Learning objective: build your kids cyber street smarts. You can't start cyber security and awareness too early. Kids need to be streetwise and cyber smart as early as they can be. The longer you leave it, the more at risk they will be as well as the people and institutions they interact with. Criminals are just waiting for them to act before they think.

The Fundamental Six: here are six fundamental tips to build into your discussions and curriculum for kids on identity theft and the online environment:

(i) **Check before you click –** ask yourself, am I comfortable with the information I'm about to share online? You've got to assume someone else is able to access what you share (criminals and future employers to name two!)

(ii) **Don't accept the default –** configure your system to its highest security settings. The default settings for most aren't that high and assist direct marketers track your child's movements online to target their products more effectively.

(iii) **Be strong and regular –** we don't mean in a digestive sense. Create strong passwords (recommend case sensitive, alpha-numeric passwords of at least nine characters). Change these regularly and ensure you have disabled your "key-chain" (for Macs). Don't know what that is? Click here.

(iv) **Don't wait to update –** run your virus scans regularly and ensure you download the latest updates. That means for your mobile and tablet devices too.

(v) **It's awesome to ask –** if you are a little unsure about what to do ask a friend or family member. It's not awesome to keep quiet.

(vi) **Do all devices –** don't forget that anything that has connection to the Internet needs all of the above. Don't forget your smart phones, tablets, laptops as well as your PCs.

Some Real Life Discussion Prompters

(i) **Sally** saw a post from one of her friends asking for details about her first school. Sally sent her what she needed and then saw another request for details on her Mum's maiden name (name before she got married). Her friend said it was for a project. Sally passed the details. What she didn't know was that her friend wasn't posting on her social network, it was someone who had stolen her friend's identity and now Sally was the target. What would you have done if you were Sally?

(ii) **Jono's** Dad just bought him a tablet to remain connected when he goes away on holidays. He's just synced his new tablet and has all the great apps he previously downloaded on his Dad's tablet. Jono's just started to use online banking and always has trouble remembering his account number and password. To make it easy he's saved these details in his "Notes" application on the tablet. Whenever the option presents he also requests that his other applications remember his usernames and passwords. Why should or shouldn't Jono do this?

Some Real Life Discussion Prompters

(iii) **Eve** was just emailed a fantastic opportunity to complete a survey where she could win a trip overseas. The email came from a company known for its security awareness. Eve got right to it. The questions were pretty detailed, including date of birth, place of birth, where she banked and with who, how much she spent each month, what she purchased, whether she had any brothers or sisters. It took about twenty minutes to complete before she hit submit. Within a short time Eve received an email from her brother asking to confirm her banking details. What would you advise Eve to do?

(iv) **Cody** just got a call on his mobile from his service provider stating that they have just detected a fault with his account and that there is a better plan they can put him on. The operator asks Cody to confirm his full name, date of birth, email address and account number. Cody provides these details and the operator tells him he will receive details on the new plan via email. Cody receives the email and clicks on the link provided for details of the new plan. A few days later his mobile phone stops working and his bank advises him that there have been a number of transactions on his bank card that need him to confirm they are correct. How do you think this has happened?

If something bad happens or is suspected of happening, here's some ID First Aid we recommend:

What's Needed Now - Immediate Response

- ☑ **Call iDcare (1300 432 273 Aust / 0800 201 415 NZ)**
  - **Develop an inventory of 'at risk' details**
  - **Get a free tailored response plan**
  - **Regain control and get back on track**
- ☑ **Report to Police and get a reference number & copy**
- ☑ **If it's online (PC, Macs, Tablets, Mobiles)**
  - **Reset passwords and PINs**
  - **Clear history and remove Cookies**
  - **Undertake a complete system virus scan**
  - **If necessary, reinstall operating system**
  - **Check your privacy settings**
- ☑ **Contact your financial institution(s)**

What's Needed Going Forward – Mitigating the Risk

- ☑ **Ensure your devices have the latest security updates**
- ☑ **Check your credit history**
  - **Veda (veda.co.nz or veda.com.au)**
  - **Dunn & Bradstreet (dnb.co.nz or dnb.com.au)**
  - **Experian (experian.com.au – Aust only)**
  - **Centrix (centrix.co.nz – NZ only)**
- ☑ **Check your transaction statements closely**
- ☑ **Regularly change your passwords and PINs**
- ☑ **Keep your documents locked and secure**
- ☑ **Never communicate personal details on social media sites**
- ☑ **Never open and click on links from emails you don't know**

REMEMBER ORGANISATIONS DON'T CALL YOU OR EMAIL YOU FOR YOUR PERSONAL DETAILS. IF THEY DO, SHOULD YOU STAY?

iDcare is Australia and New Zealand's National Identity Theft Victim Support Centre. We are a registered charity and not-for-profit organisation dedicated to supporting individuals, businesses and government agencies respond to identity theft and misuse events. iDcare does not charge individuals for our service, nor do we collect personal information.