Hack Attack Investigation

A data and cyber safety teaching and learning resource

Information and Implementation Guide for Principals and Teachers

The *Hack Attack Investigation* resource is an interactive learning tool that has been developed by the *Institute of Applied Technology (IATD),* in consultation with the *NSW Digital Skills and Workforce Compact*, for distribution to Stage 4 in schools across New South Wales.

The resource has been developed in H5P which is a platform used to create interactive learning content for students. The H5P resource is accessed via direct link to the IATD website, through a browser.

Purpose

Hack Attack Investigation is designed to provide an engaging, real-world learning experience that promotes digital awareness, curiosity, problem solving, and cybersecurity literacy.

The investigation centres on a fictitious student, Kai, whose personal information has been compromised by a cyber hacker. Students are challenged to examine information across a range of digital platforms, apps and tools, piecing together clues to understand how Kai's personal information was compromised.

Educational outcomes

This learning tool is designed to:

- Support the delivery of Technology and Applied Studies (TAS) content aligned with the Australian Curriculum and NSW syllabus outcomes relating to digital awareness and problem solving.
- Engage Stage 4 learners through authentic and relatable scenarios that reflect contemporary digital environments.
- Foster interest in future pathways and careers in data, technology and cybersecurity. This aligns with NSW Digital Compact.
- Provide an accessible learning experience for all schools, including those with limited digital capabilities, devices or learning management systems.

Key learning outcome

TE4-DIG-01 – demonstrates technological literacy to safely interact in digital environments.

The project supports learning about:

- 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.

Access and delivery

- The resource is hosted on an H5P platform under licence by TAFE NSW.
- Access is provided via a direct link and does not require a login or account.
- The investigation is designed to be completed in one extended lesson.
- Students can progress through the content at their own pace.

Instructions for Teachers

The resource can be used as a complete lesson sequence within a Digital and communication technologies unit or teachers can select individual activities 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.

No certificate of completion is issued at the conclusion of the activity (H5P is not enabled to generate certificates). If required, teachers can review learners' summaries as evidence of completion by asking learners to take screenshots of the “Summary” page.

Before commencing the activity:

1. Explain that they will be investigating how personal information can be collected and used to gain access to an individual's digital profile.
2. Encourage students to work independently through the investigation, recording any key findings or reflections as required by the teacher.
3. Familiarise yourself with the discussion questions included after the investigation, referring to the “Your Future in Cybersecurity” video.
4. Refer to the Activity Summaries (point 8 below) for summaries for each activity for quick reference.
5. Share the link with students: **www.iat.tafensw.edu.au/stage-4-hack-attack-investigation**

Important notes

Please advise students of the following before they begin:

- Each activity provides progress feedback as learners complete tasks however, the H5P platform **does not save progress** for returning to later. Students who exit the activity before completion will need to restart the investigation from the beginning when they return.
- As they progress through the resource, learners should complete all activities. This includes 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.
- There are expanded instructions to guide learners embedded in each activity.

Principal/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. Technical requirements are internet connection and desktop or laptop device access for learners.

Activity summaries

The following provides a summary of each activity for teacher reference.

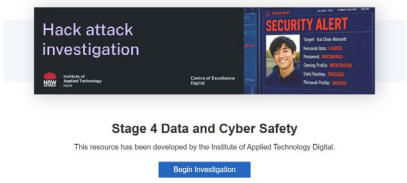
Each activity includes:

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

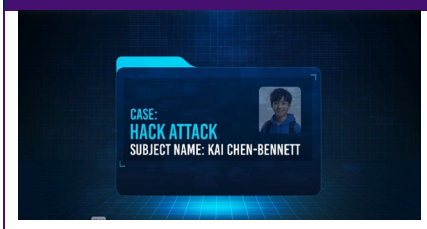
Before starting the investigation

Play the video "Your Future in Cybersecurity" to learners to start the conversation about what cybersecurity jobs involve. The video introduces real people who are successfully working in data and cybersecurity. Learners will revisit this topic with some discussion questions at the end of the investigation.

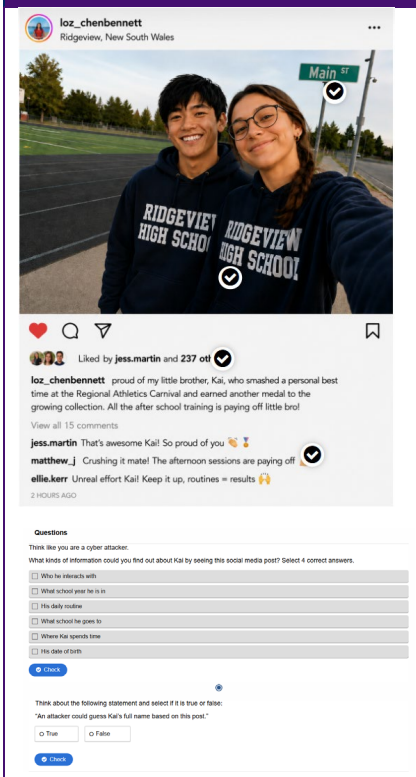
H5P landing page 0/11

Landing Page	Summary
	This is the landing page for the resource. Learners are required to select the blue "Begin investigation" button to begin their investigation. Note: the resource works best when used in full screen mode. Learners can enter full screen by selecting this icon in the top right corner of the resource: 

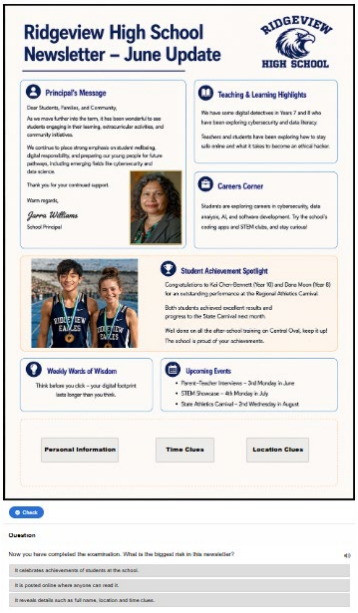
Activity 1/11

Introduction	Summary
	**Watch video** The video explains the scenario (Kai Chen-Bennett's identity has been hacked) and invites the learner to take on the role of cyber investigator to find out what happened.

Activity 2/11

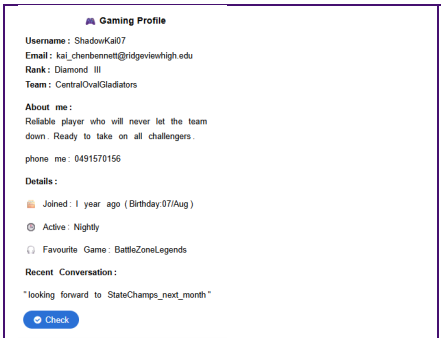
Social media post	Summary
	**Select the hotspots** The learner is invited to examine the social media post that Kai's sister, Loz, has posted and identify the pieces of information she has revealed that a hacker could use. Hotspots in the image reveal pieces of information. This task is designed to raise awareness of small details that can unintentionally give away information. **Answer the questions** The learner answers two questions which prompt them to think like a cyber attacker and consider what information about Kai is revealed by this social media post. **Complete the progress checklist** At the end of this page and all subsequent pages, the learner should check off the items under "**Check off each task that you have completed**".

Activity 3/11

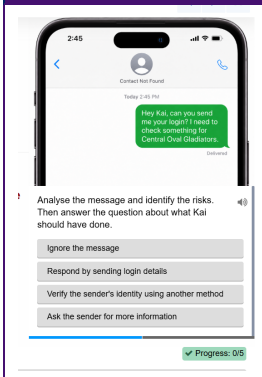
Newsletter	Summary
	**Drag and drop** The newsletter holds some information that can be connected to other pieces of information in Kai's profile. This activity requires the learner to identify a time clue, location clue and personal information by dragging and dropping the tags at the bottom of the newsletter to locations within the newsletter. If drag and drop is not available, learners can also complete the activity by selecting each item and then selecting the location in the newsletter. **Question** Learners should answer the multiple-choice question about what creates the risk in this newsletter.

Activity 4/11

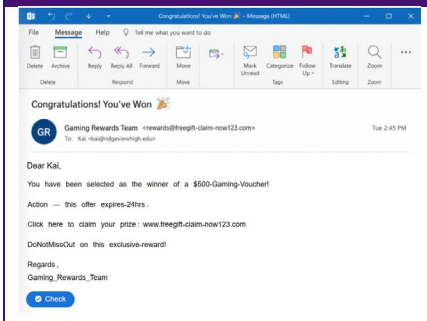
Gaming profile	Summary

	**Select words/phrases to identify** The learner is required to identify and select pieces of personal information in the gaming profile. The activity has a check button at the bottom that will reveal results. The learner can complete this task as many times as they need to move to the next activity.

Activity 5/11

Text message	Summary
	**Multiple choice question** This activity provides a social engineering text message to Kai's phone. The learner is required to decide the best way to respond to the text by choosing the appropriate answer.

Activity 6/11

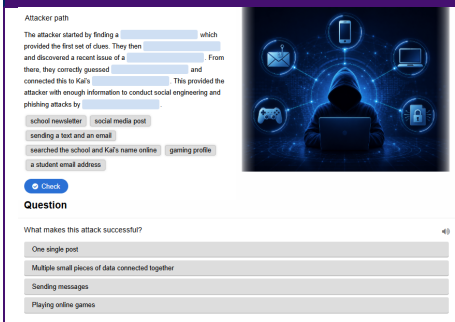
Email	Summary
	**Select words/phrases to identify** The learner is required to identify the words or phrases that are suspicious or designed to tempt Kai to respond to the email or select a link. The learner can attempt this activity as many times as they need to by selecting the 'retry' button. A 'show solutions' button is also included to support learning.

Activity 7/11

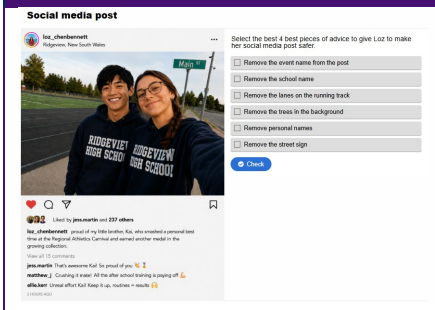
Detective board	Summary

	**Drag and drop** The learner is required to sort the clue types into categories to develop an understanding of how different pieces of information can complete an overall picture. Learners are able to check their answers and retry the activity as many times as they need to complete their tasks.

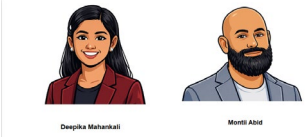
Activity 8/11

Sentence completion	Summary
	**Complete the sentence** The learner is required to complete the sentence by dragging and dropping the words or phrases provided into their correct position. If drag and drop is not available the learner can select the phrase and then select its location. This confirms learner understands how the hacker operated in this scenario. Learners can check their answers and repeat the activity as needed before progressing to the next activity.

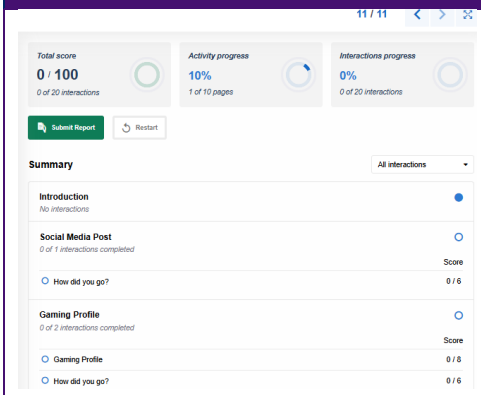
Activity 9/11

Identity theft prevention	Summary
	**Multiple choice question** The learner is required to identify pieces of information to recommend what could have been done to prevent identity clues being given away. Learners can check their answers and complete as many times as they need to.
	**Drag and drop** The learner is required to replace clues with deidentifying pieces of information that expose Kai's digital identity on the gaming platform. Learners can check their answers and complete as many times as they need to.

Activity 10/11

Real world cyber investigators	Summary
	**Watch, listen, discuss** Learners consider how real jobs relate to the cyber investigation they have just undertaken. Questions for discussion are included.

Summary page 11/11

Summary page	Summary
	This activity 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. Note that this resource does not support saving work. Once a learner closes the window their progress will reset..

Contacts

Project Manager IATD	**Matilda Fay**	Matilda.Fay@tafensw.edu.au
Education Lead IATD	**Michelle O'Dea**	Michelle.odea4@tafensw.edu.au
Senior Operations Manager	**Sonya O'Brien**	Sonya.obrien3@tafensw.edu.au

Document History

No	Date	Approved by	Amendment
1	10/09/2026	Michelle O’Dea	Initial release