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

THE CIA TRIAD LESSON

The slides present the CIA Triad as a model for understanding information security. The warm-up introduces information security and personally identifiable information (PII). Students engage in an activity to transmit "secret" information. Identity theft and its consequences are investigated. A writing prompt explores how phishing emails and fake social media accounts can impact information security.

LAB ENVIRONMENT

Classroom or computer lab with Internet access and a projection device for the slides. The slide presentation guides the instructor through the learning activities.

LAB FILES NEEDED

- CIATriad_Presentation.pptx

GUIDING QUESTIONS

What is "trust" based upon in the online world?

How does the CIA Triad affect information security?

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.

Over the course of at least two months in 2017, 143 million Americans were impacted by the Equifax data breach. Equifax failed to apply a security patch. The hackers acquired names, Social Security numbers, birth dates, addresses and even some driver's license information.

PERSONALLY, IDENTIFIABLE INFORMATION/STEP 1

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

- Social security number
- Age
- Race
- Phone number(s)
- Medical information
- Financial information
- Biometric data

PII is data that has value to a hacker to either steal identity or commit a criminal act. The consequences of a data breach can be relatively minor or devastating losses can result from a phishing attack. Loss of productivity, financial loss, legal liability, loss of credibility, market share and opportunities can be impacted, even loss of life.

ALICE-BOB-EVE/STEP 2

A small group activity (3 students per group) challenges a sender to send a "secret" number to a receiver, transmitting the message through the eavesdropper. The point of the activity is to get students thinking about information security. The students in the roles of Alice and Bob can privately discuss how they will securely transmit a "secret" number, but they cannot discuss the actual number. The role of Eve (the eavesdropper) is to attempt to intercept the number. Alice and Bob should determine a method of "secret" communication. For example, they may decide to use the Caesar or shift cipher. If Alice and Bob successfully communicate the "secret" number, then confidentiality has been preserved.

Following this activity, the slide presentation introduces the foundation of information security, the CIA Triad. The slides provide essential vocabulary. The definitions are from the NIST (National Institute of Standards and Technology) glossary.

IDENTITY THEFT/STEP 3

Students then explore the "Avoiding Identity Theft" Federal Trade Commission (FTC) website which is included in the slide deck to explore security controls for identity theft. The FTC provides consumer information on identity theft and students should explore the information and answer these questions:

1) What is identity theft?
2) Why does it matter?
3) How can I protect myself?

1) Identity theft is a serious crime. Identity theft happens when someone uses information about you without your permission.
2) You will be responsible for what the thief does while using your personal information. You might have to pay for what the thief buys. This is true even if you do not know about the bills.
3) Anti-virus, anti-spying or security software, firewalls, user training, keep software up-to-date, be wary of pop-ups, check URLs, beware of redirects.

CIA TRIAD/STEP 4

After presenting the slides, students will consider how the CIA Triad relates to information security by answering the following writing prompts.

Writing Prompts: 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 ACTIVITIES

The challenge activities are optional. In the first challenge, students compose a phishing email to demonstrate their understanding of how phishing works. In the second challenge, students research a privacy law.

WHAT TO SUBMIT

Students conduct research in Step 3 of the lesson. In Step 4 students compose a response to the writing prompt.

ACKNOWLEDGEMENTS

"Avoiding Identity Theft." *Consumer.Gov.* Federal Trade Commission. 4 Aug. 2012.