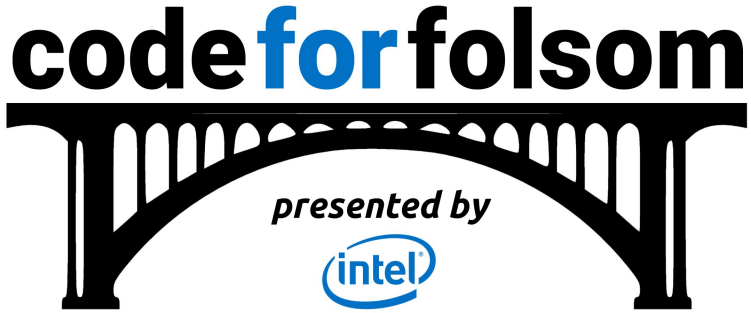


Introduction to Cyber Security

Session 1

A cybersecurity boot camp organized by YELLOW CIRCLE

Introductions

Instructors

- Name
- Job / Company
- Industry Experience
- Something interesting

Volunteers

- Name
- Job / School
- Something interesting

Session Overview

Introduction to Cyber Security

- Increasingly in-demand
- A field of Computer Science
- Not a "hacking" class
- Explore ways of exploitation
    - *Computers, Programs, Networks, People*
- Prevention, or minimize damage

Session Overview

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

Session Overview

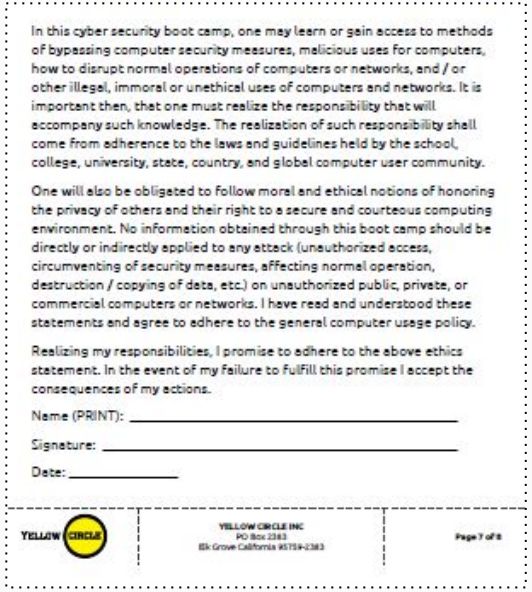
Permissions & Access

- No permission = Do NOT access
- Lack of security does not imply permissions
- Apply learned materials with care

Student Activity

Ethics Statement

- Volunteers to pass copies
- Read the 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: _____

YELLOW CIRCLE

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

Page 7 of 8

Ethics Statement Discussion

- Follow laws and guidelines
  - *School*
  - *State*
  - *Country*
  - *Global community*
- With Great Power Comes Great Responsibility

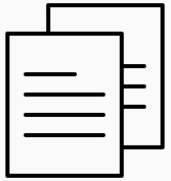
Student Activity

Ethics Statement Discussion

- Honor other's
  - *Privacy*
  - *Rights to secure environment*
  - *Rights to courteous environment*

Ethics Statement Discussion

- Not unauthorized:
  - *Access*
  - *Circumvention of security measures*
  - *Affect normal operation*
  - *Destruction / copying of data*



Student Activity

Ethics Statement Signing

- Print name, sign, and date
- Relax, volunteers will collect the signed sheets

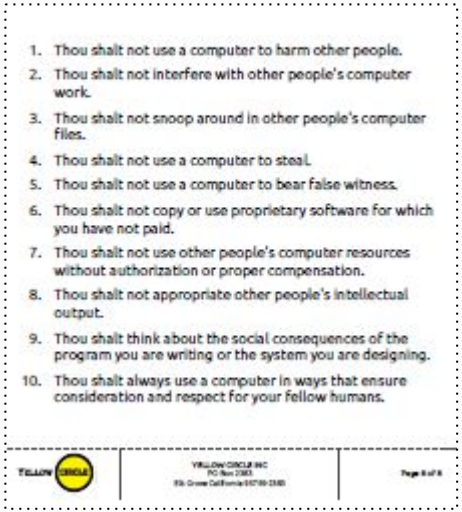
Scenarios

- What would you do?
- Did the people involve act ethically?
- Who was harmed in this interaction, who is the victim?

Student Activity

Ten Commandments of Cyber Ethics

- Volunteers to pass copies
- Read the commandments

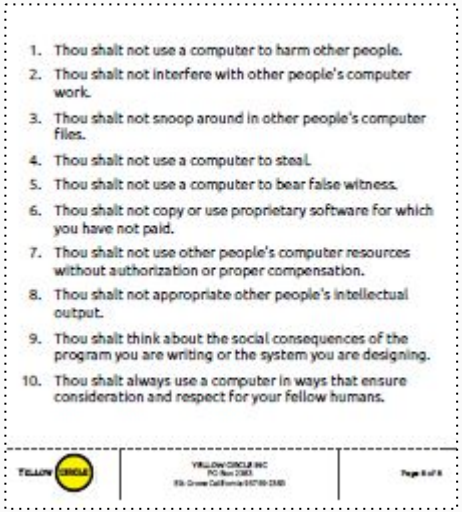


1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy 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.

Student Activity

Ten Commandments of Cyber Ethics

- Form groups / pairs
- Discuss one commandment per group

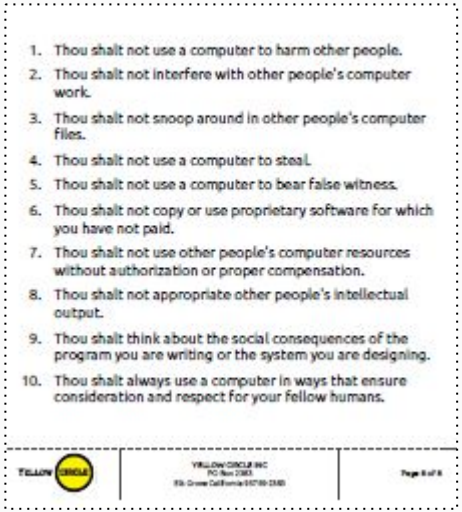


1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy 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.

Student Activity

Ten Commandments of Cyber Ethics

- For your commandment:
  - *Create an example*
  - *Create a non-example*
- Present to class



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.

Re-evaluate Scenarios

- What is the ethical response?
- What responses are not appropriate?
- Link the behavior back to commandments

Hacking Events / History

Major Hacking Events

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

Student Activity

Research Major Hacking Events

- Form groups / pairs
- One event per group
- Research
- Present

Research Major Hacking Events

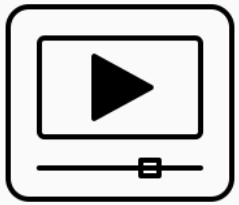
- Who was attacked?
- Who was the attacker (or who is thought to be if unclear)?
- What was the motive (money, political, warfare, prank)
- What was the result of the attack?
- How can this type of attack be prevented in the future?

Hacking Events Discussion

- Hackers gain a detailed knowledge of a computer system
- Hackers then find vulnerabilities

TED Talks : Hire the hackers

- Lets watch it:
  - *https://www.ted.com/talks/misha_glenny_hire_the_hackers*
  - *Teacher materials: video-1.1*
- Pause / Skip video for discussions



Closing / Wrap-up

What we learned?

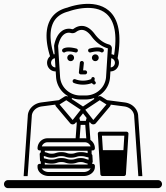
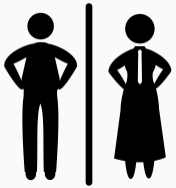
- Different way to keep yourself safe online
- Methods hackers use to gain access
- What can we do as individuals to prevent this?
- What should companies or governments do about hacking?

Session Feedback

How are we doing?

- Pass survey sheet
- Students:
  - Fill in Session #
  - Fill in Room #
  - Answer questions
- Volunteers to collect surveys

What's next...

End of session 1

- Time for break
- Snacks served in Cafeteria
- Remember to use restrooms