LCE Lesson

Community Living > Digital and Online Skills > Digital Safety and Security

Lesson Code	DSS2
Short Objective	Online risks and threats
Competency	Describe online risks and threats, such as cyberbullying, phishing, and identity theft, and strategies to mitigate them.

Send to AI | Download | Print

Curriculum Standards

- **CCSS.ELA-LITERACY.SL.9-10.1:** Initiate and participate effectively in a range of collaborative discussions with diverse partners.
- **CCSS.ELA-LITERACY.RI.9-10.7:** Analyze various accounts of a subject told in different mediums.

Essential Question(s) / I Can Statement(s)

Essential Question(s):

- How can I protect myself from online risks and threats such as cyberbullying, phishing, and identity theft?

I Can Statement(s):

- I can identify common online threats such as cyberbullying, phishing, and identity theft.
- I can describe strategies to protect myself from online threats.
- I can explain how to respond to online threats in a safe and appropriate manner.

Lesson Objective(s) – Student Learning Outcome(s) for this learning experience

By the end of this lesson, students will be able to:

- Identify three common online threats: cyberbullying, phishing, and identity theft.
- Describe three strategies to mitigate each threat.
- Demonstrate appropriate responses to online threats through role-play scenarios.

Material/ Resources, Technology, Instructional Strategy [HLP 1]

- Anchor charts illustrating cyberbullying, phishing, and identity theft
- Scenario cards for role-play activity
- Worksheet: “Identifying Online Threats and Responses”
- Online safety checklist
- Markers, chart paper
- Projector to display online safety videos
- Interactive whiteboard for group brainstorming
- Online quiz platform (e.g., Kahoot or Google Forms) for formative assessment

Assessment/Evaluation [HLP 4, 5, 6]

Informal Formative Assessments: How progress towards lesson objectives is monitored as you are teaching

- Observation during role-play activity.
- Completion of “Identifying Online Threats and Responses” worksheet.

Formal Summative Assessments:

- Use a section of the LCE battery related to Digital and Online Skills to document student mastery of the lesson objectives.
- Online safety quiz assessing students’ understanding of online threats and response strategies.

Academic Feedback:

- Provide immediate feedback during class discussions to correct misunderstandings and reinforce correct responses.
- Use praise and constructive comments to encourage student participation and understanding.

Assessment/Evaluation Modifications:

- Visual aids (charts, posters) designed with symbols, images, and color coding to support students with different cognitive and language abilities, making the information accessible to those who might struggle with text-heavy content
- Allow extra time for responses.
- Provide vocabulary list or cards with pictures to support understanding of key terms.
- Read aloud or allow for use of text to speech software to read LCE battery or other written measures.
- Allow differentiated responses (i.e., expressing understanding in various formats [e.g., written, drawing, verbal].

Language Expectations [HLP 14: Cognitive and Meta-Cognitive Strategies, 15: Scaffolded Supports]

Key Language Task:

- Students will engage in small group discussions, analyzing scenario cards and identifying appropriate responses to each online threat

Expressive Communication Demands:

- Explaining strategies for handling online threats during group work.
- Presenting group findings to the class.

Receptive Communication Demands:

- Listening to peer feedback during group work.
- Reading scenario cards to identify online threats.

Academic Vocabulary: Specialized terms and phrases students need to understand

- Cyberbullying
- Phishing
- Identity theft
- Mitigate
- Prevent
- Strategy

Content Vocabulary: Key vocabulary words, symbols, or sounds used in the lesson

- Online threats
- Social media
- Personal information
- Password protection

Everyday Vocabulary: Potential terms used in everyday life to support generalization of skills

- Online safety
- Staying safe
- Protecting personal info

UDL Language Supports:

- Anchor charts with key terms and definitions.
- Sentence stems for group discussions (e.g., “One way to prevent ___ is by ___.”).
- Visual representations of online threats.
- Peer pairing for collaborative activities.

Targeted Supports for the Key Language Activity and support a specific language demand (function, vocabulary, syntax or discourse)

1. Language Function: Describing and Recommending

- **Sentence Stems: Provide structured sentence frames to guide responses. Examples:**
  - *This is an example___ of because___ .*
  - *A red flag for this type of threat is __.*
  - *A safe response would be to___ because___ .*
- Anchor Chart with Vocabulary: Display key vocabulary (cyberbullying, phishing, identity theft, red flag, report, block) with definitions and sample sentences.
- Think-Aloud Modeling**:** Model how to respond to a scenario using the sentence stems. For example:
  - *In this scenario, the email asks for a password and says it's urgent. That's a red flag for phishing because real companies won't ask for passwords in emails.*

2. Vocabulary Demand: Academic and Content-Specific Language

- **Graphic Organizer – Frayer Model: Provide a Frayer Model for each key term (e.g., phishing). Include:**
  - Definition
  - Characteristics/Red Flags
  - Examples
  - Non-Examples
- Word Wall**:** Display key terms with visuals, definitions, and example sentences.
- Vocabulary Cards: Provide laminated vocabulary cards with definitions and sentence frames.

3. Syntax Demand: Constructing Complete Sentences and Using Conditional Language

- **Conditional Sentence Frames: Provide structured frames that include cause-effect language. Examples:**
  - *If___ , then you should___ .*
  - *When___ happens, the best response is to ___.*
- **Modeling with Examples and Non-Examples:**
  - Present a correct response and a non-example.
  - *Correct: If someone sends you a message asking for your password, you should not respond because it could be phishing.*
  - *Non-Example: You should click the link to find out who sent the email.*
- Fill-in-the-Blank Practice: Provide practice sentences with blanks for key phrases (e.g., *If you see___ , then___ .*).

4. Discourse Demand: Structured Group Discussions

- **Graphic Organizer – Compare/Contrast Chart: Use a chart with columns for each type of threat (cyberbullying, phishing, identity theft). Include rows for:**
  - Red Flags
  - Potential Impact
  - Safe Responses
- **Discussion Prompts: Provide structured prompts for initiating and maintaining discussion:**
  - *What makes this scenario a case of __?*
  - *How do you know?*
  - *What could the person do to respond safely?*
- **Speaking/Listening Checklist: Provide a checklist for active listening and respectful communication:**
  - *Make eye contact.*

- *Ask clarifying questions.*
- *Respond using sentence stems.*

Higher Ordered Thinking Questions, Activities, Engagement [HLP 18: Strategies to Promote Student Engagement]

Questions:

- What patterns do you notice in the language used in phishing emails versus legitimate emails? How can recognizing these patterns help you stay safe online?
- How is cyberbullying similar to and different from in-person bullying? What impact might each have on the victim?
- What common red flags do phishing and identity theft scenarios share? Why do you think scammers use these tactics?
- Which response strategy do you think is the most effective for dealing with phishing emails? Why?
- Imagine you receive a message from someone claiming to be your bank, asking for your account information. How would you decide whether or not to respond?
- If a friend tells you they've been targeted by cyberbullying but doesn't want to report it, how would you advise them? Why?
- How could you create a checklist for identifying phishing emails that other students could use to stay safe online?
- Design a response plan for someone who has just realized their social media account has been hacked. What steps should they take?
- What strategies would you use to avoid becoming a victim of identity theft? How do these strategies connect to what you've learned about phishing and online safety?
- Think about a time when you received a suspicious email or message. How would you handle it differently after today's lesson?
- Why is it important to learn about online threats even if you think you already know how to stay safe?

Activities:

- Case Study Analysis: Provide students with case studies that describe real-life incidents of cyberbullying, phishing, or identity theft. Include specific details about what happened, how the victim responded, and the outcome. Ask students to work in pairs to analyze the case and answer questions such as: What were the red flags in this scenario? How effectively did the person respond? What could they have done differently? What would you recommend as the best response strategy? Have each pair present their analysis to the class and justify their recommended response strategy. Students create a follow-up plan for the person in the case study, outlining steps to prevent future incidents.
- Design a Cyber Safety Resource Guide: Assign students to create a Cyber Safety Resource Guide that includes: A glossary of key terms (e.g., phishing, identity theft, red flag). A flowchart of response strategies for different online threats. A checklist of safe online behaviors. A list of resources for reporting online threats (e.g., school counselor, IT department, trusted adult). Encourage students to use visual elements (e.g., icons, diagrams) to make the guide accessible to all learners. Have students present their guides to younger students or parents during a Cyber Safety Awareness Day.
- Investigate and Debate: Divide students into two groups. Assign one group to argue for stricter regulations on social media platforms to protect users from cyber threats. Assign the other group to argue against stricter regulations, emphasizing personal responsibility and freedom of speech. Provide time to research evidence to support their arguments, including data on phishing, identity theft, and cyberbullying incidents. Conduct a structured debate, allowing each side to present arguments and rebuttals. After the debate, students write a reflective response that addresses the question: What is the most effective way to balance online safety with personal privacy?
- Create a Social Media Safety Plan: Provide a template with sections for: Identifying common online threats. Recognizing red flags (e.g., unknown senders, urgent language). Steps for responding to each type of threat. Personal action steps for maintaining privacy (e.g., changing passwords regularly, monitoring accounts). Encourage students to include specific examples and strategies tailored to their own online habits (e.g., social media, gaming, email). Have students review and critique each other's plans to ensure thoroughness and accuracy.

Instructional Strategies [HLP 12, 13] This section will include aspects written above and is organized by HLP 16: Explicit Instruction & HLP 15: Scaffolded Supports

Lesson Part 1

Opening

Description of Activities and Instruction (Teacher Does) 1

Step 1: Activate Prior Knowledge

- Display a relevant visual prompt (e.g., an image of a phishing email or a social media post with a suspicious link).
- Ask students: “What do you notice about this email/post? What makes it seem suspicious?”
- Record student responses on a whiteboard or interactive board, grouping them into categories (e.g., phishing, cyberbullying, identity theft).
- Connect student responses to lesson content by saying: “Today, we will learn how to identify these types of online risks and how to respond to them safely.”
- Utilize a KWL chart to have students list what they Know, Want to know, and what they will Learn during the lesson.

Step 2: State the Learning Objectives

- Write the objectives on the board or display them using a projector.
- **Read each objective aloud clearly:**
  - “By the end of today’s lesson, you will be able to identify three common online threats: cyberbullying, phishing, and identity theft.”
  - “You will also learn three strategies to respond to each threat safely.”
- Encourage students to repeat the objectives aloud to reinforce understanding.
- Ask a volunteer to restate the objectives in their own words to confirm understanding.

Step 3: Set a Purpose for Learning

- **Display a brief video clip showing a real-world scenario of online threats (e.g., a phishing attempt or cyberbullying incident):**
  - Search internet to find video using search terms such as a phishing attempt or cyberbullying incident
- Before playing the video, say: “Think about how the people in this video are affected and what they could have done differently.”
- After the video, ask: “Why is it important to learn about online threats? How can knowing these strategies help you in your everyday life?”
- Reinforce the purpose by connecting the lesson to potential real-life consequences, such as identity theft or reputation damage.

Step 4: Engage Students

- Present a short, relatable story about a high school student receiving a suspicious email or encountering cyberbullying on social media.
- **Ask guiding questions:**
  - “What would you do if you received this message?”
  - “Have you ever seen or heard about a similar situation?”
- Allow for brief partner discussions using a “Turn & Talk” strategy.
- Circulate and listen to student conversations, noting common misconceptions or points of confusion to address later.

Step 5: Provide an Overview

- **Display a visual agenda or lesson outline with the following structure:**
  - 1. Introduction to Online Threats (Cyberbullying, Phishing, Identity Theft)
  - 2. Identifying Online Threats - Group Activity
  - 3. Strategies for Mitigating Online Threats

    - 4. Role-Play Scenarios and Responses
    - 5. Exit Ticket and Review
- Verbally walk students through each section, clarifying how each part connects to the overall objective.
- Allow time for questions about the lesson structure.

Step 6: Connect the lesson to students' daily experiences by discussing how the lesson can be applied at home, school, or community

- Ask students: “Where do you typically interact with people online? At home? At school? On social media?”
- Display a Venn diagram labeled Home, School, Community and have students brainstorm potential online risks in each setting.
- **Provide examples:**
    - “At home, you might get a suspicious email.”
    - “At school, someone could send a mean message through a group chat.”
    - “In the community, you might be asked to share personal information for a contest or survey.”
- Connect these examples to the lesson objective by emphasizing that the strategies learned will apply to all three settings.

Step 7: Clarify Expectations

- **Display a checklist of expected behaviors during group discussions and activities:**
    - Stay on task.
    - Respect others’ opinions.
    - Listen actively.
    - Ask for clarification if you’re unsure.
- Review each item, emphasizing that the lesson involves sensitive topics and that respectful communication is essential.
- Provide specific examples of acceptable language (e.g., “I disagree because...” or “Can you explain what you mean by...?”).
- Ask students to signal their understanding of expectations with a thumbs-up/thumbs-down check.

Step 8: Check for Understanding

- **Conduct a quick, informal assessment using a “Three-Question Check-In”:**
    - “What are the three online threats we will learn about today?”
    - “Why is it important to know how to respond to these threats?”
    - “What is one way you might respond to a suspicious email?”
- Allow students to respond verbally, in writing, or by using response cards (e.g., A/B/C multiple choice).
- Provide corrective feedback to clarify misunderstandings, if necessary.

Script *(if needed)*

**[Display a slide with an image of a suspicious email. The email shows a message claiming the student has won a prize and requests personal information to claim it.
Point to the image and pause to allow students to observe.]**

Take a look at this email. What do you notice about it? What stands out to you?
[**Wait for student responses. As students share, nod and write key phrases on the board, such as “asking for personal information,” “unfamiliar sender,” “too good to be true.”]**

Great observations. You’re noticing some red flags. Today, we’re going to dig deeper into these types of messages and learn how to protect ourselves from online threats like phishing, cyberbullying, and identity theft.

[Draw three columns on the board labeled Cyberbullying, **Phishing**, **Identity Theft. Write student responses in the appropriate columns, organizing their input.]**

[Move to the whiteboard or projector and display the learning objectives. Point to each objective as you read it aloud.]

By the end of today's lesson, you will be able to do three things:

- *Identify three common online threats: cyberbullying, phishing, and identity theft.*
- *Describe strategies to respond to these threats safely.*
- *Demonstrate appropriate responses to these threats through role-play scenarios.*

Why do you think it's important to know how to handle these situations?
[Wait for student responses, then acknowledge and validate responses.]

Exactly. The more you know, the safer you can be online.

[Play a short, one-minute video clip showing a teenager receiving a suspicious email, experiencing cyberbullying, and having their identity stolen online.]

As you watch, think about how the characters are affected by each situation. How did they respond? Was it effective?

[Pause the video after each scenario to ask:]

- *What do you think the person could have done differently to stay safe?*
- *Why do you think it's so important to recognize these types of threats?*

[Wait for responses, then summarize.]

Today, we're going to learn some simple, effective strategies that you can use to protect yourself in similar situations. Let's get started.

[Walk to the front of the room and hold up a printed scenario card. The card describes a situation where a student receives a message from a "friend" asking for their login information to access a game account.]

Let me tell you a quick story. Jordan gets a message from someone claiming to be their friend, asking for their game login information. What should Jordan do?

[Pause, allowing students to respond. Point to a student who raises their hand.]

Why do you think that's a good or bad response?

[If necessary, prompt with additional questions: *What could happen if Jordan gives out their login information?]*

[Summarize key points and write them on the board under the column labeled Phishing.]

[Move to the whiteboard. Write the following agenda for the lesson:]

1. Introduction to Online Threats
2. Identifying Online Threats - Group Activity
3. Strategies for Mitigating Online Threats
4. Role-Play Scenarios and Responses
5. Exit Ticket and Review

Here's what we're going to do today:
First, we'll talk about the three main types of online threats: cyberbullying, phishing, and identity theft.
Next, you'll work with a partner to analyze some scenarios and identify the threats involved.
Then, we'll discuss strategies for protecting yourself online.
After that, we'll do a role-play activity where you practice responding to these threats.
Finally, you'll complete an exit ticket to show what you learned.

[Point to each section as you go through the agenda, then ask:]

Any questions about what we're doing today?

[Move to the front of the room and distribute sticky notes to each student. On the board, draw a three-section Venn diagram labeled Home, **School**, **Community**.]

Think about the places where you use the internet every day – at home, at school, and in your community. On your sticky note, write down one place you go online and one potential risk you might face there.

[Give students one minute to write their responses. Then, call on a few students to share and stick their notes in the appropriate section of the Venn diagram.]

Notice how some risks overlap between different areas? Whether you're at home, at school, or in the community, online risks are everywhere. That's why it's important to know how to protect yourself in all of these settings.

[Move to the interactive whiteboard. Display the "Group Discussion Expectations" slide, which lists:]

- Stay on task.
- Respect each other's opinions.
- Listen actively.
- Use appropriate language.

Before we get started with group work, let's go over some expectations. When you're discussing with your partner or group, make sure to:

[Point to each item as you read it aloud.]
Stay on task – focus on the scenario and identifying the threat.
Respect each other's opinions – you might not all agree, and that's okay.
Listen actively – ask questions and make sure you understand what your partner is saying.
Use appropriate language – keep the conversation on topic and constructive.

[Ask a volunteer to restate the expectations in their own words. Confirm understanding by saying:]
Does everyone feel clear about what's expected during group work?

[Hold up a thumbs-up/thumbs-down card.]
Before we move on, let's do a quick check-in.
Thumbs up if you feel confident about what we're learning today.
Thumbs sideways if you're feeling okay but have a question.
Thumbs down if you're feeling confused and need more explanation.

[Scan the room to gauge understanding. If some students show thumbs down, ask:]
What specific part do you feel unclear about? Let's clarify before we move on.

UDL Strategies 1

- Display anchor charts with key vocabulary and definitions for cyberbullying, phishing, and identity theft. Include visual examples (e.g., phishing email, cyberbullying text).
- Use a short video clip showing realistic scenarios of each type of online threat. Provide captions for accessibility.
- Provide a K-W-L Chart (Know, Want to Know, Learned) to activate prior knowledge and set a purpose for learning.
- Use a Think-Pair-Share activity to engage students in discussing what they already know about online threats.
- Allow students to respond verbally, in writing, or by drawing examples of online threats.
- Provide sentence frames (e.g., A sign of phishing is ___ because ___.) to scaffold language for students who need support.

Lesson Part 2

Instructional Procedures/Learning Tasks:

If desired, use **Co-teaching strategy**

Parallel teaching: Split the class into two groups based on specific needs (e.g., reading level, familiarity with online threats, language proficiency). Group 1 (with Teacher A) includes students who need more explicit instruction and step-by-step guidance in identifying threats. Group 2 (with Teacher B) includes students ready to engage in more complex scenarios and practice response strategies.

Teacher A: Display the anchor charts for Cyberbullying, Phishing, Identity Theft. Use scenario cards and focus on identifying red flags in each type of threat. Ask guiding questions: What makes this message suspicious? How do you know this is phishing? Provide immediate feedback and reinforce key points using sentence stems and visual cues.

Teacher B: Distribute scenario cards that include specific online threats. Facilitate role-play activities where students practice responding safely to each type of threat (e.g., blocking, reporting, deleting). Provide feedback on the effectiveness of each response and suggest improvements.

After 15-20 minutes, bring both groups back together. Have each group share one key takeaway or strategy they practiced (e.g., identifying red flags, practicing safe responses). Facilitate a brief whole-class discussion to reinforce how identifying threats and

responding safely are connected.

Description of Activities and Instruction (Teacher Does) 2

Step 9: Explain (Teacher Models)

- **Prepare Visual Aids and Materials:**
  - Display three anchor charts labeled Cyberbullying**,** Phishing, and Identity Theft with key characteristics and examples.
  - Prepare a set of three sample scenario cards, one for each type of threat (cyberbullying, phishing, identity theft).
  - Load a short, pre-selected video clip or screenshot of a phishing email, cyberbullying text, and identity theft attempt.
- **Introduce the Objective and Purpose:**
  - State the specific objective for identifying and responding to online threats.
  - Emphasize the importance of recognizing these threats to stay safe online.
- **Activate Prior Knowledge:**
  - Pose questions about students' prior experiences with online threats.
  - Record responses on the board to identify misconceptions or existing knowledge.
- **Explicitly Define Each Online Threat:**
  - Present each threat (cyberbullying, phishing, identity theft) using visual aids.
  - Clearly explain the characteristics of each threat.
  - Show a real or simulated example (e.g., phishing email or cyberbullying text).
  - Break down key elements that indicate a potential threat (e.g., urgent language, requests for personal information).
- **Model Identification and Response for Each Threat:**
  - Demonstrate how to spot each threat using scenario cards or projected images.
  - Verbally model a safe response (e.g., not clicking suspicious links, reporting cyberbullying).
  - Use a think-aloud strategy to explain the reasoning behind the response.
- **Use Multiple Examples for Clarity:**
  - Provide at least one example for each threat to ensure understanding.
  - Use varied contexts (e.g., social media message, suspicious email) to broaden application.
- **Check for Understanding:**
  - Use quick formative assessments (thumbs up/down or a brief question) after each example.
  - Encourage students to ask questions if they are unclear about any threat.
- **Reinforce Key Points:**
  - Summarize the characteristics of each threat.
  - Highlight the strategies to respond safely (e.g., blocking, reporting, not sharing personal information).
  - Connect the modeled strategies to the upcoming group practice activity.

Script *(if needed)*

[Display three anchor charts labeled Cyberbullying, **Phishing**, and **Identity Theft. Arrange the charts side by side where all students can see them clearly.]**

Point to the posted learning objectives.

Today, we're going to learn how to identify three common online threats – cyberbullying, phishing, and identity theft – and practice strategies to stay safe online.
[**Pause and look around the room to ensure students are paying attention.]**
We're going to break each of these down, look at real examples, and practice how to respond safely.

[Move to the whiteboard. Write the words Cyberbullying, **Phishing**, and **Identity Theft in three columns.]**

Raise your hand if you've ever heard of any of these terms before. What do you think they mean?

[Wait for student responses. Write their responses under the appropriate column. Acknowledge responses with nods and affirmations like "Good point," "That's right," or "Let's add that to our list."]

Great. We're going to take a closer look at each one and learn exactly what they look like and how to handle them safely.

[Stand next to the Cyberbullying chart. Point to the definition and examples listed on the chart.]

Cyberbullying happens when someone uses technology to intentionally harm or harass another person. This can include mean text messages, spreading rumors online, or posting embarrassing photos.

[Hold up a scenario card labeled Cyberbullying. **Read it aloud:]**
Lina receives a text from a classmate that says, "You're so ugly. No one likes you." The classmate then posts it in a group chat with other students.

[Pause and look at the class.]
What do you notice about this message? How do you think it makes Lina feel?
[**Wait for student responses. Nod and validate their responses.]**

Now, let's think about how Lina could respond safely. She could take a screenshot, block the sender, and report the message to a trusted adult or school counselor.

[On the Cyberbullying chart, write the strategies: Screenshot, Block, Report.]

[Move to the Phishing chart. Point to the definition and examples listed on the chart.]

Phishing is when someone tries to steal personal information by pretending to be a trusted source. It usually happens through email, texts, or fake websites.

[Display a printed phishing email on the document camera or projector. Point to the subject line: "Urgent! Your Account Is Locked. Click Here to Verify."]

Take a close look at this email. What stands out to you?
[**Wait for responses, then say:]**
Notice how it says 'Urgent' and asks you to click a link to verify your account. This is a common phishing tactic. Let's break it down.

[Highlight elements on the email with a marker or laser pointer: misspelled words, urgent language, suspicious link.]
If you see an email like this, do not click the link. Instead, forward it to a trusted adult, delete the email, and run a security check on your device.

[On the Phishing chart, write the strategies: Do Not Click, Report, Delete, Check Security.]

[Move to the Identity Theft chart. Point to the definition and examples listed on the chart.]

Identity theft is when someone uses your personal information – like your name, Social Security number, or credit card details – without your permission. This can lead to serious problems, like someone stealing money from your bank account.

[Hold up a scenario card labeled Identity Theft. **Read it aloud:]**
Jamal shares his gaming account password with a friend. Later, he notices that his account has been used to make several purchases without his permission.

[Pause and look around the room.]
What mistake did Jamal make?
[**Wait for responses. Confirm and clarify as needed.]**

Sharing passwords – even with friends – can lead to problems like this. Instead, Jamal should keep his passwords private and monitor his accounts regularly.

[On the Identity Theft chart, write the strategies: Keep Passwords Private, Monitor Accounts, Report Unauthorized Activity.]

[Stand in front of all three charts and point to each one as you summarize.]

Let's review. Cyberbullying involves using technology to hurt someone. Strategies to handle it include taking a screenshot, blocking the sender, and reporting it.
[**Point to the Phishing chart.]**
Phishing involves trying to steal personal information through fake messages. Avoid clicking suspicious links, report it, and delete the

email.
[**Point to the Identity Theft chart.]**
Identity theft happens when someone uses your personal information without permission. Keep your passwords private and monitor your accounts regularly.

[Look around the room and ask:]
Any questions before we move on to practice identifying these threats on your own?

[Wait for questions and clarify as needed.]

Step 10: Guided Practice (Teacher and Students Practice Together)

- **Prepare Materials and Resources:**
  - Print scenario cards featuring examples of cyberbullying**,** phishing**, and** identity theft (e.g., text message, email, social media post).
  - Distribute a worksheet titled Identifying Online Threats and Safe Responses with sections for each type of threat.
  - Ensure that visual aids (anchor charts for each threat) remain posted and accessible for reference during the activity.
- **Group Students Strategically:**
  - Pair or group students based on diverse skill levels to encourage peer support and facilitate discussion.
  - Assign specific roles within each group (e.g., reader, recorder, reporter) to promote participation and structure.
- **Introduce the Guided Practice Activity:**
  - Provide clear instructions for the activity:
    - Review each scenario card.
    - Identify the type of threat (cyberbullying, phishing, identity theft).
    - Discuss the appropriate response strategy using the anchor charts as a reference.
    - Record responses on the Identifying Online Threats and Safe Responses worksheet.
- **Model the First Example Together:**
  - Select one scenario card and read it aloud to the class.
  - Ask guiding questions:
    - *What type of threat is this? How do you know?*
    - *What are some safe ways to respond?*
  - Prompt students to refer to the anchor charts and identify the correct response strategy.
  - Demonstrate how to record the response on the worksheet, using complete sentences and key vocabulary.
- **Monitor Group Work and Provide Support:**
  - Circulate among groups, listening to discussions and providing corrective feedback as needed.
  - Ask probing questions to encourage deeper thinking:
    - *What makes you think this is phishing rather than identity theft?*
    - *How might the person feel in this situation? What could they do to protect themselves?*
  - Redirect students to the anchor charts or previously discussed examples if they appear uncertain.
- **Provide Immediate Feedback:**
  - Observe each group's responses and provide targeted feedback, reinforcing correct identifications and suggesting improvements where necessary.
  - Encourage students to explain their reasoning for identifying each threat and choosing a response strategy.
- **Facilitate Group Reporting and Whole-Class Discussion:**
  - Invite each group to share one scenario and their recommended response with the class.

- Prompt the class to provide feedback or suggest alternative strategies.
- Reinforce key points by summarizing the response strategies for each type of threat (e.g., Report, Block, Do Not Click, Keep Passwords Private**).**

- **Check for Understanding Before Moving Forward:**
  - Conduct a quick formative assessment (e.g., thumbs up/thumbs down, brief Q&A) to gauge student understanding of the threats and response strategies.
  - Address any misconceptions or clarify points of confusion before transitioning to independent practice.

Script *(if needed)*

[Hold up the worksheet titled Identifying Online Threats and Safe Responses and show it to the class.]

Now that we've gone over what cyberbullying, phishing, and identity theft look like, it's your turn to practice identifying these threats and figuring out the best ways to respond.
[**Pass out the worksheet to each student.]**

In a moment, you'll work with a partner. Each pair will get a set of scenario cards. You'll read each card, decide what type of threat it is, and write a safe response on your worksheet.

[Hold up a scenario card as a visual cue.]
For example, you might get a card like this one – a text message that says, 'You're so stupid. No one likes you.' What kind of threat do you think that is?
[Wait for student responses. Nod to acknowledge correct answers.]

Exactly – cyberbullying. And what could you do to respond safely?
[Wait for responses, then say:]
Right – you could take a screenshot, block the sender, and report it to a trusted adult.

[Write the response on the whiteboard: Screenshot, Block, Report.]

[Divide the class into pairs. Assign each student a role – Reader and R**ecorder**. **Distribute one set of scenario cards to each pair.]**

*You'll work with your partner to go through each scenario card. The **Reader** will read the card aloud, and the **Recorder** will write down the type of threat and a safe response on the worksheet.*

[Walk around the room to ensure each pair is ready to begin.]
Remember, use the anchor charts to help you identify the threats and choose a safe response. You have 10 minutes to work through the cards. Let's get started.

[Move from group to group, listening to discussions and providing immediate feedback.]

[Approach a pair working on a phishing scenario card. Lean down to observe their worksheet.]
I see you've identified this as phishing. How did you know?

[Wait for the student to point out key phrases like "urgent" or "click here to verify."]
Nicely done. Now, what's a safe way to respond?

[If students struggle to provide a response, point to the Phishing anchor chart as a visual reminder.]
Check the anchor chart – what does it say about responding to phishing emails?

[Approach a group working on an identity theft scenario card.
Observe as they write down their response. Nod in agreement if it is correct.]

Good thinking – keeping your password private is a great strategy. What else could you do in this situation?

[If they miss a key response, prompt them:]
What if someone has already accessed your account? What should you do next?
[Wait for responses. Guide them to include Report Unauthorized Activity and **Change Password.]**

[After 10 minutes, signal for students to stop working and return their attention to the front of the room.

Let's come back together as a class. I'd like each group to share one scenario and your recommended response.

[Call on one pair to share their phishing scenario. Point to the Phishing anchor chart as they speak.]

What was your scenario? How did you identify it as phishing? And what was your safe response?

[Wait for the pair to respond. Nod and summarize their key points.]
That's exactly right – if it asks for personal information or has a suspicious link, don't click it. Instead, report it and delete the email.

[Repeat this process with other groups, covering at least one scenario for each type of threat (cyberbullying, phishing, identity theft).]

[Stand at the front of the room and hold up a thumbs-up/thumbs-down card.]
Before we move on to independent practice, let's do a quick check-in.
Thumbs up if you feel confident identifying these threats and choosing a safe response.
Thumbs sideways if you're still a little unsure.
Thumbs down if you're feeling confused and need more examples.

[Scan the room for responses. Address any thumbs down or sideways signals with additional examples or clarification.]

Great job so far. Now, we're going to move into independent practice, where you'll apply what you just learned to new scenarios.

[Move to the independent practice section of the lesson.]

Step 11: Independent Practice (Students Practice Alone)

- **Prepare Independent Practice Materials:**
  - Develop an independent practice worksheet titled Identifying Online Threats and Safe Responses – Independent Practice with new, individual scenarios covering cyberbullying, phishing, and identity theft**.**
  - Include sections for:
    - Identifying the type of threat (cyberbullying, phishing, identity theft).
    - Describing specific red flags that indicate a threat.
    - Writing a safe response strategy for each scenario.
  - Provide sentence stems to scaffold student responses (e.g., *This is a ___ threat because ___. A safe response would be ___.*).
- **Provide Clear Instructions and Expectations:**
  - Clearly state the task:
    - Students will read each scenario independently, identify the type of threat, and write a safe response strategy.
  - Remind students to use the anchor charts as reference tools.
  - Explain that each response should include:
    - The type of threat.
    - At least two red flags that indicate a threat.
    - A recommended safe response strategy.
- **Monitor Student Progress and Provide Support:**
  - Circulate around the room to observe student work.
  - Check for correct identification of threats and accurate response strategies.
  - Provide targeted feedback to students who appear confused or are struggling to identify red flags.
  - Prompt students to refer to the anchor charts or previously modeled examples if they are unsure.
- **Offer Targeted Support and Scaffolding:**
  - Provide additional prompts or sentence stems for students who need more support (e.g., *If you see a message that asks for your password, this is likely a ___ threat.*).
  - Allow students who need extra support to verbally explain their responses before writing them down.
  - For students with language processing difficulties, provide a visual checklist of common red flags associated with each type of threat.
- **Encourage Self-Checking and Reflection:**
  - Before collecting the worksheets, instruct students to re-read their responses and check for completeness:
    - Is the threat clearly identified?
    - Are specific red flags mentioned?

        - Is the response strategy appropriate and specific?
    - Prompt students to make corrections or add missing information as needed.

- **Collect Student Work for Assessment:**
    - Collect the completed worksheets for review.
    - Use a rubric to assess each response for:
        - Correct identification of the type of threat.
        - Identification of appropriate red flags.
        - Accurate and specific response strategies.

- **Provide Immediate Feedback and Reinforcement:**
    - Review one or two sample responses with the whole class to reinforce key points.
    - Provide general feedback (e.g., *Great job identifying phishing threats. Remember, if you see a request for personal information, it's a red flag.*).
    - Highlight exemplary responses and clarify misconceptions as needed.

Script *(if needed)*

[Pass out the worksheet to each student as you speak.]

Now that we've practiced identifying online threats together, it's your turn to work independently. You each have a worksheet with three new scenarios – one for cyberbullying, one for phishing, and one for identity theft.

[Point to the first section of the worksheet.]
For each scenario, you will:

- *Identify the type of threat.*
- *Describe at least two red flags that make it a threat.*
- *Write a safe response strategy. Be specific – what would you do to stay safe?*

[Move to the anchor charts posted in the room and gesture to them.]
Remember, you can use the anchor charts as a reference. Think about what we discussed in guided practice – what are the warning signs? What's the best way to respond?

Take your time, read each scenario carefully, and write complete responses. You have 15 minutes to complete the worksheet. If you finish early, double-check your work to make sure each section is complete.

[Circulate around the room, moving from desk to desk. Pause at a student who is staring at the worksheet without writing.]

Are you stuck? Let's look at the first scenario together. What do you think this person is trying to do by asking for your password?

[If the student is unsure, point to the Phishing anchor chart.]
Check out the phishing chart. What does it say about people asking for personal information?

[Wait for the student to respond, then nod.]
Good, now write that down as the type of threat. What's a safe response strategy?

**[Approach a student who has written a brief response, such as "Tell someone."
Lean down to their level and point to the response.]**

You're on the right track – telling someone is a good start. What else could you do to protect yourself?
[**Wait for the student to think, then say:]**
Remember, in a phishing scenario, you can also delete the message and run a security check. Let's add that to your response.

[Stand at the front of the room and clap your hands once to get students' attention.]

You have about five minutes left. Before you finish, I want you to re-read your responses.

[Point to the board where the checklist is displayed:

- **Is the threat clearly identified?**
- **Did you list two red flags?**

- **Is your response strategy clear and specific?]**

Take a moment to check your work against this checklist. Make sure each response is complete before you turn it in.

[Walk around the room with a basket. Hold it out for students to place their completed worksheets in.]

Once you've checked your work, go ahead and place your worksheet in the basket. If you need more time, just raise your hand and I'll come to you.

[Wait until all worksheets are collected, then place the basket on your desk.]

[Stand at the front of the room and hold up one anonymous worksheet as a sample. Read the scenario and the student's response aloud.]

Let's look at one example together. This student identified the threat as phishing and listed two red flags: the email asked for personal information and used urgent language. Their response strategy was to delete the email and report it to a trusted adult. Excellent job – that's exactly what we're looking for.

[Set the worksheet down and face the class.]
Overall, I saw a lot of strong responses. Remember, the goal is to be specific – not just "tell someone," but also explain what else you could do, like block the sender or run a security check.

[Pause and look around the room.]
Any questions before we move on to the closing activity?

[Wait for any questions. Address them as needed before transitioning to the closing section.]

UDL Strategies 2

- Keep anchor charts visible as a reference throughout the lesson.
- Use color-coding to differentiate between types of threats and corresponding response strategies (e.g., red for phishing, blue for cyberbullying).
- Provide a T-Chart where students list red flags on one side and appropriate response strategies on the other.
- Use an interactive whiteboard or online quiz platform (e.g., Kahoot, Quizizz) to assess understanding of key concepts in real time.
- Provide a checklist for students to track their progress (e.g., I correctly identified the type of threat, I named two safe responses).
- Allow students to choose how they complete the independent practice:
  - Write a paragraph response.
  - Draw a comic strip showing a safe response to a threat.
  - Record a verbal explanation using a tablet or audio recorder.
- Break down multi-step tasks (e.g., identifying a threat, choosing a response) using task analysis steps posted on the board.

Lesson Part 3

Closure

Description of Activities and Instruction (Teacher Does) 3

Step 12: Summarize key Points

- **Review the Key Concepts:**
  - Display the anchor charts for Cyberbullying**,** Phishing**,** and Identity Theft to reinforce the three types of threats.
  - Highlight the primary red flags associated with each threat (e.g., urgent language for phishing, personal attacks for cyberbullying).

- Revisit the strategies for responding safely (e.g., report, block, delete, monitor accounts).

- **Use Visual Cues:**
  - Point to specific examples on the anchor charts as you summarize key points.
  - Use a graphic organizer or checklist to visually reinforce the key takeaways.
- **Engage Students in a Brief Q&A:**
  - Ask: *What are the three main online threats we discussed today?*
  - Call on a few students to respond, ensuring each threat is mentioned and briefly defined.

Step 13: Check for Understanding

- **Use a Quick Exit Ticket:**
  - Distribute an exit ticket with three questions:
    - *Identify one red flag for phishing.*
    - *What is one safe response to cyberbullying?*
    - *What should you do if someone asks for your password?*
  - Collect the exit tickets to assess understanding of key concepts.
- **Conduct a Quick Verbal Review:**
  - Ask for thumbs up/thumbs down to gauge confidence in identifying each type of threat.
  - Call on a few students to share one strategy for responding safely to each type of threat.

Step 14: Relate the Lesson Objectives

- **Revisit the Learning Objectives:**
  - Display the learning objectives on the board.
  - Read each objective aloud and ask students to give a thumbs up/thumbs sideways/thumbs down to indicate how well they feel they met each objective.
- **Connect Objectives to Student Learning:**
  - Ask: *How do the strategies we practiced today help you stay safe online?*
  - Invite a few students to share how they could apply what they learned in their daily online interactions.

Step 15: Connect to Real-Life Applications

- **Pose Real-World Scenarios:**
  - Provide two or three real-life scenarios involving online threats (e.g., receiving a suspicious text, seeing a mean comment on social media).
  - Ask: *How could you use what you learned today to respond safely to these situations?*
  - Allow time for brief partner discussions, then share responses as a class.
- **Encourage Personal Connections:**
  - Ask: *Think about a time when you or someone you know received a suspicious message or saw something hurtful online. How would you handle it differently now?*

Step 16: Encourage Student Reflection

- **Prompt Individual Reflection:**
  - Distribute reflection slips with prompts such as:
    - *What was the most important thing you learned today?*
    - *What is one question you still have about staying safe online?*

- **Encourage Peer Sharing:**
  - Pair students and have them share their reflections with a partner.
  - Invite a few volunteers to share their reflections with the class.

Step 17: Provide Closure Activities

- **Review Key Vocabulary:**
  - Display key terms (e.g., phishing, identity theft, cyberbullying) and ask students to provide a brief definition or example for each.
- **Conduct a Final Q&A Session:**
  - Open the floor for remaining questions or clarifications.
  - Address any misconceptions or gaps in understanding.
- **Celebrate Student Effort:**
  - Provide specific praise for student participation, focus, and thoughtful responses.
  - Acknowledge the importance of being informed about online safety.

Step 18: Assign Follow-up Work

- **Introduce the Follow-Up Assignment:**
  - Assign a brief homework activity:
    - *Keep a log of any suspicious online messages, texts, or emails you receive over the next week. Note the type of threat and how you responded.*
- **Provide Clear Instructions:**
  - Explain how to complete the log, including specific details to record (e.g., what the message said, how they knew it was suspicious, what action they took).
- **Clarify Expectations and Due Date:**
  - Clearly state the due date and how/where to submit the assignment (e.g., in class, via Google Classroom).
  - Remind students to bring their completed logs to the next lesson for a follow-up discussion.

Script *(if needed)*

[Move to the front of the room and stand next to the anchor charts for Cyberbullying, **Phishing**, and **Identity Theft**. **Point to each chart as you speak.]**

Before we wrap up, let's review the key points we covered today. We talked about three main online threats – cyberbullying, phishing, and identity theft.

[Point to the Cyberbullying chart.]
Cyberbullying is when someone uses technology to hurt or harass someone else. Remember, the key signs include mean messages, spreading rumors, and posting embarrassing photos. What should you do if you're targeted?

[Wait for student responses. Nod and affirm correct answers.]
Good – screenshot, block, and report.

[Point to the Phishing chart.]
Phishing happens when someone tries to steal personal information by pretending to be a trusted source. Watch for urgent language, requests for personal info, and unknown links. What's a safe response?

[Wait for responses.]
Yes – don't click, report it, and delete it.

[Point to the Identity Theft chart.]
Identity theft is when someone uses your personal information without permission. Keep passwords private, monitor accounts, and report unauthorized activity.

[Walk to the board and write three quick questions:]

1. What is one red flag for phishing?

2. What is a safe response to cyberbullying?

3. What should you do if someone asks for your password?

Before we move on, I want everyone to grab a sticky note and write down your answers to these three questions. Take two minutes to do that now.

[Wait for students to write. Circulate to observe responses. Collect the sticky notes and quickly scan them for accuracy.]

Great job – I see a lot of correct responses. Looks like most of you are on track. If you missed one, don't worry – we're going to keep practicing these strategies.

[Move to the objectives posted on the board. Point to each objective as you read it aloud.]

Today, our goal was to identify online threats and describe safe ways to respond. Think back to the scenarios you practiced – how did you do? Thumbs up if you feel confident identifying cyberbullying, phishing, and identity theft. Thumbs sideways if you're still a bit unsure. Thumbs down if you're feeling lost.

[Scan the room and note any thumbs down or sideways. Acknowledge them with a nod.]

If you're still feeling unsure, that's okay – we'll keep practicing these skills in upcoming lessons.

[Walk to the front of the room and hold up a printed text message that says, *You're so ugly. No one likes you. Why don't you just leave?]*

Imagine you're scrolling through your messages and see something like this. What kind of threat is this?

[Wait for responses. Nod when someone says cyberbullying.]
Yes – this is cyberbullying. What are two things you could do to respond safely?

[Wait for responses. Affirm correct answers.]
Great – you could take a screenshot and report it to a trusted adult.

[Hold up a printed email that says, *Urgent! Your account is locked. Click here to verify your password.]*
Now, what about this email? What kind of threat is this?

[Wait for responses.]
Phishing – exactly. What should you do?

[Wait for responses.]
Right – don't click the link. Report it and delete it.

[Pass out reflection slips with the following two prompts:]

1. What was the most important thing you learned today?

2. What is one question you still have about staying safe online?

Take a few minutes to think about what we discussed today. Write down your responses to these two questions. Be honest – your reflections help me know what to review and what to keep practicing.

[Circulate as students write. Provide support to any students who appear stuck or confused.]

[Walk to the board and write the words Cyberbullying, Phishing, Identity Theft.]

Before we finish, let's do a quick review. I'm going to call on a few of you to give me one red flag and one response strategy for each type of threat.

[Call on one student for cyberbullying. Call on another for phishing. Call on a third for identity theft.]
Great responses – it's clear that you're starting to get the hang of identifying and responding to these online threats.

[Walk back to the front of the room and face the class.]
Give yourselves a round of applause for your hard work today. These are really important skills that will help keep you safe online.

[Hold up a worksheet titled Online Threats Log – Follow-Up Assignment and show it to the class.]

For homework, you're going to keep a log of any suspicious messages, emails, or texts you receive over the next week. Your job is to write down:

- *What the message said.*
- *What type of threat you think it was.*
- *What you did to respond or what you could have done to respond safely.*

[Pass out the worksheet and walk around to ensure every student has one.]

This assignment is due next week. We'll review your logs in our next lesson and discuss what you found. If you don't receive any suspicious messages, that's okay – just write down a reminder of the response strategies we practiced today.

[Return to the front of the room and look around to make eye contact with students.]
Any questions before we wrap up?

[Answer any remaining questions]

UDL Strategies 3

- Provide both written and verbal options for completing the exit ticket (e.g., Write one strategy for responding to a phishing email, or Explain it to a partner).
- Allow students to choose between writing, drawing, or recording their follow-up assignment (e.g., logging suspicious online messages).
- Provide a checklist for self-assessment that includes:
  - I can identify three types of online threats.
  - I can describe safe responses for each type of threat.
  - I feel confident using these strategies in real-life situations.

Resources

- Archer, A. L., & Hughes, C. A. (2011). Explicit instruction: Effective and efficient teaching. New York: Guilford Press.
- Bowman-Perrott, L., Gilson, C., Boon, R. T., & Ingles, K. E. (2023). Peer-Mediated Interventions for Students with Intellectual and Developmental Disabilities: A Systematic Review of Reviews of Social and Behavioral Outcomes. Developmental neurorehabilitation, 26(2), 134–154. https://doi.org/10.1080/17518423.2023.2169878
- Collins, B. C. (2022). Systematic instruction for students with moderate and severe disabilities. 2nd Edition. Baltimore, MD: Paul H. Brookes Publishing Co.
- Golden, C. (2018). The Data Collection Toolkit. Baltimore, MD: Brookes Publishing.
- Nelson, G., Cook, S. C., Zarate, K., Powell, S. R., Maggin, D. M., Drake, K. R., Kiss, A. J., Ford, J. W., Sun, L., & Espinas, D. R. (2022). A systematic review of meta-analyses in special education: Exploring the evidence base for high-leverage practices. Remedial and Special Education, 43(5), 344–358. https://doi.org/10.1177/07419325211063491
- OpenAI. (2025, January 3). ChatGPT (Version 4). https://chat.openai.com
- Sam, A., & AFIRM Team. (2022). Antecedent-Based Interventions Brief Packet, Updated. The University of North Carolina at Chapel Hill, Frank Porter Graham Child Development Institute, Autism Focused Intervention Modules and Resources. https://afirm.fpg.unc.edu/antecedentbased-interventions
- Travers, H. E., & Carter, E. W. (2022). A Systematic Review of How Peer-Mediated Interventions Impact Students Without Disabilities. Remedial and Special Education, 43(1), 40-57. https://doi.org/10.1177/074193252