Protect your kids online

This fact sheet is designed to help parents talk to their children about online safety and protecting their identity from criminals. Even though your children may be technically proficient on the computer and using the Internet, you can still talk to them about safe online practices.

This fact sheet has been prepared by the Australian Bankers' Association (ABA) and the Australian Federal Police (AFP). Banks and the AFP are committed to helping Australians understand how some simple steps can protect their identities from theft.

IT'S EASY TO BE OVERWHELMED BY TECHNICAL JARGON BUT THE BASIC MESSAGE IS ALWAYS THE SAME

It's easy as a parent to be overwhelmed by the language used by your kids when they start talking about the latest technology. However, children still need parental advice to help them use the Internet safely. No matter what the technology, the reality is that some safety advice that you discuss with your children about how they can protect themselves from criminals does not change.

This fact sheet will help you understand some of the major online threats to your children's identity and gives you some practical tips on how you can talk to your children about these issues. This security information is something that every parent can discuss with their children and is no different to teaching your kids to be wary of strangers.

Knowledge of safety tips can go a long way to helping your kids pick up some of the basics to protect themselves online. You don't expect your children to know how to respond if they are approached by strangers until you talk to them about how to behave in this situation. In the same way, you wouldn't expect your children to know how to protect themselves and their identity from criminals, particularly when they are online. You can't always be there to monitor your kids 24/7, so it is important as parents to do as much as you can to help your kids to help themselves.

MY KIDS KNOW MORE ABOUT COMPUTERS THAN I DO!

Some adults may feel intimidated by the Internet, the home computer and are baffled by some of the terms and technology used. While it could be that your children may have more detailed skills than you in using the latest technology on your computer, children still need parental advice to help them safely use the Internet. You don't need to be an expert on how

all the technology works to identify some of the threats to your kids when they go online or to teach them how to deal with a problem if it occurs.

WHAT ARE THE RISKS?

Think of the Internet like walking through an open door into a world where almost anything goes. There is some content which you would be comfortable for your children to see and other content which you would prefer your children were not exposed to.

It may be worthwhile discussing appropriate safety guidelines for using the Internet with your kids and an Internet content filter may be useful for young children. An Internet content filter is a piece of software that helps manage access to online content on your home computer. Installing an Internet content filter reduces the risk of your family coming into contact with something upsetting or dangerous online but like a seat belt in a car it does not offer total protection.

Internet content filters offer a range of different functions to block, screen or monitor unwanted material. Unfortunately, there is no single action or Internet content filter that does everything and it is not advisable to have two or more Internet content filters installed on your computer at the same time. At present, Internet content filter technology is still being developed for use with mobile phones.

Also understand that many people can look at the material which your children post in their blogs, on social networking websites, discuss in chat rooms or provide via their mobile. Unfortunately, in cyberspace, just as in the real world, criminals are looking for ways to use the technology to commit crime and do harm.

Sometimes people who have had their identities stolen by a criminal have inadvertently caused the compromise themselves by sharing too much information, including by responding to hoax or phishing emails, instant messaging or posting too much personal information about themselves on the Internet. For example, if your children reveal their dates of birth, address, telephone number and email account details, they may be unwittingly providing enough information for criminals to steal an identity and use those details to commit other crimes.

Caution must be taken with phishing emails which are scams designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Criminals might send millions of fraudulent email messages that appear to come from websites you trust, like your bank or other legitimate businesses and request that you provide personal information. Everyone, including children, should be wary of unsolicited email.

It's important to remember that banks will never send you an email asking for personal security details like your Internet banking password or PIN. If you or your child receives a phishing email – do not respond to it and delete it from your system. Do not click on any links in the email as the link may take you or your children through to a hoax website which has been set up by the criminals to collect personal information.

COMMUNICATING YOUR ISSUES

If you start by telling your child never to do something most children will ask "why not?" and then try to find out for themselves by doing it anyway!

Discussing the potential dangers with your children therefore needs care and sensitivity and involves helping them to see for themselves how they might get into difficulty, rather than just blanket "dos" and "don'ts".

No one likes to be talked-down to and your kids are no exception! If you help your kids to understand some of the negative consequences of their actions online that is probably far more effective than just telling them that they can't or shouldn't do something without an explanation as to why they can't or shouldn't do something.

Make sure you explain the "because" of the behaviour you are asking them to adopt and not just the "don'ts" of online behaviour. Children have a remarkable ability to understand a lot when adults take the time to explain it to them in the same way that you would like people to explain things to you that you have never heard of or didn't understand before!

WHAT ARE THE RISKS OF POSTING TOO MUCH PERSONAL INFORMATION ONLINE? WHY SHOULD YOU AND YOUR KIDS CARE?

Personal details your children post on the Internet can be a target for criminals. One example is that criminals have programs that trawl the Internet searching for personal information which can be used to defraud or do harm.

Criminals can use personal information posted on the Internet by your kids to steal or take over your kid's identity. From that, criminals can create fake IDs and commit a range of other crimes, using your child's identity as a cover for their criminal activities. Criminals can create fake birth certificates, driver's licences and passports. Once this is done, criminals can use these identity documents to get involved in all sorts of criminal activity, such as child pornography, drug trafficking, money laundering and counter-terrorism financing, opening up false lines of credit with banks, other credit agencies and Internet Service Providers and telecommunications providers in your child's name.

SAFETY TIPS

Just as you would talk to your children about how to safely cross the road or how to respond if they are approached by a stranger, you can also have a conversation about how they can protect themselves online. The earlier you start talking to your kids about safe online behaviour, the easier it will be for them to develop good habits.

Some safety tips you might share with your kids include:

- **Don't post too much information online –** online social networking can be a great way for kids to exchange photos, expand their networks and pursue new interests. However, publishing personal information online comes with risks attached. It gives criminals access to information which they can use to steal your identity and commit a range of crimes. Make sure social networking profiles are private and suggest that children limit their online friends to only those they know in the real world.

- **Don't answer questions with too much information** – such as when responding to questions over the Internet or when using instant messaging, in chat rooms or blogs or by responding to phishing emails and other online scams.
- **Be careful in choosing screen names** – choose screen names which do not reveal too much personal detail or an email address. Do not choose anything that reveals gender, location or age.
- **People aren't always who they say they are -** not everyone online is honest. You need to help your children understand that, even though they may believe they are communicating with a person claiming they are a young person, a criminal could be deceiving them. The anonymity of the Internet allows criminals to pretend to be someone they are not.
- **Be very careful about publishing photos online or sending them via phone –** children should be careful about publishing photos of themselves, their friends and family on the Internet. Just remember, it's not only the people whom you want to share these photos that may be able to see them. Photos posted on the Internet or sent by mobile phone may be accessible to people you don't know and can make it easier for a stranger to find you or to impersonate you.
- **Don't publish your email address online** – this is a major cause of receiving unsolicited email. These emails are often phishing scams.
- **Treat all unsolicited email with caution** – it is very important to be sceptical about emails asking for personal information or which ask you to 'go to' or 'click on' a link to a certain website. Caution must be taken with phishing emails which are seemingly authentic messages that appear to have come from banks, other financial institutions or legitimate businesses but are designed to lure recipients into divulging personal data such as bank account numbers and passwords. Everyone, including children, should be wary of unsolicited email.
- **Do not click on a link in an email** - open your browser and type the address.
- **Discuss where your child can and can't go on the Internet** – just as you would discuss why your child cannot watch a movie rated 'R' or 'MA' or 'M' , it is a good idea to have a conversation about the content they might access on the Internet. Advice for anyone who has come across Internet content they feel is inappropriate or illegal may be found at the Australian Communications and Media Authority: www.acma.gov.au
- **Ensure your child knows they can talk to you about anything they experience online** – it's important that you explain to your children that, if they are concerned about what they have done or what they have seen online, they can come and speak to you and that you'll understand and help them deal with the issue.

SECURE THE HOME COMPUTER OR YOUR CHILD'S LAPTOP

It is important to protect any computer, including any computer your children use if they are using the Internet.

Only use a trusted and secure computer. Using publicly shared computers, such as those at

Internet cafes, is strongly discouraged, especially for Internet banking, conducting any online transactions or providing sensitive personal information to any source.

We recommend you secure your home computer and child's laptop by:

- Installing reputable anti-virus and firewall protection on your computer. This provides additional layers of protection that help to reduce your risk of exposure from viruses that can rob your computer of valuable personal information.
- Regularly update your virus protection software – updates for virus protection and security can be set up to occur automatically.
- Install any security patches for your operating system and other software installed on your computer and keep these up-to-date.
- Parents may also like to consider the placement of the computer in the home. If the home computer is in a high traffic area of the house, it may be harder for a child to access inappropriate content or behave inappropriately online.

DO THE SAME THREATS EXIST WHEN MY KIDS ARE USING A MOBILE TELEPHONE?

The next generation of mobiles and handheld devices already offer Internet services, such as access to social networking profiles and instant messaging, so the same threats exist, just like when you access the Internet on your computer.

You should advise your children not to provide phone numbers to people they don't know; that means the number of their mobile, yours or their friends and applies to landlines as well.

Another threat that has emerged is "smishing". Smishing is basically the text messaging version of "phishing". Criminals have been using this technique to lure children into providing personal details about themselves through text messages.

Just as we advise you not to respond to emails where the sender is unknown, the same goes for text messages from telephone numbers you don't know. Usually these messages outline offers that are 'too good to be true' and invite the recipient to respond or provide personal information. You or your children shouldn't respond to these offers which are usually scams.

WHAT DO I DO IF I THINK MY CHILD HAS BEEN TARGETED BY CRIMINALS ONLINE OR HAS HAD THEIR IDENTITY COMPROMISED?

If you or your child has been the victim of a crime, you must report it to Police in your State or Territory, or to Crime Stoppers on 1800 333 000.

If you suspect that someone may be attempting to target you or your child, you may like to consider the following options:

- Block communication - more information on how to stop unwanted contact can be found at www.thinkuknow.org.au
- Block communication through the mobile phone by contacting the telephone provider;

- Delete social networking profiles, websites, or email accounts and report it to the relevant administrators of the website. If you or your child sets up a new profile account on a social networking website, make sure the highest security settings are activated.

FURTHER INFORMATION

There is a lot of information on the ABA website and the banks' websites on how you can secure your home computer if you are using the Internet.

The ABA, Australian Securities and Investments Commission (ASIC) and the AFP have worked together to produce a website called 'Protect Your Financial Identity' www.protectfinancialid.org.au which also provides tips on how you can avoid becoming a victim.

The ABA also provides two useful fact sheets on its website:

- Protect Your Financial Information Online
- Protect Your Financial Identity

The AFP is implementing a program called 'ThinkUKnow' - www.thinkuknow.org.au - an Internet safety program delivering interactive training to parents, carers and teachers through primary and secondary schools in the ACT, NSW and Victoria using a network of accredited trainers. The ThinkUKnow program will be available across Australia in 2010.

This fact sheet can be found on the following websites:

ABA: www.bankers.asn.au

AFP: www.afp.gov.au

Created: August 2009

Internet: www.bankers.asn.au www.afp.gov.au

Phone: 02 8298 0417 Fax: 02 8298 0402