Cyber Challenge 1: Information Privacy and Security

https://groklearning.com/course/cyber-hs-infosec/

About this activity

The world of cybersecurity can often be inaccessible to school students. This Challenge aims to provide students an authentic and accessible insight into cybersecurity.

The first step in understanding cyber security is knowing how to keep you and your information safe from people and software seeking to do you harm.

In this challenge, students begin by analysing the sharing habits of typical teen characters as they interact on social media.

The four modules of this challenge are:

1. Purposeful sharing
2. Simple passwords
3. More difficult passwords
4. Trickier sleuthing

The learning materials in every module include notes, guided experimentation, programming activities and problems to test understanding and skills. The video resources are designed both to teach students about specific programming/cipher concepts, but also to give students a view into what working in cybersecurity is really like, and what people working in this field do on a day to day basis.
The people in the videos are all employees of the organisations they represent, and work in variety of roles ranging from a security analyst, all the way to the Chief Security Information Officer.

Age

This challenge targets students in year 7 and 8. It is also suitable for students in older years who need to think about their information security and privacy (timing will differ).

Language

No programming languages used.

Time

The Challenge is designed to be completed over 4-6 hours.

Key Concepts

Key Concept	Coverage
Privacy	Freedom from damaging publicity, public scrutiny, surveillance, and disclosure of personal information, usually by a government or a private organization. https://en.wiktionary.org/wiki/privacy
Security	The condition of not being threatened, especially physically, psychologically, emotionally, or financially. https://en.wiktionary.org/wiki/security
Risk	1. A possible, usually negative, outcome, e.g., a danger. 2. The likelihood of a negative outcome. https://en.wiktionary.org/wiki/risk
Ethics	1. (philosophy) The study of principles relating to right and wrong conduct. 2. The standards that govern the conduct of a person, especially a member of a profession. https://en.wiktionary.org/wiki/ethics

Objectives (Content Descriptions)

ICT General Capabilities

Apply digital information security practices	independently apply strategies for determining the appropriate type of digital information suited to the location of storage and adequate security for online environments
Apply personal security protocols	identify and value the rights to identity, privacy and emotional safety for themselves and others when using ICT and apply generally accepted social protocols when using ICT to collaborate with local and global communities

What are we learning? (Abstract)

After completing the modules, students will be able to:

- Determine what information is best kept private
- Explain the difference between good and bad passwords and why
- Be conscious of what they are sharing over time
- Understand risks to personal safety from careless sharing

Module outline

The Challenge consists of four modules:

1. Purposeful sharing
   This module introduces the concept of sleuthing - gathering information from what friends post online. It is always done openly and without malice. Students should start to understand just how much information is being given away online.
2. Simple passwords
   This module introduces students to poor password practices like using very common, easily crackable passwords. Password cracking is always done with the express permission of the characters within the challenge. It's important to also address the ethics of hacking with the students.
3. More difficult passwords
   This module extends students past thinking about simple to crack passwords and includes difficult to hack passwords that are nevertheless <something> because they have been leaked and are being used in multiple accounts. Students should begin to think about the impacts of someone gaining access to their email account and also the benefits of two factor authentication.
4. Ethics of sleuthing
   This module is an extension of all that has been learned. Skills are put to use in different ways and the students should think about how much personal information can be gathered from innocuous seeming things.

Types of component:

Discussion	**Worksheet**	**Computer-based Activity**	
Group Activity	**Unplugged Activity**	**Video**	**Read**
Animation	**Reflection**	**Game**	**App**

Challenge Introduction — why study information privacy and security?

Let's start with a definition: cyber security is a fancy name for a collection of tools and methods that people or companies use to protect themselves, their networks, systems or programs from attack. Attackers are usually trying to get access to electronically stored sensitive information, or to steal money.

So understanding these tools and methods is a pretty good way to learn how to keep yourself safe online. But not just that - cyber security is a great source of future jobs. There is a significant shortage of people with the skills to help protect companies and other people, and that's according to AustCyber — the Australian Cyber Security Growth Network.

To learn about cyber security we're going to look in on a group of friends who chat and share stuff with each other on a couple of apps. Let's go!

New Vocabulary

Privacy: Freedom from damaging publicity, public scrutiny, surveillance, and disclosure of personal information, usually by a government or a private organization.

Security: The condition of not being threatened, especially physically, psychologically, emotionally, or financially.

Risk: A possible, usually negative, outcome, e.g., a danger. *Also* The likelihood of a negative outcome.

Ethics: The study of principles relating to right and wrong conduct. *Also* The standards that govern the conduct of a person, especially a member of a profession.

Activity 1 - Purposeful sharing

Preparation and timing

No prior knowledge is required for this activity.

Overview

- What is privacy?
- What information online can put you at risk?
- What does it mean to be “purposeful” about what you share?

Suggested Implementation

Video:
Watch the video Growing Up Digital - Privacy Segment http://fuse.education.vic.gov.au/?YDGLC5

Take notes about one thing you agree with, one thing you disagree with and one thing you thought was interesting or hadn’t thought of before.

Discussion:
Share points from the notes taken from the video.
Do the students generally agree or disagree with the video? Do they agree or disagree with each other?

In the video the students talk about “Oversharing”, in the resources we talk about “Purposeful sharing”.
What do you think are the differences between these two terms? Do you like the use of oversharing? Or Purposeful sharing or some other term and why?

Lead the students to talk about what is meant by oversharing or purposeful sharing. The terms are very similar, the reason we chose purposeful sharing is because it doesn’t imply that sharing is **bad** just that you need to be thoughtful about the picture you’re building about yourself.

Example questions: Have you heard a message that children shouldn’t share much at all on social media? Is that practical? Where do you think the line is between what’s OK to share and what isn’t? Is not sharing at all on social media practical? Why?

Through previous cyber safety education programs or from home, students may have been given messages ranging from “don’t go on social media” to “be careful on social media”. Depending on the prior learning of students in the class, the discussion can either start from checking what they know about purposeful sharing or examples they might be able to provide of purposeful sharing.

Maybe talk about different content being appropriate for different audiences. Discuss the fact that even when you share with only a few people that data is only as safe as the platform it's posted on and the site has access to everything for marketing purposes.

Unplugged Activity: Cyber Security Card Games "Know your risks"

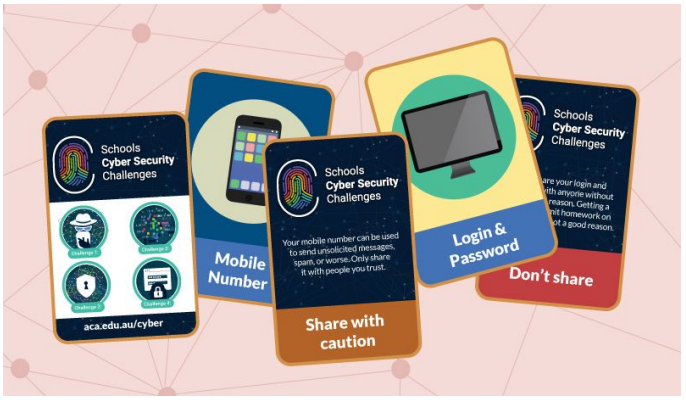
Download and print the cards from the ACA website using the link below. Cut them up to play the game - 1 set per 2-3 students.

Cyber security card game "Know your risks" https://cmp.ac/cyber-cards

Card game instructions

Aim: To get students thinking about how much information they share, how pieces of information can be joined to form a detailed picture of them and to get students to think about and articulate the risks.

How to play:
There are three categories of cards, **"Don't Share"**, **"OK to Share"** and **"Share with caution"**.



1. Students are given the cards and told to look at the picture side and in pairs or groups of three to sort the cards into the three piles as quickly as they can (We generally give them a 60-90 second timer to encourage them to think quickly).

2. Students then turn over the cards to see if they put any in the wrong pile (i.e. they disagree with our assessment of the risks).

3. Read the blurb from the back of the cards regarding why we categorised that piece of information this way.

4. Then have a class discussion about what they agree with or disagree with and why. Students who were more cautious than our categorisation should consider whether that's how they actually act on the internet of if they have shared risky information.

Information
Most students we've tested the game with have actually sorted the information more cautiously than we did. The reason we didn't just categorise everything as risky or "not ok to share" is because we want to take into account the realities of social media and how important it is in teenagers' lives... we didn't want to encourage students not to share anything because it’s unrealistic.

Computer-based Activity : Cyber Challenge 1: Information Privacy and Security
Complete Module 1: Purposeful sharing
https://groklearning.com/course/cyber-hs-infosec/

Video:

Watch the video: These children face the reality of growing up online I UNICEF
https://www.youtube.com/watch?v=hAKTF486eMY

End of Module discussion questions:

Reflection **Group Activity**

The world has changed, teens overwhelmingly spend much of their social lives online.

Discuss in small groups:
Why are the students in the UNICEF video so uncomfortable about strangers knowing so much about them when the students themselves posted this information?

Come up with 5 Rules of Engagement to give to kids who have never been on social media before. How would you advise them to keep themselves safe and their private information private?

Activity 2 - Basic Passwords

Preparation and timing

No prior knowledge is required for this activity.

Overview

- Why do we need passwords?
- What are common password mistakes?
- What makes a good password?

Suggested Implementation

Unplugged Activity **Group Activity**

Mastermind...

Go to this website: https://www.wikihow.com/Play-Mastermind-With-a-Pencil-and-a-Piece-of-Paper

Print out enough Mastermind templates for the class. Templates can be found at https://cmp.ac/mastermind

Follow the instructions on the Wikihow page to play the game of mastermind with paper…

Information
This activity is letting students realise how easy simple and short passwords are to crack. It's so easy that human can do it in about 12 steps so how quickly could a computer "guess" that short password?

Discussion:

In the game students "cracked" a 4-character long password simply.
What do you think that tells you about the length of passwords?

Come up with the first rule of passwords!

Computer-based Activity
Complete Module : Simple Passwords
https://groklearning.com/course/cyber-hs-infosec/

Wrap up:

Reflection **Group Activity**
Passwords are used everywhere

In small groups students start to develop the rules of good passwords - at least 3.

They should also come up with a symbol that represents a password. Direct the students to look at the complete emoji list https://getemoji.com/ ... which one do they choose to best represent password safety and why?

Information
Some students are likely to pick a padlock and others might possibly pick a shhh face. It's worth having a couple that you've selected to encourage discussion about what features of each image represents a password and which don't.

Activity 3 - More Difficult Passwords

Preparation and timing

Before starting this activity the students should have completed the “Simple Password” activity. This is an extension of those ideas.

Overview

- Why do we need passwords?
- What are common password mistakes?
- What makes a good password?

Suggested Implementation

Video:
Watch the video: Cyber Security (by Crash Course Computer Science)
https://www.youtube.com/watch?v=bPVaOlJ6ln0 (12:30)

> **Information**
> Note that this video is designed to get across a lot of information in a very short amount of time. The students are not expected to understand all that information is the first viewing. It’s more important that they engage with it and have a discussion afterwards.

This video moves pretty fast. Write down 2-3 things you learned from the video, maybe that’s a definition or maybe it’s something you haven’t heard of before or something that made you think..

Discussion:
What did we learn from the video?
Get students to share their 2-3 things they learned with another student and decide which of the 4-6 things they both agree are the most important.
Then get the pair to work with another group, and try to convince the other group why the thing they thought was important should be chosen by all four...
Continue this process until there is one agreed point as the most important. Why did we all agree this was the most important one? Share a couple of the others.

Computer-based Activity
Complete Module 3: More Difficult Passwords
https://groklearning.com/course/cyber-hs-infosec/

Reflection **Group Activity**
Passwords are used everywhere

In the small groups from last time students finish developing the rules of good passwords.

Put rules in a document and include the emoji from the last module.
Share the rules with the class, do any groups differ on the rules? Do the rules match what is currently used as your school password policy? If not can you imagine or find out why not?

Bonus Discussion:
We've found this password checker online (https://howsecureismypassword.net/), you can enter your password and find out how secure it is. Is it a good idea to use a tool like this? (**Note**: definitely don't put your passwords into any website tools ever!)

At companies that really care about security you have to change your password immediately if you ever enter it into a different website (e.g. if you use it on another account). Why do they do this? Is it important or overkill?

Other companies have a mandatory policy to force employees to change their passwords regularly (e.g. every 3 months). What might be some of the advantages and disadvantages of this?

Information
If the students are coping with the ideas in the Bonus discussion lead the discussion to talk about Biometric data such as fingerprints, iris scans and facial recognition. What kinds of issues are raised by these forms of security?
Lead students to thinking about what happens if a fingerprint or iris scan gets hacked… what do you do then? These are tricky ideas, there isn't really a solution. Multi-factor Authentication is really the only mitigation of issues with biometric data.

Activity 4 - Ethics of sleuthing

Preparation and timing

This is an extension that students will benefit from completing but they should focus on completing Modules 1-3 first because they form the core of the unit. This unit will focus on the ethics of “white-hat” vs “black-hat” hacking.

Overview

- Who could be looking at your information online?
- The ethics of snooping.
- Ethical hacking.

Suggested Implementation

Video:
Watch the video: Cyber Soldiers: White-hat hackers (by CBS News)
https://www.cbsnews.com/news/cyber-soldiers-cbsn-on-assignment/ (11:42)

EXTENSION: Read
https://www.itpro.co.uk/hacking/30282/what-is-ethical-hacking-white-hat-hackers-explained

Discussion: Socratic Circle/Seminar

> **Information**
> The Socratic seminar is a formal discussion, based on a text, in which the leader asks open-ended questions. Within the context of the discussion, students listen closely to the comments of others, thinking critically for themselves, and articulate their own thoughts and their responses to the thoughts of others. They learn to work cooperatively and to question intelligently and civilly. (89)
> *Israel, Elfie. “Examining Multiple Perspectives in Literature.” In Inquiry and the Literary Text: Constructing Discussions n the English Classroom. James Holden and John S. Schmit, eds. Urbana, IL: NCTE, 2002.*

Setup:

Students should be warned in advance of watching the video (and extension students reading the text) that they will need to continually refer back to the video and text in question to support their discussion.

Room arrangement:

Often an arrangement where the students can see each other to respond, agree and disagree is the best room arrangement for this activity. Perhaps, finding another space will be necessary because computer labs are often not set up for socratic seminars.

Student expectations:

There are clear differences between a discussion and a debate. A debate usually involved, prepared statements and rebuttals and two definite sides. It is spoken out to an audience rather than in to the people in the discussion. A discussion usually involves shifting opinion, to and fro between participants and a multitude of different sides and not one clear winner.

Teacher Expectations:

Have clear open-ended questions ready. (We have given you a few but you could also add more or different ones.)

Be in control of the time.

Adjudicate when discussions shift off topic and bring it back to the text and video.

Moderate if a few students are dominating the discussion and direct the questions to particular students.

Questions

Why do you think hacking exists?

Why do people become hackers?

What's the difference between a white hat and black hat hacker? (lead students to the idea that it's an internal decision to be one or the other and the skill-set is the same)

Why do companies pay white hack hackers?

Is it better for the company to hire a white hat hacker in advance or to pay someone who communicates with a company to demonstrate a vulnerability they have found after they have already located it? Support your answer.

Is it OK to hack people's accounts if you aren't stealing or benefitting from it?

Computer-based Activity

Complete Module 4: Trickier sleuthing

https://groklearning.com/course/cyber-hs-infosec/

Reflection **Group Activity (recommend a Break out Activity here)**

Cyber Security Breakout

Information

As the last module in the unit, it's a good idea to make it a bit special. Encourage engagement for a review exercise with a "Breakout activity". Use the activity to reinforce the learning from the last 3 modules and reward the students that find their way into the physical or virtual box with stickers or lollies. You can see more information about how to set this up in the following blog post from the edtechteam:

https://www.edtechteam.com/blog/2017/08/break-out-of-classroom/

Breakout Activity

This activity is designed to be the final activity in the Australian Computing Academy Schools Cyber Security Challenge: Information Privacy and Security.

It is designed as a breakout activity but can be delivered any way that suits the classroom in which it is being used.

There are four activities that are related to security and privacy.

Breakout setup:

Have a lockbox available with four locks. (There is a digital version that is less of a competition which can be done with four web pages with password access)

Have a prize (stickers or a bag a chocolate help)

Pair the students up because working on these problems together is a good way to overcome problems that individual students can encounter alone.

Print enough copies of the four challenges for each group to have 4 challenges. Only give out one challenge at a time.

Overview:

The four challenges are attached with answer sheets:

1. Terrible Password Crossword: Students can refer to the list of top 25 passwords to find the answers (Note: Numbers are used as well as letters) Hidden Word: PRIVACY
2. Fistbump profile: Belinda Brooks is worried that she might be giving her location away. Find 5 things on her profile that she should consider changing.
3. Code Breaker: Use the patterns in English to solve the code and find the secret word. The secret word is SAFETY. The quote is interesting in context and could be worth discussing as a class.
4. Logic Puzzle: Students use deductive reasoning to find the child who lives in which house with which pet by reading the social media posts. Answering the questions at the bottom with the first letter of the answer spells the secret word PRESCRIPTION

The full activity with all worksheets can be found at https://cmp.ac/breakout