ETHICAL DILEMMAS

Lesson Description: Pose questions to students to show the complexity of making some decisions. Assist students in understanding ethical dilemmas and what they can do to avoid such situations. Students work together and discuss the dilemmas.

Prerequisite Knowledge: Basic cybersecurity hand principles

Length of Completion: 55 minutes

Level of Instruction: This lesson is for middle and high school students at all levels. Regardless of the age or cybersecurity level, everyone can consider their roles in ethical dilemmas.

Applicable First Principles &/or Concepts:

GenCyber Cybersecurity Concepts

Confidentiality and Think Like an Adversary

Resources that are Needed: The instructor needs the trolley dilemma and ethical dilemma examples, as well as case studies if needed.

Accommodations Needed: No special accommodations are needed.

CYBERSECURITY EDUCATION AND RESEARCH CENTER
@ The University of Wyoming
www.uwyo.edu/CEDAR
www.cowpokes.camp
www.uwcedar.io/community/cowpokes/wikis

LEARNING OUTCOMES

LESSON LEARNING OUTCOMES

Students will be able to:

- Describe computer security including "piggy-backing" or "shoulder surfing"
- Detect "piggy-backing" or "shoulder surfing" in examples and explain how to deter a person from doing so
- Explain their roles in the social network environment and the impact of just one post (visuals can be included here)
- Explain the impact of giving out passwords or user IDs to unauthorized persons
- Explain the impact of posting information that, when used in conjunction with publicly known information, could result in identity theft or worse
- List different ethical considerations of posting something on social networking including copyright protected information, intellectual property information, personal Information (including someone else's birthday or other personal information), testing information, information on how to crack passwords or hack others' accounts and password or other identifying information on another account that could help a "black hat" hack a site or a user identification
- Explain social networking etiquette in response to specific situations or scenarios including:
  - Public use of technology
  - Use of technology while participating in a live social event
  - Use of technology while in class
  - Use of technology while driving, mowing the lawn or performing another function that could lead to distraction and destruction
- List problems associated with the misuse of social networking posts, passwords, or the illegal use of another person's identity
- Adapted from: https://www.brighthubeducation.com/teaching-methods-tips/129278-cybersecurity-ethics-education-for-students/

LESSON DETAILS

Interconnection: After learning about the hand concepts, students use that knowledge to understand ethical dilemmas.

Assessment: Formative assessment - Listen to students' arguments and logic in defending answers to the ethical dilemmas and pose questions to promote critical thinking.

Extension Activities: If needed, case studies in cybersecurity are discussed as a large group and in smaller groups. Link: https://virginiacyberrange.org/courseware/cyber-basics-module-5-legal-and-ethics/case-studies-cybersecurity-law-ethics-and-privacy

Additionally, real-world scenarios can be analyzed: https://www.facilitiesnet.com/security/article/5-Real-World-Incidents-Offer-Cybersecurity-Lessons-for-FMs---18191

Real-world dilemma - Photo alteration (Retouching reality): https://www.commonsense.org/education/lesson/retouching-reality-9-12

Differentiated Learning Opportunities: For the advanced learner, case studies can be dissected and pro/con lists are created. For the novice learner, simple pro/con lists are created for more simple ethical dilemmas (e.g., You find $5 on the floor of the school cafeteria, what do you do?)

LESSON

Warm Up: On the board, place a diagram of a trolly problem (adapted for autonomous vehicles), clearly identify the two options (do not use leading identifiers, 1/2, A/B, rather use some code word -perhaps using some cybersecurity topic - e.g. encryption algorithms "DES" / "AES"). As students walk in have them write their choice on a post-it. Collect the post-its and place them in the appropriate location

Lesson: Begin with a discussion on if there is "right or wrong" answer. Build up to the idea of a moral code - why are some situations easy for us

to agree upon while others are incredibly difficult? Replace the trolley problem with a situation about a known vulnerability on a website (or gaming system).

Here is one sample: "You suspect a vulnerability exists in a game, sharing the vulnerability will bring down the game for an entire week (and loss of income for the company), not sharing the vulnerability will cause some gamers to lose their historical data for the past week (and loss of income for many) ." Think Pair Share: Discuss the ethical dilemma above.

Repeat the above but now add incentives for the student - e.g. personal gains for them or their friends. Think Pair Share: Does personal gain change how you would approach the situation.

Then bring the scenario into a more realistic realm - "sharing credentials to streaming service - or not." Students should take a moment to capture the pros/cons to each decision, then share their pro/con lists with their neighbors. The room creates a list on the board for this simple scenario.

Ask students to each come up with several moral / ethical dilemmas they have faced (including bullying and reporting). Write out a pro/con list for different decisions. Pose the following class discussion topic - are pro/con lists enough to make moral/ethical decisions?

Continue discussion with the current landscape of types of hackers (white, grey, black) and their moral codes. Time dependant - have students read

> https://www.lifewire.com/black-hat-hacker-a-white-hat-hacker-4061415;and time permitting, https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Open up a discussion on what ultimately differentiates types of hackers - "authorization" and "motivation." Beyond moral codes, we also have legal codes - regardless of your moral code, the only acceptable answer to "hacking" is explicit (written) pre-authorization.