



THE DIGITAL UNIVERSE OF YOUR CHILDREN

ONLINE TIPS FOR PARENTS

RISKS ONLINE

The best defences against online risks are openness, awareness and education. Talk with your children about their online lives, share their experiences and learn from them. Help them to use technology positively and responsibly, and give them boundaries, guidance and support. Below are a number of risks that you can talk to your children about:

1 IDENTITY THEFT

Identity theft is the theft of personal data to impersonate an individual, usually for financial gain. The issue isn't new, but has been intensified by the internet, giving criminals new routes to gather personal data on a much larger scale. Criminals use a variety of methods to gather personal data ranging from harvesting data already published online (such as on online profiles and social networking sites) to using a combination of spam, phishing and pharming techniques. The best prevention against identity theft is, without a doubt, to advise your child not to publish personal details such as bank account number(s), addresses, telephone numbers, passport details etc.

2 SPAM, PHISHING AND PHARMING

Spam emails are unwanted messages that are typically distributed in bulk. Spam messages may contain commercial content such as pornography, pharmaceuticals, dubious financial transactions, or 'too good to be true' offers.

Phishing attacks are where users are sent emails tricking them into 'updating' their personal details online via a fake website (i.e. imitating a bank). These websites save this personal information and use it for other damaging objectives.

Pharming is the process of redirecting users to a fraudulent copy of a legitimate website, again with the aim of stealing personal data and passwords for criminal intent. Talk to your children about how to identify phishing and pharming attacks.

3 GROOMING

Child grooming refers to all activities deliberately undertaken to befriend and establish an emotional connection with a minor. The aim of this 'special relationship' is to lower the child's inhibitions in preparation of sexual abuse or exploitation. Child grooming may be used to lure minors into illicit businesses such as child prostitution or child pornography.

4 CYBERBULLYING

Cyberbullying is the use of technology to deliberately hurt, upset, harass or embarrass someone else. Cyberbullying can occur using practically any form of connected media, from nasty text and image messages using mobile phones, to unkind blog and social networking posts, or emails and instant messages, to malicious websites created solely for the purpose of intimidating an individual.

Cyberbullying can be even more harmful than normal forms of bullying in several ways. As there is a:

- ▶ Possibility to electronically invade the home and personal space of the victim.
- ▶ Greater potential size of the audience.
- ▶ Greater speed of spreading upsetting messages or images.
- ▶ Difficulty in controlling anything posted or circulated electronically.
- ▶ Perceived anonymity to Cyberbullying, due to its faceless nature which can lead to children becoming involved in activities that they wouldn't dream of in the real world, whether as the perpetrator or as a bystander.

Let your children know that it's OK to block 'buddies' or just disconnect from the website if someone or something is making them feel uncomfortable online. Ultimately, they are in control, if they do choose to block or disconnect, it's still a good idea for them to talk through the issues with a known and trusted adult: this can help children and young people to reaffirm that they acted in safe and positive way.

NEED MORE INFORMATION?

Find out more from the Insafe network:
www.saferinternet.org

