Deviance and Computer Crimes

TOPIC: ETHICS

GRADES: 9-12

LESSON DURATION: TEACHER DISCRETION (MULTIPLE DAYS)

SOFT SKILLS: RESEARCH, COMMUNICATION, COLLABORATION, CRITICAL THINKING

Introduction:

- This lesson revolves around the idea of computer crime and could be included in a sociology course during the unit on deviance. The purpose of this lesson is to give students an understanding of the ways in which crime occurs via a computer to better protect oneself. Ideally, the teacher would introduce the importance of ethics before beginning this lesson.

Learning Outcomes:

- Students will learn and adhere to basic ethics when it comes to technology usage.
- Students will articulate computer crime as a form of deviant behavior.
- Students will develop forms of punishment for deviant computer behavior.

Materials:

- Visual: Laws & Ethics

Activities:

1. The teacher should first begin with an overview of the difference between ethics and laws. This may be a review of earlier course material. A visual comparing laws and ethics is available here.
2. The teacher should then explain that today students will learn about deviance via a computer crimes. Computer-related crimes are on the rise. To understand the types of crimes, students will be assigned a famous incident.
3. Students should be placed in small groups. Each group will be assigned one incident. The group should fulfill the following:
   A. Develop a class presentation over the incident.
   B. Items to include: title page with the incident name, group member names, and a visual.
   C. Overview of the incident. Students should explain the cybersecurity issues and terminology. This part may be difficult. Allow students ample time to research and understand the way in which the crime was committed.
   D. Deviance described. How was the behavior deviant?
   E. How did it work?
   F. Who was to blame? Were they caught? Punished?

G. What laws were broken? What ethical standards were broken? Students should cite the ACM Code of Ethics or the Ten Commandments of Computer Ethics when discussing this issue.
H. What was the impact? Who was impacted?
I. Could it have been prevented? How?

4. Each slide should have a graphic and be easy to read. Be sure to proofread and run spell check.
5. Each group should then present to the class. The teacher can develop a rubric at his/her discretion. A rubric that could be formatted as needed is available at https://www.bie.org/object/document/9_12_presentation_rubric_ccss_aligned
6. Topics for group presentation:
   - *The Morris Worm (1998)*
   - *Citibank and Vladimir Levin (1994)*
   - *Kevin Mitnick (1995)*
   - *Omega Engineering and Timothy Lloyd (1996)*
   - *Worcester Airport and "Jester" (1997)*
   - *Solar Sunrise (1998)*
   - *The Melissa Virus (1999)*
   - *The Love Letter Virus (2000)*
   - *The Code Red Worm (2001)*
   - *Adil Yahya Zakaria Shakour (2001-2002)*
   - *The Slammer Worm (2003)*
   - *US Electric Power Grid (1997-2009)*
   - *Conficker (2008-09)*
   - *Fiber Cable Cut (2009)*
7. As each group is presenting, the students in the class should classify each cybercrime as one of the following:
   A. The computer as a target (using a computer to attack other computers)
   B. The computer as a weapon (using a computer to commit a crime)
   C. The computer as an accessory (using a computer to store illegal files or information)