Lesson 1: Causes of Cybercrime

Key stage 3: Year 8

This is the first of two lessons on cybercrime, designed with the support of the National Crime Agency (NCA) and National Cyber Crime Unit (NCCU), which explore the causes and effects of cybercrime for young people and increase their resilience to cybercrime.

Learning objective

- To learn about the causes of cybercrime

Learning outcomes

By the end of the lesson, students will be able to:

- describe what cybercrime is, using key terms
- evaluate the reasons why someone may become involved in cybercrime
- describe or demonstrate decision making and risk assessment skills in relation to cybercrime

Climate for learning

Make sure you have read the accompanying teacher guidance notes before teaching this lesson for guidance on establishing ground rules, the limits of confidentiality, communication and handling questions effectively.

Resources required

- Box or envelope for anonymous questions
- Lesson 1: PowerPoint
- Resource 1: Explain to an alien
- Resource 2: Code breaker
- Resource 3: Bobbie's story

Key words

Cybercrime, hacking, DDoS, modding

Activity	Description	Timing
1. Introduction	Outline the objectives, outcomes and ground rules.	-
2. Baseline assessment	Students explain their current understanding of cybercrime to an alien using 4 prompt questions	10min
3. Code breaker	Students 'crack the code' to decipher the definition of cybercrime	5min
4. Idea shower	In 2 groups, students suggest either examples of cybercrime or reasons why someone might commit cybercrime	10min
5. Bobbie's story	Introduce Bobbie's story using the chat log and take a class vote about Bobbie's choices	15min
6. Analysing Bobbie's story	Students respond to questions exploring Bobbie's motives	10min
7. Signpost support	Ensure students are aware of support services related to cybercrime	5min
8. Endpoint assessment	Summarise student progress using a 3, 2, 1 exit card	5min

Baseline assessment

Introduction

Revisit ground rules and remind students of the anonymous question box where they can submit questions during the lesson. Share the learning objectives and outcomes with students using slide 2.

Baseline assessment activity

Using **PPT slide 3**, ask students to imagine they are explaining what they know about cybercrime to an alien. On **Resource 1: Explain to an alien** students respond to the following questions:

- What is cybercrime?
- What sort of crimes can be committed online?
- Why might someone get involved in cybercrime?
- What are the consequences of cybercrime?

Collect the sheets in and keep them until next lesson, when students will revisit this baseline activity.

Core activities

Code breaker

Hand out **Resource 2: Code breaker** (also on **slide 4**) and ask students to crack the code to work out the definition of cybercrime. Once students have had some time to work out the puzzle, share the definition with students using **slide 5**.

NB: It may be necessary when defining cybercrime to highlight the difference between cyber-enabled-crime (such as hacking, DDoSing, identity theft) which this lesson will focus on, and other more general online safety issues that students may have raised (such as grooming, bullying or trolling).

Idea shower: crimes & causes

Split the class in half. Now that they know the definition of cybercrime, ask one half of the class to list as many cybercrimes as they can think of. Ask the other half of the class to list the reasons why people might commit cybercrime.

This task could also be completed in pairs, asking one student in each pair to focus on either examples or reasons why.

Take feedback, highlighting some of the following answers:

Examples of cybercrimes: hacking a website, data theft, disabling websites (DDoS), identity theft (see also teacher guidance document)

Possible reasons for cybercrime: for political reasons, for money, for power or control, peer influence, demonstrating skills, because it feels 'risk free' 'victimless' and 'anonymous' (it is important to emphasise that these are misconceptions).

Challenge

Students are likely to find it more challenging to suggest reasons why someone might commit cybercrime.

15 Bobbie's story

Take the class through Bobbie's story using slides 7-11. You could ask two volunteers to read out the chat log as each character.

Slide 12: Allowing the students 30 seconds to reflect and make their decision, take a class vote (using thumbs up/thumbs down or green/red cards if available) at the end of the chat log – Is Bobbie making a good decision?

Ask for volunteers to explain their reasons why they have voted either yes or no.

Some reasons to emphasise during this discussion might include:

Bobbie is breaking the law and at risk of being caught by police (which could have an impact on his future career, that Bobbie has been persuaded to do this by someone else he doesn't really know, the damage to the bank as a business (in terms of reputation, future security, cost), the impact on customers who will lose trust in the bank and who might think their money and personal details are unsafe.

10 Analysing Bobbie's story

Hand students **Resource 3: Bobbie's story** (this is a printed version of the conversation).

Ask students to analyse Bobbie's story using the questions on slide 13:

I. What techniques did H@cktor use to convince Bobbie to take down the bank's website?
II. What do you think convinced Bobbie to agree?
III. What do you think H@cktor's reasons are for wanting to take down the bank's website?
IV. When during the conversation could Bobbie have made a different decision or acted differently?

Students may identify:

i. Switching between flattery and insults, using inclusive language "us", suggesting hacking will lead to power & control, emphasising the challenge and skills required, minimising the risk, claiming Bobbie will be respected by the hacking forum, using emotive language "hero" etc.

ii. Could have been any of the factors above, although gaining respect from other hackers seemed to be the deciding factor.

iii. It's important to point out that we don't know much about who H@cktor is and so his motives are unclear. It may be for political reasons; however, this is not a justifiable reason to break the law. Often people on anonymous hacking forums are there for their own gain, and could even be part of a criminal gang. Getting involved in an act such as taking down a bank's website is highly dangerous for a young person and H@cktor is transferring these criminal risks from himself to Bobbie. It is at least possible that while the bank's website is disabled other cybercriminals could launch a cyber-attack on the bank, which would cause more damage to the bank's reputation and threaten the security of their customer's personal details.

iv. The most important point is that Bobbie is free to exit the conversation at any time. As soon as he begins to feel worried or uncertain, he should remove himself from the chat. The conversation takes a darker turn when H@cktor starts talking about 'Power' and cyberwars, which should be a warning sign to Bobbie, and he is clearly uncomfortable with the chat. When Bobbie raises initial concerns, H@cktor stops replying, this would be another good moment to exit the chat.

> *NB: Teachers may want to go through the chatlog as a class for a second time, highlighting all the possible warning signs to ensure the class has identified them all (some are much more subtle than others) and pointing out that anything that causes a person concern in a conversation is an indicator to leave the chat.*

Challenge

A challenge question has been provided on slide 13 to map Bobbie's emotions through the conversation.

Support:

Students could highlight on resource 3 where they think H@cktor is trying to convince / manipulate Bobbie. Teachers may wish to direct students to focus on particular phrases, such as:

- *"Sounds like ur ready for a new challenge"*
- *"Bet you've not done anything big though or we'd have heard about it"*
- *"Should have known ud be scared. Dunno why I invited u to this forum. 4get it. Just stick to ur easy little hacks & playing ur little games"*
- *"You'll be a HERO if you can take down one of those smug high street banks"*

Plenary/ Assessment of learning

Endpoint assessment

Use an exit card to demonstrate students' progress. Students should complete the following:

- 3 things I learnt today
- 2 skills I have developed in this lesson
- 1 question I still have about cybercrime

These responses should be handed to the teacher as students leave the room. Ensure these are kept for the next lesson, when the questions will be revisited.

Reflecting on today's learning & signposting support

Using **slide 14**, highlight sources of support for young people, including both anyone who thinks they may have been a target of cybercrime, or anyone who thinks they might have perpetrated (or been encouraged to perpetrate) a cybercrime.

**Sources of support should include both in-school support and local or national organisations.*

Extension activity

Supporting others

Ask students to carry out research (or create their own ideas) about how people can protect themselves online from cyber-attacks. They could create a top-ten list of tips or design posters to raise awareness around school. Recommended websites for research include:

- https://www.childnet.com/young-people
- https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/

Giving advice

Ask students to imagine they are writing an email to someone who has been a victim of cybercrime. They should offer them advice about what to do next and where to seek additional support.