Unit 2 Human Factor

Content Area: **Computer Science**
Course(s):
Time Period: **Marking Period 1**
Length: **1 Week**
Status: **Published**

Brief Summary of Unit

This unit focuses on how humans affect cybersecurity. We discuss concepts of social engineering and how to protect against them as well as the significance of phishing and OSINT (Open Source Intelligence). We conclude with examining how to adhere to a "clean desk" policy.

Revised Date: July 2025

Standards

ELA.L.SS.11–12.1	Demonstrate command of the system and structure of the English language when writing or speaking.
ELA.L.KL.11–12.2	Apply knowledge of language to understand how language functions in different contexts, to make effective choices for meaning or style, and to comprehend more fully when reading or listening.
CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
TECH.9.4.12.DC.6	Select information to post online that positively impacts personal image and future college and career opportunities.

Essential Questions

- How and why is open-source intelligence used legally to gather free, public information?
- How can humans pose a risk to an organization?
- How can we protect against social engineering?
- Why is phishing considered the largest source of malware delivery and identity theft?

Enduring Understandings

- Humans can make careless mistakes that can lead to a security breach.
- Open-Source Intelligence is gathered through free, publicly available means.

- Phishing is the largest single way that malicious actors achieve their goals.
- There are many ways to protect against social engineering and they do not require advanced technological knowledge.

Students Will Know

- How to protect against the seven steps most commonly found in a hacking attempt.
- The definition of a clean desk policy.
- The different means of social engineering.

Students Will Be Skilled At

- Detecting when they may be on the receiving end of a social engineering attempt and how to mitigate the risk of that happening.
- Examining the available privacy settings on social media sites, and using them to specify who can see personal information.
- Examining their digital footprint, and taking steps to ensure it is positive as well as not too revealing.
- Identifying the characteristics of a "Clean Desk Policy" and if such a policy is being observed.

Assessment

Assessments

- Formative: Teacher observations, student-centered discussions, classwork, student-centered labs.
- Summative: Quizzes, tests, projects.
- Alternative: Verbal discussions and debriefs.

Learning Plan

This curriculum follows cyber.org's "Cybersecurity 1" course as listed in the "One Semester Plan." Go to https://cyber.instructure.com/login/canvas and apply for a teacher account. Under "High School 9-12," you will find the Cybersecurity 1 course with detailed lesson plans and pacing. They assume roughly 45 minute classes. Below is a modified pacing guide to align more smoothly with our rotating drop schedule.

There are 5 assessment days that can be used throughout the course with the timing below if none of the "if time allows" lessons are taught. These days can be used for quizzes/tests as the teacher sees fit.

- Section 2.1 - Social Engineering

    - 2.1.1 - Social Engineering **(1.5 Classes)**
- Section 2.2 - Phishing & OSINT
    - 2.2.1 - Phishing **(0.5 Class)**
    - 2.2.2 - OSINT **(1 Class)**
    - Skip lesson 2.2.3 unless time permits
    - 2.2.4 - Mitigating the Human Risk **(1 Class)**

Materials

- Core instructional materials: Core Book List
- Supplemental materials: Resources from the cyber.org curriculum "Cybersecurity 1."

- Computers
- Teacher created activiites
- Teacher created notes
- Websites to research current events

Integrated Accommodation & Modifications

Possible accommodations/modification for Introduction to Cybersecurity