



**i am the key to building a safer USA**

## **SECURITY: CYBER CITIZENSHIP WEBCAST FIVE**

### **Grades 9-12**



*NOTE: This project is supported by Grant No. 2002-MU-MU-K003 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.*

---

---

## OVERVIEW

### Security: Cyber Citizenship – Suggested For Grades 9 through 12

#### Goals

Learners will develop an awareness of the citizenship responsibilities involved with Internet usage as well as current security threats such as steganography, hacking, hactivism, and cyber terrorism.

#### Description

This webcast is designed to increase student awareness of the concept that there are dangers associated with Internet usage. This lesson addresses cyber citizenship with issues inherent to Internet usage, steganography, hacking, hactivism, and cyber terrorism. The primary objective of this lesson is to equip students with knowledge that will enable them to make responsible choices regarding their usage of the Internet and to empower them to be better cyber citizens.

This lesson is comprised of several key elements:

- 1) The webcast delivered via <http://www.isafe.org>
- 2) Three directed discussion breaks during the webcast for the students in the classroom, facilitated by the classroom instructors
- 3) Cooperative group exercises at the conclusion of the webcast which include implementation of a Youth Empowerment activity
- 4) Pre- or post-assessment if either first or last lesson in your i-SAFE program.

#### Mandatory Webcast Forms

- Administer the assessment online at [www.isafe.org](http://www.isafe.org) if beginning or concluding the i-SAFE program.

If you have any questions, please contact the i-SAFE Education Department at [education@isafe.org](mailto:education@isafe.org).

---

## LESSON PLAN

### Introduce the i-SAFE program

Explain that i-SAFE America is a nonprofit educational foundation dedicated to:

- Enabling kids and teens across the United States to recognize and avoid dangerous, destructive or unlawful online behavior.
- Empowering them to be proactive in communicating their knowledge and understanding of Internet safety issues to their peers, family and community.

### Complete the Pre Assessment

Administer the pre assessment online at [www.isafe.org](http://www.isafe.org) if this is the first lesson completed for i-SAFE.

### Explain the Learning Objectives

The i-SAFE webcast, *Security: Cyber Citizenship*, will enable students to:

- Be able to identify key general attributes of the threats to the security of computers and information via the Internet:
  - Steganography
  - Hacking
  - Hactivism
  - Cyber Terrorism
- Be able to identify and understand critical attributes of the sources and consequences of Steganography in regards to individuals and to society:
  - Legal but used illegally?
  - Hidden and unknown
- Be able to identify and understand critical attributes of the sources and consequences of Hacking and Hactivism in regards to individuals and to society:
  - Unwelcome
  - Intrusive
  - Illegal
  - Damaging
  - Libelous (sometimes)
  - Targeted
- Be able to identify and understand critical attributes of the sources and consequences of Cyber Terrorism in regards to individuals and to society:
  - Use of current technology in new ways.
- Develop an understanding of how to protect themselves and their computers from external threats such as hacking
  - Firewalls
  - Security patches

---

## Select an Empowerment Activity

This webcast will highlight issues concerning cyber citizenship and Internet Security. Inform the students that as a class they will be asked to select an activity from the list or develop their own idea, in order to share information about how protect themselves and their computers during Internet usage. Upon completion of the Empowerment activity, offer the students the opportunity to take the activity outside of the classroom to mentor other students about online dangers.

As a class choose one of the following empowerment options or create your own project. This activity is an integral part of the lesson and learning process. Have Students:

- Write a letter to a newspaper about steganography, hacking, etc. as it applies to today's world.
- Draw a poster instructing others on the topics learned in this webcast.
- Create and provide a cyber citizenship pledge/certificate for students to sign saying they will be responsible online cyber citizens.
- Design your own steganography pictures. Post them around school and have students attempt to discover the hidden message. Over the PA system explain the contest and explain the dangers of steganography online.
- Host a discussion about how steganography can be used illegally/dangerously.

## Additional Outreach Options

All students are also encouraged to get involved in i-SAFE's Youth Empowerment and Outreach campaign by choosing additional options which include hosting an Internet Safety week, School Assembly, i-Parent Night, or Community Leaders' Meeting.

Select a youth empowerment activity from the Mentor Menu. Notify the students that by taking their Youth Empowerment Activities outside the classroom they are increasing Internet safety awareness and mentoring their fellow classmates. If they would like to get more involved with promoting Internet safety, they can join the i-SAFE Student Mentor Program by filling out copies of the Mentor Menu in your Professional Development Manual or by going to [www.isafe.org](http://www.isafe.org) and registering.

*Details for planning Youth Empowerment events may be copied from the Youth Empowerment Activities Section of the Instructor manual, or may be accessed online at [www.isafe.org](http://www.isafe.org) - click kids and teens.*

Inform the students that i-SAFE's Outreach team is ready to provide assistance, and to give special recognition, to students, classes, or schools, who do exceptional projects. Contact them at [Outreach@isafe.org](mailto:Outreach@isafe.org).

## Access the Webcast

Access the webcast at [www.isafe.org](http://www.isafe.org). Please note: you must be a registered school in order to access the webcast. If you do not have a School ID number, please contact the Education Department ([education@isafe.org](mailto:education@isafe.org)).

---

A high speed Internet connection (T1, ISDN, DSL or Cable Modem) is needed to view the webcast. If you do not have a computer with a high speed Internet connection, If you do not have a computer with a high speed Internet connection, please contact your District Coordinator or the i-SAFE Professional Development Consultant for your area.

### **Activity 1**

Pre-webcast discussion

Introduce the topic: Inform the students that today they will be talking about Cyber Citizenship and Internet Security issues in discussions about steganography, hacking, hactivism, and cyber terrorism.

**Question #1** – Ask students to define what they know about the cyber community and their role as citizens in it. Discuss what roles and responsibilities they take on as a member of this community.

**Question #2** – Discuss activities on the Internet that occur that are not in the parameters of a responsible cyber citizen. Explain that the focus of the lesson is on steganography, hacking, hactivism, and cyber terrorism. Ask students how and why these might occur.

Introduce key vocabulary that will be used in the webcast:

- Steganography
- Hacking
- Hactivism
- Cyber Terrorism

**Play the webcast; pause at the first discussion break.**

---

# WEBCAST - SECURITY: CYBER CITIZENSHIP

## Synopsis of Webcast – Part I

The hosts discuss the concepts of cyber citizenship and introduce the concepts of encryption and steganography. The concept of online steganography is explored along with its potential abuse.

### Discussion 1

This is the first discussion break in the webcast. Lead the students in a discussion about steganography to get their understanding and viewpoints.

**Question #1:** In the study, no examples of steganography use were found. Does this mean that it doesn't exist on the web? What are some potential abuses of steganography?

- By terrorists
- By criminals
- By common citizens unintentionally

**Question #2:** Do you think our government should screen for terrorist use of this technology? Why or why not?

Despite no current factual evidence to support terrorist or criminal usage of steganography, does this mean it doesn't exist? Could this technology be abused in the future? If abuse can or does occur, what can be done about it?

**Play the webcast; pause at the next discussion break.**

## Synopsis of Webcast – Part II

The hosts explain hacking and hactivism. The various types of hacking are discussed and explored along with the positive and negative consequences.

### Discussion 2

Lead the students in a discussion, using the following open-ended questions as a guide, to discuss the concept and consequences of hacking online.

**Question #1:** How does hacking affect the common cyber citizen? What are some consequences for all concerned?

**Question #2:** Do you agree with hactivism? Should people hack into websites that promote beliefs they disagree with? Unlike protesters who march or demonstrate and are willing to be arrested, hactivists are anonymous. So is hactivism true civil disobedience?

**Question #3:** Is web graffiti art, like tagging may be considered art in the real world? Should it be considered freedom of expression?

**Play the webcast; pause at the next discussion break.**

---

## Synopsis of Web Cast – Part III

The hosts continue to present information on hacking including consequences, prevention tips, and specific examples. Mention is made of how the items discussed so far can be used by a terrorist.

### Discussion #4

Lead the students in a discussion of the impact of security issues for all concerned.

**Question #1:** How would you feel if a hacker cut off your phone service and you needed to call 911? How can hacking cause real damage? What are other possible consequences and scenarios?

**Question #2:** What do you think is involved in being a good citizen on the web? How do the topics discussed in this webcast apply to cyber citizenship?

## CULMINATING ACTIVITY

1. Review the empowerment activity chosen earlier in the lesson. Briefly discuss how the activity will be implemented. For example, if students are going to create posters, plan the following:
  - Where will they obtain further information for the posters?
  - Will they use class time, etc.?
  - Will individuals or cooperative groups do the posters?
2. At this time allow students to develop their empowerment activity selection.

### Inform Students About I-Safe's Youth Empowerment And Outreach Program

- i-Safe has provided the students a unique opportunity to get involved in the National i-SAFE Student Mentoring Program. This program allows students to get involved in fun Internet safety awareness activities, work with other students nationwide, and gives opportunities for national recognition. If your students are interested in taking the next step and becoming mentors, please have them fill out the Mentor Menu or email i-SAFE at [mentors@isafe.org](mailto:mentors@isafe.org).
- The i-Safe Outreach team is ready to provide assistance. You can contact them with any questions or concerns at [Outreach@isafe.org](mailto:Outreach@isafe.org)

### Complete the Post Assessment

Administer the post assessment online at [www.isafe.org](http://www.isafe.org) if this is your last lesson for i-SAFE.