

Identity Exposed

EXERCISE-IN-A-BOX LESSON PLAN

OVERVIEW

This lesson educates students about online harassment forms such as trickery, doxxing, and cyberstalking, emphasising the importance of responsible and respectful online behaviour. Students will develop skills and strategies to protect themselves and their peers from online harm.

LEARNING OBJECTIVES

Students will be able to:

- Explain the concept of cyberstalking and doxxing, and how they can be used to harass and intimidate individuals online.
- Analyse the tactics of trickery, such as pretending to be someone else online to gain information, and the malicious intentions behind such behaviour.
- Understand the importance of taking steps to protect oneself from anonymous online attacks, especially in keeping personal information private.

DURATION

60 minutes + project work (duration as needed)

KEYWORDS

- **Trickery:** When someone uses deception or lies in order to trick someone else into giving them sensitive information, such as passwords, personal details, or even secrets.
- **Doxxing:** When someone publicly shares private and personal information about someone else, such as their full name, address, phone number, or other identifying details. This form of cyberbullying is extremely dangerous as it can make the person vulnerable or exposed.
- **Cyberstalking:** When someone repeatedly uses technology to harass, intimidate, or threaten another person. This can include things like sending repeated or threatening messages, following someone's online activity, or posting harmful or false information about them.

INTERNET INDEPENDENT FRAMEWORK

The learning objectives in this workshop are aligned with the **Cyberbullying & Abuse** pillar of the Internet Independent Framework. Visit cyberlite.org for more information.

Identity Exposed

EXERCISE-IN-A-BOX LESSON PLAN



WARM-UP 5 MINUTES

Slide 1

Say: Today, we will be discussing cyberbullying and abuse, particularly on instances when you are interacting with anonymous online users. As you get older, you get to experience more parts of the online world - from entertainment to social media and games. In this lesson you will be learning how your private information can make you vulnerable online and why you should always practise cyber safety.

Slide 2

Ask: What types of personal information should you never share online?
You should never share your full name, address, identification number, or any other personally identifiable information that can be used to locate you.

Slide 3

Ask: Do you think it's ever okay to post someone else's personal information online without their permission?
No, it is never okay to expose someone's personal information as it infringes on their right to privacy.



DEFINE THE KEYWORDS 15 MINUTES

Slide 4

Ask: Does anyone know what trickery, doxxing, or cyberstalking mean?
Allow students to guess or extrapolate meanings. Guide them to think about it in the lesson's context of cyberbullying.

Slide 5

Read the contents of the slide aloud.

Discuss: What are some motivations a bully might have to use trickery?
Trickery is a form of betrayal that happens often on social media or in text messages with this age group. There are many reasons why a cyberbully might use trickery to expose someone - it might be out of revenge or with the intention to harm them. Ask students to suggest some reasons and discuss openly.

Slide 6

Read the contents of the slide aloud.

Discuss: Why is it dangerous for your personally identifiable information to be shared publicly?

Gather as many answers as possible to generate a list of reasons why this would make someone's online presence extremely vulnerable. Some reasons may include unknown strangers may be able to locate you in real life, impersonate you online, or make you susceptible to cyberattacks.

Slide 7

Read the contents of the slide aloud.

Discuss: What should you do if you ever experience cyberstalking?

Cyberstalking is a serious type of online abuse, which has legal implications in many countries. Have students research and understand the laws and rights that an individual has in your country. Discuss what kind of support network is available to them, for example school counsellors or victim support centres in your local area.



INVESTIGATE THE SCENARIO

30 MINUTES

Slide 8

Say: In this next section, you will be investigating a scenario that starts from an online game. Remember to keep the keywords we've just learned in mind. I will be showing you five pieces of evidence which we'll discuss together. Think critically about the information we're examining and consider the discussion questions.

(Optional) Select five students to read as these characters: Andrew, Gary, Shelly, Tony, and Annie.

Slide 9

Read this online game chat between Andrew, Shelly, Gary, and Tony.

Discuss the following questions:

1. Why do you think Andrew has reacted this way? Do you think he has a right to be angry?

Some students may think Andrew has a right to be angry in this instance as Gary shot and killed his character. Andrew might be upset because he wanted to play the game longer but has been eliminated from the game. On the other hand, some may see Andrew's reaction as an extreme overreaction.

2. What do you think the last line that Andrew said means? How would you feel if you were Gary?

Andrew's last line is a threat to Gary, although it is vague and left to interpretation. In certain games there are heightened exposures to violence, which leads to a normalisation of aggressive, offensive, and obscene language in these environments. Call on volunteers to share experiences they've had with such aggressive language and interactions in online games.

Slide 10

Read the call transcript between Andrew and Shelly.**Discuss** the following questions:

1. How can you describe the emotion Andrew is feeling? Who do you feel empathy for in this situation?

Andrew is feeling offended and angry that Gary has eliminated him from Call of Aliens. Students should not feel empathy for Andrew as he is expressing rage and the desire for revenge in a dangerous way.

2. Shelly ends the call by saying she wants to stay out of it. What do you think Shelly's responsibility might be as a good digital citizen?

By wanting to stay out of it, Shelly is becoming a bystander to a cyberbullying situation that is happening in front of her. Instead, she should try to calm Andrew down or warn him against doing anything rash.

Slide 11

Read this direct message conversation between Gary and Annie.**Discuss** the following questions:

1. From this interaction, do you trust Annie's words? Do you think she has positive or negative intentions?

This conversation gives us no reason to suspect that Annie has negative intentions towards Gary. However, it looks like Gary only accepted Princess Annie's friend request very recently. Students who choose to trust Annie outright should consider thinking twice about trusting an online stranger so quickly.

2. When you meet other users online, it can be hard to identify who is trustworthy. What are some indications of a bad actor you can look out for?

Call on students to list out potential indications of negative intentions, such as offering something that seems too good to be true or rushing to ask for your personal information.

3. Do you think Gary has done anything wrong here? Should he give out his address and phone number in order to receive Annie's gift?

Yes, Gary has done something wrong by giving out his address and phone number to an online stranger he doesn't know. This is extremely dangerous behaviour as it is impossible to know who is on the other side of the screen, and is not cyber safe.

Slide 12

Read the transcript from Andrew's livestream.**Discuss** the following questions:

1. Now that Andrew has revealed that he tricked Gary into thinking "PrincessAnnie002" was a real person, how does it change your perception of the previous conversation? Go back and think about which questions you

might answer differently.

Allow students to reflect on how they feel – did they feel tricked? For students who chose to trust Annie, ask them to share their thoughts after this revelation. Trickery is a malicious form of cyberbullying and abuse which can present itself in many different ways. Remind students to exercise good judgement whenever they're online and to critically think about who they're talking to.

2. How did Andrew's trickery escalate the situation beyond the initial accident in the game?

Andrew used trickery to obtain Gary's personal information and shared it publicly (doxxing) with a large number of followers. Gary is now a target for all kinds of cyber attacks, online abuse and harassment, and can be easily located in real life by a group of anonymous online users.

3. Identify and discuss the impact doxxing and cyberstalking can have on a person.

Andrew has put Gary in an extremely dangerous and vulnerable position by doxxing Gary. The long-lasting implication is that Gary's private information is now leaked online and is likely unable to make that information private again. Doxxing and cyberstalking can have serious impact on a person's mental health, as it can cause an individual to feel anxious and scared.

Slide 13

Read Gary's report to the police.

Discuss the following questions:

1. How could this situation have been prevented, and what can be done to help Gary now?

Users should be cautious about sharing personal information online and should not trust individuals they don't know well. Gary should seek legal help to report the crime and find a support network to help him through this situation.

2. Even though cyberbullying takes place online, it can have serious real-world consequences. What kind of legal violations did Andrew commit through his actions?

Have students research and discuss the laws and rights for victims of online abuse in your local area.



PROJECT WORK

DURATION AS NEEDED

Slide 14

Say: Your project assignment is to debate this statement: Tech companies should be responsible for making the internet a safe space, not individuals or governments. Decide if you will be debating in support of tech companies, individuals, or the government. Prepare and present your argument with strong evidence.

Slide 15

Say: Read the instructions and questions carefully

1. Choose a side. Begin by deciding which side of the debate you will be on: tech companies, individuals, or the government.
2. Research your side of the argument and gather evidence to support your position. Consider using statistics, news articles, and expert opinions to back up your claims.
3. What role should tech companies, individuals, or the government play in creating a safe online environment?
4. What are the potential drawbacks or consequences of relying on tech companies, individuals, or the government to make the internet a safe space?
5. How can tech companies, individuals, or the government work together to create a safer online environment?
6. Prepare, practice, and present a compelling argument using your research.

Note for Teachers

This project-based learning assignment is open-ended by design, so you have the flexibility to direct the project outcome as desired. It can be carried out individually or in collaborative groups.

Slide 16

Hold a classroom debate where each side gets to present their arguments in support for tech companies, individuals, or governments. Students may also take turns to present a rebuttal statement.

**KEY TAKEAWAYS**
10 MINUTES

Slide 17

Say: Here are some things we've learned from this lesson.

1. Never share your personal information to people you don't know or trust online in order to protect yourself from online attacks such as doxxing or cyberstalking.
2. Manipulating someone to give information is considered trickery, and should never be tolerated by upstanders.
3. Cyberstalking and doxxing are extremely harmful and damaging forms of online abuse, and should be reported immediately.

Ask: What are some key takeaways you've learned from this lesson?
Call on volunteers to share what they've learned.

