

Hack Attack Investigation - Teacher Guide

About Hack Attack Investigation

Hack Attack Investigation is an interactive learning tool (resource) specifically designed for Stage 4 students in New South Wales high schools.

The resource has been developed in H5P - a platform used to create interactive learning content - and teachers can access it directly through a browser: <https://www.iat.tafensw.edu.au/stage-4-hack-attack-investigation>

Hack Attack Investigation has been developed by the Institute of Applied Technology, a National Centre of Excellence led by TAFE NSW, in consultation with the NSW Department of Education through the [NSW Digital Skills and Workforce Compact](#).

1. Purpose of Hack Attack Investigation

Hack Attack Investigation is an engaging, real-world learning experience for students that explores digital awareness, curiosity, problem solving, and cyber security literacy.

The investigation focuses on a fictitious student named Kai, whose personal information has been compromised by a cyber hacker.

Students are challenged to examine identifiable information across a range of digital platforms, apps, and tools, to piece together clues to understand how Kai's digital profile was accessed.

2. Topic areas covered

Hack Attack Investigation introduces students to data and cyber safety topics including:

- personal information and digital identity
- privacy and the responsible use of data
- cybersecurity and the protection of information
- identifying potential online and cyber risks
- strategies for protecting data and accounts
- safe, responsible and ethical behaviour when using digital technologies.

3. Outcomes

The resource has been designed to help teachers in:

- Supporting the Stage 4 outcome: TE4-DIG-01 – demonstrates technological literacy to safely interact in digital environments, Technology 7–8 Syllabus (2023)
- Supporting delivery of the Technology and Applied Studies (TAS) content, aligned with both Australian Curriculum and NSW syllabus outcomes related to digital awareness and problem solving.
- Engaging Stage 4 students through authentic, relatable scenarios that reflect modern digital environments.

- Fostering student interest in future learning pathways and careers in data, technology, and cyber security, aligned with NSW Digital Compact commitments.
- Providing an accessible learning experience for students in all schools, including those with limited digital capabilities, devices, or learning management systems.

4. Curriculum lead considerations

Teaching professionals may wish to share this resource with TAS, Computing Technologies and Digital Technologies teachers as part of broader digital citizenship and cyber awareness initiatives. The resource requires minimal technical setup and is suitable for implementation across a wide variety of school contexts.

5. Accessing Hack Attack Investigation

- *Hack Attack Investigation* is hosted on a H5P platform under licence by TAFE NSW.
- Students do not need to create an account to log in.
- Access to the internet and desktop or laptop device access for students is needed.
- Access the resource via: <https://www.iat.tafensw.edu.au/stage-4-hack-attack-investigation>
- The investigation is designed to be completed in one lesson.

6. Guidance for teachers

- *Hack Attack Investigation* has been designed for students to complete at their own pace, within one lesson.
- Teachers can use the resource as a complete lesson sequence within a Digital and communication technologies unit or selected individual activities can be used to complement an existing program.
- The interactive activities can be used for explicit teaching, individual student learning, class discussion, formative assessment and revision. This gives teachers flexibility to incorporate the resource into their existing Technology 7–8 scope and sequence.
- Students do not receive a certificate of completion as HP5 is not enabled to generate certificates. If needed, teachers can review learners' summaries as evidence of completion by asking learners to take screenshots of the Summary page.

Before students start:

- Encourage students to work independently through the investigation, recording any key findings or reflections you require them to make as they complete.
- Familiarise yourself with the discussion questions included after the investigation, referring to the Your Future in Cybersecurity video.
- Refer to the Learning Activity Summaries section in this guide, for a quick reference of each learning activity.

Guidance to provide students:

- Explain they will be investigating how personal information can be collected and used to gain access to an individual's digital profile.
- As they progress through each activity they will receive progress feedback, however the H5P platform does not save progress for returning to later. If students exit the activity before completion, they will need to restart the investigation from the beginning when they return.
- As they progress, they need to complete all activities, including checking off the items at the bottom of each page where it says 'Check off each task that you have completed'. These actions will register in their summary upon completing the activity.
- Each activity includes expanded instructions to guide them through each activity.

7. Overview of learning activities in Hack Attack Investigation

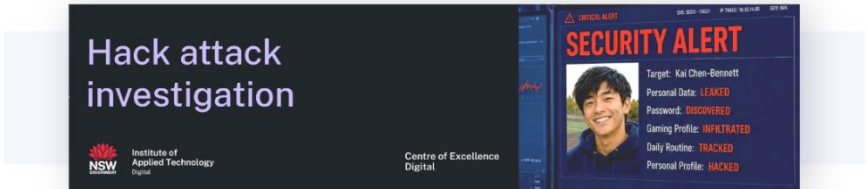
Each learning activity includes:

- listed tasks for students to explore
- clues to support students to complete their tasks
- a checklist at the bottom of each activity to demonstrate understanding. The checklist aligns to the tasks.

Before students start the investigation – Your Future in Cybersecurity video

- Play the 'Your Future in Cybersecurity' video to students, which introduces real people who work in data and cybersecurity, to start the conversation about what jobs in cybersecurity involve.
- You can revisit this topic with students using discussion questions at the end of the investigation.

7.1 Landing page – 0/11

Overview	Landing page
This is the landing page for the resource. Students need to select the blue 'Begin investigation' button to start their investigation. Note: the resource works best when used in full screen mode. Students can enter full screen by selecting this icon in the top right corner of the resource: 	 Stage 4 Data and Cyber Safety This resource has been developed by the Institute of Applied Technology Digital. Begin Investigation

Activity 1/11

Overview	Introduction
Watch video The video explains that Kai Chen-Bennett's identity has been hacked and invites students to take on the role of cyber investigator to find out what happened.	

7.2 Activity 2/11

Overview	Social media post
Select the hotspots Students are invited to examine the social media post Kai's sister Loz has posted and identify the pieces of information she has revealed that a hacker could use. Hotspots in the image reveal pieces of information. This task is designed to raise awareness of small details that can unintentionally give away information.	

Answer the questions Students answer two questions which prompt them to think like a cyber attacker and consider what information about Kai has been revealed by this social media post.	Questions Think like you are a cyber attacker. What kinds of information could you find out about Kai by seeing this social media post? Select 4 correct answers. ☐ Who he interacts with ☐ What school year he is in ☐ His daily routine ☐ What school he goes to ☐ Where Kai spends time ☐ His date of birth
---	--

Check

☐ True

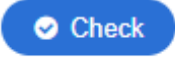
☐ False

Check

7.3 Activity – 3/11

Overview	Newsletter
Drag and drop The newsletter holds some information that can be connected to other pieces of information in Kai's profile. Students need to identify a time clue, location clue, and personal information by dragging and dropping the tags at the bottom of the newsletter to locations within the newsletter. If drag and drop is not available, students can also complete the activity by selecting each item and then selecting the location in the newsletter. Question Students answer the multiple-choice question about what creates the risk in this newsletter.	 The newsletter is titled "Ridgeview High School Newsletter – June Update". It features the school's logo in the top right corner. The content is organized into several sections: Principal's Message: A message from Jenna Williams, School Principal, welcoming students, families, and the community. It mentions the school's focus on digital responsibility and preparing students for future pathways like cybersecurity and data science. Teaching & Learning Highlights: A section highlighting digital detectives in Years 7 and 8 who have been exploring cybersecurity and data literacy. It mentions that teachers and students have been exploring how to stay safe online and what it takes to become an ethical hacker. Careers Corner: A section highlighting students exploring careers in cybersecurity, data analysis, AI, and software development. It mentions the school's coding apps and STEM clubs, and stay curious! Student Achievement Spotlight: A section celebrating two students, Kei Chom-Dorsett (Year 10) and Dana Moon (Year 8), for an outstanding performance at the Regional Athletics Carnival. It mentions that both students achieved excellent results and progress to the State Carnival next month. It also mentions that the school is proud of their achievements. Weekly Words of Wisdom: A section with a quote: "Think before you click – your digital footprint lasts longer than you think." Upcoming Events: A list of events: Parent-Teacher Interviews – 2nd Monday in June; STEM Showcase – 4th Monday in July; State Athletics Carnival – 2nd Wednesday in August. At the bottom of the newsletter, there are three boxes labeled "Personal Information", "Time Clues", and "Location Clues". Below the newsletter image, there is a "Check" button and a "Question" section. The question asks: "Now you have completed the examination. What is the biggest risk in this newsletter?". There are three multiple-choice options: - It celebrates achievements of students at the school. - It is posted online where anyone can read it. - It reveals details such as full name, location and time clues.

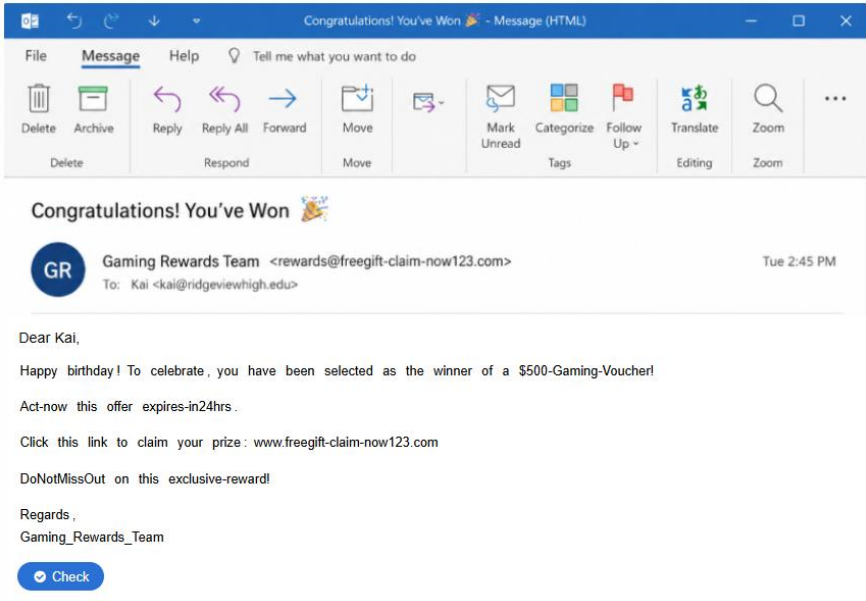
7.4 Activity – 4/11

Overview	Gaming profile
Select words/phrases to identify Students need to identify and select pieces of personal information in the gaming profile. The activity has a check button at the bottom that reveals the results. Students can complete this task as many times as they need to move to the next activity.	 Gaming Profile Username : ShadowKai07 Email : kai_chenbennett@ridgeviewhigh.edu Rank : Diamond III Team : CentralOvalGladiators About me : Reliable player who will never let the team down . Ready to take on all challengers . phone me : 0491570156 Details :  Joined : 1 year ago (Birthday:07/Aug)  Active : Nightly  Favourite Game : BattleZoneLegends Recent Conversation : "looking forward to StateChamps_next_month " 

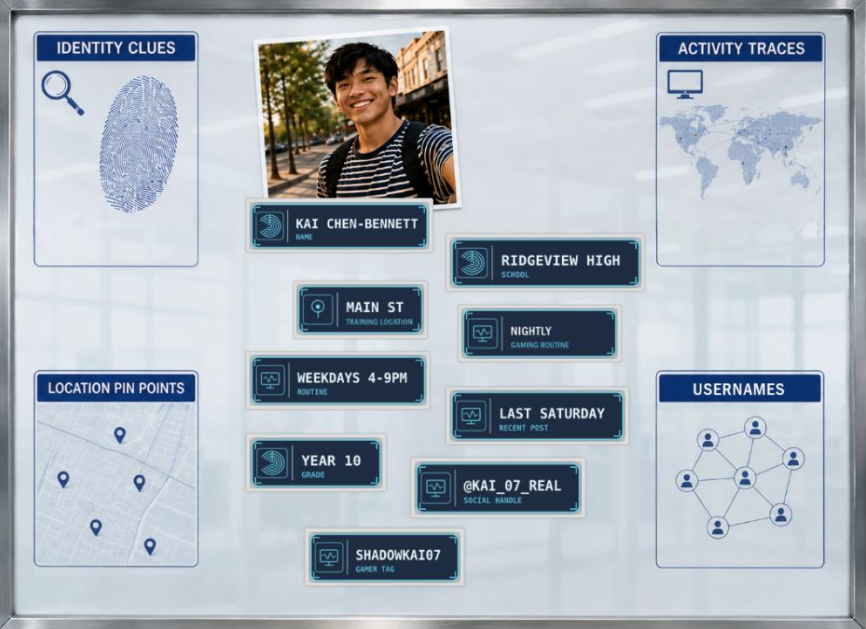
7.5 Activity – 5/11

Overview	Text message
Multiple choice question This activity provides a social engineering text message to Kai's phone. Students need to decide the best way to respond to the text by choosing the appropriate answer.	What would have been the best action for Kai to take when he received this message? Verify the sender's identity using another method Call the number that sent the message to verify their identity Respond by sending login details Respond to the message asking for more information

7.6 Activity – 6/11

Overview	Email
Select words/phrases to identify Students need to identify the words or phrases that are suspicious or designed to tempt Kai to respond to the email or click on a link. Students can attempt this activity as many times as they need to by selecting the 'retry' button. A 'show solutions' button is also included to support learning.	 The screenshot shows an email interface with a ribbon menu (File, Message, Help) and a toolbar with icons for Delete, Archive, Reply, Reply All, Forward, Move, Mark Unread, Categorize, Follow Up, Translate, and Zoom. The email content includes a 'GR' logo, the sender 'Gaming Rewards Team', and a 'Check' button at the bottom.

7.7 Activity – 7/11

Overview	Detective board
Drag and drop Students need to sort the clue types into categories to develop an understanding of how different pieces of information can complete an overall picture.	 The Detective board interface features several categories and clue cards: IDENTITY CLUES: Includes a magnifying glass icon and a fingerprint icon. LOCATION PIN POINTS: Shows a map with several location pins. ACTIVITY TRACES: Includes a world map icon. USERS NAMES: Shows a network diagram with several user icons. Clue Cards: - KAI CHEN-BENNETT (NAME) - MAIN ST (TRAINING LOCATION) - WEEKDAYS 4-9PM (ROUTINE) - YEAR 10 (GRADE) - SHADOWKAI07 (GAMER TAG) - RIDGEVIEW HIGH (SCHOOL) - NIGHTLY (GAMING ROUTINE) - LAST SATURDAY (RECENT POST) @KAI_07_REAL (SOCIAL PROFILE)

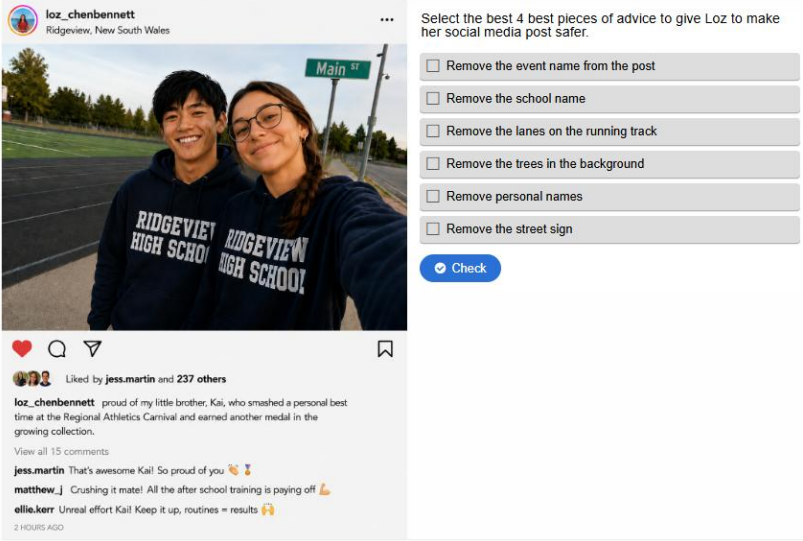
Multiple choice question Students answer a multiple choice question. Students can check their answers and retry the question as many times as they need.	Question What makes this data dangerous? Each piece is separate It is not useful It allows someone to connect identity, location, and behaviour It only shows one detail
---	--

7.8 Activity – 8/11

Overview	Attack path reconstruction
Complete the sentence Students need to complete the sentence by dragging and dropping the words or phrases provided into the correct position. If drag and drop is not available, students can select the phrase and then select its location. This confirms the student understands how the hacker operated in this scenario. Students can check their answers and repeat the activity as many times as they need before moving to the next activity.	Attacker path The attacker started by finding a [] which provided the first set of clues. They then [] and discovered a recent issue of a []. From there, they correctly guessed [] and connected this to Kai's []. This provided the attacker with enough information to conduct social engineering and phishing attacks by []. school newsletter social media post sending a text and an email searched the school and Kai's name online gaming profile a student email address Check Question What makes this attack successful? One single post Multiple small pieces of data connected together Sending messages Playing online games



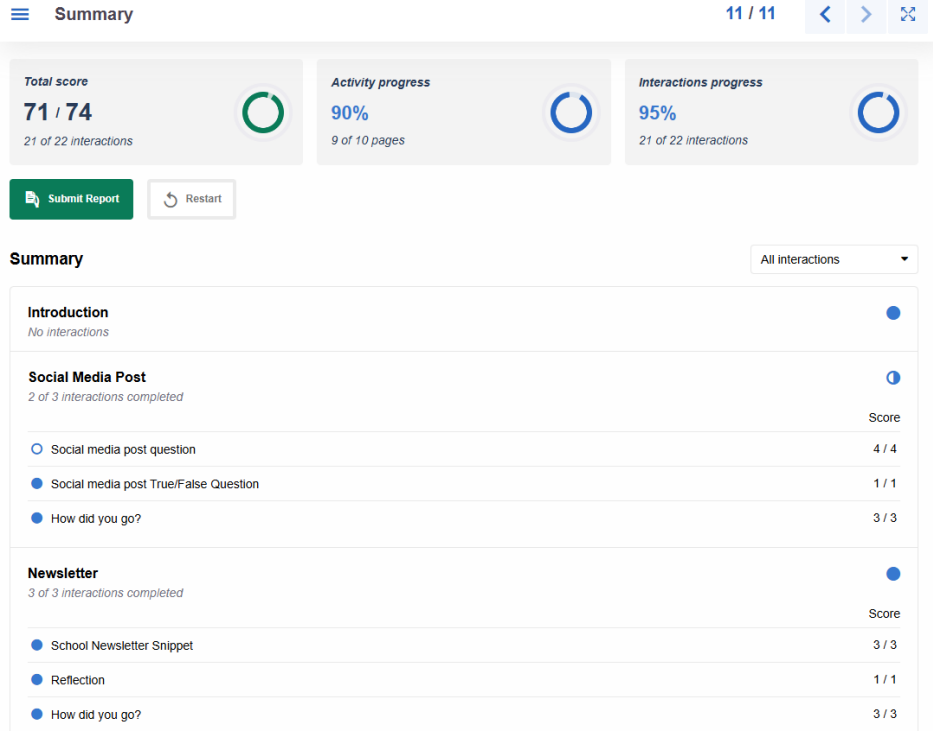
7.9 Activity – 9/11

Overview	Cyber threat prevention activities
Multiple choice question Students need to identify pieces of information to recommend what could have been done to prevent identity clues being given away. There are 4 correct answers. Students can check their answers and complete as many times as they need to.	Social media post  Select the best 4 best pieces of advice to give Loz to make her social media post safer. ☐ Remove the event name from the post ☐ Remove the school name ☐ Remove the lanes on the running track ☐ Remove the trees in the background ☐ Remove personal names ☐ Remove the street sign Check
Drag and drop Students need to replace clues to remove personal information from Kai's gaming profile. Students can check their answers and complete as many times as they need to.	Gaming profile Select and drag items from the box on the right to the gaming profile on the left to replace the risky details with safer options.  Check

7.10 Activity – 10/11

Overview	Real world cyber investigators
Watch, listen, discuss Students consider real world jobs related to the cyber investigation they have just undertaken. Discussion questions are included.	 Montii Abid Turn  Deepika Mahankali Turn < Card 2 of 2 Card 1 of 2 > Some questions to think about Connecting to the investigation How was your job as a cyber investigator in this exercise similar to Deepika and Montii's jobs? Skills for success The experts talked about problem solving, curiosity, communication and technology skills. Which of these skills do you think you are already good at? Which skills would you like to get better at? Exploring cyber careers How do you see the importance of people working in cybersecurity in the future?

7.11 Summary page – 11/11

Overview	Summary																	
This page provides the learner with a summary of their results. The learner can revisit tasks by selecting an item in this list, or by navigating with the arrows at the bottom of the screen. If required, teachers can review learners' summaries as evidence of completion by asking learners to take screenshots of the 'Summary' page. Students do not need to select 'submit report'. Note that this resource does not support saving work. Once a learner closes the window their progress will reset.	 The screenshot displays the 'Summary' page for a learner. At the top, there are three progress indicators: 'Total score' (71 / 74, 21 of 22 interactions), 'Activity progress' (90%, 9 of 10 pages), and 'Interactions progress' (95%, 21 of 22 interactions). Below these are buttons for 'Submit Report' and 'Restart'. The main section is titled 'Summary' and shows a list of completed tasks with their scores. The tasks are grouped into sections: 'Introduction' (No interactions), 'Social Media Post' (2 of 3 interactions completed), and 'Newsletter' (3 of 3 interactions completed). Each task has a score and a 'How did you go?' question. <table border="1"><thead><tr><th>Section</th><th>Task</th><th>Score</th></tr></thead><tbody><tr><td rowspan="3">Social Media Post</td><td>Social media post question</td><td>4 / 4</td></tr><tr><td>Social media post True/False Question</td><td>1 / 1</td></tr><tr><td>How did you go?</td><td>3 / 3</td></tr><tr><td rowspan="3">Newsletter</td><td>School Newsletter Snippet</td><td>3 / 3</td></tr><tr><td>Reflection</td><td>1 / 1</td></tr><tr><td>How did you go?</td><td>3 / 3</td></tr></tbody></table>	Section	Task	Score	Social Media Post	Social media post question	4 / 4	Social media post True/False Question	1 / 1	How did you go?	3 / 3	Newsletter	School Newsletter Snippet	3 / 3	Reflection	1 / 1	How did you go?	3 / 3
Section	Task	Score																
Social Media Post	Social media post question	4 / 4																
	Social media post True/False Question	1 / 1																
	How did you go?	3 / 3																
Newsletter	School Newsletter Snippet	3 / 3																
	Reflection	1 / 1																
	How did you go?	3 / 3																

8. Contacts

Contact the Institute of Applied Technology Digital: iatdigital@tafensw.edu.au

9. Document History

No	Date	Approved by	Amendment
1	15/09/2026	Michelle O'Dea	Initial Release.