|  |  |
| --- | --- |
|  | Concept Assignment 7  PLTW Computer Science CSP Core Training |

# Cybersecurity

|  |  |
| --- | --- |
|  | Learning Objectives |

LO.7.1 While working through Activity 2.1.5, the teacher will:

* Learn about Public Key Encryption, SSL Certificates, and Certificate Authorities.
* Practice a simulated Public Key Encryption exchange of a message.
* Investigate the purpose of a Certificate Authority and an SSL Certificate.

LO.7.2 While working through Lesson 2.3.1, the teacher will:

* Learn about the ways that users and their data are vulnerable to attack.
* Research the history of some infamous attacks and schemes.
* Determine how to keep your identity and data safe in the digital world.

LO.7.3 While completing Activity 2.3.4, the teacher will:

* Explore the hacking competition picoCTF.
* Understand the difference between ethical and nonethical behavior with a computer.
* Use acquired knowledge and external resources to solve several hacking challenges.

|  |  |
| --- | --- |
|  | Introduction |

### Overview of Cybersecurity

Cybersecurity is exciting to students. Sleuthing is fun, cyber capture-the-flag competitions abound, and being a supersmart hacker is glorified in pop culture with mystique and honor. Cybersecurity workers are in short supply. And all of the 1.1 million job openings in computer occupations require cyber knowledge.

Unfortunately, the idea of being knowledgeable in cybersecurity can appeal to a student’s mischievous side. It’s crucial to establish an understanding of the law and the standard for professional ethics no later than the middle-school grades—early in students’ learning experiences in networked computing concepts—and then repeatedly emphasize them through the high school experience.

Networked computing has made it easy to get on the wrong side of the law very quickly. A small, relatively ignorant action can cause significant damage. Poking around on networked computers can abruptly and easily blur from being legal to being a felony, without much skill or knowledge required. Ethical decision-making regarding cyber principles is required early in a student’s learning trajectory. Therefore, it’s essential that cyber ethics and cyber law be taught thoroughly, with passion, and before and commensurate with the student’s understanding of how to mess around in the workings of the internet.

The most age-appropriate goals for young teens relate to privacy, scrutiny of their digital footprint, using social media to enhance social interactions and culture, and a zero tolerance for cyber bullying. In addition to these immediate needs of teens, the security of our country depends on our citizenry maintaining secure computing resources. Employers depend on their employees maintaining a secure and hygienic approach. Even the basics that all computer users need are daunting: using secure password practices, correctly configuring home firewalls, correctly operating antivirus software, correctly allowing and disallowing software installations and updates, and interpreting a browser’s report of an encryption certificate problem can all be complex. Young teens can start learning these concepts alongside the more obvious needs to keep their digital footprint appropriate.

### Overview of Cybersecurity in the Course

* Activity 2.1.1 introduces cyber ethics and cyber law.
* In Activity 2.1.3, students become familiar with a Linux operating system and networking protocols. These are important foundations for later use related to cybersecurity.
* In Activity 2.1.5, students learn about encryption, including paired key encryption.
* Activity 2.2.4 provides an opportunity to address SQL injection using vulnerabilities in the code provided. This topic is not addressed directly in the curriculum.
* Activity 2.3.1 covers cyber hygiene for a nonspecialist computer user.
* Activity 2.3.4 is intended to excite students about cybersecurity through two different opportunities to engage in ethical hacking. In the first, students increase their knowledge of Linux to access “secret” information on the server. In the second, students solve a series of problems in a cybersecurity competition.

|  |  |
| --- | --- |
|  | AP CSP Enduring Understandings (EU) and Learning Objectives (LO) |

In Lesson 2.3 you will increase your students’ ability to maintain good cyber hygiene and excite students about careers in cybersecurity. You’ll lead students to consider the interaction between governance and the impact of the internet. You’ll connect cybersecurity concerns to the time efficiency of algorithms and introduce the concept that some problems cannot be solved by an algorithm, but can be approximately solved using heuristics. Specific concepts that are addressed include:

* Networked computing has tremendous impact, both beneficial and harmful, on governance, privacy, and security. EU7.3 through LO7.3.1 [P4].
* Some problems cannot be solved in reasonable (or polynomial) time, and other problems cannot be solved at all. EU4.2 through LO4.2.1 [P1], LO4.2.2 [P1], LO4.2.3 [P1], and especially LO4.2.4 [P4].
* Significant knowledge and attention are required for secure use of the internet. EU6.3 through LO6.3.1 [P1].

|  |  |
| --- | --- |
|  | Part 1: Security on the Web |

1. Complete Activity 2.1.5 Secure Protocols.

|  |
| --- |
| Submission Item |
| 1. Create a graphical or textual artifact that explains the concepts involved in Public Key Encryption, SSL Certificates, and a Certificate Authority. |

* Review Activity 2.3.1 The Vulnerable User.
* Discuss Parts 1 and 2 with a small group.

1. Review the lists of malware and attacks in number 8. Perform research on one as directed by your Master Teacher. Create a slide about your topic to share with the group.

|  |
| --- |
| Submission Item |
| 1. Activity 2.3.1: Submit a slide about the malware or attack you researched. |

* Review the 2.3.1 presentation. Share with the group something interesting or new to you.
* Project 2.3.4: Explore a cybersecurity competition.

1. Join a team for the picoCTF competition with several other participants as directed by your Master Teacher. Work through several of the tasks in the competition with your group.

|  |
| --- |
| Submission Item |
| 1. Project 2.3.4: Explain solutions to four interesting or challenging capture-the-flag tasks. |

|  |  |
| --- | --- |
|  | Part 2: Considering Classroom Implications |

1. Several cyber competitions are available for students. EasyCTF runs a quarterly competition, for example. While Project 2.3.4 can be a fun, in-class exposure to these competitions, your students are likely to be even more excited by a competition that is in the “live” stage of competition. Typically, these competitions run for 7–10 days and are open to teams as small as one student and as large as 10 students.

Consider your options for creating this opportunity for students. From what other classes could you recruit students? Where could the students meet after school, and who might be willing to supervise them? A mentor is not usually needed for capture-the-flag competitions, but can certainly make a competitive program stronger. Consider T-shirts, posters with a team logo, or other ways to promote the idea of a formal team. Record your plans.

1. The distinction between good, ethical hackers and criminals and “script kiddies” is new for some people, and the ethics component of any cyber ethics/cybersecurity/cyber defense/cyber sleuthing education is paramount. Describe how you’ll handle a student who expresses excitement about being able to hack into computers.

|  |
| --- |
| Submission Item |
| 1. Write a reflection about the things you learned today. Consider highlighting new things you’ve learned, items you need to consider for implementing this in your classroom, and ideas and suggestions you heard from others. Use the questions above as prompts, but don’t feel limited or constrained by just those questions. |