Whatcom COMMUNITY COLLEGE

NCyTE CENTER

PERSONAL DATA VULNERABILITIES

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

PERSONAL DATA VULNERABILITIES

The Vulnerabilities CCL introduces AP Computer Science Principles (AP CSP) students to the concept that information and data may be susceptible to attack by an adversary. After an introductory exercise to discuss the meaning of the word vulnerability, students use the web application Spokeo to complete an activity to discover what data may be vulnerable. A discussion of Social Engineering leads students to complete the CCL with an activity exposing the metadata related to images on a smart phone.

OVERVIEW

Prerequisite Knowledge: Students should have basic knowledge of how to use a web browser and how to access the pictures on their mobile phone.

Length of Completion: This CCL should take approximately 100-120 minutes.

Level of Instruction: This CCL should be presented to AP CSP students within the first six weeks of the school year.

Learning Setting: This CCL includes individual, paired work, and group lecture & discussion.

Lab Environment: Students will need access to the internet and their mobile phone. If students do not have a mobile phone, pre-packaged photos will be supplied. Journals can be formal notebooks, paper, or online (i.e. Google Docs, Evernote).

Activity/Lab Tasks: Three hands-on activities are included in this CCL. The first is activity using the website, spokeo.com, that students discover personal data is available with a click of the mouse. The second activity uses only visual data from images and allows students to think like an adversary in order to gain private information. The third activity allows students to discover the metadata embedded within images taken on a smart phone.

Instructional Files and Online Resources that are Needed:

- 01.PersonalDataVulnerabilities_Overview.docx
- 02.PersonalDataVulnerabilities_Presentation.pptx
- 03.PersonalDataVulnerabilities_Spokeo_Activity.docx
- 04.PersonalDataVulnerabilities_WhoIsThisPerson_Activity.docx
- 05.PersonalDataVulnerabilities_DataExtraction_Activity.docx
- 06.PersonalDataVulnerabilities_DataExtraction_Pictures Folder
    - pic1.jpg
    - pic2.jpg
    - pic3.jpg
    - pic4.jpg

YouTube Video: "Cyber Insecurity: Why You Are The Vulnerability" by John LaCour. TEDxCharleston. Nov 15, 2016.

Assessment: Journals and worksheets will be assessed. No summative assessment is included.

LEARNING OBJECTIVIES AND AP CSP ALIGNMENT

Lesson Learning Objectives

Students:

1) explain what a vulnerability is and how they impact cybersecurity,
2) identify elements of their personal data which may be vulnerable to attack,
3) explain why keeping data safe is important both personally and for professional organizations.

Associated AP CSP Sub Learning Objectives

AP Computer Science Principles Course, Big Idea 2: Data

- DAT-2.A: Describe what information can be extracted from data.
    - DAT-2.A.1: Information is the collection of facts and patternsextracted from data.
    - DAT-2.A.2: Data provide opportunities for identifying trends, makingconnections, and addressing problems.
    - DAT-2.A.3: Digitally processed data may show correlation between variables. A correlation found in data does not necessarily imply a causal relationship exists. Often additional research is needed to understand the exact nature of the relationship.
    - DAT-2.A.4: Often a single data source does not contain the necessary data to draw a conclusion. It may be required to combine data from a variety of sources to formulate a conclusion.
- DAT-2.B: Describe what information can be extracted from metadata.

    - DAT-2.B.1: Metadata are data about data. Metadata is associated with the primary data; the primary data may be an image, a Web page, or other complex object.
    - DAT-2.B.2: Changes and deletions made to metadata do not change the primary data.
    - DAT-2.B.3: Metadata are used for finding, organizing and managing information.
- DAT-2.D: Extract information from data using a program.
    - DAT-2.D.3 Search tools are useful for efficiently finding information

AP Computer Science Principles Course, Big Idea 5: Impact of Computing

- IOC-2.A: Describe the risks to privacy from collecting and storing personal data on a computer system.
    - EK 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.4: Devices, websites, and networks can collect information about a user's location.
    - 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.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.
    - 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.
    - 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.C: Explain how unauthorized access to computing resources is gained.
    - IOC-2.C.1:Phishing is a technique that is used 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.

LESSON DETAILS

Overview of Lessons: The CCL is broken down into two 60-minute lessons taught on consecutive days.

LESSON 1

Warm Up:
Journaling and Think/Pair/Share Activity
Journal question(s):

- What does it mean to be vulnerable?
- When is a person vulnerable?
- What other things can be vulnerable?

Give students time to write in their journals. Students should then share their responses with an elbow partner. Select a few students to share with the class. Teacher should lead the class discussion towards data privacy vulnerabilities.

Define Vulnerability: After the Think/Pair/Share and discussion, students should write their own definition on security vulnerability in their journals. Revisit this definition throughout the lesson.

Presentation:
02.PersonalDataVulnerabilities_Presentation.pptx

Notes on the slides as well as this lesson plan, help guide the instructor.
Begin slide show with CCL objectives (slide 2), then continue to definition of Vulnerability (slide 3).

Facilitate class discussion of why data might be considered private and therefore vulnerable.

Spokeo Activity:
03.PersonalDataVulnerabilities_Spokeo_Activity.docx

Hand out the Spokeo worksheet. Students complete the activity using an adult they are familiar with; then using themselves (slide 4).

a. Discuss the differences found and discuss the "digital footprint".
b. Bring the topic of Social Engineering. Show YouTube video: "Cyber Insecurity: Why You Are the Vulnerability"
c. Follow Social Engineering Slides (Slide 5-Slide 11)

"Who Is This Person?" Activity:
04.PersonalDataVulnerabilities_WhoIsThisPerson_Activity.docx

a. Journal Questions: Why do people share images on Social Media? What data might be gathered from pictures (Slide12)?
b. Then Think/Pair/Share.

LESSON 2

Introduce the term metadata and continue with slide show (Slide 13).

Data Extraction Activity:
05.PersonalDataVulnerabilities_DataExtraction_Activity.docx
06.PersonalDataVulnerabilities_DataExtraction_Pictures Folder

- pic1.jpg
- pic2.jpg
- pic3.jpg
- pic4.jpg

Complete Data Extraction Activity. Images are available in the marked folder. This activity could be used as an individual activity, paired activity, or as a group activity (Slide 14).

Assessment of Learning: As a closing activity, ask students to write in their journals their definition of security vulnerability and how their own personal data, might be considered a vulnerability (Slide 15).

Cyber Ethics Discussion: Discuss Cyber ethics and its definition(s) (Slide 16). Have students watch, "Henrietta Lacks, the Tuskegee Experiment, & Ethical Data Collection: Crash Course Statistics #12". Then discuss questions (Slide 17). Note, discussion questions can be done as a whole group, small group, think/pair/share or a journaling activity.

ACKNOWLEDGEMENTS

Resources:

University of Alabama-Huntsville 2019 GenCyber Student Camp.

"Watch this hacker break into a company", CNN Business, Published on Jun 1, 2016.

This is how hackers hack you using simple social engineering, Oracle Mind Published on May 1, 2016.

"Henrietta Lacks, the Tuskegee Experiment, & Ethical Data Collection: Crash Course Statistics #12" Crash Course, Published on Apr 18, 2018.

"Parks and Recreation - Ron vs. Online Privacy (Episode Highlight)" Parks and Recreation, Published on Nov 2, 2017.

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