
# ThinkUKnow e-Newsletter - June 2015

At a school recently, I brought along some relics of my technological past, including an incredibly not smart phone. The most exciting feature on this mobile phone was the game "Snake", there wasn't even a camera on the phone. After being mocked by today's teens as a glorified paperweight, I spoke with friends about how much easier it was to show mobile phone etiquette back when a phone was just a phone (with a few cool games too!)

These days, however, we have incredibly smart devices within reach almost at all times. While this provides us with a lot of benefits and opportunities, there are also some challenges and concerns that we need to overcome. In this edition of the ThinkUKnow e-newsletter, we're going to look at some issues to be mindful of when using mobile devices.

**I gave permission for what?**

When downloading an app, or using it for the first time, you are often asked to grant permissions for the app to access certain features of this device. This might be to your photos, camera, microphone, contacts or even your messages. Unfortunately, many people simply grant these permissions without fully understanding what information will be collected, how securely it will be stored or how it could be shared. Most of this is outlined in the app's privacy policy…which no one seems to read.

## Time2Talk

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

Have you ever used your mobile on the toilet?

Do you know what information your apps can access about you?

Do you know how to disable geotagging?

What can you do to secure your mobile?

Before allowing an app to access features on your phone, think about what information could be accessed and whether the potential risk of harm is worth using the app. You can retrospectively remove permissions given to apps, so it's a good idea to check and see what settings are currently in place and modify them if required. Also have a look at the customer reviews or feedback for the app to see if other users have raised concerns. Or you could just read the privacy policy…

**Geotagging**

One of the permissions to be mindful of is the access the GPS capability on your device. If your camera has access to your GPS, every photo you take will have the GPS coordinates of where it was taken embedded in the metadata of the image. If this photo is then posted online, someone could access that location information. If photos are taken at home, you could potentially be broadcasting your home address.

Geotagging might sound scary, but it's quite easy to switch off. Simply disabling the GPS capability on your device for the camera (and any other app or feature that doesn't need to know where you are at any given point in time) is all it takes. For more information, you can visit our page on geotagging.

**Bacteria**

According to a recent report, some 25 % of 18-29 year olds use social media on the toilet (Sensis 2015). Now, unless they've got their home office set up in the bathroom, chances are they are using their mobile devices while on the toilet. If that fact alone doesn't make you squirm, let's think about the bacteria from the toilet that's now on your phone.

Combine this with the other bacteria your hands catch and pass onto your device throughout the day, bacteria which thrives in the conditions your phone lives (pocket or handbag) and it's no wonder that some studies suggest that your phone may be up to 18 times dirtier than a public toilet.

But when was the last time you cleaned your mobile phone? It's not something we often concern ourselves with, but regularly wiping down your phone can limit the spread of this bacteria. So the next time you are about to borrow someone's phone, or lend your own, make sure to wash your hands before and after!

**Malware**

Mobile malware does exist and can affect all types of mobile devices. There are more than 6 million samples of mobile malware and approximately 5 % of Australians are infected (McAfee Labs Threats Report February 2015). It may not seem like a huge threat, but if the information on your device was compromised or accessed without your permission, what would the fallout be?

There are anti-virus programs which can be applied to mobile devices and can protect you from mobile malware. More importantly, we need to apply secure practices when using mobile devices, such as only downloading apps from the legitimate stores, not connecting your devices to unsecured networks or devices and practising the same security behaviours you would on a computer or laptop.

**I didn't back it up**

If something did go wrong with your mobile device, you need to ensure you've backed up as much of the information as you can. Our mobile devices often store hundreds of photos and other memories which we would like to protect. This means regularly backing up the device, either onto a laptop/computer or the cloud.