SENIORS ONLINE SECURITY

Fraudulent Emails

4 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

Fraudulent emails
A training guide for seniors

#4 out of 5 training guides available

This training guide provides Australian Seniors with information about fraudulent emails as well as strategies to protect themselves from responding.

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 problem of fraudulent emails

Too often, emails that appear in our inboxes aren't what they seem. While you might get lots of emails from family, friends and from mailing lists that you have signed up to, there are also often a lot of emails from people you don't know. These emails usually ask you to send through personal details about yourself, whether it is your name, address and birth date or other more personal things, like drivers licence number or bank account details. The emails might also ask you to send money, even if it is a small amount. The emails may seem genuine, but unfortunately they are not. This module will show you how to protect yourself when using email.

Overview of this training module

This module looks at different types of fraudulent emails that ask for personal information or money. By the end of this module you will be able to:

- → Understand what is meant by the term advanced fee fraud;
- → Understand what is meant by the term phishing;
- → Name the different ways in which these emails appear in our inbox;
- → Understand why people respond to fraudulent emails;
- → Know what to do if you think you have received one of these emails; and
- → Know who to contact if you have responded and think you may have become a victim.

This module will give you information and simple strategies on how to protect your personal information and money when using email.

What is advanced fee fraud?

While it might seem like a complicated concept, advanced fee fraud is quite simple. Essentially, it is an email which asks you to send through a small amount of money, promising the return of a larger amount of money.

All advanced fee fraud schemes will ask for what seems like a small amount of money upfront, in order for you to claim a larger amount. Unfortunately, once you have sent the first amount of money, further requests will always come through asking for more. There will always be another tax, or a release fee, or an administration fee, or another reason why you can't receive your money, and why you need to send more. Once a person is caught up in this, it is very difficult for them to get out, and victims can lose tens of thousands, hundreds of thousands, or even millions of dollars as a result.

This type of fraud is not new and has been around for a long time, even before the internet. However, the internet has made it easier for people to send these types of frauds out to the masses, for relatively little cost. A person might send out 1,000 emails, and if they only get a couple of responses, it makes it worth their while.

Advanced fee fraud can come in a lot of different forms. Some of the most popular ways are described here:

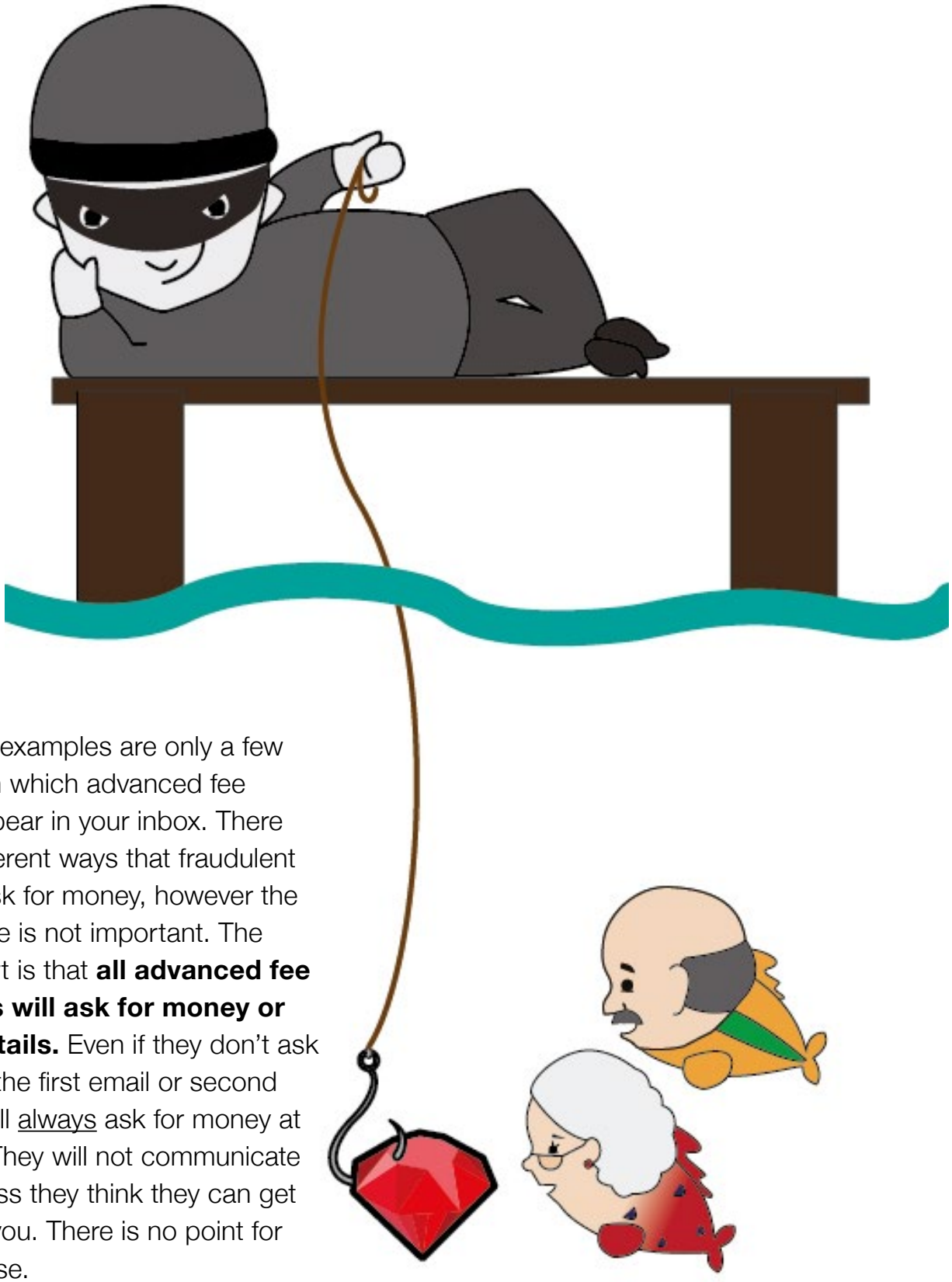
Lottery: You receive an email, congratulating you as the winner of a lottery. You are asked to send an amount of money (administration fees or taxes) for your prize to be released.

Inheritance: You receive an email notifying you as the beneficiary to a deceased estate (the deceased person may or may not have your surname). You are asked to send an amount of money (death certificate, taxes, administration fees etc) for the estate to be released to you.

Investment: You receive an email presenting you with an opportunity to invest in a new business venture. You are asked to send through an amount of money in order to buy into this opportunity.

Charity: You receive an email asking you to contribute to a special cause or charity. You are asked to send an amount of money to show your compassion towards the cause.

Romance: You are involved in a relationship with someone you met online. After a while, you receive an email from them detailing something bad which has happened to them or a family member (an accident or an illness). You are asked to send money to assist them (for example with medical costs).



The previous examples are only a few of the ways in which advanced fee fraud can appear in your inbox. There are many different ways that fraudulent emails can ask for money, however the story they give is not important. The important part is that **all advanced fee fraud emails will ask for money or personal details.** Even if they don't ask for money in the first email or second email, they will always ask for money at some point. They will not communicate with you unless they think they can get money from you. There is no point for them otherwise.

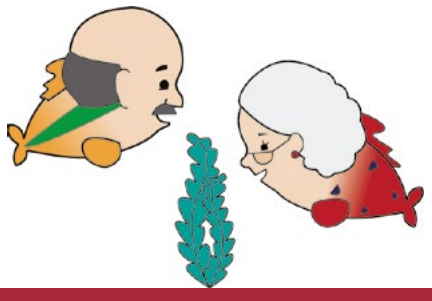
Later in this module, we will look at what you can do if you think you have received an advanced fee fraud email. In the next section we will look at a different type of fraudulent email.

What is phishing?

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, your telephone or internet service provider, or any other institution that you do business with. They might claim that there has been a problem with your account, and that it has been suspended. They might claim that the business has lost your details and needs you to reconfirm them. Similar to the advance fee fraud emails in the previous section, 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.** This can either be through responding to the email they have sent you, or it could be through clicking on a link they have put in the email. If you click on the link, it will take you to a page that looks real, but it is not. They will then use your personal details to access your existing money or they might set up new accounts or lines of credit in your name.

You might not think that personal information is important, or that it is valuable to anyone but yourself. However, this is not true. Sending personal information is the same as sending money. Your details can be used in the same way as cash. Your personal details are as important to you as the money which is in your bank account, which is why it is just as important to protect them.



Revision questions

The following questions are to see how well you have understood the concepts of advanced fee fraud and phishing.

Each question has multiple options but there is only one correct answer. Answers to these questions can be found at the back of this booklet.

Question 1

What is advanced fee fraud?

a) A computer virus

b) Emails which ask for a small amount of money to obtain a larger amount of money

c) Emails which tell a funny story

d) A chain letter

Question 2

What are the different types of advanced fee fraud?

a) Lottery and Investment

b) Inheritance

c) Any email which asks for personal information or money

d) All of the above

Question 3

If the email just asks for personal information, is it ok to respond?

a) Yes, sending personal information is harmless

b) Yes, because the sender just wants to be friends with you

c) No, because personal information is just as important as money

d) No, because you would rather send money

Question 4

What is a phishing email?

a) An email which talks about fishing

b) An email from a business that asks you to confirm your personal information

c) An email from the bank which asks you for money

d) A computer virus

Question 5

What are the characteristics of a phishing email?

a) Terrible spelling and grammar

b) The use of real company logos

c) There are no specific characteristics

d) All of the above

Question 6

How do people receive advanced fee fraud and phishing emails?

a) They are randomly generated

b) They are targeted at specific people and groups

c) Both a) and b)

d) Neither a) nor b)

How to protect yourself from responding to fraudulent emails

The first part of this booklet has looked at what is meant by the terms advanced fee fraud and phishing. These types of emails may appear in your inbox from time to time and it is important to be able to recognise them. This next section looks at simple ways in which you can protect yourself from responding to these emails.

USE AN EMAIL FILTER

Email filters are a good way of stopping some of these 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 advanced fee fraud and phishing 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.

USE THE DELETE KEY

The delete key can be your best friend when managing your emails. If you receive an email from a person or a company that you don't know or recognise, the safest option is to delete it. If the email is really important, the person or company will find another way to contact you. Don't be afraid to delete an email without reading it. There is no reason why you have to read every email you receive. There is also no reason why you have to reply to every email. You may think you are being polite in responding to every email, but this isn't necessary. If you respond to a fraudulent email, the sender will know the account is active. They will try to keep contact with you, to get your personal details or money. The easiest and safest option is simply to delete emails from those you don't know or are not expecting.

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 you have to reply just because the 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 for it and what it is for.

There are so many ways that other people will try to get money from you. It may come under the premise of a lottery win, through the promise of an inheritance, through the presentation of a job opportunity or investment, or it might come from a person you believe you are in a relationship with. It might come in any number of other ways that haven't been mentioned here. How you are 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 it. If you are unsure about the legitimacy of the request, take your time to do your research.

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 ask for advice. 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.

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

People are not perfect and there may be times where despite your best efforts, you have responded to a fraudulent email. You may have sent personal details or you may have sent an amount of money. If this is the case, the most important thing is not to panic. There are some steps you can take to minimise what has happened. The following section looks at the importance of reporting your crime and what you can do to avoid it happening again.

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. The type of information you sent, will determine what you need to do.

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

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

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

IF YOU HAVE SENT MONEY...

If you have sent money as the result of an email request, 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), then 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 at all. If you have sent money within Australia, police are more likely to able to investigate this.

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.

A NOTE ABOUT ONLINE FRAUD VICTIMISATION

There are a lot of myths around online fraud victimisation, which are not helpful for people who find themselves in these situations. The following section outlines some of these myths and how you can help to overcome them to improve the situation for online fraud victims.

Once a person realises that they have become a victim of online fraud, there are a number of emotions the person might feel. For example, the victim may feel embarrassed, ashamed, silly, anxious, scared, angry or depressed. It is important to know that thousands of people respond to fraudulent emails. While nobody you know may have told you, chances are someone you know has responded at some point. Many victims will blame themselves for what happened.

It does not devalue the person in any way. All types of people can become victims, young and old, educated or not, professionals or tradespeople. There is no one group who is immune to this type of victimisation. Some very smart people, in very powerful positions have become victims of fraud. They are still smart people despite responding to a fraudulent email.

Many people think that victims of online fraud are easily deceived, greedy and that they deserve what happens to them. This is simply not the case. Victims generally believe in the truth of the person they are communicating with and the legitimacy of their situation. It is only down the track, when they have lost large amounts of money, that they realise it was all not true. This can have devastating consequences on the victim and their families.

Many people also think that victims of fraud only lose money. The truth is that they lose so much more. Online fraud victimisation can affect a person's health. A lot of victims suffer from depression. It also puts stress on a person's relationship with their family and friends. Imagine that you are the breadwinner of the family and you have lost tens of thousands of dollars to fraud. Imagine that you have lost your life savings and your superannuation to your involvement in fraud. Imagine having to tell your family that all the money you had saved, and that they had saved, is gone. Imagine realising that a person you trusted had so badly deceived you. This has a huge impact on the victim and it also has a huge impact on their family.

The majority of online fraud victims will never tell their families the true extent of what has happened. They feel too ashamed and too embarrassed to share their experiences with those they love about being tricked by another person. Many will suffer in silence because they are afraid of how their families and friends would react. They feel that their family and friends will not understand and will further stigmatise and isolate them.

From the outside, sometimes it is hard to understand how a person can become involved in fraud and lose such large amounts of money, over such a long period of time. However, we have to remember that everyone has a weakness and vulnerability, and unfortunately, there are people who will exploit this. People don't plan to become victims of online fraud, but when it happens, they need to be able to trust those around them for support and for assistance to get their lives back on track.

If someone you know tells you about their involvement in online fraud, understand that it is not easy for them to tell you this. Try not to be angry or upset with the person, as generally they are already going to feel this themselves. Listen to their story and try not to judge their actions. Victims need support and reassurance from those around them, in order to be able to move forward. Encourage the person to get help where needed and report the matter to their local police. It is likely to be a tough journey ahead, but if the victim believes they have the support of those around them, it will certainly make it a little bit easier.

Conclusion

This module has looked at advanced fee fraud and phishing emails. By now, you should have a good understanding what is meant by these concepts. There are so many different ways that the emails can appear in your inbox and they will be constantly changing. However, there are simple steps that you can take to avoid replying to one of these emails.

This booklet has looked at ways to try and avoid responding to advanced fee fraud or phishing emails. If you ever receive an email asking for personal details or an amount of money, no matter who the email is from or what the email says, you should stop and think twice before replying. It doesn't matter how you are approached, the goal of the email is to get your personal details or your money, and this is what you want to avoid.

As a rule, you should never send personal details or money in response to an email. No matter who the email is from, or what reason is given for wanting the money, it is very likely to be fraud. There are hundreds of different stories and thousands of different lies which can be used to try and convince you the truth about a situation. You don't have to reply to every email you receive and you certainly don't have to send something just because you are asked to.

However, this booklet has also looked at what you can do if you become a victim of online fraud. Despite their best intentions, some people will respond to an email, believing it to be true. Some people will send personal details or money, and this does not mean that they are silly or greedy or deserving of victimisation. In fact it is quite the opposite. Victims need to be supported and encouraged to report the incident. This booklet has outlined some of the things which victims should do if they believe they have been defrauded.

The use of email is a great way to keep in touch with your family and friends. Most of the time, the emails you receive will be those you want to read. However, you are likely to receive unwanted emails in your inbox from time to time, and these emails will try to get your personal details or your money. By remembering the rule of not sending personal details or money to anyone who sends you an email, you can protect yourself, your personal details and your money, and continue to enjoy communicating with your family and friends.

Revision scenario

Alan received an email from a solicitor notifying him that he was the beneficiary to an inheritance. The deceased person had his family name and he vaguely recognised the name as a distant relative. The email asked Alan to reply by email to indicate that he had received this notification. Seeing as though the email didn't ask for anything, Alan didn't see the harm in responding.

1) Do you agree with Alan's actions? What should he be careful of in the future?

Alan received a reply to his email straight away. The email confirmed that he was the beneficiary to the estate of the deceased. It outlined details of the financial and property holdings that were left by the deceased. It also outlined the process for Alan to claim the estate. It listed the various administrative steps that were required, as well as the cost associated with this. There were taxes listed as well as administrative fees, which totalled approximately $8,000. The solicitor stated that he had been close friends with the deceased and as a result was not charging for his services. The costs were only those which were necessary and were dictated by the government.

Alan was unsure about this. He spoke to his family and they were also a little sceptical. The email had a phone number, so Alan decided to call the number and speak to a person. He called the number and the solicitor answered his call. He was a very friendly man, who was able to confirm all the details of the email and reassure Alan of the validity of his claim to the inheritance. Alan also thought he was very kind not to be charging for his own services. After this phone call, Alan felt better about the situation and transferred the $8,000 via a wire transfer as requested.

2) Why do you think that Alan eventually sent the money as requested? What do you think the consequences will be for Alan?

A few days later, Alan received another email from the solicitor. It said that there had been a few changes in the schedule of taxes relating to the deceased. There had been an increase in fees and the addition of a death benefits tax, which had previously not existed. Lastly, there was a fee to release the death certificate overseas. With the administration fees associated with these new taxes, there was now an outstanding amount of $15,000. This needed to be paid before Alan could access the full amount of the estate. Alan was shocked. He hadn't thought he would have to pay any further costs. He phoned the solicitor and asked him to take this amount out of the full value of the estate. However, the solicitor said that this was not possible, as the estate was currently frozen and the fees had to be paid prior to this being released. Alan hung up, very frustrated at what was happening.

A few hours later, Alan received a phone call from the solicitor who said that he had spoken with the government department and was able to negotiate a settlement of $12,000. This would guarantee that the remainder of the estate could be released by the end of the week. While Alan was still angry at having to pay more money up front, considering he had already invested $8,000, he agreed to pay the $12,000. He went to the bank to arrange a loan, given that the money he would receive at the end of the week would more than cover these expenses.

3) What do you think will be the outcome of Alan's decision to send more money? What do you think will be the consequences of his actions?

Answers to revision questions

Question 1

What is advanced fee fraud?

a) A computer virus

b) **Emails which ask for a small amount of money to obtain a larger amount of money**

c) Emails which tell a funny story

d) A chain letter

Advanced fee fraud emails are those which ask for a small amount of money at first, with the promise of a larger amount of money in the long term. However, once a first payment is made, further payments are required and the larger amount of money never eventuates. Victims can lose large amounts of money trying to get the amount they were first promised.

Question 2

What are the different types of advanced fee fraud?

a) Lottery and Investment

b) Inheritance

c) Any email which asks for personal information or money

d) **All of the above**

There are common types of advanced fee fraud schemes, such as investment, lottery, investment, job advertisements, and romance fraud. However, this list is not exhaustive and advanced fee fraud can take on any form. The way it is presented is not important, the fact that it will always ask for a small amount of money in return for a larger sum of money is what must be remembered.

Question 3

If the email just asks for personal information, is it ok to respond?

a) Yes, sending personal information is harmless

b) Yes, because the sender just wants to be friends with you

c) **No, because personal information is just as important as money**

d) No, because you would rather send money

Personal information is just as valuable to offenders as cash. Sending personal details may seem harmless, but offenders can use these to access your money and set up new accounts or lines of credit and loans in your name. Personal information can also be traded between criminals in the same way that money can be exchanged. It is important to protect your personal information in the same way that you protect your money.

Question 4

What is a phishing email?

a) An email which talks about fishing

b) **An email from a business that asks you to confirm your personal information**

c) An email from the bank which asks you for money

d) A computer virus

A phishing email is one that looks like it has come from a legitimate business and asks you to confirm or provide personal details. It might come from a bank, a telephone service provider, an internet service provider or another financial institution. It may ask you to respond to the email or provide a link that will take you to a fake website. Phishing emails look genuine but they are not. Real companies will never ask you to send personal details in an email.

Question 5

What are the characteristics of a phishing email?

a) Terrible spelling and grammar
b) The use of real company logos
c) There are no specific characteristics
d) **All of the above**

There are no specific characteristics to a phishing email. Sometimes they will have spelling mistakes, but other times they will not. They will generally use a company logo to increase the chance you think it to be true. Whatever the email looks like, it is important to know that it will always ask you for personal details. These should never be provided over email.

Question 6

How do people receive Advanced Fee Fraud and Phishing emails?

a) They are randomly generated
b) They are targeted at specific people and groups
c) **Both a and b**
d) Neither a nor b

Fraudulent emails can be random or targeted at specific people. Random emails will be sent to a large number of people, in the hope that a few reply. In other instances, a person or a group may be targeted in a specific way to increase the chance that they reply. Regardless of how the email ends up in your inbox, it will always ask for money or personal details, and these should never be provided.

Answers to the revision scenario

1) Do you agree with Alan's actions? What should he be careful of in the future?

The inheritance email that Alan has received is an example of an advanced fee fraud email. The fact that the deceased has Alan's surname could have occurred one of two ways. The first is that Alan has a common surname and it is just coincidence that this has occurred. The second way is that he has been specifically targeted by criminals who have been able to access details of his family history. A growing number of people have large amounts of information about themselves and their families posted on the internet, and this can increase the chances that they are targeted like this.

Even though the initial email does not ask for anything, if Alan replies to this email, he is guaranteed to receive a request for money in future emails. Sometimes criminals will not ask for money straight away to increase the chances that a person responds. However, the request for money will always come, as that is the sole purpose of these emails.

2) Why do you think that Alan eventually sent the money as requested? What do you think the consequences will be for Alan?

As expected, once Alan replied to the email, he received a request to send money. This is said to cover taxes and administration costs associated with the estate. This is a plausible reason for Alan to send money, and the amount requested is not too big for him to immediately raise suspicion. It is also not surprising that the phone number provided in the email led to the solicitor. You should never contact people through phone numbers that they have provided, as they do not help you to verify the information being presented.

Criminals are very good at manipulating people's emotions and getting them to do what they want. In this situation, the solicitor has told Alan that he is not charging a fee for his services, because he was so close to the deceased. Alan, believing this to be a sign of the solicitor's character, has increased the trust he has placed in him. Often criminals will use these types of means to gain a person's trust.

Even though Alan has transferred the initial amount of money as requested, he will not receive the estate as promised. Further problems are guaranteed, which will require more money to release the estate. Once a victim has sent one payment, offenders will do whatever it takes to get more money out of the victim.

3) What do you think will be the outcome of Alan's decision to send more money? What do you think will be the consequences of his actions?

As expected, there has been a new problem which requires a further payment to secure the release of the estate. In these types of circumstances, it is very difficult for the victim to be able to verify the truth of what they are being told. It is hard to research the processes and fees of other countries and to understand the legal processes surrounding a person's death. This lack of knowledge works in favour of the criminals who can present changes like this one, and get further money out of the victim.

It is also not surprising that the solicitor has apparently negotiated a reduction in fees from $15,000 to $12,000. This is meant to indicate to Alan that the solicitor is on his side and has been able to reduce the overall payment required to release the estate.

Many victims will continue to send small amounts of money, because they have already invested part of their own finances in the process. Many victims will take out loans and mortgages and borrow money from others in order to pay the fees requested. They believe that when they receive the funds as promised, they will easily clear their debt. However, the amount of money requested by the offenders continues to increase as does the amount of debt incurred by the victim.

Despite the promise of releasing the estate by the end of the week, this will not occur. If Alan sends through the $12,000 as requested, there will be another problem or drama which requires further money. Alan should cease all contact with the solicitor and refuse to send any further payments. He should then contact both his bank and the police to report this crime.

It is sometimes hard to understand how people like Alan get caught up in these types of fraudulent situations. However, we must remember that the criminals involved in these situations are very skilled at what they do and are very skilled in manipulating people and their emotions. The best advice is to not reply to the initial email. Once contact has been made with the offenders, they will do everything possible to try and trick the victim into sending them large amounts of money.


FREE
Golden Ticket

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.