LESSON PLAN

PRIVACY & CYBERSECURITY ONLINE: HOW LONG?

The videos in this lesson total approximately 55 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 65 minutes)
OPTION 2: OR you can make this lesson longer by spending more time on the breakouts, perhaps 5 to 7 minutes…(Total 90 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: What is privacy?
Key message: In the real world, it's the right to be left alone or not feel intrusion. Information privacy is the right to protect your personal information, data. And this is difficult because we are *drawn to* devices and social media. We need to start by understanding that *as humans* there's a reason we love to share, so we will need to make a choice about how we wish to lock up our digital house!

2. **SECTION 2: BREAKOUT**

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes.
Key message: Teachers need to help students connect with the fact that there are things worth deeply protecting because together they are important to any individual – many things are private or heard-earned!
Ask them: "What do you want to protect and keep safe on your phones, computers, tablets, gaming consoles etc? What matters enough to keep safe?"

3: Teacher action >> Play video - Part 2

Topic: Unpacking what's in the Digital House!
Key message: Kids absolutely love the things they create or own online – inside games it could be their 'worlds', their 'skins', their currency. But also our photos our passwords and our accounts. Together this forms part of our **'digital identity' – who we are online** – and that's why we need to protect our devices and data. Unfortunately we also need to explain why humans (adults and kids) want to steal from, break, damage, or hurt people online? Making money - or their troubled past experiences - are key reasons.

SECTION 4: BREAKOUT

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes.

Ask them: "What do you want to protect and keep safe **in real life** and what measures do you take to protect it"

Key message: Some families use house alarms, locked doors, we lock cupboards, have seat belts in cars, we use dog leads. We need this level of care online…because there is a greater likelihood of a hack, breach, theft online …than at home.

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

Topic: Kids overlook that a privacy breach can come from the strangest of places – friends, siblings, and not just hackers.

Key message: Kids overlook that a privacy breach can come from the strangest of places – friends, siblings, and not just hackers. The point is that many people (adults) experience hacks, breaches theft in their lifetime. So be careful which websites and games you choose…!

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

Topic: Personal versus private
Key message: There is a big difference between how we behave in real life and how we behave online. We try out personalities more online. Once we understand this, we then need to be conscious of what are the different levels of what we should share.

SECTION 7: BREAKOUT

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes.

Ask them: "What's the difference between personal and private?"
Key message: It's sometimes quite surprising how kids (and even some adults) don't know this difference. The more we share that's **private (unique to us),** the easier it is for a stranger/hacker to build a story about us, and approach us!

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

Topic: Explaining personal versus private
Key message: In this section, we share a video from the leaders in online safety in the United States, Common Sense Media, which very re-inforces what we are working on in this lesson. The video helps to visualize the concept.

9. Teacher action >> Play video 6

Topic: What to share and what not to share
Key message: Unfortunately in a world of sharing, we see kids and adults share way too much, where they live, where they are at any moment (Snapmaps), a photo of a credit card or ID. We then get kids to dig into what happens when a device is breached, so they connect to the consequences.

SECTION 10: BREAKOUT

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes.

Ask them: "What could happen if someone has your password. There are many different things they could do maliciously?"

Key message: Let them share their findings! When we hear from others about how mean people can be, we realise and **feel the consequences.** It impresses the need to be secure.

10. Teacher action >> Play video 7

Topic: Phone and app settings
Key message: Ideally the setting up of a phone is the job of a parent. However, many parents don't know how, which leaves it to teachers to assist. Settings are not complicated. We just actually need to open them up and work through them. Try it with your students. Open an app (Snapchat or Tik Tok) and then click on the menu in top corner and work down to Privacy / Security.

SECTION 11: BREAKOUT

Break students into groups of 2, 3 or 4 and give them 3 to 5 minutes.

Ask them: When have you been **clickbaited**? What is the worst type of clickbait, Who has been badly tricked by clicking on a link and been hacked, personally abused or threatened by someone, or they have destroyed something of yours online?

12. Teacher action >> Final tip

Topic: Tune in to your 'gut'

If you get a feeling that something isn't right, don't share, don't connect with a stranger, don't click on a link. Move on. Your body and brain has a way of knowing things! Trust it.

13. Teacher action >> Download quiz

Topic: Revision!

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

DON'T FORGET TO DOWNLOAD THE TEST!

ENJOY!

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