LESSON PLAN

PRIVACY & CYBERSECURITY ONLINE: HOW LONG?

The videos in this lesson total approximately 75 minutes. In between sections, there are extra breakout / discussion sections of around 3 to 5 minutes where the students can discuss their lives online and connect with the reality of the training.

OPTION 1: You can simply play the videos - and do shorter breakouts of 2 to 3 minutes when prompted by the presenter on screen. (Total 90 minutes)
OPTION 2: OR you can make this lesson longer by spending more time on the breakouts, perhaps 5 to 7 minutes...(Total 120 minutes for the full experience)

WHAT'S EXPECTED OF YOU!

- **Download the lesson plan < yes, this document! > plus the (optional) teacher pack**
- **Play the videos within this lesson, look at Step 4 on your "Lesson Dashboard"**
- **Stop for group breakout / discussion sessions (approx. 3 to 5 mins - you decide how long)**
- **Complete the lesson**
- **Ask students to answer questions in an informal quiz, or take a written assessment**

WHAT WILL MAKE THIS LESSON SUCCESSFUL?

- **Preparation**: Download the lesson plan, read it, and place it by your PC. It's your map.
- If you like, watch it beforehand, so you feel comfortable with the content mentioned.
- Be interested / open and **not judgmental**, that's your enemy in this "subject": Teens may shock you with how exposed they are. See it more as a fascinating expose of a generation.
- However, many teens **may not want to talk** about this aspect of their life publicly.
- **It's ok not to know it all about their apps, trends etc.** Ask them to show you, or explain it. You don't need to have an answer, just to listen. If they need an answer, Google will have it, or you can email us on info@mysocialife.com if you have a tough question.
- **Watch the room** for students who feel uneasy – they may have experienced issues online (like sexting, bullying or trolling, for example). Check in after class that they are ok.
- Don't press anyone hard to speak publicly – social media and popular culture can be very cruel and some students use their knowledge or their following to assert who is cool, or who knows what. Publicly spotlighting can mean being shamed in front of their class. Or online later.

1. **Teacher action >> Play from intro**

Topic: How much do you know about privacy?
Key message: Privacy seems pretty simple on the surface. Most people think it's about settings. Few understand the concept of data points and data bundles (the information that websites and social platforms pick up from our behavior online). So in this introduction we establish that it's more complex than it seems and kick off with one simple metaphor – 'The Digital House.'

SECTION 2: BREAKOUT

Ask your students: "What is something in your life that you take steps to protect? Why? And how do you protect it?

Do you protect things **online** with the same energy and commitment?"

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes to discuss how they could "run some checks" on content or people.

3: Teacher action >> Play video - Part 2

Topic: Data points – what are those, and what do they do?
Key message: Anyone that is consuming information in the media will be, to some degree, influenced by it – even the news leans us (adults) in one direction or another. The results of our media choices can have positive and negative results. So do we fully own that our media consumption has this type of impact? You cannot hope to change outcomes and behaviours, or start to learn self-regulation, if you are not aware of the type of impact something has on you.

SECTION 4: BREAKOUT

Make the connection!

Ask your students:: "What are you watching or playing that may influence the way you see the world, your own body, your own potential?"

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes to discuss how they could "run some checks" on content or people.

5. **Teacher action >> Play video – Part 3**

Topic: In our surveys from students, many of them say they don't care that much about being tracked. But when you realise the cost of influence on the way you might see things, and that you are, to some degree, being used as a guinea pig by big social platforms to make money, it can change (some of) your students' perspective. The hard part is that we are stuck with this tracking, and we love to be online.

SECTION 6: BREAKOUT / EXERCISE

Online exercise: Ask your students (if they can access an iPad or computer) to take the OCEAN Test – an online psychometric profiling task, revealing how your personality profile changes as you answer the questions, and how that personality affects the way you "consume" media.

Link here:
https://ocean.tacticaltech.org/en/base/youth/

7. **Teacher action >> Play video – Part 4**

Topic: Misinformation
Key message: On the internet, pretty much anyone can say anything they want. They can post anything they want, and they can share untruths. If we are being fed information by bored people who want to try and get followers, or get attention, we are going to need to be pretty sharp in being able to see true from false.

SECTION 8: BREAKOUT

Online exercise: Take the misinformation quiz – either on your classroom screen, or they can use the link on their devices - just seven questions and see how much your students know.

Link here:
https://misinformationmedic.com.au/health-check/

8. Teacher action >> Play video 5

Topic: Privacy tools!

Key message: In this section we take a look at what your students can do to check their online profile, and see if their email address had been hacked without them even knowing. The challenge is that they may appear like they don't care or they know this stuff, but it's unlikely. These tools are not easy to find. It's taken us years to dig them all out. Those who see themselves as a bit of a cyber detective will enjoy it, or those who like privacy.

SECTION 9: BREAKOUT

Exercise: Either on your classroom screen, or they can use the link on their devices – go to www.privacytools.io
and see how much is there?

Link here: www.privacytools.io

10. Teacher action >> Play video 6

Topic: Privacy tools (Continued, Part 2)

Key message: More cool tools to offer proof of just how much we don't know we are tracked and how that information influences what we get 'served' online.

11. SECTION 11: BREAKOUT

Exercise: Inspect how your students' favourite websites are tracking their activity online using the **Blacklight** tool. How might this kind of behaviour disproportionately impact certain groups of people?

Link here: https://themarkup.org/blacklight

6. Teacher action >> Play video – Part 7

Topic: Privacy tools (Continued, Part 3)

Yes, that's right more tools. Why? Simply because there are so many ways that our privacy and security can be threatened. In this example – PIM EYES – people can steal our image (our photo) and pretend to be us. 'Catfishing!'

SECTION 12: BREAKOUT / EXERCISE

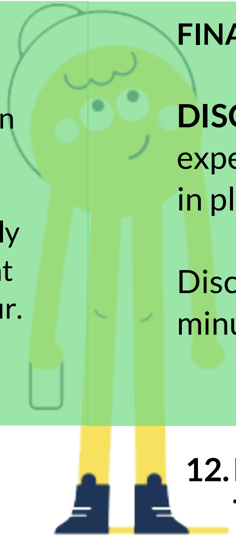
Online exercise: This is just an optional extra if you have time, and they are fascinated by the tools. Sometimes students feel like "they get the point, and it's enough of the tools already'.

If they can use their devices try the 'Pim Eyes' website at your discretion.

Link here: https://pimeyes.com/en

8. Teacher action >> Play video 8, 9 and 10

Topic: Cybersecurity
Key message: After closing up the privacy section with a basic checklist, we we look at the external threats, things like viruses, ransomware, and clickbait. Some they will know, some they will only know a little, but the idea here is just to show that there's a lot of cyber fraud and criminal behaviour. As they get older, they will see and hear about it more.



FINAL BREAKOUT

DISCUSS: Which cyber issues have you experienced, and what measures do you have in place – are they enough do you think?

Discuss in your groups of 2 or 3 for 3 to 5 minutes.

Phone : +27 83 455 4808
Email : info@mysocialife.com
www.mysocialife.com

12. Final action >> Download quiz

Topic: Revision!
You can make this a verbal quiz for fun, or a written test? It's really up to you.