ThinkUKnow e-Newsletter - Volume 2 Issue 6

Last week was National Cyber Security Awareness Week (NCSAW), a timely reminder to look at what online safety and security practices your family has in place. NCSAW is organised by the Department for Broadband, Communications and the Digital Economy (DBCDE) and involves participants from government, industry, education and community groups. NCSAW is a great way to get people thinking about their cyber security and we want to encourage you to think about how this affects you and your family throughout the year.

The top tips for NCSAW 2011 were:

1. Install and renew your security software and set it to scan regularly.
2. Turn on automatic updates on all your software, including your operating system and other applications.
3. Think carefully before you click on links and attachments, particularly in emails and on social networking sites.
4. Regularly adjust your privacy settings on social networking sites.
5. Report or talk to someone about anything online that makes you uncomfortable or threatened.
6. Stop and think before you post any photos or financial or personal information about yourself, your friends or family.
7. Use strong passwords and change them at least twice a year.
8. Talk within your family about good

Time2Talk

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

Have you ever received a post from a friend that was suspicious?

How would you identify a scam on Facebook/in your emails?

Do you understand how to use privacy settings?

What are three things you should never post online?

Regularly adjust your privacy settings on social networking sites.

We strongly advise that children and young people set their social networking sites to “private” or “friends only”. This allows them greater control over who has access to their content. For advise on how to enable these settings, please visit our how-to guide.

To illustrate the impact of the various privacy settings on Facebook, we’ve crunched some of the numbers for you. According to Facebook, the average user has 130 friends (although we know that many young people have many more Facebook friends than online safety.

In this issue of our e-newsletter, we're going to focus on those cyber security concerns which are most relevant to children and young people.

Think carefully before you click on links and attachments, particularly in emails and on social networking sites.

Unfortunately, cyber criminals are capitalising on the popularity of social networking sites such as Facebook and using them to distribute malware and scams.

A common example is an email which purports to be from Facebook or Twitter, asking the user to verify their account details or their account will be deleted. This is a scam which uses similar techniques to others: a sense of urgency, a threat, appearing to be from a legitimate source. It's important to remind children and young people to look for signs of a scam and to be aware that these types of emails are fake. For more information on scams, please visit SCAMwatch.

Other security concerns for social networking sites include malware which appear as posts on a user's wall encouraging them to click on a link. It might be a link to a video with the message "Check out this vid – HILARIOUS!" or something similar. When a user clicks on the link, a page appears instructing them to download updated software in order to view the video. This software, instead, contains malware and infects the user's device.

Children and young people should be encouraged to use caution when clicking on links in social networking sites. If the link seems out of character from the person who sent it, they should delete the post by clicking the X on the right-hand side of the post (on Facebook). If they really wish to view the video, they should type in the address of the vendor (such as YouTube) and search for the video. If they have clicked on a suspicious link, they should run a virus scan, change their password to a strong one and warn their friends.

that!). If your profile is set to "Friends Only", only those 130 people can access your content. If your profile is set to "Friends of Friends", potentially 16,900 people can access your content. Finally, if your profile is set to "Everyone", then the 670 million Facebook users and potentially the 1.9 billion internet users can access your content via internet search engines.

All the privacy settings in the world, however, mean nothing if you accept people you don't know nor trust as online contacts. Managing your privacy is a combination of privacy settings, choosing online contacts wisely and thinking before you post.

Stop and think before you post any photos or financial or personal information about yourself, your friends or family.

Pausing for 2 seconds before clicking "Enter" or "Send" and considering the outcomes of actions can save children and young people a lot of grief when it comes to sharing things online. Once something is creating in a digital format and shared, you lose control over who sees it and what they do with it. Encouraging young people to think before they post can help them to protect themselves and the people around them.

App Safety and Security

We've had a lot of parents contact us in relation to smartphone apps and determining their suitability for their children. We've developed some resources on this topic which you can view on our website