Australian Government

Protecting Yourself Online

What Everyone Needs to Know

Australian Government

Protecting Yourself Online

What Everyone Needs to Know

ISBN: 978-1-921725-20-3

© Commonwealth of Australia 2010

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney General's Department, National Circuit, Barton ACT 2600 or posted at http://www.ag.gov.au/cca

Disclaimer

The information in this publication is solely intended to provide a general understanding of the subject matter and to help people assess whether they need more detailed information.

The material presented in this publication is not and must not be regarded as legal advice. Users should seek their own legal advice where appropriate.

While everything practicable has been done to ensure the information in this book is accurate, no liability is accepted for any loss or damage whatsoever that can be attributed to reliance on any of that information.

Introduction

We have openly welcomed the internet into our lives.

For most of us the internet is part of our daily routine for keeping in touch with friends and family, working, studying, shopping and paying bills.

While the internet offers us many benefits, there are also a range of safety and security risks associated with its use.

These include threats to the integrity of our identities, our privacy and the security of our financial transactions, as well as exposure to offensive and illegal content and behaviour.

To help keep all Australians safe and secure online, the Australian Government offers a range of information and advice from a number of different sources, including the

- Attorney-General's Department
- Department of Broadband, Communications and the Digital Economy
- Australian Communications and Media Authority
- Australian Competition and Consumer Commission
- Australian Federal Police, and
- Office of the Privacy Commissioner.

This publication brings a lot of this information together in one handy booklet, to help you stay safe and secure when using the internet – whether dealing with scams, spam, banking or bullying.

Reduce your risk

There are no absolute guarantees that you can protect all of your information online – but by following the advice in this booklet you can significantly reduce your risk of becoming a victim of cyber crime.

A bit unsure?

Taking the necessary steps to protect yourself online can be a bit daunting – especially to those less familiar with technology or internet jargon. However, there are simple steps you can take to protect yourself online.

By taking the time to understand online risks and how to minimise them, you can gain greater confidence in how to be safe and secure when using the internet.

This booklet provides a range of information to help protect you online

- **six simple tips** that you should always follow
- further information on various online issues, including **basic steps** that you are strongly encouraged to take
- some sections of this booklet also provide **additional information,** for those of you who may wish to take further precautions.

You can also refer to the glossary at the end of this booklet, to help you understand some online terms, including those marked throughout this booklet.

Read on to find out what you need to know to help protect yourself online.

Contents

A summary

There are a lot of steps you can take to protect yourself online – and it can seem a bit complicated, especially if you are new to using the internet.

This booklet provides a range of information to cater for you – no matter how experienced or inexperienced you are.

Whether you are new to using the internet or a regular user – there are **six simple tips** that you need to follow to help protect yourself online

1 install security software and update it regularly

2 turn on automatic updates so all your software receives the latest fixes

3 set a strong password and change it at least twice a year

4 stop and think before you click on links or attachments

5 stop and think before you share any personal or financial information – about you, your friends or family

6 know what your children are doing online – make sure they know how to stay safe and encourage them to report anything suspicious.

What these steps show is that protecting yourself online is about more than just how you set up and use your computer or mobile phone. It's also about being smart in what you do and the choices you make while using the internet.

There are criminals who use the anonymity of the internet to run old and new scams. Many of these are scams that most people would spot a mile away if they were attempted in the 'real world'.

So it's important to remember that while the technology may be new, the old wisdom still applies. If something you see online seems suspicious or too good to be true, it probably is.

Further information on the steps you can take to be safe online are provided in the following chapters.

This booklet is available online at **www.ag.gov.au/cybersecurity** and **www.staysmartonline.gov.au.**

How to secure your computer

The average time it takes to attack an unprotected computer connected to the internet is measured in minutes.[1]

So it's important to protect your computer properly. Otherwise you may be putting yourself and possibly your family and friends at risk.

Make sure your computer is protected from harmful emails and viruses, and from unauthorised people accessing your internet connection and personal information.

Setting and protecting your passwords

Passwords aren't absolutely unbreakable, but they can help prevent criminals from accessing your computer.

Here are some **basic steps** you can take to set and protect your password

- choose a 'strong' password
    - a minimum of eight characters
    - a mix of upper and lower case letters
    - at least one number, and
    - at least one symbol
- change your password regularly, at least twice a year. For added security of online banking, passwords need to be changed more regularly
- if you think your computer may have been infected by a virus, you should disconnect your computer from the internet and use a separate or different computer that is not infected to reset passwords for online services.

[1] According to the US Computer Emergency Response Team www.us-cert.gov/reading_room/before_you_plug_in.html#I

Installing security software

To help secure your computer you need security software. You can install separate security products according to your needs, or an all-in-one package that includes virus protection, spyware protection, a firewall – and parental controls if you have children.

Here are some **basic steps** you should think about

- install security software that protects your computer from viruses and spyware, and includes a firewall
- have your security software set to update automatically
- renew your security software when the subscription is due.

Also, beware of scareware – these are pop-up messages or unsolicited emails informing you that your computer is compromised and inviting you to purchase software to repair it. These messages aim to trick you into believing your computer is already infected, and that purchasing the software will help get rid of it. Quite often the message and the software are fake.

Turning on automatic updates

Software companies issue regular, free updates to their software to fix security and other problems. These fixes are called patches, and they should generally be applied as soon as they're available.

Most software will have an option called 'check for updates' under the help drop-down menu. You should check this regularly. A lot of operating system and application software can now be set to update automatically – you should enable this option wherever it is available.

> *A firewall acts like a security guard at the door of your house – it checks who and what enters or leaves.*

Updating your web browser and using its security settings

A web browser is the software you use to view websites.

Most computers come with a web browser already installed. However, web browsers are regularly updated to fix security flaws, so it is important to update your web browser to the latest version.

Web browsers also come with security settings so it is important to set it up with the right security settings to protect your personal information, as hackers know how to exploit web browser settings.

The higher you set your security levels, the fewer options and functions you will have available, but your internet access will be more secure. You have to decide on the right balance for you between being as secure as possible and experiencing every feature of every website.

Your browser's security functions can usually be found in one of the drop-down menu items. Most browsers provide advice on each of the security settings and explain the advantages and disadvantages of enabling or disabling functions and high and low security settings.

Here are some **basic steps** you can take when setting up your web browser

- set up your own security settings on your web browser
- if in doubt – set the security levels to high
- use the latest version – so update your web browser as new versions become available.

Controlling your internet connection

More and more Australians are connecting to the internet using a broadband connection, whether it is ADSL, wireless or cable.

If you are using a voice-over-IP (VoIP) service you will need to keep your internet connection on at all times. However, if this is not the case then it is best to turn off your internet connection when you aren't using it.

In addition to desktop computers and laptops, many people also connect to the internet by mobile devices such as smart phones. If you have valuable information on such devices, it's a good idea to enable their security settings too.

Here are some **basic steps** you can take to control your internet connection

- always turn off your internet connection when you aren't using it
- if you have an ADSL or wireless modem then you should endeavour to change the default password.

For more information check the instructions in the manufacturer's handbook or seek advice from your Internet Service Provider (ISP).

Some **additional steps** you can take to control your internet connection are

- use a password to protect any device that connects to your network – such as smart phones, and routers
- set up separate accounts – only access the internet by using an account with limited access, rather than by an administrator account.

Securing your wireless network

Wireless networks are a great way to make the internet more accessible and to share information between devices online.

But an unsecured network is just like an unprotected computer – it leaves your personal and financial information vulnerable.

If you run a wireless network at home or in your business there are a few steps you need to take to make it secure. If you are unsure of how to change your wireless settings, follow the instructions in the manufacturer's handbook or seek advice from your ISP.

Here are some **basic steps** you can take to control your internet connection

- assign a password so that any device that is attached to the network must know the password to connect
- change the Service Set Identifier (SSID), the name that identifies the wireless network. Don't use a name that makes your network easy for others to identify
- make sure your network encryption is turned on
- adjust the broadcast power so that your network is not accessible from next door or in the street.

Checklist of basic steps to secure your computer

☑ set and protect your passwords, change them at least twice a year

☑ install and maintain security software

☑ turn on automatic updates for software

☑ set up your own security settings on your web browser

☑ control your internet connection

☑ secure your wireless network.

How to be smart online

The steps outlined in the previous chapter to secure your computer are an important start in protecting yourself online. However, simply setting up and maintaining your computer correctly is not enough to fully protect yourself and your family and friends.

You also need to be smart about what you do and the choices you make online. This means being aware of potential risks while transacting online, particularly where money is involved. It's important to show commonsense and not be tricked into doing things online that you wouldn't feel comfortable doing in the 'real' world.

Preventing viruses and other malware

Malicious software or malware is a generic term for software that is designed to specifically damage, disrupt or take control of systems.

Types of malware include things such as viruses, trojans, worms and spyware.

Your computer can be infected by malware through email messages, visiting compromised websites, and downloading infected files.

Here are some **basic steps** to prevent malware

- scan email attachments with security software before opening them
- don't open email attachments if you're not expecting them or you don't know the sender
- never click on links in emails received from unknown sources
- only download files from websites you trust
- double check that the URL or website address is correct
- be wary when exchanging files over peer to peer networks with colleagues and friends
- read the licence agreement and terms of use before you download software and don't download it if you don't trust the terms and conditions
- never click on an 'Agree', 'OK' or 'No' button to close a window on a website you don't trust. This can launch spyware onto your computer. Instead, click the red 'X' in the corner of the window.

If you suspect that your computer has been hacked or infected by a virus

- scan your entire computer with fully updated anti-virus and anti-spyware software
- report unauthorised access to your ISP
- if you suspect that any of your passwords have been compromised, call the relevant service provider (e.g. ISP or bank) immediately
- if you need assistance in removing malware from an infected computer, please visit **www.staysmartonline.gov.au** to find resources and services that can help you.

The Cyber Security Alert Service is a free subscription based service that provides information on the latest computer network threats and vulnerabilities in easy to understand language.

It also provides solutions to help manage these risks.

You can sign up for the free Cyber Security Alert Service at **www.staysmartonline.gov.au/alert-service**

Reducing spam

Spam is electronic junk mail sent to your email account, mobile phone number, or instant messaging account.

The content of spam messages varies. Some messages promote legitimate products or services, while others will attempt to trick you into providing bank account or credit card details. Many spam messages contain offensive or fraudulent material, and some spread computer viruses.

Spam now makes up the majority of email traffic. Billions of unwanted spam messages clog up the internet, disrupt email delivery, reduce productivity and irritate users.

Here are some **basic steps** to reduce and manage spam

- speak to your ISP about spam filtering
- if you don't know who sent you an email, delete it
- don't reply to spam emails
- don't reply to or forward chain letters that you receive by email
- don't open attachments in any messages if the source of the message is unknown or is suspicious
- don't give your email address away unless you are confident the recipient is a trusted party
- add the spam address to 'junk senders'. Most email programs have the ability to add them to a 'junk senders' list which blocks them next time they try to email you
- report spam to the ACMA at **www.spam.acma.gov.au**.

Here are some **additional steps** to reduce spam

- if the source seems genuine, and the message appears to promote a legitimate Australian business, contact the business and ask them to take you off their mailing list, or try the unsubscribe facility
- be very careful about using your personal email address on any websites
- protect your private email account by creating separate email accounts for use when conducting online transactions or social networking
- change your email address, especially your private email address, if it has been discovered by spammers.

If you have been spammed you can report it or lodge a complaint with the ACMA – refer to **www.spam.acma.gov.au** or phone 1300 855 180.

Spam SMS can be reported to 0429 999 888.

Securing your money online

There are criminals who will try to find holes in your security measures and internet habits when you're doing online transactions – including paying bills, shopping and banking. They will try to trick you into revealing your personal details and account details so they can steal your information, money and property.

So make sure your computer is protected from online security threats and that you have smart online habits.

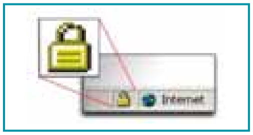
Online payments

Do what you can to satisfy yourself that any online payment you make is secure. Companies that offer a secure payment system will tell you so before you start to provide your credit card details.

Although there are a number of things you can look for on a secure web page, the unfortunate fact is that scammers may be able to reproduce logos to give you the impression that a fake website is secure.

If you have doubts, it's safer not to proceed.

Here are some **basic steps** to ensure your online payments are as safe as possible



- check you are on a secure page – a key or lock icon will appear somewhere on your browser, and the URL or web address will begin with https (instead of just http)
- double check that the URL or website address is correct – and not just similar to the legitimate website
- some web browsers also colour code the address bar to identify these websites with advanced security certification features.

Shopping online

Online shopping is convenient and reasonably safe – as long as you take precautions.

When you are shopping online, be wary if

- the website looks suspicious or unprofessional
- the website is offering bargains that look too good to be true, or
- you think you won't get what you pay for.

Here are some **basic steps** to make sure your online shopping is as safe as possible.

Before making the purchase

- know who you are dealing with – check that the contact details are correct
- know what you are buying – read the description of the product carefully – check the size, colour, value and safety of the product
- read all the fine print including refund and complaints handling policies
- check the currency, postage and handling, and other charges – there may be extra charges you aren't aware of
- check the final cost before paying, including any currency conversions and additional shipping costs.

Making the payment

- only pay by a secure web page and use a secure payment method. Avoid money transfers and direct debit, as these can be open to misuse
- never send your bank or credit card details by email – only by a secure web page
- always print and keep a copy of the transaction.

If you have doubts, it's safer not to proceed

Banking online

Online banking is convenient and reasonably safe – as long as you take reasonable precautions.

Here are some **basic steps** to ensure your online banking is as secure as possible

- always type or bookmark your financial institution's URL or website address into your browser – never use a link to your financial institution that has been sent to you by email or that is on a website. These may lead to fake websites

- always log out from your internet banking session and close your internet browser when you have finished

- if any window pops up during an internet banking session, be suspicious, especially if it directs you to another website which asks for your account information or password

- don't send your financial information by email to anyone

- avoid using a public computer to do your online banking

- make sure you are aware of the security advice provided by your financial institution.

Protecting yourself from scams and fraud

Unfortunately there are scams and scammers on the internet. Some scams are especially designed to take advantage of the way the internet works.

A scam might come to you in the form of an email, or contact from an unknown person through websites such as dating sites, online forums, or social networking sites.

Scams are usually designed to either steal your money or trick you into revealing personal information. Scams may relate to things such as employment surveys, investments, lotteries, charities, and pharmaceuticals.

Here are some **basic steps** to avoid scams

- don't transfer money, or provide credit card or bank account details to anyone you don't know and trust

- verify the company or charity before agreeing to any offers, you can do this by checking their business contact information or business registration number

- think twice – and use your common sense before agreeing to anything

- don't act impulsively – always get independent advice if an offer involves money, time or commitment

- stay one step ahead of the scammers – visit the SCAMwatch website at **www.scamwatch.gov.au** to learn more about scams that target you and the steps you can take to protect yourself.

If you have spotted a scam or have been targeted by a scam, there are many government agencies in Australia you can contact for advice or to make a report. The best agency to contact depends on where you live and what type of scam is involved.

If you are not sure which agency would be the best one to contact in your circumstances, contact the ACCC at **www.scamwatch.gov.au** or phone the ACCC Infocentre on 1300 302 502.

If it seems too good to be true – it probably is

DAVID WAS SCAMMED $450 AND COULDN'T PAY HIS RENT

"I'm really busy with work, so I signed up to online banking and found it was an easy way to pay my bills and maintain my accounts.

One day I received an email from my bank saying that my account had some irregularities and that I needed to log into a secure site to confirm my identity. It had the proper logo and everything, so I clicked on the link in the email and typed in my details.

I was still worrying about my account later that day, so to be safe I rang the bank to double check that the problem was fixed. It was then that the bank lady told me that the message was a scam designed to trick me into revealing my banking passwords and details.

She said the bank didn't email its customers like that. She was really helpful and froze my account straight away. I was relieved but someone had already taken out $450. It could have been much worse but I didn't have enough to pay the rent that week and I had to change all my banking details and get new cards, which was a pain.

After the bank finished its investigation and found that I had been scammed, it replaced the $450 in my account."

Phishing

Phishing is a type of scam. A phishing email will direct you to a website that looks like the real website of a retailer or financial institution.

The website is designed to encourage you to reveal personal or financial details, 'phishing' for information such as your credit card numbers, account names, passwords, and other personal information.

It's important to note that legitimate banks, financial institutions and government authorities will never ask for your account details or passwords by email – or by phone.

Here are some **basic steps** to avoid phishing scams

- don't respond to an email purporting to be from your bank
- avoid clicking on a link in an email – always type or bookmark the URL or website address, into the web browser
- when you are on a banking website, look for a key or padlock icon and that the website address begins with https, to make sure the site is secure
- be sceptical if you receive a request to update, validate or confirm your personal information.

Money transfer scams and advance fee fraud

With the rise of internet banking it is easy to transfer money online. Unfortunately this has also meant an increase in the number and types of scams that try to trick you into sending your money to scammers.

Once you send money to someone it can be very hard to get it back – especially if they are overseas. Worse still, you could be recruited as a money mule and find yourself in an illegal money laundering ring.

Scammers use all sorts of stories to try and get your money. For example, don't be lured by the prospect of a new job opportunity where you are offered large commissions for transferring money to other employees. Likewise, don't be fooled by an email telling you that you have inherited a large sum of money from a long lost relative – and that you need to pay some fees to claim the inheritance – this is a scam.

Here are some **basic steps** to avoid being involved in a money transfer scam or advance fee fraud

- don't fall for elaborate stories – try to remove the emotion from the situation and think before you act
- don't respond to emails offering you the chance of making easy money
- don't transfer money for, or provide your credit card or bank account details to, anyone you don't know and trust.

LYN WAS TAKEN FOR A RIDE BY AN ONLINE LOVER

"I joined a dating site. Pretty soon I was talking to a nice man from Europe. He told me all about his home town and even sent me photos. He was gorgeous.

After six months he told me he loved me and I also thought I'd found love again. A few months later he told me his mother had cancer and had to have chemotherapy. He said he couldn't afford to pay for it and he didn't know what to do.

I felt so sorry for him. I'd recently had a family member go through cancer treatment so I agreed to help him out. I took out loans so that he could pay the hospital bills. After sending the money, I never heard from him again. I had to sell my house to repay the debt."

Protecting your identity and privacy

Identity theft refers to using another person's name or other personal information, usually for financial gain.

While the internet has improved communications and the ease of doing business, the downside is that fraudsters and other criminals may have more opportunities to obtain details about you, your home, and your personal life.

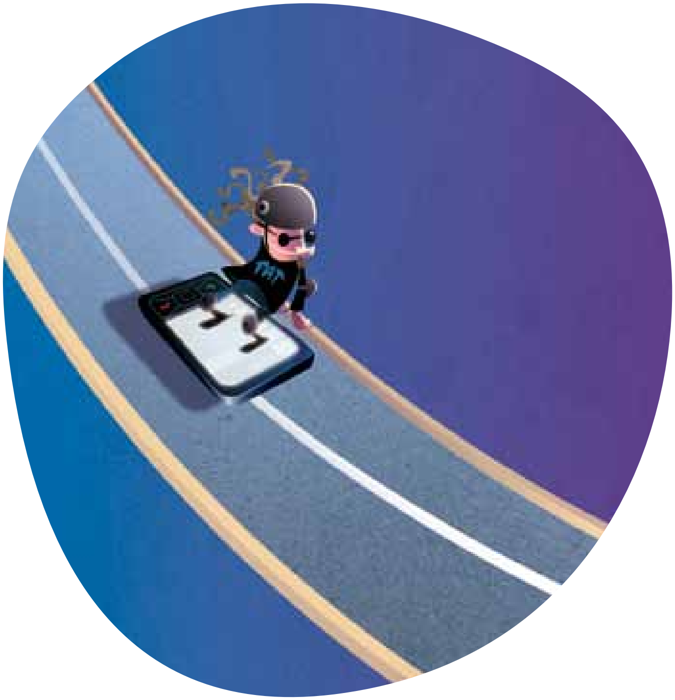
By stealing your identity, a person may access your bank account, obtain credit cards or loans in your name, and potentially ruin your credit rating.

Here are some **basic steps** to protect your identity and privacy online

- don't share your personal information in an email, SMS or on a social networking site with people you don't know and trust
- avoid using public computers to access your personal information – if you do use a public computer, clear the history and close the web browser before you leave the terminal
- avoid using Wi-Fi hotspots for sensitive internet use. These are often open and unencrypted. A hacker may be able to break into your computer through a hotspot and potentially access your personal information.

If you think your personal information has been inappropriately used or accessed online, you can lodge a complaint with the Office of the Privacy Commissioner at **www.privacy.gov.au** or phone 1300 363 992.

Treat your personal information as you would treat your money – don't leave it lying around for others to take



Here are some **additional steps** to protect your identity and privacy

- thoroughly check your account statements
- destroy personal information – don't just throw it out
- check your credit report at least once a year – this can help you catch any unauthorised activity. Credit reports can be ordered from
  - Veda Advantage at **www.mycreditfile.com.au** or phone 1300 762 207
  - Dun and Bradstreet at **www.dnb.com.au** or phone 13 23 33
  - Tasmanian Collection Service at **www.tascol.com.au** or phone 03 6213 5555
- only conduct business, visit sites or become involved with websites that have adequate privacy policies that cover at least
  - who your information will be passed onto
  - why the information is being collected
  - how the information will be used
  - how you can access information the organisation holds about you.

JUSTIN'S ONLINE FRIEND STOLE HIS IDENTITY

"I got into the social networking craze and added all sorts of people as friends even though I didn't know most of them.

I thought if I could set my profile to private so only my friends could view it I'd be safe. So I thought I could post lots of information and not be at risk. I posted things like what schools I went to, my phone number and my birthday.

With my personal information viewable an online friend was able to forge documents using my history. He then got a credit card in my name and ran up a debt of $500.

Since then I am very careful about what I post, even if I think it's private."

Checklist of basic steps to be smart online

PREVENTING MALWARE AND REDUCING SPAM

- ☑ stop and think before you click. Never click on links in emails from unknown sources
- ☑ don’t open email attachments if you’re not expecting them or you don’t know the sender
- ☑ scan email attachments with security software before opening them
- ☑ always delete spam without opening it
- ☑ don’t give your email address away unless you are confident the recipient is a trusted party

TRANSACTING ONLINE AND PROTECTING YOURSELF FROM SCAMS AND FRAUD

- ☑ check you are on a secure page
- ☑ use a secure payment method
- ☑ don’t send your financial information by email
- ☑ don’t respond to emails offering you the chance of making easy money
- ☑ don’t transfer money for, or provide your credit card or bank account details to, anyone you don’t know and trust

PROTECTING YOUR IDENTITY AND PRIVACY

- ☑ don’t share your personal information in an email, SMS or on a social networking site with people you don’t know and trust
- ☑ avoid using public computers or Wi-Fi hotspots to access your personal information.

How to be safe online

Just as you need to be smart when transacting online, you also need to be aware of the risks of social networking, particularly when interacting with people that you haven't spoken to or met in person.

The unfortunate reality is not everyone is who they claim to be online.

Social networking safely

Social networking sites have become very popular ways to communicate online.

People use them to stay in touch with friends, make new friends or business connections, and share information and opinions about a range of topics.

However, some people using these sites are threatening and may use your information to embarrass you or damage your reputation.

Criminals can also use your information to steal your identity. Indeed, some criminals will use social networking sites to find out more about you and your interests so they can target you more efficiently with scams. This is known as spear phishing.

So be very careful about the information you share and how you protect it. Criminals may also attempt to use this information to facilitate other illegal activities in the real word.

The social networking sites will often offer you options to control the type of information you share with other users and options to manage the people you want to interact with. However, you still need to be careful about what personal information you put online and who you accept as your 'friend'.

Here are some **basic steps** to help protect you

- set your online profile to private and be discerning about who you accept as your 'friend'
- protect your accounts with strong passwords
- have a different password for each social networking site so that if one password is stolen, not all of your accounts will be at risk
- think before you post – expect that people other than your friends can see the information you post online
- don't post information that would make you or your family vulnerable – such as your date of birth, address, information about your daily routine, holiday plans, or your children's schools
- don't post photos of you or your family and friends that may be inappropriate – or that your family and friends haven't agreed to being posted
- never click on suspicious links – even if they are from your friends – they may have inadvertently sent them to you
- be wary of strangers – people are not always who they say they are. It's a good idea to limit the number of people you accept as friends
- always type your social networking website address into your browser or use a bookmark.

Here are some **additional steps** to help protect you

- check if your social networking site has a safety centre. This will provide a number of tips and examples of best practice when social networking online
- remember that any information available about you online is potentially there forever. You can check what information about you is publicly available online by typing your own name into a search engine.

If you suspect any fraudulent use of your identity you should report it to your social networking service provider and your local police.

If you or your child has been harassed or bullied on a social networking site, go to **www.thinkuknow.org.au** for advice and tips.

If you are concerned about online behaviour that involves sexual exploitation of a child or other criminal activity, you should report this to your local police, or phone CrimeStoppers on 1800 333 000.

Only accept 'friends' online that you know in 'real life'

SARAH WAS BEING HARASSED BY A STRANGER

"I like social networking because it's a good way of keeping in touch with what my friends are doing. I can see the photos they've posted, and they can see mine. I've also made new friends online.

One day I received a friend request from someone I'd never met before. 'Claire' was about the same age as me, and I could see from her profile that we liked the same music, so I accepted.

Everything was ok for a while, and we would sometimes chat online. But then Claire started writing nasty things about me and sending me threatening messages.

I was really upset, so I checked my social networking site's safety information to see what I could do about it. Following their advice, I reported her using the 'report' link, and also blocked her so that she can't contact me again.

Now I am much more careful. I have increased the privacy settings on my profile so that only my friends can contact me, and I only accept friend requests from people I have met in real life."

Dealing with offensive content

When you are using the internet, you may encounter content that you find offensive – such as explicit sexual activity, child pornography, or material containing excessive violence or sexual violence, drug use, or criminal activity.

You can make a complaint about offensive online content to the ACMA.

You can do this by completing the relevant online form at **www.acma.gov.au/hotline** or by sending an email to online@acma.gov.au

Make sure you take note of the website address so the ACMA can access the online content.

If the content is sufficiently serious, such as child pornography, the ACMA may refer the material to the appropriate law enforcement agency.

You can also contact your local police to report serious, illegal online content.

Here are some **basic steps** to deal with offensive online content

- take note of the website address so the ACMA can access the online content
- make a complaint to the ACMA – by completing an online form or sending an email
- help protect your children from offensive content by installing and maintaining a content filter on your computer or using parental controls on your security software.

Report any inappropriate content to the ACMA **www.acma.gov.au**, or phone 1800 880 176.

Protecting your children online

The internet offers an exciting world of experiences for children and the whole family. It can be entertaining, educational and rewarding.

However, using the internet also involves risks and challenges.

Children might be exposed to content that is sexually explicit, violent, prohibited or even illegal. They may also experience cyber bullying or be at risk from contact by strangers.

Children may – unknowingly or deliberately – share personal information without realising they may be victims of identity theft, or that they are leaving behind content that might not reflect well on them in the future.

Here are some **basic steps** for you to protect your children online

- for younger children, set up your computer security software to only access approved websites and email addresses. This is known as whitelisting and will help to block inappropriate content
- remind your children not to talk to strangers online
- monitor and supervise internet use by having the computer in a visible place in your home
- tell your children that if they are uncomfortable talking to you they can contact the Cybersmart Online Helpline (Kids Helpline) at **www.cybersmart.gov.au**.

Here are some **basic steps for your children** when they're online

- never give out any personal information. This includes your name, address, phone number, any family information, where you go to school or where you play sport
- think before you post or share photos with people online
- never share your passwords, not even with your friends
- don't open any attachments in emails from people you don't know and trust.

Stranger danger applies to people online, just as it does in 'real life'

Dealing with cyber bullying

Unfortunately, your children may be exposed to cyber bullying. This can include

- receiving abusive emails or texts
- unkind messages or inappropriate images being posted on social networking sites
- being excluded from online chats.

Like other forms of bullying such as verbal abuse, social exclusion and physical aggression, cyber bullying may result in the targeted person developing social, psychological and educational issues.

While cyber bullying is similar to 'real life' bullying it also differs in some ways

- it can occur 24/7 and a child can be targeted at home
- it can involve harmful material being widely and rapidly sent to a large audience, for example, rumours and images can be posted on public forums
- it can provide the bully with a sense of relative anonymity and distance from the target, so there is a lack of immediate feedback or consequences.

Here are some **basic steps** to help deal with cyber bullying

- increase your online security and privacy and block communications from cyber bullies
- monitor where your children go online
- reassure your children that you love and support them and you will help them
- report cyber bullying to your children's school and your ISP.

Dealing with online grooming

Online grooming is when an adult forms a relationship with a child or younger person with the intent of later having sexual contact or committing other crimes.

This can take place in chat rooms, instant messaging, social networking sites and email.

The Australian Federal Police works in partnership with ISPs in the battle against the sexual exploitation of children online and provides an online reporting form at the ThinkUKnow cyber safety website – **www.thinkuknow.org.au**

Here are some **basic steps** to help deal with child grooming

- monitor where your children go online
- educate your children not to share personal information online
- remind your children to never meet someone in person who they have met online unless a responsible adult is also present
- report suspicious behaviour to your local police or Crime Stoppers by phoning 1800 333 000.

Here are some **additional steps** for you to protect your children online

- explore the internet with your children – consider using safe zones and exploring child-friendly websites. Bookmark websites for them that you have approved
- let your children know that not all websites are suitable and if they encounter a site that makes them feel uncomfortable, they should leave the site immediately, either by clicking on 'back' or closing the browser altogether
- reassure your children that they won't be denied access to the internet if they report seeing inappropriate content
- for older children, consider tools that block access to chat rooms and prevent giving out personal information
- check to see if your ISP is Family Friendly by looking for a lady bird logo on their website. These ISPs must adhere to the Internet Industry Association codes of practice. They offer information and online tools to help parents and children use the internet in a fun and safe way.

If you or your child has been harassed or bullied on a social networking site, go to **www.thinkuknow.org.au** for advice and tips.

If you believe someone has behaved inappropriately or in a sexual manner towards your child or children, report it to your local police, or phone Crime Stoppers on 1800 333 000.

Checklist of basic steps to be safe online

SOCIAL NETWORKING SAFELY

- ☑ set your profile to private
- ☑ protect your accounts with strong passwords
- ☑ use discretion when accepting ‘friends’
- ☑ never click on suspicious links – even if they are from your friends
- ☑ don’t post information that would make you or your family vulnerable, such as your date of birth and address
- ☑ don’t post photos of you or your family and friends that may be inappropriate – or that your family and friends haven’t agreed to being posted

DEALING WITH OFFENSIVE CONTENT

- ☑ take note of the website address
- ☑ make a complaint to the ACMA

PROTECTING YOUR CHILDREN ONLINE

- ☑ install and maintain a content filter on your computer or use parental controls on your security software
- ☑ for young children, set up your computer to only access approved websites and email addresses
- ☑ monitor where you children go online
- ☑ educate your children not to share personal information online
- ☑ report cyber bullying to your child’s school and your ISP
- ☑ remind your children to never meet someone in person who they have met online unless a responsible adult is also present
- ☑ tell your children that if they are uncomfortable talking to you they can contact the Cybersmart Online Helpline (Kids Helpline) at **www.cybersmart.gov.au**
- ☑ report suspicious behaviour to your local police or Crime Stoppers by phoning 1800 333 000.

Where to go for more information

Cyber security

- **www.staysmartonline.gov.au** – for individuals and small business
- **www.cert.gov.au** – for large companies
- copies of the Australian Government's Cyber Security Strategy are available at **www.ag.gov.au/cybersecurity**

Cyber safety

- **www.cybersmart.gov.au**
- **www.thinkuknow.org.au**
- **cybersafety@acma.gov.au** or phone 1800 880 176
- **www.netalert.gov.au** or phone 1800 880 176

Identity security

- **www.ag.gov.au/identitysecurity**

Offensive content

- **www.acma.gov.au**

Online shopping

- **www.accc.gov.au** or phone 1300 302 502

Privacy

- **www.privacy.gov.au**

Scams and fraud

- **www.scamwatch.gov.au**

Spam

- **www.acma.gov.au/spam**
- phone the spam hotline on 1300 855 180
- spam SMS can be reported to 0429 999 888

Where to go to report online incidents

Fraud

- report any loss or fraud attempt to your service provider (eg bank, social networking site), your ISP, and your local police

Identity theft

- report any fraudulent use of your identity to your service provider (eg bank, social networking site), your ISP, and your local police

Malware

- if you are having difficulties removing malware from your computer report the matter to your ISP

Privacy

- if you think your personal information has been interfered with online, you may be able to complain to the Office of the Privacy Commissioner at **www.privacy.gov.au** or phone 1300 363 992

Scams and phishing

- report any scams to the ACCC at **www.scamwatch.gov.au** or phone the ACCC Infocentre on 1300 302 502 during business hours

- also report any scams to your service provider (eg bank, social networking site), your ISP, and your local police

Spam

- you can report or complain about spam to the ACMA – refer to **www.spam.acma.gov.au** or phone 1300 855 180

Other

- you can also report any online incident to Crime Stoppers by phoning 1800 333 000

Glossary of some online terms

ADSL or asymmetric digital subscriber line is a broadband internet connection using telephone lines to connect to the internet. It offers higher speeds then traditional 'dial up' connections

Blacklist a list of website addresses or email addresses that cannot be accessed by a user

Bot a single compromised computer, sometimes called a zombie

Botnet a network of compromised computers, sometimes called a zombie army

Broadband a type of fast internet connection, it includes ADSL, Ethernet, cable, wireless or satellite connections. Unlike dial up connections, broadband offers internet access which is 'always on'

Encryption a process where information is transformed to make it unreadable to devices that don't have the encryption key. Most wireless network routers include encryption functions as a security setting

Firewall protects a computer network from unauthorised access – it may be hardware, software or a combination

ISP or Internet Service Provider is the company that you pay to provide you with access to the internet

Malware is short for malicious software and is a generic term for software that is designed to specifically damage, disrupt or take control of systems

Modem a device that links a computer to other computers or the internet through a telephone line

Phishing a type of scam, generally sent by email, that will direct you to a website that looks like the real website of a retailer or financial institution. The website is designed to encourage you to reveal financial details, 'phishing' for information such as your credit card numbers, account names, passwords, and other personal information

Post is when you make information available online. This can include updating your social network details or placing photos of yourself on a website

Router is a device used to connect computer networks together

Scareware is fake security software that is sent to users by unscrupulous tactics, such as messages on compromised websites

Smart phone is a mobile phone that has advanced capabilities such as being able to access the internet

SMS or Short Message Service is more commonly referred to as 'texting'. It is used to send short messages over mobile phones. MMS or Multimedia Messaging Service is similar to SMS but is used to send messages that include multimedia content such as photos

Software is a general term for various kinds of programs used to operate computers and related devices

Spam indiscriminate unsolicited bulk email – or electronic junk mail

Spear phishing is a more targeted form of phishing. A spear phisher will use real information about you to make the scam seem more realistic or convincing

Spyware a type of malware that is used to spy on people using the internet and collect information about their online activities for the purposes of marketing

Trojan a type of malware disguised as a legitimate program

URL or Uniform Resource Locator is the address of a web page on the internet

Virus a type of malware that attaches itself to a program or file – which is how it spreads from one computer to another. It can be spread by human action, such as sharing infected files or sending emails with viruses as attachments

Whitelist a list of website addresses or email addresses that can only be accessed by a user

Worm a type of malware that is similar to a virus but can spread without human action

Zombie a single compromised computer, sometimes called a bot.