ThinkUKnow e-Newsletter - Volume 4, Issue 5

Privacy, or lack thereof, seems to be a constant malign of the digital age. From kids revealing too much information (TMI), to hacktivists revealing sensitive military data, there is no shortage of stories relating to privacy to reference. One of the major questions being asked of late, “is privacy dead?” Perhaps our definition of privacy has evolved over time and one of the most recent catalysts to change has been to rise of social networking sites. In this issue of the ThinkUKnow e-newsletter, we’re going to look at some privacy-related issues and provide some practical steps on managing privacy.

Parents and children - where does privacy begin and end?

In most of our discussions with children and young people, it is obvious that privacy is very important to them, but it is mostly about keeping things private from their parents. So where do we balance a child’s desire for privacy, with parental obligations to keep their child safe. First and foremost, children and young people need to know exactly what information their parents need to know, and why. For example, who it is that they’re video-chatting to ensure they aren’t being exposed to inappropriate communications.

Talking with your child about what information you need as a parent to keep them safe will assist in creating an open dialogue on privacy and hopefully reduce the temptation to covertly monitor your child’s activities. Having these discussions is also useful practice in comprehending privacy policies of apps and social media. These policies outline what private information will be collected, by

Time2Talk

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

What sort of personal information do you think I (as a parent) should know?

Would you trust all your Facebook friends to keep a secret?

What would I be able to learn about you based on the pictures you share online?

How much communication happens between players in an online game? Do you think you could be giving away any private information?

A picture tells a thousand words

Private information can not only be revealed in words, but images and videos as well. Not only could the picture show where a young person goes to school, plays sport or works simply by looking at the uniform they are wearing, but geotagging could reveal even more which isn’t visible to the naked eye.

Geotagging is the process of embedding GPS information in the metadata of a file, most commonly pictures. There are several programs which allow users to extract this

whom, and for what purposes.

A useful conversation starter around privacy is often “Why are you so concerned about what information I, as your parent, can see, when you are giving away all your personal information to an overseas company without even reading their privacy policy?”

It’s only as private as the people who know

We’ve spoken numerous times about having the most secure privacy option on social media sites and apps, but all these settings are made redundant when the wrong people are given access as friends, followers or contacts. Private information is only as secure as the people who know it choose to protect it. Even a “Friends” only account can be unsafe if the people added as friends are not people who are known and trustworthy.

Privacy settings are the first step in privacy management, the next important step is making sure that friends really are people who can be trusted with personal information. A loose acquaintance has nothing to lose from revealing personal information so it’s best not to provide them access to it.

As National Cyber Security Awareness Week takes place later this month, it’s a good opportunity to firstly review privacy settings and make sure online contacts are people you know and trust with your personal information.

metadata and identify exactly where the photo was taken. This sort of information, commonly embedded in instagram and twitter photos, could be misused for a number of criminal purposes.

We need to encourage all users, and children and young people in particular, to consider what private information they may be revealing in a photo and to ensure that geotagging is disabled for the camera on their smart phone.

Games aren’t just about having fun

Many children and young people know how to implement these privacy management strategies with apps and social media, but can seem to forget them the moment they play a game. Although young people will play games for enjoyment and friendship, there are others who use these games to obtain private information, exploit others or harass users.

When we talk about privacy management with children and young people, we need to explicitly mention gaming as an environment where managing your privacy is crucial. We need to impress upon young people that not everyone plays by the rules in online games and they need to be careful who they chat with and what they share.

As a practical measure, encourage your child to choose a username in any online games which does not reveal their year of birth (for example, billy99 would indicate the child is 14) or where they may live.

The internet does not forget

It’s never too early to start talking with your child about privacy management as their information could stay online forever. Effective privacy management skills are essential components of digital literacy and we all need to work together to ensure children and young people develop these important strategies.