Information Security Series

Bob Brown – Kennesaw State University
Bob.Brown@Kennesaw.edu

This is a series of three sessions, each planned for a class period of about 50 minutes. This was developed with older students in mind, but will probably work for any middle or high school grade. It is likely to work best if presented over a period of three or six weeks rather than all at once.

The series does not include anything about "the Internet is a scary place." By middle school, student have already heard that. Students who engage with this material will come away with a grounding in the basics of computer and information security, a fundamental understanding of encryption and its importance, and a recognition that not all threats are equally likely or equally severe. They will come away with an understanding of *why* they must do some things and must not do others.

Prerequisite: Working familiarity with computing equipment, such as desktop computers, tablets, or smart phones.

First Session: Information Security Fundamentals

- Lecture, with slides, covering the following (15 minutes)
    - Properties of a secure system (confidentiality, integrity, availability)
    - Aims of attackers (disclosure, alteration, denial)
    - Goals of information security (prevention, detection, response)
- Class discussion: who are these attackers? (5 minutes +/-)
- Class discussion with scenarios, *e.g.* Alice changes the amount of a gift card. Is that disclosure, alternation, or denial? How related to confidentiality, integrity, availability? (10 minutes)
- Lecture about information assets (hardware, software, data) (5 minutes)
- Class discussion: what are a middle school student's information assets; each student to make a list (to end of period)

Students who complete this session successfully will be able to:

- List the three properties of a secure system and briefly describe each
- List the aims of attackers and match each one with the corresponding property of a secure system
- Identify some actors (attackers) who threaten computer security
- List the goals of information security
- Given a relatively simple computer system, identify the assets to be protected.

Second Session: Encryption

- Lecture, with slides, covering the following (15 minutes)
    - Why encryption is important
    - Fundamentals of encryption: the Caesar Cipher
    - A more advanced algorithm: the Vigenère Cipher
- Class exercise: encrypt a secret message using the Vigenère cipher (10 minutes)
- Class discussion: length of encryption keys; keys should be both long and random; same for passwords. (5 minutes)
- Lecture: the key exchange problem and public key crypto. (15 minutes)
- Take-home exercise: generate your own public key (5 minutes of class time, and a handout. Not graded)

Students who complete this session successfully will be able to:

- State the purpose of encrypting data and relate that purpose to the properties of a secure system
- With guidance, encrypt messages using a simple cipher algorithm
- Describe the fundamental operation of public key cryptography
- Explain the key exchange problem and tell how it is solved by public key cryptography.

Students who are particularly engaged will have generated their own public keys.

Third Session: Threat Analysis

- Lecture, with slides, covering the following (15 minutes)
    - Information assets, states, and controls (the McCumber Model)
    - Reminder: Confidentiality, integrity, and availability
    - Reminder: your information assets (from the first session)
- Class discussion (15 minutes)
    - What are the bad things that can happen to your information assets
    - Which of them is the worst, and what does "worst" mean, anyway? Which is next?
    - What measures can be used to counter the worst threats.
- In-class exercise: list the protections you should apply to your own information assets (10-15 minutes)

Students who complete this session successfully will be able to:

- Identify threats to the assets listed in session one
- Arrange threats in order of most likely and most severe
- List measures that can be used to protect against threats.