, Alan received a telephone call from a man saying that he had kidnapped Maya. He said that she had unpaid debts of $100,000 and unless Alan transferred the money to him, he would kill Maya. He gave him 48 hours to fulfil this. In the background, Alan could hear a woman screaming and he was certain it was Maya. He felt sick at the thought she was kidnapped, as well as knowing he didn't have that amount of money available.

4) What should Alan do in this circumstance?

Answers to revision questions

1) Social networking only occurs over the internet.

True **False**

Social networking occurs in real life as well and has done so for a long time. However, the internet has made communicating with a variety of people much easier and more popular.

2) Online communication is the same as face to face communication.

True **False**

Communicating online has some very different characteristics compared to talking face to face. When talking to someone over the internet, it is much harder to verify what they are saying. Online communication relies very heavily on people being honest about themselves, and this can be easily exploited.

3) Identity theft, fraudulent emails and malware are all things to look out for when using social networking sites.

True False

These are all things to look out for. Social networking sites are great to use but are also attractive for those who want to obtain your personal details and money.

4) You should respond to every email that you receive.

True **False**

There is no reason why you have to respond to every email that you are sent. If you receive a fraudulent email, the best thing to do is just delete it. You are not obligated to send a reply. Once you reply to a fraudulent email, the sender knows the email account is active and they will try very hard to get your personal details.

5) You may not know if your computer has malware installed on it.

True False

You can accidentally download malware onto your computer without knowing it. 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.

6) Information you post on the internet can only be seen by your contacts.

True **False**

Depending on your security settings, the information that you post on the internet can be seen by everyone. You need to think through the amount and type of information that you post about yourself on the internet. Once you have put something on the internet, you lose control over it.

7) Social networking sites are attractive targets for criminals.

True False

Social networking sites are very attractive targets for criminals. This is because they are very popular and have large numbers of people using them. There is also a wealth of information readily available on these sites. Social networking sites provide people with a means of communicating with others and trying to deceive them into sending personal details or money.

8) People post too much information about themselves on the internet.

True False

Many people post a lot of information about themselves on the internet. You need to think carefully about the level of information and the type of information that you post about yourself on the internet. Do people need to know everything?

9) Sending personal information over the internet is harmless.

True **False**

Personal information is just as valuable as money. It can be used in the same way as cash. It is important that you protect your personal information with the same level of security that you protect your money. Never send personal information in response to an email you

have received. No matter what the email says and how genuine it looks, it is very likely to be fraudulent.

10) There is nothing you can do to prevent identity crime.

True **False**

While there is never a guarantee that you won't become a victim of identity crime, there are many things you can do to protect yourself, such as limiting the amount of information that you post online; never responding to an email request for personal details; using the security settings on all of your accounts; and using strong passwords on your accounts.

Answers to the revision scenario

1) What are some of the dangers that Alan needs to think about when using an online dating website?

While online dating websites can be great ways to meet people, Alan needs to be careful about a few things. First, he needs to think about the amount and type of information that he puts in his profile. It may be tempting to post lots of details about himself, but the more he puts online, the more likely he is to become a victim of identity theft, or become a target for fraud. Alan also needs to think about the security settings offered by the website. He should look at these and change them to suit his needs and what he is comfortable with. Alan should also make sure that his anti-virus protection is up to date, and avoid responding to any emails which come with attachments or links, as these could potentially download malware onto his computer.

2) What do you think about Alan's situation? Do you have any reason to suspect fraud?

It is not surprising that Alan has found someone on the internet who has a lot in common with him. Online dating poses challenges in being able to verify the truth of the information that another person is presenting. If Alan put on his profile that he loves dogs and cycling, it would not be surprising for a reply to come from someone who also loves those things. It is very easy to give a person what they want when the face to face element is removed.

It is also not surprising that a request has come through for money. Although Maya did not directly ask Alan for money, it is likely her intention was always there. However, she played it in a way that she knew Alan would offer the money and remove the need for her to ask. If she asked, he may have said no, however by turning it on Alan to offer the money, she knows she is more likely to get it.

The fact that a request has come just after Alan has been promoted is no coincidence. It is likely that during their daily conversations, Alan shared with Maya his news of being promoted at work. Most people share what happens in their lives with those around them and it is likely that this occurred in this situation. It makes Alan a more attractive target for Maya and increases his potential value.

3) What should Alan do in this circumstance?

Alan should think very carefully before sending the money. Alan is accepting at face value everything about Maya and what she has said to him. He has no way of verifying any of the details that Maya has provided and is completely reliant on his trust in who she is. Online communication makes it very hard to verify the truth about a person, compared to face to face communication. If Alan does send the money, it is unlikely to resolve the situation and he is guaranteed to get more requests down the track for more. It doesn't matter who the person is and how well you think you know them, or what the story is, **you should never send money to a person in response to an email request.**

4) What should Alan do in this circumstance?

It is not surprising that Alan has been asked to send a larger amount of money. Even though he has sent through a previous amount, the request for more money was inevitable. Although it is hard to believe, criminals will use extreme stories and threaten violence to try and get money out of their victims. Criminals will manipulate people's emotions and their belief in the relationship. If Alan sends through the money as requested, it is unlikely to resolve the situation. It is very likely that in the future, something else will happen which requires Alan to send further amounts of money. It is likely that Maya has been defrauding Alan the whole time and has been cooperating with other men to make Alan believe that her life is in danger.

Alan should cease contact immediately and contact the police. Although it is very unlikely that he will ever get his money back, he should still notify the police that this has occurred. If Alan has provided any personal details to Maya, he should contact these agencies to let them know what has happened and change any passwords.

Alan is one of many people who get defrauded through an online relationship. Criminals will use whatever means possible to try and get a victim to send money, and if this means manipulating their emotions in extreme ways, they will always do this. Their goal is to get money and they don't care how they achieve this. It is very important to remember that you should never send money from an email request, no matter who is asking for it and why they need it. It will almost always end in heartache.

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.