How to help children be safe online

Parents and caregivers can support children of all ages to have safe and positive experiences online

Top cyber smart tips for parents

- Always consider your child's age and maturity and how this may impact their safety online
- Learn how to set parental controls and limit access to adult content
- Disable in-application purchases on your child's phone
- Ensure your child knows to only share personal numbers and details to people they know and trust offline
- Turn off a phone's location settings when using it to access social media sites
- Create a family media agreement with tech-free zones such as cars, bedrooms and meals. Help your child learn to filter information online and navigate fact from fiction
- During SIM card registration, check that the personal information you share will be well protected.

Protecting your child's privacy online

A few simple steps can help parents and children keep their information private when using the internet.

Use privacy settings and review them frequently:

- All social media platforms offer privacy settings. Sit down with your children and go over their privacy settings.
- On Facebook, the safest privacy setting to use is 'Only Me'. Also, check your app settings on Facebook to see what you've agreed to share with each app.
- When your child gets a new device or signs up for a new website or , establish their privacy preferences. Follow directions during initial set up.
- Although it might not be practical to read every Terms of Service contract, it is good to remind children to be aware of what information they are agreeing to share before they start using applications, websites or devices.

Use two-factor authentication:

- Most social media platforms offer two-factor authentication, which allows you to authorise only certain devices to access an account. It increases your security because it prevents people from logging into your account if they have your password.

Delete old accounts and update your passwords:

- Hackers can get to you by going through your previous social media profiles. To find old accounts, Google your name; you might be surprised at what you find.
- Update your passwords and choose strong passwords.

Children must be aware of information shared online:

- Teach children about definitions of address, phone number, birthdate and other personal information.
- Make sure they understand the basics of good online behavior, including the impact and potential repercussions of posting or commenting online.

Protections for children:

- Some legal restrictions are in place to help protect your child's consumer privacy and ensure they are using age-appropriate websites and applications.
- For example, the Lukautim Pikinini Act 2015 explicitly elaborates on measures to ensure the protection and privacy of each child. It stresses the importance of parental/guardian consent when using or sharing a child's image or information. Parents' awareness of their obligations under the legislation will help them to support online safety.

Cyberbullying

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. Parents play a critical role in preventing and responding to cyberbullying.

What to do if your child experiences cyberbullying:

- Contact the site administrator to have bullying content removed.
- Report bullying to the school if it is coming from another student. Schools are encouraged to develop their policies to protect students and can help stop bullying.
- Talk to your child or young person about getting support if they are very upset.
- Report any serious threat to local police. A threat made online could be against the law.
- Children under the age of 18 with a mobile phone should have parental control and limitations on phone and internet access.

Parents must ensure that children and young people know:

- How to ignore bullying messages and how to block unwanted contact on email, social media, chat rooms, games and other programs
- To keep a record of bullying messages so you can report it
- How to support a friend if they are being bullied, and to tell a responsible adult
- Not to bully others.

Tips for internet safety and preventing cyberbullying:

Know your technology. If you allow your children to carry mobile phones or work with other technologies, learn how to use them yourself. Take an interest in your children's online world.

Set reasonable limits. Help your children learn to make responsible decisions about using technology by establishing guidelines and exerting control when necessary. Investigate all the features of the technology they use. Mobile phones with internet access should have the same guidelines and safety measures as those for household computers.

Get to know you children's online friends. Help your children learn the difference between a real friend and a friendly stranger. Monitor their virtual friendships. Instruct them never to meet online friends.

Talk with your children if you suspect they are being bullied. Changes in your child's behavior and attitudes can signal that they are being bullied at school or online. Victimised children are more likely to have difficulty sleeping, headaches, nervousness, stomach aches, and make excuses to avoid going to school.

Help children understand the difference between tattling and reporting. We must help children speak up when they are being victimised or witness someone else being victimised. There is a difference between tattling and reporting. Tattling is when you tell something to get someone in trouble. Reporting is getting someone help to keep them safe.

Show your children you love them and will protect them. Children who are bullied are at risk of a variety of mental health problems such as depression, anxiety, diminished self-esteem and social withdrawal.

Protecting children from image-based abuse

Image-based abuse can include the non-consensual sharing of images, including the illegal distribution and sharing of 'nudes' i.e., naked images.

Children are vulnerable to being pressured into sending private, and sometimes explicit images of themselves via social media, chat rooms, and text messages when they are engaging with strangers online. This practice is a violation of domestic law, and is a serious threat to the privacy of children.

If a child is below the age of 18, the sharing of their private images is always a crime. The above protective measures apply, however other actions for parents include:

- Talk to children about the nature of online images, and that they can never be completely removed from the internet and so should never be sent to anyone. Consider explaining that sharing their own images may also be a crime if they are under 18.
- If your child's privacy has been violated, submit a request with the relevant website, or contact an e-safety authority to try and have the image removed. Screenshot it for evidence.
- This experience can be highly traumatising for children, so consider supporting them through engaging a counsellor.

For more tips and information visit https: //www.facebook.com/pngsaferinternet-committee

Acknowledgement: Sponsored by the Australian Federal Police Cyber Safety Pasifika team in collaboration with the PNG Safer Internet Committee.