

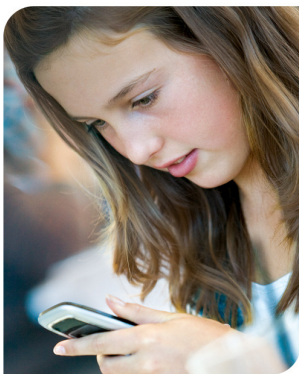


Educating Australian kids, parents and carers about safe and secure internet and technology use is a key priority for Telstra.

The web and technology changes fast and it takes time to ensure that we're on top of these changes to keep our experiences safe.

Telstra takes its responsibility as a trusted internet services provider and integrated telecommunications company seriously. We work with industry, government, community organisations and internet users to address the range of evolving online risks and to develop measures that promote online safety.

- We have been working to help Aussies enjoy their online experiences for many years.
- We recognise the need for every age-group to access information and expertise to allow them to safely obtain full value from their online experience. This continuing commitment is reflected in our awareness programs, retail product offerings and customer communications.



TELSTRA'S TIPS FOR KIDS:

1. Only use the internet when you have your parents' OK.
2. Don't ever chat with strangers online just as you wouldn't talk to a stranger at a shopping centre – not everyone is who they say they are.
3. Some sites are not meant for kids – if you're not sure which sites you can look at ask your parents or teachers.
4. Don't open things from people you don't know. Ask your parents to look at them first.
5. Don't answer messages that are scary, have bad words or are mean. Show them to your parents.
6. Passwords are secret - only share them with your parents never your friends
7. Change your passwords a couple of times a year. Ask your parents if you need help.
8. Be nice when you are talking to people online. If you wouldn't say it to their face, don't say it online or by text message.
9. Never give out personal information, like your address, phone number, password, photographs or birthday.
10. If you feel like you are being bullied talk to someone you trust – don't deal with it on your own. Your parents, teacher or even the Kids Helpline can help you. You can call Kids Helpline on 1800 551 800.

TIPS FOR TEENAGERS:

1. Be careful about talking to people you meet online. Not everyone is who they say they are.
2. Don't post, send or share anything you wouldn't want your parents, teachers, future employers or someone who may be making unwanted advances towards you to see.
3. Remember what you post online stays online for a long time - so think before you click!
4. Keep your private information private – do not give out personal details online like your birthday or address, even on social networking sites like Facebook.
5. Your username and password should belong to you, and only you.
6. Remember to change your passwords regularly. Passwords should be completely random and unique, but still memorable. Try using numbers and letters.
7. Don't leave a computer whilst your account is still logged in - anyone could start using it.
8. If you wouldn't say something to someone offline then don't say it online.



9. Monitor your online and mobile usage. Not all content you view online is free to browse. If you're with BigPond, look out for green dot content as it doesn't count towards your download limit. Look at your usage meter regularly or think about getting a pre-paid account.
10. If you feel like you are being bullied talk to someone you trust – don't deal with it on your own. Your parents, teacher or even the Kids Helpline can help you. You can call Kids Helpline on 1800 551 800 - it's Australia's only free, private and confidential, telephone and online counselling service specifically for people aged between five and 25.

TIPS FOR ADULTS:

1. Use your common sense. If an offer, scheme or sale seems to be too good to be true then it probably is.
2. Keep your private information private – do not give out personal details online such as your birthday and address, even on social networking sites like Facebook.
3. Be wary of emails, phone calls or SMS messages from unknown sources asking you to update, validate or confirm your account details, password or personal information.
4. Remember what you post online stays online for a long time so think before you click.
5. Change passwords at least twice a year.
6. Passwords should be completely random and unique, but still memorable. Try using numbers and letters.
7. Don't leave a computer whilst your account is still logged in because anyone could start using it.
8. Install security software and update regularly to prevent potential viruses and fraud.
9. Always type the address of a website you are wanting to look at in the address bar.
10. Ensure your mobile phone is PIN locked

TIPS FOR SENIORS:

1. Change passwords at least twice a year.
2. Passwords should be completely random and unique, but still memorable. Try using numbers and letters.
3. Install security software and update regularly.
4. Think before you click on links or attachments from unknown sources - it could have a virus.
5. Be careful about what information you disclose about yourself and others online.
6. Don't leave a computer while your account is still logged in, anyone could start using it.
7. Be wary of emails, phone calls or SMS messages from unknown sources asking you to update, validate or confirm your account details, password or personal information
8. Don't respond to offers, deals or requests for your details - independently check the offer.
9. Never send money, credit card, account or other personal details to unsolicited offers. Scams often ask for this kind of information in this way.
10. Always type the address of a website you are wanting to look at in the address bar.



TELSTRA'S TIPS FOR PARENTS TO HELP PROTECT YOUR KIDS IN THE ONLINE WORLD:

1. Keep the family computer in an open area such as the kitchen or living room where it can be monitored.
2. Understand the sites and technology your kids use and know who they're talking too.
3. Create a list of online 'rules' with the family eg. time limits, list of OK sites to visit.
4. Educate your kids so they know not to give out personal details online without parental knowledge.
5. Make sure your kids know what to do and where to go if they encounter cyber-bullying.
6. Regularly sit with your kids when they are on the internet or look over their shoulder. Let them know you are keeping track of their online activity.
7. Keep online friendships online – never let your kids go to meetings with 'online' friends without parental supervision.
8. Talk with your family about the risks of internet use, particularly in chatrooms.
9. Reinforce positive behaviour and values in the online world.
10. Don't ignore new technologies – kids and teens will use them, if not at home then at their friends' houses or in the school yard.
11. Install software or services that can filter or block offensive websites. Visit www.acma.gov.au for more information or www.bigpond.com/internet/services/security/ for a suitable product.

12. Visit www.cybersmart.gov.au for other valuable information on how you can keep your kids safe online

TIPS FOR HELPING YOU SHOP SAFELY ONLINE:

1. Do some research. Check out other items in a similar condition - is the asking price reasonable?
2. Find out as much as you can about the item. Read the description carefully and check the photos closely. If you're unclear about any details, ask the seller for a bit more info. For big ticket items such as cars and boats, it is always worth going to inspect them first.
3. Check the payment and delivery options. Make sure you understand the payment and delivery options and any other terms or conditions the seller is stipulating before you commit to buying the item.
4. Know who you're buying from. Check the seller's feedback and ratings from previous transactions. Reading feedback from other buyers is a great way to judge if a seller is an honest and reliable trader.
5. Choose a payment method you feel comfortable using. Safer payment methods provide you with proof of payment. Never send cash in the mail or use money transfer services (eg Western Union or Money Gram) to send payments to people you don't know.
6. Be aware of the latest online scams. Pay particular attention to sales where the item seems underpriced.
7. Trust your instinct. Things that seem too good to be true often are!
8. If you have concerns regarding the legitimacy of a particular seller or advertisement(s) contact the website that is hosting the advertisement(s) for their advice.
9. Be very wary of anyone requesting you to send funds overseas, it could be a scam.
10. Be aware that counterfeit goods are sold on line as well, if unsure of an item's legitimacy ask the seller if a certificate of authenticity comes with the item.



TIPS TO HELP KEEP YOUR MOBILE PHONE SAFE:

1. Be careful who you provide with your mobile phone number and respect your friends' privacy by not giving away their details.
2. Ensure your mobile phone is PIN locked.
3. Ensure you know what to do and where to go if you receive unwanted text or voice messages.
4. Notify your mobile service provider if your phone is lost or stolen.
5. Monitor online usage – not all content viewed on a mobile phone is “free to browse”. Think about if a pre-paid plan would suit you better.
6. Think before you send. The person who you send text, picture or video to may not be the only one who will see them.

TELSTRA'S HANDY TIPS FOR ONLINE GAMING:

1. Keep your private information private - create safe nicknames, usernames and gamer tags.
2. Play online or download games from reputable sites. Proven sites are not likely to give your machine malware problems or abuse your personal information.
3. Make sure you understand a game's ratings and terms and conditions before you start - this will help you understand what type of behaviour is expected of you.
4. Cyber-bullying can happen in the gaming world too. If you experience anyone who is abusive block further contact and let your parents know if you feel threatened.

COMMON SCAMS TO BE AWARE OF....

1. **Phishing**

Beware of any unsolicited emails from organisations requesting you to update your personal/financial details. To make their emails look genuine, the phishers may have copied an organisation's logo, images or even their entire website. Call your service provider if you are unsure.

2. **Wire Transfer Scams**

Beware of any sellers requesting you to send funds overseas - this scam involves the seller engaging the buyer off-site (usually via email) and convincing them to send money through an international money transfer service for an item that will never be shipped.

3. **Domestic Non-Delivery Fraud (Domestic)**

Beware of ads for high value electronic items advertised for a low price - unsuspecting buyers make contact and send funds to the seller but never receive the item.

4. **Buyer Fraud Scam**

Beware buyers requesting you send the item you are selling overseas. They may send a fake invoice from a financial provider to dupe you into thinking they have paid.