

Follow Me Around Paris

EXERCISE-IN-A-BOX LESSON PLAN

OVERVIEW

Students will learn about the risks and potential consequences of oversharing personal information on social media platforms and using public Wi-Fi networks, as well as the dangers of geotagging their locations. This lesson aims to raise awareness about online privacy and security.

LEARNING OBJECTIVES

Students will be able to:

- Describe the risks associated with geotagging and location sharing on social media.
- Demonstrate an understanding of how public wifi networks can be unsecure
- Analyse the risks of oversharing on social media and develop strategies for protecting their privacy while still engaging with social media.

DURATION

60 minutes + project work (duration as needed)

KEYWORDS

- **Geotagging:** A feature that allows you to add location information, like the name of a place or its coordinates, to a photo or video you post online.
- **Public Wifi Network:** Public wifi networks are wifi networks available for anyone, typically in places like coffee shops, airports, or libraries. Public networks can be unsafe to use because bad actors or malicious criminals can intercept your connection and potentially steal your personal information, such as your passwords, credit card information, or other sensitive data.
- **Oversharing:** Oversharing on social media is when you share too much personal information online, such as your location or phone number. Sharing too much information online can have serious negative consequences as it leaves you vulnerable to many cyber risks.

INTERNET INDEPENDENT FRAMEWORK

The learning objectives in this workshop are aligned with the **Privacy & Information Security** pillar of the Internet Independent Framework. Visit cyberlite.org for more information.

Follow Me Around Paris

EXERCISE-IN-A-BOX LESSON PLAN



WARM-UP 5 MINUTES

Slide 1

Say: Today, we will be learning about privacy and information security. When we go on social media, we're interacting and sharing our content with millions of users. It can then be tricky to understand what kind of content is appropriate to share on the internet.

Slide 2

Ask: Do you post anything on social media? How do you choose what to share online?

This is a good opportunity for teachers to gather insight on your students' social media habits and their motivations of posting online. Some may post to share photos and videos with friends, others might do it to go viral and get lots of followers.



DEFINE THE KEYWORDS 15 MINUTES

Slide 3

Ask: Does anyone know what geotagging, public wifi network, or oversharing mean?

Allow students to guess or extrapolate meanings. Guide students to think about these key concepts in the context of privacy and information security.

Slide 4

Read the contents of the slide aloud.

Discuss: Have you ever shared your location or checked into a place on social media? Why or why not?

Location sharing or geotagging is a key feature on social media apps such as Instagram and Snapchat, where users can tag where their photos or videos were taken.

Slide 5

Read the contents of the slide aloud.

Discuss: Where would you normally find free public wifi (outside of the school or home)?

Popular public places that offer free public wifi networks are libraries, coffee shops, or shopping malls. When connected to public wifi, it is important to

remember not to enter in any sensitive information such as credit card details as it is a vulnerable, unsecure network that can be intercepted by hackers.

Slide 6

Read the contents of the slide aloud.

Discuss: What's the difference between sharing and oversharing on social media?

Sharing on social media can be posting photos of friends having fun at a birthday party or videos of their pets doing funny things. The content does not expose the user's personal information, location, or any other identifiable information. Oversharing means you leave information like your address, live location, or phone number for the internet to access.



INVESTIGATE THE SCENARIO

30 MINUTES

Slide 7

Say: In this next section, we will explore a scenario about Kyle Kenner's trip to Paris as a famous celebrity. Remember to keep the keywords we've just learned in mind as I show you five pieces of evidence we'll investigate together. Think critically about the information we're examining and consider the discussion questions.

(Optional) Select three students to read as these characters: Kyle Kenner, Detective Henri, and a journalist of Global News Daily. Commenters: Kenner Fan For Life, Scarlet, Delilah, Woo-Jin, and Marissa.

Slide 8

Read Kyle Kenner's livestream on social media.

Discuss the following questions:

1. Do you think it's a good idea for Kyle to livestream and share her exact location? Why or why not?

No, it's not a good idea for Kyle to livestream her exact location. Because it's a live stream, that means anyone can find out where she is at that moment. This can be very dangerous as she doesn't know who may be watching her online.

2. Why might it not be safe for Kyle to overshare her shopping on social media?

Kyle is a famous celebrity who is livestreaming her luxury shopping spree with her fans on social media. It may not be safe for Kyle to overshare her expensive purchases because sharing her shopping or buying habits on social media can make her a target for theft or fraud. Cybercriminals can use this information to target you with scams or steal your identity.

Slide 9

Read Kyle Kenner's social map.

Discuss the following questions:

1. What specific details about Kyle's activities and location did she share on her social media platform?

Kyle has shared all the details of her entire day on social media, including the time and place of each activity. From this map, we're able to see where Kyle is staying, where she went shopping, and which places she visited for lunch and dinner.

Slide 10

Read this social media post by Kyle.

Discuss the following questions:

1. How do you think the thieves were able to find out which hotel Kyle was staying at?

The thieves were able to find out which hotel Kyle was staying at by following her social map where she checked into her hotel and posted the location online. Her oversharing has led to the gang being able to track her down.

2. What are some potential negative consequences that Kyle could face as a result of geotagging her location on social media?

Some negative consequences include an overexposure of her location and activities, which has landed in the wrong hands as she didn't know who was following her online and offline. She has not protected her own privacy and has put herself in danger.

Slide 11

Read this police report by Detective Henri.

Discuss the following questions:

1. How could Kyle have prevented these crimes from occurring?

Kyle could have prevented the cyberattack on her bank account if she didn't connect to a public wifi network while dining at Cafe de Eiffel Tower. She also could have prevented the robbery of her diamond ring by not oversharing her location and activities online.

2. What could Kyle have done to protect her device from getting hacked on a public wifi network?

Kyle should have connected to a VPN network to protect her device when connected to a public wifi network. She should also refrain from entering sensitive data into websites when connecting to a public network, such as her banking details.

3. What behaviours should Kyle change so this doesn't happen again?

Kyle should learn not to overshare on social media and flaunt her expensive purchases to people as it is a strong motivation for criminals to rob her. She should also be careful when connected to a public wifi network.

Slide 12

Read this article in the Global News Daily.

Discuss the following questions:

1. How could Kyle protect her privacy while still sharing her experiences with her followers?

To protect herself online, it's important for Kyle to be mindful of the information she shares on social media. Avoid posting location information, especially in real-time, and review your privacy settings to ensure that you are only sharing information with trusted individuals. It's also important to use strong and unique passwords, enable two-factor authentication on your accounts, and avoid using public Wi-Fi networks for sensitive transactions.

2. How can geotagging contribute to the danger of oversharing on social media?

Geotagging can contribute to the danger of oversharing by providing precise location information to followers and potential criminals. This information can be used to track movements and plan attacks.



PROJECT WORK

DURATION AS NEEDED

Slide 13

Say: Your project assignment is to create a handbook to help people protect their privacy and personal information while using social media platforms. The handbook should have suggestions and rules that emphasise safe online practices and highlight potential risks and dangers associated with oversharing, geotagging, and using public wifi networks.

Slide 14

Say: Read the instructions and questions carefully.

1. What personal information should be kept private and not shared on social media? List the best practices of online safety and why people should follow them when using social media. For example, you should never give out personal information and share your location.

2. What are the potential risks associated with geotagging and oversharing on social media?

3. How can users adjust their privacy settings to protect their personal information?

4. Develop rules and guidelines to help protect personal information and privacy while using social media.

5. Organise the handbook into sections based on the social media platforms and topics covered.

Note for Teachers

This project-based learning assignment is open-ended by design, so you have the flexibility to direct the project outcome as desired. It can be carried out individually or in collaborative groups.

Slide 15

Ask: Would anyone like to share the solution they have come up with?
Call on volunteers to share their projects.

**KEY TAKEAWAYS**

10 MINUTES

Slide 16

Say: Here are some things we've learned from this lesson.

1. While social media can be a good way to connect with others, it is never a good idea to overshare your activities on social media. Think about the types of information you should keep private to keep yourself safe.
2. Don't geotag your posts, especially in real-time (such as live streaming). You never know who is watching or following you.
3. Public wifi networks are unsecured connections, so hackers can easily intercept your device. Make sure you are on a secure, private wifi network if you are making online payments or entering sensitive information.

Ask: What are some key takeaways you've learned from this lesson?
Call on volunteers to share what they've learned.