# 

| **Activity Name** | **Length of Time 0:00** | **Cyber Hours** |
| --- | --- | --- |
| **CIA Research** | **:55** | **1** |

## 

| **Description** | Introduces students to 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. |
| --- | --- |
| **Learning Objectives** | Students will understand and practice the CIA Triad as a model for understanding information security. |
| **TA Instructions** | WARM UP: WHAT INFORMATION IS VALUABLE TO A HACKER?  The Office of Personnel Management (OPM) serves as federal employees' storehouse of personnel records. In 2015, OPM discovered a data breach where data was stolen, including names, addresses, places of birth, Social Security numbers, financial information, fingerprints, and background checks on millions of people.  In 2017, 143 million Americans were impacted by an Equifax data breach. Equifax failed to apply a security patch, so the violation occurred for at least two months. The hackers acquired names, addresses, birth dates, Social Security numbers, and driver's license information.  STEP 1: PERSONALLY IDENTIFIABLE INFORMATION/STEP 1  Prompt: What defines personally identifiable information (PII)? What are some possible effects of a data breach involving this information?  “To distinguish an individual is to identify an individual.”  PII is any information about a person maintained by an organization—it includes:   * Social Security number * Age * Passport number * Driver’s license number * Race * Taxpayer identification number * 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.  Examples: Loss of productivity, financial loss, legal liability, loss of credibility, market share, and opportunities can be impacted, even loss of life.  The Organization for Economic Cooperation and Development (OECD) Fair Information Practices promote the protection of PII. These practices are:   * Collection limitation: there should be a limit to the amount of data collected by an organization * Data quality: PII should strictly be acquired for the purposes it is intended to be used * Use limitation: PII should not be disclosed or availed for purposes except those specified * Purpose specification: the purpose for which PII is collected should be specified before the data is put to its intended use * Security safeguards: personal data should be protected using security safeguards against risks such as unauthorized access or modification * Openness: PII must be guided by an openness policy which allows for proving the existence/nature of PII * Individual participation: a person should have the right to confirm whether a data controller possesses any PII regarding them, have any PII related to them communicated to them, and be able to advocate for PII erasure or amendment when necessary * Accountability: PII controllers should be accountable for the data they handle   STEP 2: SENDER / RECEIVER / EAVESDROPPER  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 the sender and receiver can privately discuss how they will securely transmit a “secret” number, but they cannot discuss the actual number. The role of the eavesdropper is to attempt to intercept the number. The sender and receiver should determine a method of “secret” communication. For example, they may decide to use the Caesar or shift cipher. Confidentiality has been preserved if the sender and receiver successfully communicate the “secret” number.  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 glossary of the NIST (National Institute of Standards and Technology).  STEP 3: IDENTITY THEFT  Students then explore the “Avoiding Identity Theft” Federal Trade Commission (FTC) website in the slide deck to explore security controls for identity theft. The FTC provides consumer information on identity theft, and students should study the information and answer these questions:  1) What is identity theft?  2) Why does it matter?  3) How can I protect myself?  Possible responses:  1) Identity theft happens when someone uses your information 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, keeping software up-to-date, being wary of pop-ups, checking URLs, beingware of redirects, and protecting mailboxes.  STEP 4: CIA TRIAD  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 regarding confidentiality, integrity, and availability? How do fake social media accounts breach the CIA Triad? What security controls could protect the user?  CHALLENGE ACTIVITIES  The challenge activities are optional. In the first challenge, students compose a phishing email to demonstrate their understanding. In the second challenge, students research a privacy law.  WHAT TO SUBMIT  Students conduct research in Step 3 of the section. In Step 4, students compose a response to the writing prompt. |
| [**Artifacts and Links**](https://drive.google.com/drive/folders/1mNsCW5dRUiHjE_Zoi3p7YjO1RsRJFhVK?usp=share_link) | | [Avoiding Identy Theft](https://consumer.gov/scams-identity-theft/avoiding-identity-theft) |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| **Additional Information** |  |

## 

## 

## 