ThinkUKnow e-Newsletter - Volume 5, Issue 7

Being safe and secure when using the internet is much like trying to stay fit and healthy; at different times throughout the year we need to protect ourselves from different challenges. As spring approaches, we prepare for hayfever and when it's summer we take steps to protect ourselves from sun damage. Likewise, the challenges we face from internet and mobile scams are heavily influenced by current events and yearly occurrences.

When it is time for us to complete our tax returns, we are more likely to receive scams claiming to be from the Australian Tax Office. When a major disaster or tragedy strikes, we are confronted by those who claim to be charities offering a means to support victims, when in fact they are simply defrauding well-meaning citizens. We can see this currently in the aftermath of the Malaysian Airlines MH17 tragedy with people using fake social media pages to take money from people who wish to support families of the victims.

So how do we overcome these challenges? Just as we would take steps to maintain a healthy lifestyle, we need to cultivate good habits in ourselves and the children we care for to prevent falling victim to online and mobile scams. In this issue of the ThinkUKnow e-newsletter, we will cover some good practices to develop in our regular routine of technology usage.

Think before you click

Modern technologies have dramatically improved our ability to communicate with others, but it's important to make sure that the speed of those technologies does not

Time2Talk

In this section we look at ways to start talking with children and young people about their use of technology.

How would you recognise a scam?

How do you know where you will end up when you click on a link?

How can you assess how safe a website is?

When was the last time you changed your passwords?

Monitor your accounts

A good habit to cultivate is to routinely check any bank accounts for suspicious transactions. With many of us now paying bills through direct debit and receiving statements online only, we can overlook any small discrepancies in our transactions. Regularly looking over statements and making sure they correspond with transactions can help us to identify any unauthorised payments which may indicate that our account details have been used by others without our permission.

It's also helpful to monitor our own social media and email accounts as they too may

bypass our sense-checking abilities. Rather than let our emotions guide us, we need to pause and think before we click on any links in emails or social media posts. It's much safer to cut and paste, or type the URL into the browser to make sure we end up at our intended destination.

Many scams rely on us responding straight away and may pressure us to do this by creating a sense of urgency. There is always time to read the fine print or ask someone for advice before responding.

Do a bit of background research

Before submitting personal information or sending money online, it is important to make sure that the organisation is reputable and the site is secure. First make sure that if you are donating money to a charity it is one that is registered and has legitimate contact information. If you can only find information about it in the email or message you have received, chances are it doesn't really exist.

Before putting sensitive information into a web form, such as credit card or bank account details, make sure that it is hosted on a secure server. This is indicated by https at the beginning of the URL, and a padlock or green tick depending on your browser. Forms hosted on a secure server encrypt the information transmitted so that it cannot easily get into the wrong hands.

have been compromised if we have fallen victim to a scam. Some social media accounts allow you to see which devices and locations have been used to log into the account and can help identify if some unauthorised person has accessed the account. It's also a good practice to regularly change the passwords to accounts and make sure we use different passwords for different accounts.

Give yourself a cyber safety health check

Do all your devices have reputable anti-virus software installed and maintained?

Do all your accounts have strong passwords?

Are you aware of how your bank will contact you and how you will receive bills electronically?

Do you regularly monitor your accounts and statements?

Do you and your family regularly discuss cyber safety and security?