ThinkUKnow e-Newsletter - Volume 3 Issue 6

National Cyber Security Awareness Week is held in June each year to remind all Australians of their obligations and obstacles in managing the security of their devices and information. Awareness weeks are important events in driving attitude and behavioural change, the dilemma is maintaining those changes throughout the year. In this edition of the ThinkUKnow e-newsletter, we're going to look at some non-technical steps to help your family become more cyber secure.

Take it slowly

Many scams are successful because they force users into acting or responding quickly, with very little time spent thinking about what they are actually doing. Encourage your family to go about things a bit more slowly, allowing time for their brain to kick in. If you receive an email claiming that your account will be shut down if you don't respond immediately, step away from the device and really think about what you are doing.

This simple step may stop you falling for a scam and losing money.

Have a separate credit card for online purchases

If your credit card is compromised online, it can have some nasty consequences for your finances. If you are able to, organise a separate credit card which is only used for online purchases and lower the credit limit as well.

This simple step could minimize the impact

Time2Talk

This section provides some useful conversation starters for talking with young people about their use of technology.

Have you seen any scams on Facebook?

How do you know the difference between a scam and the real thing?

What are some details which you should never share online?

When was the last time you changed your passwords?

Talk about scams

There can often be a sense of shame in admitting that you've fallen for a scam and people can avoid talking about these embarrassments. New scams are created every day and it can be hard to keep up with the latest threat. It can be worthwhile regularly talking about scams: those you've heard from friends, experienced yourself, seen on the news or strange communications you've received and are unsure about.

This simple step could alert you to scams you may have otherwise fallen for.

of any online compromise to your credit card details.

Look for https

Websites that begin with http**s** and not simply http are housed on a secure server where information is encrypted when transmitted. Whenever you are asked to transmit sensitive information such as credit card details or personal information, you should ensure that the website is using a secure server. Most banking and shopping websites do use secure servers but before you enter in any information, double-check that the website begins with http**s**.

You can also set your Facebook profile to only be viewed on a secure server. This can be activated by accessing your *security settings* and enabling *secure browsing*.

This simple step will ensure better security for the information you share online.

Have a list of details not to be shared online

Some scams operate under the guise of a competition where users are asked to enter in some details in order to claim their prize. Some people, caught up in the excitement of winning something may forget that these details shouldn't be shared online.

It may be worthwhile writing down a list of details that shouldn't be shared online or need a parent's permission before sharing. This list could include items such as address, mother's maiden name, phone number, passwords or credit card numbers. Placing this list in the areas where family members access the internet may serve as a visual reminder of what should and shouldn't be shared online.

This simple step could aid family members remembering their cyber security obligations.

Set up two password change days a year

The Australian Government advises users to change their passwords at least twice a year. To remind you to change your passwords, designate two password change days a year and mark them in your calendar or set a reminder on your phone.

These password change days are great occasions to reinforce the need for strong passwords: mixture of upper and lower case letters, numbers and keyboard symbols. You can even use pass phrases as an even stronger protective mechanism. Passwords or pass phrases should be different for each account you use.

This simple step could improve the security of your accounts and prevent them being compromised.

Has your school/organisation hosted a ThinkUKnow event?

You can book a ThinkUKnow event for your school/organisation which is targeted at parents, carers and teachers by accessing our online booking tool. You can also talk to a member of our booking team by phoning (02) 9023 8909.