6.Protecting yourself from online scams

Video summary

A short classroom film for secondary schools introducing students to the key skills needed to recognise potentially harmful online scams. In the film, presenter and documentary filmmaker James Blake explains some common scamming techniques (for example, sending you a direct message that plays to your emotions and encourages you to click on a link), arming students with the ability to identity online risks and respond appropriately.

The film also describes the 'sextortion' scam, for which advice for teachers is provided below. Please read this and view the film before showing it to your class.

Before watching

Establish a safe learning environment. Remind students that being scammed online is common, and the goal is to learn strategies, not judge others. Encourage students to focus on general online behaviour rather than sharing sensitive experiences.

In preparation for watching the film in class, ask students to:

- Think about a time they received a suspicious email, message, or link. What made it seem suspicious? How did they respond?
- List different types of online scams or threats they know about. Can they name three ways scammers might try to trick someone online?
- Prompt students to consider the information they share online. What personal information do they share on social media, apps, or websites, and who might be able to see it?

Please note that the video explains the 'sextortion' scam and we advise watching it before sharing it with your class. Teachers should approach these topics carefully to ensure students feel safe, supported, and informed, rather than fearful or silenced.

Sextortion is a form of online blackmail where someone is coerced or threatened into sharing sexual images, money or information online, and under UK law it is illegal and treated as a serious safeguarding and criminal matter, with the law designed to protect victims rather than punish them for coming forward.

In line with *Keeping Children Safe in Education (KCSIE)*, you should:

- Explain that sextortion is a form of abuse and exploitation, and victims are never to blame.
- Use hypothetical scenarios only and avoid encouraging students to share personal experiences in class.
- Reassure students that seeking help is always the right thing to do and that the law exists to protect children, not punish them.

Teachers should make clear that:

- Sextortion is illegal and often involves criminal exploitation. It can be reported to the police.
- Students who report concerns will not get into trouble for speaking to a trusted adult.

If a student makes a disclosure, teachers must:

- Not promise confidentiality
- Listen and reassure
- Follow the school's safeguarding procedures and pass concerns to the Designated Safeguarding Lead (DSL) without delay.

Across Bitesize, we advise young people that they should always tell someone about the things they're worried about. They could tell a friend, parent, guardian, teacher, or another adult they trust. If they're struggling with their mental health, going to a GP can be a good place to find help. A GP can outline the support available, suggest different types of treatment and offer regular check-ups

If young people are in need of urgent support there are links to helpful organisations on **BBC Bitesize Action Line**.

While watching

There are 'pause points' in the video for students to engage in tasks. You can either pause at these suggested points (you will need to manually pause the video to give your students enough time to complete these tasks) or watch the film through and try the activities afterwards.

Activity 1

The first task requires students to discuss what emotion three direct online messages are trying to trigger:

Message 1
From: GiveawayOfficial
Message: 🥳 CONGRATULATIONS! 🥳 You've been randomly selected as one of our 10 lucky winners! You've won a £500 gift card to spend on anything you want. Claim your prize before it expires in 1 hour!

Message 2
From: Account Support
Message: ⚠️ URGENT SECURITY ALERT: We've detected an unusual login to your account from an unrecognised device. To prevent immediate suspension, you must verify your identity by logging in here...

Message 3
From: User8431
Message: Hey, this is a bit random but I think I've seen you around? Someone made a secret profile about you, it's kinda cute lol. I can't believe what they wrote, see for yourself...

Possible student responses:

Message 1 – aims to make the recipient feel lucky and excited. It creates time pressure, triggering a fear of missing out and prompting impulsive action.

Message 2 – aims to create fear, anxiety and urgency. The threat of account loss or compromise is designed to make the recipient act quickly without thinking critically.

Message 3 – plays on intrigue and the desire for social approval. It also uses casual, friendly language to reduce suspicion, encouraging the recipient to click the link.

Give students a maximum off five minutes for discussion followed up with whole class feedback.

Activity 2

In the second activity, students will analyse some mock social media posts to identify all the red flags (e.g. suspicious links, urgent language, bad grammar, or anything that just feels a bit off). They can then build a checklist of what makes a safe and reliable post.

Possible checklist:

- Unrealistic promises or rewards
- Urgency / pressure to act quickly
- Requests for personal information or money
- Unverified or suspicious links / websites
- 'Too good to be true'
- Unsolicited contact
- Emotional manipulation
- Poor spelling and grammar
- Overuse of emojis or hype language

After watching

Provide students with a set of example messages, posts, or emails (school-appropriate). Challenge students to identify the red flags in each and explain why they are suspicious and suggest how they would pause and respond safely.

Ask students to create a short plan for staying safe online. This could include:

- How to check links and verify sources
- Ways to protect personal information
- Steps to take if they suspect a scam

Where next?

BBC Bitesize's Other Side of the Story resources are designed to help students navigate fake news and misinformation and be more critical and curious about what they see and share online.

There are several relevant pages relating to online scams that you could set students for independent study or explore as a class:

- How to spot a scam
- How to outsmart scammers
- BBC Scam Safe quiz: How scam savvy are you?

Curriculum notes

This film will be relevant for several curriculum areas:

Citizenship and PSHE Key Stage 3 and 4: teaches online safety, digital wellbeing, and managing personal information; helps students understand risks, develop resilience, and make responsible decisions online; links to understanding financial scams, personal security, and protecting privacy; connects to understanding rights and responsibilities in digital spaces; promotes awareness of scams, fraud, and online manipulation as societal issues; encourages students to act responsibly online and help others stay safe.

Computing Key Stage 3 and 4: develops digital literacy and cybersecurity awareness; encourages critical thinking about online content, links, and messages; supports safe and ethical use of technology, including protecting accounts and personal data.

English Key Stage 3 and 4: helps students analyse persuasive language, attention-grabbing tactics, and emotional manipulation; supports critical evaluation of messages, posts, or adverts in digital media.