



THE UNIVERSITY
of ADELAIDE

CYBER SECURITY EDUCATION FOR SCHOOLS

A new series of teacher professional development courses and resources from CSER's national K-12 Digital Technologies Education program.

Computer Science Education Research Group (CSER)
The University of Adelaide
csermoocs.adelaide.edu.au

adelaide.edu.au

CRICOS Provider Number 00123M

NEW MOOCs on Teaching Cyber Security & Awareness in Schools!

CSER's free, self-paced MOOCs (Massively Open Online Courses) aim to build Primary and Secondary teachers' confidence and capacity to integrate the learning of Cyber Security and Awareness into the classroom. The MOOCs contain practical classroom activity ideas and examples of career pathways in this critical and growing sector.



Cyber security for all

Our use of technology and access to information is growing rapidly and cyber security and awareness are now essential knowledge and skills for our digital world. Understanding how our digital world works, how it is designed to protect us and how we can keep our information safe is critical for both adults and children to learn. AustCyber, Google Australia and CSIRO have partnered to support CSER to develop free professional learning MOOCs, resources and training addressing this need.

MOOC content

This course breaks down and clarifies the important areas of cyber security, cyber safety and cyber awareness as part of integrated classroom learning in schools.

We have two free courses available for teachers on teaching cyber security and awareness - one for primary teachers (K-6) and one for secondary teachers (Years 7-10). Our courses unpack the key concepts and present practical classroom activities you can use to address key learning within the Australian Curriculum: Digital Technologies and ICT Capabilities. Topics include: data security; encryption and cryptography; networks; information systems and safety; cyber security risks and security measures; cyber ethics and more!

All our courses provide access to a rich community of teachers sharing ideas and resources to support classroom learning. To access our Cyber Security and Awareness MOOCs and communities, visit csermoocs.adelaide.edu.au/available-moocs

CYBER AWARENESS
The knowledge, attitude and behaviours that aim to protect our information assets.

CYBER SECURITY
The practice of protecting computers, networks, programs and data from digital attacks.

CYBER SAFETY
Safe and responsible use of Information Communication Technologies.

www.csermoocs.adelaide.edu.au

PL-in-a-Box

PL-in-a-Box supports professional learning (PL) of Digital Technologies in your school or community. These resources are designed to support you or your team in delivering free professional learning sessions, workshops or events. We have created free PL-in-a-Box packs for our Cyber Security & Awareness MOOCs for download on our resources page at csermoocs.adelaide.edu.au/resources

Find out more and connect with us at csermoocs.adelaide.edu.au

WE ARE SEEKING AUSTRALIAN CYBER SECURITY STORIES



AustCyber claims cyber security is a booming global sector with 52 different types of roles and 18,000 cyber security jobs needing to be filled in by 2026. Sharing stories about the diverse and exciting cyber security roles and ways people harness these critical skills across all kinds of industries is one way to raise awareness. Exposing students to these hot digital careers may inspire a study pathway never considered before.

We have created a Cyber Security & Awareness playlist for teachers and schools to use on our CSER YouTube page. The videos we have curated are a start, but we need your help to curate more diverse examples!

We would love to showcase more stories of the incredible Cyber Security champions in our Australian communities and across a range of industries. Whether you're looking after a school or business network, working for a large STEM organisation or need to consider cyber security and awareness as part of your professional role (in marketing, finance, teaching or more), **we would love to feature your story!**

How to get involved?

It's simple: take your phone and record a video in under 5 minutes! Tell us:

- What is your role and where do you work?
- What did you study?
- What do you do in your role or what does a typical day look like?
- What do you enjoy about your job?
- What skills are important in your role?
- Why is your job important or why is cyber security & awareness knowledge and skills critical to your role?

Email your short video to us at cser@adelaide.edu.au or Tweet it at us @cserAdelaide

See our YouTube Playlist at <https://bit.ly/CybersecurityCareersPlaylist>

HOW CAN I TEACH CYBER SECURITY IN THE PRIMARY CLASSROOM?

Cyber security provides an increasingly important and relevant context for teaching young children key areas of the Australian Curriculum: Digital Technologies. Here we highlight a few example ideas from our latest cyber security MOOC for K-6 Teachers.

A Data Selfie

Data plays a critical role in understanding how we leave traces of our information online and how people can extract information about us. Inspired by 'Hello Ruby', a series of books by Linda Liukas, we expand on the Data Selfie activity. Students list elements of their recent online activity history (or using some fake data about a character) and in groups they try to piece the information together to guess who the profile is for based on the data. Students consider: What do they like? What does their online behaviour tell us about who they are?

DataSelfie

Write up the following information.

- 5 things you've searched online
- 4 things you've liked or given thumbs up to
- 3 videos you've watched
- 2 places you've been with a mobile phone
- 1 person you've messaged with

Adapted from [source]

If I were an algorithm, this is how I would imagine this DATA as a person

They would like Ads like this

They would read websites like this

A Network Scavenger Hunt

Young students can start by recognising which familiar devices use wireless networks and which objects are not connected to a network. Building on this, students can explore how technology has evolved over time to become less "wired" through identifying differences in past and present technology. Using these foundational ideas, students start by classifying different technologies in their groups and then undertaking a scavenger exercise.

Is it connected to a Network?

There are many different objects and digital devices all around us - in our homes and in our classroom.

Take a look around. Can you find other objects? Where would a printer, keyboard or home assistant fit and why?

<p>Not connected</p> <p>BeeBot Toy car USB</p>	<p>Wired</p> <p>Rotary phone MaKey MaKey Wired Mouse</p>
<p>Wireless (Bluetooth)</p> <p>Bluetooth Robots Bluetooth speakers Bluetooth headphones</p>	<p>Wireless (WiFi)</p> <p>Tablet Laptop Smart phone</p> <p>Some of these devices also have Bluetooth so that they can connect with other Bluetooth devices.</p>

Spot the Difference!

Being able to apply critical thinking and analysis to the information we receive is important. How savvy are students in being able to tell what is real and what is fake? Can they tell when someone is trying to access private information? In this activity, students look at teacher-constructed 'phishing' letters or emails. They use their newly learned skills to identify any phishing indicators - stopping scammers in their tracks!

ARE YOU READY?

Can you spot the signs that this is a phishing email?

subject: ~~YOUR URGENT ACTION NEEDED~~

GamePlace: <no-reply@gameplace.com>

Dear valud customer

Thank you for purchasing a 12-moth online subscription with GamePlace. You can download exclusive ~~content~~ using the codes below for the next 12 hours. You can ~~also~~ share this email and codes with your friends. Hurry, so you don't miss out!

SHEIKADSL901 B0ESLKEH231 LULSPEAKO765

CLICK HERE

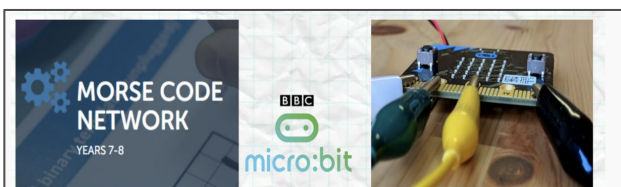
Access the full lesson plans and more in the Primary Years Cyber Security & Awareness MOOC at csermoocs.adelaide.edu.au/available-moocs

CYBER SECURITY ACTIVITIES FOR HIGH SCHOOL

There are many interesting activities that you can use to develop cyber security and awareness knowledge and skills with high school students that align to the Australian Curriculum: Digital Technologies.

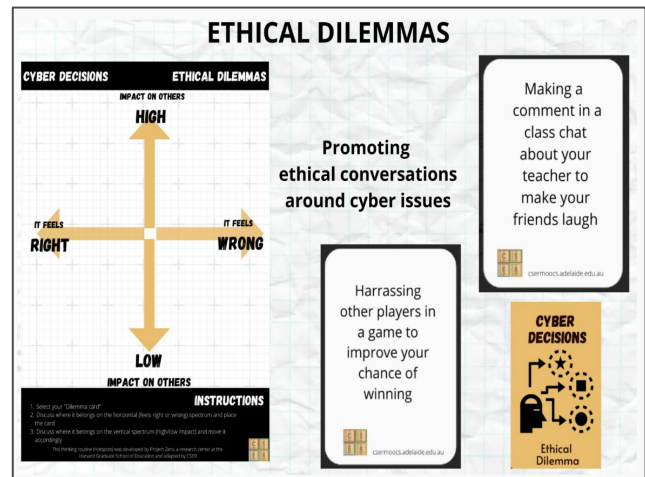
A Data Selfie

In Year 7 and 8, students explore networks and analyse the properties of networked systems and their suitability and use for the transmission of data types. They acquire, analyse, validate and evaluate various types of data, and appreciate the complexities of storing and transmitting that data in digital systems. To gain hands-on experience, we showcase a [lesson](#) developed by DLTV for the Digital Technologies Hub in which students use a BBC Micro:bit to simulate a packet switching network, using Morse code as a metaphor.



Developing an ethical lens

In years 7 and 8 students are expected to apply ethical behaviours, identifying cultural considerations when participating in online communities. By years 9 and 10 there is a progression to follow protocols, and to influence and develop their own guidelines for facilitating an ethically considerate environment. Inspired by an activity on the *Thinking Hotspots* routine by Project Zero, we present an activity in which students use our CSER Ethical Dilemma cards to critically think about ethical issues and to engage in analytical discussion and reflection. Students pick a card, discuss the issue and then place the card on the provided quadrant template. Our cards are free to download in our MOOC.



Race to re-build blockchain

Blockchain is a cutting-edge security method. In years 7-10 students are to investigate and analyse data transmission and security and to critically reflect on privacy and security requirements, risks and protocols. **Hashing** is a fundamental part of understanding how blockchain works as it uses complex algorithms to generate hash codes for each block which are very difficult for someone to break into and edit; providing an interesting context. In teams, students can use mathematical problem-solving to figure out hash numbers for blockchain blocks using a secret hash algorithm provided by the teacher. By figuring out the hash numbers, they can rebuild the transactions in the correct sequence, with the aim to be the team who wins the race! This is a simple *representation* of how Blockchain works, providing a basis for learning about the complexities of blockchain, risks and potential uses.

Blockchain hash algorithm

First letter of sender name + First letter of receiver name + (dd + mm + yy) * transaction quantity - previous hash number

Note: Alphabet letters need to be converted into the numeric place in the alphabet (e.g. A= 1, R = 18). Capitalisation does not matter. Our blockchain hash should have 3 digits (e.g. 321 or 004).

Transaction

Sender: Betty Howard
Receiver: Sam Hamilton
Date: 30/09/20
#4
Previous hash: 129

Example:

$$= B + S + (30 + 9 + 20) * 4 - 129$$

$$= 2 + 19 + (30 + 9 + 20) * 4 - 129$$

Access the full lesson plans and more in the [Secondary Years Cyber Security & Awareness MOOC at csermoocs.adelaide.edu.au/available-moocs](https://csermoocs.adelaide.edu.au/available-moocs)