eSafety Newsletter

Autumn term 2015
Parent / Carer edition

In this edition we identify potential risks for your children online and on social media.

Sexting

The act of sending (someone) sexually explicit photographs or messages via mobile phone is becoming more of a problem for our teenage children. This huge issue has had wide media coverage recently.

Case study from a call-in on ITV's This Morning (15th June 2015)

When Jennifer was 13, she was tricked into sending a naked photograph of herself to a boy. To persuade her, he said that another girl had sent him photographs before. Unfortunately she obliged and he circulated the photo to his friends at school the next day. Jennifer lost all her friends and that photograph has been a thorn in her side ever since. She is now 21 and the photograph is still out there. Once something is on the internet, it cannot be removed.

What can be done about this?

According to the BBC, 'a campaign is being launched to give children and their parents advice if a child becomes involved in so-called sexting.

The National Crime Agency (NCA) has said that child protection officers are investigating an average of one case involving sexting every day.

It said sending nude or explicit images of themselves on social media had become "normal" among teenagers. A series of videos offering advice is being published online'.

More information can be found here: **http://www.bbc.co.uk/news/uk-33130827**

Anti-radicalisation

Your child/children need reminding that they cannot trust everyone they meet online. Let them know that some people will lie to them and try to alter their opinions on certain matters. Tell them that they should be careful and let you know if they feel uncomfortable, worried or frightened about any online activity. If a child is at risk, you can report the issue to CEOP (Child Exploitation and Online Protection) for immediate response at **https://www.ceop.police.uk/Ceop-Report/** or call 101 and ask for the Child Online Safeguarding Team.

Schools on the HICS network (HICS stands for Hertfordshire Internet Connectivity Services) are protected by a market-leading filtering platform, barring access to inappropriate websites. However, as no filtering solution is 100% reliable, we need schools to work with us and report any inappropriate content to the SITSS Connectivity service desk on **sitss.internet@lea.herts.sch.uk**

The right to be forgotten...

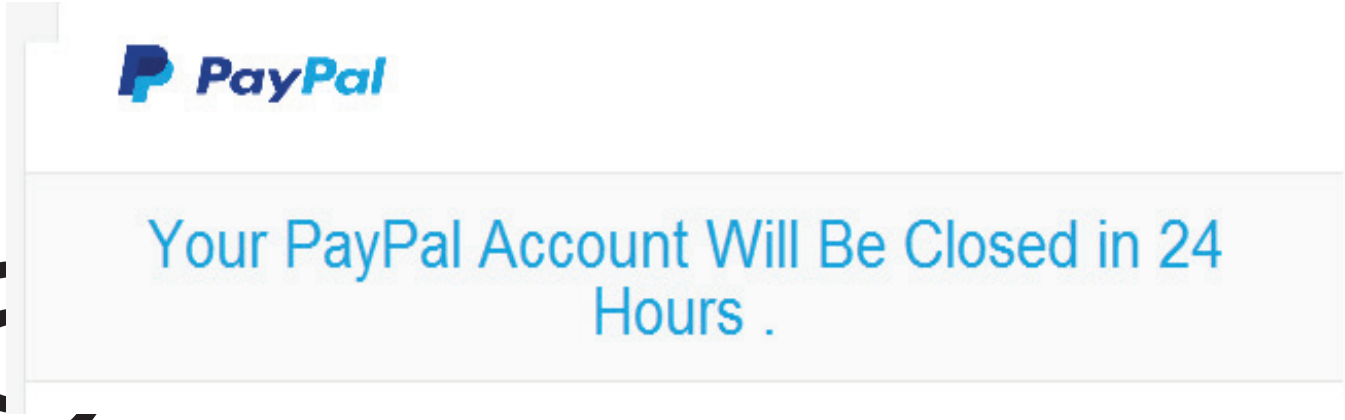
Due to a ruling by the Court of Justice of the European Union last year, Google are working towards your right to request that search engines remove results for queries that include a person's name. You can make a request under this ruling but for them to comply, the results shown would need to be inadequate, irrelevant, no longer relevant, or excessive. This could be useful if a young person was being victimised for an online mistake. Click here to find out more **https://www.google.co.uk/policies/faq/**

How do I get my child to listen to me about online safety?

It can be difficult to get children to listen to reason sometimes. We can all offer eSafety advice but our children can be good at making all the right noises and promptly forgetting or ignoring our instructions. If only there was a website which was designed to look like fun, yet in fact designed to give small but important nuggets of eSafety advice to our children. Fortunately there is, and it even caters for younger children 'under 7'! **http://www.phonebrain.org.uk/** . This site focuses on saving the children money by giving sound advice but it is a very useful tool for eSafety education. Look out for the section for parents too.

It isn't just children who are the target...

Parents normally do their best to protect children from online dangers but often adults are the target. This particular example is an attempt at 'phishing' – a method by which the personal details of victims are fraudulently collected by criminals for later use. Luckily the poor use of English in this PayPal phishing scam will help most people identify its true purpose, although it might trick some unfortunate people. Please take note that you should never follow links from emails requesting personal information. If ever a company emails to request that you log into your account or confirm your personal details, they should ask you to visit their website rather than insert a link. If they do ask you to click on a link, you can still close the email and navigate to their website for yourself.



For eSafety advice & training visit:
http://www.thegrid.org.uk/eservices/safety/training/index.shtml
Herts for Learning Autumn Term 2015

Herts for Learning