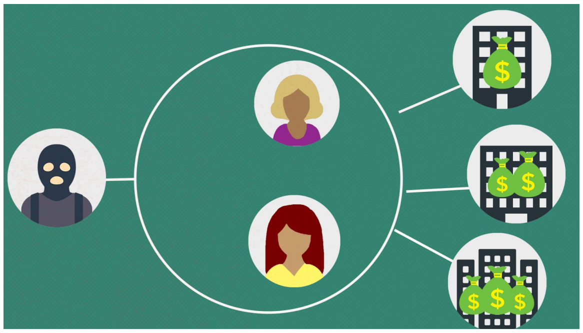
The Lowdown
Connecting newsroom to classroom

Lesson Plan: Who's Snooping on You Online?

By Andrea Aust



Featured Resources

Above the Noise: Who's Snooping on You Online?

The Lowdown: How Bots and Trolls Influenced the 2016 Election and Threaten Our Democracy

Opening Quick-Write Prompt

Do you know what personal information is tracked and gathered by the apps and sites that you use? What concerns do you have about cybersecurity, if any?

A quick write allows students to write down their thoughts before discussing the opening question in order to increase participation and make the discussion more accessible to English Language Learners.

Objective

- Students will analyze cybersecurity risks, how information about their online activity is monitored and used, and ways they can protect their privacy online.
- Students will evaluate cybersecurity risks, write a response about what concerns them most and develop their own threat model.

Essential Question and Lesson Context

What can you do to protect your privacy online?

Companies routinely track our activities online -- what we search, what we buy, what videos we watch and what we post to social media. Most of the time this tracking is used for targeted ads. And while this may seem relatively harmless, there is sometimes more at play than just companies trying to sell us stuff. Our information can be bought and used by people in order to influence our opinions about issues or political candidates through not-so-scrupulous methods.

So how do we know if we're doing enough to protect our privacy? While protecting everything from everyone all the time may be overwhelming, you can create a threat model to protect the stuff that's really important to you from the people that pose the greatest threats. Here are the five questions to answer to build your threat model:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to avoid those consequences?

Key Vocabulary

Pre-teach key vocabulary before students do the activity, especially if you have English Language Learners. After going over the simple definition, consider providing a visual aid or having students draw one. More ideas for how to pre-teach vocabulary can be found here.

Word	Simple definition
Authentication (n.)	The process of verifying the identity of a user, in order to give the user access to an account, files, program, etc. *When I use my debit card, I have to enter my PIN for **authentication.***
Civil liberties (n.)	The freedoms individuals have that the government can not interfere with *The right to be free of government searches, speak freely and practice a religion of your choice are **civil liberties**.*
Cybersecurity (n.)	The protection of computers, networks and programs from damage, theft of data or disruption of services *As more of our daily activities move online, **cybersecurity** becomes an even more important issue.*
Data broker (n.)	A company that gathers information from a lot of sources, organizes it into categories and then sells it to other companies *Some businesses buy information from **data brokers** in order to show specific ads to people online.*
Encryption (n.)	A way of protecting information by translating it into a code so that only people who have a password can read it *Many apps and websites use **encryption** to keep communications and transactions secure.*
Surveillance (n.)	A close watch over something or someone *Digital **surveillance** often happens when you use free apps.*
Virtual private network (n.)	A group of computers that are connected and can be used to encrypt information that is being sent over the Internet *Using a **virtual private network** will keep your information safe when connecting to wifi at the local coffee shop.*

Investigate

- Discuss the quick-write prompt to gauge what students think about this issue. What concerns do students have about cybersecurity?
  - ***NOTE****: The quick-write prompt is designed to begin the conversation and prepare students to write more detailed responses later in the lesson.*

- Ask students if they know what personal information is tracked and gathered by the social media apps and sites that they use. How do they think this information may be used? Make a list on the board.

- Read The Lowdown post on the role that Russian trolls and bots played in the 2016 U.S. election, and how such interference can threaten the democratic process. Ask students if they saw any evidence of this in their social media feeds in the run-up to the election, and how they determined whether or not to take the information seriously. Also have students consider and discuss how much they think such misinformation actually influenced voter behavior.

- Have students watch the Above the Noise episode as a class.
  - **Stop the video at 1:08 and ask:** What is threat modelling?
  - **Stop at 2:06:** Review the five questions that make up a threat model; (you may want to list these on the board). Clarify any that the students don't understand.
  - **Stop at 3:13 and ask:** What are some ways to keep your password secure?
  - **Stop at 3:48 and ask:** What are data trackers? How do they collect and use your information? Why do you think this could be a problem?
  - **Stop at 5:12 and ask:** Do you know what information your school or district is collecting from you while you are using a school computer? *(Note to teachers: Find this out ahead of time if you don't already know. This is an excellent chance to learn about your school's and/or district's privacy policies. You may also want to save this discussion until the end of the video.)*
  - **Stop at 6:13 and ask:** What is end-to-end encryption? Why and when would you want to make sure you're using it? How do you know if a website that you are using is encrypted?
  - **Stop at 6:41 and ask:** Why are open wifi networks risky? How can you protect yourself while using an open wifi network?

- Ask students if anything in the Above the Noise episode surprised them. In pairs, have students take turns sharing any new concerns about cybersecurity they have with each other.

- **Transition to the Make and Share:** Tell students they will have a chance to share their concerns about cybersecurity and thoughts about cyberattacks related to the election in the comments section of The Lowdown. The first time they comment, students must sign in to Disqus, a free discussion app embedded in The Lowdown.
    - To sign in to Disqus, click the "Comments" button at the bottom of The Lowdown.
    - Click the blue "Get Started" button in the gray "Welcome to Disqus" box.
    - Students will need to enter a username. We recommend first name, last initial.
    - After signing in for the first time, students must verify their email address before commenting. A verification email will appear in their inbox once they sign in to Disqus.

Make and Share

- Individually or in small groups, students post responses in the comments section about their concerns about cybersecurity in general or about cyberattacks related to the election.
    - Responses should be supported by evidence from the Above the Noise episode, The Lowdown post, or other research on the topic. (See source list)
    - Encourage students to reply to other comments after posting their response. Remind them to use evidence to support their claims and respectful language when replying to others.
- Students can create their own response or use the following questions as a starting point:
    - What concerns you most about cybersecurity?
    - How can we balance online privacy vs the convenience of using websites and apps?
    - When you think of your personal "threat model" what comes to mind? What personal data do you think is the most important to protect?
    - How can you best ensure that the information you get is accurate and from a real source?

Assessment/Reflection

- Students reflect on what they have learned either through a class discussion or in writing:
    - What is your biggest takeaway about cybersecurity and protecting your information online?
    - What was it like to post your responses publically and reply to other posts? What did you learn from other students? What do you hope they learned from

you? What will you do the next time you post a comment in response to The Lowdown?

Circle chats, small-group discussions and think-pair-share provide a safer space for students to practice speaking and listening, and also boost participation during whole-class discussions.

Extension/Homework

Create a threat model: Have students create a threat model for their biggest personal privacy concern using the five questions listed in the lesson context and in the Above the Noise episode.

Write/speak locally: Students turn their response to this issue into a letter, short speech or presentation, then research ways to make their voice heard in their community. (Example: Speaking during the public comment section of a city council meeting, posting in an online forum, etc.) For a list of how to contact local officials in your area, check out KQED Learning's Local Election Toolkit.

Common Core Standards and NGSS

CCSS.ELA-Literacy.CCRA.R.1	Read closely to determine what the text says explicitly and to make logical inferences from it; cite specific textual evidence when writing or speaking to support conclusions drawn from the text.
CCSS.ELA-Literacy.CCRA.R.7	Integrate and evaluate content presented in diverse media and formats, including visually and quantitatively, as well as in words.
CCSS.ELA-Literacy.W1	Write arguments to support claims with clear reasons and relevant evidence.
NGSS.SEP.7	Engaging in argument from evidence
NGSS.SEP.8	Obtaining, evaluating and communicating information
NGSS Appendix J: Core Idea 2	Influence of engineering, technology and science on society and the natural world