Be Connected

Introduction to internet safety

Let's help make sure we use the internet safely.

Computer and email security

Some of the main online risks include:

- **Viruses**, which spread from computer to computer through the Internet. Some are just a nuisance, others can also delete your data.
- **Trojans**, which are innocent looking programs that try to trick you into installing them.
- **Spyware**, programs that steal information like passwords or bank account details.

There are steps you can take to protect yourself and your computer from online threats.

1. Use **antivirus software**, which helps find, stop and remove viruses.
2. Use **anti-spyware software**, which helps stop your data being stolen.
3. Use a **firewall**, which helps protect your computer from unauthorised access from the internet.
4. Keep your internet security software up to date.
5. If you received antivirus software with a new computer, renew it when the trial runs out, or obtain free software such as AVG. Please note that Windows 10 comes with effective anti-virus software called Windows Defender. Windows will keep it up to date on your behalf.
6. If uncertain, get advice from **https://www.staysmartonline.gov.au/**.

Introduction to internet safety

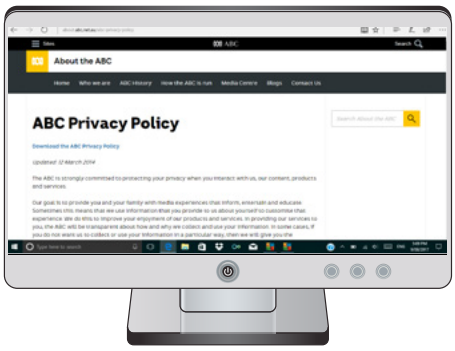
You should take extra care not to expose your computer to malicious software.

1. Think twice before opening emails - and especially email attachments - from people you don't know.
2. Deal with businesses online that you know to have a good reputation. Search for information about a company before you buy.
3. Make regular backups of all the information on your computer. If your computer does become infected, you will still have access to all your important data.

Protect yourself and your computer from online threats

Use of personal data on the internet

Sometimes it is necessary to provide personal information online, but there are limits to how much information you should share, and remain aware of your rights.



Laws govern the use of personal information by private companies in Australia

- Only provide information to legitimate companies if it's needed to verify your identity.
- Avoid posting personal information (date of birth, home address and so on) to public forums such as Facebook. Personal information can be used by criminals for identity theft.
- Laws govern the use of personal information by private companies. In Australia, that is the Privacy Act 1988.
- The Freedom of Information Act may apply to information you provide to government bodies.
- Reputable companies have policies on how they care for personal information. Read their privacy policies on their websites.
- For further information on consumer rights or up to date information on protecting yourself from scams, please visit the ACCC: **https://www.accc.gov.au/consumers.**

Introduction to internet safety

Online payment and secure areas

Beware of the information you share online

Buying things online can be convenient, and there are some quick checks to help ensure you pay safely.

1. Does the company you're dealing with have a good reputation? Check the company's privacy and return policies on its website. Use a search engine to find out more about the company.
2. Purchase using a credit card or PayPal. Both offer some form of buyer protection.
3. Just before entering your credit card information, check the **Address bar** of your browser. A secure site should be marked with a padlock and the website should start with **https:** (not just **http:**).

Child safety online

Children are less experienced in the world and so are more at risk from:

- Viewing explicit materials.
- Disclosure of personal information.
- Bullying and harassment.

Internet chatrooms and social media are places where approaches could be made. Never let your child meet up with anyone they've 'met' online unless they're accompanied by an adult.

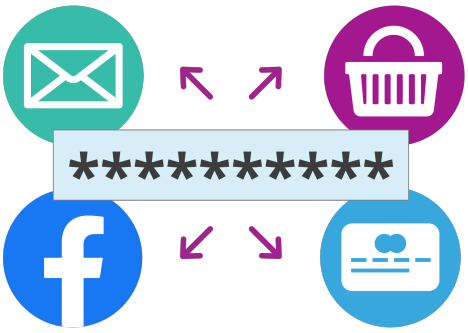
There is protective action you can take top help children stay safe online.

1. Create the child's own user account for the computer.
2. Switch on parental controls for that user account.
3. For Google, turn **SafeSearch** on, and for Bing or Yahoo, set SafeSearch to '**strict**'.
4. Set YouTube to 'restricted', along with any other video sites.
5. Talk to your child about the dangers they could face online.

If a child has accidentally ended up in a dangerous situation online, report it to the Office of the eSafety Commissioner at:
https://www.esafety.gov.au/complaints-and-reporting.

Safe Passwords

Here are some top tips for creating a strong password, one that can't be guessed by other people.



Why we need safe passwords

Many websites will ask for personal details, such as your name, address, date of birth or credit card information. To protect that information, you have to create a password. Creating a good password that can't easily be guessed is an important way of protecting yourself online.

Why good passwords matter

If somebody else gets hold of your password, they can use that password to access the personal accounts on the websites you've visited. That means that your email, banking, shopping and social media accounts might be hijacked.

A good password makes it much harder for someone to guess your password, which means that your personal accounts can be far more secure.

What not to do

There are some common mistakes that people make when creating passwords. These include:

- Using obvious or super simple passwords, such as **1234**, **password** or **qwerty**
- Using personal information, like birthdays, or the names of pets or family members
- Using dictionary words, such as **Friday**, **pizza** or **holiday**
- Using the same password for multiple websites.

You should avoid making these mistakes yourself. Instead, you should create a **good password**, one that can't be easily guessed.

How to create a good password

A good password looks like it's just a jumble of letters, numbers and symbols. For example, **3br@T2** or **Figit32!** are good passwords.

But remembering those types of passwords can be hard, so there are some tricks you can use to create good passwords that you can remember.

- You can use the substitution method. This is where you take a word and replace several letters with numbers, symbols and uppercase letters. For example, **friday** could become **f7!Day**.
- You can use a phrase or lyric that you remember and make the password from the first letter of each word. For example, **Married on the 24th of July** could be used to remember the good password, **Mot24oJ**.

Storing passwords in a web browser

Over time, you'll need to remember a lot of passwords. Your web browser can help with that. Just follow these steps:

1. When you enter the password on a website, your browser will ask if it you would like it to remember the password.
2. Only click **Yes** if you own the computer. If you're on a public computer, click **No** or **Never**.
3. If you clicked **Yes**, the next time you visit that website, the password will be filled in for you.

Regardless of how secure your device is, we recommend you never allow your browser to remember your myGov account, online shopping account or online banking account usernames or passwords.

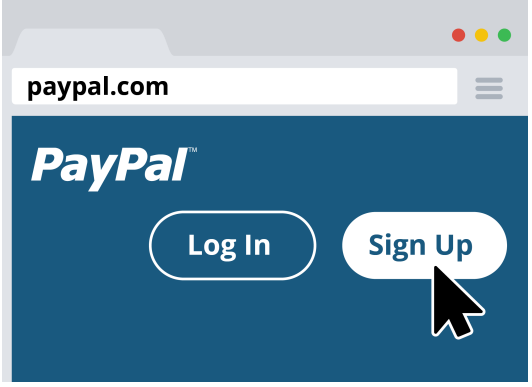
Keeping it up

You should create a new good password every time you're asked to create a new password. As an added precaution, you can change your most important passwords every few months.

If you've forgotten your password, there is usually a **forgotten password** link or button when you try to log in. Click on it, and you can arrange for the website to send you a new one by email.

Paying safely online

There are different ways to pay online, but which should you choose, and what is the safest way to pay?



Payment options

When you go through a shopping site's checkout, you'll be asked to choose how you'd like to pay. The most common options include:

- **Credit card**, using your Visa, Mastercard or American Express.
- **Direct debit** or **direct deposit**, where you're asked to transfer money directly from a bank account.
- **PayPal**, which is a service especially designed for online purchases. When you buy something, PayPal actually makes the payment on your behalf. You then pay back PayPal using a credit card or your bank account.

Buying on a trusted site

An important part of online shopping is trust. Do you trust the website you're buying from? If it's a company you have a relationship with, such as your electricity or phone provider, then trust is not an issue. It's OK to pay with any method because you know you can sort things out with the company if something goes wrong.

What to do if I don't fully trust a site?

If you are buying from a website you've never dealt with before, it's best to use credit card, or even better, PayPal. Credit cards and PayPal have a special kind of buyer protection, where you may receive a refund if things go wrong. Even if the website refuses to give you a refund, your credit card company or PayPal may still reverse the charges. That way, there's less risk for you. PayPal has an added benefit – you don't even need to give the site your credit card details. PayPal makes the purchase for you, then you pay PayPal.

What to do if a purchase goes wrong

Sometimes an online shopping experience goes bad. The goods don't arrive, or the wrong goods arrive, or the product is faulty. Don't panic, just follow these steps:

1. Contact the website you purchased the item from and try to sort things out directly.
2. If you think you've made a reasonable effort to resolve the issue, then you should contact your credit card provider or PayPal, and provide it with a report.
3. Wait for the credit card provider or PayPal to investigate. If they agree that there's a problem, they will reverse the charges. This is called a **chargeback**.

Shop away

Shopping on the internet can be very safe. Exercise some common sense about who you give money to online, and take advantage of the protection offered by chargebacks, and it can be just as safe as traditional shopping.

Avoiding scams and tricks

Here are some top tips for recognising and avoiding scams and tricks on the internet.

On the internet, you cannot always be sure that people are who they say they are. Being aware of internet tricksters is one of the most important steps towards avoiding them. Once you know their tricks, you should be able to spot a scam more easily.

The phishing scam

Phishing scams are the most common form of scam on the internet. They usually start with an email or phone call that seems to be from a business you trust, asking you to 'confirm' your account details. When you confirm your details, they're actually being gathered by the scammer. If you get an email asking for personal information, you should follow these steps:

- **Never** click on any links in the email.
- **Delete** the email.
- Help others know about the scam by reporting it to the Australian Competition and Consumer Commission's (ACCC) **ScamWatch website** at www.scamwatch.gov.au.

If you're really worried, you can always call the company that the email appears to be from directly. Just be sure to use your own contact information – not anything in the email.

Banks and government institutions will **NEVER** ask you to confirm personal details via phone, email or text message, and they won't close your account or arrest you for not responding. Any such messages are scams and you should ignore them.

The unexpected money scam

With this scam, you receive an email promising a lot of money in the future for a small upfront fee. Some examples include:

- An 'inheritance' that you can get if you only pay an admin fee.
- A 'lottery' that you've won, but you need to pay a fee to get paid out.
- A big payout in the future if you just help someone out right now.

If someone you don't know contacts you and offers a lot of money for a small upfront payment, it's probably a scam. Ignore that person and delete the email.

Money for nothing scams

These are scams that ask you to pay money for something that doesn't exist. Look for things like:

- Emails offering the opportunity to join a major investment opportunity, at a heavily discounted rate.
- People on dating websites that express deep affection for you very quickly, but then ask for help with medical and other expenses.
- Fake charities that contact you after major disasters.
- Callers telling you that there's a problem with your computer or your tax return.

These are likely to be scams and should be ignored.

Learning more about scams

The best place to report and learn more about scams is the Australian Competition and Consumer Commission's **ScamWatch website**, which can be found at www.scamwatch.gov.au.

Knowledge is power

Scams are intended to take advantage of your good nature, but if you're careful about sharing personal information online, use common sense about who you give money to, and keep your guard up, the internet can be a safe place to explore.
