******

**U**NIT OVERVIEW

| **Title of PBL Unit:**  **Target Grade Level(s): 6-9**  **Subject(s): Science**  **Author(s): Melanie Drown, Dedra Ingram, Kelsey Gibbons, Jennifer Vandever** |
| --- |

| **Problem Statement: There has been a cybercrime attack in the community. What can we do to prevent this from happening again?** |
| --- |

| **Unit Overview and Table of Contents:**  **Lesson 1 - Presenting the phenomenon (Kelsey)**  **Lesson 2 - Intro to Cybercrime - Introduce types of cybercrime & have groups do independent research & present (Melanie)**  **Lesson 3 - Impact of Cybercrime - case study testimonial exercise (Dedra)**  **Lesson 4 - Criminal & Civil Investigation/ Criminal & Civil Enforcement (Jennifer V)**  **Lesson 5 - Think like a Criminal - motivations, who they target (Kelsey)** |
| --- |

| **Standards:**  **Educational Technology Learning Standards, Grades 6-8**  2.b. Students demonstrate and advocate for positive, safe, legal and ethical habits when using technology and when interacting with others online  **3.d. Students explore real-world issues and problems and actively pursue an understanding of them and solutions for them.**  **7.b. Students use collaborative technologies to connect with others, including peers, experts and community members, to learn about issues and problems or to gain broader perspective.** |
| --- |

| **21st-Century Skills: Problem-Solving, Collaboration, Critical Thinking, Technology Literacy** |
| --- |

| **Locally and/or Personally Relevant for Students: Involves commonly used items in the students life: the internet, computers, cellphones, etc.** |
| --- |

| **Connections to Career and Educational Pathways: Cybercrime - the education, enforcement or technology side. Connections to Microsoft Digital Crimes Unit.** |
| --- |

**LESSON OVERVIEW**

| **Lesson 1: Presenting the Phenomenon** |
| --- |

| **Problem Statement: There has been a cybercrime attack in the community. What can we do to prevent this from happening again?** |
| --- |

| **Lesson Objectives:**   * **Students will be introduced to an example of cybercrime and will begin to brainstorm how to use education, technology and enforcement to address cybercrime.** |
| --- |

| **Lesson Standards: 3.d. Students explore real-world issues and problems and actively pursue an understanding of them and solutions for them.**  **7.b. Students use collaborative technologies to connect with others, including peers, experts and community members, to learn about issues and problems or to gain broader perspective.** |
| --- |

| **Materials:**  **SMART Board**  **Laptops/Chromebooks**  **Internet Access**  [**Lesson Slideshow**](https://docs.google.com/presentation/d/1Klysj2nHj-dPnS4ZKy4hMqBXoKk19rhxMUj5s6GK-Qk/edit?usp=sharing) |
| --- |

**If relevant to a single lesson, please include:**

| **Lesson 21st-Century Skills: Problem-Solving, Collaboration** |
| --- |

| **Lesson-Locally and/or Personally Relevant for Students: Involves student’s teacher, touches on topic that may have affected students and will most likely affect them at some point in their life.** |
| --- |

| **Lesson-Connections to Career and Educational Pathways: Cybercrime - the education, enforcement or technology side. Connections to Microsoft Digital Crimes Unit.** |
| --- |

**LESSON PREPARATION**

| **Time Required: 45 min** |
| --- |

| **Grouping of Students for Instruction: Teams (if possible given COVID restrictions)** |
| --- |

| **What is the instruction? (Consider the PBL procedure that is being addressed here):**  **This is the hook lesson.**  **Students will be shown an email that their teacher has “received”. The class will be asked what they notice about the email and students will share out.**  **Students will brainstorm an answer to the question:**   1. **What should my teacher do?**   **If groups are stuck teachers may ask the following questions to guide their thinking:**   * **Should they follow the instructions in the email? Why/why not?** * **Should they tell anyone about the email? Why/why not?**   **Students will debrief with the class - either via Padlet, Nearpod, etc. - some way to share answers with the class.**  **Teacher will then go over what action they took.**  **Students will then work together again to answer the following questions:**   1. **What should we have learned before to know how to handle this situation?** 2. **Is there a technological fix to make this not happen again/prevent this?** 3. **What are we going to do to the people who have sent this?**   **Students will again debrief with the class and share their answers.**  **Teacher will finish with a short presentation on how the email shown was an example of cybercrime and set the stage for what the students will be learning over the next few weeks.** |
| --- |

| **Possible Accommodations:**  **Intentional Groupings - put students in different groups**  **Follow up guiding questions for the 1st question:**   * **Should they follow the instructions in the email?** * **Should they tell anyone about the email?** |
| --- |

| **Possible Extensions:**   * **When going over student responses on what their teacher should do, have students decide which response is the best course of action and why** * **Go over what happens when we press the Spam button and how that is reporting and the importance of reporting.** * **Have students make posters on different examples of cybercrimes** |
| --- |

| **Possible Assessment: Unit Project** |
| --- |

| **References and Resources:**  [**Lesson Slides**](https://docs.google.com/presentation/d/1Klysj2nHj-dPnS4ZKy4hMqBXoKk19rhxMUj5s6GK-Qk/edit?usp=sharing) |
| --- |

**LESSON OVERVIEW**

| **Lesson 2: Intro to Cybercrime- Drown** |
| --- |

| **Problem Statement: There has been a cybercrime attack in the community. How can we identify the type of crime, in order to know our next steps?** |
| --- |

| **Lesson Objectives: Identify different types of digital crime through research. Differentiate between digital crimes using critical thinking skills. Understand the main types of digital crime in order to know next steps for solving.** |
| --- |

| **Lesson Standards- OSPI EdTeach Standards:**  **7.b. Students use collaborative technologies to connect with others, including peers, experts and community members, to explore different points of view on various topics.**  **7.d. Students work with others using collaborative technologies to explore local and global issues.**  **1.d. Students are able to navigate a variety of technologies and transfer their knowledge and skills to learn how to use new technologies**  **2: Digital Citizen - Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.**  **3. Knowledge Constructor - Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts and make meaningful learning experiences for themselves and others.** |
| --- |

| **Materials:**   * **Intro to Cyber Crime Video** [**https://www.youtube.com/watch?v=NAcN93O8b6w&t=137s**](https://www.youtube.com/watch?v=NAcN93O8b6w&t=137s) * **Digital Crime Escape Room PowerPoint-** [**Digital Crime Escape Room**](https://seattleschools-my.sharepoint.com/:p:/g/personal/madrown_seattleschools_org/EevryAt7q15Nh1-c2FE4xusBDsIk2IGFX7mHshHUzXtQiw?e=Ydgbfo) * **Escape Room Recording Document (to upload with a notes app of some kind ex.OneNote)** [**Digital Crime Escape Room Notes**](https://seattleschools-my.sharepoint.com/:w:/g/personal/madrown_seattleschools_org/EcsFbGJ4FN1DjSuRxESLq0UBqzcZNKc84xt95a_WY3x0TQ?e=tTyiJo) * **Exit Ticket (can upload on any kind of platform ex.Schoology)** [**Click here to duplicate exit ticket to have for yourself**](https://forms.office.com/Pages/ShareFormPage.aspx?id=WNEx1HRgMkiHg1Hqb23SJ8bES25sI5RGpcicVC7SBCRUNjkwMTdVMUNVTVMwWVZIQTk4UEk4WVk5SS4u&sharetoken=OSUIFLXq2k03A4MIeymY) |
| --- |

**If relevant to a single lesson, please include:**

| **Lesson 21st-Century Skills: Collaborate with peers, communicate with people around them, use critical thinking to differentiate between similar crimes, problem solve when choosing the incorrect escape room answer, obtain information literacy through practice of identifying digital crimes/scams.** |
| --- |

| **Lesson-Locally and/or Personally Relevant for Students: Showing XboX scammer popups, child cyber trafficking, and scam emails are all relevant to this age level.** |
| --- |

| **Lesson-Connections to Career and Educational Pathways: Continued throughout the unit- conversations and research around the careers involved to stop the crimes, enforce laws, educate others, etc.** |
| --- |

**LESSON PREPARATION**

| **Time Required: 2+ days** |
| --- |

| **Grouping of Students for Instruction: Partners (if odd numbers, one student can opt to work alone rather than a group of 3)** |
| --- |

| **What is the instruction? (Consider the PBL procedure that is being addressed here):**  **Pre-Lesson: Make sure that the links above work and can be downloaded. Distribute the note page and powerpoint to students using your preferred digital platform. Put students into partnerships (2 students) prior to the lesson day.**  **Warm up: Open up a class discussion with the prompts “What is cyber crime? What are examples of cyber crime that you know of?”. Record student responses on an anchor chart or digital counterpart. Watch the Youtube Video linked above that introduces some basics of Cyber Crime. Record new information learned from the video on the anchor chart.**  **Activity: Teacher will explain to students how to use the digital escape room powerpoint (directions on slide 2), and what the activity focuses on (identifying digital crime examples). Students will be in their partners and will share responsibilities. One student will be in charge of the powerpoint and research, and one student will be in charge of recording the research and communicating the results. Students will work through the escape room with the goal of finding all of the clues and “escaping”. As students work through, they will be using search engines to figure out which of the answers is the correct one. They will record their research findings on a separate note taking document. Students will need to show their research and explain how they knew which answer was correct, while citing their sources. See note sheet for more instructions.**  **Exit Ticket: Students will complete the exit ticket above as a check for understanding.** |
| --- |

| **Possible Accommodations: Preferential partnerships, vocabulary word sheet, printing student recording sheet rather than uploading into a digital workspace, skip clue 7 (trafficking) for a less mature audience** |
| --- |

| **Possible Extensions: Deep dive in partners or groups of 3 into one specific cyber crime presented, and share knowledge with the class.** |
| --- |

| **Possible Assessment: Exit ticket included, possible to make a Kahoot with the crime examples from the powerpoint.** |
| --- |

| **References and Resources: fbi.gov, Zoe Krum from Microsoft** |
| --- |

**LESSON OVERVIEW**

| **Lesson 3: Impact of Cybercrime- Ingram** |
| --- |

| **Problem Statement:**  **What is the impact of cybercrime on the victim and perpetrator.** |
| --- |

| **Lesson Objectives:**   * Students will be able to define and give examples of Cyber Crime * Evaluate the impact of committing cybercrime for both the target and perpetrator |
| --- |

| Lesson Standards:2.b. Students demonstrate and advocate for positive, safe, legal and ethical habits when using technology and when interacting with others online |
| --- |

| **Materials:**  SMART Board (Any device where you can record student voice and project it will work)  Laptops  Internet Access  Access to Cybercrime Vocab  Digital Cybercrime Cases |
| --- |

**If relevant to a single lesson, please include:**

| **Lesson 21st-Century Skills:** Critical Thinking, Collaboration, Technology Literacy |
| --- |

| **Lesson-Locally and/or Personally Relevant for Students:** Students socialize and work (school) online which puts them at risk for cybercrime. |
| --- |

| **Lesson-Connections to Career and Educational Pathways:** Cybercrime unit at tech facility. Possible guest speaker opportunity via Zoe Krumm, Microsoft employee |
| --- |

**LESSON PREPARATION**

| **Time Required:** 2-3 days |
| --- |

| **Grouping of Students for Instruction:** Students will work in teams to dive deeper into their groups specific digital crime article. |
| --- |

| **What is the instruction? (Consider the PBL procedure that is being addressed here):**  **Day 1**  **Lesson will begin with a whole group discussion on what crimes are and listing student examples on the SMART Board (ie Intimidation, Burglary, Fraud, Stalking, Hate Speech, etc.). We will then examine the impact it has on the victim and the motivation for committing the crime by the perpetrator (teacher continues to record responses on SMART Board.) Teachers will then ask students to discuss with their table teams about which crimes listed could take place online and if the motivation for committing those crimes is the same. After a short table discussion the teacher will have teams share out what they discussed and highlight the crimes and motivations that can occur online.**  **Day 2/Day 3**  **The teacher will then share a case study, whole group, and will assist students in examining the following; Impact (Who was impacted? How?Why?), Motivation (What was gained? Monetary? Retaliation?), Enforcement (Did it break a law? Was the perpetrator caught?) and Prevention (How could this have been avoided? Would education assist in prevention?).**  **Following the whole group discussion, table groups (6-10 groups) will receive their own cybercrime case where they will examine and record, within their small groups; Impact, Motivation, Enforcement, and Prevention. While they are reading through the case they will underline/highlight words that are unfamiliar to them. They will then share their findings with the class.**  **The words that they highlighted/underlined are created into a Quizlet of vocab words they can study from.** |
| --- |

| **Possible Accommodations:**   * **Rubric to aid students in reaching mastery** * **Grouping student--low level with high level** |
| --- |

| **xtensions: Q&A with Microsoft Cybercrime** |
| --- |

| **Possible Assessment: Were they successful in finding the information stated in the rubric.** |
| --- |

| **References and Resources:**  **Technology Standards:**  [**https://www.k12.wa.us/student-success/resources-subject-area/educational-technology-edtech**](https://www.k12.wa.us/student-success/resources-subject-area/educational-technology-edtech)  **FBI Case Files:**  [**https://www.fbi.gov/investigate/cyber**](https://www.fbi.gov/investigate/cyber)  [**CASE FILE 1-A BYTE OUT OF HISTORY.docx**](https://lwsd-my.sharepoint.com/:w:/g/personal/dingram_lwsd_org/EZC4d7sH5lhDrLHDBiL-kjgBaDAldSTtLmcyIC3Xe6Vd1g?e=OyF7ut)  [**CASEFILE 2- Botnet Operation Disabled.docx**](https://lwsd-my.sharepoint.com/:w:/g/personal/dingram_lwsd_org/EeLDBVYjrXxFvM57X_5EWhIBhntrBG6Lrvzjx0fwWuF3Og?e=qa8JeJ)  [**CASEFILE 3-Cyber Criminal Forum Taken Down.docx**](https://lwsd-my.sharepoint.com/:w:/g/personal/dingram_lwsd_org/EXy3TkUn8NBOn2kB2XlV2cABgbBHlZp1fX2Ovsb-Af1I5A?e=jgvZ2m)  [**CASEFILE 4-Operation Ghost Click.docx**](https://lwsd-my.sharepoint.com/:w:/g/personal/dingram_lwsd_org/EVCRCP5hMHpCg9qoSs4dZ0EB6SlFngrEuSQE-8K5usDDPw?e=cPL879)  [**CASEFILE 5-MORRIS WORM.docx**](https://lwsd-my.sharepoint.com/:w:/g/personal/dingram_lwsd_org/EV9Uo8nMGApGqrHsAvIcSO0BlNp1XIoGGeBv6ts0icoweQ?e=JQrnLl) |
| --- |

**LESSON OVERVIEW**

| **Lesson 4: Criminal & Civil Investigation/ Criminal & Civil Enforcement** |
| --- |

| **Problem Statement: There has been a cybercrime attack in the community. What can we do to prevent this from happening again? How does the FBI and other CSI combat cybersecurity?** |
| --- |

| **Lesson Objectives:**  **Students will learn types of cyber crime.**  **Students will be introduced to how the FBI combat cybercrime and will brainstorm how to use education, technology and enforcement to address cybercrime.** |
| --- |

| **Lesson Standards:**  **3.d. Students explore real-world issues and problems and actively pursue an understanding of them and solutions for them.**  **7.b. Students use collaborative technologies to connect with others, including peers, experts and community members, to learn about issues and problems or to gain broader perspectives.** |
| --- |

| **Materials:**  **Nearpod**  **PBSLearningMedia.org, Cyber Security Video Series (teachers’ choice)** |
| --- |

**If relevant to a single lesson, please include:**

| **Lesson 21st-Century Skills:** Critical Thinking, Collaboration, Technology Literacy |
| --- |

| **Lesson-Locally and/or Personally Relevant for Students:** Students socialize and work (school) online which puts them at risk for cybercrime. |
| --- |

| **Lesson-Connections to Career and Educational Pathways:**  **FBI cyber security** |
| --- |

**LESSON PREPARATION**

| **Time Required: 45-60 minutes** |
| --- |

| **Grouping of Students for Instruction:**  **Small work groups for collaboration**  **Whole group instruction** |
| --- |

| **What is the instruction? (Consider the PBL procedure that is being addressed here):**  **PRIOR to the lesson: Visit PBSLearningMedia.org, CyberSecurity Videos. Choose the video or videos that best fit you and your class needs from assessments in previous lessons.**  **You will use NearPod to conduct the lesson. (this is a direct instruction, group collaboration, small group collaboration, research media)**  **Students will brainstorm how to combat cyber crime.**  **Students will research how the FBI combats cyber crime.**  **Students will create a poster to show learning in a creative capacity that can be used in their final PBL.** |
| --- |
|  |

| **Possible Accommodations:**  **English Learner translations and captions**  **Chunking**  **Scaffolding** |
| --- |

| **Possible Extensions:**  **More PBSLearning.org videos for further exploration** |
| --- |

| **Possible Assessment:**  **Formative quiz**  **Formative exit slip** |
| --- |

| **References and Resources:**  **PBSLearningMedia.org** |
| --- |

**LESSON OVERVIEW**

| **Lesson 5: Think like a Criminal - Motivations, Who they Target** |
| --- |

| **Problem Statement: There has been a cybercrime attack in the community. What can we do to prevent this from happening again?** |
| --- |

| **Lesson Objectives: Students will be able to compare their preconceptions about cybercriminals to the reality of who cybercriminals are as well as be able to identify motivations behind cybercrime.** |
| --- |

| **Lesson Standards:**  **3.d. Students explore real-world issues and problems and actively pursue an understanding of them and solutions for them.** |
| --- |

| **Materials:**  [**Lesson Slides**](https://docs.google.com/presentation/d/1zLfUPggVKJKpArAYua3UqD-7OAZD_tMQ_VcX8sGNypA/edit#slide=id.gfbda1f6ced_0_47)  [**Lesson Reading**](https://docs.google.com/document/d/14m-ETYqmLcoN7hRwLVrU4noJVg7mPspEKarUm295jB4/edit#)  [**Reading Questions**](https://docs.google.com/document/d/1BH6eec3iEuBymfylC9VFovXsPlGXa_FR_-kB0bN7CRk/edit#) |
| --- |

**If relevant to a single lesson, please include:**

| **Lesson 21st-Century Skills: Critical Thinking, Collaboration** |
| --- |

| **Lesson-Locally and/or Personally Relevant for Students: Students will likely encounter cybercrime throughout their lifetime, and this lesson helps them understand the motivations behind the crime.** |
| --- |

| **Lesson-Connections to Career and Educational Pathways: Cybercrime - the education, enforcement or technology side. Connections to Microsoft Digital Crimes Unit.** |
| --- |

**LESSON PREPARATION**

| **Time Required: 45 minutes** |
| --- |

| **Grouping of Students for Instruction: Partners or Groups** |
| --- |

| **What is the instruction? (Consider the PBL procedure that is being addressed here):**  **Students start by brainstorming with the class who they think the “classic” cybercriminal is.**  **Students then spend 10-15 minutes of class reading with their partner an article of an interview with a Russian Cybercriminal and answering some questions about the article. While they are reading through the article they are underlining/highlighting words that are unfamiliar to them.**  **The questions are debriefed with the class and students share what they learned that may have surprised them.**  **The words that they highlighted/underlined are added to the Quizlet of vocab words from Lesson 3 that they can study from.** |
| --- |

| **Possible Accommodations:**   * **Intentional Grouping** * **Translated Text** * **Break down text into smaller pieces** |
| --- |

| **Possible Extensions:**   * **Students make slideshows or posters showcasing different motivations behind cybercrime** * **Students take the vocab words from Quizlet and create definition posters** |
| --- |

| **Possible Assessment: Were they successful in using the text to answer the questions about the cybercriminal** |
| --- |

| **References and Resources:**  [**https://blog.talosintelligence.com/2021/02/interview-with-lockbit-ransomware.html**](https://blog.talosintelligence.com/2021/02/interview-with-lockbit-ransomware.html)  [**https://www.youtube.com/watch?v=3YDSxvaiyiw**](https://www.youtube.com/watch?v=3YDSxvaiyiw) |
| --- |