Child safety and cyber-flashing

Cyber-flashing happens when a stranger sends an obscene picture, unsolicited, to your phone via Wi-Fi or Bluetooth. It's a form of sexual harassment and there have been prosecutions for it under existing laws.

The term 'cyber-flashing' first hit the news in 2015, after a woman on a train received explicit pictures on her iPhone which had been sent to her via Apple's file-sharing function (AirDrop).

Cyber-flashing is not new – it has been possible since the introduction of Bluetooth. However, the growing trend for smartphone use among children means that there's more risk of it happening to them.

It's also not just an iPhone issue. There are many file-sharing apps that make it possible on Android and Apple phones.

What are the concerns?

You may have seen news reports or heard concerns raised about:

> **The large number of young women receiving unwanted images:** a 2018 YouGov poll found that 41% of women aged between 18 and 36 had been sent an unsolicited photograph of a penis

> **The potential for large-scale abuse of children:** most 12 to 15 year-olds (83%) and a growing proportion of 8 to 11 year-olds (39%) owned a smartphone in 2017. In 2017-18 there were almost 12,000 prosecution procedures for sexual exploitation of children through photographs

> **Security problems with Apple's AirDrop:** it's easy to allow anyone to 'air drop' images onto an iPhone, and the automatic preview feature means recipients can see images even if they haven't chosen to open them

> **The range of file-sharing apps freely available:** most people don't have time to keep on top of the latest apps/features and their potential issues – for example, SHAREit is a very popular file-sharing app for Android users, with over 500 million downloads worldwide, but do you know its features?

What safety options are available to parents?

Restrict who can send files to your child's phone

Most file-sharing apps will allow users to restrict who can send files to them via Wi-Fi or Bluetooth. Check the settings and user instructions for your child's apps, and make sure your child knows how to operate these controls.

For AirDrop on iPhones:

> Open '**Control Centre'** (swipe up from the bottom of the screen or down from the upper-right corner, depending on the model)

> Press firmly on the network settings card in the upper-left corner. This will reveal more connectivity controls

> Tap the **AirDrop** icon

> Select '**Contacts Only'**, or '**Receiving Off'** (to not receive AirDrop requests)

Or, do this by going to Settings > General > AirDrop.

Turn off file-transfer apps

Advise your child to do this when they're not using the apps (including Bluetooth). If the apps need to be on, advise your child to use PIN protection and only allow contact from people they know.

Tell your child never to open files from someone they don't know.

Make sure your child knows how to report a cyber-flashing incident

If your child does not feel in immediate danger, they should take a screenshot and report the incident to the police via the non-emergency numbers:

> If it happens on public transport, text 61016 or call 0800 40 50 40

> If it happens anywhere else, call 101

If your child feels scared or in immediate danger, they should call 999 straight away. They may also want to move to a place of safety – find someone in authority to talk to, e.g. platform staff, a security guard or a shop manager.

If the incident occurs on school premises, your child should talk to an adult they trust at once.

What else can I do?

Further tips

Find out what file-sharing apps your child uses and download them. Look at the security settings and check with your child that their settings are restricting unsolicited images/files. Some of the most popular are:

> Google Drive

> Dropbox

> Microsoft OneDrive

> AirDroid

> Zapya

Look out for signs that something has upset or distressed your child

The signs listed below are not specific to cyber-flashing or social media use more generally, but can be an indication that something is bothering your child. If you see changes in behaviour, talk to your child.

> Signs of distress, such as being withdrawn, aggressive, or lacking in confidence

> Performing poorly in school without a reason

> Making changes to try to fit in, e.g. changing appearance

> Self-harm

Safeguarding
Training Centre
from The Key

❯ Displaying nervous or secretive behaviour when using their mobile phone or a computer

The National Society for the Prevention of Cruelty to Children (NSPCC) has guidance on talking about difficult topics with your child to keep them safe:

[Talking about difficult topics, NSPCC](#)

http://www.btp.police.uk/61016_text_service1.aspx

Sources

This factsheet was produced by Safeguarding Training Centre from The Key.

❯ [Four in ten female millennials have been sent an unsolicited penis photo, YouGov, 16 February 2018](#)
https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic

❯ [Children and parents: media use and attitudes report 2017, Ofcom](#)
https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-2017

❯ [Violence against women and girls, Crown Prosecution Service](#) (see the 2017-18 report)
https://www.cps.gov.uk/publication/violence-against-women-and-girls

❯ [Use AirDrop on your iPhone, iPad, or iPod touch, Apple](#)
https://support.apple.com/en-gb/HT204144#setoptions

❯ [61016: our non-emergency text number, British Transport Police](#)
http://www.btp.police.uk/61016_text_service1.aspx