Whatcom COMMUNITY COLLEGE

NCyTE CENTER

CYBER ETHICS LESSON

Mark Emry, McNeil High School, Round Rock ISD, Austin, TX

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

CYBER ETHICS

This Cybersecurity-Concept Lesson (CCL) is designed to be a capstone activity. It engages students to reflect on the ethical decision-making process behind cybersecurity issues. Students will choose from a list of debate resolutions, research the topic, and present their findings. Findings will be presented in a position paper. However, a video, or an actual debate with a classmate(s) are other possibilities.

OVERVIEW

Prerequisite Knowledge: Students should complete one of the CCL pathways found in the roadmap. The roadmaps are a list of CCLs which address each of the five Big Ideas in the Advanced Placement Computer Science Principles framework.

Length of Completion: The CCL is designed to take approximately 250-300 minutes.

Learning Setting: This CCL is intended for a classroom with Internet access.

Lab Environment: A standard computer lab a classroom with laptops or 1-to-1 devices..

Activity/Lab Tasks: Students will need time to research a topic of their own choice for the position paper.

- 02.CyberEthics_Presentation.pptx
- 03.CyberEthics_PositionPaperTopics.docx
- 04.CyberEthics_PositionPaper_Rubric.docx

LEARNING OBJECTIVES AND AP CSP ALIGNMENT

Lesson Learning Objectives

Students will be able to:

1) Apply the definition of cyber ethics to the subfield of cybersecurity ethics.
2) Develop a position on a topic and compose a paper reflecting their opinion and knowledge of the topic.

ASSOCIATED AP CSP SUB LEARNING OBJECTIVES

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 1: CREATIVE DEVELOPMENT

- CRD-1.A: Explain how computing innovations are improved through collaboration.
    - CRD-1.A.1: A computing innovation includes a program as an integral part of its function.
- CRD-2.A: Describe the purpose of a computing innovation.
    - CRD-2.A.1: The purpose of computing innovations is to solve problems or pursue interests through creative expression.
    - CRD-2.A.2: An understanding of the purpose of a computing innovation provides developers with an improved ability to develop the computing innovation.
- CRD-2.B: Explain how a program or code segment functions.
    - CRD-2.B.4: The behavior of a program is how a program functions during execution and is often described by how a user interacts with it.
- CRD-2.C: Identify input(s) to a program.
    - CRD-2.C.6: Input can come from a user or other applications.
- CRD-2.D: Identify output(s) produced by a program.
    - CRD-2.D.2: Program output is usually based on a program's input or prior state (such as internal values).

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 5: IMPACT OF COMPUTING

- IOC-1.A: Explain how an effect of a computing innovation can be both beneficial and harmful.
    - IOC-1.A.2 As computing evolves, the way people complete tasks often changes to incorporate new computing innovations.
    - IOC-1.A.3: The total effects of a computing innovation are not always anticipated in advance.
    - IOC-1.A.4: A single effect can be viewed as both beneficial and harmful based on an individual's perspectives.
- IOC-1.B: Explain how a computing innovation can have an impact beyond its intended purpose
    - IOC-1.B.1: Computing innovations can be used in ways that the creator had not originally intended.
    - IOC-1.B.2: Some of the unintended ways computing innovations can be used may have a harmful impact on society, economy, or culture

    - IOC-1.B.3: Responsible programmers try to consider the unintended ways their computing innovations can be used and the potential beneficial and harmful effects of these new uses.
    - IOC-1.B.6: Rapid sharing of the program or the results of running a program with a large number of users can result in significant impacts beyond the intended purpose or control of the programmer.
- IOC-1.F: Explain how the use of computing could raise legal and ethical concerns.
    - IOC-1.F.1: Material created on a computer is the intellectual property of the creator or an organization.
    - IOC-1.F.2: Ease of access and distribution of digitized information raises intellectual property concerns regarding ownership, value, and use.
    - IOC-1.F.3: Measures should be taken to safeguard intellectual property.
    - IOC-1.F.8: Using computing to harm individuals or groups of people raise legal and ethical concerns.
    - IOC-1.F.9: Computing can play a role in social and political issues which in turn often raise legal and ethical concerns.
    - IOC-1.F.11: Computing innovations can raise legal and ethical concerns.
- IOC-2.A Describe the risks to privacy from collecting and storing personal data on a computer system.
    - IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.
    - IOC-2.A.2 Search engines can record and maintain a history of searches made by users.
    - IOC-2.A.3 Websites can record and maintain a history of individuals who have viewed their pages.
    - IOC-2.A.4 Devices, websites, and networks can collect information about a user's location.
    - IOC-2.A.5 Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.
    - IOC-2.A.6 Search engines can use search history to suggest websites or for targeted marketing.
    - IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.

    - IOC-2.A.10 Commercial and governmental curation of information may be exploited if privacy and other protections are ignored.
    - IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.
    - EK IOC-2.A.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.
    - IOC-2.a.13: It is difficult to delete information once it has been placed online.
    - IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.
- IOC-2.B Explain how computing resources can be protected and can be misused.
    - Encryption is the process of encoding data to prevent unauthorized access to information. Decryption is the process of decoding the data.
    - IOC-2.B.6 Certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.
    - IOC-2.B.7 Computer virus and malware scanning software can help protect a computing system against infection.
    - IOC-2.B.8 A computer virus is a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.
    - IOC-2.B.9 Malware is software intended to damage a computing system or to take partial control over its operation.
    - IOC-2.B.10 All real-world systems have errors or design flaws that can be exploited to compromise them. Regular software updates help fix errors that could compromise a computing system.
    - IOC-2.B.11 Users can control the permissions programs have for collecting user information. Users should review the permission settings of programs to protect their privacy.
- IOC-2.C Explain how unauthorized access to computing resources is gained.
    - EK IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be

used to access sensitive online resources, such as bank accounts and emails.

- IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.
- IOC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.
- IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.
- IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.
- IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.
- IOC-2.C.7 Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.

LESSON DETAILS

Overview of Lessons: This CCL should be delivered in one lesson. Student will need two-to-three days to complete the paper. A peer review using the rubric would be an optional activity before the student turns the paper in for a grade.

Warm Up: Following the slide presentation, a discussion of digital technology takes place engaging students in a topic which is relevant and necessary for the lesson, and subsequent position paper.

Lesson: The teacher should follow the Cyber Ethics Presentation to introduce the topic of Cyber Ethics.

After the presentation and discussions, the class should finish the presentation which focuses on the position paper.

Following the presentation, students should be given the position paper topics worksheet. The worksheet can be printed or given via an LMS, such as Google Classroom. Provide students with time to read the topics and ask questions.

The rubric should be reviewed and discussed before students begin their research and then again throughout the writing process.

Active Learning Activity: This CCL includes the active learning of researching the topic and writing the paper. An optional peer review of a classmate's paper would also fit in this category.