



AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## AFA CYBER ETHICS MODULE



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



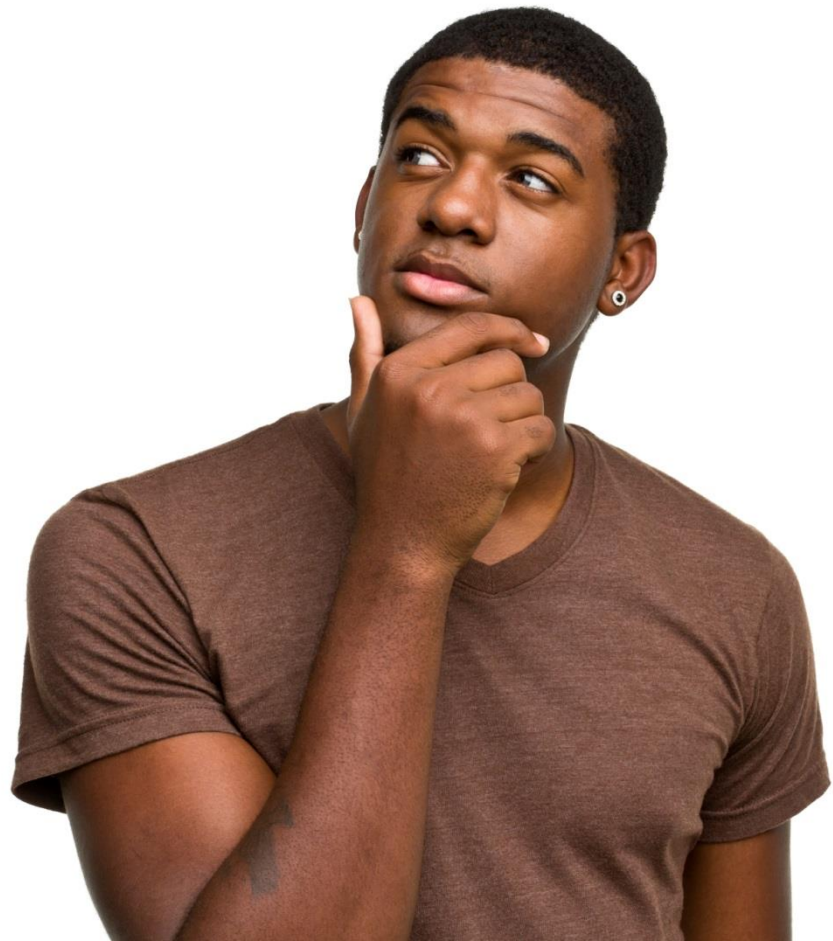
# Objectives

- Understand what ethics are and why they are important
- Understand how to act ethically
- Understand the responsibility that comes with knowing and using cybersecurity principles
- Understand how to apply ethics to real-world situations



# Introduction

- Ethics is about right and wrong
- What is right?
- What is wrong?
- How do we know?





# Why Ethics?

- Promotes a sense of fairness
- Creates a set of rules or acceptable behaviors
- Ethical practices help us identify and what unacceptable behavior “looks” and “feels” like





# What is Ethics?

- Standards for right and wrong
  - What we should do in different situations
  - Can be both written and unwritten
    - Written: company mission statements, school policies on academic dishonesty
    - Unwritten: don't "cut" in a line, opening doors or holding elevators for people





# Sources of Ethics

- Laws
- Feelings
- Societal Norms
- Religion
- Philosophy
- Family





# Ethical Behavior

- Do people make good decisions?
- Do people always make good decisions?
- Do YOU make good decisions?
- Do YOU always make good decisions?
- Does a bad decision mean you're unethical?



# Understanding vs. Behavior

- Knowing right from wrong doesn't automatically mean we DO the right thing







# Ethical Behavior Requires

- Courage
  - See something, say something
  - Be willing to go against your friends/peers
  - Stand up to bullies
- Humility
  - Even you can make a wrong decision
  - Are you a better than the average driver?
  - Are you more ethical than the average person?



# Questions

- Does the Internet make it easier or harder to act ethically?
- Is it easier or harder to do the right thing when others are watching?
- Is it easier or harder to do the right thing when it means that you have to choose between friends?



# Principles of Cyber Ethics

## Do not:

- ☐ Do not use a computer to harm other people.
- ☐ Do not interfere with other people's computer work.
- ☐ Do not snoop around in other people's computer files.
- ☐ Do not use a computer to steal.
- ☐ Do not use a computer to bear false witness.
- ☐ Do not copy or use proprietary software for which you have not paid.
- ☐ Do not use other people's computer resources without authorization or proper compensation.
- ☐ Do not appropriate other people's intellectual output.

## Do:

- ☐ Do think about the social consequences of the program you are writing or the system you are designing.
- ☐ Do always use a computer in ways that ensure consideration and respect for your fellow humans.





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## CURRENT EVENT ONE

### Terry Childs

As told by former San Francisco Mayor Gavin Newsom  
to Slate Magazine



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Terry Childs

- Should Terry Childs have been arrested?
- Which principle(s) of cyber ethics did Terry Childs violate, if any?





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## CURRENT EVENT TWO

**Desmond Hague**

Former CEO of Centerplate



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Desmond Hague

- Should Mr. Hague have been forced to resign?





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## CURRENT EVENT THREE

**Wesley Autrey**

Subway Superman



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)





# Wesley Autrey

- Could we have done the same thing?





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## AFA CYBER ETHICS MODULE

### Ethics Activity



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SCENARIO 1

### Hack, No Hack?



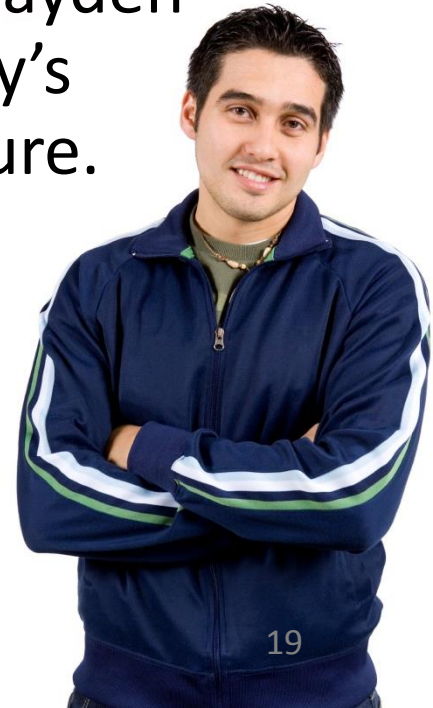
[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Scenario 1: Hack, No Hack?

Emily posted a picture of your friend Jayden on Instagram. The picture makes it look as if Jayden is consuming alcohol, but you know that he wasn't. Your friend Jayden is very upset and Emily refuses to take the picture down. Jayden asks for your help in getting into Emily's Instagram account to remove the picture.

**What should you do?**





# Scenario 1: Hack, No Hack?

- A. You don't want Jayden to get into trouble. So you tell him that you're only going to help this once. Then you use a tool that you found on the Internet to help Jayden get into Emily's Instagram account and remove the picture.
- B. You let Jayden know that Instagram allows people to report images that violate their rules. You help Jayden contact Instagram to have them remove the picture and you let him know that it may take a few days to get an answer.
- C. You don't want to be a bad friend, so you help Jayden remove the picture. Then, you change the Emily's password so she can't repost the picture. Later, you borrow Emily's phone and delete the picture from there too so that this situation will be over.
- D. You explain to Jayden that it's his fault for being in the picture in the first place and Emily shouldn't have to take down the picture. You also explain how things can stay on the Internet forever and that you don't want to be friends with people who don't make good decisions.



# Scenario 1: Hack, No Hack?

## Discussion





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SCENARIO 2

**How do we deal with a bully?**



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



## Scenario 2: Bullies

You and your friends are playing an online game and a classmate, Alex, is logging on and breaking the rules. Alex's obnoxious behavior is making it very difficult for you and your friends to enjoy the game. You have reported him to the game publisher, but he keeps creating new accounts and harassing you.

You recently found a tool on the Internet that allows you to remove a person's computer from the game temporarily. The website where you found the tool says that it doesn't cause any long term damage.

**What should you do?**







## Scenario 2: Bullies

- A. You should use the tool you found just this once so you can enjoy your game in peace.
- B. You and your friends have paid for this game like everyone else and you deserve to play it without being harassed. You should use the tool anytime Alex comes on and starts harassing you.
- C. You look up the standards of conduct and complaint procedures for the game. You tell your parents, or another adult, about Alex's harassment and ask them to help you report the behavior appropriately.
- D. All the things that Alex is doing to you, you should do back to him. He should treat people the way he wants to be treated.



# Scenario 2: Bullies

## Discussion





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SCENARIO 3

**Am I still responsible?**



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



## Scenario 3: Am I still responsible?

It is Sophia's first day as an intern in a computer security firm, and she and her supervisor, Christopher, walk by another intern's computer workstation. The workstation has not been locked down and they notice that the browser is currently opened to the user's banking website.

Christopher, is a well-respected person in the firm, but a bit of a practical joker, and decides play a joke on this person's unsecured computer. He logs out of the banking website to protect the user and then proceeds to change the computer desktop background to kitten images.



## Scenario 3: Am I still responsible?

Sophia feels uncomfortable about what Christopher is doing, and asks if his actions are a good idea; he states “Nah, it’s not a big deal, besides it’ll teach him a lesson.” She laughs and says, “Okay, then we should make the background My Little Ponies.” Christopher locks down the station, and he and Sophia step aside and wait to see what happens.





# Scenario 3: Am I still responsible?

1. Have Sophia and Chris acted ethically? Why or why not?
2. The intern returns, unlocks his station, and becomes visibly upset. He logs back into his banking site and furiously begins looking at his transaction history. Sophia notices that he looks upset, approaches the intern, and apologizes for what happened and assures him that nothing malicious happened. The intern is initially irritated but then tells her it is ok. He was just initially scared and was worried about someone stealing his banking information. Does the intern's acceptance of the joke exculpate Christopher and Sophia's actions ethically? Why or why not?



# Scenario 3: Am I still responsible?

## Discussion





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SCENARIO 4

### Good Intentions



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)





## Scenario 4: Good Intentions

Ashley recently took a computer security class where she learned about Wi-Fi. She learned that some Wi-Fi passwords can be easily broken.

Ashley, who is excited about what she has learned in class, shares what she learned with her aunt. Her aunt states that the store where she works has Wi-Fi with one of these easily broken passwords, but doesn't disclose to Ashley what that password is.



## Scenario 4: Good Intentions

Ashley tells her aunt that is a problem but her aunt tells her that they have very good IT people who will keep them protected. Ashley really wants to help the store where her aunt works, so she breaks the password to prove to her aunt that the system really is broken.





## Scenario 4: Good Intentions

1. Has Ashley acted ethically? Why or why not?
2. Assume Ashley did not use the password to access the Wi-Fi or any other systems connected to the Wi-Fi. She only showed her aunt the password to help make the store more secure. Does this change your answer?



# Scenario 4: Good Intentions

## Discussion





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SCENARIO 5

### Privileged Information



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Scenario 5: Privileged Information

Jessica has a group project due tomorrow, and she and her friends have been working hard on it. Yesterday, her group gave the final copy to Derek so that he could print it out and turn it in. Unfortunately, Derek is out sick today and not answering his phone. The group is at risk of getting a lower grade if the project is turned in late. Jessica has seen Derek type in his password multiple times and knows that she can get into his email account where their project is stored.

**What should she do?**



# Scenario 5: Privileged Information

- A. She should use the password just this once to retrieve and print the assignment so that the group doesn't get a bad grade. It would be unfair if the group were punished because one person was sick. Derek certainly wouldn't want them to get a bad grade.
- B. She should use the password to get and print the assignment. When Derek gets back, she should tell him what happened and help him choose a new password. That way it's not a big deal because she told him what happened and her friends won't get mad that she didn't use what she knew to help them get a good grade.
- C. She should tell the teacher the situation and ask the teacher to make an exception just this once and allow the group to turn in the project late. In the future, she should always make sure that multiple people in the group have access to the final project to avoid this type of situation.
- D. She should log into Derek's account to get and print the assignment. Then she should immediately change the password and let Derek know the new password when he gets back. She should also show him how to avoid other people learning his password by watching him type it in.



# Scenario 5: Privileged Information

## Discussion







AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## Scenario 6

### Responsible Actions



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Scenario 6: Responsible Actions

Joel is a competitor in the CyberPatriot National Finals Competition. During the competition you can overhear a member of another team talking from across another partition. You're not actively trying to hear his conversation, but he is a little louder than the others, and his voice projects rather well.





# Scenario 6: Responsible Actions

You overhear him suggest checking a port number that you didn't think about, and it inspires you to check the same port for vulnerability. The CyberPatriot Rules Book states that you should receive no outside assistance which includes direct and indirect advice.



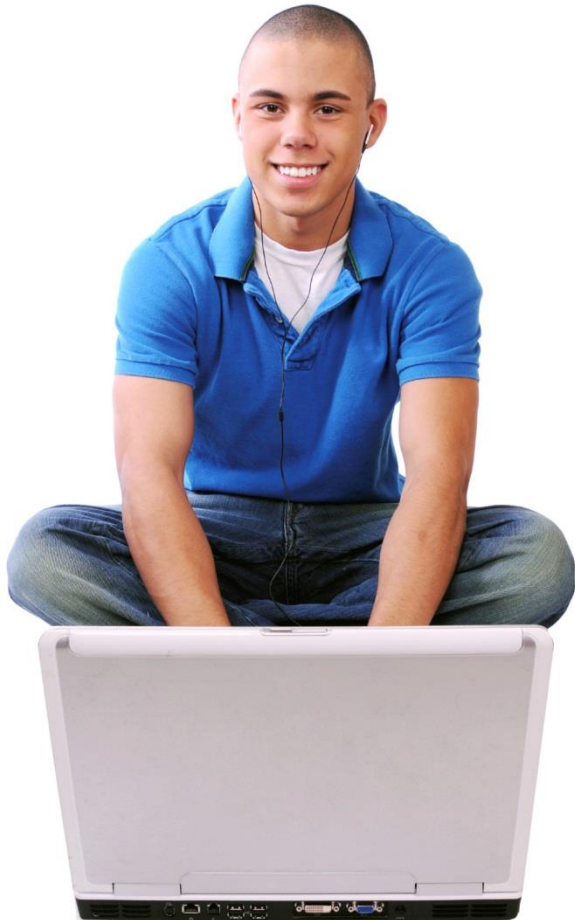
# Scenario 6: Responsible Actions

1. Is Joel obligated to report what he has overheard? Why or why not?
2. What if Joel tells the participant to quiet down and that he can hear him talking? Does that exculpate Joel from what he has overheard?



# Scenario 6: Responsible Actions

## Discussion





# Summary

- Understand what ethics are and why they are important
- Understand how to act ethically
- Understand the responsibility that comes with knowing and using cybersecurity principles
- Understand how to apply ethics to real-world situations