E-Safety Newsletter Issue 4

Welcome to our e-safety newsletter for Parents. We hope you find the information useful and informative.

In an increasingly digital world, more and more toys and devices aimed at children now have internet-connected technology. As the Christmas shopping season begins, many of you will be considering buying them for your children. Concerns have been raised in recent months that the growth in toys containing sensors, microphones, cameras, data storage and other multi-media capabilities could put the privacy and safety of children at risk. There have also been data protection concerns relating to some products over what data is collected, by whom, where it is stored and how it is secured. You wouldn't knowingly give a child a dangerous toy, so why risk buying them something that could be easily hacked into by strangers? In the same way that safety standards are a primary consideration for shoppers buying toys, we want parents to take a pause and think about both the child's online safety, and also the potential threat to their own personal data such as bank details, if a toy, device or a supporting app is hacked into.

Here are a few tips to help parents in their decision making:

1 Research the security of a product before buying

Doing your homework before buying a connected device should allow you to recognise those with poor security. We recommend that you research online reviews and manufacturers' websites for information on privacy notices and policies. You should also look to see how a product will be updated in the future if a security issue is identified.

2 Take care when shopping online

At this time of year, when online shopping is nearing its peak, scammers may be more likely to try to access your personal information such as bank account or credit card details. Only use secure sites when shopping online – secure sites usually carry the padlock symbol. Get Safe Online has advice on how to protect yourself.

3 Take your time

Don't wait until Christmas Day, when excited children will want to just turn on a new toy or device and skip as much of the set-up process as they can. Take the time beforehand to read the manual and familiarise yourself with the security and privacy options available to you.

4 Change passwords and usernames from default

Default passwords and usernames for many devices are freely available on the web. You should always change the defaults immediately and choose a suitably strong password. Use a different password for each account and device. If a device doesn't allow you to change the default password, you should strongly consider whether it is worth keeping it.

5 Is your router secure?

Your router is the first line of defence on the perimeter of your home network. If you have devices connected to your network, the default settings of your router might be exposing them to the internet and therefore everyone else. Create a strong password and look out for and install security updates.

6

If there’s a two-step identification option – use it

Two-factor authentication offers you an additional layer of security when logging in to an online service. While few devices will offer this capability, the website you use to view its data might.

7

Be camera aware – you never know who’s watching

Some toys and devices are fitted with web cameras. The ability to view footage remotely is both their biggest selling point and, if not set up correctly, potentially their biggest weakness. If you have no intention of viewing footage over the internet, then turn the remote viewing option off in the device’s settings, or else use strong, non-default passwords.

8

Location, location, location

One of the main selling points of children’s smart watches is the ability for parents to know where their children are at all times. However, if this isn’t done securely, then others might have access to this data as well. Immediately get rid of default location tracking and GPS settings and set strong, unique passwords.

9

Bluetooth ache

It is not just potentially insecure web connections that can put children‘s online safety at risk. Some toys and devices have been found to have unencrypted WiFi connections or unsecured Bluetooth connections which can be easily accessed by strangers. If there is no option to secure these in the device’s settings, consider whether using the device is worth the risk. If there is an option to protect them with either a password or a PIN ensure you choose a strong one.

If in doubt, don’t splash out

If you are not convinced a smart toy or connected device will keep your children’s personal information safe, then don’t buy it. If consumers reject products that don’t protect them, then developers and retailers should soon get the message. If you’ve purchased a device that you’ve since discovered is insecure, complain to the manufacturer or retailer and see if you can return it.

Safety alert: see how easy it is for almost anyone to hack your child’s connected toys

Connected toys with Bluetooth, wi-fi and mobile apps may seem like the perfect gift this Christmas. But Which? have found that, without appropriate safety features, they can also pose a big risk to your child’s safety. It has revealed concerning vulnerabilities in several devices that could enable anyone to effectively talk to a child through their toy. They present their findings on just four – the Furby Connect, I-Que Intelligent Robot, Toy-fi Teddy, and CloudPets cuddly toy:

By following the link below you can find out more information.

Read more: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/ - Which?

Internet safety checklist for young children

Agree boundaries - Be clear what your child can and can’t do online – where they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share. Agree with your child when they can have a mobile phone or tablet.

Explore together - The best way to find out what your child is doing online is to ask them to tell you about what they do and what sites they like to visit. If they’re happy to, ask them to show you. Talk to them about being a good friend online.

Put yourself in control - Install parental controls on your home broadband and any internet-enabled devices. Set up a user account for your child on the main device they use and make sure other accounts in the household are password-protected so that younger children can’t access them by accident.

Stay involved - Encourage them to use their devices in a communal area like the lounge or kitchen so you can keep an eye on how they’re using the internet and also share in their enjoyment.

Talk to siblings - It’s also a good idea to talk to any older children about what they’re doing online and what they show to younger children. Encourage them to be responsible and help keep their younger siblings safe.

Search safely - Use safe search engines such as Swiggle or Kids-search. You can save time by adding these to your ‘Favourites’. Safe search settings can also be activated on Google and other search engines, as well as YouTube.

Check if it’s suitable - The age ratings that come with games, apps, films and social networks are a good guide to whether they’re suitable for your child. For example, the minimum age limit is 13 for several social networking sites, including Facebook and Instagram.

Have a secure Christmas

By taking some time and care beforehand and following the advice above, you can still see a child’s face light up when they open their new, web-connected Christmas present, safe in the knowledge that you are keeping them secure as well as happy.