RELATIONSHIPS EDUCATION

MODULE E
Online Relationships

O37 - Recognising and reporting risks and harmful content

Year 5
Summer Term: Lesson 3

Lesson Overview

Lesson 3: Recognising and reporting risks and harmful content

Engage & Activate	Whole Class & Paired Activities	What are risks?	 **15 minutes**
Explore & Explain	Group Activity	Types of online risks	 **15 minutes**
Elaborate & Reflect	Whole Class & Group Activities	Reducing risks	 **20 minutes**
Evaluate & Review	Whole Class & Paired Activities	Review learning	 **10 minutes**

Lesson Plan

Lesson 3: Recognising and reporting risks and harmful content

Aim	To recognise and manage risks and harmful content

Lesson Objectives

In this lesson pupils will:

Explore what is meant by risk

Consider the types of risks they may encounter online

Explain how to manage risks associated with being online

Learning Outcomes

By the end of this lesson pupils will have:

Defined and given examples of general and online risks

Considered how to reduce risks online

Discussed how to report content which is upsetting, harmful and hateful

Key Vocabulary

cyber | scam | malware | phishing

Resources

 Highlighters

 Pens / Pencils

 Resource sheets

Lesson Plan

Engage & Activate

Lesson 3: Recognising and reporting risks and harmful content

Whole Class & Paired Activities

What are risks?

Introduce learning objectives and learning outcomes.

Discuss key vocabulary and **share** definitions from below.

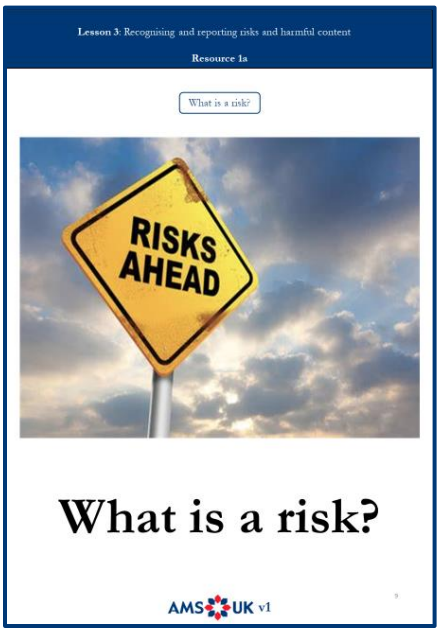
Display Resource 1a.

Ask pupils: What is a risk?

Write pupil responses on the whiteboard.

Explain that a risk is being exposed to harm or danger. If we do something risky there is a possibility of something bad happening to us or others.

Give an example of managing risk:
Before a class go on a school trip, the class teacher makes the journey first to the location in order to assess the risks and to decide if it's safe enough to take you, e.g., risk of tripping when stepping off the coach; risk of getting lost due to crowds etc.



Key vocabulary

cyber	involving, using, or relating to computers, especially the internet
scam	an illegal plan for making money, especially one that involves tricking people
malware	software that is designed to damage the way a computer works
phishing	an attempt to trick someone into giving information over the internet or by email that would allow someone else to take money from them, for example by taking money out of their bank account

Lesson Plan

Engage & Activate

Lesson 3: Recognising and reporting risks and harmful content

Whole Class & Paired Activities

What are risks?

Explain that just like physical risks around us there are also many risks associated with using the internet that we need to be aware of and manage.

Ask pupils, to discuss in pairs examples of:

- physical risks
- online risks
- risks that we could face physically and online (e.g. falling for scams)

Take feedback and **discuss** answers.

Lesson Plan

Explore & Explain

Lesson 3: Recognising and reporting risks and harmful content

Group Activity

Types of online risks

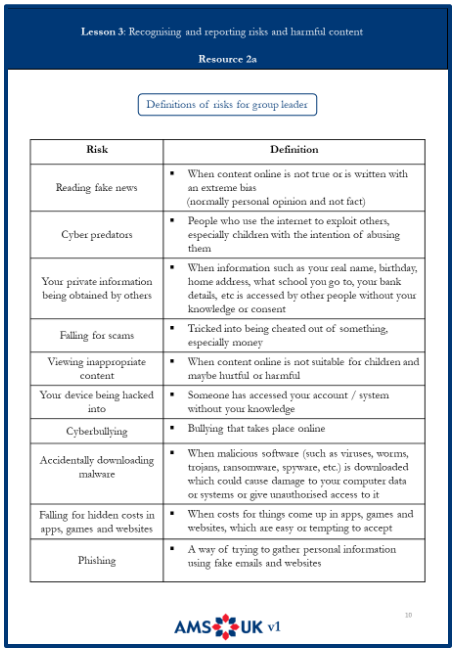
Split class into groups of **five**.

Appoint a group leader for each group and give him/her **Resource 2a**: Definitions of risks.
Group leader does **not share** this with the rest of the group.

Give each group **one** copy of **Resource 2b**: Risks online.

Group leader **reads** out each definition from **Resource 2a** and group members **choose** the risks from **Resource 2b** which match each definition read out.

Take feedback and **explain** any terminology not understood.



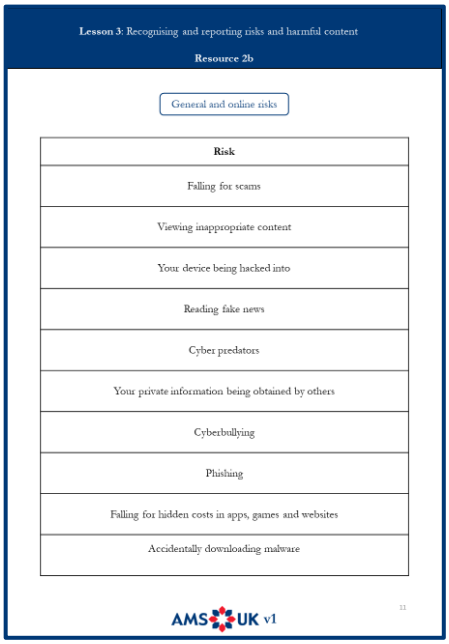
Lesson 3: Recognising and reporting risks and harmful content

Resource 2a

Definitions of risks for group leader

Risk	Definition
Reading fake news	▪ When content online is not true or is written with an extreme bias (normally personal opinion and not fact)
Cyber predators	▪ People who use the internet to exploit others, especially children with the intention of abusing them
Your private information being obtained by others	▪ When information such as your real name, birthday, home address, what school you go to, your bank details, etc is accessed by other people without your knowledge or consent
Falling for scams	▪ Tricked into being cheated out of something, especially money
Viewing inappropriate content	▪ When content online is not suitable for children and maybe hurtful or harmful
Your device being hacked into	▪ Someone has accessed your account / system without your knowledge
Cyberbullying	▪ Bullying that takes place online
Accidentally downloading malware	▪ When malicious software (such as viruses, worms, trojans, ransomware, spyware, etc.) is downloaded which could cause damage to your computer data or systems or give unauthorised access to it
Falling for hidden costs in apps, games and websites	▪ When costs for things come up in apps, games and websites, which are easy or tempting to accept
Phishing	▪ A way of trying to gather personal information using fake emails and websites

AMS UK v1



Lesson 3: Recognising and reporting risks and harmful content

Resource 2b

General and online risks

Risk
Falling for scams
Viewing inappropriate content
Your device being hacked into
Reading fake news
Cyber predators
Your private information being obtained by others
Cyberbullying
Phishing
Falling for hidden costs in apps, games and websites
Accidentally downloading malware

AMS UK v1

Lesson Plan

Elaborate & Reflect

Lesson 3: Recognising and reporting risks and harmful content

Whole Class & Group Activities

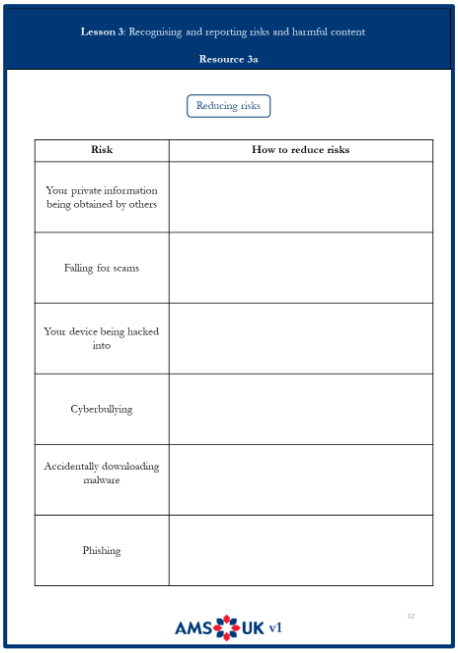
Reducing risks

Give each group **Resource 3a**.

Ask pupils how they can reduce risk online- for example we can reduce the risk of falling for a scam by not responding to uninvited contacts, even if they are telling us we have won lots of money.

In groups, pupils **consider** how to reduce risks for each item on **Resource 3a**.

Take feedback using **Resource 3b** to guide discussion.



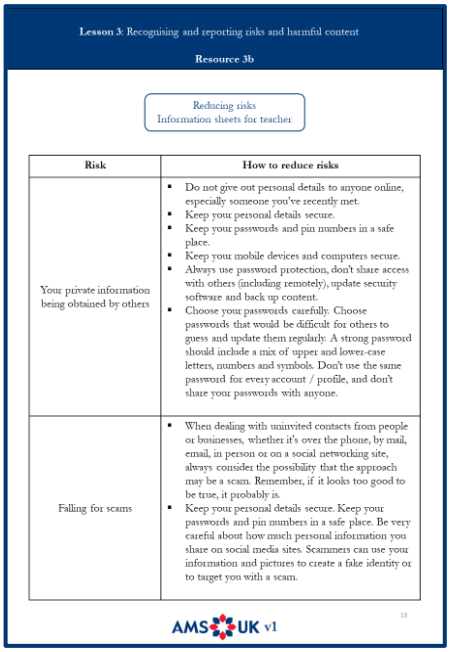
Lesson 3: Recognising and reporting risks and harmful content

Resource 3a

Reducing risks

Risk	How to reduce risks
Your private information being obtained by others	
Falling for scams	
Your device being hacked into	
Cyberbullying	
Accidentally downloading malware	
Phishing	

AMS UK v1



Lesson 3: Recognising and reporting risks and harmful content

Resource 3b

Reducing risks
Information sheets for teacher

Risk	How to reduce risks
Your private information being obtained by others	▪ Do not give out personal details to anyone online, especially someone you've recently met. ▪ Keep your personal details secure. ▪ Keep your passwords and pin numbers in a safe place. ▪ Keep your mobile devices and computers secure. ▪ Always use password protection, don't share access with others (including remotely), update security software and back up content. ▪ Choose your passwords carefully. Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower-case letters, numbers and symbols. Don't use the same password for every account / profile, and don't share your passwords with anyone.
Falling for scams	▪ When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is. ▪ Keep your personal details secure. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

AMS UK v1

Discuss what pupils would do if they were to see content which is upsetting, harmful and hateful.

Explain that they should **talk about it** (speak to a trusted adult) and **report it**.

Use the teacher notes from **Resource 4** to support your discussion.

Lesson Plan

Evaluate & Review

Lesson 3: Recognising and reporting risks and harmful content

Whole Class & Paired Activities

Review learning

Explain that in addition to doing all the other things mentioned in this lesson to stay safe online, we should also ask Allah to protect us from all types of harm as there is no protection without His protection.

This is an important du'a for protection that we should read **three** times in the morning (after Fajr prayer) and **three** times in the evening (after Asr prayer.)

بِسْمِ اللهِ الَّذِي لَا يَضُرُّ مَعَ اسْمِهِ شَيْءٌ فِي الأَرْضِ وَلَا فِي السَّمَاءِ وَهُوَ السَّمِيعُ الْعَلِيمُ

'(I seek protection) in the Name of Allah, the Name with which nothing in the Heavens and Earth can be harmed and He is the All-Hearing, the All-Knowing.'

Abu Dawood

Review learning by referring to learning objectives and learning outcomes.

Pose questions to check understanding and clarify misconceptions using **think, pair, share**:

- What is a risk?
- Tell me **three** online risks.
- Name **one** way I can reduce online risks.
- What should you do if you feel unsafe or have seen harmful content on the internet?

What is a risk?

What is a risk?

Definitions of risks for group leader

Risk	Definition
Reading fake news	▪ When content online is not true or is written with an extreme bias (normally personal opinion and not fact)
Cyber predators	▪ People who use the internet to exploit others, especially children with the intention of abusing them
Your private information being obtained by others	▪ When information such as your real name, birthday, home address, what school you go to, your bank details, etc is accessed by other people without your knowledge or consent
Falling for scams	▪ Tricked into being cheated out of something, especially money
Viewing inappropriate content	▪ When content online is not suitable for children and maybe hurtful or harmful
Your device being hacked into	▪ Someone has accessed your account / system without your knowledge
Cyberbullying	▪ Bullying that takes place online
Accidentally downloading malware	▪ When malicious software (such as viruses, worms, trojans, ransomware, spyware, etc.) is downloaded which could cause damage to your computer data or systems or give unauthorised access to it
Falling for hidden costs in apps, games and websites	▪ When costs for things come up in apps, games and websites, which are easy or tempting to accept
Phishing	▪ A way of trying to gather personal information using fake emails and websites

Resource 2b

General and online risks

Risk
Falling for scams
Viewing inappropriate content
Your device being hacked into
Reading fake news
Cyber predators
Your private information being obtained by others
Cyberbullying
Phishing
Falling for hidden costs in apps, games and websites
Accidentally downloading malware

Reducing risks

Risk	How to reduce risks
Your private information being obtained by others	
Falling for scams	
Your device being hacked into	
Cyberbullying	
Accidentally downloading malware	
Phishing	

Reducing risks:
Information sheets for teacher

Risk	How to reduce risks
Your private information being obtained by others	▪ Do not give out personal details to anyone online, especially someone you've recently met. ▪ Keep your personal details secure. ▪ Keep your passwords and pin numbers in a safe place. ▪ Keep your mobile devices and computers secure. ▪ Always use password protection, don't share access with others (including remotely), update security software and back up content. ▪ Choose your passwords carefully. Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower-case letters, numbers and symbols. Don't use the same password for every account / profile, and don't share your passwords with anyone.
Falling for scams	▪ When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is. ▪ Keep your personal details secure. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

Reducing risks:
Information sheets for teacher

Risk	How to reduce risks
Your device being hacked into	▪ Turn off anything you don't need. Hackers can use certain features on your phone to get at your information, location or connection. So, instead of keeping your GPS, wireless connection and geo-tracking on all the time, just turn them on when you need them. ▪ Only download apps from trustworthy sources that have established a good reputation. Make sure you update your software and apps regularly and get rid of old apps you don't use. ▪ Use a password, lock code or encryption on all devices. Make sure you have good passwords and never use the auto-complete feature for passwords. Use the storage encryption feature on your phone to protect your private data and set your screen to timeout after five minutes or less.
Cyberbullying	▪ Have a private account and allow comments only from and to known friends. ▪ Do not respond and tell a trusted adult immediately, if this happens. ▪ Spend more time in real life, so that problems in virtual life do not become your only reality.

Reducing risks:
Information sheets for teacher

Risk	How to reduce risks
Accidentally downloading malware	▪ Keep your computer and software updated. ▪ Think twice before clicking links or downloading anything. ▪ Be careful about opening email attachments or images. ▪ Don't trust pop-up windows that ask you to download software. ▪ Limit your file-sharing. ▪ Use antivirus software.
Phishing	▪ Be cautious about all communications you receive. If it appears to be a phishing communication, do not respond. Delete it. ▪ Do not click on any links listed in the email message, and do not open any attachments or pop-ups. ▪ Install a phishing filter on your email application and also on your web browser. These filters will not keep out all phishing messages, but they will reduce the number of phishing attempts.

What should you do if you see content which is upsetting harmful and hateful – teacher notes

Talk about it

Speak to an adult you can trust about what you've seen. It could be a family member, teacher or youth worker. They might be able to help clear things up and sort out your concerns. If you stumbled across something online by accident, that adult may have some tips for how to avoid seeing that upsetting thing in the future. They can also help you find the report button on a site. If you don't have anyone you can speak to at home or school, there are services you can call, email or chat to online such as Childline, Childnet and NSPCC. Contacting these organisations is free and confidential. These services are there to listen and help you with what to do next. They won't try to stop you from going online, and you won't be in trouble if you found the worrying content on a site, you're not old enough to go on.

Report it

If you've seen something online that makes you feel uncomfortable or that upsets you, it's important to report it where you can. If it's on social media, you can find our list of where to do this on the following webpage:

- https://www.bbc.com/ownit/dont-panic/reporting-issues-social-media

You can report YouTube, Instagram, Snapchat, TikTok, Twitter, etc.
Reporting content won't mean you can't access the site in future, but it will alert the platform that this content is something to take a bigger look at. It will also help you stop seeing content like it again. If you see something on a website that you're really worried about, there are a few places you can report this to, if you want to take matters further. You can find them listed on the Safer Internet Centre's website:

- https://www.saferinternet.org.uk/advice-centre/need-help

Try to talk to an adult you can trust about what you've seen, so that they can help you to report it.

Reference: taken from BBC Own It:

- https://www.bbc.com/ownit/dont-panic/what-to-do-if-you-see-something-upsetting-online

TEACHER NOTES

Schools may cover some of this content in ICT.

For those pupils who have not covered this content in ICT, this lesson will introduce a lot of new vocabulary and terminology

Because of this, teachers may decide to cover this lesson over **two** lessons or at least set aside additional time to ensure learning is embedded.