

Do Now

Life Online – How can we make the internet safer?



'Why weren't you online last night?' Tom asked Farrell.

'Aww, my mom spent ages updating everything at home to make the internet safer.'

'Your mom is so extra.' Said Farrell.

'Well, not really,' replied Tom. 'See a fifty-year-old creep was talking to my lil' bro through the PlayStation, my dad had his car re-registered to some guy in Scotland and my mom's bank account was emptied by a hacker in Brazil. I do kinda' get it.'

Discuss: Is making the internet safer 'extra' or a necessity?



What do we mean by the terms 'online predator', 'troll' and 'cyber-crime'?

I think these terms mean...

CLUES: fake identity, bullying, theft



Online Trolls - an online bully who deliberately tries to offend, cause trouble or directly attack people by posting derogatory comments on posts.

Cyber-crime – criminal activities carried out by means of computers or the internet. Could be stealing information or using your identity for criminal purposes.

Online predator - someone that seeks contact with children and teens on the internet for abusive and exploitative purposes that are often sexual.

Learning outcomes:

Describe how to identify risk and manage personal safety in increasingly independent situations, including online.

Develop strategies to identify and reduce risk from people online that you do not already know, assess when and how to access help.

Life Online – How can we make the internet safer?



Why are we focusing so much on internet safety anyway? Well, there are many good reasons for this. Read the statements below and vote to see if you think they are true or false as a class. **We'll reveal the answers on the next slide.**

About 37% of young people between the ages of 12 and 17 have been bullied online. 30% have had it happen more than once.

60% of young people have witnessed online bullying. Most do not intervene.

Reports of data breaches (hacking for your information) are increasing. Since 2001, the victim count has increased from 6 victims per hour to 97, a 1517% increase over 20 years up to 2023.

With an average of 97 cyber crime victims per hour, this means there is a victim of cyber crime every 37 seconds.

Life Online – How can we make the internet safer?



ALL OF THE STATEMENTS ARE TRUE

Internet safety isn't something that just young people need to study either – as those cyber crime statistics apply to adults.

About 37% of young people between the ages of 12 and 17 have been bullied online. 30% have had it happen more than once.

60% of young people have witnessed online bullying. Most do not intervene.

Reports of data breaches (hacking for your information) are increasing. Since 2001, the victim count has increased from 6 victims per hour to 97, a 1517% increase over 20 years up to 2023.

With an average of 97 cyber crime victims per hour, this means there is a victim of cyber crime every 37 seconds.

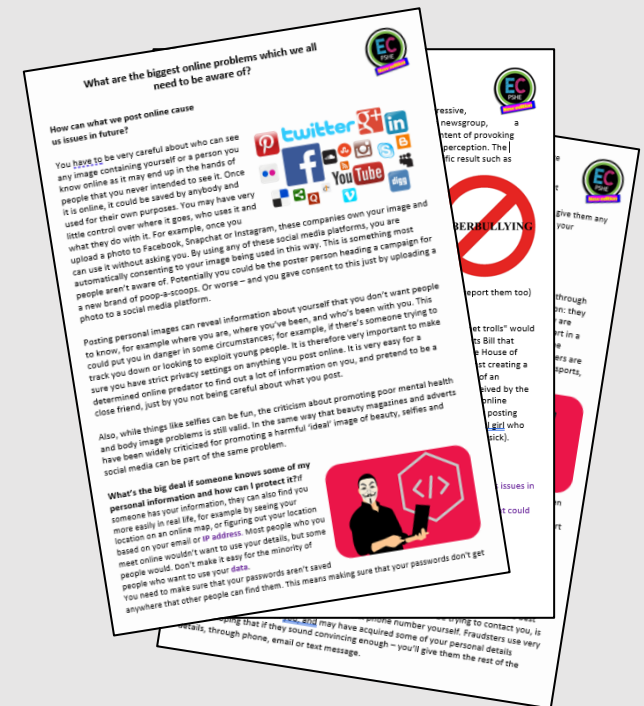
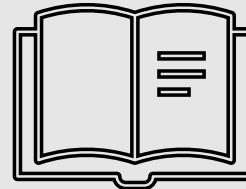
Life Online – How can we make the internet safer?



We will now find out more about the biggest dangers we all face on the internet today, why these are such important issues to everyone online, as well as how we can take steps to combat them.

Reading – Thornden Three

- Read the information carefully
- Complete the questions in your booklet (see next slide).



We will now find out more about what are the biggest online problems which we all need to be aware of? How can what we post online cause us issues in future?

THORNDEN THREE = GUIDED READING



You have to be very careful about who can see any image containing yourself or a person you know online as it may end up in the hands of people that you never intended to see it. Once it is online, it could be saved by anybody and used for their own purposes. You may have very little control over where it goes, who uses it and what they do with it. For example, once you upload a photo to Facebook, Snapchat or Instagram, these companies own your image and can use it without asking you. By using any of these social media platforms, you are automatically consenting to your image being used in this way. This is something most people aren't aware of. Potentially you could be the poster person heading a campaign for a new brand of poop-a-scoops. Or worse – and you gave consent to this just by uploading a photo to a social media platform.

Posting personal images can reveal information about yourself that you don't want people to know, for example where you are, where you've been, and who's been with you. This could put you in danger in some circumstances; for example, if there's someone trying to track you down or looking to exploit young people. It is therefore very important to make sure you have strict privacy settings on anything you post online. It is very easy for a determined online predator to find out a lot of information on you, and pretend to be a close friend, just by you not being careful about what you post.

Belong - Care - Aspire - Succeed

We will now find out more about what are the biggest online problems which we all need to be aware of? How can what we post online cause us issues in future?

THORNDEN THREE = GUIDED READING



Also, while things like selfies can be fun, the criticism about promoting poor mental health and body image problems is still valid. In the same way that beauty magazines and adverts have been widely criticized for promoting a harmful 'ideal' image of beauty, selfies and social media can be part of the same problem.

What's the big deal if someone knows some of my personal information and how can I protect it? If someone has your information, they can also find you more easily in real life, for example by seeing your location on an online map, or figuring out your location based on your email or **IP address**. Most people who you meet online wouldn't want to use your details, but some people would. Don't make it easy for the minority of people who want to use your **data**.

You need to make sure that your passwords aren't saved anywhere that other people can find them. This means making sure that your passwords don't get saved on computers, phones or tablets that other people use. You can also change your passwords regularly to help stop people guessing them.

If you play online games with other people, you need to be very careful about what you tell the people you're playing with. There is no need to let them know your personal details. Even if you think that these people are your friends, you shouldn't give them any information that they could use to track you down. Remember, if you give someone your information online they can use it in the real world.

We will now find out more about what are the biggest online problems which we all need to be aware of? How can what we post online cause us issues in future?

THORNDEN THREE = GUIDED READING



Online fraud refers to a number of different types of criminal activity carried out through the internet. Each of the different types of online fraud have two things in common: they are carried out by people breaking the law, and, in the vast majority of cases, they are carried out on unsuspecting victims, who either don't realise that they're taking part in a scam, or didn't know the real purpose behind the transaction. The motivation of the fraudsters is usually to obtain money from their victims, but sometimes the fraudsters are looking to steal more than money – for example, personal identification details, passports, profiles and so on.

A good example of this which unfortunately, quite a few people still fall for on a daily basis is something called Romance Fraud – this refers to fraudsters who pose as genuine love interests on internet dating sites. They establish what feels like a genuine relationship with their victim, who may believe that the relationship is potentially serious, long-term or emotionally meaningful. Once the victim's trust has been gained, the fraudsters get the victim to reveal personal details, which are then stolen and used in identity theft. The fraudsters may also ask the victim to send money or bank card details on the pretext of needing payment for a flight, taxi or other means of transport to come and meet them.

They may also give the victim sob stories about family members needing money for medical treatment, or other financial requests. This turns out to be a total fabrication, and the money is taken by the fraudster, who then instantly disappears from the victim's life.

Belong - Care - Aspire - Succeed

We will now find out more about what are the biggest online problems which we all need to be aware of? How can what we post online cause us issues in future?

THORNDEN THREE = GUIDED READING



You can avoid this by being extremely careful online with who you give out personal details to, and never giving money to people that you don't know in real life. The same kind of fraud is also perpetuated by fraudsters who may pretend to be from your bank. The best way to handle any correspondence, if you think your bank MAY be trying to contact you, is to never reply – but to phone the official bank phone number yourself. Fraudsters use very clever techniques to trick you, and may have acquired some of your personal details already, hoping that if they sound convincing enough – you'll give them the rest of the details, through phone, email or text message.

What are online trolls? Can anything be done about them?

A troll is a person who posts or makes inflammatory, insincere, digressive, extraneous, or off-topic messages online (such as in social media, a newsgroup, a forum, a chat room, an online video game), or in real life, with the intent of provoking others into displaying emotional responses, or manipulating others' perception. The behaviour is typically for the troll's amusement, or to achieve a specific result such as disrupting a rival's online activities or purposefully causing confusion or harm to other users online. Trolling is a form of cyber-bullying.

Belong - Care - Aspire - Succeed

We will now find out more about what are the biggest online problems which we all need to be aware of? How can what we post online cause us issues in future?

THORNDEN THREE = GUIDED READING



There is a saying which has a lot of value to it – don't feed the trolls. Don't engage with them – because if you do, you are giving them EXACTLY what they want. Most sites have a 'report abuse' button, the best thing to do is use this straight away, as most sites are quick to ban people today – even if it's just a suspension whilst they investigate further. If more than one person reports the abuse (you could ask a parent/guardian or a friend to report them too) then they are far more likely to be banned altogether.

In October 2014, the UK's Justice Secretary, Chris Grayling, said that "Internet trolls" would face up to two years in jail, under measures in the Criminal Justice and Courts Bill that extend the maximum sentence and time limits for bringing prosecutions. The House of Lords Select Committee on Communications had earlier recommended against creating a specific offence of trolling. Sending messages which are "grossly offensive or of an indecent, obscene or menacing character" is an offence whether they are received by the intended recipient or not. Several people have been imprisoned in the UK for online harassment, including a twenty-year-old man was jailed for twelve weeks for posting offensive jokes to a support group for friends and family of April Jones (a school girl who disappeared and was later found to be murdered – yes, trolls really can be that sick).

Trolls, online fraudsters, privacy, images and data

Now you have read the information, complete the questions below. We'll discuss these as a class shortly.

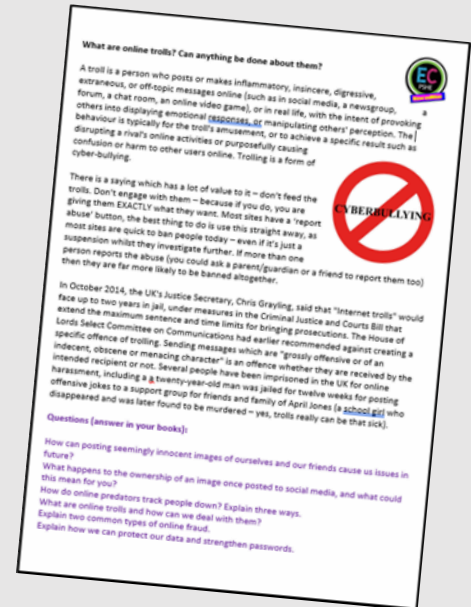
How can posting seemingly innocent images of ourselves and our friends cause us issues in future?

What happens to the ownership of an image once posted to social media, and what could this mean for you?

How do online predators track people down? Explain three ways.

What are online trolls and how can we deal with them? Explain two common types of online fraud.

Explain how we can protect our data and strengthen passwords.



How can we stay safe online? There are so many different precautions we can take to protect ourselves. Let's hear some top advice on the issue.

**Watch the clip and complete the questions in your booklet.
We'll go through the answers together afterwards.**

https://www.youtube.com/watch?v=P04OGnrLe_Y



1. What should you NEVER share?
2. Can posts remain online even after you delete them?
3. Why should you check links twice before clicking on them?
4. Why should you avoid public access internet hotspots?
5. Why should you only visit websites that start with https:// ?
6. What should you do if you are cyberbullied?
7. Why should you turn off your Bluetooth?
8. Why should we use complicated passwords?



How many did you get right?

You now have time to correct any answers you missed.

What should you NEVER share?

Passwords, bank account information, social media account access or real-life address online.

Can posts remain online even after you delete them?

Yes

Why should you check links twice before clicking on them?

Because this is how criminals try to infect your systems with malware and viruses (and also in turn steal your data).

Why should you avoid public access internet hotspots?

Hackers sometimes create these to steal your data/personal information

Why should you only visit websites that start with https:// ?

This means that the site is secure (no one else can see what you're doing on it)

What should you do if you are cyberbullied?

Document the incident, block the account (and reporting them too is best)

Why should you turn off your Bluetooth?

People can use it to see what's on your devices.

Why should we use complicated passwords?

They're far less easy to hack



How can we build resilience when life throws us challenges?



Useful mental health helplines and charities:

Childline. Support for people under 19 in the UK. Call: 0800 11 11

Young Minds. Child and adolescent mental health charity. Call: 0808 802 5544 (parents' helpline)

Mind. Mind is a charity that provides advice and support for people experiencing a mental health problem in England and Wales. Call: 0300 123 3393 (Mon to Fri, 9am to 6pm)

Rethink Mental Illness. Support and advice for people living with mental health problems. Call: 0300 5000 927 (Mon to Fri, 9.30am to 4pm)

SANE. National out-of hours mental health charity offering emotional support, guidance and information. Call: 0300 304 7000 (4.30pm to 10.30pm)

Mental Health Foundation. Information and support for anyone with mental health problems or learning disabilities.

Need Support? You're Not Alone

If anything in today's lesson has affected you, or you want to talk to someone, there is help available.



Mental Health & Low Mood

YoungMinds – <https://www.youngminds.org.uk>
Kooth – <https://www.kooth.com>
Mind – <https://www.mind.org.uk>

Talk to Someone

Your Tutor or Head of Year – We're here to help.
Wellbeing Team and School Nurse
Report a Concern on Satchel
Safeguarding Team with the Purple lanyards

Healthy Lifestyle

NHS Every Mind Matters – <https://www.nhs.uk/every-mind-matters>
Change4Life – <https://www.nhs.uk/change4life>

Apps That Can Help

Calm – For mindfulness and sleep.
Headspace – Meditation and stress relief.
Clear Fear – Manage anxiety (designed for young people).
MeeTwo – Anonymously talk to other teens, moderated by experts.

Eating Concerns

Beat Eating Disorders –
<https://www.beateatingdisorders.org.uk>
NHS Live Well – Eating Disorders –
<https://www.nhs.uk/mental-health/conditions/eating-disorders/>



Belong - Care - Aspire - Succeed