SENIORS ONLINE SECURITY

Five Distinct Areas

- Computer security
- Identity crime
- Social networking
- Fraudulent emails
- Internet banking

Computer security

An awareness of computer security

- There are several ways that the security of your computer can be broken:
  - Malware
  - Identity Crime
  - Fraudulent Emails
  - Unsecured Networks
- However, each of these can be overcome with a few simple steps.

Malware

- Short for “malicious software”, malware is designed to disrupt the normal running of your computer.
- Malware comes in many forms, each with a different purpose.
- Malware can be downloaded from an attachment or through visiting a compromised website.
- You might not know your computer is infected.

Identity crime

- Identity crime is the unauthorised use of your personal details, to commit fraud or other crimes.
- One of the most common types of identity crime is the use of stolen credit card details to purchase goods or services.
- People store a lot of personal information on their computers, therefore it is important to protect this.

Fraudulent emails

- These types of emails will appear in your inbox and can look genuine.
- They might come from your bank, or another organisation, which you do business with, and ask you for personal information.
- They might also come as an email with an attachment, which if opened, will infect your computer with malware.

Unsecured networks

- Many people have wireless networks at home which allows more than one person to access the internet at the same time.
- If this network is not secured, then anyone can use the internet connection, the internet download allowance and access information stored on the computer.

How to protect your computer

- There are several strategies that can help you protect your computer.
- By following these simple steps, you can greatly reduce the likelihood that your computer security is broken.

10 steps to protect your computer

1) Use antivirus protection and have an active firewall
   - Install and regularly update antivirus protection and a firewall.
   - Regularly scan your computer and back up data.
2) Regularly update your software
   - Update software, as newer versions will fix weaknesses and problems in earlier versions.

10 steps to protect your computer

3) Never reply to an email with personal details
   - Fraudulent emails will not always be obvious.
   - Personal details should be guarded in the same way as money.
   - Talk to someone if you are unsure of an email.

4) Use a strong password
   - Try to use different passwords, that contain at least 8 characters and a combination of letters, numbers and symbols.

10 steps to protect your computer

5) Use an email filter

- An email filter can automatically delete fraudulent emails before they reach your inbox.
- However, just because an email is in your inbox, doesn't mean it isn't fraud.

6) Avoid clicking on links in emails

- Clicking on links in emails from people you don't know can take you to an infected website and allow malware to download on your computer.

10 steps to protect your computer

7) Avoid opening email attachments

- Email attachments may seem harmless but they can have malware in them, which once opened will infect your computer.
- Always scan an attachment before opening it.

8) Secure your own network and use a firewall

- This will only allow authorised people to access your network and your internet connection.

10 steps to protect your computer

9) Avoid using public unsecured networks

- Wherever possible, use your own secured network, that you can control.
- If using a public network, avoid doing things like internet banking.

10) Surf safely

- The internet is a great resource, but try to stick to reputable websites, particularly when giving personal information (such as credit card details).

If your computer is not secure…

- There are steps you can take if you think your computer security has been broken.
  - Don’t panic or ignore it!

1) Malware
   - Scan your computer with antivirus protection.
2) Personal details compromised
   - Contact relevant agencies to cancel accounts or change passwords.

Identity crime

What is identity crime?

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

Identity fraud, refers to when a person obtains money, goods, services or other benefits, by using a false identity. A common type of identity fraud, is the misuse of a person's credit card details.

Identity theft, refers to when a person steals another's person's details, or information, in order to gain money, goods, services or other benefits. It includes the unauthorised use of a person's identity, living or dead.

Losing control of your identity

- There are several ways, in which your identity, can be compromised:
  - Posting too much information on the internet
  - Fraudulent emails
  - Malware
- However, these can be overcome with a few simple steps.

If you think you are a fraud victim

- There are steps you can take if you think that you may have become a victim of identity crime.
  - Don’t panic or ignore it!

1) Your personal details have been compromised
   - Contact relevant agencies to cancel accounts or change passwords.

If you think you are a fraud victim

2) Have you noticed suspicious/unauthorised activity on your account?
   - Contact the relevant organisation immediately to cancel your cards and change your passwords.
3) Have you received a bill or statement that isn't yours?
   - Contact the relevant agency immediately to find out what has happened.

Reporting Fraud

- You can report fraudulent emails to the Australian Communications and Media Authority via email at:

  report@submit.spam.acma.gov.au

- You should report financial theft to the police.

Posting information on the internet

- One of the biggest threats to our identity, is placing excessive amounts of information on the internet, with inadequate security settings.
- The internet isn't as private as we might think, and our information can be viewed by people other than our contacts.

Fraudulent emails

- These types of emails will appear in your inbox and can look genuine.
- They might come from your bank or another organisation that you do business with and ask you for personal information.
- They might ask you to reply to their email or they might provide a link to provide your personal details.

How to protect your identity

- There are several strategies, which can help you, protect your identity.
- By following these simple steps, you will greatly reduce the likelihood that your identity is compromised.

Steps to protect your identity

1) Limit what details you put on the internet
   - Carefully consider the amount and type of information that you make available to others.
2) Never reply to an email with personal details
   - Fraudulent emails will not always be obvious.
   - Personal details should be guarded in the same way as money.
   - Talk to someone if you are unsure of an email.
   - Don’t feel pressured to respond.

Steps to protect your identity

3) Knowing and using security settings

- Make sure that you have security setting activated on all your accounts and profiles.
- Don’t rely on the default setting as this may not be as secure as you think it is.

4) Use a strong password

- Try to use different passwords, that contain at least 8 characters and a combination of letters, numbers and symbols.

Steps to protect your identity

5) Use antivirus protection and have an active firewall
   - Install and regularly update antivirus protection and a firewall.
6) Avoid using public computers
   - Wherever possible, use your own secured network, which you have control over.
   - If using a public network, avoid doing things like internet banking.

Steps to protect your identity

7) Carefully select the websites you use
   - The internet is a great resource, but try to stick to reputable websites particularly when giving over personal information (such as credit card details).
8) Monitor your accounts and statements
   - Regularly check your accounts, to ensure that the only transactions that appear, are those which you have authorised.

Steps to protect your identity

9) Destroy your personal information appropriately
   - Keep valuable documents with personal details on them in a safe place.
   - Shred all of your documents before placing them in the rubbish.

Social Networking

What is social networking?

- It is all about connecting and communicating with people.
- It isn't just confined to the internet, however the internet has increased the ease and popularity of communication.
- It operates through various websites where people can post profiles and initiate/receive contacts from other people.

Online communication

- It is all about connecting and communicating with people.
- It isn't just confined to the internet, however the internet has increased the ease and popularity of communication.
- It operates through various websites, where people can post profiles, and initiate/receive contacts from other people.

An awareness of social networking

- Social networking sites are a great way to communicate with people, but there are a few issues you need to be aware of:
  - Identity crime
  - Fraudulent emails
  - Malware
- These are discussed earlier in the presentation.

How to protect yourself on social networking sites

- There are several strategies, which can help you protect yourself, when using social networking sites.
- By following these simple steps, you will greatly reduce the likelihood that you become a victim of a crime while communicating with people on social networking sites.

Protecting yourself while social networking

1) Limit what details you put on the internet
   - Carefully consider the amount and type of information that you make available to others.
2) Knowing and using security settings
   - Make sure that you have security setting activated on all your accounts and profiles.
   - Don’t rely on the default setting as this may not be as secure as you think it is.

Protecting yourself while social networking

3) Use a strong password

- Try to use different passwords that contain at least 8 characters and a combination of letters, numbers and symbols.

4) Avoid clicking links in emails

- Clicking on links in emails can take you to an infected website and allow malware to download on your computer.

Protecting yourself while social networking

5) Never reply to an email with personal details
   - Fraudulent emails will not always be obvious.
   - Talk to someone if you are unsure of an email.
   - Don’t feel pressured to respond.
6) Never send money in response to an email
   - The situation may seem genuine and you may trust the person, but once you have sent the money there is no way to get it back.

Online dating sites

- These are legitimate ways to meet people.
- However, criminals can use these sites to gain money from unsuspecting victims.
- They seek to manipulate a person's good will and their emotions and exploit the relationship.
- This can have a devastating effect on victims.
- Be extra cautious when using these sites.

If you think you are a fraud victim

- There are steps you can take if you think that you may have become a victim of fraud on a social networking site.
  - Don’t panic or ignore it!

1) Contact the social networking site.
   - Most sites have a way to report someone to investigate having them removed or blocked.
2) Use the delete key.
   - Delete people from your contacts.

If you think you are a fraud victim

3) If you have sent money, there are a few steps you can take:
   - Contact your bank and see if the transaction can be cancelled.
   - Contact the wire transfer service to see if the transaction can be cancelled.
   - Contact the police to report your loss.

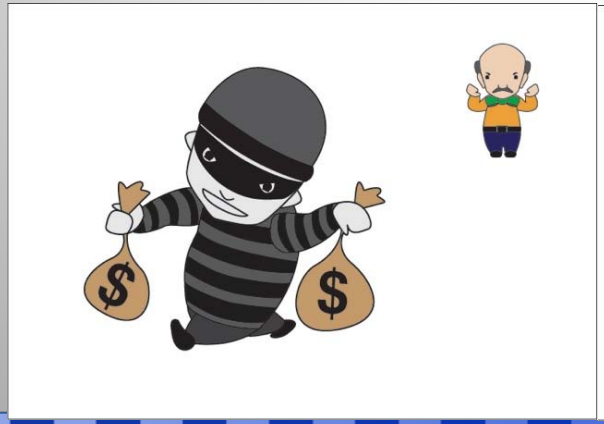
You are unlikely to get the money back, but it is important for you to report it.

Reporting Fraud

- You can report fraudulent emails to the Australian Communications and Media Authority via email at:

  report@submit.spam.acma.gov.au

- You should report financial theft to the police.



Fraudulent Emails

What is advanced fee fraud?

- It is an email that asks for a small amount of money, with the promise of a larger amount of money in the future.
- Once you send an initial amount, there will always be requests for further money and you will never receive the larger promised amount.

What is advanced fee fraud?

- There are many ways that these emails can appear in your inbox, but no matter what the story, all emails will ask for money.
  - Lottery notifications
  - Inheritance notifications
  - Investment opportunities
  - Charity contributions
  - Romance fraud

How to protect yourself from fraud

- There are several strategies which can help you protect yourself from responding to a fraudulent email.
- By following these simple steps, you will greatly reduce the chances of this occurring.

Protecting yourself from fraud

1) Use an email filter
   - An email filter can automatically delete fraudulent emails before they reach your inbox.
   - However, just because an email is in your inbox, doesn't mean it isn't fraud.
2) Use the delete key
   - Never be afraid to delete an email that you are suspicious of.
   - You are not obliged to reply to an email, just because it has been sent to you.

Protecting yourself from fraud

3) Never reply to an email with personal details
   - Fraudulent emails will not always be obvious.
   - Talk to someone if you are unsure of an email.
   - Don't feel pressured to respond.
4) Never send money in response to an email
   - The situation may seem genuine and you may trust the person, but once you have sent the money there is no way you can get it back.

If you think you are a fraud victim

- There are steps you can take if you think that you may have become a victim of fraud.
  - Don’t panic or ignore it!

1) If you have sent personal details
   - Contact relevant agencies to cancel accounts or change passwords.

If you think you are a fraud victim

2) If you have sent money, there are a few steps you can take:
   - Contact your bank and see if the transaction can be cancelled.
   - Contact the wire transfer service to see if the transaction can be cancelled.
   - Contact the police to report your loss.

You are unlikely to get the money back, but it is important for you to report it.

Online fraud victimisation

- It is hard to understand how a person becomes a victim of this type of fraud.
- This type of fraud can have devastating consequences for victims, which are more than just financial losses.
- Most victims feel too embarrassed or ashamed to tell anyone (including police) and don’t get the help and support they need.

Internet Banking

What is internet banking?

- It allows customers to conduct some of their banking through their financial institution's website.
- While you cannot physically withdraw money, there are a range of other transactions which can be done (transfers, payment of bills).
- It is available 24/7, 365 days per year.

An awareness of internet banking

- While internet banking provides an opportunity to do a range of transactions from the comfort of your own computer, there are a few issues to be aware of:
  - Phishing emails
  - Malware
- However, each of these can be overcome with a few simple steps.

Phishing emails

- Phishing emails will ask you to provide your personal information.
- It might be from a bank or other financial institution.
- It might look genuine and seem plausible.
- It might ask you to reply to the email or provide a link for you to enter your personal details.

How to protect yourself when banking

- There are several strategies which can help you protect yourself when using the internet to do your banking.

Protecting yourself when banking

By following these simple steps, you will greatly reduce the chances of something adverse happening to you.

1) Use antivirus protection and have an active firewall
   - Install and regularly update antivirus protection and a firewall.
   - Regularly scan your computer.

Protecting yourself when banking

2) Avoid using public computers
   - Wherever possible, use your own computer as you know what security mechanisms you have in place and the current state of your computer security.
3) Never reply to an email with personal details
   - Fraudulent emails will not always be obvious.
   - Personal details should be guarded in the same way as money.
   - Talk to someone if you are unsure of an email.

Protecting yourself when banking

4) Never provide your personal details through an email link
   - The link is likely to take you to a fraudulent website which will capture your personal details for another person to use.
5) Use strong passwords
   - Try to use different passwords that contain at least 8 characters and a combination of letters, numbers and symbols.

Protecting yourself when banking

6) Monitor your accounts and statements
   - Regularly check your accounts to ensure that the only transactions which appear are those which you have authorised.
7) Take advantage of extra protection for your accounts.
   - Many banks and other financial institutions offer extra security features for internet banking, such as confirmation text messages or tokens which generate one time only passwords.

Conclusion

- The internet has great benefits in terms of communicating, doing business and being entertained.
- By following the steps outlined in this presentation, you should be able to enjoy the internet in a confident and safe manner!

Important information

- A copy of this presentation is available for download at:

http://communitysafety.police.wa.gov.au

Further information…

For more information about online security issues,

go to:

www.scamwatch.gov.au

www.cybersmart.gov.au

For more information about computers and technology,

go to:

www.ascca.org.au

Acknowledgements: Queensland University of Technology and Queensland Police