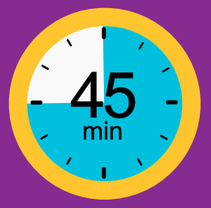
Story Time: “Oh, No... Hacked Again!” by Zinet Kemal



This lesson can take up to 45 minutes. It can be broken down into smaller lessons or extended as required.

Ages 7-9

The lesson has been designed for learners aged 7-9. The “checkpoints” offer differentiation strategies to scale learning as required.

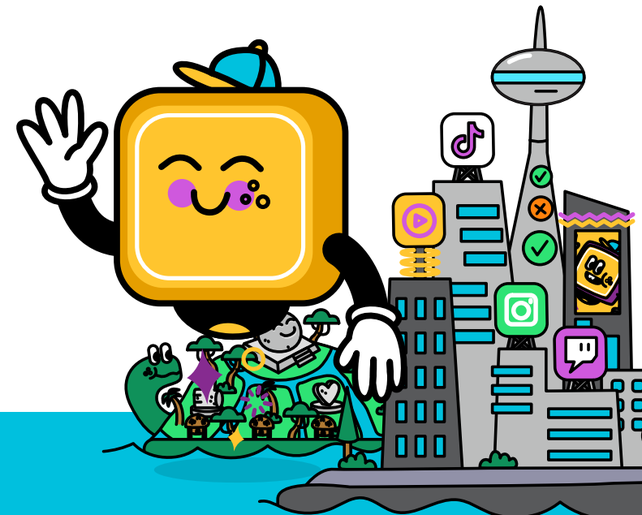
eSmart DIGITAL LICENCE

Join us on the quest!

This lesson is part of the eSmart Digital Licence program

By completing just four engaging lessons, including this one, your class can earn their eSmart Digital Licences—signalling their understanding of safe and responsible online behaviour. Start now and guide your learners toward becoming confident and positive digital citizens.

Learn more about the program
be.esmart.org.au/dl/overview



About this lesson

Overview

Note: This activity requires your class to have access to the book “Oh, No... Hacked Again! A Story About Online Safety” by Zinet Kemal. The story is recommended for ages 6-12. Check with your school library, or, hardcover versions can be purchased via various stockists such as Booktopia.

In this story time activity, students explore a range of preventative measures that aim to protect against being hacked. “Oh, No... Hacked Again!” is a story about Elham, an eight-year-old girl who plays online games. While she loves playing online, Elham struggles with making safe decisions regarding her cyber security. Throughout the story, Elham leans on her mum and siblings to help stay safe while navigating online spaces.

This activity is relevant for:

- Students who are engaging in online activities such as gaming, social media, or using messaging services to connect with family and friends.
- Helping students to identify situations where they should ideally seek support before offering personal information, or enacting other security risks.
- Expanding notions of what “hacking” is and how it presents online, and the possible impacts of these activities.

Activity setup

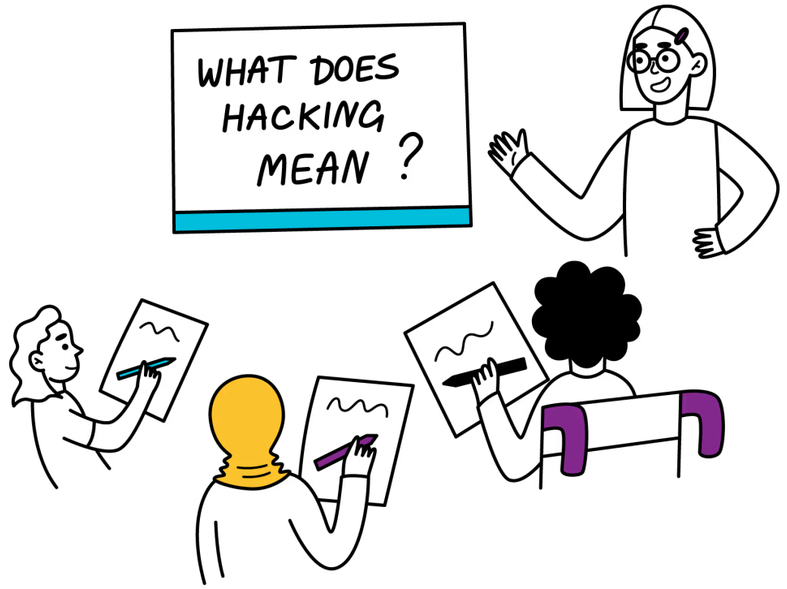
Download the “Student Activity Pack” from the Resources section. This worksheet can be printed and pasted into student workbooks, or, it can be distributed digitally using Google Classroom or similar.

Download the “Educator Tip Sheet”. This resource can be used to support and guide student discussion by offering tips in relation to the themes discussed in the book.

Learning intentions & success criteria

By completing this activity, our class intends to:

- Discuss the meanings and possible impact of being hacked.
- Identify a range of protective and help-seeking strategies in relation to cyber security and potentially harmful contact that is made by others online.



Lesson instructions

1 What (or who) is a hacker?

Direct students to the Activity Sheet. Students will fill in the "Wanted" poster for a hacker, by drawing a picture of what they think a hacker looks like. Students will explain what the hacker has done, and how their actions have impacted others.

Once complete, ask for volunteers to describe their hacker to the class. As they are explaining their character, write a list on the board that summarises all the things that hackers are thought to do online. Refine student understanding about what hackers are, and what they do, throughout the course of the discussion. Discussion points might include:

- Hackers are individuals who use their technical skills to gain unauthorised access to computers, networks, and data.
- White Hat Hackers use their skills to improve security by finding and fixing vulnerabilities in systems. Black Hat Hackers are malicious hackers who exploit vulnerabilities for personal gain, such as stealing data, damaging systems, or spreading malware.
- Hackers can create and distribute malware (viruses, worms, Trojans) to damage or gain control of systems, steal information, or spy on users.
- By stealing personal information, hackers can impersonate individuals, commit fraud, or access sensitive accounts.
- By installing keyloggers, hackers can record keystrokes on a victim's device to capture passwords, credit card numbers, and other sensitive information.
- Hackers can listen in on unencrypted communications to gather information or spy on conversations.
- Hackers, sometimes state-sponsored, infiltrate organisations or government systems to steal sensitive information or gain strategic advantages.

2 Read the story

Read “Oh, No... Hacked Again! A Story About Online Safety” by Zinet Kemal.

Throughout the story, the following questions can be used as discussion prompts, or, they can be utilised as a post-story discussion depending on preference. The “Hacked Again: Teacher Resource” offers recommendations and tips in relation to these questions.

- What do you think might happen next?
- Have you heard of situations like this happening before?
- What would you do if you found yourself in this scenario?
- How do you think [this character] must be feeling right now?
- What would you hope a trusted adult would do in that situation?
- What is one tip we can take away from what happened to Elham in this instance (and repeat throughout).

3 Exit pass

Following the story and discussion, ask students to write down on their worksheets at least three strategies for keeping safe online.

Ask students to share their strategies, and refine the discussion as necessary by referencing security tips from the “Educator Tip Sheet”.

Aligned curriculum

Australian Curriculum (Version 9.0)

Years 3 and 4: General Capabilities
Digital Literacy

Managing online safety:

- Level 3: Report negative or harmful online behaviour by seeking help from trusted adults.

Year 3: English

- AC9E3LE02: Discuss connections between personal experiences and character experiences in literary texts and share personal preferences.
- AC9E3LE04: Discuss the effects of some literary devices used to enhance meaning and shape the reader's reaction, including rhythm and onomatopoeia in poetry and prose.

Year 4: English

- AC9E4LE02: Describe the effects of text structures and language features in literary texts when responding to and sharing opinions.
- AC9E4LE04: Examine the use of literary devices and deliberate word play in literary texts, including poetry, to shape meaning.

My Time, Our Place

Outcome 2: Children and young people are connected with and contribute to their world.

Children and young people develop a sense of belonging to groups and communities and an understanding of the reciprocal rights and responsibilities necessary as active and informed citizens.

This is evident when children:

- Understand the concept that while digital technology can connect us, it is also vitally important to maintain our face-to-face and interpersonal connections too.

CASEL Framework

- Self-management: The abilities to manage one's emotions, thoughts, and behaviours effectively in different situations and to achieve goals and aspirations.
- Responsible decision-making: The abilities to make caring and constructive choices about personal behaviour and social interactions across diverse situations.

Tips for Educators
Protecting Online Security

Recommendations for Maintaining Online Safety

The following recommendations aim to support discussion with students based on the story "Oh, No... Hacked Again!" by Zinet Kemal. Broadly, these recommendations offer ways for educators, parents and students to prevent hacking, unwanted contact, spam, malware, and other harmful interactions while playing games and using the internet.

Protect personal information.

It is strongly advised for students never to share personal information such as full name, address, phone number, school, or passwords online. However, personal information can be even further protected using the following methods:

- Create unique passwords for different accounts and change them regularly. Use a combination of letters, numbers, and symbols.
- Use two-factor authentication (2FA) whenever possible to add an extra layer of security to accounts.
- Use reputable antivirus software and keep it updated to protect against malware and other threats.
- Keep operating systems, games, and other software up to date to ensure they have the latest security patches.
- Utilise and routinely check the privacy settings on social media and gaming platforms, to control who can make contact and see information.
- Avoid posting your email addresses in public forums or profiles to reduce the risk of spam.
- Enable and configure spam filters in email accounts to help keep spam messages away.

Establish Safe Apps, Websites, and Spaces

Guide students to use websites and apps that are safe and age-appropriate. Safe websites are those that have content suitable for children their age and are designed with their safety and well-being in mind. These sites often have parental controls, content filters, and child-friendly interfaces that minimise exposure to inappropriate contact.

The eSafety Guide, provided by the Office of the eSafety Commissioner, is an excellent place to start investigating the security features, block and report systems, and age-appropriateness of apps and websites.

Top tips:

- Only download games and updates from official websites or reputable app stores.
- Advise students to be careful of chatting with others in games. Avoid sharing personal information and report any suspicious or inappropriate behaviour.
- Check privacy settings, set parental controls, and investigate the platform's blocking and reporting strategies prior to allowing children to utilise particular games or apps.
- Make sure that any "help", blocking or reporting features are communicated to children before they use the app or platform. Check their understanding of the situations that are appropriate for blocking and reporting, and model the process for them.
- Children should be encouraged to use digital devices in public areas of the home or school, where adults can supervise their online activities and provide assistance before situations escalate.
- Advise children to be cautious of free in-game offers, advertisements or downloads, as they can sometimes be used to distribute malware that hacks personal information.

Activity Sheet

Hackers and Unwanted Contact

Instructions

Fill in the "Wanted" poster for a hacker. Draw a picture of your hacker on the poster. Explain what they have done, and how their actions have impacted others.

This hacker is wanted by the authorities for:

This hacker's actions have impacted others by:

Exit Pass

Write down three strategies to prevent hacking and keep safe online.