Australian Government

# Protecting Yourself Online

## What Everyone Needs to Know

SECOND EDITION

Australian Government

# Protecting Yourself Online

## What Everyone Needs to Know

SECOND EDITION

ISBN: 978-1-921725-68-5

© Commonwealth of Australia 2011

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia (http://creativecommons.org/licenses/by/3.0/au/deed.en) licence.

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3.0 AU licence (http://creativecommons.org/licenses/by/3.0/legalcode).

**Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the It's an Honour (http://www.itsanhonour.gov.au/coat-arms/index.cfm) website.

**Contact us**

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Telephone: (02) 6141 6666
copyright@ag.gov.au

**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

Many of us 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, playing games, 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 electronic communications, in particular 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 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 Australian Information 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

Being aware of what risks you face online will help you make informed choices about how you use the internet.

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 the internet. However, there are simple steps you can take to protect yourself and your family 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

- **8 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 who wish to take further precautions.

Mobile computing is now a dominant trend. While the term 'computer' is used throughout this document it's important to remember that your phone, tablet computer, game console and even refrigerator may be able to connect to the internet. The processing power in these devices and the amount of personal information they hold is equivalent to a small computer so only thinking about security for 'computers' misses the reality of the modern world.

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

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.



# Contents


**A summary** 2

Eight simple tips to help protect yourself online 2

**How to secure your computer** 4

Install security software 4
Turn on automatic updates 5
Use standard user accounts 5
Set and protect your passwords 5
Avoid running out of date software 7
Use smart settings for your web browser 7
Control your internet connection 7
Securing your wireless network 8
Checklist of basic steps to secure your computer or other internet enabled devices 9

**How to be smart online** 10

Prevent viruses and other malware 10
Reduce spam 11
Secure your money online 12
Avoid scams and fraud 15
Be aware of phishing 17
Know how to spot money transfer scams and advance fee fraud 17
Protect your identity and privacy 18
Checklist of basic steps to be smart online 21

**How to be safe online** 22

Social networking safely 22
Deal with offensive content 24
Protect your children online 25
Deal with online child grooming 27
Checklist of basic steps 29

**Where to go for more information** 30

**Where to go to report online incidents** 31

**Glossary of some online terms** 32

# 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 whether you have had a little or a lot of experience online.

Whether you are new to using the internet or a regular user – there are **8 simple tips** that you need to follow to help protect yourself online:

| | |
|---|---|
| 1 | Install and renew your security software and set it to scan regularly. |
| 2 | Turn on automatic updates on all your software, including your operating system and other applications. |
| 3 | Think carefully before you click on links and attachments, particularly in emails and on social networking sites. |
| 4 | Regularly adjust your privacy settings on social networking sites. |
| 5 | Report or talk to someone about anything online that makes you uncomfortable or threatened – download the Government's Cybersafety Help Button. |
| 6 | Stop and think before you post any photos or financial or personal information about yourself, your friends or family. |
| 7 | Use strong passwords and change them at least twice a year. |
| 8 | Talk within your family about good online safety. |



What these steps show is that protecting yourself online is about more than just how you set up and use your computer, mobile phone or any internet enabled device. 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. While many of these are scams that most people would spot a mile away if they were attempted in the 'real' world, online scams are very sophisticated and often harder to detect.

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

Further information about online issues and 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**.

You can request hard copies of this publication from **cybersecurity@ag.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.

## Install security software

To help secure your computer you need reputable security software. The easiest software to install is an all-in-one package that includes virus and malware protection, spyware protection, a firewall – and parental controls if you have children. If you're not sure what software is reputable ask at your local computer store or look for IT magazine or online surveys of security software.

Here are some **basic steps** you can take to secure your computer

- install reputable security software that protects your computer from viruses, malware 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 that tell you that your computer is compromised and want you to purchase software to repair it. These messages aim to trick users into believing your computer is already infected, and that purchasing the software will help get rid of it. Checking your security settings and making sure your pop-up blocker is on may help avoid this. There have also been instances where users have received a phone call purporting to be from a security company advising them that their computer is at risk. Quite often the message and the software are fake.

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

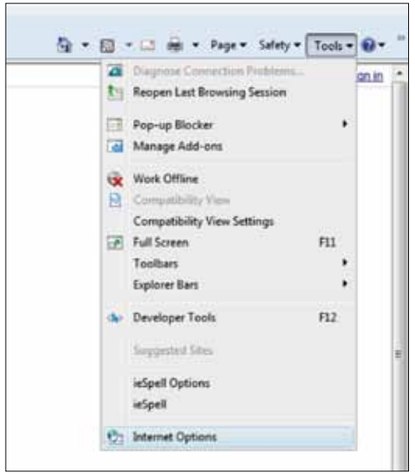


## Turn on automatic updates

Reputable software companies often issue 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. Security fixes are also included in general updates, even if they don't mention it.

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.

**What is a drop down menu?**




## Use a standard user account

Your computer has two types of user account options, a standard or administrative account. Creating and using a standard user account for most daily tasks, such as surfing the web and reading emails, will reduce the amount and type of malware that is able to infect your computer.

Many forms of serious malware require a user to be running an administrator account in order to successfully infect your computer. Going online with a standard user account greatly reduces the effectiveness of many types of malware.

The Stay Smart Online website has factsheets on how to set up standard user accounts. Visit **http://www.staysmartonline.gov.au/factsheets** to find out more.

## Set and protect 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
- avoid using words found in the dictionary – try a passphrase instead

- have different passwords for different activities and change them regularly, particularly those for sensitive transactions such as banking, social networking and your computer logon
- don't store a list of your passwords on your computer in a word document – this makes it easy for anyone who gets into your computer to access your social networking, banking and other accounts
- Select 'no' when your computer offers to automatically remember a password when logging into a website, especially banking, social networking and web mail accounts. This is because scammers can use malware to find these stored within the PC.

  If it helps to write your passwords down, do so – but hide them somewhere safe, away from prying eyes and not together with your computer logon. An even better idea is to use a passphrase.


**THE CHALLENGE TODAY – PASSWORDS AND REMEMBERING THEM!**

Ensuring that your passwords are secure is important. If your password is captured, guessed or stolen, someone could impersonate you online, steal money from your bank account, send emails in your name or change files on your computer – to name just a few of the possible outcomes.

Passwords do not have to be a single word, base your password on a phrase or sentence - a passphrase. Think of a phrase then change some of the characters to make it a strong password:

*I wish I could eat 12 meat pies a day* becomes iWice12!mp@d

*I love my cat* becomes i<3myc@t

*Some where over the rainbow, blue birds fly* becomes 5w0tR,Bbf}

(just don't use these examples)

That way, as long as you use a few random capitalisations and symbols you can write down the phrase and keep it in your wallet or near your computer and no one will be able to guess your password!



## Avoid running out of date software

Discontinued products that are no longer for sale or are out of date are more likely to make your computer insecure. This can include the software that runs your computer and other computer programs.

## Use smart settings for your web browser

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

Do not use the 'remember' function for passwords that give access to financial or personal information like your banking or social networking accounts. This ensures that if your web browser gets attacked, you don't lose all of your sensitive passwords.

Most computers come with a web browser already installed. However, there is no guarantee that the web browser has been set up with the right security settings for your needs. Hackers know how to exploit web browser settings, so it's important to select the right settings to protect your personal information.

The higher you set your security levels, the fewer options and functions you will have available, but the more secure your internet access will be. 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. But know that this may restrict your ability to view and use some websites or the functions on them
- use the latest version – so update your web browser as new versions become available.

## Control your internet connection

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

In addition to desktop computers and laptops, many mobile devices, such as smart phones, can be used to access the internet. It's just as important to enable security settings for smart phones, or any other device with internet connectivity – particularly where it contains private or sensitive information.

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

- use a strong password to protect physical access to any device that holds personal information on it – such as computers, smart phones, and routers
- always turn off your internet connection when you aren't using it

- If you have an ADSL or wireless modem then you should always change the default password.

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

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

- set up separate accounts – only access the internet by using an account with limited access, rather than by an administrator account.

Here are some **basic steps** you can take to secure your smart phone and its internet connection

- use a PIN or password, so no one can access your private data if your phone is lost or stolen
- like your computer, set automatic updates or check regularly for downloads to your phone's operating system and applications
- only download applications from official stores or from a trusted source, such as your own bank
- take control of your smart phone - turn off your Wi-Fi and Bluetooth when not in use or change your settings so that your phone asks for permission to join a new wireless networks.
- only connect your phone to a secure (encrypted) wireless network and while it's alright for general browsing don't use public wireless networks for important online transactions such as banking
- be careful about how you allow your phone to broadcast your location – such as GPS applications. Do you really want a thief to know where you live and when your house is empty?
- tampering with your phone's software or operating system (sometimes known as jailbreaking) may leave it exposed to additional security vulnerabilities

## Secure 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. Securing your wireless connection can prevent unknown people from accessing your wireless connection for excessive downloads or illegal activities.

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.

Here are some **basic steps** you can take to control your wireless network

- assign a password so that any device that is attached to the network must know the password to connect. Don't just use the default passwords as these are widely known and make sure you use a strong password
- 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, such as your family's name or business name
- make sure your network encryption is turned on and, just like your software, use the latest encryption available on the device.

If you are unsure of how to do this follow the instructions in the manufacturer's handbook or seek advice from your ISP.

### Checklist of basic steps to secure your computer or other internet enabled device

- ☑ install and maintain security software
- ☑ turn on automatic updates for software
- ☑ use a standard user account
- ☑ set and protect your passwords, use a different password for different accounts
- ☑ set up your own security settings on your web browser
- ☑ control your internet connection
- ☑ secure your wireless network.

Still unsure about how to stay secure online? Visit page 30 to find out where to go for more information.

# How to be smart online

The steps outlined in the previous section 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.

## Prevent 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 or 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 emails or attachments if you're not expecting them or you don't know the sender
- think carefully before you click on links and attachments in emails and on social networking sites
- only download files from websites you trust
- double check that the URL or website address is correct, as the link may redirect you towards a fake address, which may look similar to the legitimate site
- be wary when exchanging files over peer to peer networks
- 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, visit **www.staysmartonline.gov.au** to find resources and services that can help you.
- you can also find more security related information and assistance on the icode website **www.icode.net.au**.

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**

The Internet Industry Association in conjunction with the Australian Government has developed a voluntary code of practice for ISPs. The icode is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.

Make sure you use an ISP that is compliant with the icode, look for the Trustmark below on their website.

## Reduce spam

Electronic junk mail is commonly known as spam. These are electronic messages you haven't asked for that are 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 following a link to a scam website where you will be asked to enter your 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 spam

- speak to your ISP about spam filtering
- if you don't know who sent you an email, delete it
- if the message appears to be genuine, but unsolicited in nature, reply with 'STOP' (for SMS) or use the unsubscribe facility (for email). On the other hand, if a message appears to be from a questionable source, avoid replying as it may alert the scammer that you have an active email address or phone number
- don't reply to or forward chain letters that you receive by email
- think carefully before you click on links and attachments in emails and on social networking sites
- 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 email or SMS spam to the Australian Communications and Media Authority (ACMA) at **www.spam.acma.gov.au** or forward spam SMS messages to 0429 999 888

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.
- 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 account password regularly
- consider changing your email address if it's discovered by spammers
- update your email program as new versions often have built-in security and the latest spam identification options.

There are laws against spam in Australia. 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 forwarded to 0429 999 888.

## Secure 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.



**Be smart about online payments**

Do what you can to satisfy yourself that any online payment you make is secure. Companies that offer secure payments 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 symbols 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 – the URL or web address will begin with https (instead of just http) and a key or padlock icon will appear somewhere on your browser. But remember, this will only guarantee a secure payment process – it does not guarantee the identity of the website operator.
- 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.


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

**Be aware while 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 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. Where possible, avoid upfront payment of any kind or money transfers and direct debit, as these can be open to misuse and it is rare to recover money sent this way
- when shopping through official classified websites, or online auction sites, ensure you complete the transaction through the website's payment system. If you transact outside these systems you lose any protection that the site offers
- 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 think you have provided your account details to a scammer, contact your bank or financial institution immediately.

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

**JESSICA'S PEDIGREE PUP WAS TOO GOOD TO BE TRUE**

"I was thinking about buying a dog and was looking through an online classifieds website.

I fell in love with the photo of little Buster instantly. He was a 2 year old golden cocker spaniel with adorable ears. He also had an impressive pedigree. Best of all he wasn't even very expensive as his family was moving overseas and they wanted to make sure he went to a good home.

I contacted the seller immediately and after a lengthy email exchange, they decided that I was a good fit to take care of Buster.

I made a money transfer of $375 to pay for Buster to be transported to me and went on a pet shopping spree so that Buster had everything he needed when he arrived.

I went to the airport to pick him up but they said they had no record of Buster in their systems. I tried calling the seller but the phone number was disconnected.

I contacted the online classifieds website to find more contact information, but they told me I was the victim of a classifieds scam and that several other people had complained about the ad.

Besides the $375 I lost to the scammer I was also left with a pile of dog toys and food that I didn't need"



**Bank online securely**

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

- never use a link to your financial institution that has been sent to you by email or that is on a website. If these were from fake emails these may lead to fake websites
- Once you have arrived at a website, double check that the web address is correct – scammers can use malware to make your computer redirect you to a scam copy of a legitimate website
- always log out from your internet banking session and close your internet browser when you have finished
- if any windows pop up unexpectedly during an internet banking session, be suspicious, especially if they direct you to another website which asks for your account information or password. If this happens, do not enter your account information, password or any personal details into the site and close the window immediately
- don't send your financial information by email to anyone
- avoid using a public computer or public Wi-Fi connections to do your online banking
- make sure you are aware of, and act on, the security advice provided by your financial institution.

## Avoid scams and fraud

Scams are dishonest tricks designed to fool you into giving someone your money, passwords, personal details or other valuables.

Scammers love the anonymous nature of the internet. If you are shopping, banking, socialising or playing games online, be on the lookout for people, emails or websites which try to deceive you.

Dodgy sites and dodgy dealers are not always easy to spot but knowing some of the warning signs can reduce your risk.

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

- protect your identity: your personal details are private and invaluable – keep them that way and away from scammers

- don't respond: ignore suspicious emails, letters, phone calls or text messages – press 'delete', throw them out or just hang up
- don't let scammers push your buttons: scammers will play on your emotions to get what they want
- resist the personal touch: watch out for scammers posing as someone that you know and trust, pretending to know you, or pretending to be from well known public companies or government departments
- stay one step ahead of scammers: visit the SCAMwatch website at **www.scamwatch.gov.au** to learn more about scams that might target you. You can also subscribe to their email alerts at **https://www.scamwatch.gov.au/content/index.phtml/tag/ScamWatchEmailAlert**

If you have identified a scam or been a victim of fraud

- report it to your service provider (eg bank, or a social networking site), your ISP, and your local police
- you can report it to the ACCC via the SCAMwatch website (**www.scamwatch.gov.au**) or by calling 1300 795 995.

**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 which looked like it had come 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."



## Be aware of phishing

Phishing emails used to be associated with banks, but these days scammers will try to trick you into providing your personal and banking details by pretending to be from all sorts of well known and respected organisations, including government agencies.

While some emails will have tell tale scamming signs such as misspelt words or poor grammar, others can look like the real thing, using corporate logos and links to genuine looking websites.

If you receive one of these emails – and chances are you probably will – do not follow any of the links. You could also lose money and put your accounts at risk if you provide any of your personal details.

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

- never respond to requests for personal information in an unexpected email or on a website linked to from an unexpected email, even if it is supposedly from your bank or an organisation you know or trust
- be sceptical if you receive a request to update, validate or confirm your personal information – if in doubt, contact the organisation by phone
- never enter your personal, credit card or online account information on a website if you are not certain it is genuine
- check the website address carefully, remember that scammers often set up fake websites with similar addresses to real ones
- 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
- never send your personal, credit card or online account details via email.

## Know how to spot 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 can earn large commissions for transferring money to other employees. Likewise, don't be fooled by an email saying 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

- 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
- verify any person or company before you transfer money or provide your credit card or bank account details.

**LYN WAS TAKEN FOR A RIDE BY AN ONLINE LOVER**

"I joined a dating site to see what it was like. Pretty soon I was talking to a nice man from Greece. He told me all about his home town and even sent me photos. He seemed really nice.

After six months he told me he loved me and I couldn't have felt happier. 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."

## Protect your identity and privacy

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

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, where you live, 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

- check your privacy and security settings on your social networking profile, never give away your account details, and regularly update your computer security software
- use strong passwords and change them regularly – the personal information you put in your social networking profile may be used by scammers to guess your passwords
- don't share your personal information in an email, SMS or on a social networking site with people you don't know and trust
- don't accept a friend request or follow a request from a stranger – the best way to keep scammers out of your life is to never let them in
- avoid using public computers to access your personal information. If you do use a public computer, check to see if the service provider has any secure settings. Always remember to clear the history, close the web browser and log out 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 Australian Information Commissioner at **www.privacy.gov.au** or phone 1300 363 992

If you suspect any fraudulent use of your identity you should report it to the website operator (eg bank or social networking site), your ISP and your local police.


*You wouldn't hand your personal and financial details over to a stranger in the street so don't do it online.*

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

- thoroughly check your account statements, including credit cards, bank statements, telephone and internet bills
- destroy or shred 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

- check out websites' privacy policies. 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
- if you do not agree with how websites and companies will use your details, do not provide them.

## JUSTIN'S ONLINE FRIEND STOLE HIS IDENTITY

"I set up a profile on a social networking site, added all my friends and posted a few pictures. I filled out some of the basic optional fields, such as my birthday, hometown, email address and my interests. I also joined a few groups, such as my old school and one of my old jobs.

I chose secure settings so that only my friends could see my profile – I thought this was safe enough.

I started getting a few friend requests from people I didn't know, but I accepted some of them because they had similar interests to me or were friends with my friends.

With so much of my personal history available, one of these new 'friends' was able to forge documents and even make a fake ID using my photo.

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

- ☑ Think carefully before you click on links in emails or on social networking sites. It's always better to type the address into the address bar yourself
- ☑ 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
- ☑ don't give your email address away unless you are confident the recipient is a trusted party.

### TRANSACTING ONLINE AND AVOIDING 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
- ☑ verify any person or company before you transfer money, provide your credit card or bank account details.

### 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 or provide personal information.

Still unsure about how to stay smart online? Visit page 30 to find out where to go for more 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. Not everyone you meet online is trustworthy enough to be considered a friend.

## 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 have ill intentions 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.

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 world.

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** you can take to stay safe when using social networking sites

- set your online profile to private or 'friends only'
- 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 to people you know or have met in real life and trust
- always type your social networking website address into your browser or use a bookmark.

*Never accept a friend request from a stranger*

Here are some **additional steps** you can take to stay safe when using social networking sites

- 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
- learn how third party applications on social networking sites use your information. You can often control this by accessing your privacy or security settings
- download or find out more information on the Cybersafety Help Button at www.dbcde.gov.au/helpbutton. It is an online resource that gives easy access to cyber safety help and information.

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

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

Download the Cybersafety Help Button at **www.dbcde.gov.au/helpbutton**. It's an online resource that gives children, teenagers, parents and teachers instant access to help and information on cyber safety issues 24/7.

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.

**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."

## Deal with offensive content

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

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

You can do this by completing the relevant online form at **www.acma.gov.au/hotline** or by calling 1800 880 176. Make sure you take note of the offensive website's 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 such as child pornography.

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, sending an email or making a phone call
- 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 and letting them know that they can do if they come across offensive content.

Report any inappropriate content to ACMA by completing the relevant online form at **www.acma.gov.au/hotline** or by calling 1800 880 176.

## Protect 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 become victims of identity fraud, 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
- think carefully before you 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

- never respond to negative messages but save the message and the details of the sender. If you are a parent, you may want to save the message so your child doesn't keep reading it and feel worse
- monitor where your children go online
- remind your children to only have people they know and trust as online friends/contacts
- reassure your children that you love and support them and you will help them
- report cyber bullying to your children's school and/or the relevant social networking site or service provider
- if your child has been involved in cyber bullying and seems distressed or shows changes in behaviour or mood, seek professional help. You can do this through the Cyber Smart Online Hotline at **www.cybersmart.gov.au/report.aspx**. This provides free, online counselling for children and young people. Your child's school may also be able to provide support and guidance
- download or find out more information on the Cybersafety Help Button at **www.dbcde.gov.au/helpbutton** so that your child can access support immediately if they are bullied.

## Deal with online child grooming

Online child grooming is when an adult forms a relationship with someone under the age of 16 with the intent of later having sexual contact with that child or young person.

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

Signs that a young person might be the target of online grooming may include excessive use of the computer, late night computer use and secretive computer use, changes in sexualised language and behaviour—either becoming more or less sexualised in language, behaviour and dress—and a change in the way they relate to friends or family. These signs do not necessarily mean a young person is being groomed. They could also be signs that a young person is experiencing more general social issues associated with growing up.

If you think that you or your child is being groomed online, then contact the Australian Federal Police (AFP) by completing an online reporting form at the ThinkUKnow cyber safety website – **www.thinkuknow.org.au**.

The AFP works with state and territory police, other agencies and ISPs in the battle against online sexual exploitation of children.

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** or **www.cybersmart.gov.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.

If there is a threat to your child's safety the police can help. In a life threatening and time critical situation call Triple Zero (000).

Download the Cybersafety Help Button at **www.dbcde.gov.au/helpbutton**. Its an online resource that gives children, teenagers, parents and teachers instant access to help and information on cyber safety issues 24/7.



## 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'
- ☑ think carefully before you 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 – photos that your family and friends haven't agreed to being posted or that identify where you live, work or go to school.

### 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
- ☑ download the Cybersafety Help Button at **www.dbcde.gov.au/helpbutton.**

Still unsure about how to stay safe online? Visit page 30 to find out where to go for more information.

# 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**
- **www.icode.net.au** for information on the Internet Industry Association's voluntary code of practice on cyber security (the icode)

## Cyber safety

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

## 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**
- SCAMwatch twitter – follow SCAMwatch on Twitter at http:twitter.com/SCAMwatch_gov or @SCAMwatch_gov

## Spam

- **www.spam.acma.gov.au**
- phone the spam hotline on 1300 855 180
- spam SMS can be forwarded 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 fraud and 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 or contact a professional to remove it. The icode website has information on finding professional help at **http://icode.net.au/professional-help.php**

## Privacy

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

## Offensive content

- Report any inappropriate content to ACMA by completing the relevant online form at **www.acma.gov.au/hotline** or by calling 1800 880 176

## Scams and phishing

- report any scams to the ACCC on the SCAMwatch website at **www.scamwatch.gov.au** or phone the ACCC Infocentre on 1300 795 995 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 for spam SMS forward the message to 0429 999 888

## Online grooming

- you can report online grooming to the AFP by completing the online reporting form at **www.thinkuknow.org.au**

## 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 a 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

**Passphrase** a password based on a sentence or phrase, which is then altered by replacing some letters with numbers and symbols to make it a strong password

**Peer to peer networks** when two or more computers are connected and share resources

**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

**PIN** personal identification number

**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** electronic junk mail

**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 be accessed by a user. |
| **Wi-Fi** | wireless fidelity – a type of wireless networking technology |
| **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. |