ONLINE SAFETY NEWSLETTER

Providing online safety information for parents and carers

In this issue:

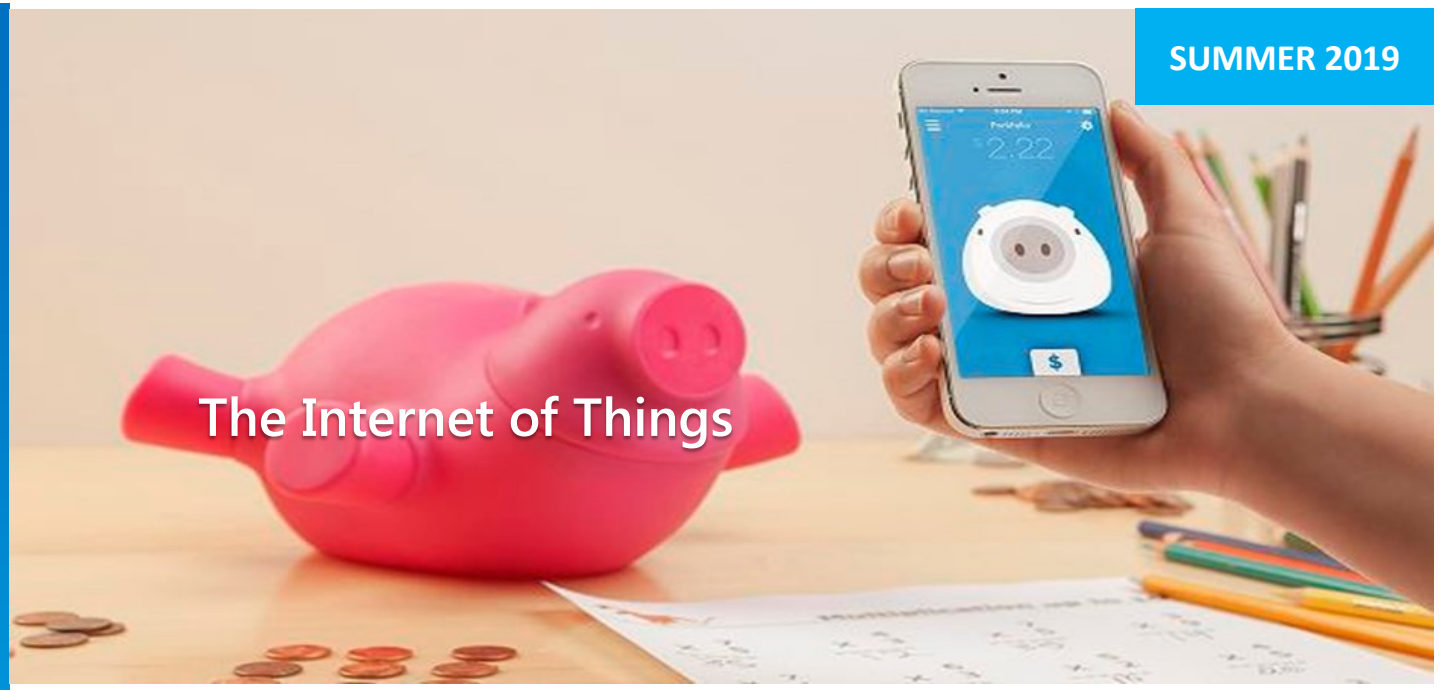
- **The Internet of Things**
- **Viral scares**
- **Anonymous apps**

Devon & Cornwall Police | Dorset Police | PCC | DORSET POLICE & CRIME COMMISSIONER

Strategic Alliance

Get this newsletter sent to your inbox
https://bit.ly/2KcNU2M

SUMMER 2019



What is the Internet of Things?

The Internet of Things are internet-enabled devices such as smart speakers like Alexa and Siri, internet-connected toys, fitness trackers and even Bluetooth enabled toothbrushes. Parents need to be aware of the risks associated with these types of devices.

Some devices collect personal information such as audio, video or images, location data, some allow children to search for age-inappropriate content and some allow children to make 'in-app' purchases and spend money, often on parental accounts. In addition, some devices are vulnerable to being accessed or monitored remotely.

Making the Internet of things safer

- Understand how it works: research carefully before buying and read the manual – the device may communicate via unsecured Wifi or Bluetooth or may record video or audio of the child that can then be transmitted to servers or other devices
- Set up the device correctly: change default passwords and set any parental controls
- Talk to and supervise children using devices: do not assume that devices are safe

More information can be found at https://bit.ly/2VReEhY

Viral scares

Earlier this year, you may have seen stories and warnings about online scares or suicide challenges. In the most recent case, a particular scary image was being circulated in imagery and videos on YouTube videos likely to be viewed by young children, and a number of small children did see imagery that scared them. The reports stated that the imagery was linked with suicide challenges and had been linked to deaths abroad, and that the accounts relating to the image would hurt them or encourage children to hurt themselves.

One of the reasons the story escalated was the sharing of concerns on social media by parents and carers (including celebrities such as Kim Kardashian) without checking the story. Incorrect reporting by usually reliable sources of information, such as the BBC, increased the panic even further.

Undoubtedly, there were some children who did see scary imagery on YouTube but, contrary to reports, YouTube videos were not hacked. It is likely that some users downloaded videos, inserted imagery and then re-uploaded videos on new channels and used hash tags that other users could search for. Other videos were set up by YouTubers as pranks or memes. It is essential that parents understand that even on YouTube Kids, videos are not checked by a human before being made public. Videos are checked using computer algorithms, but if the algorithm has not seen the issue previously it may not be able to identify the content as being inappropriate.

Many parents contacted schools expecting the school to take action. While schools can give advice to children and parents, most of the issues were happening at home where parents are responsible. Some schools spoke to children or parents about the specific concern, and this unintentionally led to children seeking out material featuring the image and being distressed.

In this situation, parents need to look at how they are protecting children from seeing inappropriate content online.

Dorset Police

Be Share Aware NSPCC

internet matters.org

ask about games From The VSC Rating Board

O2 NSPCC Let's keep kids safe online

Follow our top tips...

1. Ensure your children are using appropriate sites using age ratings provided or review sites such as Common Sense Media. YouTube is suitable for children 13 years and over. Even on Youtube Kids, which is intended for younger children, children can come across inappropriate content that has fallen through the net (see above) and it also has adverts. Children are much less likely to see inappropriate content on sites such as CBeebies/ CBBC as these sites will be checked before content is made public
2. Younger children need supervising when online to control what they are accessing and who they can message or chat with
3. For older young people, have clear boundaries and monitor what they are doing
4. Have open conversations with children and reassure them that if they see inappropriate content you can help them
5. Report inappropriate content to the platform it is on
6. Don't pass on scare stories without checking thoroughly – if necessary check with the NSPCC/O2 helpline

More information on this can be found at ThinkUKnow https://bit.ly/2V8R3FI

Anonymous apps

We have seen a recent increase in the number concerns reported by parents over nasty comments on anonymous messaging or feedback apps. There have been many of these types of apps over the years including ask.fm, Sarahah, Tellonym and now Yolo. These apps market themselves as being forums for getting honest feedback. Most work by you opening an account and sharing a link via social media or other platform to your online contacts asking for feedback. Unfortunately, some young people will receive bullying, threats, suggestions that they should harm or kill themselves, or other unpleasant comments, often as pranks, but sometimes from someone trying to hurt or embarrass them. While a number of these apps have subsequently been banned by the App store and Google Play store because of their poor moderation and users reporting bad experiences, similar apps are appearing all the time.

In addition, sometimes young people will share the link to the app in a public part of their social media, such as their Instagram bio, in which case random people can see it and use it.

The latest craze is Yolo (meaning you only live once), which has reached number 1 in the App store downloads and has an age 12+ rating. The popularity of this app seems, at least in part, to be because the app is used via Snapchat, meaning users can shared the link via their existing Snapchat networks. Users can also add an 'Ask me anything 'sticker to their stories which can be responded to – any further response from the user will also be posted onto their story. Currently there is no version for Android but this will almost certainly be available soon.

If your child is wanting to use this type of app, you need to consider what the impact might be for them if (or perhaps when) they receive unpleasant messages .

If you need more information see this review, https://www.net-aware.org.uk/news/anonymous-messaging-apps-whos-asking/