Whatcom COMMUNITY COLLEGE

NCyTE CENTER

INFORMATION SECURITY AND THE CIA TRIAD

Nancy Stevens, First Flight High School, Kill Devil Hills, NC

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

INFORMATION SECURITY AND THE CIA TRIAD

Students will:

1) explain confidentiality, integrity, and availability (CIA Triad) as the foundation of information security,
2) explore how email phishing attacks, fake social media accounts, ransomware, and identity theft can violate the cybersecurity goals of confidentiality, integrity and availability, and
3) describe security controls that can be used to protect computing resources.

OVERVIEW

Prerequisite Knowledge: Familiarity with how the Internet works

Length of Completion: The CCL is designed to take approximately 100-150 minutes.

Learning Setting: Traditional face-to-face setting or a blended classroom.

Lab Environment: Classroom or computer lab with projection for slide presentation. Internet access and word processing software are required.

Activity/Lab Tasks: The "Gone Phishing" lesson introduces email phishing through an online quiz. The next activity presents a phishing scenario, followed by a fake social media request. Think-Pair-Share activity prompts students to consider trust in online interactions. The second lesson, "The CIA Triad" examines data breaches using the CIA Triad as a model for information security. Data security measures, personally identifiable information, and identity theft are explored. Writing prompts are included for assessment.

- 01.InformationSecurityandtheCIATriad_Overview.docx
- 02.InformationSecurityandtheCIATriad_Presentation.pptx
- 03.InformationSecurityandtheCIATriad_GonePhishing_Activity.docx
- 04.InformationSecurityandtheCIATriad_CIATriad_Activity.docx
- 05.InformationSecurityandtheCIATriad_CIATriad_Activity_Solutions.docx

LEARNING OBJECTIVES AND AP CSP ALIGNMENT

LESSON LEARNING OBJECTIVES

Students explain how phishing attacks, fake social media accounts, and ransomware breach confidentiality, integrity, and availability; 2) understand that trust in online interactions depends upon confidentiality, integrity, and availability; 3) understand how phishing leads to unauthorized access to computing resources or information; 4) identify examples of personally identifiable information.

ASSOCIATED AP CSP SUB LEARNING OBJECTIVES

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 2: DATA

- LO DAT 1.A Explain how data can be represented using bits.
    - DAT-1.A.5 Abstraction is the process of reducing complexity by focusing on the main idea. By hiding details irrelevant to the question at hand and bringing together related and useful details, abstraction reduces complexity and allows one to focus on the idea.

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 4: COMPUTING SYSTEMS AND NETWORKS

- LO CSN-1.A Explain how computing devices work together in a network.
    - CSN-1.A.3 A computer network is a group of interconnected computing devices capable of sending or receiving data.
- LO CSN-1.D Describe the differences between the Internet and the World Wide Web.
    - CSN-1.D.1 The World Wide Web is a system of linked pages, programs, and iles.

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

LO 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.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

LO IOC-2.C Explain how unauthorized access to computing resources is gained.
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.

LESSON DETAILS

Overview of Lessons: There are 2 lessons.

- Lesson 1 Gone Phishing
- Lesson 2 CIA Triad

LESSON 1 GONE PHISHING

- 02.InformationSecurityandtheCIATriad_Presentation.pptx
- 03.InformationSecurityandtheCIATriad_GonePhishing_Activity.docx

Upon completion of this lesson:

Students understand how phishing can lead to unauthorized access to computing resources and information.

Warm Up: Students will contribute to a word cloud describing cybersecurity risks using an interactive online presentation tool (such as Mentimeter). Display this prompt for students: *What are 3 words that come to mind when you think about online security risks?*

Teaching Tip: Mentimeter is a free tool enabling the teacher to create an interactive word cloud. The teacher creates the prompt for the word cloud, and then shares the access code with students. The word cloud can then be displayed. The popularity of each term is reflected in the size of the word. You may want to assign the word cloud the day prior to this lesson, which will give you time to review the responses.

Lesson: Lead a brief discussion with students about the responses displayed in the word cloud. The warm-up provides the instructor with some understanding of what students identify as security concerns.

Establish that risks are inherent by engaging in online activities (email phishing, fake friend requests, social media bots, ransomware, data breach). Even if you do not participate in social media, your friends and family can post your photo and personal information. Current estimates indicate that phishing accounts for 90% of data breaches. If students are not familiar with email phishing, there are several websites with examples of phishing emails. The slide deck includes links to these websites for student exploration. Students then examine two scenarios. The first scenario is a phishing email and the second scenario is a fake social media account.

Additionally, there is a link to an article about a spear-phishing email attack. This slide allows for discussion on cyber ethics, definitions and who is responsible when an attack or breach occurs.

The Think-Pair-Share activity establishes the difficulty in assessing trust in the digital realm. Students should independently think about the prompt, "*What do phishing emails or fake social media accounts tell us about trust in the online world?*" Students discuss with a partner and then share answers as a whole group. The responses from the Think-Pair-Share activity need to be recorded in some manner so that all students can see the results.

Active Learning Activity: Think-Pair-Share activity requires access to the PowerPoint slides presenting the email phishing attack (slides 10-17).

LESSON 2 CIA TRIAD

- 02.InformationSecurityandtheCIATriad_Presentation.pptx
- 04.InformationSecurityandtheCIATriad_CIATriad_Activity.docx
- 05.InformationSecurityandtheCIATriad_CIATriad_Activity_Solutions.docx

Upon completion of this lesson Students:

1) understand that confidentiality, integrity, and availability are the foundations of information security;
2) understand that trust in online interactions depends upon confidentiality, integrity, and availability.

The CIA Triad is presented as a model for information security through the PowerPoint presentation. The CIA Triad lab exercise consists of two writing prompts in which students apply the CIA Triad to the potential security breach posed by the phishing attempt and consider what controls could prevent or protect the user.

Warm Up: What information is valuable to a hacker?
In 2015, the Office of Personnel Management (OPM) discovered a data breach. OPM serves as the storehouse of personnel records for federal employees. The stolen data included names, addresses, places of birth, social security numbers, financial information, fingerprints, and background checks on millions of people. In 2017, the Equifax data breach exposed the data of 143 million people.

Prompt: *What defines personally identifiable information (PII)? What are some possible effects of a data breach involving this information?*

Lesson: After the warm-up and establishing what constitutes PII, continue the slide presentation on the foundation of information security. The slides introduce the CIA Triad and provide definitions. Students will visit the FTC's website and explore identity theft and protective measures. After presenting the slides, students will consider how the CIA Triad relates to information security through a writing activity.

Active Learning Activity: "Avoiding Identity Theft" from the Federal Trade Commission is included in the slide deck for students to explore security controls for identity theft.

Active Learning Activity: How does an email phishing attack breach information security in terms of confidentiality, integrity, and availability? How do fake social media accounts breach the CIA Triad? What security controls could have prevented or protected the user?

Challenge Activity: Two optional activities are provided as extensions to this lesson. In the first challenge, students compose a phishing email. In the second challenge, students research privacy laws.

ACKNOWLEDGEMENTS

Resources:

Pesante, L. "Introduction to Information Security [PDF]" February 06, 2013. CISA.

Cole, M., Esposito, R., Biddle, S., & Grim, R. (2017, June 5). Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election. *The Intercept.*

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