Lesson Plan*

LESSON TITLE: Fundamentals of Information Security

SUMMARY:

This module presents essential fundamentals of information security concepts including Confidentiality, Integrity, Availability, and non-repudiation. Various components of a typical information system will be presented including software, hardware, data, users, etc. The module will highlight the importance of humans as a central component of any system and how human errors are the typical cause of system compromises. The common saying that “humans are the weakest link of the security chain” will be expounded with several real-world examples. In such context, other cybersecurity concepts will be fully explained. The concept of Keep It Simple will be introduced as a technique that will help minimize human errors as participants will have a better understanding of the systems they need to defend. Additionally, when discussing various components of an information system, the concept of Defense in Depth will yield itself well. For example, the discussion will include an explanation of how various components can be viewed as different layers of security that attackers must then defeat to conduct a successful attack. Moreover, common attacker motivations will be discussed which will familiarize participants with adversary mindsets and introduce essential ethical aspects.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

TIME REQUIRED: 120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples	
Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts. 2. Evaluate and analyze the availability of information systems while achieving defense in depth against Internet frauds.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Lab Computers
Internet Access
Account on GenCyber Coins system
Lab handouts

Describe any Previous Knowledge that may be Required:

Basic Math and problem solving skills.

How will you facilitate the learning?

- Describe the Warm-up Activity:

The instructor will explain the basic components of a typical Information system and discuss how we can protect these systems while making explicit links to the six GenCyber Cybersecurity concepts. Several examples will be used to hook the students on the discussion with emphasis on the 4 C's (Communication, Collaboration, Creativity, and Critical thinking).

- Describe the Focused Activity:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve this, one approach is to use a series of lab-based activities to enable students to “do it yourself” to enhance their comprehension of taught contents. Such lab activities include "Bug Bounty" and "Reconnaissance" from the GenCyber Coin Site. One other approach is to use mobile technology to enhance participant involvement using their phones (BYOD) to participate in interactive exercises such as online quizzes (Kahoot) and simulations.

Bug Bounty: This tool allows students to "think like an adversary" and attempt to find bugs in the GenCyber Coin game website. Secure coding concepts, ethical hacking, and human error will be discussed as students work through finding the bugs.

Reconnaissance: This game again encourages students to "think like an adversary" by conducting social engineering based research on the GenCyber faculty and staff. This activity provides a more in depth and hands-on look into how human error, and the human desire to share personal information, may cause breaches in security. This activity will be introduced in this module, and can be conducted during the remainder of camp.

- Describe the Teacher Instruction:

N/A

Mapping to GenCyber Cybersecurity First Principles:

☐	Domain Separation	☐	Abstraction
☐	Process Isolation	☐	Data Hiding
☐	Resource Encapsulation	☐	Layering
☐	Modularity	☐	Simplicity
☐	Least Privilege	☐	Minimization

Mapping to GenCyber Cybersecurity Concepts:

☑	Defense in Depth	☑	Availability
☑	Confidentiality	☑	Think Like an Adversary
☑	Integrity	☑	Keep It Simple

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	A number of assessment approaches will be adopted: 1- Regular observation of campers performance in the given tasks 2- Interactive competitive quizzes as discussed above. 3- Oral questions and walking around.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

Potential use and applications of the covered activities will be discussed so that students can use/apply these ideas and activities at their schools in programming, science and similar clubs. Students will also have access to the GenCyber Coin game indefinitely, and can continue learning and exploring on the site.

Acknowledgements:

Many thanks for Ms. Lydia Taylor for her excellent contributions to the design and testing of this module's activities.

Many thanks to Dr. Vitaly Ford for the use of his interactive and engaging GenCyber Coin Game website.