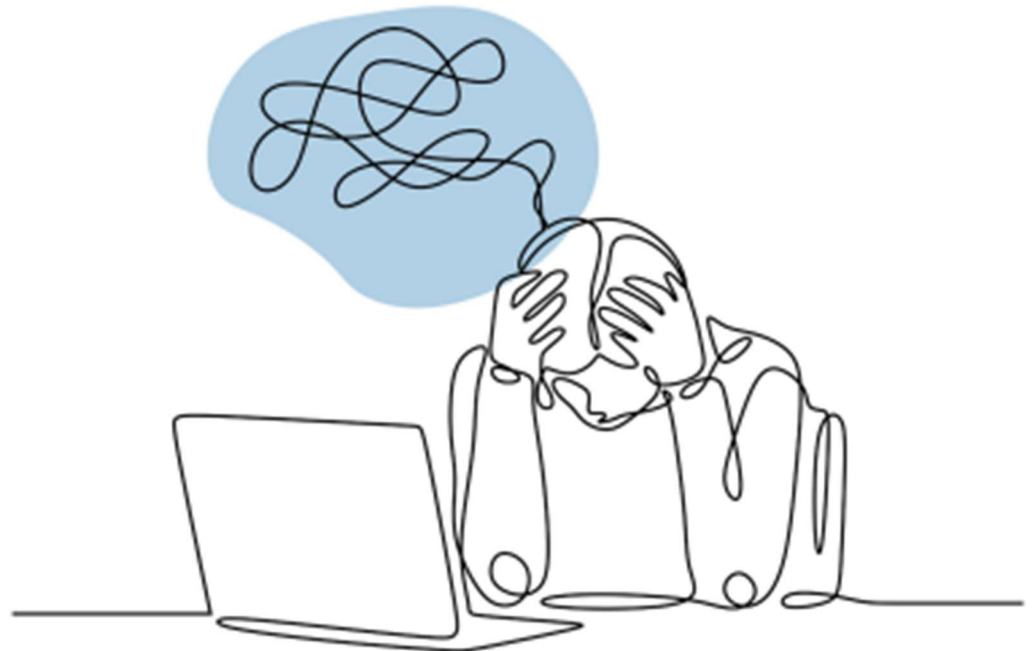


Critical Literacy and Online Awareness



This project has been funded with support from the Interreg 2 Seas Program

www.orpheusproject.eu

www.interreg2seas.eu/en/ORPHEUS

Title:

Critical Literacy and Online Awareness, Training for professionals

Authors:

**Annie Kirby, Vasileios Karagiannopoulos, Shakiba Oftadeh-Moghadam –
University of Portsmouth**

Céline Devienne – Greta Grand Littoral

Material produced by members of the ORPHEUS - Consortium does not purport to reflect the official policy, opinion or position of any individual organisation, agency, employer or institution, and thereby individual members of the Consortium cannot be held responsible for material produced, authored and/or disseminated by other partners.

The ORPHEUS – Consortium
City of Mechelen – Belgium
Portsmouth City Council – United-Kingdom
University of Portsmouth – United-Kingdom
Artevelde University of Applied Sciences – Belgium
Greta Grand Littoral – France
Ceapire – Belgium
University College Roosevelt – The Netherlands
ContourdeTwern – The Netherlands



Project Management and secretariat

Project Manager: Hilde Lauwers, hilde.lauwers@mechelen.be

Administrative and financial expert: Kathy Marivoet, Kathy.marivoet@mechelen.be

© ORPHEUS 2019 – 2023

Unless otherwise indicated, the copyright, database rights and similar rights in all material published are owned by ORPHEUS. All rights reserved. Citation, reproduction and/ or translation of these publications, in whole or in part, for educational or other non-commercial purposes are authorized provided the source and the author's name are fully acknowledged.

Table of contents

1 Introduction.....	4
Who is this training for and what is its aim?.....	4
Background.....	5
Young people, social media and online risk.....	6
The importance of online critical literacy.....	7
2 Training Programme: Overview.....	9
How to use this training manual – read this before you begin!.....	9
Flexible use.....	9
Adaptability and Future Proofing.....	9
A note on impartiality.....	10
Approach.....	11
Additional material.....	12
Overview.....	13
How to use this manual – summary graphic.....	14
3 Preparation.....	15
Small-Medium-Large.....	15
Small.....	15
Medium.....	16
Large.....	17
4 Training.....	18
Small-Medium-Large.....	18
Small.....	18
Main Module: Critical Literacy and Online Awareness.....	19
How to use the trainer notes.....	21
Topic 1: Introduction, aim, learning outcomes, reflection questions.....	22
Topic 2: False Information: Definitions & Categories.....	25
Topic 3: False Information – Propagation and Risk.....	42
Topic 4: Fact-Checking and Tips for Spotting Fake News.....	47
Topic 5: Practical Exercises – Verifying Online Information.....	55
Step-by-Step Guide to Choosing Your Own False Information Examples.....	61
Topic 6: In the Workplace – Empowering Young People.....	62
Topic 7: Summary and Close.....	65

Large.....	69
Topic 2– Cybercrime: Definitions and Impact.....	72
Topic 3– The Do’s and Don’ts of Staying Safe Online.....	78
Topic 4– Scenarios.....	89
Topic 5– Summary and Close.....	93
Optional Module B: Cyberharassment.....	94
Topic 2 – Cybercrime.....	94
(3-4 minutes, Slide 3)	94
Topic 3 – Cyberharassment, Intimidation, Cybersexism (10-15 minutes, Slides 4-8)	94
Topic 4 – Case Study Workshop (30-40 minutes, Slides 9-15).....	95
Resources and advice.....	95
Topic 5 – Summary and Close (3-5 minutes, Slides 17-18).....	98
Optional Module C: Mini-Module – Legislation.....	98
5 Follow-up.....	99
Small-Medium-Large.....	99
Follow-Up Activity 1: Safeguarding.....	101
Follow-up Activity 2: Bespoke Activity Design.....	104
ORPHEUS.....	106
Safe spaces.....	107
Pedagogy.....	108
The Prevention Pyramid.....	109
Puzzle Model on the Risk Factors for Violent Extremism.....	110
7 Reference list.....	111



1 Introduction

Who is this training for and what is its aim?

KEY OBJECTIVES

Professionals to gain an understanding of the different types of false information young people may encounter online;

Professionals to gain an understanding of how and why false information online spreads and how it may put young people at risk;

Professionals to gain the skills, knowledge, ability and confidence to support young people to develop their critical thinking skills to be able to evaluate effectively the information they encounter online.

TARGET GROUP

The training programme contained in this manual is intended to be delivered to professionals such as:

Teachers and educators;

Youth workers;

Anyone else working with young people in formal or informal contexts.

KEY TOPICS

Key terms and definitions: disinformation, misinformation, fake news;

How does false information spread online and what are the risks to young people?

Common examples of false information online;

Fact checking and fact checking organisations;

How to evaluate information online including text, images and videos;

Guided activities to build confidence and experience in evaluating online news;

Discussion scenarios to build confidence in supporting and advising young people.

Background

The overall aim of the Orpheus Project is the development of an integrated prevention model that steers young people away from becoming involved in violent extremism. This training, on 'Critical Thinking and Online Awareness', supports that aim by providing professionals, including youth workers, teachers and educators, the knowledge, skills and confidence they need to be able to support young people to develop their critical literacy and build resilience to false information online, reducing their susceptibility to online grooming by means of exposure to disinformation.

When young people visit online spaces such as social media and chat rooms, they may be exposed to individuals and groups who would wish to recruit them into violent extremist activity. Initial 'grooming' is often through propaganda and disinformation, alongside the normalisation of racism and hateful behaviour and research has shown that individuals can become politicised through exposure to false information (Baldauf et al., 2019).

A key concept in this training, and in the Orpheus project overall, is to acknowledge and respect the 'actorship' of young people and, as such, this training is designed to ultimately empower young people by developing their media and information literacy skills and to enhance their critical thinking and their sense of global democratic citizenship. This involves moving from a purely safeguarding perspective, that may cultivate a passive approach to risk from children, to a more empowering and resilient stance.

If professionals are to be able to support young people to develop critical literacy and resilience to false information online, they must first gain the skills, knowledge and confidence to be able themselves to effectively evaluate online information. This training supports youth workers, teachers and other professionals to develop their own skills, knowledge and confidence, which they can then, in turn, pass on to the young people they work with. Ultimately, young people will develop their online critical literacy skills making them more resilient to online grooming by means of exposure to disinformation and reducing the risk of them becoming involved in violent extremism.

As you work through this manual, you will see that the majority of examples and activities included are not related directly to violent extremist content, but instead take an indirect approach, focusing on the building of skills in evaluating different types of online information. By empowering young people to see beyond disinformation and fake news and providing them with the tools to challenge all the controversial information they consume, they will be more resilient not only to extremist grooming, but also to other criminal or undesirable behaviour they may encounter online, such as grooming into sexual behaviour, bullying, hate speech and fraud.

Young people, social media and online risk

Young people’s engagement with social media is ever increasing and has become one of the most popular forms of communication, with an eclectic range of platforms, frequently changing and often ephemeral in nature, readily available (Home Affairs Select Committee, 2017; Van Ouytsel et al., 2020; Liang, 2015).

The OECD Programme for International Student Assessment found that on average, 15-year-olds across 35 countries and 5 continents spent 146 minutes on the internet on school days (excluding school activity) and 184 minutes on weekend days. Just over one-quarter of these were classified as extreme internet users, using the internet for at least six hours a day at weekends. On school days, just under 93% of 15-year-olds accessed the internet or used chat / social networks before or after school (OECD, 2015). 15-year-olds in Belgium, France, the Netherlands and the United Kingdom equalled or exceeded these averages in most cases, with the Netherlands and the United Kingdom showing particularly high levels of internet and social media usage.

	Average number of hours spent online (outside of school)		% of students using internet / chat / social networks before or after school	% of students using internet / chat / social networks before or after school
	Weekdays	Weekends		
Average across all OECD countries	146	184	26.1	92.8
Belgium	146	199	29.1	95.2
France	127	191	26.5	88.3
Netherlands	159	211	33.0	96.3
United Kingdom	188	224	37.3	94.8

There are myriad positive benefits to young people of being online, including access to information and education, self-expression, and the formation of friendships. For example, research by UNICEF found that between 43% and 64% of 9 to 17 years olds from 11 countries used the internet to access news, and 12% to 17% used it for discussing political issues (Cho & Byrne, 2020), indicating the potential for the internet to provide a positive platform for young people wishing to explore civic engagement. However, social media platforms share attractive features, are interactive, and are populated by a very young demographic, who may be more receptive and react more emotionally to negative political news on social media platforms (Park, 2015).

However, alongside these positive benefits, the potential of social media platforms and encrypted internet communications, such as WhatsApp or Viber, has attracted the attention of criminals and these platforms have also become tools in the hands of groups advocating for terrorist causes and violent political extremism. Research has highlighted the extensive use of social media platforms by terrorist groups for acquiring funding through the sale of illicit substances and items, such as drugs and cultural relics, the distribution of propaganda and for recruiting young people across the globe to join their cause. Online grooming is now a safer and much more globalised way of spreading extremist messages and approaching disaffected and marginalised young people in order to enlist them to politically violent causes (Ibrahim et al, 2017; Klausen, 2015; Alava et al., 2017).

The importance of online critical literacy

To empower young people to use the internet in a positive way, it is essential that they are able to evaluate effectively information that they encounter and are able to come to an informed opinion as to its veracity. It is just as important to be able to identify factual information and be confident of this, as it is to be able to identify false information. However, research has shown that people (not just young people) are poor at identifying false information. Various studies have been conducted indicating that people were able to identify false information on a scale ranging between 53% and 78% of the time depending on the study design (compared to algorithms designed to identify false information which were effective 80%-90% of the time) and that both casual and trained readers believed false information (Kumar & Shah, 2018).

Research has also shown that people's ability to evaluate information is influenced by their own preconceived notions, also known as confirmation bias. For example, Garret et al (2019) have shown how individual's political opinions influenced their perception of satirical news stories as true or false. Additionally, some online spaces may encourage the formation of echo chambers and filter bubbles, where individuals are exposed more frequently to information, attitudes and opinions

which accord with their own, leading to reinforcement and the perception that a given view is more prevalent than it may be in wider society, especially if an individual exclusively uses online sources to access news (Kitchens et al, 2020; Sindermann et al, 2020).

In relation specifically to young people, research undertaken by the National Literacy Trust in the UK found that not only did false information online risk damaging children's wellbeing by increasing anxiety, damaging self-esteem and skewing their worldview, but that only 2% of children had the critical literacy skills they needed to be able to tell if news was real or fake (National Literacy Trust, 2018a). It is vital that young people develop the necessary skills to be able to question and evaluate the vast quantities of information they are likely to encounter online during their lifetimes.



2 Training Programme: Overview

How to use this training manual – read this before you begin!

Flexible use

This training is designed to be delivered flexibly, to suit the specific context for each group. For example, the precise job role of the trainees, their previous experience, how much time is available to complete the training and whether you are delivering the training in person or online. As the trainer, you have the freedom to make your own assessment and use, skip and combine parts in a way that best suits the needs of the trainees.

Adaptability and Future Proofing

As you work through this manual you will see that it contains a number of ‘real-life’ examples of false information including both in the ‘categories of false information’ section and in the practical activities for verifying online information. When delivering the training may wish to replace some or all of these examples with alternatives that you have chosen yourself. Reasons to choose your own examples may include:

- You wish to provide examples more relevant to the particular context in which you are delivering the training (e.g., the country / region or the professional role of the participants);
- Because some or all of the examples provided in this manual are no longer available online;
- You simply want to use additional or more up to date examples.

A significant challenge of creating training about false information online is that examples can quickly become obsolete or superseded, as current affairs move on. For example, during the development phase of this training the COVID-19 pandemic occurred, which led to a huge amount of false information online and even now, as the training package is being finalised, Ukraine has been invaded, also resulting in a huge number of examples of false information being posted and shared online. Therefore, it is essential that trainers themselves have the knowledge and confidence to be able to keep this training up to date by choosing their own examples of false information when necessary.

When choosing your own false information examples to work with, we recommend obtaining them from a fact-checking organisation that is a [signatory](#) of the International Fact-Checking Network [code of principles](#).

There are many fact-checking organisations covering different countries and languages signed up to this code. If choosing fact-checking organisations from this list is not possible, then choose a fact-checking organisation or organisations relevant to your context and conduct your own research to assure yourself they abide by appropriate principles including transparency, impartiality and fairness.

Most fact-checking organisations have a link on their website detailing their most recently fact-checked stories, which you can browse for inspiration. Alternatively, it is usually possible to conduct a search for specific outcomes e.g., information that has been ranked as true or false or a mixture, depending on what you need.

Remember, the goal is not to tell the training participants what is ‘true’ and what is ‘false’ but to provide them with the tools to make their own evaluations (skills which, in turn, they can share with young people in a professional context) and this should be borne in mind when selecting examples. For example, if a piece of information has been widely-reported, consider using a link to a report from a less well-known publication if one is available, to avoid ‘tipping off’ the participants as to whether the information is likely to be true or false merely on account of which organisation has published it.

Finally, as online information can change at any time, we recommend checking all online links, including any you have recently researched, as closely as possible to the date of the training delivery to ensure they are all still working.

A [step-by-step guide](#) to choosing your own examples is included in the module on [Critical Literacy and Online Awareness](#) module.

A note on impartiality

It is important to remember that your job is not to tell anyone what to believe, or what is true or false. It is only to provide the individuals participating in the training with the skills they need to make their own informed evaluations about information they encounter online, and to be able to support the young people they work with to do the same. As much as objectivity may be the goal, no one is truly impartial, including the developers of this training, although every attempt has been made to provide examples covering a range of socio-political views. There is more information about bias in [Topic 3: False Information – Propagation and Risk](#).

To mitigate bias as far as possible, the examples we have used in this training have been fact checked using a reputable fact checking organisation with a stated commitment to transparency, impartiality and fairness.

Approach

This training is divided into three phases: preparation, training and follow-up. Each of these phases is further subdivided into small, medium and large options, as set out in the overview below. This results in a matrix with nine possibilities. You are free to make your own assessment as to which parts of the training to use. You may wish to deliver the entire training course or to skip parts and make your own compilation of elements in this manual. After all, every context and every group of professionals requires a slightly different approach. With this manual, you have the possibility to pick and mix sections from the matrix so that it is tailored to every setting and to the time you have available.

As you read the training material, you will find the following icons to assist you:



This icon indicates a core activity. If you are short of time, focus on these activities to ensure the participants cover all the essential learning.



This icon indicates a suggested activity. These activities add depth and additional knowledge but may be omitted if time is short.



This icon indicates the KEY LEARNING POINTS that your training participants should get out of each activity.



This icon indicates a Timesaver Tip, giving you the option to adjust how certain activities are delivered if you are short of time.



This icon indicates a Training Tip to help you deliver the learning as effectively as possible.



This image indicates an ideal point to schedule a break in your training session.

Additional Trainer Notes

Additional trainer notes appear in a blue box like this. These notes provide further background information and suggestions for further reading about each training topic. **You do not have to teach all of the information in the trainer notes (or, indeed, read all the information in the trainer notes).** They are included to supplement the core and suggested activities and key learning points and to support you to feel more confident in your knowledge as the trainer. Use them if you feel you would like a bit more detail about specific topics before you teach them, or if you consider a particular group may benefit from a more detailed input on a given topic.

It is entirely up to you how much use you make of the additional trainer notes.









Additional material

In addition to the information in this manual, additional material is available including:

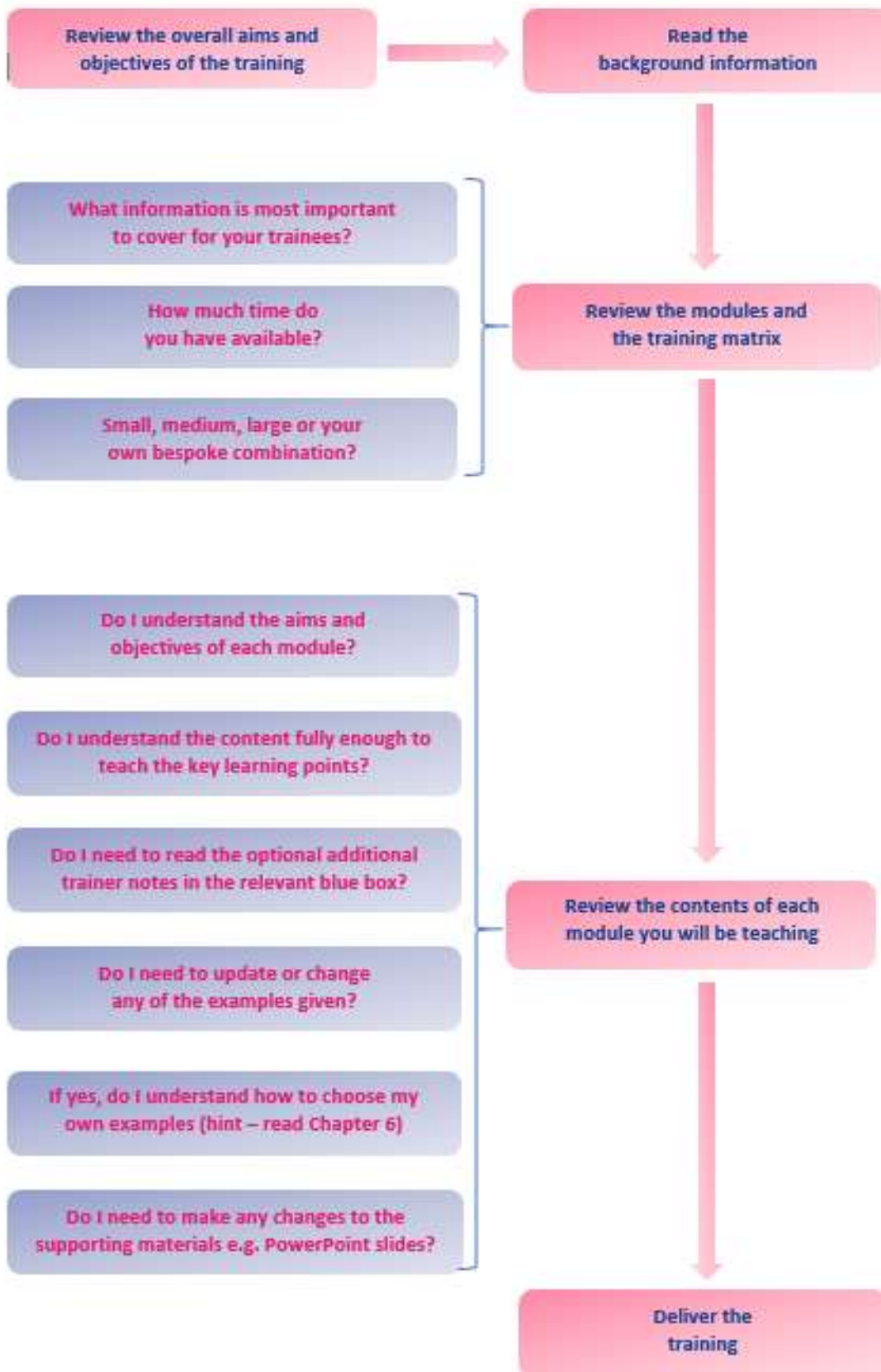
- optional PowerPoint slides with accompanying trainer notes;
- a resource pack (to be provided to the professionals once they have completed their training or, if they are completing the small version of the training, to be provided as a workbook).

Overview

The matrix below summarises the proposed training content for each of the training phases – preparation, training and follow-up – with each phase having a small, medium and large option that can be mixed and matched as described above.

	Preparation	Training	Follow-up
	10min Self-evaluation questionnaire	15-30min Self-study - read the introduction in the resource pack, along with the slides and accompanying trainer notes	10min Self-evaluation questionnaire
	 + Reflection questions	120-180min Critical Literacy and Online Awareness module. If all the activities are completed this module should take around 180 minutes. However, it can be adapted to 120 mins by selecting fewer activities or focusing on specific areas depending on the needs of the group.	 + Reflective journal
	 + Discussion group on reflection questions	+300min  + Two additional optional modules on Cyberawareness and Online Safety are available: Optional Module A – Cybercrime Awareness (90 mins approx) and Optional Module B – Cyberharassment (60 mins approx). There is also a short optional mini-module covering legislation (15 – 30 minutes)	+60min  + Safeguarding and Activity Design

How to use this manual – summary graphic





3 Preparation

Small-Medium-Large



Small

The aim of the preparation phase is to give participants an opportunity to reflect in advance of the training on their own online critical literacy and past experiences with encountering online disinformation. For the short version of the preparation phase, which should take about 10 minutes, participants need only rank their confidence in the following key competency areas. The answers to this questionnaire are private, and for the trainees' own reflection:

Choose the response on the scale from strongly disagree to strongly agree that most closely matches how confident you feel about each of the competency areas below	Not confident	Slightly confident	Somewhat confident	Confident	Very confident
Enhance the critical literacy of young people in relation to online information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Help young people understand the potential harm caused by false information online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support young people to effectively evaluate online information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support young people to be more resilient to false information online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Teach young people how to protect themselves from cybercrime	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Explain and enhance online privacy for young people	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Educate young people about the impact and implications of engaging in online hate speech and harassment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Help young people manage the pressures of social media	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

You do not need to share these answers with anyone. They are for your personal reflection. At the end of the training you will be asked to repeat this exercise and compare your answers, helping you to see where you have improved and if there remain any gaps in your knowledge that you can work through in the resource pack.



Medium

For the medium version of the preparation phase, which should take about 40 minutes, participants should complete the self-evaluation questionnaire and reflect on the following questions in advance of the training session:

REFLECTION QUESTIONS

What is your understanding of the terms? Disinformation, Misinformation, Fake News?

Can you think of a time when you've encountered false information online? If yes, how did you know it was false? If no, how confident are you in your ability to identify false information?

What do you think are the potential risks to young people of encountering false information online?

Can you think of a time when the young people you work with were influenced by news or other information online, which you knew or suspected was not true? Did you address this with them? If yes, how? If no, why not?



Large

For the large version of the preparation phase, which should last about 90 minutes, participants should complete the activities from the small and medium options. In addition, participants should be invited to attend a facilitated discussion group to explore further their responses to the reflection questions. Consider recording their responses on a flip chart or other appropriate methods so that they can be referred to during the training phase if needed.

Suggested Focus Group Ground Rules (you may add any additional ground rules you feel are appropriate)

1. Participation is voluntary.
2. The facilitator / trainer will ensure that all participants have a chance to talk.
3. If necessary, the focus group will be halted to provide the opportunity to take breaks.
4. Participants will be reminded to respect one another's privacy and not to divulge what they hear in the group.
5. The facilitator / researcher will make any reasonable accommodations a participant may need to enable them to take part comfortably in the focus group.



4 Training

Small-Medium-Large



Small

The small version of the training phase may be used if only 15-30 minutes is available for the training.

This option is a self-study option. Participants should read the information contained in the resource pack including:

- the presentation slides and accompanying notes, to provide professionals with the information and further reading resources they need to help them consider how they will transfer their knowledge to the professional context to support the young people they train;
- suggestions as to how the professionals can adapt the base content included in this training course to meet the needs of their specific professional context, including advice on how to select examples of false information to discuss with young people.



Medium

A medium size face-to-face training can be used when you have 2 to 3 hours.

Main Module: Critical Literacy and Online Awareness

This module is designed to take approximately 3 hours to deliver in full, but it can be adapted to make it shorter by varying which activities are included.

Aim:

To provide professionals with the knowledge, skills and confidence to support and empower young people to develop their online critical literacy and resilience to false information online.

Learning Outcomes:

1. Explain the meaning of the following terms: Misinformation, Disinformation, Fake News
2. Identify common categories of false information
3. Explain how and why false information spreads
4. Explain the harm caused by false information online
5. Identify the major fact checking organisations and explain their benefits
6. Identify, explain and apply the online critical literacy skills needed to evaluate information
7. Transfer the knowledge and skills gained during this training into the workplace to support young people to develop their own online critical literacy skills

Participants:

The optimal number of participants for this training is 6-12.

If you wish to run a smaller group, you may need to adapt some of the group work activities so that they can be done without having to split the group up.

If you wish to run a larger group, you may need to adapt some of the activities, particularly those that involve group work and reporting back findings, to ensure there is sufficient time for everyone to contribute.

Pre-Requisites:

Participants should have completed the pre-training questionnaire and, in addition, read and reflected on the following questions in advance of the training:

1. Can you think of a time when you've encountered false information online? If yes, how did you know it was false? If no, how confident are you in your ability to identify false information online?
2. Can you think of a time when, on reflection, you may have shared false information online? If yes, why did you share it? If no, why do you think other people may share false information online?
What do you think are the potential risks to young people, if any, of encountering false information online?
3. Can you think of a time when the young people you work with were influenced by news or other information online that you knew or suspected was not true? Did you address this with them? If yes, how? If no, why not? (If you cannot think of an example specifically relating to the young people you work with, consider this question more broadly, in relation to family members, friends and people you engage with online.)

Slides and trainer notes are available to support delivery of this module. However, it is also possible to deliver this training using whiteboard/flip charts and printed handouts as an alternative, if PowerPoint slides are not convenient to use. Where the group is asked to evaluate critically images, these can be printed out or accessed online.

This module is divided into 7 topics and takes approximately 3 hours to complete, if all core and optional activities are included. Timings may vary depending on how many participants there are and how they respond to each individual activity. It is advisable to be prepared to amend the number of optional activities undertaken depending on how fast or slowly each group progresses through the activities.

	Topic	Suggested Timing	Slides
1	Introduction, aim, learning outcomes, reflection questions	15 minutes	1-4
2	False Information: Definitions & Categories	30minutes	5-11
3	False Information: Propagation & Risk	15 minutes	12-14
4	Fact-Checking and Tips for Spotting Fake News	15 minutes	15-18
5	Practical Exercises: Verifying Online Information	40 minutes	19-22
6	In the Workplace: Empowering Young People	40 minutes	23-27
7	Summary and Close	10 minutes	28-30





How to use the trainer notes

The trainer notes for this module are provided below, along with the number of the relevant supporting slides. If you choose to use the supporting slides, you may wish to activate 'Presenter View' (by right clicking on the first slide once you've begun the presentation and selecting the appropriate option from the pop-up menu), which will enable you to see the relevant notes as you progress through the presentation. (The notes will not be projected onto the screen with the content of the slides – only you will be able to see them on the screen of your device.)

We recommend that prior to delivering the training you fully familiarise yourself with the content of the trainer notes. Check that any websites you plan to access during the training are working. Make sure any examples you are still using remain available and relevant. If you are using the supporting slides rehearse running the presentation, to familiarise yourself with the order in which the content appears and any animations.



Training Tip:

We strongly recommend that participants in this training also complete at least the short version of the training provided for 'Dealing with Controversial Issues'. This will support them when transferring their learning back into the work place and supporting young people directly, in the case of any difficult or challenging issues arising.

As the trainer, you may also wish to review the 'Dealing with Controversial Issues' training, to ensure you have a basic grasp of its contents and can relate it to the scenarios presented in this Critical Literacy training.

Topic 1: Introduction, aim, learning outcomes, reflection questions

Slides 1-4

Suggested time spent on this topic: 15 minutes

Introduction (Slide 1)

Trainer introduces themselves and gives a brief introduction detailing:

- Health and safety considerations;
- Ground rules, respect for others, confidentiality, non-judgmental space;
- Toilets;
- Fire exits;
- Comfort breaks (if planned);
- Refreshments (if available);

- A very brief overview explaining that the training will start by reviewing the aims and learning outcomes, will then cover the key areas of knowledge they need to learn, before moving onto guided practical and discussion activities.

A note on confidentiality:

As a general principle, we recommend communicating to training participants that 'whatever is said in the room, stays in the room.' In other words, everyone present should respect confidentiality and undertake not to share outside of the training environment any information disclosed by other participants. This is important, because it creates a 'safe' training space. However, it should also be stressed that there are limits to confidentiality, for example if a participant discloses something that raises a safeguarding concern in relation to a young person, or if a participant was to disclose that they had committed a criminal offence.

Aim and Learning Outcomes (Slides 2-3)



Core activity:

Introduce the overall aim of the training session. You could have this pre-written on a flip-chart / whiteboard / smartboard or you could use the optional PowerPoint slide provided:

“To provide you with the knowledge, skills and confidence to support and empower young people to develop their critical literacy and resilience to false information online.”



Suggested activity:

Ask each member of the group to briefly introduce themselves, describe their role working with young people, and their personal objective for today's training session. Record their personal objectives on a whiteboard / flip-chart / smartboard (or ask participants to write their objectives on post-it notes and stick them up on a wall, which may be done anonymously if preferred).



Core activity:

Introduce the 7 learning outcomes, either by writing them in advance on a flip chart / whiteboard or using the optional PowerPoint slide. You will come back to these during the summary at the end of the training session.

1. Explain the meaning of the following terms: Misinformation, Disinformation, Fake News
2. Identify common categories of false information
3. Explain how and why false information spreads
4. Explain the harm caused by false information online
5. Identify the major fact checking organisations and explain their benefits
6. Identify, explain and apply the online critical literacy skills needed to evaluate information
7. Transfer the knowledge and skills gained during this training into the workplace to support young people to develop their own online critical literacy skills



Suggested activity:

Depending on the personal objectives provided by the participants during the previous activity, you may be able to draw links between their answers and the learning outcomes. If their expressed personal objective is outside of the purview of this training, take this opportunity to manage their expectations, focusing on the positive – what they will cover in this session, rather than what they will not.

Advise the participants you will come back to these learning outcomes at the end of the session to review.

Reflection Questions 1 & 2 (Slide 4)



Core activity:

Remind the participants of Q1 & Q2 of the prerequisite reflection questions and facilitate a brief discussion about this. You may have written the questions up in advance on a whiteboard / flip chart, or you can use the optional PowerPoint slide provided.

1. Can you think of a time when you have encountered false information online? If yes, how did you know it was false? If no, how confident are you in your ability to identify false information online?
2. Can you think of a time when, on reflection, you may have shared false information online? If yes, why did you share it? If no, why do you think other people may share false information online?

You may wish to briefly record a few key points raised on a flip chart / whiteboard to refer back to as you work through the training session, but this is not compulsory.

An alternative method for delivering this activity is to divide the group into pairs or small groups to discuss their responses to these questions. Rotate around each group to listen in to their discussions if you choose this option. You may wish to

debrief this activity succinctly with the whole group once the discussions are concluded by asking for a spokesperson to report the key points for each group.

Topic 2: False Information: Definitions & Categories

Slides 5-11

Suggested time spent on this topic: 30 minutes

False Information Definitions (Slide 5)



Core activity:

Introduce the participants to the following 3 definitions, using either the optional PowerPoint slide, distributing the printable sheet or by writing them on the flip chart / whiteboard.

Disinformation: false information created deliberately with the intention of causing harm or for profit

Misinformation: false information but not created/shared with the intent of causing harm

Fake News: false information presented as genuine news, which is usually created deliberately for harm or profit [disinformation] but may also be created / or shared without malicious intent [misinformation]



Suggested activity:

Ask the participants if they can think of any examples for each of the definitions. Participants may provide high-level examples (e.g., hoaxes or propaganda for disinformation, urban legends for misinformation) but may also provide specific examples of false information they have encountered. Ensure you have consulted the examples provided in the trainers' manual so that you are able to facilitate this discussion effectively.

KEY POINTS TO COVER FOR BOTH CORE AND OPTIONAL ACTIVITIES:



- Disinformation is created with *intent* (harm or profit);
- Misinformation is usually shared with good intentions but can still be harmful;
- ‘Fake News’ is most often a form of ‘disinformation’ but it can also be ‘misinformation’ if not created with intent (e.g., sloppy journalism or fake / pseudo-science).

It is also important to bear in mind that the term ‘fake news’ may be deployed by powerful people to try to undermine verifiable news reports that are not favourable to them. Can you or the group think of any examples when this has happened recently?

Additional Trainer Notes: Disinformation and Misinformation

Below are some more in-depth explanations of the difference between disinformation and misinformation, with references. You do not need to share these with the training participants – they are purely for your own knowledge and preparation, if needed.

Disinformation - false information knowingly and deliberately disseminated with the intention of manipulating people. It is often orchestrated and makes use of resources such as automated technology and hacking.

Misinformation - false information but believed to be true by the person disseminating it.

There is a third type of information - Mal-information - essentially true information deployed maliciously to cause harm to an individual, organisation or country (for example publicly outing a gay politician with the intention of harming their political career). This sort of information is not covered in this training but you may find it useful to be aware of it in case any of the participants asks a relevant question.

An alternative definition of “disinformation” from the European Commission’s High-Level Expert Group on fake news and online disinformation is: “includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally *cause public harm or for profit*”. [italics added]

Sources:

Directorate-General for Communications Networks Content and Technology. (2018). *A Multi-Dimensional Approach to Disinformation: Report of The Independent High-Level Group on Fake News and Online Disinformation*. <https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation>

UNESCO. (2018). *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*. <https://unesdoc.unesco.org/ark:/48223/pf0000265552>

Additional Trainer Notes: Fake News

Trainer Note:

The explanation of “fake news” given above is the working definition used throughout this training. However, there are many other more complex and

nuanced definitions available that you may wish to familiarise yourself with. Depending on the context (for example what role that participants in your training have working with young people, and the age of the young people they work with) you may wish to discuss the meaning of “fake news” in greater depth. The below quote, from the High-Level Expert Group, provides a good example of a more complex definition should you need one:

“The term [fake news] is inadequate to capture the complex problem of disinformation, which involves content that is not actually or completely “fake” but fabricated information blended with facts, and practices that go well beyond anything resembling “news” to include some forms of automated accounts used for astroturfing, networks of fake followers, fabricated or manipulated videos, targeted advertising, organized trolling, visual memes...It can also involve a whole array of digital behaviour that is more about circulation of disinformation than about production of disinformation, spanning from posting, commenting, sharing, tweeting and re-tweeting etc.”

The UNESCO report on journalism and fake news argues that ‘disinformation’ and ‘misinformation’ are often conflated as ‘fake news’ but the term ‘fake news’ is problematic because:

“‘[N]ews’ means verifiable information in the public interest, and information that does not meet these standards does not deserve the label of news. In this sense then, ‘fake news’ is an oxymoron which lends itself to undermining the credibility of information which does indeed meet the threshold of verifiability and public interest – i.e., real news.”

False Information Categories (Slides 6-11)

This training references six categories of false information. This is not an exhaustive list and the categories selected generally fall within the broad definition of 'fake news' (as opposed to, for example, fake reviews left on a selling website, designed to make you buy a product or service). They include both misinformation and disinformation type examples.



Core activity:

Present the following categories of online false information to the participants:

1. Clickbait / misleading headlines
2. Biased / sloppy journalism
3. Satire / Parody
4. Propaganda
5. False / Pseudo science
6. Manipulated images / videos

Options available for delivering this content:

- Use the PowerPoint slides provided – these are pre-populated with examples of each category, including images. (You can find the sources of the examples in the additional trainer notes below);
- Update the PowerPoint slides provided, populating the slides with your own examples that you feel may be more relevant to your context or merely more up to date (see the trainers' manual for advice on how to choose your own examples);
- Create printed out versions of each example and provide them to the participants;
- Write each category up on a flip chart and facilitate a brief discussion of each, asking the group for examples and drawing out the main points contained in the trainer notes for each category.



KEY POINTS:

1. Clickbait / misleading headlines – where the headline does not match the accompanying story or the story does not live up to the promise of the headline. Usually created for the profit gained from users ‘clicking’ on the headline;
2. Biased / sloppy journalism – where a story is framed to fit a preconceived narrative or has been poorly fact checked;
3. Satire / parody – usually created for profit but not intended to harm. May be mistaken for genuine news, especially if the content conforms with the reader’s personal biases;
4. Propaganda – not new, think of famous propaganda examples throughout history (e.g., government created propaganda in wartime). But can be spread effectively online (e.g., memes, ‘fake news’ stories) and is commonly used by those with extremist views (examples alt-right use of Pepe the frog, ISIS online propaganda, left wing Russian Internet Research Agency);
5. False / pseudo-science – can be created as political disinformation (climate change, pandemic lockdowns), for profit (selling products) or with good intentions (how to avoid catching COVID);
6. Manipulated images / videos – relatively easy to make with modern technology, can be convincing on first glance.



Although it is possible to devote a lengthy period to the categories of false information, we recommend trying to keep this section to a 30 minutes maximum limit. This is because examples and types of false information can and will change, so it is more important to spend time on the activities designed to increase participants’ skills in evaluating online information, which will remain relevant even if the types of false information change in the future.

Additional Trainer Notes – Clickbait / Misleading Headlines

A BBC News article defines clickbait in the following very helpful way:

“Put simply, it is a headline which tempts the reader to click on the link to the story. But the name is used pejoratively to describe headlines which are sensationalised, turn out to be adverts or are simply misleading” (Frampton, 2015).

Clickbait, is content is driven by profit – drawing more ‘clicks’ to the media organisation’s page means they can charge more for advertising. Typically, clickbait headlines promise more than they deliver.

Consumers may click even if they know its clickbait because the headline exploits their curiosity. Bizarre topics, quizzes, optical illusions, lists with a headline that suggests an item near the end of the list is especially horrifying or surprising, a challenge to the reader’s intelligence are all effective clickbait subjects.

This is demonstrated by the images of clickbait headlines which appear on the slide- an image of the actor Dakota Fanning from the *Reductress* website.

The slide for the misleading headlines shows a screenshot of an article from Le Journal Des Femmes, which seems to claim that side effects of the COVID vaccination have resulted in 1 death and 6 serious side effects in France. However, this article has been fact-checked by AFP Factual, and found to be misleading. The source for Le Journal Des Femme’s article was a press release issued by L’Agence Nationale De Sécurité du Médicament et des Produits de Santé, which ensures the safety of health-related products.

While the press release in question no longer appears to be available, AFP Factual explains that it specified that there is no evidence linking the death of a person who died shortly after being vaccinated to the vaccine. This information is mentioned in Le Journal Des Femme’s article, several paragraphs in, but the headline and the opening paragraph still suggested the existence of an established link between the vaccination and a death, which is untrue. The article was subsequently widely shared on social media in support of anti-vaccination arguments.

Research shows that misleading headlines affect readers’ recall of the facts contained in the following story and that subtle misinformation is more damaging than blatant (and therefore more easily identifiable) misinformation. An [article published in The New Yorker \(Konnikova, 2014\)](#) cites a *Daily Express* article (Rawle, 2013) as an example of a misleading headline. The headline is: “Air Pollution Now Leading Cause of Cancer”, when, in fact, the article states that air pollution is “a leading *environmental* cause of cancer deaths.” [emphasis added] At the end of the article is a quote from an expert confirming, “although air pollution increases the risk of developing lung cancer by a small amount, other things have a much bigger effect on our risk, particularly smoking.”

Sources and further reading:

Davidson, L. (2018, April 17). Generation Rent: Third of Millennials Face Renting for Their Entire Lives and Never Own Their Own Homes. *The Sun*. <https://www.thesun.co.uk/money/6069081/third-of-millennials-face-renting-for-their-entire-lives-and-never-own-their-own-homes/>

Frampton, B. (2015, September 14). Clickbait: The Changing Face of Online Journalism. *BBC News*. <https://www.bbc.co.uk/news/uk-wales-34213693>

Konnikova, M. (2014, December 17). How Headlines Change the Way We Think. *The New Yorker*. <https://www.newyorker.com/science/maria-konnikova/headlines-change-way-think>

Rawle, T. (2013, October 17). Air pollution now leading cause of lung cancer. *Daily Express*. <https://www.express.co.uk/life-style/health/437473/Air-pollution-now-leading-cause-of-lung-cancer>

Rubin, A. (2020, February 4). Wow! This Child Actress is All Grown Up, and You Won't Believe How Much She Hates Your Obsessions with What She Looks Like Now. *Reductress*. <https://reductress.com/post/wow-this-child-actress-is-all-grown-up-and-you-wont-believe-how-much-she-hates-your-obsession-with-what-she-looks-like-now/>

Staines, C. (2018, May 9). When Headlines Aren't Quite as They Seem. *Full Fact*. <https://fullfact.org/blog/2018/may/headlines-arent-quite-as-they-seem/>

Additional Trainer Notes – Biased / Sloppy Journalism

The slide for this category includes two fictionalised examples of headlines about President Trump leaving office, to show how the same event might be interpreted differently by sources with different biases. We have included this as an example of how you can create your own examples to use in the training if you feel this is more appropriate. You can use these examples in the training, or replace them with ‘real life’ examples of your choosing, such as the one below relating to members of the British Royal Family, if you prefer.

In 2020, a BuzzFeed article compared a range of newspaper headlines about two members of the British Royal Family, the Duchess of Cambridge and the Duchess of Sussex, providing an excellent example of the way bias can influence the way a newspaper story is framed. In this case, the headlines for the Duchess of Cambridge are positive and the headlines for the Duchess of Sussex are negative even when covering the same subjects / issues (Hall, 2020).

Examples of sloppy journalism include biased information, only interviewing people who represent one side of the story, information containing errors, voluntary or involuntary omissions and biased interpretations.

The *Washington Post* published an article in December 2016 claiming a Russian operation had hacked a Vermont utility, putting the US electrical grid security at risk (Eilperin & Entous, 2016). The online story was later corrected confirming there had been no penetration of the US Electrical Grid because it was not attached to the hacked facility. A further article was published a few days later confirming no Russian hacking had taken place (Nakashima & Eilperin, 2017). This is a good example of both bias – the journalist framed the story to fit a preconceived narrative – and sloppy journalism that was not properly fact checked. An editorial in *Observer* went so far as to argue that the *Washington Post* story was more serious than merely sloppy journalism and an example of a newspaper tailoring facts to fit a predetermined narrative (“Fake News, Sloppy News...”, 2017).

An important point to remember is that bias may be both subtle and ‘a consequence of unconsciously imprinted ideas and social practices’ and can manifest even when neutrality is the aim. Research carried out by Swansea University uncovered subtle bias in the reporting by Dutch newspapers about the perpetrators of mass shooting events in the USA, concluding that Muslim perpetrators were more often described as terrorists than white perpetrators, and religion and ethnicity were mentioned more prominently in articles about non-white perpetrators, “strengthening the link between Islam, ‘foreign’ and ‘terrorism’” (De Veen & Thomas, 2020).

Sources:

De Veen, L. and Thomas, R. (2020). Shooting for Neutrality? Analysing Bias in Terrorism Reports in Dutch Newspapers. *Media, War & Conflict* (1-19).

<https://journals.sagepub.com/doi/pdf/10.1177/1750635220909407>

Eilperin, J. & Entous, A. (2016, December 31). Russian Operation Hacked a Vermont Utility, Showing Risk to U.S. Electrical Grid Security, Officials Say. *Washington Post*.

https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html

Fake News, Sloppy News and Bad News. (2017, May 1). *Observer*.

<https://observer.com/2017/01/fake-news-sloppy-news-and-bad-news/>

Hall, E. (2020, January 13). Here Are 20 Headlines Comparing Meghan Markle To Kate Middleton That May Show Why She and Prince Harry Left Royal Life.

Buzzfeed. <https://www.buzzfeednews.com/article/ellievhall/meghan-markle-kate-middleton-double-standards-royal>

Nakashima, E. & Eilperin, J. (2017, January 2). Russian Government Hackers Do Not Appear to Have Targeted Vermont Utility, Say People Close to Investigation.

Washington Post. https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5_story.html

Additional Trainer Notes – Satire / Parody

The three articles screenshotted on the slide can be found here:

Biden Unveils Skin Color Chart to Determine Who Gets Federal Aid. (2021, January 12). *Babylon Bee*. <https://babylonbee.com/news/biden-releases-skin-color-chart-to-determine-who-gets-federal-aid>

Trump Blames Nation's Susceptibility to Coronavirus Outbreak on Weakness of America's Race-Muddled Gene Pool. (2020, May 11). *The Onion*. <https://www.theonion.com/trump-blames-nation-s-susceptibility-to-coronavirus-out-1843392614>

The *Babylon Bee* article is a good example of how truth is blended with fiction. The first part of the quote given in the article (see below) announcing the priority of Black, Latino, Asian and Native American owned small businesses is accurate. The second part of the quote regarding the provision of a colour chart is completely made up.

“Our priority will be Black, Latino, Asian, and Native American-owned small businesses, women-owned businesses,” Biden informed the nation. “We are sending out a new color chart to all agencies involved to make sure there is no malarkey with white males and those with melanin deficiencies cutting in from where we are placing them at the back of the line” (“Biden Unveils...”, 2021).

Research published in *The Conversation* in 2019 indicated that individuals were not always able to distinguish satirical news from real news, and that political affiliation had an impact on the likelihood of believing a particular story to be true [confirmation bias]. For example, 23% of Republicans believed a satirical story in The Babylon Bee attributing fabricated negative statements about Jews to US Democratic and Muslim politician Ilhan Omar, compared to only 8% of Democrats. In another example, 14% of Democrats (compared to 5% of Republicans) believed a satirical Onion story about Alabama's restrictive abortion bill and a 12-year-old victim of sexual abuse who wanted an abortion was true. In other words, research participants were found to be more likely to believe an item of satirical news was true, the more closely the claim in the article aligned to their political beliefs (Garrett, Bond & Poulsen, 2019).

Sources:

Garrett, R. K., Bond, R. & Poulsen, S. (2019, August 16). Too Many People Think Satirical News Is Real. *The Conversation*. <https://theconversation.com/too-many-people-think-satirical-news-is-real-121666>

Additional Trainer Notes – Propaganda

The images on the Propaganda slide are:

A still from a video by New China TV mocking the USA's response to COVID-19 (New China TV, 2020);

An image of Pepe the frog, an initially harmless cartoon that was appropriated by the far-right as a hate symbol and propagated through the use of memes as a way to normalise hate-speech online (Associate Press and Griffith, 2019);

An image of Pepe the frog photoshopped onto a photograph of Thierry Baudet, a popular figure in Dutch alt-right culture (Bastiaanse, 2019);

A version of the popular 'Distracted Boyfriend' meme. This popular meme is a stock image of a man out with his girlfriend, caught by her staring at another woman. The labels on the individuals can be changed to almost anything, suggesting that a person or group (represented by the man) is beginning to look away from something that previously interested them (represented by the girlfriend) towards something new (the other woman). In most cases, the labels applied are amusing and harmless, but it can also be used for propaganda purposes, as in the article on the slide. Because the meme is so ubiquitous and people are used to it being funny and harmless, this is another example of how online memes can be used to normalise propaganda and / or hate speech ("Distracted Boyfriend", 2018);

Further examples of online propaganda include:

the sanctioning of Russia's RT news channel by the UK media watchdog Ofcom, imposing a £200,000 fine for breaching impartiality rules while reporting the Salisbury nerve agent attack, and the wars in Syria and Ukraine (Dearden, 2018). More recently, Ofcom revoked RT's licence to broadcast in the UK as a result of 29 ongoing investigations into the impartiality of their reporting in relation to the Russian invasion of Ukraine (Ofcom, 2022).

Chinese propaganda surrounding the Covid-19 pandemic –including the use of 'sock puppet accounts' to spread propaganda favourable to China on social media. (A 'sock puppet' is a term used to refer to a false online identity, for example one used to comment on online articles promoting a particular opinion) (Kao & Shuang Li, 2020).

Sources and further reading:

Anti-Defamation League. (n.d.) *Pepe the Frog*.

<https://www.adl.org/education/references/hate-symbols/pepe-the-frog>

Associated Press & Griffith, K. (2019, May 18). Judge Allowed Cartoonist Who Created Pepe the Frog to Continue His Lawsuit Against Alex Jones' Infowars For Selling A Poster of The Character That Became an Emblem of The Far-Right. *Daily Mail*. <https://www.dailymail.co.uk/news/article-7043569/Judge-allows-cartoonist-created-Pepe-Frog-continue-lawsuit-against-Alex-Jones-Infowars.html>

Bastiaanse, R. (2019, March 20). Memes, 4chan And the Strategic Ambivalence of Thierry Baudet. *Diggit Magazine*.
<https://www.diggitmagazine.com/column/memes-4chan-and-strategic-ambivalence-thierry-baudet>

Brzeski, P (2020, May 4). China Mocks Trump's Response to Coronavirus in Lego-Like Animation. *The Hollywood Reporter*.
<https://www.hollywoodreporter.com/news/china-mocks-trumps-response-coronavirus-lego-like-animation-1293049>

CBC News. (2016, October 6). *Is Pepe the Frog a Hate Symbol?* YouTube.
<https://www.youtube.com/watch?v=lg1Hoi-g6Y&t=43s>

De Cristofaro, E. (2018, December 12). Memes Are Taking the Alt-Right's Message of Hate Mainstream. *The Conversation*. <https://theconversation.com/memes-are-taking-the-alt-rights-message-of-hate-mainstream-108196>

Dearden, L. (2018, December 20). RT Could Be Banned from Broadcasting in UK For Breaching Impartiality Rules. *Independent*.
<https://www.independent.co.uk/arts-entertainment/tv/news/rt-russia-today-ofcom-banned-impartiality-skripal-syria-galloway-propaganda-a8692141.html>

Distracted Boyfriend. (2018 [updated 2021]). *Know Your Meme*.
<https://knowyourmeme.com/memes/distracted-boyfriend#photos>

Faife, C. (2017, June 1). How 4Chan's Structure Creates a Survival of the Fittest for Memes. *Vice*. <https://www.vice.com/en/article/ywzm8m/how-4chans-structure-creates-a-survival-of-the-fittest-for-memes>
<https://www.technologyreview.com/2018/06/11/142394/this-is-where-internet-memes-come-from/>

Kao, J., & Shuang Li, M. (2020, March 26). How China Built A Twitter Propaganda Machine Then Let It Loose on Coronavirus. *ProPublica*.
<https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>

MIT Technology Review. (2018, June 11). *This Is Where Internet Memes Come From*. June 11, 2018. <https://www.technologyreview.com/2018/06/11/142394/this-is-where-internet-memes-come-from/>

New China TV. (2020, April 30). Once Upon A Virus... YouTube.
<https://youtu.be/Q5BZ09iNdvo>

Ofcom. (2022, March 2022). *Ofcom Revokes RT's Broadcast Licence*.
<https://www.ofcom.org.uk/news-centre/2022/ofcom-revokes-rt-broadcast-licence>

Panneton, D. (2019, March 22). Online Memes May Seem Frivolous but They Normalize Hate with Potentially Deadly Results. *The Globe and Mail*.
<https://www.theglobeandmail.com/opinion/article-online-memes-may-seem-frivolous-but-they-normalize-hate-with/>

Additional Trainer Notes – False / Pseudo Science

False information online relating to science can be created as political disinformation (climate change denial, denial of the existence of evolution), for profit (selling products e.g., weight loss aids) or with good intentions (e.g., inaccurate information about how to avoid catching COVID, but which has been shared with good intentions).

A key difference between science and pseudoscience is that science “is set up to *challenge* its claims and look for evidence that might prove it false,” whereas pseudoscience “is set up to look for evidence that supports its claims” - in other words, cherry-picking the available evidence to support a desired conclusion (Stemwedel, 2011 - citing the philosopher Karl Popper).

The coronavirus pandemic has seen many examples of false science information being shared online which have the potential to be harmful to health, including the circulation of advice on how to avoid catching COVID, which is inaccurate and could cause harm by creating a false sense of security, and vaccine denialism, where, the efficacy of clinically proven vaccines is undermined.

The examples contained on the slide for this topic are:

a screenshot of a Facebook post which claims that COVID can be cured by drinking garlic water.

Cisse, D. (2020, March 3). Coronavirus: Bonne Nouvelle [image containing text].
Facebook.

<https://www.facebook.com/photo.php?fbid=3166970513334711&set=a.434404883257968&type=3&theater> captured by Perma.cc <https://perma.cc/J26V-L7BJ?type=image>

a fake news headline about a COVID-19 vaccine affecting DNA which we created ourselves to show how easy it is to do;

The Facebook post about drinking garlic water to cure COVID, which was circulated thousands of times in various languages, was factchecked by AFP Factual using multiple scientific, medical and government sources and found to be false (AFP Pakistan, 2020).

Other examples of pseudo or fake science include some claims made to support health and beauty products. Pakman (2017) alleges that GOOP, the wellbeing and beauty company owned by the actor Gwyneth Paltrow, uses pseudoscientific claims to market its products, including suggesting customers undertake practices such as vagina-steaming, jade vaginal eggs and apitherapy (being stung by bees). These practices are potentially physically harmful but there is, particularly for younger people, also the risk of harm to body image - for example, GOOP has been accused of glorifying diet culture by promoting the idea of a 'leanest, liveable weight' (Moss, 2018).

Sources and further reading:

Carroll, S.B. (2020, November 8). The Denialist Playbook. *Scientific American*.
<https://www.scientificamerican.com/article/the-denialist-playbook/>

David Pakman Show. (2017, June 27). Gwyneth Paltrow's Scam Products Called Out by NASA. *YouTube*. <https://www.youtube.com/watch?v=PBHpD-9loSQ>

Montesin, M. (2020, March 10). French Government Confirms That Cocaine Does Not Cure Coronavirus. *Happy Mag*. <https://happymag.tv/french-government-confirms-that-cocaine-does-not-cure-coronavirus/>

Moss, R. (2018, February 9). Gwyneth Paltrow's Goop Slammed for Telling Women How to Be Their 'Leanest Liveable Weight'. *Huffington Post*.
https://www.huffingtonpost.co.uk/entry/gwyneth-paltrows-goop-slammed-for-telling-readers-how-to-be-their-leanest-liveable-weight_uk_5a7c1fafe4b0c6726e0f9af8?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xILmNvbS8&guce_referrer_sig=AQAAANrspXTU945SwADraMYqV7olQuXaGWYAu6CzCiCD1RYCn8cE3PMXvWOy8uaSHfuF8dggcojzwqaJOIV6wvGDmf6GhrsB7kEvlT26teq50THQBITCCA4SG_HHoeMliqbZTHEfCwcDWcAQWsihxP7JZ9BT6d22xJSW8Wck5DPx3jIT

Ouatik, B. (2020, March 13). Non, Aucune Boisson Ne Guérit Le Coronavirus. *Radio-Canada*. <https://ici.radio-canada.ca/nouvelle/1664623/mythes-eau-boissons-chaudes-alcool-coronavirus-faux>

Stemwedel, J.D. (2011, October 4) Drawing the Line Between Science and Pseudo-Science. *Scientific American*. <https://blogs.scientificamerican.com/doing-good-science/drawing-the-line-between-science-and-pseudo-science/>

Vijaykumar, S. (2019, August 7). Pseudoscience Is Taking Over Social Media and Putting Us All at Risk. *The Independent*.
<https://www.independent.co.uk/news/science/pseudoscience-fake-news-social-media-facebook-twitter-misinformation-science-a9034321.html>

Additional Trainer Notes – Manipulated Images / Video

Deepfake videos are relatively easy to make with the right software and have been used among other things to make it appear as though politicians have said or done something that would be damaging to them or not in accordance with their political views, or to 'stitch' famous people (usually women) onto porn videos without their consent. Research conducted by the University of Amsterdam using a relatively poor quality deepfake video of a Dutch politician created by the researchers found that the majority of a panel of 287 people who were shown the video judged it to be genuine (University of Amsterdam, 2020).

The example deepfake videos included on the slide are below. A key point to bear in mind when watching these videos is that they have all been made by people who are open about the fact that they are making deepfake videos, for the purposes of demonstrating how the technology might be misused. For this reason, it may be easier to identify these videos as being deepfake than those made by people whose intent is to deceive.

NBC News. (2019, October 27). Deep Fakes: How They're Made and How They Can Be Detected. *YouTube*. <https://www.youtube.com/watch?v=C8FOOP2a3dA>

Channel 4. (2020, December 25). The Alternative Christmas Message 2020. *Facebook*. <https://www.facebook.com/watch/?v=243343943850219>

Ume, C. (2021, March 5). DeepTomCruise TikTok Breakdown. *YouTube*. <https://www.youtube.com/watch?v=wq-kmFCrF5Q>

Additional examples, not shown on the slide, are:

The Telegraph. (2019, November 12). Jeremy Corbyn Urges Voters to Back Boris Johnson for Prime Minister in Disturbing Deepfake Video. *YouTube*. <https://www.youtube.com/watch?v=EkfnjAeHFAk>

Sources and further reading:

Cuthbertson, A. (2019, February 8). What Is Deepfake Porn? AI Brings Face-Swapping to A Disturbing New Level. *Newsweek*. <https://www.newsweek.com/what-deepfake-porn-ai-brings-face-swapping-disturbing-new-level-801328>

Hern, A. (2020, January 7). Facebook Bans Deepfake Videos in Run-Up to US Election. *The Guardian*. <https://www.theguardian.com/technology/2020/jan/07/facebook-bans-deepfake-videos-in-run-up-to-us-election>

Paul, K. (2019, October 7). California Makes Deepfake Videos Illegal but Law May Be Hard to Enforce. *The Guardian*. <https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce>

University of Amsterdam. (2020, August 24). *Would you fall for a fake video? UvA Research Suggests You Might*. <https://www.uva.nl/en/content/news/press-releases/2020/08/would-you-fall-for-a-fake-video-uva-research-suggests-you-might.html?cb&cb>

Villas-Boas, A. (2019, November 30.) China Is Trying to Prevent Deepfakes With New Law Requiring That Videos Using AI Are Prominently Marked. *Business Insider*. <https://www.businessinsider.com/china-making-deepfakes-illegal-requiring-that-ai-videos-be-marked-2019-11?r=US&IR=T>



Timesaver Tip:

If you judge that the group you are training would benefit from spending less time on the background (definitions / categories of false information) and more time on the practical elements (verifying online information / discussion scenarios), you may wish to replace the activities provided under Topic 2 with one or more of the following options. Remember to adjust your timings accordingly:

- Facilitate a group discussion, asking the group to provide examples of “false information” or “fake news” they have seen online. As they provide you with examples, record them on a whiteboard or flipchart. You may wish to suggest examples of your own to ensure a full range of the categories are included. As you debrief the activity you can provide as much detail about the definitions of disinformation, misinformation and fake news as you feel is appropriate for the group. (Suggested time 10 minutes.)
- Create your own additional examples to use in the practical verification activities (see advice [in Chapter 2](#) on how to choose and create your own examples) expanding the range of categories of false information represented and ensuring there are some examples of misinformation and some of disinformation. If you choose this option, be sure to manage the debrief/discussion of the activities to ensure that the definitions of disinformation, misinformation and fake news are covered, as well as highlighting the different types of false information. (Suggested time 15 minutes per example for research plus 10 minutes for each group to report their findings.)

Topic 3: False Information – Propagation and Risk

Slides 12-14

Suggested time spent on this topic: 15 minutes

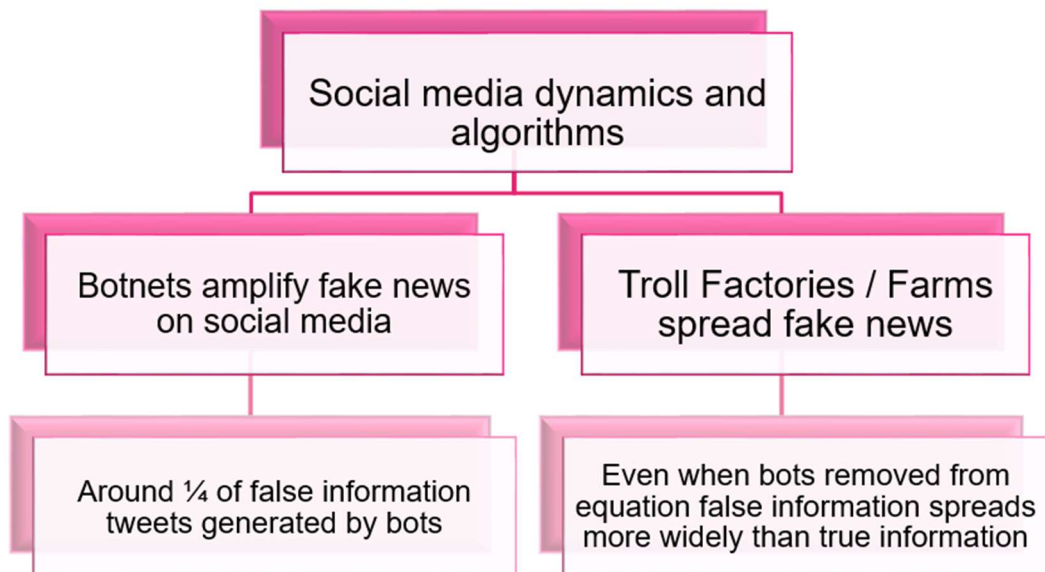
How false information spreads (Slide 12)



Core activity:

Present the information below either by showing the optional PowerPoint(s) slide, or by drawing a diagram (example below) on a whiteboard / flip chart.

How false information spreads



KEY POINTS

- False information has been shown to spread faster and more widely online than true information – via social media dynamics and algorithms;
- It can be shared by technology (bots), and humans (organised e.g., a troll factory or by individuals clicking and sharing on social media);
- A social media bot is automatically programmed to post and share content
- A troll factory is a team of people employed to spread fake news or other content on social media with the purpose of covertly influencing public opinion.

Additional Trainer Notes – How False Information Spreads

Social media dynamics and algorithms promote the spreading of fake news. A bot is any automated computer programme that runs on the internet, many of which have legitimate uses such as web crawlers which index information for search engines, and chatbots used for online forum moderation. The type of bot that contributes to the spread of false information online is an automated social media account, which can link up into a network with other similar bots to spread misinformation and disinformation.

Further reading:

Abeshouse, B. (2019, February 8). Troll Factories, Bots and Fake News: Inside the Wild West of Social Media. *Al Jazeera*.

<https://www.aljazeera.com/blogs/americas/2018/02/troll-factories-bots-fake-news-wild-west-social-media-180207061815575.html>

DW English. (2018, April 16). Manipulative Social Bots. *YouTube*.

<https://www.youtube.com/watch?v=e14aK8s4QIA>

Kaspersky. (n.d.) *What Is A Botnet?* <https://www.kaspersky.fr/resource-center/threats/botnet-attacks>

Knight Foundation. (n.d.). *How Much “Fake News” Can We Identify on Twitter?*

<https://knightfoundation.org/features/misinfo/>

Perekalin, A. (2019, May 15) Uncovering Fake News Bots. *Kaspersky Daily*.

<https://www.kaspersky.com/blog/fake-news-bots/26943/>

The harm caused by false information (Slides 13-14)

Participants will have been asked to reflect on this topic in advance of the training, using reflection question 3:

What do you think are the potential risks to young people, if any, of encountering false information online?



Core activity:

Facilitate a 10-minute discussion drawing on the participants' expertise in working with young people. Try to encourage the participants to think about harm in a broader context as well as harm caused by specific incidents of false information. When debriefing this discussion, make sure to include any of the points listed below that have not already been raised by the participants:



KEY POINTS

- Promotes echo chambers, filter bubbles and confirmation bias (see explanations for each of these terms in the additional trainer notes or use the optional PowerPoint slide provided)
- Strengthens resentment and can fuel outrage, leading to polarisation between groups
- Can undermine democratic political processes and values shaping public policy (health, science, finance) (Directorate-General for Communications Networks, 2018).
- Can lead to people becoming politicised by false information

In addition, specifically in relation to children:

- Exposure to fake news can:
 - Increase children's anxiety;
 - Damage their self-esteem;
 - Skew their world-view.
- Only 2% of UK children have the critical literacy skills needed to tell if news is real or fake (National Literacy Trust, 2018a).

Source and further reading:

National Literacy Trust. (2018a). *Fake news and critical literacy: The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools*.
https://cdn.literacytrust.org.uk/media/documents/Fake_news_and_critical_literacy_-_final_report.pdf



Training Tip:

You may wish to consider introducing at this point a discussion about how the personal biases of the training developers, the trainer and the trainees may shape the way they have engaged with this training, with a view to encouraging them to think about how this may translate into the workplace when working with young people. How may their own personal biases affect the way they support young people to approach evaluating information online? How may the young people's personal biases affect the way they evaluate information?

Additional Trainer Notes – The Harm Caused by False Information

A report by the Online Civil Courage Initiative found that not only does disinformation spread more widely and quickly on social media than verified news, but that the actors responsible for disseminating fake news can make use of 'echo chambers' and 'filter bubbles' to promote their particular agenda. For example, during the 2017 German parliamentary election, 8 out of 10 of the most widely disseminated fake news articles concerned refugees and crime. This has consequences for the use of fake news to strengthen resentment and fuel outrage, which can lead to people becoming politicised as a result of having interacted with disinformation (Baldauf, Ebner & Guhl, 2019).

The European Commission High Level Group on Fake News and Online Disinformation noted that:

*“[w]hile not necessarily illegal, **disinformation** can nonetheless be harmful for citizens and society at large. The risk of harm includes threats to democratic political processes, including integrity of elections, and to democratic values that shape public policies in a variety of sectors, such as health, science, finance and more”* (Directorate-General for Communications Networks, 2018).

Research by the National Literacy Trust found that only 2% of children have the necessary critical literacy skills to be able to identify whether news is real or fake. The research also found that fake news promotes 'a culture of fear and uncertainty amongst young people', and that almost two-thirds of teachers believe fake news increases children's anxiety, harms their self-esteem and skews their world-view. Almost half of older children get their news from websites and social media, but only a quarter of these children trust the online sources they are using (National Literacy Trust, 2018a).

Sources and further reading:

Baldauf, J., Ebner, J. and Guhl, J. (eds). (2019) Hate Speech and Radicalisation Online: The OCCI Research Report. *Institute for Strategic Dialogue*.

<https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>

National Literacy Trust. (2018a). *Fake news and critical literacy: The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools*.

https://cdn.literacytrust.org.uk/media/documents/Fake_news_and_critical_literacy_-_final_report.pdf

Echo Chambers

When a group of people with similar opinions interact only with each other (often but not exclusively on social media), which prevents their exposure to alternative viewpoints and creates the impression that their view is more widely held than it is.

Filter Bubbles

When social media algorithms show users, content based on their previous interactions it can result in only information and opinions that reinforce their beliefs being shared.

Confirmation Bias

People are more likely to accept or notice information if it appears to support what they already believe or expect.

Topic 4: Fact-Checking and Tips for Spotting Fake News

Slides 15-18

Suggested time spent on this topic: 15 minutes

Fact Checking (Slide 15)



Core activity:

This content can be delivered in a variety of ways:

- 1 – Use the optional PowerPoints provided, which lists some of the main fact checking organisations & their evolution / work with social media platforms
- 2 – Update the PowerPoints to include fact checking organisations from your country / region or to make a more up to date list of fact checking organisations (see advice in the manual for how to do this)
- 3 – Facilitate a *brief* discussion asking the participants which fact checking organisations they are aware of, and what fact-checking activity if any they are aware of on the social media platforms they use, facilitating the discussion so that all of the key information below is covered.



KEY POINTS:

- International Fact Checking Network has a voluntary code of principles including fairness and non-partisanship, transparency and an open and honest corrections policy – as of February 2022, there were 114 verified active signatories to the code;
- Information generally verified on a sliding scale e.g., True, mostly true, mixture of true and false, mostly false, false (with a separate flag for satire / parody);
- Social media platforms such as Facebook, Instagram and TikTok & Twitter work with fact checking organisations to evaluate and flag or remove false information;
- Some false content exempt, e.g., opinion (unless it violates community standards e.g., a risk of violence) and false content posted by politicians;
- Fact checking constantly evolving in response to current events;
- Very few sanctions for social media companies who fail to remove false or other harmful content.

Additional Trainer Notes – Fact Checking Organisations

In 2006, Facebook (and Instagram) started working with third-party fact-checking organisations and individuals in various countries to fact check the content uploaded by users. Fact-checkers must be certified by the International Fact-Checking Network (IFCN). They can mark content as “true”, “partly true”, “false”, “partly false”, “false title”, “not applicable for evaluation”, “satire”, “hoax”, “opinion” and “not evaluated”.

In 2019 Facebook started allowing fact-checkers to check ads and flag them as false. US fact-checkers were permitted to remove paid ads they thought were false. However, content posted by politicians is exempt from this on the grounds that, according to Mark Zuckerberg, “in a democracy it is important that people can see for themselves what politicians are saying” (Reardon, 2019).

Zuckerberg appeared before the US House Financial Services Committee in October 2019. Opinions about the decision not to fact-check political content were split along party lines, with Republicans being largely in favour, seeing it as avoiding political censorship, and Democrats critical because Zuckerberg admitted hate speech and disinformation posted by political candidates was unlikely to be flagged.

One Netherlands-based fact-checking organisation ended its partnership with Facebook because of their position on not vetting political content. Other organisations, including Lead Stories, have lobbied Facebook to change its policy.

In December 2019 started to use part-time community reviewers to flag content to the fact-checking organisations to speed up the fact-checking process.

Consequences for social media platforms failing to tackle false information and other harmful content have to date been limited:

The German Network Enforcement Act (2018) obliges social media companies to:

Provide accessible procedure for reporting criminally punishable content;

Take down or block access to unlawful content promptly;

Inform complainants of decisions with reasons;

Submit reports on their handling of complaints about criminally punishable content (Facebook fined €2.3million for underreporting in 2019);

2020 – UK watchdog Ofcom announced it would fine and / suspend social media platforms which fail to deal with harmful content;

USA-based platforms protected by Section 230 Communications Decency Act which mitigates their responsibility for content uploaded by their users.

Sources and further reading:

Home Affairs Select Committee. (2017) *Home Affairs Committee Hate Crime: Abuse, Hate and Extremism Online*.

<https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf>

Meta Journalism Project. (2021, June 1). How Facebook's Third-Party Fact-Checking Program Works. *Facebook*.

<https://www.facebook.com/journalismproject/programs/third-party-fact-checking/how-it-works>

Reardon, M. (2019, October 23). Facebook's Zuckerberg Gets Grilled Over Political Ad Policy. *CNET*. <https://www.cnet.com/news/politics/facebooks-zuckerberg-gets-grilled-over-political-ad-policy/>

Schneider, O., & Sabourian, C. (2018). Policing the internet – 'fake news' and social media offence update. *Kingsley Napley*.

<https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/policing-the-internet-fake-news-and-social-media-offence-update>

Smith, A. (2020, November 6). What is Section 230 and Why Does Trump Want It Revoked? *The Independent*. <https://www.independent.co.uk/life-style/gadgets-and-tech/features/trump-section-230-twitter-us-government-b1644936.html>

Tardaguila, C. (2019, December 17). *Starting Today, Facebook Will Have A Team of Community Reviewers Working in the U.S.* Poynter. <https://www.poynter.org/fact-checking/2019/starting-today-facebook-will-have-a-team-of-community-reviewers-working-in-the-u-s/>

Some English and French Language Fact-Checking Organisations

Ferret Fact Service <https://theferret.scot/fact-check/>

Full Fact <https://fullfact.org/>

International Fact Checking Network <https://www.poynter.org/ifcn/>

MediaWise Teen Fact-Checking Network <https://www.poynter.org/teen-fact-checking-network/>

Snopes <https://www.snopes.com/>

Politifact <https://www.politifact.com/>

Tips for Verifying Online Information (10 minutes, Slides 16-18)



Core activity:

Present tips for verifying information online to the group.

The two preferred options for delivering this content are:

- Using the optional PowerPoint slides
- Have the group come up with their own tips, recording them on a whiteboard / flip chart, ensuring that as you facilitate and debrief this activity, all the key points mentioned below are included.



KEY POINTS:

Consider credibility of author / platform

- Check URL to ensure it's not mimicking a reputable news site (e.g., www.bbc.c0m instead of www.bbc.com);
- Check 'About' & 'Contacts' information for any website for information about who works there & how organisation is funded – be suspicious if this information is missing;
- Search name of author / journalist to find out what else they've written;
- Check the social media profile of whoever posted the information and evaluate their possible motives for sharing it – are they a real person or a bot? What sort of information have they shared before? Whom do they follow / who follows them? (Make sure you have familiarised yourself with the information in the trainers' manual about how to spot a bot).

Look beyond the headline

- Is the headline consistent with the story?
- Do dates and timelines make sense?
- Are there spelling and grammar mistakes or is the style sensationalised?
- Is the story trying to stir up negative emotions or promote conspiracies?
- Is the story meant to be a joke, parody or satire?

Do your own research

- Does the story have credible supporting sources?
- Is the story being reported by other, trusted websites?
- Do the images in the story show what they say they show? (Reverse image search)
- Is the story being shared by a bot or troll factory?



Training Tip:

You may wish to demonstrate some of the tips, such as reverse image search or how to spot a bot, processes with which you can familiarise yourself in advance by following the instructions contained in the additional trainer notes below. Don't forget to adjust your timings.



Timesaver Tip:

If you have limited time, you may choose to skip the above activities and provide printed copies of the tips (available in the resource pack) to the participants, which they can then use for reference during the verification activities.

Additional Trainer Notes – Tips for Verifying Online Information

Reverse Image Search – Google

Right click on image and select 'Search Google for image'.

Google will find and show you visually similar images as well as webpages that use this image, enabling you to click through and find out in what context and on what dates the image has been used previously.

At the top of the results Google will also indicate what it thinks is the original version of the image, which can help with establishing its date. This is not fool proof though. In this case, it is necessary to click through the visually similar images to find the original.

At the top of the results Google will also indicate what it thinks is the original version of the image, which can help with establishing its date. This is not fool proof though. In this case, it is necessary to click through the visually similar images to find the original.

An alternative method of conducting a reverse image search is to go to www.tineye.com. Tineye works similarly to a reverse search using Google but allows you to upload or paste an image into the search field and may be more convenient if screenshotting or saving an image to a smartphone, for example.

Verifying videos

Has the information in the video been reported elsewhere by a reliable media source?

Is anything in the video obviously doctored?

Is there any basic information missing (such as date / location, names of individuals)?

Does it use demeaning, insulting or inflammatory language?

Are the details consistently reported with each share (e.g., location, date, context)?

Screenshot then reverse image search

Type a brief summary of the content of the video into a search engine to see if it's been reported elsewhere (e.g., girl gets hit by a car while doing 'My Feelings' challenge)

Verifying social media posts

Consider who is posting the information and what their agenda might be.

Is it a real person or a bot?

Whom do they follow? Who follows them?

What else have they posted in the past?

Is anyone in the replies refuting the information? (Not fool proof! Don't forget about echo chambers!)

Do a reverse image search to see if any images have been published before and in what context.

How to spot a bot

Has the account posted an unusually high number of times or to an unnaturally regular schedule?

Has the account posted identical content to a number of other accounts? (potential Botnet)

Is the user profile missing information or following a pattern similar to other bots?

Does the account follow a similar naming pattern to other accounts posting similar content?

'Botometer' and other similar tools can evaluate social media accounts for you

Botometer is an online resource from Indiana University Network Science Institute for assessing the likelihood that a Twitter account is a bot. Enter the handle of any Twitter account to see how this works. Once the Botometer has given its rating, you can click on the account name for further information about how the rating was calculated and on the 'details' tab for more information about the account and how often it tweets.

<https://botometer.osome.iu.edu/>

Further reading:

Knight, W. (2018, July 18). How to Tell If You're Talking to A Bot. *MIT Technology Review*. <https://www.technologyreview.com/2018/07/18/141414/how-to-tell-if-youre-talking-to-a-bot/>



Topic 5: Practical Exercises – Verifying Online Information

Slide 19-22

Suggested time spent on this topic: 40 minutes

Verifying Online Information – Exercises (Slides 19-22)



Core activity:

Practical exercises evaluating online information.

This activity is an opportunity for participants to practice verifying some examples of online information. It is recommended that a minimum of 3 examples be provided – 1 online news article, 1 social media post and 1 video, if possible. Additional examples can be included if time allows.

Options available for delivering this content include:

- Using the PowerPoint slides and examples provided in this training manual
- Update the PowerPoint slides, choosing up to date examples relevant to your own / the participants' context/country/region. Advice to help you select relevant examples is available in [Chapter 2](#) of this training manual
- Providing printed out examples for discussion [some examples are provided in the training manual to assist you or you can choose your own following the advice in [Chapter 2](#)] – and provide instructions to the participants on how to get online (e.g., using their own devices or devices in a computer room if available in your training venue) to assess the information

Selected examples should ideally cover various options from a range from true, mostly true, mixture, mostly false and false. If you have time, you could also include examples that are satire / parody, unproven, outdated, miscaptioned, correction attribution, misattributed, scam, legend, or whatever categories are used by your choice of fact-checking organisation. It is also advised that examples should be balanced overall, for example do not have all your 'false' examples from one political perspective.

You could work through these examples as a group, asking participants to give you suggestions about how to verify each example. If you have access to the internet and a projector, you could follow the groups' instructions and walk the whole group through each example.

Alternatively, you could split the participants into pairs or small groups, giving them time to verify an example on their own, then have each group come back to report their findings to the plenary group.

This is a particularly useful method if you do not have access to a PowerPoint projector to enable the participants to watch you walk through an example online. Participants can either use their own devices to evaluate information, if internet access / Wi-Fi is available, or can simply discuss and record the actions they would take to evaluate the information, which can then be discussed and debriefed with the main group. It is recommended you allow 10-15 minutes for the groups to research their question, and a further 5-10 minutes for each example to be reported and discussed in the plenary group. Therefore, if you had four examples assigned to four different groups, this would take approximately 25-55 minutes (10-15 minutes while all groups conduct their research, 20-40 minutes debriefing each example in turn). If you assign the same example to more than one group, then the debrief time can be reduced, but generally we recommend being generous with the estimated timings for this activity.

Additional Trainer Notes: Verifying Online Information – Activities



Training Tip:

In many cases, when researching these examples, participants will come across relevant articles on fact-checking websites. Checking to see what conclusion professional fact-checkers came to about the same information is a valid and efficient option when assessing online information. However, for the purposes of these activities and the participants' learning experience, we recommend that you require them to identify at least one source to support their conclusions that is not from a professional fact-checking organisation.

Girl holding koala – social media post

Aoki, S. [@steveaoki]. (2020, January 4). *My Heart Breaks For #Australia. A Few Ways You Can Help.* 💔 💔 🐼 🐼. [images attached]. *Twitter.*

<https://twitter.com/steveaoki/status/1213589859152973826>

Options for evaluating this photograph, and which you should explore together as a group or encourage the participants to explore if they are working in small groups, include:

Conducting a [reverse image search](#) (see advice on pages 39-40 of this manual);

Conducting a text search e.g., 'koala girl bushfire' or whichever combination of words the participants choose;

Conducting a text search using a social media platform's own search function.

These activities should result in a range of sources being located including or similar to the following articles:

Capron, A. (2020, January 7). Koala Et Kangourous Sauvés, Fausse Photo Satellite...: Cinq Fausses Images Sur Les Feux En Australie. *Les Observateurs*.

<https://observers.france24.com/fr/20200106-intox-feux-australie-images-photos-videos-fake-incendies-koala-kangourou>

Greenfield, B. (2020, January 7). Girl in A Gas Mask, Holding A Koala: The Truth Behind That Viral Australian Bush Fires Photo. *Yahoo! Life*.

<https://twitter.com/yahoolife/status/1215947758663880705>

Wilson, C. (2020, January 14). False and Misleading Information Is Spreading Online About the Aussie Bushfires. Here's What's Real and What's Not. *Buzzfeed News*. <https://www.buzzfeed.com/cameronwilson/unverified-false-information-list-australian-bushfires?bfsource=relatedmanual>

Review of the located resources should lead the participants to discover that this is a photo-shopped image created by Thu Pham-Moore and originally posted on her Instagram account (@thuie) (The post has since been deleted). She wanted to make a point about people being concerned with trivial things while the bushfires were ongoing and included a disclaimer making it clear the image was photoshopped.

When manipulated images are posted with a disclaimer, the disclaimer can be 'lost' as the images is repeatedly shared on social media. Bearing this in mind, possible ratings the participants could decide upon in relation to this image include 'false', 'misattributed', 'out of context'.

My Feelings/Keke Challenge - YouTube video

Noob Destroyer. (2018, July 31). Girl Hit by Car Doing 'In My Feelings' Challenge. *YouTube*. <https://www.youtube.com/watch?v=SDfIKttkcEA>

This YouTube video shows a young woman standing in the road by her open car door, singing and dancing, before apparently being struck by a car. **Participants should be given the opportunity to withdraw from this activity.** You could either play the video to the group, using a projector, or send the link by email to participants for use in small group discussions. The 'My Feelings' challenge was a popular internet challenge where people get out of their cars to stand in the road and dance to the Drake song 'My Feelings.'

Options for evaluating this video, which you should either work through with the group or encourage them to explore in small groups, include:

Checking to see if the information has been published elsewhere (e.g., searching online for any newspaper articles about a woman being struck by a car while doing the 'My Feelings' challenge);

Identifying that the video is missing basic information such as the name of the woman and the date / location of the incident;

Internet search e.g., typing “did a girl get hit by a car doing the in my feelings challenge?”

The [advice for verifying online videos](#) on page 40 of this manual.

Search results may include the below video (1min 40 secs) from KHOU-TV and this article from fact-checking organisation Snopes, both of which confirm that the video is fake.

Evon, D. (2018, July 23). Is This ‘Keke Challenge Gone Wrong?’ Video Real? *Snopes*. <https://www.snopes.com/fact-check/keke-challenge-gone-wrong/>

KHOU 11. (2018, July 26). Verify: Woman Hit by Car During ‘Keke’ Challenge? *YouTube*.

https://www.youtube.com/watch?v=gSAz2g-0_w

In summary, this video is a confirmed fake, that was created and shared on Instagram by @lofi3d (<https://www.instagram.com/lofi3d/>) including a disclaimer that the video had been edited, but it was subsequently re-shared with this caveat removed, similarly to the way in which the Koala bushfire manipulated photograph was shared, without its original disclaimer.

Cookie Monster Rock – ‘Trust My Science’ online news article

Brosseau, F. (2021, January 28). Un Collectionneur De Minéraux Découvre « Macaron Le Glouton » En Ouvrant Une Agate. *Trust My Science*.

<https://trustmyscience.com/collectionneur-mineraux-decouvre-cookie-monster-dans-agate/>

English language alternative from Nerdist.

Hart, M. (2021, January 26). Gemologist Cracks Open Rock, Finds Cookie Monster’s Face. *Nerdist*. <https://nerdist.com/article/cookie-monster-rock-discovery-gemologist/>

These articles are from an online website and claim that a gemologist discovered a rock that when split in half resembled the face of the Cookie Monster from the children’s television show Sesame Street. The links to the articles are above and one or both can be shared with the participants.

Options for evaluating this article include:

Check to see if the webpage has an ‘About Us’ section and contact information;

Does the article have an author cited?

Conducting an internet search to see if anyone else has reported on this issue;

Are reports consistent with details e.g., dates / location?

Reverse image search (although we recommend in order to enhance the participants' learning experience that this activity focuses on verifying the online news site and story).

Having reviewed the above the participants will discover that the website has an 'About' section and a 'Contact' section, albeit the contact section provides email addresses only. The article has an author cited and although there are several similarly named journalists, it is possible to find information about this writer's previous publication and employment history. An internet search for 'Cookie Monster rock' indicates multiple news outlets have covered the same subject, including some well-known, reputable organisations such as NBC. The story has also been verified as true by fact-checking organisations including Snopes.

Evon, D. (2021, January 26). Is the Cookie Monster Rock Real? *Snopes*.

<https://www.snopes.com/fact-check/cookie-monster-rock/>

Ignacio, L. (2021, January 28). Cookie Monster Rock Found in Brazil Goes Viral. *NBC*.

<https://www.nbcnews.com/news/world/cookie-monster-look-alike-rock-found-brazil-goes-viral-n1255908>

German quarantine breaks to be held in refugee camps – New York Post online news article

Brown, L. (2021, January 18). German quarantine breakers to be held in refugee camps. *New York Post*.

<https://nypost.com/2021/01/18/german-quarantine-breakers-to-be-held-in-refugee-camps/>

This is another online article example and steps participants will need to take will be similar to the Cookie Monster Rock example, so we suggest assigning these two examples to different groups to avoid repetition.

Once those steps have been taken, the participants will have the following information (accurate as of April 2022):

The website has an '[About New York Post](#)' section including its senior leadership, owner (News Corp) and history, claiming that it was founded in 1801 by Alexander Hamilton. It also has a [webpage listing all of its current columnists](#). Further online research reveals that it is a conservative-leaning print and online tabloid newspaper;

The article has an author cited, and a brief online search reveals they have also written for several other tabloid newspapers in various countries;

The story references previous newspaper articles published in The Telegraph (UK) (very similar in substance to the NY Post article) and Germany's Welt am Sonntag newspaper, and a search reveals many other versions of this story published around the world. The Welt am Sonntag

This example is a particularly challenging one about which to draw conclusions, but the key point here to tease out in the debrief is that a longer and more complex story of which most examples are behind paywalls has been picked up by other outlets and stripped down, so that only the more sensationalised aspects of the report are included. For this reason, the fact checking organisation Snopes concluded that this story (the original version of it published in *Welt am Sonntag*) is a mixture of true and false, but it could equally be categorised as misleading. Similarly, an online article published on the FranceInfo website, concludes that while arrangements were made for some repeat quarantine breakers to be confined in hospitals and converted refugee camps, in some German provinces, this did not apply to all COVID-19 patients as had been rumoured on social media (FranceInfo, 2021). This is an important example to include in the training, as there will not always be a clear-cut answer as in the previous examples, so it is helpful for participants to experience evaluating information where the final categorisation is not straightforward.

Sources:

Kasprak, A. (2021, January 26). Is Germany Planning to Put Quarantine Violators in Detention Centers and Refugee Camps?' *Snopes*. <https://www.snopes.com/fact-check/germany-covid-camps/>

Luyken, J. (2021, January 17). Germans Who Keep Refusing to Quarantine Could Be Put in Detention Centres Under New COVID Rules. *The Telegraph*. <https://www.telegraph.co.uk/news/2021/01/17/germans-keep-refusing-quarantine-could-put-detention-centres/>

Naber, V.I., Lutz, M. & Büscher, W. (2021, January 17). Länder planen Zwangseinweisungen für Corona-Quarantänebrecher. *Welt am Sonntag*. <https://www.snopes.com/fact-check/germany-covid-camps/>

Step-by-Step Guide to Choosing Your Own False Information Examples

As discussed previously, you may wish to include some of your own examples of false information online, either for the verification activities or as examples in the different categories of false information. We have provided below a step-by-step guide to assist you in choosing your own examples, which should be read in conjunction with the advice on adapting and future-proofing your training in [Chapter 2](#).

Step 1: Decide on the type of example you are looking for e.g. clickbait / satire / propaganda.

In this case, we are going to search for an example of a social media post relating to the war in Ukraine that we would like our training participants to verify.

Step 2: Choose a fact-checking organisation:

Go to the website showing the Verified Signatories of the International Fact-Checking Network Code of Principles:

<https://ifcncodeofprinciples.poynter.org/signatories>

CTRL-F to search for your country (or another country that speaks the same language – to broaden out the potential pool of examples). On the date of search, we find some French language organisations signed up to the code including [France 24 – Les Observateurs](#) and [FranceInfo](#). We also selected the English language fact checking organisation, [Full Fact](#).

Step 3: Search for an example:

Using the search function on each organisation's webpage to search for 'Ukraine', locating a number of potential examples including:

- This story from *Les Observateurs* explaining how they verified a video, widely shared on Twitter and purporting to be from the BBC, which claimed that Poland was planning to send troops to Ukraine, confirming it to be false: Dejaifve, A. (2022, May 9). Un Faux Reportage Attribué À La BBC Affirme Que La Pologne s'apprête à attaquer L'Ukraine. *Les Observateurs*.

<https://observers.france24.com/fr/europe/20220509-un-faux-reportage-attribu%C3%A9-%C3%A0-la-bbc-affirme-que-la-pologne-s-appr%C3%AAtte-%C3%A0-attaquer-l-ukraine>

- This article from *FranceInfo*, explaining how it ascertained a number of photos and videos relating to the war in Ukraine and circulating on social media to be either fake or taken out of context, including an explosion claimed to be the bombing of a Ukrainian power plant, but which was actually an industrial accident

in China in 2015, and how an image of Ukrainian president Volodymyr Zelenskyy holding up a Ukrainian national football shirt embossed with his name and a swastika was proven to be manipulated:

Angrand-Benabdallah, P and Galopin, A. (2022, March 25). Guerre En Ukraine: 20 Photos Et Vidéos Détournées Qui Ont Circulé Depuis Le Début Du Conflit. *FranceInfo*. https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/vrai-ou-fake-guerre-en-ukraine-20-photos-et-videos-detournees-qui-ont-circule-depuis-le-debut-du-conflit_5004650.html

o This article from *Full Fact* confirming that a black and white photograph of a crowded train platform, shared on social media and claimed to have been taken in Ukraine, in March 2022 is genuine, despite it having been flagged by some Facebook users as potentially false:

O’Leary, Joseph. (2022, March 15). Photograph of Crowded Railway Station Is from Ukraine in March 2022. *Full Fact*. <https://fullfact.org/online/ukraine-crowded-railway-station-black-and-white/>

Step 4: Create your example

All the examples include references / links to sources and explanations of how the information was verified. Use these to create activities / examples similar to the ones already included in the training, using the sources as appropriate (e.g. image search, checking the ‘about’ page of a website etc) to guide the training participants to work through the verification process themselves and come to their own determinations about the veracity of the claims.

Topic 6: In the Workplace – Empowering Young People

Slides 23-28

Suggested time spent on this topic: 40 minutes

Reflection Question 4 (Slide 23)



Core activity:

Facilitate a brief discussion with the group in relation to the below question. This activity is designed to be an introduction to the scenario discussions following.

Can you think of a time when the young people you work with were influenced by news or other information online that you knew or suspected was not true? Did you address this with them? If yes, how? If no, why not? (If you cannot think of an example specifically relating to the young people you work with, consider this question more broadly, in relation to family members, friends and people you engage with online.)

Discussion Scenarios (Slides 24-26)



Core activity:

During this section, the participants will discuss a range of scenarios involving young people and potentially false information online that they could encounter in the workplace. Examples are provided in the training manual, but you may wish to create your own scenarios relevant to your participants' specific roles working with young people, and national / cultural context.

Option 1 for delivering this content, is to display each scenario, either on a PowerPoint slide, or provided as a printout to participants, and facilitate a group discussion on how it might best be dealt with, recording responses on a whiteboard / flip chart as appropriate.

Option 2 is to divide the participants into pairs or small groups and assign them one scenario to discuss among themselves, and then come back to present their thoughts to the group. If you choose this option, it is recommended that you visit each group in turn during their discussions to make sure they are progressing along the appropriate path of supporting critical literacy for the young person.



KEY POINTS

Whichever option you choose, the key learning points that you need to facilitate are:

- Practical application of methods to evaluate online information
- The transfer of skills into the workplace – how will participants use their newly gained skills to support the young people they work with to develop their own critical literacy and resilience to false information online?
- To learn from one another – by sharing their thoughts participants will be able to gain ideas and inspiration from their peers.

Scenario 1:

Beth, a young person you work with, asks for your advice about a post on social media she has seen that says she can protect herself from catching COVID-19 by smoking cannabis.

How would you go about supporting Beth to evaluate critically this information?

Scenario 2:

Mo comes to you very angry and upset because he has seen a video online that appears to show soldiers committing atrocities in his country of origin.

How would you go about supporting Mo to verify whether the video he has seen is genuine?

Scenario 3:

During a safe space session, Jazz discloses the following:

“A friend has sent me a video through WhatsApp. It was TV news announcing that China had disseminated COVID-19 around the world deliberately in order to weaken the USA. In addition, it said that the Chinese government had been fined several million dollars after the American trial.”

How will you respond to Jazz’s comment?



Training Tip:

It is important that these scenario exercises are differentiated from the previous activities on verifying online information. There will be some overlap, in terms of identifying actions that can be taken to evaluate information, but an essential element of these scenarios is to consider them in the context of working with young people. The answers will depend on whether the participants are teachers, youth workers or in some other role, where they engage with other young people, for example in the classroom, a youth club or elsewhere, and what facilities are available (e.g., could they sit down at a computer with internet or not?) There are no right or wrong answers, but participants should be encouraged to think explicitly about how they will use their newfound knowledge in the workplace, and to share their ideas with their peers for the benefit of all.

Topic 7: Summary and Close

Slides 27-30

Suggested time spent on this topic: 10 minutes

Presentation of Resource Pack (Slide 27)

Presentation of Resource Pack (5 minutes)

This training comes with a resource pack for participants, designed to support them in transferring the knowledge and skills they have gained from completing this training course into the workplace, to help support the young people they work with to develop their own online critical literacy. At the end of the training session, you should distribute the resource pack to participants, briefly present it and explain its purpose and how to use it.



Training Tip:

We recommend that you do not distribute the resource pack to participants until you reach the end of the training as the supporting notes and further reading include the answers to some of the suggested activities.



Core activity:

Distribute the resource packs and briefly explain how the participants can use these packs in their workplaces to help them support and empower young people. See the additional trainer notes for more advice on how to use the resource packs.

Additional Trainer Notes – Resource Pack

This training course is based on the principle that the content of the training for professionals working with young people - youth workers and teachers - should be as similar as possible to that which would be delivered directly to the young people themselves. The specific examples used or time devoted to each category may differ, as well as the balance between theory and practical, depending on the age group of the young people. However, the base content will be similar, introducing the different types of false information to young people and practicing the skills needed to make an informed assessment as to the veracity of information they may encounter online.

The resource pack consists of:

the presentation slides and accompanying notes, to provide professionals with the information and further reading resources they need to help them consider how they will transfer their knowledge to the professional context to support the young people they train;

Suggestions as to how the professionals can adapt the base content included in this training course to meet the needs of their specific professional context, including advice on how to select examples of false information to discuss with young people;

Handouts covering the 3 main tips for spotting false information.

In addition to the resources contained in the pack, you may also wish to advise participants that a PowerPoint based training package on cyberawareness designed for young people is available in the 'Toolbox' section of the Orpheus website. It covers many of the same topics included in this training package, but adapted to meet the needs of a younger audience. This can serve as a source of inspiration for professionals when working with young people or may, if desired, be delivered directly to the young people they work with.

<https://orpheusproject.eu/toolbox/>

Participants should use the resource pack as a source of reference and inspiration for transferring their knowledge into the workplace to support and empower the young people they work with to develop their online literacy and cybercrime awareness.

A key consideration when thinking about supporting young people to develop their online critical literacy is the constantly changing parameters. For example, not only is news, and therefore 'fake news' and other forms of online disinformation, constantly changing, so are the social media platforms used by young people to share and disseminate information. This means that many of the examples given

in this training may already be out of date, or superseded by topics more interesting and relevant to young people. The objective is to empower young people to make their own informed assessments of the information they encounter online and, therefore, participants will need to adapt their knowledge to suit the specific context within which they work, for example which age group of young people they work with, and whether they are a teacher or a youth worker or a different profession.

We recommend that participants review the slides and training notes provided in the resource pack. The resource pack also suggests some ways in which they can adapt this information for their own use in the workplace.

We also strongly recommend that participants review the ORPHEUS Project training on Dealing with Controversial Issues, as this will provide them with the tools they need to manage any difficult conversations that may arise when addressing these topics with young people.

Further resources

English Language Resources

The National Literacy Trust is an independent charity providing literacy skills to disadvantaged children. It has a comprehensive collection of Fake News and Critical Literacy Resources aimed at teachers, parents and pupils at both Primary and Secondary school level:

National Literacy Trust. (n.d.) *Helping Your Child Understand the News.*

<https://literacytrust.org.uk/family-zone/9-12/newswise-home/>

National Literacy Trust. (2018). *Fake news and critical literacy: The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools.*

https://cdn.literacytrust.org.uk/media/documents/Fake_news_and_critical_literacy_-_final_report.pdf

The British Council has provided a resource to support teachers in using fake news critically in the classroom:

Wilding, A. (2020, March 10). How to Use Fake News Critically in The Classroom.

British Council. <https://www.britishcouncil.org/voices-magazine/use-fake-news-classroom-critically>

The BBC has collated a number of its resources designed to help young people identify fake news and false information, as well as exploring the social, political and economic impact of news reporting and developing critical literacy skills across different types of media:

BBC. *Help Your Students Spot False News*. (n.d.)

<https://www.bbc.co.uk/programmes/articles/4fRwvHcfr5hYMMItFqvP6qF/help-your-students-spot-false-news>

The BBC collection includes *iReporter* - an online game for young people that puts them in the role of a reporter having to evaluate news stories for broadcast, scored on balance, accuracy and speed. BBC. (n.d.) *iReporter*.

<https://www.bbc.co.uk/news/resources/idt-8760dd58-84f9-4c98-ade2-590562670096>

Review Learning Outcomes (Slide 28)



Core activity:

Return to the list of seven learning outcomes and briefly summarise in a few sentences how the training has met each learning outcome, ticking them off or adding emojis (smile, heart, star, etc.), getting agreement from the group to confirm each learning outcome has been met. *

1. Explain the meaning of the following terms: Misinformation, Disinformation, Fake News
2. Identify common categories of false information
3. Explain how and why false information spreads
4. Explain the harm caused by false information online
5. Identify the major fact checking organisations and explain their benefits
6. Identify, explain and apply the online critical literacy skills needed to evaluate information
7. Transfer the knowledge and skills gained during this training into the workplace to support young people to develop their own online critical literacy skills

*If one of the learning outcomes has not been met for some reason, make a note of it and commit to following it up with the participants at a later date e.g., by sending a clarification email.



Core activity:

Return to the whiteboard / flip chart record of personal objectives participants had for the training session. Have these personal objectives been met? If so, acknowledge this by ticking them off, or adding emojis. If not, from the knowledge and expertise you have gained while preparing to deliver this training, are you able to suggest where the participant could find out what they wanted to know? Is there anything you can look up and email to the participants later, for example by referring to the additional trainer notes in this manual, or by visiting our online platform.

Once the learning outcomes and personal objectives have been debriefed, and any outstanding questions have been answered, you may close the session.



Large

If you have more time, you can introduce the participants to either or both of the optional complementary modules on Cyberawareness and Online Safety Training.

Optional Module A covers awareness of and resilience against cybercrime and Optional Module B covers cyberharassment (including cyberbullying and cybersexism). These modules would be particularly useful for a group that had limited experience of using the internet and are suitable to be delivered either in advance of, or after, the Critical Literacy training. Optional Mini-Module C contains legislation and enforcement information to enable you to provide this background information to the participants should you judge it appropriate for their role working with young people.

Optional Module A: Cybercrime Awareness and Online Safety

This module on **Cybercrime Awareness and Online Safety** is designed to take approximately 1 hour to deliver in full.

Aim:

- To provide professionals with the knowledge, skills and confidence
- to support and empower young people to build their resilience to cybercrime and to take responsibility for their online safety.

Learning Outcomes:

- To understand the different types of cybercrime young people might encounter online and what the impact on them might be.
- To gain the skills, confidence and knowledge to be able to support young people to identify and protect themselves from cybercrime.
- To empower young people to use the internet safely.

Participants:

The optimal number of participants for this training is 6-12.

If you wish to run a smaller group, you may need to adapt some of the group work activities so that they can be done without having to split the group up.

If you wish to run a larger group, you may need to adapt some of the activities, particularly those that involve group work and reporting back findings, to ensure there is sufficient time for everyone to contribute.

Pre-Requisites:

Participants should have completed the critical literacy and online awareness module, including the pre-training questionnaire.

Slides and trainer notes are available to support delivery of this module. However, it is also possible to deliver this training using whiteboard/flip charts and printed handouts as an alternative, if PowerPoint slides are not convenient to use.

This module is divided into 4 topics and takes approximately 1.5 hours to complete, if all core and optional activities are included. Timings may vary depending on how many participants there are and how they respond to each individual activity. It is advisable to be prepared to amend the number of optional activities undertaken depending on how much time it takes each group to progress through the activities.

	Topic	Suggested Timing	Slides
1	Introduction, aims and learning outcomes	10 minutes	1-2
2	Cybercrime: Definitions & Impact	10 minutes	3-6
3	The Do's and Don'ts of Staying Safe Online	30 minutes	7-16
4	Scenarios	30 minutes	17-23
5	Summary and Close	10 minutes	24-25

Topic 1 – Introduction, Aims and Learning Outcomes

Aims and Objectives (Slides 1-2)

What this training covers:

Learning Objectives:

- To understand the different types of cybercrime young people might encounter online and what the impact on them might be;
- To understand how young people can protect themselves from cybercrime.

Learning Outcomes:

- To be able to support young people to identify and protect themselves from cybercrime
- To empower young people to use the internet safely



Core activity:

Present the aims and objectives on the slide (suggested time 2-3 minutes)



Suggested activity:

Prior to presenting the aims and objectives, ask the training participants what they would hope to learn from the training session and record on the whiteboard. Should their answers not be included within the scope of the training, take the opportunity to manage their expectations. You may wish to return to this list and review when wrapping up the training (this activity can be done before the core activity).

Topic 2– Cybercrime: Definitions and Impact

What is Cybercrime?

Slides 3-4 (10 minutes)



Core activity: (suggested time 3-5 mins)

Present the definition on the slide. The slide has an animation, meaning that initially only the headline answers will be visible so you may wish to invite the participants to suggest examples for each bullet point, before clicking to reveal the answers.



Suggested activity: (5-10 mins)

Prior to presenting the definitions on the slide, ask the group participants to try to define the meaning of cybercrime themselves and record their answers on a flip chart, whiteboard or via electronic means if you are delivering this training online (e.g., chat box or online whiteboard). It is likely you will get a mix of answers including examples of specific cybercrimes (phishing, online fraud, cyberbullying) and possibly some attempts to define the notion of cybercrime. All of these answers can be recorded before moving on to the core activity and presenting the definitions on the slide. You may wish to compare the answers given by the participants with the definition on the slide. We suggest delaying any in-depth discussion of specific types of cybercrime until Slide 5 'Types of Cybercrime'.



Suggested activity:

Ask the participants if they or anyone they know (in particular the young people they work with) has been a victim of cybercrime (advise them to only disclose if they feel comfortable in doing so). What was the nature of the cybercrime? What was the outcome? What was the impact on the victim?

Additional Trainer Notes – Cybercrime: Definitions

Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a borderless problem that can be classified in three broad definitions:

Crimes specific to the Internet, such as attacks against information systems or phishing (e.g., fake bank websites to solicit passwords enabling access to victims' bank accounts);

Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code;

Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Source:

European Union (Migration and Home Affairs. (n.d.) *Cybercrime*.

https://ec.europa.eu/home-affairs/cybercrime_en

cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and

cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Source:

HM Government. (2016) *National Cyber Security Strategy 2016-2021*.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Malware is simply a term for different types of malicious software that could have an adverse effect on an organisation or individual. Further information about different types of malware is available from:

National Cyber Security Centre. (n.d.). *NCSC Glossary*.

<https://www.ncsc.gov.uk/information/ncsc-glossary>

Hacking is a very common term that simply means gaining unauthorised access to computer system, personal account, computer network or digital device. This could be as simple as gaining access to someone else's online account using a stolen or guessed password. Another example would be the compromising of a business's computer network using malicious software to steal information.

National Cyber Security Centre. (2017, December 17). *Guidance on Recovering A Hacked Account from The National Cyber Security Centre.*

<https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

Identity theft / fraud – the criminal use of someone else's personal details to commit a crime. This can happen, for example, if you disclose personal information in response to a phishing / scam email, or if details that you have provided to a business have been stolen.

“Identity theft is a method used to carry out criminal activity, involving unauthorised use of your name and personal details to either steal from you, or commit a crime in your name. Identity theft can be carried out either online, physically using printed documents, or by a combination of the two.”

Source:

Get Safe Online. (n.d.). *Preventing Identity Theft.*

<https://www.getsafeonline.org/protecting-yourself/safeguarding-identity/>

Phishing / Spear-Phishing – phishing is a play on the word ‘fishing’ and it refers to attempts by cybercriminals to ‘hook’ in victims – for example by sending scam emails encouraging recipients to click on a link which would upload malicious software their computer, or direct them to a fake website where their personal details and passwords could be harvested. ‘Phishing’ emails & texts can be sent in bulk to large numbers of recipients, meaning only a few people need to be tricked into clicking on the link or otherwise disclosing their information to make it worthwhile for the cybercriminal. Phishing can also be carried out via social media for example via posts that include links that lead to counterfeit websites.

‘Spear-phishing’ is a form of phishing where a cybercriminal's actions are directed towards a specific person and made to appear as if it comes from a trusted source.

Sources and further reading:

National Cyber Security Centre. (2021, November 26). *Phishing: Spot and Report Scam Emails, Texts, Websites and Calls.*

<https://www.ncsc.gov.uk/collection/phishing-scams>

Kaspersky. (n.d.) *What is Spear Phishing?* <https://www.kaspersky.com/resource-center/definitions/spear-phishing>

Get Safe Online. (n.d.) *Social Media Phishing.*

<https://www.getsafeonline.org/protecting-your-computer/social-media-phishing/>

Romance fraud

When a cybercriminal uses a fake profile to form a romantic relationship with a victim online with the intent of gaining the victim's trust and asking for money or enough personal information to steal their identity:

Source: Action Fraud. (n.d.) *Romance Fraud*. <https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud>

IT Service Fraud

This can take a number of forms including:

Telephone calls posing as legitimate IT companies such as Microsoft or Apple, offering to fix your computer (and therefore requesting you to grant access to your computer remotely or pay money in some other way);

Unsolicited emails including attached 'security updates';

Asking for payment to validate your software.

Source:

Action Fraud. (n.d.) *Remote Access Tool Scams*.
<https://www.actionfraud.police.uk/a-z-of-fraud/computer-software-service-frauds>

Extortion and Ransomware

Extortion can range from being a victim of ransomware, where malicious software is activated on your device with the threat to delete all your files unless you pay a sum of money to release them, to having been persuaded to engage in sexual acts online which are recorded via webcam and used to coerce the victim to either pay money or engage in further sexual acts (sextortion).

Ransomware threats can include messages alleging activity such as the viewing of porn on the part of the victim, to try and make it more difficult for the victim to seek help or put pressure on them to pay the ransom, for fear of exposure

Sources:

National Cyber Security Centre. (n.d.) *A Guide to Ransomware*.
<https://www.ncsc.gov.uk/ransomware/home>

National Crime Agency. (n.d.) *Sextortion (Webcam Blackmail)*.
<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>

DDoS – Distributed Denial of Service Attacks

When legitimate users are prevented from accessing computer services due to the site having been overloaded with requests from multiple computers or locations – usually used against businesses so won't be discussed during this training

Source:

National Cyber Security Centre. (2018, March 15). *Denial of Service Guidance*.
<https://www.ncsc.gov.uk/blog-post/denial-service-guidance>

Hate crime / Illegal content

When unlawful hate crime material is distributed online – for example content that stirs up hatred on the grounds of race, religion or sexual orientation, content that harasses or glorifies violence against individuals or groups based on protected characteristics. Other illegal content includes, for example, images of child sexual abuse.

Sources:

True Vision. (n.d.) *Internet Hate Crime*. https://www.report-it.org.uk/reporting_internet_hate_crime

Child Exploitation Online Protection Command. (n.d.) *Are You Worried About Online Sexual Abuse or The Way Someone Has Been Communicating with You Online?* https://www.ceop.police.uk/safety-centre/?_ga=2.222363292.609605449.1605696094-1834616103.1533735816

Internet Watch Foundation. (n.d.) *Hello & welcome to our reporting page*.
https://report.iwf.org.uk/en?_ga=2.188823852.609605449.1605696094-1834616103.1533735816



Suggested activity: (5-10 mins)

Prior to presenting the definitions on the slide, ask the group participants to try to define the meaning of cybercrime themselves and record their answers on a flip chart, whiteboard or via electronic means if you are delivering this training online (e.g., chat box or online whiteboard). It is likely you will get a mix of answers including examples of specific cybercrimes (phishing, online fraud, cyberbullying) and possibly some attempts to define the notion of cybercrime. All of these answers can be recorded before moving on to the core activity and presenting the definitions on the slide. You may wish to compare the answers given by the participants with the definition on the slide. We suggest delaying any in-depth discussion of specific types of cybercrime until Slide 5 'Types of Cybercrime'



Suggested activity:

Ask the participants if they or anyone they know (in particular the young people they work with) has been a victim of cybercrime (advise them to only disclose if they feel comfortable in doing so). What was the nature of the cybercrime? What was the outcome? What was the impact on the victim?

Impact on Young People (10 minutes, slide 5-6)

Slides 5-6:



Core activity: Present the statistics contained on both slides.



Suggested activity:

Briefly ask the participants whether they think these statistics are broadly accurate for the young people they work with. If no, why not?

Additional Trainer Notes – Impact on Young People

Slide 6 shows the results of a survey conducted in 2019 across all EU member states and the UK in relation to peoples' attitudes towards cybersecurity. The table shows the responses from 15–24-year-olds – across all the member states including the UK & individually for Belgium, France, the Netherlands and the UK – as to whether they had experienced particular types of cybercrime in the past 3 years.

As the group for their thoughts on these statistics? What do the results show are the sorts of cybercrime young people are most and least likely to have fallen victim to? Are these results surprising? Did participants expect them to be better or worse or about the same, or for the cybercrimes to be ranked differently? Anything that stands out to them in relation to the young people they work with?

Sources:

Cho, A., & Byrne J.P.Z. (2020) Digital Civic Engagement by Young People. *UNICEF Office of Global Insight and Policy*. https://www.unicef.org/sites/default/files/2020-07/Digital-civic-engagement-by-young-people-2020_4.pdf

European Commission (2020). *Special Eurobarometer 499 Report: Europeans' Attitudes Towards Cybersecurity*.
<https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2249>

OECD. (2017). *Use of Internet/Chat/Social Networks Before and After School*.
https://www.oecd-ilibrary.org/education/pisa-2015-results-volume-iii/use-of-internet-chat-social-networks-before-and-after-school_9789264273856-table206-en

Topic 3– The Do's and Don'ts of Staying Safe Online (30 minutes, Slides 7-15)

This section covers the 'do's and don'ts' for staying online in relation to each of the following categories:

- Email / texts
- Internet
- Passwords / security
- Social media



Core activity:

Present the information on the slides using the trainer notes below to support you if needed.



Suggested activity:

Invite the group to briefly discuss, for each category:

- Which of these safety points do they already do?
- Which they are aware of but don't usually bother with
- Which they weren't aware of
- What do they think the answers to the above 3 questions will be for the young people they work with?



If you do not wish to use the slides provided, an alternative option for covering this content is to facilitate a group discussion asking the participants to make their own suggestions as to what the do's and don'ts should be for each category. During the discussion and debrief, try to draw out the key points below. The additional trainer notes provide you with additional background knowledge and further reading on each topic should you require it.

Additional Trainer Notes – Do's and Don'ts of Staying Safe Online

Emails / texts

Impersonal greetings – if you have an account with a company, they will always address you by name. It is possible for cybercriminals to know your name too, but for spam emails they're more likely to be casting a wide net and use impersonal greetings

Spelling and grammar – poor spelling and grammar should always be a clue that something's not right. However, do bear in mind that some cybercriminals are very professional so even if an email or text has perfect spelling and grammar, this alone is not enough to guarantee that it's genuine

Spam / junk filters. If your filter lets some spam through you can help your email provider to improve in the future by marking the email as spam

Storing your bank's phone number offline is a useful way to ensure you can contact your bank if you have suspicions about an email or text, without having to rely on a phone number given in the text or email you're suspicious about. If you've received a suspicious phone call, remember to ensure the line is clear before ringing out. Cybercriminals can keep the call open after you think they've hung up, and when you dial out could pretend to be your bank. If in doubt, make another call in between to someone you know – that way you can be sure the cybercriminals are no longer on the line.

Spoofing Cybercriminals have a number of methods for making an email look as if it is genuine. They can call the email account anything they like including the name of your bank or other organisation. You can check the email address that sits beneath an account name by hovering over it with your mouse, but remember the email address can also be made to look similar to genuine emails. If the email address contains a long string of letters or numbers be very suspicious, but also look out for less obvious clues, such as the number zero '0' being substituted for the letter 'O' etc.

SMS Text messages can be 'spoofed' to make them appear as if they've come from a trusted organisation in your contacts – and can even appear in a chain of messages alongside legitimate messages from the trusted organisation. Therefore, it is recommended that you do not click on links in text messages even if they appear to come from a trusted organisation.

Don't be rushed into taking action – cybercriminals often try to create a false sense of urgency to try and get you to act on their email / text without properly thinking it through – for example by telling you your email account will be deleted

if you don't verify it within the next 24 hours, or that your bank account has already been compromised.

The UK based 'Take Five' campaign encourages people to take a few minutes to think before parting with money or information only, and to not allow yourself to be rushed or panicked into taking action. <https://takefive-stopfraud.org.uk/>

Further reading:

Get Safe Online. (2015, June 9). *Fraudsters Use Spoof Texts in New Bank Scam*. <https://www.getsafeonline.org/news/fraudsters-use-spoof-texts-in-new-bank-scam/>

Internet

Find websites online instead of clicking on links Websites can be 'spoofed' just as emails and text addresses can. One way cybercriminals can do this is by replacing letters and numbers in a web address so that they resemble the genuine web address – a simple way of doing this for a cybercriminal might be to substitute '0s' for 'Os' but Cyrillic or Unicode characters that look very similar to Latin Characters can also be used. Therefore, it is recommended that you navigate to web addresses by typing the URL into the search bar rather than clicking on links. If you don't know the organisation's web address, you could search for their website using a reputable search engine, but be cautious as search results can also be manipulated. Good antivirus software will highlight any dangerous websites to you.

Further reading:

Hern, A. (2017, April 19). Unicode Trick Lets Hackers Hide Phishing URLs. *The Guardian*. <https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers>

Check website is secure When shopping or providing potentially sensitive information online, make sure the website is secure e.g., is has https:// (as opposed to the non-secure http://) and a padlock in the address bar. Even if the website is secure, however, you should be aware that this only means that information being sent to the website (such as your credit card details) is encrypted and can't be intercepted and stolen *en route* to the website. It does not guarantee that the website is genuine – some cybercriminals can and do obtain https:// security certificates for their websites. Likewise, some non-secure websites will be genuine, but you shouldn't type any sensitive personal or financial information into them as it could be intercepted by cybercriminals. If a website redirects you to third-party payment services make sure it is genuine and secure before entering your payment details.

Further reading:

Get Safe Online. (n.d.). *Shopping*. <https://www.getsafeonline.org/shopping-banking/shopping1/>

Limits of https / padlock A 'secure' website only means that information you send to the website, such as credit card details or other personal information, is encrypted so that it cannot be intercepted *en route*. It does not guarantee that the website is genuine, as it's possible for a person with dishonest intent to obtain a security certificate for their website.

Further reading:

Which. (2021, November 15). *How to Spot A Fake, Fraudulent or Scam Website*. <https://www.which.co.uk/consumer-rights/advice/how-to-spot-a-fake-fraudulent-or-scam-website>

Security / Passwords

Installing software updates as soon as possible is important to patch any known security flaws or weaknesses that could be exploited by cybercriminals to steal your personal information or compromise your devices. It is recommended that you set software and devices to update automatically.

Source & further reading:

National Cyber Security Centre. (2021, December 21). *Top Tips for Staying Secure Online: Install the Latest Software and App Updates*. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates>

Antivirus / antispyware software Some operating systems such as Windows and iOS include antivirus tools so make sure they're switched on, but it's also worth considering additional antivirus software which can be researched online to see what the most appropriate product for you is. If you use a smartphone or tablet, you don't need antivirus software providing you only install apps from official stores.

If you receive phone calls or unsolicited emails offering to help remove viruses and malware from your computer hang up / don't reply as this is a common scam.

Ransomware – can sometimes include a threat to expose illegal or embarrassing activity on the part of the victim to try and pressure the victim to pay rather than seek help. There is no guarantee that payment of the ransom will result in the cybercriminals releasing your files. It is recommended that if your device is infected with ransomware, help is sought from a trustworthy source.

Source & further reading:

Get Safe Online. (n.d.) *Ransomware*. <https://www.getsafeonline.org/protecting-yourself/ransomware/>

Strong, unique passwords It's important that cybercriminals can't easily guess your passwords. Bear in mind cybercriminals may have access to software that can make thousands of password 'guesses' (known as Brute-forcing) in a short space of time. Also bear in mind that if your data has been compromised (for example, if you have an account with an organisation that has a data security breach) then your password might be on a list of leaked passwords – this is why it's important for each account to have a different password, to protect them in the event one account is compromised.

Options for creating strong passwords include:

choosing three random words that people won't associate with you

using numbers, symbols and combinations of upper / lower case letters. (Bear in mind that cybercriminals are familiar with changing letters to numbers, such as E to 3 and S to 5 etc)

Use a line of a song or poem that people would not associate with you.

Pick a phrase and use the first character of each word to create a password.

There are various password checkers online that can let you know how secure your passwords are (we do not recommend entering actual passwords into these checkers, but you could input something that's similar in structure to find out how secure it is). One example is: <https://password.kaspersky.com/>

This site enables you to see if a particular password appears on a database of leaked passwords: <https://haveibeenpwned.com/Passwords>

Further reading:

National Cyber Security Centre. (2016, October 27). *Three Random Words or #ThinkRandom*. <https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0>

Get Safe Online. (n.d.). *Passwords*. <https://www.getsafeonline.org/protecting-your-computer/passwords/>

Consider using a reputable password manager - a password manager will generate and store strong passwords for you – the only password you need to remember is the one for accessing your password manager account.

Remember to research first by reading reviews and / or getting personal recommendations to make sure the password manager you choose is reputable and secure. It's best to activate 2-factor authentication for logging into any password manager for additional security.

Further reading:

National Cyber Security Centre. (2021, December 21). *Password Managers: Using Browsers and Apps to Safely Store Your Passwords*.

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>

Activate 2-/multi-factor authentication – this provides an extra level of security when logging into accounts – for example in addition to entering your password you will also receive an email / text message / automated phone call with a one-time use code (this can also be generated using a special app) to enter in addition to your password to access your accounts. This means that if your password is compromised, a cybercriminal attempting to access your accounts will be asked for a 1-time passcode that they would also need access to your phone / email to generate. (Some smartphones enable you to use your fingerprint rather than a passcode as the second layer of security)

Further reading:

Get Safe Online. (n.d.) *Passwords*. <https://www.getsafeonline.org/protecting-your-computer/passwords/>

National Cyber Security Centre. (2018, August 8). *Two-Factor Authentication (2FA): New Guidance from the NCSC*. <https://www.ncsc.gov.uk/blog-post/two-factor-authentication--2fa---new-guidance-from-the-ncsc>

Take particular care with your email password – if your email account is compromised, then all of your account passwords could be reset simply by a cybercriminal clicking on the 'forgotten password' link for other accounts and accessing your email account to reset them

Further reading:

National Cyber Security Centre. (2018, December 21). *Use A Strong and Separate Password for Your Email*. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email>

Don't rely on free public Wi-Fi for accessing your online accounts Public Wi-Fi hotspots are not secure and the information you send using it could be intercepted by third parties. If you need to access sensitive personal data when out and about

(including logging onto social media etc) it is more secure to use 4G. If public Wi-Fi is the only option, make sure you use a VPN (virtual private network) – this provides end-to-end encryption so that anyone intercepting your data would not easily be able to decipher it. However, bear in mind that your VPN provider may be able to access records of websites etc that you visit.

Further reading:

Get Safe Online. (n.d.) *Virtual Private Networks*.

<https://www.getsafeonline.org/smartphones-tablets/virtual-private-networks-vpns/>

Social Media

Review your privacy settings

It's a good idea to regularly review your privacy settings on each social media platform you use, to make sure you're not sharing information more widely than you thought.

Blocking and reporting

Most social media platforms have a means of blocking or removing people you don't wish to engage with. It's worthwhile making sure you know how to report abusive / inappropriate behaviour (and what the platform's rules are) so that you can report inappropriate posts (although reporting does not necessarily mean a post will be removed – it will be assessed by the social media platform's team in line with their terms and conditions of use)

Further reading:

Childnet. (n.d.) *Privacy Settings*. <https://www.childnet.com/young-people/secondary/privacy-settings>

Childnet. (n.d.) *Social Media*. <https://www.childnet.com/young-people/secondary/social-media>

Think U Know. (n.d.) *Joining Social Media*.

https://www.thinkuknow.co.uk/11_18/lets-talk-about/socialising-online/joining-social-media/

It's important to remember that the social media platforms popular with young people can change frequently, so the important thing to remember is to always check the community guidelines and security / privacy / safety features when starting to use a new platform.

Think before sharing / liking

We cover misinformation and disinformation in detail in the main module of this training package 'Online Literacy'. Some posts are also "' like" farms' – these will often offer an extremely generous prize, inviting you to like in order to be in with a chance of winning, or feature a child or other person with a serious medical condition, for example, asking you to 'like' the post to show support. Although initial post might be harmless, once enough likes have been obtained, the original content of the post can be changed (e.g., to promote products or a link to malware added).

Further reading:

Better Business Bureau. (2020, June 10). *BBB Tip: Like-Farming Is a Facebook Scam Still Going Strong*. <https://www.bbb.org/article/news-releases/17149-like-farming-a-facebook-scam-still-going-strong>

Once you've posted information online you no longer control it. This is true even if you have your privacy settings locked down, as any 'friend' you share it with may still be able to share it, either by screenshotting it or downloading an image. Even if you delete your original post, someone may have taken a screenshot and share it from their own account.

Don't disclose sensitive information such as your date of birth or address. Also bear in mind that it's to inadvertently disclose 'fragments' of sensitive information without realising such as parts of telephone numbers and dates of birth, or potential answers to security questions (favourite colour, sports team) so be aware of any quizzes or games asking you to do this.

Reporting Cybercrime (5 minutes, Slide 16)



Core Activity

Present the information on the slide using the trainer notes for support.

Depending on the circumstances, cybercrime can be reported to a number of organisations and agencies. Who would you report it to?

- The organisation concerned (e.g., the bank or the vendor)
- The police? Under what circumstances?
- The social media platform
- Charities and helplines
- Specialist support



Suggested activity –

prior to presenting the information on the slide, ask participants if they would report cybercrime if they experienced it and to whom? Make a note of their answers and compare it to the information on the slide.



Suggested activity:

Initiate a brief discussion as to what they think the specific agencies they would report to in their region / country are or how they would find out if they don't know.

Additional Trainer Notes – Reporting Cybercrime

For the UK: (this information is also in the resource pack)

Fraud and other cybercrime: report to Action Fraud:

<https://www.actionfraud.police.uk/>

Online grooming/child sexual exploitation: Report to Child Exploitation and Online Protection Command (CEOP):

<https://www.ceop.police.uk/safety-centre/>

For reporting hate crime: See TrueVision: <https://www.report-it.org.uk/>

If someone is in immediate danger: Police emergency: 999, otherwise dial 101 non-emergency number (if fraud online they may redirect you to Action Fraud)

If money is lost, speak to your bank immediately.

If you are concerned that a person is being radicalised online, you can report it to your local Multi-Agency Safeguarding Hub (MASH)

Reporting extremist material can be done via <https://actearly.uk/>

For reporting images of child sexual abuse - Internet Watch Foundation

https://report.iwf.org.uk/en?_ga=2.1534644.424843882.1606143216-1834616103.1533735816

If someone has experienced their intimate images being shared online, they can contact Revenge Porn helpline for support:

<https://revengepornhelpline.org.uk/>

EUROPE advice

<https://www.europol.europa.eu/report-a-crime/report-cybercrime-online>

Topic 4– Scenarios

Scenarios (45-75 minutes, Slides 17-26)



Core activity:

During this section, the participants will discuss a range of scenarios involving young people and cybercrime activity that potentially poses a risk to them. Some examples are provided in this training manual, but you may wish to create your own scenarios relevant to your participants' specific roles working with young people, and national / cultural context.

Option 1 for delivering this content, is to display each scenario, either on a PowerPoint slide, or provided as a printout to participants, and facilitate a group discussion on how it might best be dealt with, recording responses on a whiteboard / flip chart as appropriate.

Option 2 is to divide the participants into pairs or small groups and assign them one scenario to discuss among themselves, and then come back to present their thoughts to the group. If you choose this option, it is recommended that you visit each group in turn during their discussions to make sure they are progressing along the appropriate path of supporting cyberawareness for the young person.



KEY POINTS

Whichever option you choose, the key learning points that you need to facilitate are:

- Practical application of methods to evaluate online information;
- The transfer of skills into the workplace – how will participants use their newly gained skills to support the young people they work with to develop their own critical literacy and resilience to false information online?
- To learn from one another – by sharing their thoughts participants will be able to gain ideas and inspiration from their peers.

Scenario 1:

David, who is 16, tells you that he's been chatting with someone he met when playing World of Warcraft on PlayStation – James, who claims to be 19, and they developed a romantic relationship. Eventually, they started chatting on skype and James convinced David to send a naked picture of himself to him.

After that, James sent David a message telling him to pay him £500 in Bitcoin or he would email his photo to his FB and WoW friends. David actually paid him in Bitcoin, but extortion threats are ongoing. David has been warned that, if he goes to the police, his photo will be released anyway.

What would you recommend David do now?

Scenario 2:

Tilly, aged 12, gets a Smartphone for her birthday and decides to explore social media for the first time. She creates accounts on Twitch, Twitter, TikTok, Facebook, Snapchat, YouTube, Reddit and Instagram, adding lots of friends including anyone who sends her a friend / follow request.

What advice would you give Tilly about her online activity?

Refer back to the 'Do's and Don'ts of staying safe on social media to facilitate the discussion for this scenario

Scenario 3:

Bill, who is 16, has recently opened up his own bank account to pay in his wages from his part-time job that he's saving up to buy his first car. He receives a text from his bank advising him that his online bank account has been hacked and he needs to move his money to another account to stop it being stolen. There is a link in the text message that he can click on to resolve the problem.

What advice would you give Bill?

Refer back to the 'Do's and Don'ts of staying safe – emails and texts – to facilitate the discussion on this scenario

Scenario 4:

Nik, aged 14, confides in you that they are being bullied online. Their mum has suggested deleting all their social media accounts and staying offline, but Nik doesn't want to do this as they also have many friends online. The bullying has got so bad they can't sleep or eat, and they keep constantly checking social media to see what is being said about them.

What advice would you give Nik?

Scenario 5:

Priya, who is 17, tags you in the following quizzes she has already completed on Instagram:

What would you do?

Favourite food:	The last four digits of your phone number are the things you need to make you happy.	
First pet:		
First school:		
Favourite sports team:	Tag yourself:	
Year of birth:	0 Cuddles	5 Romance
First pet's name:	1 Naughtiness	6 Laughter
Favourite colour:	2 Wine	7 Love
Mother's maiden name:	3 Sex	8 A lie-in
Name of street you grew up on:	4 Money	9 Chocolate
Middle name:		

Refer back to 'Do's and Don'ts of staying safe on social media' to facilitate the discussion.

Scenario 6 part 1:

Latisha shows you a website she has found selling extremely cheap designer handbags. She's very pleased as she wants to buy a handbag as a gift for her mum who's been ill and needs cheering up.

What would you advise Latisha to look out for when deciding whether to buy a handbag from the website?

Scenario 6 part 2:

Latisha follows your advice and discovers the following. What do you think Latisha should do now?

- The spelling and grammar on the website all seem correct
- It has a professional looking shop page for credit card and shipping information to be entered
- The website's URL begins with http://
- The website has a 'Contact Us' page with an email address for asking questions but no postal address
- The photos of the handbags are exactly the same as the photos on the handbag designer's own website

- On its home page, the website states the following statement, alongside a photograph of a padlock:

Our website is fully secure and padlocked!

Refer back to the 'Do's and Don'ts of staying safe – internet' when facilitating this discussion.

Additional Trainer Notes for Cybercrime Scenarios

When reviewing the group responses on this scenario, you may wish to play one or both of the optional videos. Potential advice that could be provided includes:

Report to police (either 999 if happening now or 101 if already happened)

DO NOT pay any money - as further demands for money may follow & there's no guarantee that payment will stop the explicit material being posted

Stop communicating with the person immediately

Report to your internet service provider (if possible, suspend your account but don't delete it)

Take screenshots of all your communication, write down all the details you can such as the person's name / username or ID, any URL associated with their account

If you're under 18, report to CEOP

Source & further advice:

National Crime Agency. (n.d.) Sextortion (Webcam Blackmail).

<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>

Scenario 2:

Further reading:

Ballard, J. (2019, October 25). Teens use these social media platforms the most.

YouGov America. YouGov America. <https://today.yougov.com/topics/lifestyle/articles-reports/2019/10/25/teens-social-media-use-online-survey-poll-youth>

Scenario 4

Possible answers:

Block and Report

Abstain from playing (what are the downsides of this response e.g., putting the responsibility on Nik?)

Screenshot any offensive or harassing messages

Make privacy settings strong

How do you feel about this resource by Childline?

Childline. (2014, November 17. Building Confidence After Bullying Online. *YouTube*. <https://www.youtube.com/watch?v=9HocoOVVUDY>

Further reading:

BBC. (2017, May 31. 'One in two' young online gamers bullied, report finds. <https://www.bbc.co.uk/news/technology-40092541>

Childline. (n.d.) *Gaming*. <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/>

Remember – cyberbullying is dealt with in more detail in [Optional Module B: Cyberharassment](#).

*Topic 5– Summary and Close
(10 minutes, Slides 24-25)*



Core activity:

Return to the list of learning objectives and outcomes and briefly summarise in a few sentences how the training has met each learning outcome, ticking them off or adding emojis (smile, heart, star, etc), getting agreement from the group to confirm each learning outcome has been met.*

Learning Objectives:

- To understand the different types of cybercrime young people might encounter online and what the impact on them might be
- To understand how young people can protect themselves from cybercrime
- Learning Outcomes:
- To be able to support young people to identify and protect themselves from cybercrime
- To empower young people to use the internet safely

*If one of learning outcomes has not been met for some reason, make a note of it and commit to following it up with the participants at a later date e.g., by sending a clarification email.



Core activity:

Return to the whiteboard / flip chart record of personal objectives participants had for the training session. Have these personal objectives been met? If so, acknowledge this by ticking them off, or adding emojis. If not, from the knowledge and expertise you have gained while preparing to deliver this training, are you able to suggest where the participant could find out what they wanted to know? Is there anything you can look up and email to the participants later?

Once the learning outcomes and personal objectives have been debriefed, and any outstanding questions have been answered, you may close the session.

Optional Module B: Cyberharassment

Topic 1 – Title, Agenda, Topics *(2-3 minutes, Slides 1-2)*

There are no trainer notes for these slides. Trainers can use the information contained on the slides to provide a brief overview of the session to come, including the topics and activities to be covered.

Topic 2 – Cybercrime (3-4 minutes Slide 3)

This slide presents a brief definition of cybercrime, followed by an overview of recent cybercrime statistics for your region. There are no additional trainer notes as all the information is on the slide. However, you may wish to check the source supplied for your region to see if there are more recent statistics available by the time you present this training.

If you have time in the session, you could generate a brief discussion among the participants as to their thoughts on the definitions and statistics.

Topic 3 – Cyberharassment, Intimidation, Cybersexism (10-15 minutes, Slides 4-8)

These slides present some key features of cyberharassment, intimidation and cybersexism.



Cyberharassment

Suggested activity - you may wish to generate a brief discussion among the participants as to whether they are aware of cyberharassment or cyberbullying taking place among the young people they work with. Do they recognise the features included on the slide, or does the cyberharassment in their context present differently? If it is different, in what way, and why do they think that is? Any thoughts they share can then be returned to later in the training session, when you are discussing the case studies.



Intimidation

Suggested activity - you may wish to discuss with the group the ways in which online bullying may intersect with offline bullying – what are the similarities and differences? Is there always a clear line between the two types of harassment? Can online bullying spill over into the offline world and vice versa and what might be the consequences of this for young people?



Cybersexism

Suggested activity - You may wish to discuss with the group the ways in which the power structures associated with sexism (as well as homophobia and prejudice against other marginalised identities) in the offline world may be replicated in online harassment. Are they aware of any of these patterns occurring among the young people they work with? This can be returned to when discussing the case studies.

Topic 4 – Case Study Workshop (30-40 minutes, Slides 9-15)

Resources and advice

Slide 9 contains links to resources and advice on how to tackle cyberharassment, including cyberbullying and online sexual harassment. These resources, as well as any other relevant resources the participants may find online, can be used during the case study workshop to inform the discussion and answers the participants present to the group.

Department for Education. (2014). *Cyberbullying: Advice for Headteachers and School Staff*.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069987/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Facebook. (2022). *Put A Stop to Bullying*.

<https://www.facebook.com/safety/bullying/>

Kidscape. (n.d.) *Cyberbullying and Digital Safety*.

<https://www.kidscape.org.uk/advice/advice-for-parents-and-carers/cyberbullying-and-digital-safety/>

Kidscape. (n.d.) *Top Tips for Dealing with Bullying*.

https://www.kidscape.org.uk/media/134268/top-tips-for-schools_final.pdf

National Crime Agency. (n.d.) *Sextortion (Webcam Blackmail)*.

<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>

Revenge Porn Helpline. (n.d.) *Help and Support for Under 18s*.

<https://revengepornhelpline.org.uk/how-can-we-help/under-18s/>

Revenge Porn Helpline. (n.d.) *What to Do If You Have Had Intimate Images Shared Online Without Your Consent*. <https://revengepornhelpline.org.uk/information-and-advice/need-help-and-advice/intimate-images-shared-without-consent/>

Stonewall and Childnet. (2021). *Staying Safe Online: Practical Strategies to Best Support All Children and Young People Online, Including Those Who Identify as LGBT*.

https://www.stonewall.org.uk/sites/default/files/a4_toolkit_staying_safe_online_2021-update.pdf

The Diana Award. (n.d.) *Imagine: A School Free from Bullying*.

<https://www.antibullyingpro.com/>

UK Safer Internet Centre. (n.d.) *Professionals Online Safety Helpline*.

<https://www.antibullyingpro.com/https://saferinternet.org.uk/professionals-online-safety-helpline>

UK Safer Internet Centre. (n.d.) *Helping Children and Young People Stay Safe Online*. <https://saferinternet.org.uk/>

Victims of Image Crime. (n.d.) *Victims of Image Crime: Speak Out!*

<https://voic.org.uk/>

Case studies

Slides 11-16 present various case studies that can be assigned to the participants, working in groups, to research and discuss what actions they would take to support the young person and come back to the group to present their answers. You, as the trainer, have the freedom to select whichever case studies you think are most relevant to the context of your group or even create new ones. The activities have been designed to be assigned to different groups working simultaneously, to maximise learning, as each group will learn from the other during the presentation stage.



Case Study 1 - Cybercrime

This case study summarises the more detailed learning contained in [Optional Module A: Cybercrime Awareness and Online Safety](#) and therefore may be omitted if participants have already completed that module. Depending on what aspects of cybercrime you feel are most relevant to your participants, you may provide the slides from Optional Module A as research material, or provide the links to some of the additional reading to assist the group in their research and discussion.



Case Study 2 – Cyberharassment

This case study invites participants to consider what actions they would take if they suspected a young person they work with is being cyberbullied. It can be adapted to suit different contexts (e.g. schools, youth organisations). You may wish to direct the group to the relevant cyberbullying advice resources listed above (and also on Slide 9 of the supporting PowerPoint for this module) or invite them to research online for other relevant resources to help them with their discussions and reflections, before reporting back to the whole group.



Case Study 3 – Intimidation

This case study deals with a young person who has experienced online bullying as a result of being a member of the LGBT community. In addition to the general resources on dealing with cyberbullying already mentioned above, participants may find it helpful to refer relevant resources on Slide 9. Can the group locate any other advice about cyberbullying specifically related to young people who are LGBT?



Case Study 4 – Non-consensual intimate images

This case study addresses the non-consensual posting online of intimate images (including video), also known as ‘revenge porn’. This may also include ‘sextortion’ which is the threat to post such images in order to coerce the victim into some behaviour they do not wish to undertake, such as further sexual activity. This group is required to research and discuss what specific advice they would give Sophie in this situation, using the relevant resources on Slide 9, or researching their own resources.

Topic 5 – Summary and Close (3-5 minutes, Slides 17-18)



Slide 16 summarises the key learning points that should have been covered in the training. Briefly summarise in a few sentences how the training has met each learning outcome, ticking them off or adding emojis (smile, heart, star, etc), getting agreement from the group to confirm each learning outcome has been met. *

- Understand and identify online threats
 - Help educate those exposed to online threats
 - Be able to search for additional information online with confidence
 - Gain and continue to develop critical thinking skills to deal with online threats
- *If one of learning outcomes has not been met for some reason, make a note of it and commit to following it up with the participants at a later date e.g., by sending a clarification email.

Optional Module C: Mini-Module - Legislation

The legislation mini-module is available as an optional add-on if you feel that the training participants would benefit from having some basic knowledge of the legislation in your country relevant to cybercrime and online false information. There are no core / suggested activities for this mini-module - simply open the relevant PowerPoint slide, locate the slide relevant to your country and present this information to the training participants. Depending on the context and time available, an alternative method of covering this material would be to assign the participants the task of researching the relevant legislation for their country and report back to the group, in which case, you can use the information on the slides to help you debrief the activity. As statute and case law can change frequently, we recommend reviewing the contents of these slides prior to delivery to ensure the laws they reference are up to date.



5 Follow-up

Small-Medium-Large

The aim of the follow up stage is to consolidate learning and providing the training participants with the opportunity to undertake further developmental activities customised to their professional context.

Small

For the short version of the follow-up phase, which should take about 10 minutes, participants need only rank their confidence in the following key competency areas. The answers to this questionnaire are private, and for the trainees' own reflection, to enable them to compare their confidence levels prior to the training (they should already have completed this questionnaire at the preparation stage) and enable them to identify if there are any areas where they still need to build their confidence / undertake additional research (which they can do, if they wish, by reading some of the additional materials suggested in the resource pack):

Choose the response on the scale from strongly disagree to strongly agree that most closely matches how confident you feel about each of the competency areas below	Not confident	Slightly confident	Somewhat confident	Confident	Very confident
Enhance the critical literacy of young people in relation to online information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Help young people understand the potential harm caused by false information online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support young people to effectively evaluate online information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support young people to be more resilient to false information online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Teach young people how to protect themselves from cybercrime	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Explain and enhance online privacy for young people	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

You do not need to share these answers with anyone. They are for your personal reflection.



The medium version of the follow-up is the completion of a confidence questionnaire and a brief reflective journal summarising what they have learnt during the training, including their thoughts on how they will transfer this into the workplace when working with young people. This should take around 40 minutes in total.



The large version of the follow-up is the completion of the confidence questionnaire and the reflective journal as described above and attendance at a facilitated discussion group with the other participants. The objective of the discussion group is for participants to share their thoughts on transferring their learning into the workplace with the objective of sharing ideas and examples about how they can support young people with online critical literacy. This should take from 60-90 minutes in total, depending on which options you choose.

The large version of the follow-up provides an opportunity for the participants to engage in one or both of the following activities, designed to supplement the core learning and to make it easier for them to transfer what they have learned into the workplace.

Follow-Up Activity 1: Safeguarding

All professionals working with young people, no matter what their role, context or region, have a duty to protect young people and safeguard their welfare, albeit the precise circumstances, legislation and procedures will vary depending on the country / region. It is possible for safeguarding issues to arise in relation to any of the topics covered in this training on Critical Literacy and Online Safety. Consider the scenarios below, choose those most appropriate for your context (or, if you prefer, create your own scenario(s)) and assign the participants to either discuss the following questions in groups, or reflect upon them in independent study:

1. Does this incident raise a safeguarding concern in your organisation / country?
2. If yes, what steps does your national law / local procedure require you to take in relation to safeguarding? Are there any additional actions you would take in addition to those set out in law / policy?
3. If no, what actions might you take instead to support this young person?

It is important that a distinction is drawn between these scenarios, and the ones included in the training modules the participants have already completed.

In the training module scenarios, the focus was on supporting and empowering young people to develop their critical literacy skills, online safety and cybercrime awareness. However, the scenarios in this section are intended to draw upon what professionals will already know about safeguarding procedures in their country / organisation and to reflect on how they will apply these principles should any safeguarding issues arise in relation to online platforms. This distinction should be borne in mind when presenting and debriefing these scenarios.

Scenario 1

Anna is 13 and a talented singer, who regularly livestreams songs on her favourite livestreaming platform. A friend of Anna confides in you that a viewer of Anna's performances has messaged Anna, offering her money if she agrees to sing a song without her top on. Anna has told her friend that she's thinking about doing it, as she wants the money for singing lessons and she thinks it will increase the interaction and likes she gets on the site.

1. Does this incident raise a safeguarding concern in your organisation / country?
2. If yes, what steps does your national law / local procedure require you to take in relation to safeguarding? Are there any additional actions you would take in addition to those set out in law / policy?
3. If no, what actions might you take instead to support this young person?

Scenario 2

Adam, who is 16, is a polite and quiet member of his peer group. You notice that he is increasingly sitting alone at break and meal times and not joining in with his friends. When you speak to Adam, he tells you he has new friends who he has met in a gaming forum. His new friends have shown him proof that a certain religious faith is part of a huge conspiracy to infiltrate influential and powerful organisations. He plans to join his new friends' online political group, which has been formed to discuss what can be done to counter the perceived threat from this religion.

1. Does this incident raise a safeguarding concern in your organisation / country?
2. If yes, what steps does your national law / local procedure require you to take in relation to safeguarding? Are there any additional actions you would take in addition to those set out in law / policy?
3. If no, what actions might you take instead to support this young person?

Scenario 3

You notice that Tom, who is 15, has a lot more money than he used to have and is buying lots of expensive clothes and devices not just for himself but for his friends. When you ask him about it, Tom tells you he has a new job but on further questioning, admits that he is creating phishing malware and selling it on the dark web. Tom doesn't think he's doing anything wrong, as he's not personally committing cybercrime and isn't responsible for what other people do with the malware once he's sold it to them.

1. Does this incident raise a safeguarding concern in your organisation / country?
2. If yes, what steps does your national law / local procedure require you to take in relation to safeguarding? Are there any additional actions you would take in addition to those set out in law / policy?
3. If no, what actions might you take instead to support this young person?

Scenario 4

During a safe space session, Lina tells you about an event that is being discussed on several of her favourite social media platforms. The planned event is a rave to be held in a local forest. It is being billed as a 'COVID Kissing Party' so that young people can catch COVID through close contact with one another, and therefore not have to risk testing positive at a future time as they will already have had the virus and will therefore be immune. Lina tells you that she plans to attend the event as she has seen a video online which explains that young people are not harmed by COVID and she wants to make sure she catches it now, and not in the summer when she hopes to go on holiday to Spain.

1. Does this incident raise a safeguarding concern in your organisation / country?
2. If yes, what steps does your national law / local procedure require you to take in relation to safeguarding? Are there any additional actions you would take in addition to those set out in law / policy?
3. If no, what actions might you take instead to support this young person?

Follow-up Activity 2: Bespoke Activity Design

The objective of this activity is to support the participants to transfer their learning into the workplace as they engage with young people in a professional context.

Using the resource pack as a reference, divide the group into pairs or small groups. Assign each group with the task of designing an activity they could undertake with the young people they work with that meets the overall aim of the training – to empower and support young people to develop their critical literacy and resilience to false information online.

This activity will be most effective if you provide a defined objective, e.g. specify what the young people who would ultimately undertake the activity should learn from it. The nature of this objective will depend on a number of factors, including the age of the young people and the professionals' role, but appropriate examples may include:

Designing an activity to help the young people you work with:

- Explain the different actions they could take to help decide whether some information they have seen on social media is true;
- Explain what actions they could take to help you stay safe when using social media;
- How they would help a friend who was being cyberbullied?

Using the resource pack as a guide, each group should design an activity which would be appropriate for the young people they work with in their professional context to participate in, to help them achieve the stated objective. Depending on the age of the young people and the professional's role in working with them, appropriate activities may include:

- Designing a quiz on a subject relevant to the training e.g., 'fake news' (designed either by the professional or by the young people themselves);
- Scripting and acting out a roleplay;
- Creating a crossword puzzle, with the answers being words relevant to cybersafety (designed either by the professional or by the young people themselves);
- Designing a cybersafety poster;
- Writing a story;
- Organising a group debate on cybersafety.

When facilitating / debriefing this activity the key point is to draw out is that the participants are the experts in their particular context and what sorts of activities will be the most appropriate for the young people they work with, and to provide an opportunity for the participants to be creative and inspired by one another's ideas.

Bear in mind that depending on the participants' role, their ideas about what would be an appropriate activity might be very different – e.g., teachers and youth workers interact with young people in very different ways. For example, a teacher may consider themselves as someone whose duty it is to hold knowledge about a subject and impart this knowledge to young people, whereas a youth worker may start from the premise that the young person 'knows' and the exchange of knowledge is more equal. Both are valid perspectives, but you should be prepared to address this depending on the role of the group participants.

Whichever role the participants have, try to encourage the perspective that young people have actorship and empowerment and may have more knowledge of some aspects of the online world than the professionals, which should be respected. The development of activities which provide space for young people to share their own knowledge and perspectives should also be encouraged.

6 This training in the Orpheus project

ORPHEUS

Offline and online **R**adicalisation **P**revention **H**olding back **E**xtremism and **U**pholding **S**ecurity

This training is part of the ORPHEUS project. In this section, we explain how the training relates to some of the key concepts in this project.

In European cities, the threat of violent extremism of all types, such as jihadi, extreme right and hate crimes, is a significant and rising social concern. The Interreg ORPHEUS project has developed alternatives to offline and online prevention of violent extremism, using an approach that is not *problem* oriented but *wellbeing* oriented. Additionally, ORPHEUS has developed new integrated and aligned services, extending the prevention service together with private and social institutions, with young people and their educators as central actors.

The key aims and outputs of the ORPHEUS project are summarised below:

1. Enhance the integral prevention model to address violent extremism

Creation of a new prevention framework: the ORPHEUS Prevention Pyramid, which combines efforts from general prevention to direct intervention and targets the interplay of different risk and protective factors.

2. Develop safe spaces for and with young people.

Stimulate and organise open dialogue, connect young people in balanced bonding with family, friends and institutions and support the public expression of their grievances.

3. Build resilience, critical thinking skills and increase confidence of educators.

Enhance key analytical skills within young people. Involve young people and educators as part of the solution. Empower educators to facilitate difficult conversations on sensitive topics.

4. Integrate online work on different levels of prevention.

Develop online alter-narratives to raise critical awareness. Develop broader internet safety techniques to keep young people safe online.

5. Provide guidance and policy recommendations for adoption of an integrated prevention method in the 2Seas area.

Eight European partners, consisting of professionals, researchers and policy makers, participate: Stad Mechelen (BE), Greta Grand Littoral (FR), Portsmouth City Council (UK), Ceapire (BE), University of Portsmouth (UK), University College Roosevelt (NL), Arteveldehogeschool Gent (BE), Contourdetwern (NL)

Safe spaces

In the ORPHEUS' framework paper, the concept of 'safe spaces' is explained as a pedagogical approach: *"The concept of safe space is not so much characterised by a location, institution, organisation... but by the **pedagogy** and philosophy behind it. The pedagogical view should be aimed at rebalancing protection and emancipation, and **(re)install 'safe spaces as laboratories'** where young people are in charge, working together in empowering ways and participate in the whole society."*

The conception of safe spaces extends to *online safe spaces*. This training is designed to equip key players (such as social and youth workers, educators, voluntary key players and peers) so that when supporting young people in safe spaces, they have the necessary skills and knowledge to facilitate conversations about online disinformation and are able to engage from a prevention perspective, reducing the risk of young people being adversely influenced by disinformation. The ultimate objective of the training is to enable key players to empower young people to come to their own, informed conclusions about information they encounter online. This approach supports young people to express their grievances in the public sphere more effectively as they will be more able to frame their grievances and evaluate alter-narratives in the context of having the skills to evaluate accurately information they encounter online, reducing the risk of becoming influenced by disinformation.



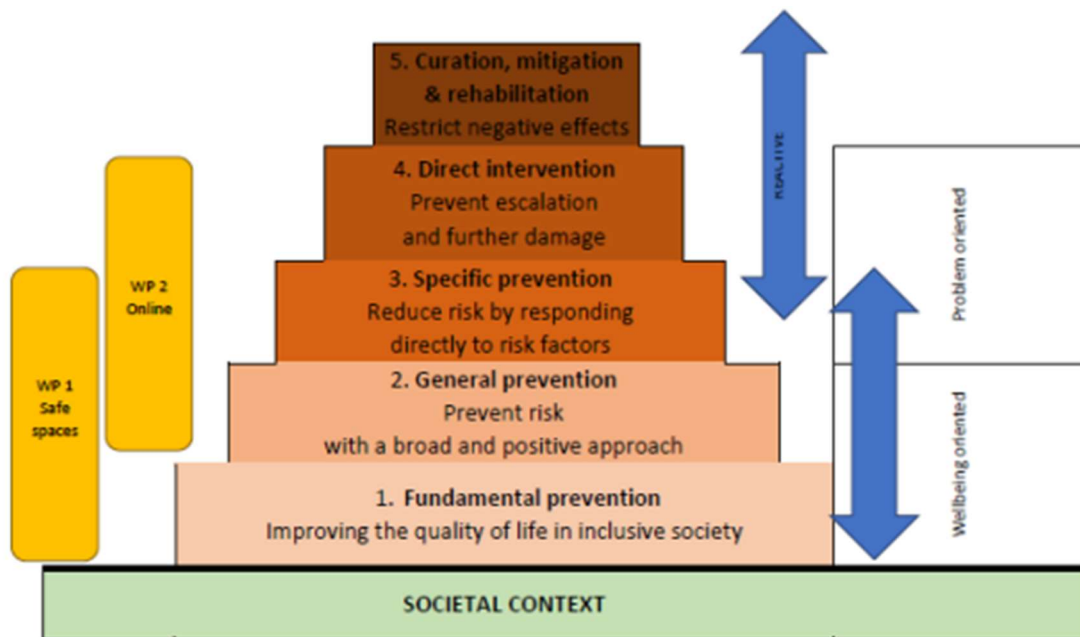
Pedagogy

We have based our didactic approach on active engagement, as we feel that there will be varying degrees of commitment and interest and therefore, such an approach bridges the gap between those more inclined to gain the knowledge and those not as interested. (Biggs and Tang, 2011). Our approach tries to impart the need to not just communicate knowledge and expect the learners to digest the knowledge independently, but it focuses on learning and assesses what needs to be learned and what are the intended outcomes of learning, what it means for the students to understand the content in the context of the intended learning goals and the provides a variety of interactive and engaging teaching and learning activities to accommodate the desired levels of understanding. (Biggs and Tang, 2011). This is based on a constructivist approach, where students are engaged in active learning, and consequently build knowledge through terms that they already understand through schemata they have already developed. (Biggs and Tang, 2011) That is why we have included a diverse mix of activities for resources for learners and their tutees as well to engage and interact with in order to digest the content and processes through examples and exercises with which they personally associate.

In order for the learning to be engaging, it also needs to be able to demonstrate why it is important and offer some value to the learner in terms of the outcome and to expect success in terms of achieving this outcome through the learning. This is what we call expectancy value theory. (Eccles, 1983) It is anticipated that the training will be provided as an important supplement to the work of social/youth workers and will increase the benefits for young people by providing them with some important critical evaluation tools and processes for engaging with the media they are currently heavily engaged with (social media, online forums etc.). The combination of this content-based training with the more methodological 'Dealing with Difficult Conversations' training will thus offer added value to the key players undertaking it, as it will reinforce core values and principles of their work such as:

1. Upholding and promoting human dignity and well-being;
2. Respecting the right to self-determination;
3. Promoting the right to participation;
4. Challenging discrimination;
5. Challenging unjust policies and practices;
6. Empowering people;
7. Challenging human rights abuses (British Association of Social Workers, 2014)

The Prevention Pyramid



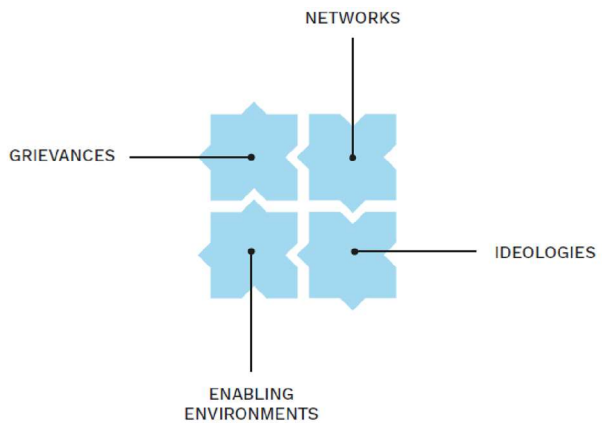
Framework for the integral prevention of radicalisation towards political violence - Görgöz, Vanhove & Van Bouchaute, elaborated on the model of Dekker, J. (2006)

This training focuses on the following levels of the Prevention Pyramid:

- **General prevention** (wellbeing oriented) - providing young people with the general skills they need to assess the veracity of information they come across online making them less likely to form opinions based on disinformation
- **Specific prevention** (problem oriented) - reducing the risk of young people being drawn into political violence because they have been influenced or politicised by disinformation

Puzzle Model on the Risk Factors for Violent Extremism

Hafez and Mullins (2015) suggest a puzzle metaphor for understanding the interplay of causal factors leading to a young person becoming involved in violent extremism, focusing on four interdependent components: grievances, networks, ideologies, and enabling environment and support structures.



In the ORPHEUS framework paper, this model is built upon to address the interplay between online and offline causal factors of political violence by:

- Strengthening positive networks for young people
- Offering legitimate channels for the public expression of grievances
- Promoting inclusive alter-narratives on society

This training encompasses all four interdependent aspects of the puzzle model. It provides youth workers and educators with the skills they need to support young people to evaluate online information, strengthening positive online and offline **networks**, while reducing the risk of young people's **grievances** and **ideologies** being influenced by the **enabling environment** of online disinformation.

The training facilitates the provision of legitimate channels for the public expression of grievances, as it supports young people in formulating their grievances within the context of an informed evaluation of online information. The training also promotes online resilience, as young people will be less likely to accept uncritically online disinformation and critical thinking by providing young people with the tools and skills they need to evaluate information online.



7 Reference list

Abeshouse, B. (2019, February 8). Troll Factories, Bots and Fake News: Inside the Wild West of Social Media. *Al Jazeera*.

<https://www.aljazeera.com/blogs/americas/2018/02/troll-factories-bots-fake-news-wild-west-social-media-180207061815575.html>

Action Fraud. (n.d.) *Remote Access Tool Scams*.

<https://www.actionfraud.police.uk/a-z-of-fraud/computer-software-service-frauds>

Action Fraud. (n.d.) *Romance Fraud*. <https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud>

Alava, S., Frau-Meigs, D. & Hassan, G. (2017). *Youth and Violent Extremism on Social Media: Mapping the Research*.

<http://unesdoc.unesco.org/images/0026/002603/260382e.pdf>

Anti-Defamation League. (n.d.) *Pepe the Frog*.

<https://www.adl.org/education/references/hate-symbols/pepe-the-frog>

Aoki, S. [@steveaoki]. (2020, January 4). *My Heart Breaks For #Australia. A Few Ways You Can Help.* 🇺🇸 🇺🇸 🇺🇸 🇺🇸. [images attached]. *Twitter*.

<https://twitter.com/steveaoki/status/1213589859152973826>

Associated Press & Griffith, K. (2019, May 18). Judge Allowed Cartoonist Who Created Pepe the Frog to Continue His Lawsuit Against Alex Jones' Infowars For Selling A Poster of The Character That Became an Emblem of The Far-Right. *Daily Mail*. <https://www.dailymail.co.uk/news/article-7043569/Judge-allows-cartoonist-created-Pepe-Frog-continue-lawsuit-against-Alex-Jones-Infowars.html>

Baldauf, J., Ebner, J. and Guhl, J. (eds). (2019) *Hate Speech and Radicalisation Online: The OCCI Research Report*. *Institute for Strategic Dialogue*.

<https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf>

Ballard, J. (2019, October 25). *Teens use these social media platforms the most*. *YouGov America*. *YouGov America*.

<https://today.yougov.com/topics/lifestyle/articles-reports/2019/10/25/teens-social-media-use-online-survey-poll-youth>

Bastiaanse, R. (2019, March 20). *Memes, 4chan And the Strategic Ambivalence of Thierry Baudet*. *Diggit Magazine*.

<https://www.diggitmagazine.com/column/memes-4chan-and-strategic-ambivalence-thierry-baudet>

BBC. (2017, May 31). 'One in two' young online gamers bullied, report finds. <https://www.bbc.co.uk/news/technology-40092541>

Better Business Bureau. (2020, June 10). *BBB Tip: Like-Farming Is a Facebook Scam Still Going Strong*. <https://www.bbb.org/article/news-releases/17149-like-farming-a-facebook-scam-still-going-strong>

Biden Unveils Skin Color Chart to Determine Who Gets Federal Aid. (2021, January 12). *Babylon Bee*. <https://babylonbee.com/news/biden-releases-skin-color-chart-to-determine-who-gets-federal-aid>

Biggs, J., & Tang, C. (2011). Teaching for quality learning at university. (4th Edn.). In *Innovations in Education and Teaching International*. Society for Research into Higher Education and Open University Press. <https://doi.org/10.1080/14703297.2013.839332>

Brown, L. (2021, January 18). German Quarantine Breakers to Be Held in Refugee Camps, Detention Centres. *New York Post*. <https://nypost.com/2021/01/18/german-quarantine-breakers-to-be-held-in-refugee-camps/>

Brzeski, P (2020, May 4). China Mocks Trump's Response to Coronavirus in Lego-Like Animation. *The Hollywood Reporter*. <https://www.hollywoodreporter.com/news/china-mocks-trumps-response-coronavirus-lego-like-animation-1293049>

Capron, A. (2020, January 7). Rescued Koalas and Kangaroos: Five Fake Images from Australia's Fires. *The Observers*. <https://observers.france24.com/en/20200107-rescued-koalas-kangaroos-fake-images-australia-fires>

Carroll, S.B. (2020, November 8). The Denialist Playbook. *Scientific American*. <https://www.scientificamerican.com/article/the-denialist-playbook/>

CBC News. (2016, October 6). *Is Pepe the Frog a Hate Symbol?* YouTube. <https://www.youtube.com/watch?v=lg1Hoi-j6Y&t=43s>

Channel 4. (2020, December 25). The Alternative Christmas Message 2020. Facebook. <https://www.facebook.com/watch/?v=243343943850219>

Child Exploitation Online Protection Command. (n.d.) *Are You Worried About Online Sexual Abuse or The Way Someone Has Been Communicating with You Online?* https://www.ceop.police.uk/safety-centre/?_ga=2.222363292.609605449.1605696094-1834616103.1533735816

Childline. (2014, November 17). Building Confidence After Bullying Online. YouTube. <https://www.youtube.com/watch?v=9HocoOVVUDY>

Childline. (n.d.) *Gaming*. <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-gaming/>

Childnet. (n.d.) *Privacy Settings*. <https://www.childnet.com/young-people/secondary/privacy-settings>

Childnet. (n.d.) *Social Media*. <https://www.childnet.com/young-people/secondary/social-media>

Cho, A., & Byrne J.P.Z. (2020) Digital Civic Engagement by Young People. *UNICEF Office of Global Insight and Policy*. https://www.unicef.org/sites/default/files/2020-07/Digital-civic-engagement-by-young-people-2020_4.pdf

Cuthbertson, A. (2019, February 8). What Is Deepfake Porn? AI Brings Face-Swapping to A Disturbing New Level. *Newsweek*.
<https://www.newsweek.com/what-deepfake-porn-ai-brings-face-swapping-disturbing-new-level-801328>

David Pakman Show. (2017, June 27). Gwyneth Paltrow's Scam Products Called Out by NASA. *YouTube*. <https://www.youtube.com/watch?v=PBHpD-9IoSQ>

Davidson, L. (2018, April 17). Generation Rent: Third of Millennials Face Renting for Their Entire Lives and Never Own Their Own Homes. *The Sun*.
<https://www.thesun.co.uk/money/6069081/third-of-millennials-face-renting-for-their-entire-lives-and-never-own-their-own-homes/>

De Cristofaro, E. (2018, December 12). Memes Are Taking the Alt-Right's Message of Hate Mainstream. *The Conversation*. <https://theconversation.com/memes-are-taking-the-alt-rights-message-of-hate-mainstream-108196>

De Veen, L. and Thomas, R. (2020). Shooting for Neutrality? Analysing Bias in Terrorism Reports in Dutch Newspapers. *Media, War & Conflict* (1-19).
<https://journals.sagepub.com/doi/pdf/10.1177/1750635220909407>

Dearden, L. (2018, December 20). RT Could Be Banned from Broadcasting in UK For Breaching Impartiality Rules. *Independent*.
<https://www.independent.co.uk/arts-entertainment/tv/news/rt-russia-today-ofcom-banned-impartiality-skripal-syria-galloway-propaganda-a8692141.html>

Department for Education. (2014). *Cyberbullying: Advice for Headteachers and School Staff*.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069987/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Directorate-General for Communications Networks, Content and Technology. (2018). *A Multi-Dimensional Approach to Disinformation: Report of The Independent High Level Group on Fake News and Online Disinformation*.
<https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation>

DW English. (2018, April 16). Manipulative Social Bots. *YouTube*.
<https://www.youtube.com/watch?v=e14aK8s4QIA>

Eccles, J. (1983). Expectancies, Values and Academic Behaviors. In J. T. Spence (Ed.), *Achievement and Achievement Motives: Psychological and Sociological Approaches* (pp. 75–146). W.H. Freeman.

Eilperin, J. & Entous, A. (2016, December 31). Russian Operation Hacked a Vermont Utility, Showing Risk to U.S. Electrical Grid Security, Officials Say. *Washington Post*. https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html

European Commission (2020). *Special Eurobarometer 499 Report: Europeans' Attitudes Towards Cybersecurity*. <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2249>

European Union (Migration and Home Affairs. (n.d.) *Cybercrime*.

Evon, D. (2018, July 23). Is This 'Keke Challenge Gone Wrong?' Video Real? *Snopes*. <https://www.snopes.com/fact-check/keke-challenge-gone-wrong/>

Evon, D. (2021, January 26). Is the Cookie Monster Rock Real? *Snopes*. <https://www.snopes.com/fact-check/cookie-monster-rock/>

Facebook. (2022). *Put A Stop to Bullying*. <https://www.facebook.com/safety/bullying/>

Faife, C. (2017, June 1). How 4Chan's Structure Creates a Survival of the Fittest for Memes. *Vice*. <https://www.vice.com/en/article/ywzm8m/how-4chans-structure-creates-a-survival-of-the-fittest-for-memes>

Frampton, B. (2015, September 14). Clickbait: The Changing Face of Online Journalism. *BBC News*. <https://www.bbc.co.uk/news/uk-wales-34213693>

Garrett, R. K., Bond, R. & Poulsen, S. (2019, August 16). Too Many People Think Satirical News Is Real. *The Conversation*. <https://theconversation.com/too-many-people-think-satirical-news-is-real-121666>

Get Safe Online. (2015, June 9). *Fraudsters Use Spoof Texts in New Bank Scam*. <https://www.getsafeonline.org/news/fraudsters-use-spoof-texts-in-new-bank-scam/>

Get Safe Online. (n.d.) *Passwords*. <https://www.getsafeonline.org/protecting-your-computer/passwords/>

Get Safe Online. (n.d.) *Preventing Identity Theft*. <https://www.getsafeonline.org/protecting-yourself/safeguarding-identity/>

Get Safe Online. (n.d.) *Ransomware*. <https://www.getsafeonline.org/protecting-yourself/ransomware/>

Get Safe Online. (n.d.) *Shopping*. <https://www.getsafeonline.org/shopping-banking/shopping1/>

Get Safe Online. (n.d.) *Social Media Phishing*.
<https://www.getsafeonline.org/protecting-your-computer/social-media-phishing/>

Get Safe Online. (n.d.) *Virtual Private Networks*.
<https://www.getsafeonline.org/smartphones-tablets/virtual-private-networks-vpns/>

Greenfield, B. (2020, January 7). Girl in A Gas Mask, Holding A Koala: The Truth Behind That Viral Australian Bush Fires Photo. *Yahoo! Life*.
<https://twitter.com/yahoolife/status/1215947758663880705>

Hafez, M. & Mullins, C. (2015). The Radicalisation Puzzle: A Theoretical Synthesis of Empirical Approaches to Home-Grown Extremism. *Studies in Conflict and Terrorism*, 38, 958–975. <https://doi.org/10.1080/1057610X.2015.1051375>

Hart, M. (2021, January 26). Gemologist Cracks Open Rock, Finds Cookie Monster's Face. *Nerdist*. <https://nerdist.com/article/cookie-monster-rock-discovery-gemologist/>

Hern, A. (2017, April 19). Unicode Trick Lets Hackers Hide Phishing URLs. *The Guardian*. <https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers>

Hern, A. (2020, January 7). Facebook Bans Deepfake Videos in Run-Up to US Election. *The Guardian*.
<https://www.theguardian.com/technology/2020/jan/07/facebook-bans-deepfake-videos-in-run-up-to-us-election>

HM Government. (2016) *National Cyber Security Strategy 2016-2021*.

Home Affairs Select Committee. (2017) *Home Affairs Committee Hate Crime: Abuse, Hate and Extremism Online*.
<https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf>

Home Affairs Select Committee. (2017) *Home Affairs Committee Hate Crime: Abuse, Hate and Extremism Online*.
<https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf>

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en#:~:text=Cybercrime%20consists%20of%20criminal%20acts,communications%20networks%20and%20information%20systems.&text=Crim es%20specific%20to%20the%20Internet,to%20victims'%20bank%20accounts

Hunter, R. (2022, March 20). Pro-Russian Propaganda Spreading in Scots Anti-Vaccine Groups. *The Ferret*. <https://theferret.scot/pro-russia-propaganda-anti-vaccine-white-rose/>

Ibrahim, N. H. B., Aris, S. R. S., & Razek, F. H. A. (2017). The Use of Facebook In ISIS Recruitment-An Exploratory Study. *Journal of Media and Information Warfare*. 10 (51–77). <https://jmiw.uitm.edu.my/images/Journal/v10c3.pdf>

Ignacio, L. (2021, January 28). Cookie Monster Rock Found in Brazil Goes Viral. *NBC*. <https://www.nbcnews.com/news/world/cookie-monster-look-alike-rock-found-brazil-goes-viral-n1255908>

Internet Watch Foundation. (n.d.) *Hello & welcome to our reporting page*. https://report.iwf.org.uk/en?_ga=2.188823852.609605449.1605696094-1834616103.1533735816

Kao, J., & Shuang Li, M. (2020, March 26). How China Built A Twitter Propaganda Machine Then Let It Loose on Coronavirus. *ProPublica*. <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>

Kaspersky. (n.d.) *What Is A Botnet?* <https://www.kaspersky.fr/resource-center/threats/botnet-attacks>

Kaspersky. (n.d.) *What is Spear Phishing?* <https://www.kaspersky.com/resource-center/definitions/spear-phishing>

Kasprak, A. (2021, January 26). Is Germany Planning to Put Quarantine Violators in Detention Centers and Refugee Camps?' *Snopes*. <https://www.snopes.com/fact-check/germany-covid-camps/>

KHOU 11. (2018, July 26). Verify: Woman Hit by Car During 'Keke' Challenge? *YouTube*. https://www.youtube.com/watch?v=gSAz2g-0__w

Kidscape. (n.d.) *Cyberbullying and Digital Safety*. <https://www.kidscape.org.uk/advice/advice-for-parents-and-carers/cyberbullying-and-digital-safety/>

Kidscape. (n.d.) *Top Tips for Dealing with Bullying*. https://www.kidscape.org.uk/media/134268/top-tips-for-schools_final.pdf

Kitchens, B., Johnson, S. L., & Gray, P. (2020). Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption. *MIS Quarterly: Management Information Systems*, 44(4), 1619–1649. <https://doi.org/10.25300/MISQ/2020/16371>

Klausen, J. (2015). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict and Terrorism*, 38(1), 2015, 1–22. <https://doi.org/10.1080/1057610X.2014.974948>

Knight Foundation. (n.d.). *How Much “Fake News” Can We Identify on Twitter?*
<https://knightfoundation.org/features/misinfo/>

Knight, W. (2018, July 18). How to Tell If You’re Talking to A Bot. *MIT Technology Review*. <https://www.technologyreview.com/2018/07/18/141414/how-to-tell-if-youre-talking-to-a-bot/>

Know Your Meme. (2018 [updated 2021]). *Distracted Boyfriend*.
<https://knowyourmeme.com/memes/distracted-boyfriend#photos>

Konnikova, M. (2014, December 17). How Headlines Change the Way We Think. *The New Yorker*. <https://www.newyorker.com/science/maria-konnikova/headlines-change-way-think>

Kulsum. (2022, March 18). False: An Image Shows Three Exhausted Ukrainian Firefighters Amid the Russian Invasion of Ukraine. *Logically*.
<https://www.logically.ai/factchecks/library/bbfe5c51>

Kumar, S. and Shah, N. (2018). *False Information on Web and Social Media: A Survey*. ArXiv, 1(1). <https://arxiv.org/pdf/1804.08559.pdf>

Liang, C. S. (2015). Cyber Jihad: Understanding and Countering Islamic State Propaganda. *GSCP Policy Paper*, 2(4), 2015, 1-12.
<https://www.files.ethz.ch/isn/189426/2015%20%20Cyber%20Jihad.pdf>

Luyken, J. (2021, January 17). Germans Who Keep Refusing to Quarantine Could Be Put in Detention Centres Under New COVID Rules. *The Telegraph*.
<https://www.telegraph.co.uk/news/2021/01/17/germans-keep-refusing-quarantine-could-put-detention-centres/>

Meta Journalism Project. (2021, June 1). How Facebook’s Third-Party Fact-Checking Program Works. *Facebook*.
<https://www.facebook.com/journalismproject/programs/third-party-fact-checking/how-it-works>

MIT Technology Review. (2018, June 11). *This Is Where Internet Memes Come From*. June 11, 2018. <https://www.technologyreview.com/2018/06/11/142394/this-is-where-internet-memes-come-from/>

Montesin, M. (2020, March 10). French Government Confirms That Cocaine Does Not Cure Coronavirus. *Happy Mag*. <https://happymag.tv/french-government-confirms-that-cocaine-does-not-cure-coronavirus/>

Moss, R. (2018, February 9). Gwyneth Paltrow’s Goop Slammed for Telling Women How to Be Their ‘Leanest Liveable Weight’. *Huffington Post*.
https://www.huffingtonpost.co.uk/entry/gwyneth-paltrows-goop-slammed-for-telling-readers-how-to-be-their-leanest-liveable-weight_uk_5a7c1fafe4b0c6726e0f9af8?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANrspXTU945SwADraMYqV7olQuXaGWYAu6CzCiCD1RYCn8cE3PMXvWOy8uaSHfuF8dggcojzwwqaJOIV6wvGD

[mf6GhrsB7kEvl26teq5OTHQB1TCCA4SG_HHoeMliqbZTHEfCwcDWcAQWsihxP7JZ9BT6d22xJSW8Wck5DPx3jIT](#)

Naber, V.I., Lutz, M. & Büscher, W. (2021, January 17). Länder planen Zwangseinweisungen für Corona-Quarantänebrecher. *Welt am Sonntag*. <https://www.snopes.com/fact-check/germany-covid-camps/>

Nakashima, E. & Eilperin, J. (2017, January 2). Russian Government Hackers Do Not Appear to Have Targeted Vermont Utility, Say People Close to Investigation. *Washington Post*. https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5_story.html

National Crime Agency. (n.d.) *Sextortion (Webcam Blackmail)*. <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>

National Cyber Security Centre. (2016, October 27). *Three Random Words or #ThinkRandom*. <https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0>

National Cyber Security Centre. (2017, December 17). *Guidance on Recovering A Hacked Account from The National Cyber Security Centre*. <https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

National Cyber Security Centre. (2018, August 8). *Two-Factor Authentication (2FA): New Guidance from the NCSC*. <https://www.ncsc.gov.uk/blog-post/two-factor-authentication--2fa---new-guidance-from-the-ncsc>

National Cyber Security Centre. (2018, December 21). *Use A Strong and Separate Password for Your Email*. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email>

National Cyber Security Centre. (2018, March 15). *Denial of Service Guidance*. <https://www.ncsc.gov.uk/blog-post/denial-service-guidance>

National Cyber Security Centre. (2021, December 21). *Password Managers: Using Browsers and Apps to Safely Store Your Passwords*. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>

National Cyber Security Centre. (2021, December 21). *Top Tips for Staying Secure Online: Install the Latest Software and App Updates*. <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates>

National Cyber Security Centre. (2021, November 26). *Phishing: Spot and Report Scam Emails, Texts, Websites and Calls*. <https://www.ncsc.gov.uk/collection/phishing-scams>

National Cyber Security Centre. (n.d.) *A Guide to Ransomware*.
<https://www.ncsc.gov.uk/ransomware/home>

National Cyber Security Centre. (n.d.) *NCSC Glossary*.
<https://www.ncsc.gov.uk/information/ncsc-glossary>

National Literacy Trust. (2018). *Fake news and critical literacy: The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools*.
https://cdn.literacytrust.org.uk/media/documents/Fake_news_and_critical_literacy_-_final_report.pdf

National Literacy Trust. (n.d.) *Helping Your Child Understand the News*.
<https://literacytrust.org.uk/family-zone/9-12/newswise-home/>

NBC News. (2019, October 27). Deep Fakes: How They're Made and How They Can Be Detected. *YouTube*. <https://www.youtube.com/watch?v=C8FO0P2a3dA>

New China TV. (2020, April 30). Once Upon A Virus... *YouTube*.
<https://youtu.be/Q5BZ09iNdvo>

Noob Destroyer. (2018, July 31). Girl Hit by Car Doing 'In My Feelings' Challenge. *YouTube*. <https://www.youtube.com/watch?v=SDfIKttkcEA>

O'Leary, Joseph. (2022, March 15). Photograph of Crowded Railway Station Is from Ukraine in March 2022. *Full Fact*. <https://fullfact.org/online/ukraine-crowded-railway-station-black-and-white/>

Observer. (2017, May 1). *Fake News, Sloppy News and Bad News*.
<https://observer.com/2017/01/fake-news-sloppy-news-and-bad-news/>

OECD. (2017). *Use of Internet/Chat/Social Networks Before and After School*.
https://www.oecd-ilibrary.org/education/pisa-2015-results-volume-iii/use-of-internet-chat-social-networks-before-and-after-school_9789264273856-table206-en

Ofcom. (2022, March 2022). *Ofcom Revokes RT's Broadcast Licence*.
<https://www.ofcom.org.uk/news-centre/2022/ofcom-revokes-rt-broadcast-licence>

Panneton, D. (2019, March 22). Online Memes May Seem Frivolous but They Normalize Hate with Potentially Deadly Results. *The Globe and Mail*.
<https://www.theglobeandmail.com/opinion/article-online-memes-may-seem-frivolous-but-they-normalize-hate-with/>

Paul, K. (2019, October 7). California Makes Deepfake Videos Illegal but Law May Be Hard to Enforce. *The Guardian*. <https://www.theguardian.com/us-news/2019/oct/07/california-makes-deepfake-videos-illegal-but-law-may-be-hard-to-enforce>

Perekalin, A. (2019, May 15) Uncovering Fake News Bots. *Kaspersky Daily*.
<https://www.kaspersky.com/blog/fake-news-bots/26943/>

Rawle, T. (2013, October 17). Air pollution now leading cause of lung cancer. *Daily Express*. <https://www.express.co.uk/life-style/health/437473/Air-pollution-now-leading-cause-of-lung-cancer>

Reardon, M. (2019, October 23). Facebook's Zuckerberg Gets Grilled Over Political Ad Policy. *CNET*. <https://www.cnet.com/news/politics/facebooks-zuckerberg-gets-grilled-over-political-ad-policy/>

Revenge Porn Helpline. (n.d.) *Help and Support for Under 18s*. <https://revengepornhelpline.org.uk/how-can-we-help/under-18s/>

Revenge Porn Helpline. (n.d.) *What to Do If You Have Had Intimate Images Shared Online Without Your Consent*. <https://revengepornhelpline.org.uk/information-and-advice/need-help-and-advice/intimate-images-shared-without-consent/>

Rubin, A. (2020, February 4). Wow! This Child Actress is All Grown Up, and You Won't Believe How Much She Hates Your Obsessions with What She Looks Like Now. *Reductress*. <https://reductress.com/post/wow-this-child-actress-is-all-grown-up-and-you-wont-believe-how-much-she-hates-your-obsession-with-what-she-looks-like-now/>

Schneider, O., & Sabourian, C. (2018). Policing the internet – 'fake news' and social media offence update. *Kingsley Napley*. <https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/policing-the-internet-fake-news-and-social-media-offence-update>

Sindermann, C., Elhai, J. D., Moshagen, M., & Montag, C. (2020). Age, Gender, Personality, Ideological Attitudes and Individual Differences in A Person's News Spectrum: How Many and Who Might Be Prone To "Filter Bubbles" and "Echo Chambers" Online? *Heliyon*, 6(1). <https://doi.org/10.1016/j.heliyon.2020.e03214>

Smith, A. (2020, November 6). What is Section 230 and Why Does Trump Want It Revoked? *The Independent*. <https://www.independent.co.uk/life-style/gadgets-and-tech/features/trump-section-230-twitter-us-government-b1644936.html>

Staines, C. (2018, May 9). When Headlines Aren't Quite as They Seem. *Full Fact*. <https://fullfact.org/blog/2018/may/headlines-arent-quite-as-they-seem/>

Stemwedel, J.D. (2011, October 4) Drawing the Line Between Science and Pseudo-Science. *Scientific American*. <https://blogs.scientificamerican.com/doing-good-science/drawing-the-line-between-science-and-pseudo-science/>

Stonewall and Childnet. (2021). *Staying Safe Online: Practical Strategies to Best Support All Children and Young People Online, Including Those Who Identify as LGBT*. https://www.stonewall.org.uk/sites/default/files/a4_toolkit_staying_safe_online_2021-update.pdf

Tardaguila, C. (2019, December 17). *Starting Today, Facebook Will Have A Team of Community Reviewers Working in the U.S.* Poynter. <https://www.poynter.org/fact-checking/2019/starting-today-facebook-will-have-a-team-of-community-reviewers-working-in-the-u-s/>

The Diana Award. (n.d.) *Imagine: A School Free from Bullying.* <https://www.antibullyingpro.com/>

The Telegraph. (2019, November 12). Jeremy Corbyn Urges Voters to Back Boris Johnson for Prime Minister in Disturbing Deepfake Video. *YouTube.* <https://www.youtube.com/watch?v=EknjAeHFAk>

Think U Know. (n.d.) *Joining Social Media.* https://www.thinkuknow.co.uk/11_18/lets-talk-about/socialising-online/joining-social-media/

True Vision. (n.d.) *Internet Hate Crime.* https://www.report-it.org.uk/reporting_internet_hate_crime

Trump Blames Nation's Susceptibility to Coronavirus Outbreak on Weakness of America's Race-Muddled Gene Pool. (2020, May 11). *The Onion.* <https://www.theonion.com/trump-blames-nation-s-susceptibility-to-coronavirus-out-1843392614>

UK Safer Internet Centre. (n.d.) *Professionals Online Safety Helpline.* <https://www.antibullyingpro.com/https://saferinternet.org.uk/professionals-online-safety-helpline>

UK Safer Internet Centre. (n.d.) *Helping Children and Young People Stay Safe Online.* <https://saferinternet.org.uk/>

Ume, C. (2021, March 5). DeepTomCruise TikTok Breakdown. *YouTube.* <https://www.youtube.com/watch?v=wq-kmFCrF5Q>

UNESCO. (2018). *Journalism, 'Fake News' & Disinformation: Handbook for Journalism Education and Training.* <https://unesdoc.unesco.org/ark:/48223/pf0000265552>

University of Amsterdam. (2020, August 24). *Would you fall for a fake video? UvA Research Suggests You Might.* <https://www.uva.nl/en/content/news/press-releases/2020/08/would-you-fall-for-a-fake-video-uva-research-suggests-you-might.html?cb&cb>

Van Ouytsel, J., Punyanunt-Carter, N. M., Walrave, M., & Ponnet, K. (2020). Sexting within young adults' dating and romantic relationships. *Current Opinion in Psychology*, 36, 55–59. <https://doi.org/10.1016/j.copsyc.2020.04.007>

Victims of Image Crime. (n.d.) *Victims of Image Crime: Speak Out!* <https://voic.org.uk/>

Vijaykumar, S. (2019, August 7). Pseudoscience Is Taking Over Social Media and Putting Us All at Risk. *The Independent*.
<https://www.independent.co.uk/news/science/pseudoscience-fake-news-social-media-facebook-twitter-misinformation-science-a9034321.html>

Villas-Boas, A. (2019, November 30.) China Is Trying to Prevent Deepfakes With New Law Requiring That Videos Using AI Are Prominently Marked. *Business Insider*. <https://www.businessinsider.com/china-making-deepfakes-illegal-requiring-that-ai-videos-be-marked-2019-11?r=US&IR=T>

Which. (2021, November 15). *How to Spot A Fake, Fraudulent or Scam Website*.
<https://www.which.co.uk/consumer-rights/advice/how-to-spot-a-fake-fraudulent-or-scam-website>

Wilding, A. (2020, March 10). How to Use Fake News Critically in The Classroom. *British Council*. <https://www.britishcouncil.org/voices-magazine/use-fake-news-classroom-critically>

Wilson, C. (2020, January 14). False and Misleading Information Is Spreading Online About the Aussie Bushfires. Here's What's Real and What's Not. *Buzzfeed News*. <https://www.buzzfeed.com/cameronwilson/unverified-false-information-list-australian-bushfires?bfsource=relatedmanual>



Social
Innovation

Interreg 2 Seas project ORPHEUS

Social innovation

