# Lesson Plan

**LESSON TITLE:** Module 8: Online Safety Practices and Threats

## SUMMARY:

The Internet can be a dangerous place. End users need to be aware of the common attack surfaces employed by hackers, scammers, and stalkers. Whether shopping online, communicating via email or text, or simply browsing webpages, users are frequently unaware of how exposed they are to electronic attack via phishing, malware, and other common scams. This is especially true for younger users, who may not appreciate the gravity of some of their choices. On the other side of the spectrum, elderly users may lack the tech savvy to differentiate a safe pop-up from a Trojan horse attack.

## GRADE BAND:

☐ K-2
☐ 3-5
☐ 6-8
☒ High School

## Time Required:

180 minutes

## Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Understand online safety practices and threats;
- Be cognizant of the inherent tradeoffs regarding connectivity, privacy, and vulnerability;
- Make more responsible choices as a digital citizen.

## Materials List:

- Lecture Presentation
- Private Investigator Exercise and Answer Key
- Educational Games

## How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

- Delivery method - participatory lecture
- Formative assessment (web-based student response system and “Fist-to-Five”)
- Gamification (periodic quizzes, leaderboard)
- Group discussion after activity
- Cooperative active learning

## This lesson includes:

☒ Mapping to Cyber Security First Principles
☒ Assessments
☒ Learning Objectives

## Mapping to Cyber Security First Principles:

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

## Assessment of Learning:

| TYPE (Examples Listed Below) | NAME/DESCRIPTION |
|---|---|
| Writing Assignment<br>Presentation<br>Other<br>Choose an item.<br>Choose an item.<br>Choose an item.<br>Choose an item. | In the private investigator exercise, participants will use various tools to extract forensic data and reconstruct a timeline of the target's actions.<br>After playing the educational video games, participants will discuss lessons learned, then create an original set of email messages that emulate common scammer patterns.  Participants will also discuss what makes a password effective, and will identify useful strategies for creating optimal passwords. |

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

Reference YouTube videos will include annotation and/or closed captioning as appropriate.  Educational games can be modified for large font size.  Google Doc presentation and exercise can be modified for large font size and high contrast.

## Description of Extension Activity(ies):

I. Exif Data Private Investigator Exercise

Participants will play the role of a private investigator and digital forensics expert whose client suspects her husband of cheating.  They will use the following tools to extract the forensic data and reconstruct a timeline of the target's actions.

- Exif Extractor
- Text Editor
- Spreadsheet Application
- Google Maps and Google's My Maps

II. Playing Educational Games
Participants will play two educational games developed at Jacksonville State University:  1) Brute Force, a password protection lane defense game; and 2) Space Scams, a phishing email game.  Players will attempt to achieve the highest possible score.  After playing Space Scams, participants will discuss lessons learned, then will climb up Bloom's taxonomy to create an original set of email messages that emulate common scammer patterns.  These messages can be integrated into the game to customize it for participants' future

use.  Similarly, after playing Brute Force, participants will discuss what makes a password effective, and will identify useful strategies for creating strong, memorable passwords.

## Acknowledgements: