Creep Quiz

More information

Shifty Shane

Fact

Only 46% of teens have turned off location-tracking features on their mobile phone or within an app.

What this means

Almost all smart devices have an inbuilt Global Positioning System (GPS). GPS is a satellite navigation system that can provide pin point location services. Most smartphone users want GPS turned on to use map navigation. Very few users really need, or even want, GPS turned on for their camera or social media apps.

Location tracking coupled with address information can help strangers identify when people are absent from their homes.

Tablet and mobile devices have parental controls which prevent access to specific features or content. Reviewing parental controls and disabling GPS for camera and social media apps will offer an extra layer of protection against providing too much information to the public.

What you can do

- Review the 'location services' or 'location settings' on your child's smart device and turn off GPS for the camera, chat and other social media apps.
- Talk to your child about the extra meaning some social media posts have. For example, the status update "So happy to be on holidays for a week – beach time!" may look like an innocent enough post. This update is telling all online friends that your child (and maybe you as well) are away from home for a week. If location services are turned on and your child has checked in to the holiday resort, everyone knows just how far away from home you are.
- Set clear rules about your child's mobile phone and online activities. Talk with your child about which websites and internet activities they are allowed to access.
- Check the age suitability of any app, website or social networking sites your child joins.

Sources

Teen and mobile applications privacy - http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy/

Gossip Gabby

Fact

58% of 18-25 year olds regret something they posted as a young teen.

What this means

Everything you post online contributes to your digital footprint. What you think you're sharing with your friends may also be viewed by a much wider audience – including future employers, workmates and landlords.

Personal information, once posted, can be very difficult to remove. Sensitive or inappropriate comments or images are generally irretrievable. This can be of particular concern if your child's online friends share sensitive information about your child or other people, to show off or provoke a reaction.

It can be useful to encourage your children to always 'think before they post' as a strategy to protect themselves, and to never post anything they wouldn't say to someone's face.

Question and Answer websites such as Ask.fm, Qooh.me or FormSpring are popular amongst young people. These types of sites generally allow users to post questions whether in text, images or video to the walls of other users' profiles. Often no mutual friendship is required and anonymous postings are frequent. Unfortunately, the anonymity feature is too often misused, with users sending abusive, bullying and inappropriate content.

What you can do

- Make cybersafety and cyberbullying part of the conversation about being a polite and responsible citizen. The golden rule of treating others the way you want to be treated applies online as well!
- Encourage children to keep online content true, useful and positive to maintain a positive digital footprint.
- If your child has a question and answer profile, it is recommended you regularly monitor the wall content and assist your child to disable anonymous questions.
- Encourage children to 'think before they click.' Ask them to think about content and the consequences of posting it. Are they aware that something that happens on the spur of the moment can still be online years later?
- Bullying and violence online are not okay at any time. Report online bullying involving school friends to your school.
- Help your child to report any inappropriate online content to the website or app and help them, to block the profile of the person responsible.
- Do not respond on your child's behalf. This may further inflame the situation.
- Serious instances of cyberbullying and inappropriate online behaviours can constitute a criminal offence. If you have concerns for your child's safety, report incidents to your local police.

Sources

Telstra survey, “Australian Digital Natives 2014: Decoding attitudes and behaviours towards cyber safety”, prepared by Pureprofile for Telstra, January 2014

Creepy Crackers

Fact

88% of self-generated explicit images of young people have been collected and put on other sites.

What this means

Strangers may pose as teenage boys and girls online and strike up conversations with children, or encourage them to share private information and photos.

If someone isn't known to your child in the real world, we recommend they are removed from their online friends list.

What you can do

Talk with your children about their digital lives. Create conversations and stay involved. The more you are aware of their online lives, the more comfortable they will be talking to you, especially when something makes them feel uncomfortable.

Encourage children to 'think before they click' to maintain a positive digital footprint. Ask them to think about content and the consequences of posting it. Would they be happy for grandma to see it? Are they aware that something that happens on the spur of the moment – a funny picture, an angry post – can still be online years later?

Be wary of friend requests from people you don't know. Review your child's contacts and followers on social networking sites/apps to reduce the risk of them associating with unknown people and inappropriate content.

Review your child's privacy settings on profiles to ensure appropriate content is visible to the public and friends.

Try to keep all internet-capable devices in visible areas of the house, like the family room.

Help balance your child's screen time by considering a curfew or rules about the times children can use devices.

Create an account on the social networking sites your child uses and ask to become friends or follow their account. This can increase your understanding of the online environments they use.

Sources

Internet Watch Foundation Report - https://www.iwf.org.uk/about-iwf/news/post/334-young-people-are-warned-they-may-lose-control-over-their-images-and-videos-once-they-are-uploaded-online

Poser Pete

Fact

The average teen will never meet 25% of their online friends.

And, 80 million Facebook accounts are bogus.

What this means

Poser Pete is a 'friend addict'. He wants as many friends or likes as possible and he doesn't care where they come from or even whether he knows them. He's just as careless with how he treats the information he has access to. If your child is friends with him, their personal information could be viewed by complete strangers.

Most social media sites allow you to like, tag and share content. Every time one of your online friends likes your post it will make it visible on their profile to all their friends. If someone in your list of friends has a public profile or unknown people in their friends list, your post can quickly be viewed by a very large audience.

What you can do

- Review liked, tagged and shared content and the privacy settings on your child's profile to check what is visible to the public and friends. Help them remove content that is negatively impacting their digital footprint or content they did not mean to share.
- Be wary of friend requests from people you don't know. Review your child's contacts and followers on social networking sites/apps with them, to reduce the risk of them associating with unknown people and inappropriate content.
- Customise the way you post on your profiles so posts aren't visible to the public.
- Parents should get to know social media. Take some time to research online networks and mobile apps, in particular the:
    - privacy settings; including how to unfriend, report and block users.
    - common features and terminology
- Search online networks for useful links such as safety centres, forms for reporting inappropriate content, and terms and conditions. It may be helpful to bookmark these pages.

Sources

Pew Internet, Teens, Social Media, and Privacy. May 21, 2013 by Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, Meredith Beaton - http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

Mashable 2012 - http://mashable.com/2012/08/02/fake-facebook-accounts/ Sourced from 10Q-filing

Scammer Steve

Fact

Over 75% of 14-15 year old users post personal information online – especially photos of themselves, their school and full name.

What this means

Be smart about the way you and your children interact with social media. Don't click suspicious links in emails, fake ads, or messages in pop-up windows. Savvy scammers create viruses and malware that could end up on your device by clicking that dodgy link.

Once on your device, these viruses and malware could be collecting your information without your knowledge. Identity theft is when your information is used by another person without your permission. Scammers could be using your information to open an account, create a profile or even borrow money in your name!

Some social media sites have additional layers of security to protect your profile (often called two-step verification). Explore the options available and tailor your security settings.

What you can do

- Review privacy and security settings on profiles to check what is visible to the public and friends.
- Customise the way you post on your profiles so posts aren't visible to the public.
- Use nicknames not full names and hide key personal details like your date of birth from being openly viewed.
- Be wary of friend requests from people you don't know. Review your child's contacts and followers on social networking sites/apps to reduce the risk of them associating with unknown people and content.
- Talk to your child about the importance of logging in to their social media profiles from the designated URL. For example, if you want to access Facebook, go to the website at www.facebook.com do not click a link from another site or email that says it will take you to your Facebook profile.
- Get your child to review their password and discuss with them:
    - that strong passwords contain a mixture of upper and lower case letters, numerals and symbols. Avoid dictionary words – especially PASSWORD! – or personal references that would be easy to work out – e.g. JaneSmith123.
    - the importance of keeping passwords private. Your child's password should be known by themselves and their parent or caregiver only.
    - that it is a good idea to have different passwords for different accounts – otherwise if one account is compromised it may give a hacker access to all your online accounts.

Sources

Australian Media and Communications Authority. (2013). Like, post, share: Young Australians' experience of social media (Quantitative Research Report). Canberrra: ACMA - http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/young-australians-and-social-media

Bully Girl

Fact

21% of 14-15 year olds reported being cyberbullied.

93 per cent of 14-15 year olds who experienced cyberbullying were likely to have told their parents.

What this means

Bullying is an ongoing abuse of power to threaten or harm another person. Cyberbullying is the broad term that describes when technology is used to verbally or socially bully another person. This cyberbullying can occur via email, mobile phones, online games and social media sites.

The increase of social media can mean that bullies are able to target their victims 24/7 on a variety of platforms. Some children do not report cyberbullying because they don't want to lose their technology or devices. Be supportive of your child and keep the conversation open.

Bullies thrive on attention. Responding, or engaging in an argument with bullies may make the situation worse.

What you can do

- Bullying and violence online are not okay at any time. Report online bullying involving school friends to your school.
- Help your child in reporting any inappropriate online content to the website or app and help them to block the profile of the person responsible.
- Discuss with your child how they can keep cyberbullying evidence if something goes wrong. Most smart phones can take screenshots and you can 'print screen' on PCs and laptops to save the evidence for later.
- Do not respond on your child's behalf. This may further inflame the situation.
- Talk with your children about their digital lives. The more you are aware of their online lives, the more comfortable they will be talking to you, especially when something makes them feel uncomfortable.
- Make sure your children know you will be supportive if they report something to you.
- Promote positive bystander behaviour: Work together with your child ahead of time to come up with safe ways to stand up to online abuse if they see it happen.
- Serious instances of cyberbullying and inappropriate online behaviours can constitute a criminal offence. If you have concerns for your child's safety, report incidents to your local police.
- Consider installing the 'Cybersafety Help Button' on all devices, available from the Commonwealth Department of Communications' website: http://www.communications.gov.au/online_safety_and_security/cybersafetyhelpbutton_download/

Sources

Australian Media and Communications Authority. (2013). Like, post, share: Young Australians' experience of social media (Quantitative Research Report). Canberrra: ACMA - http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/young-australians-and-social-media