Keeping safe online

Description

Keeping safe online

The internet offers incredible opportunities and information for people of all ages, and connects us in a way that we have never been connected before – especially in rural, regional and remote areas. We can easily stay in touch in spite of geographic distances. We can easily and safely work from home, and talk to our doctors and specialists without travelling for hours.

But with opportunity and accessibility comes risk to your identity, your information, and your online safety and mental health. We have gathered some basic tips and tools, along with some vital links, to help keep your online experiences as positive as possible.

Online Security: Everything You Need To Know

- ○ 1What is online or cyber-security?

  Online or cyber security refers to protecting data and information networks such as your computer, tablet or mobile phone. If you do not take steps to manage your cyber security, your devices can get harmful viruses that may stop them from working, or you could lose important personal information such as credit card details to criminals.

  ○ 2How to stay safe online
  - **Never trust unexpected contacts, sudden changes in processes, or requests to access your computer remotely.**If a usually trusted source, such as a family member, friend, business or Government department, requests to change or access something, contact them directly via a phone call to confirm. No legitimate organisation should pressure you to make a decision on the spot, and definitely not via text or email.**Example:** People have lost money by responding to an email from a trusted business asking at the last minute to change the account a payment is being made to (e.g. house payment).
  - Don't provide private details, approval, or credit card details when answering a phone call, text or email.
  - Don't click random links or sign up for products or services on the spot.
  - Install malware/virus software on your computer and scan software before you open it up. This will prevent issues in the vast majority of cases.
  - Don't download and install software when requested by a random contact. Many scammers will tell you to download perfectly legitimate tools such as TeamViewer , LogMeIn Rescue, GoToMyPC that allows someone to remotely access your computer. Do not install this software at this time.
  - If you're unsure about the safety of an email attachment, it's wise to scan it using your antivirus app beforehand. A helpful guideline is to open only those email attachments that you anticipate receiving. If the message appears strange, feel free to contact the sender to seek clarification.
  - There is no official Australian organisation that can threaten you in any way if you don't do something the first time they contact you.
  - No-one will ever give you free money or services.
  - Never allow anyone who calls you unexpectedly to access your computer, laptop or device.
  - If your computer, laptop, or device has been supplied by a place of work, your work IT team may safely access that computer, laptop or device. If in doubt, organise to visit your place of work with the relevant computer and get it fixed at the business location.

  For more information, see point four or visit the following websites:

  - BeConnected: Introduction to internet safety. A free, simple online course covering email safety, making credit card payments on the internet for online

shopping, child safety and how to keep your personal data safe online.
    - Australian Cyber Security Centre (ACSC): provides advice and information about how to protect you, your family and your business online.
    - Scamwatch provides information on the latest scams and spam. You can report scams here as well.
    - ACCAN: keeping yourself safe and secure online.
    - Choice Australia: Internet privacy and safety.
    - ScamWatch: Remote access scams
- 3Managing passwords
    - Choose complex passwords and passcodes for your devices.
    - Do not use personal information like your name or pets names in your passwords. You should also avoid numbers like your address, phone number, and birthdays as this information can be publicly available and easily accessible to hackers.
    - Use a password manager to store your passwords. For example, LastPass, 1Password, Norton Password Manager, Enpass, Dashlane.

  For more information, view these articles:

    - Choice Australia: How to find the best password manager
    - Choice Australia: Password manager reviews
- 4Protecting your business, organisation or farm information

  All the practices for protecting your own identity (point two) also apply to your business, employees, or property.

  In addition, you need to consider the security of your business resources such as websites, business data, social media presence, laptops, computers, mobile devices, sheds, products, and employee access to these resources.

  These websites provide reputable advice:

    - Business.gov.au: Cyber security
    - Cyber-security Cooperative Research Centre (CSCRC)
    - National Australia Bank: Six simple online security tips for farmers
    - National Australia Bank: Online security help guides for businesses
    - Internet of Things Alliance Australia: Security awareness guides
    - Norton: 10 cybersecurity best practices that every employee should know
    - Infoblox: Preparing Employees to Be Cybersafe when Working from Home
- 5Protecting yourself from identity theft

  Criminals are becoming adept at finding new ways to take money from you, find your personal details to impersonate you or your business (known as phishing), or use your

computer to send out scams, spam messages, or viruses. The below are some examples of how they do this.

1. **Phone calls**Criminals will call you on your landline or mobile phone. The call is often made by an auto-dialler that methodically works through numbers until one connects. Being on the Do Not Call register may not prevent all of these calls.

   Examples of common phishing calls include:

   - A caller representing your RSP such as Telstra, or nbn® , informing you that your internet connection or computer has been hacked or is insecure. They may also try a positive approach, saying you are eligible for a refund or discount.
   - An online supplier, such as Amazon, informing you that you're about to be charged a random amount of money. These calls are often an automated voice telling you to press "1".

   Once you speak to a real person, they may ask you to provide or confirm personal details, bank account, or credit card numbers. They may also ask you to install software on your computer so they can fix an issue.

   Don't give them any information, never provide credit card details over the phone, and don't install software. Hang up immediately.

   If you truly believe the call was real, call the relevant provider back on the number you have for them, or found on their own website. You don't lose anything by hanging up on someone, and you may save yourself from losing money.

2. **Text Messages**These turn up randomly, often with a scary message about your bank account, or a failed delivery or payment, asking you to click on a link. **Don't click on the link**.

   If you believe the message might be real, contact the trusted organisation directly through publicly available contact information, or log into your bank account by opening the website or app. You don't lose anything by not clicking on the link, and you may save yourself from having something nasty installed on your phone.

3. **EmailNever open attachments or click on links that come in via email**. This includes emails from friends and family. Check with the sender first before opening anything.

   You are also unlikely to be legitimately inheriting money from someone you don't

know, or winning the lotto, via email.

4. **Social media**You may get a random video from a friend in your direct message box, with a very generic message. In most cases, the video contains a virus. **Don’t play the video, and delete the message unread**.

   If you have played a video, immediately change your social media password and let your friends know you may have been hacked. Let the person who sent the video know they’ve also been hacked.

   Hackers may also attempt to clone profiles of friends and family and use these to contact you. If you think someone’s profile has been cloned, contact them outside of social media or through a trusted third party. Reduce the risk of your profile being cloned by protecting your password (and changing it regularly), and checking your privacy and security settings.

- 6Safely downloading software and files

  Software, apps, video files, and other content that you download from the internet can contain viruses, malware, or spyware.

  - Only download software from reputable websites – ideally, the website of the company that creates and supports the software.
  - Use the official app store for your device: Apple App Store for iPhone and iPad; Google Play Store for Android devices.
- 7Looking after your cyber-safety

  You have a right to feel private, safe and comfortable online. E-safety, also known as electronic safety or cyber-safety, means protection from harmful online content or activities.

  Examples of harmful online activities include:

  - Cyber-bullying
  - Stalking
  - Harassment
  - Trolling (posts designed to get an emotional response)
  - Abuse
  - Exploitation

If you are made to feel insecure, unsafe, uncomfortable, or upset online at any time, or if someone is using technology to harass or abuse you, turn off your computer or device and walk away. If you can, find a trusted person to talk to about what happened.

If you, or anyone you know, are feeling unsafe online, you can call:

- Lifeline – 13 11 14
- Kids Helpline – 1800 551 800
- 1800RESPECT (1800 737 732)
- 000 for threat of immediate danger from someone who knows your details

The Australian Government has established the eSafety Commissioner to help all Australians have safer, more positive experiences online. They have a range of guides about all aspects of online knowledge and safety, including support, counselling, and reporting services.

There is advice for:

- Kids
- Young People
- Parents
- Women
- Seniors

- 8How to report abuse and get help

If it feels wrong, report it or ask for help. These services will believe and support you:

- Stymie: Report school or sports club bullying
- eSafety Commissioner: Report abuse
- eSafety Commissioner: Report cyber abuse to social media services
- Dolly's Dream: Get help
- eSafety Commissioner: Counselling and support services – a comprehensive list of services to listen and provide support.

- 9Using social media safely

Social media is the name for services that encourage real-time posting of content of all kinds. It includes services like Facebook, X (formerly Twitter), Instagram, LinkedIn, Tumblr, Snapchat, TikTok, and many more.

Other sites and services can also have a social media aspect. For example, online games with a chat function or the comments sections of news, information, and blog sites.

Social media can be an excellent way to keep in touch with family and friends, discover what's happening, find new people and products, and promote your business or services.

However, its anonymity means it can also be used to bully, stalk, harass, and otherwise be unpleasant to other people. You have a certain amount of control over your own social media account, including shutting it down entirely.

These links may be helpful in understanding and effectively using social media.

- Be Connected: An introduction to social media
- eSafety Commissioner: eSafety Guide. Lists and discusses common social media services and apps.
- Lifewire: Tips and tricks for social media (covers the main social media services such as Facebook, Twitter, Instagram, Snapchat, and so on).
- Lifewire: The Top Social Networking Sites People Are Using

○ 10Managing your safety online

Being the target of repeated bad online behaviour is not your fault. You do not have to take responsibility for how other people behave toward you. You can, however, do a number of things to prevent and manage individual people's actions toward you.

1. Set your privacy levels as high as possible on social media accounts, so only the people you choose can see what you post.
2. Where possible, delete the offensive or upsetting content.
3. Block accounts that won't leave you alone.
4. Take screenshots of messages, behaviour or content that is causing you distress, and save them to an online place if you can. You can use them to report the behaviour to authorities, including police.
5. Report harassing or bullying accounts to authorities.
6. Talk to someone. There are many online and phone counselling services with caring people who will believe and support you.
7. Shut it down and walk away. Take care of your own mental health by taking a break for as long as necessary. Find more private ways to keep in touch with the people you need to, such as secure text messaging services, where strangers can't find you.

Check out the following resources for more information:

- eSafety Commissioner: Adult cyber abuse
- org: Advice for Adult Victims of Cyberbullying
- ReachOut: 5 strategies for dealing with cyberbullying
- How to take screenshots:
  - Take a screenshot on Mac
  - Take a screenshot on Windows
  - Take a screenshot on iPhone
  - Take a screenshot on iPad
  - Take a screenshot on Android
- eSafety Commissioner: Social media safety tips
- eSmart: Top 10 cyber safety tips
- Lifehacker: The Best Ways to Block Annoying People Around the Web
- eSafety Commissioner: Report social media abuse
- Open Colleges: CYBER SAFETY: An Interactive Guide To Staying Safe On The Internet
- PC Mag Australia: How to Report Abuse on Social Media

○ 11Respectful behaviour online

The internet is public. Once something is in the public domain, it's out there forever. Your friends, family, employers, employees, children, parents, grandparents, fans and enemies are all there.

Every time you interact online, you leave a digital footprint; what you say and do may be found for years, or even decades, to come. Whatever you're about to write, say, do, or display anything, think:

- Would I do this in a public crowd?
- Would I want someone else to record this and show a public crowd, now or in the future?

If the answer is "no", then don't do it. If it helps, step away from your device for a while, give yourself time to think, and come back to it later.

You can model the behaviour you want to see online, and help others. If you see anyone in trouble – for example, being bullied, harassed, stalked, or having material shared about them without their consent or knowledge:

- Report the content, or find someone to help you report it.
- If you have the ability to remove the content, do so. (For example, if you're the admin or moderator of a social media group or forum).

- Don’t forward or share it.
- Don’t take part in it.
- Leave the group or conversation.
- Say something kind or positive to the person.
- If it’s safe, take a stand against it. Ask the bully to stop, and tell them their behaviour is not ok.
- Talk privately to the person being cyberbullied – are they okay, do they need help?
- Provide them with links and resources to report problems and get support.

Further resources:

- Australian Human Rights Commission: Cyberbullying, Human rights and bystanders

Explore more of our resources

- News
  November 4, 2024
  Telstra 3G shutdown is now complete

- News
  October 25, 2024
  Phones using the 3G network to call triple zero will be disconnected on 28 October 2024

- News
  October 25, 2024
  NBN Co accelerating higher speed tiers in September 2025

- Guides
  October 17, 2024
  Connectivity definitions

- Back to resources

-

Didn’t find the answers you were after?

Chat to us on our hotline with one of our team members and let’s get the conversation

started. If we don’t answer, we’ll get back to you in no time at all.

1300 081 029

Category

1. Tech Tips

Tags

1. online safety

Date
20/01/2025
Date Created
12/03/2024