codeforgrove

CYBER SECURITY BOOT CAMP

Introduction to Cyber Security

Session 1

Sponsored by:

ca technologies

intel

KOVARUS Integrated IT Expertise

SMUD

CALIFORNIA COMMUNITY COLLEGES Doing What MATTERS™ FOR JOBS AND THE ECONOMY

ISSE SERVICES

YELLOW CIRCLE

YELLOW CIRCLE INC
PO Box 2383
Elk Grove California 95759-2383

Teacher Lesson Plan

Session Name:

Introduction to Cyber Security

Summary:

Cyber Security is an increasingly in-demand field of Computer Science. In this session we will look at the major ideas in the fields of Cyber Security or Information Assurance. This is not a "hacking" class but we are looking at the ways that computers, programs, networks, and people are exploited by hackers and what we can do to prevent or minimize the damage caused by bad actors.

Time Allotment:

75 minutes

Learning Objectives:

- Discuss ethical behavior in online context
- Ethical dilemma, gray areas
- Identify Ten Commandments of Cyber Ethics
- Describe a major hacking event
- Identify the vulnerability that led to the attacks
- Suggest ways to prevent similar attacks

Supplies:

- Scrap paper / notepad to take notes
- Laptop / computer with Internet access to research topics
- Ethics Statement for review and signature (print)
- Ten commandments (print)

Learning Activities:

- (2 - 5 minutes) - Teacher Introduction

  Introduce yourself to students. Provide your name, industry experience, current job, fun activities you do, and something awesome about cyber security. This is session one, and a very good place to define some ground rules.

- (2 - 5 minutes) - Volunteers Introduction

  Introduce volunteers that are present in classroom. Teachers will be provided with a quick bio of each volunteer who are helping in the classroom.

- (5 minutes) - Session overview

  Students need to understand that the material learned in this class should not be used to access files, networks, or other property that they do not have permission to access. Lack of security does not imply permission.

  Student activities introduce students to Ethics Statement, and Ten Commandments of Cyber Ethics.

  As a class looking at how computers are exploited, we will be learning a lot of skills that could be used to access someone's computer or network without their permission. While all of these skills are easily learned on the Internet, it is important that we agree to respect private property and never access something without permission.

- (5 minutes) - Ethics Statement review

  Have volunteers pass copies of ethics statement to students

  Ask students to read and understand Ethics Statement. Encourage questions from students. Get volunteers engaged in answering questions about Ethics Statement.

  Volunteers to collect signed copies of ethics statement from students

- (10 minutes) - Ethics Statement review

  Students need to understand that the material learned in this class should not be used to access files, networks, or other property that they do not have permission to access. Lack of security does not imply permission. Discuss each area of ethics statement with students, and make sure they understand prior to signing the statement. Inform students how important this statement is, and that everyone will get their signed copy back at the end of boot camp on Sunday afternoon. Once, everyone has read and has a common understanding of Ethics Statement, have volunteers collect signed copies from students.

- (5 minutes) - Look at several scenarios about ethical situations
  - *What would you do?*
  - *Did the people involve act ethically?*
  - *Who was harmed in this interaction, who is the victim?*

- (5 minutes) - Pass copy of “Ten Commandments of Cyber Ethics”

  Ask students to read and understand ten commandments. Encourage questions from students. Get volunteers engaged in answering questions about Ethics Statement.

- (5 minutes) - Commandments activity
  - *Have students look at "Ten Commandments of Cyber Ethics"*
  - *Students will pair up and each take one commandment.*
  - *Create an example and non-example of this commandment.Present to the class*
  - *Re-evaluate opening scenarios and describe what the ethical response is or is not appropriate.*
  - *Link the behavior back to ten commandments*

- (10 minutes) - Student group activity in pairs (2-3 students per group).

  In pairs, research one of the major hacking events of the past several years. In your research, identify several important ideas:

  Who was attacked?

  Who was the attacker (or who is thought to be if unclear)?

  What was the motive (money, political, warfare, prank)

  What was the result of the attack?

  How can this type of attack be prevented in the future?

- (5 minutes) - Major hacking events, presentation

  2010 - Stuxnet
  2011 - PSN
  2014 - Mt. Gox
  2013 - Target Christmas Shopping Credit Card Data
  2014 – Heartbleed Bug
  2015 - Jeep Hacked
  2015 - IRS hacked

- (5 minutes) - Activity review / feedback
  - *Discussion of hacking events*
  - *Hackers gain a detailed knowledge of a computer or system then find vulnerabilities.*
  - *Thinking of your own house, could you get in if you didn't have a key? What inside knowledge do you have of your own home that would allow access?*
  - *What could you change to strengthen your home-security? Would the additional security be a benefit or a hindrance? For example, 10 locks would make your door more secure but would also limit your own access in a speedy way.*

- (10 minutes) - Video - Hire the hackers from TED

  https://www.ted.com/talks/misha_glenny_hire_the_hackers

- (5 - 10 minutes) Closing / Wrap-up
  - *Ask students about different way to keep yourself safe online*
  - *What are some methods hackers use to gain unauthorized access to a computer or network?*
  - *What can we do as individuals to prevent this?*
  - *What should companies or governments do about hacking?*

- (2 minutes) - Session Feedback

  Have volunteers distribute feedback form to students, and give them few minutes to fill out the survey.

  Volunteers to collect feedback forms and save them for event manager.

- (2 minutes) - What's next?

  Inform students to head back to cafeteria for snacks / break, and remind them to use restroom before next session starts.

Ethics Statement

In this cyber security boot camp, one may learn or gain access to methods of bypassing computer security measures, malicious uses for computers, how to disrupt normal operations of computers or networks, and / or other illegal, immoral or unethical uses of computers and networks. It is important then, that one must realize the responsibility that will accompany such knowledge. The realization of such responsibility shall come from adherence to the laws and guidelines held by the school, college, university, state, country, and global computer user community.

One will also be obligated to follow moral and ethical notions of honoring the privacy of others and their right to a secure and courteous computing environment. No information obtained through this boot camp should be directly or indirectly applied to any attack (unauthorized access, circumventing of security measures, affecting normal operation, destruction / copying of data, etc.) on unauthorized public, private, or commercial computers or networks. I have read and understood these statements and agree to adhere to the general computer usage policy.

Realizing my responsibilities, I promise to adhere to the above ethics statement. In the event of my failure to fulfill this promise I accept the consequences of my actions.

Name (PRINT): ____

Signature: ____

Date: _____________

Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.