



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

## **SECURITY: MALICIOUS CODE WEBCAST FOUR**

### **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: Malicious Code – Suggested For Grades 9 through 12

#### Goals

Learners will develop an understanding of threats to the security of computers and information via the Internet.

#### Description

This webcast is designed to increase student awareness of the concept that there are dangers associated with Internet usage. It addresses Internet Security with issues inherent to Internet usage: Viruses, Worms, Trojan Horses, and Identity Theft. The primary objective of this lesson is to equip students with knowledge that will enable them to make responsible choices regarding their Internet use, to prevent security risks.

This lesson is comprised of several key elements:

- 1) The webcast delivered via <http://www.isafe.org>
- 2) Three teacher-facilitated student discussion breaks during the webcast
- 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 webcast, *Security: Malicious Code*, will enable students to:

- Be able to identify key general attributes of the threats to the security of computers and information via the Internet:
  - Malicious Code
  - Viruses
  - Worms
  - Trojan Horses
  - Identity Theft
- Be able to identify and understand critical attributes of the sources of, and consequences to individuals and society of identity theft:
  - Targeted
  - Illegal
  - Usually connected to other criminal behavior
  - Personal victimization consequences
- Be able to identify and understand how to protect themselves and their computers from external threats:
  - Resources available
  - Tips for safekeeping
- Develop a strategy to inform others of the security risks inherent to Internet Usage.

### Select an Empowerment Activity

This webcast will highlight issues concerning Internet Security issues and prevention tips. Inform the students that as a class they will be asked to select an activity from the list or develop their own idea, to share information about how protect themselves and their computers during Internet usage. As a class choose one of the following empowerment options. This activity is an integral part of the lesson and learning process. Upon completion of the YE activity, offer the students the opportunity to take the activity outside of the classroom to mentor other students about online dangers.

---

Have students:

1. Design a poster of prevention tips for various crimes and post in a public area.
2. Prepare 5-10 questions and call to interview a person at a help center for malicious code/identity theft. Share or publish a report on your findings.
3. Tackle a concept discussed in groups - like viruses, Trojan horses, malicious code, identity theft, and create posters to post in public area.
4. Create and broadcast public service announcements about why hacking/malicious code is detrimental; For example, read how much money it costs, how it victimizes, etc.
5. Research the history of hacking and its evolution; or find out penalties for your state/district on the various crimes – use the information to write and publish a news article.
6. Arrange to interview someone who handles computer crime for your district – air on cable for school.
7. Invite a speaker into class to discuss topics – personal identity theft, hacking, malicious code, etc.
8. Provide an information booth about Internet Security issues, and conduct a school pledge drive in which others will sign a pledge not to create malicious code, hack, or commit identity theft.

### **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 Internet Security and participating in discussions about the results of viruses, worms, and Trojan horses, along with resources and prevention tips.

Question #1 – Ask students to define what they know about Internet security, and in turn malicious code. Malicious code is programming code designed with a harmful intent – to hack, cause damage, etc. With Internet usage comes rights and responsibilities to protect your computer from malicious code. Malicious Code causes millions of dollars in damage every year.

Question #2 – Ask students to explain what they know about how the Internet works. Discuss how malicious code can spread across many computers so quickly. Examine the idea of interconnectedness.

Introduce key vocabulary that will be used in the webcast:

- Malicious Code
- Virus
- Worm
- Trojan Horse
- Identity Theft

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

---

## **WEBCAST - SECURITY – MALICIOUS CODE**

### **Synopsis of Webcast – Part I**

The hosts discuss the concepts of Internet Security and introduce the different types of malicious code. An overview of how the Internet works is provided as background to understanding how malicious code works and spreads.

### **Discussion #1**

This is the first webcast discussion break. Lead the students in a discussion about their understanding, experiences and viewpoints regarding malicious code.

Question #1: Have you or someone you've known experienced a virus, worm or Trojan horse? What was the outcome? What did you take away from this experience?

Cover the following:

- Time involved fixing malicious code
- Money spent – (by corporations and by individual to protect computer)
- Frustration involved

Question #2: How can you avoid Malicious Code?

Answers:

- *Anti virus software*
- *Careful use of email*
- *Careful use when downloading items*

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

### **Synopsis of Webcast – Part II**

The hosts explain malicious code. Famous viruses are used as examples. The concept of virus hoaxes is introduced. Worms are introduced with famous ones used as examples. Finally, Trojan horses are introduced and explained.

### **Discussion #2**

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

Question #1: Have you, or someone you know, been the victim of Identity Theft?

Question #2: How was it handled?

- What were consequences?
- What did victim go through?

Question #3: What did you take away from this experience?

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

---

## **Synopsis of Web Cast – Part III**

The hosts present information about Identity theft. The consequences for all involved are discussed along with prevention tips and resources. Prevention for malicious code is also discussed.

### **Discussion #4**

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

Question #1: How do security issues affect your usage of the computer.

Question #2: How do security issues affect large corporations or businesses?

Question #3: Why would people create these issues?

Question #4: What are consequences for the creators?

## **CULMINATING ACTIVITY**

1. At this point in the lesson, have students carry out the necessary steps to complete their empowerment activity.
  - Refer to the information discussed in the previous Activity and Discussion 4. As a group, organize how it will be used in the selected empowerment activity, and how the activity will be completed.  
*Note: posters, webpages, and presentations may be done in class or as a home learning activity.*
2. Inform the 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 the last lesson in your i-SAFE program.