# Lesson plan: 13-16 years

**Recommended lesson time: 60 minutes**

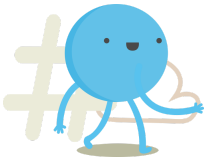
## Part one: The Digital World (10 minutes)

**Learning objective:** To understand different aspects of the digital world including behaviour, security and online risk.

Split the class into groups and ask each group to discuss these questions about the digital world (**five minutes**). Discuss each point together as a class at the end (**five minutes**).

1. Why should you check before posting an image of someone else on social media?
2. What can you do if someone you don't know keeps sending you messages online?
3. What can you do to keep your information secure online?

[**Teacher notes:** possible answers - 1. they may not want their image shared; it is their personal data; it might upset them. 2. block, report, tell a trusted adult. 3. Set a strong password for online accounts; enable two-step verification where you have to enter a password and a PIN to open a device.]





## Part two: Being a Digital Citizen (20 minutes)

**Learning objectives:**

- To understand what cyberbullying and trolling are and the differences between them.
- To know whether something is risky or safe online and why. An introduction to 'phishing'.

### Activity one – online kindness (10 minutes)

Explain the following definitions to pupils, asking if anyone has heard of the words before.

**Cyberbullying:** Cyberbullying is online bullying. It usually involves people you know. It is often accompanied by bullying in person, offline. If someone is repeatedly unkind or harasses another person online, then they are a cyberbully. Unkindness includes deliberately excluding people from shared online spaces and messaging groups and making them feel isolated, as well as doing and saying unkind things.

**Trolling:** Internet trolling is the act of deliberately writing offensive or nasty messages and comments with the aim of making other people angry or upset, and/or react to the comments.

An internet troll will often target a public figure they have never met and write comments, so they can get into an online debate or argument with others. They sometimes act anonymously or use a fake identity.

**Activity:** Ask pupils to get into pairs and come up with their own scenario for cyberbullying and for trolling. Ask them to compare them and explain how the two scenarios are different. How do they think experiencing, or witnessing, negative behaviour can affect people online?

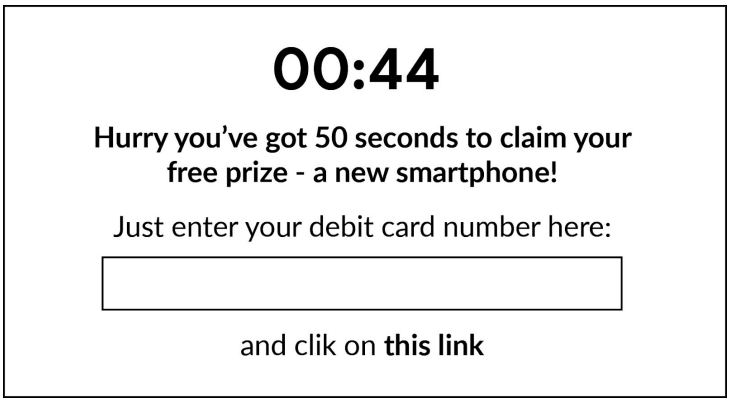
[**Teacher's notes:** Cyberbullying examples: a group of friends sending nasty messages to another pupil in the school, sharing embarrassing photos of another person to upset them. Trolling examples: leaving nasty messages on a rival football team's website comment page, sending insults by direct message online to a celebrity they have never met.]

## Activity two – An introduction to 'Phishing' (10 minutes)

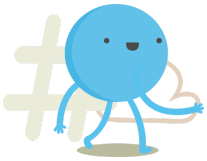
Some people try to get information from others online in order to scam them. They might try to get them to share information that is personal or trick them into giving it up. These scams are known as 'phishing' scams. Knowing how to spot risky places online can help children be safer and have more fun.

Show pupils this pop-up and ask them what they notice about it.

What are the clues that help them know it's a phishing scam and that they need to be careful not to fall for it?




[**Teacher's notes:** spelling mistake; only 50 seconds when there shouldn't be a rush. bank details not needed for a free prize; where does the link take you; why am I winning this prize without entering a competition?]





## Part three: Recovering when things go wrong (30 minutes)

**Learning objective:** To be able to understand appropriate solutions to recover from online problems and mistakes.

Anybody can make a mistake online. Even if a child is careful, accidents can happen, they may feel unsafe or people might be unkind. When things go wrong, the most important thing is that they know how to get help and recover.

Ask pupils to design a guide for a sibling or family member with top tips on what to do if something goes wrong online.

They may want to include:

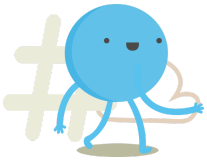
- Tell a trusted adult if you've been tricked into doing something that upsets you.
- Tell a trusted adult if you come across anything that upsets or worries you.
- Remove any mean posts or embarrassing pictures of other people.
- Learn how to block and report people.
- Change your password if you think someone else may know it.

### Teacher's notes:

Children who are resilient are more likely to benefit from opportunities online and less likely to experience harm. Resilience isn't a lesson they can learn in school or a skill they acquire – it must be fostered and nurtured. Parenting and support from trusted adults can make all the difference.

A child who is digitally resilient will be able to:

- Understand when they are at risk online.
- Know what to do to seek help.
- Learn from their experiences.
- Recover when things go wrong.





## Homework

Encourage parents to get involved in the homework activity so that children can share learning with their families. Parents can help reinforce key internet safety messages and help children to learn how to be safer online.

**Task:** Ask pupils to create a quiz for their siblings or another family member. Get them to include six questions on a piece of paper about the things they have learned in their lesson. They should also write the answers at the bottom of the paper. E.g. Q: What is cyberbullying? A: This is bullying carried out online.

Direct them to the Digiworld online game (https://bit.ly/2RQ8RFq) so they can explore all of the topics in more depth.

There are also level three worksheets available to download for: Understanding the Digital World, Being a Digital Citizen and Recovering when things go wrong.