
Cyber Security – Malicious Code

Webcast Lesson Plan

i-SAFE Lesson Plan

Suggested Grade Levels – High School

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> (click on quick link *webcasts*)
- 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. Click on the link: Assessments at www.isafe.org

Learning Objectives

Students will:

- identify key general attributes of the threats to the security of computers and information via the Internet such as viruses, worms, and Trojan Horses
- understand critical attributes of the sources of, and consequences to individuals and society of identity theft
- understand how to protect themselves and their computers from external threats
- be enabled to develop a strategy to inform others of the security risks inherent to Internet usage

Enrichment Goal

i-SAFE enrichment activities are designed so that they can be implemented by students. Provide your students with the necessary reference materials included with this lesson plan and guidance on how they can complete this activity. Suggestions include getting support from an adult advisor, school club, student council, technology team, etc. i-SAFE also offers a wide range of online support for students who register (free of charge) at www.isafe.org.

In this lesson, learners will interact in the classroom environment through group discussion and examination of online privacy issues. Learners will be provided with materials to engage in an enrichment activity, which includes a project to inform others about how to take measures to keep their computers secure.

Materials / Preparation

1. access to the Webcast, *Cyber Security: Malicious Code*
2. copies of the Enrichment Activity pages for each student
3. online i-Mentor registration (each student) to receive supporting online training videos and Student Toolkit materials

Pre Assessment

If beginning the i-SAFE program with this lesson, administer the pre assessment online at www.isafe.org by clicking on the link, Assessments, prior to the lesson. To verify School ID#, login at www.isafe.org, go to the "My Info" page and select "Find your school ID".

Lesson Procedures

All students participating in the i-SAFE curriculum are considered to be mentors. If they haven't done so already, have students enroll online by clicking on "Create Account" at www.isafe.org to take full advantage of the support and incentives offered. This may be done at any time during the lessons, or students may complete this registration at home. If you would like to register your students yourself simply go to <http://www.isafe.org/teachermentorprogram> and fill out the information for your students and email to outreach@isafe.org. Your students will then be enrolled to receive information about sharing internet safety with other students and registered to participate in contests to win prizes.

Access the Webcast

Access the webcast at www.isafe.org by clicking on quick link *Webcasts*. To find School ID Number: Login and check your "my info" page at www.isafe.org for school id #.

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, 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?

Conclusion

- Lead into a discussion about the Enrichment Activity.
- Provide a copy of the enrichment activity pages for each student.
- Discuss why it is important for students to share what they know about Cyber security issues with their peers, parents, and families.

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online.

Enrichment Activity

i-Mentor Training Network

i-SAFE provides the easy to access i-Mentor Training Network videos at no cost to help students share their knowledge about Internet safety with the uninformed. The 8-10 minute videos provide specific “how to” information on accomplishing i-SAFE outreach activities. They are available to students by going to the X-Block at www.isafe.org and selecting the i-Mentor Training Network.

The enrichment activity for this lesson is to engage students in an activity to promote cyber security education within the school and community by creating an information table and distributing information about how to protect against malicious code.

Student Instructions:

Registration

1. Go to www.isafe.org and register
2. Download the i-SAFE Student Toolkit for more information and Internet safety projects.

Information table

Students will create ways to inform the public about the risks of malicious code and how to prevent attacks on their own computers. The following is an introduction provided on the reference pages:

Unlike what many people think, computers are not designed to be maintenance free. Just like cars they need routine maintenance. And like cars – if treated well – they run better. To keep your machine running well and better yet, running securely, make sure you know some basic maintenance skills and practice proactive prevention. One way is to ensure safe and secure computing is to prevent against malicious code attacks by understanding (1) basic prevention methods to counteract malicious code, and (2) how to download virus protection software on your computer.

The security maintenance pages can be copied and handed out or used as a guide to teach others about how to protect their computers from malicious code. They include the following sections:

- The Basics – What is Malicious Code?
- Why worry?

-
- When is a good time?
 - How?
 - Four steps to prevention
 - Self Check evaluation

The “Reach Out” page provides information about how to set up and implement an information table. This resource can be applied to the creation of information table on any Internet safety topic.

Post Assessment

Administer the post assessment online at www.isafe.org by clicking on the link, Assessments, if this is your last lesson for i-SAFE. To verify School ID#, login at isafe.org, go to the “My Info” page and select “Find your school ID”.

Cyber Security Awareness!

Security System Check: Malicious Programs

Unlike what many people think, computers are not designed to be maintenance free. Just like cars they need routine maintenance. And like cars – if treated well – they run better. To keep your machine running well and better yet, running securely, make sure you know some basic maintenance skills and practice proactive prevention. One way is to ensure safe and secure computing is to prevent against malicious code attacks by understanding (1) basic prevention methods to counteract malicious code, and (2) how to download virus protection software on your computer.

The Basics – What is Malicious Code?

Malware includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a user's PC. Viruses, worms, and Trojan horses fall under this category. Each of these can cause your computer to act up.

- **Virus:** A virus is a malicious code that executes itself and replicates itself. For example – if you open an infected word file with a virus, the virus will run and then try to infect other word files on your computer (replication).
- **Worm:** To be a worm, the malicious code not only executes itself but then attempts to make copies of itself from one place to another. For example – if your infected word program then attempts to access your email account and email itself to everyone on your address list – it is a worm.
- **Trojan Horse:** A Trojan horse cannot run on its own. It depends on tricking the user into running the program. It is a program that pretends to be something it is not. One common example: A user downloads and loads a freeware game. In addition to the game, the program also installs spyware or something else in the background, which in turns runs on your computer.

Why worry?

Malicious Code can be extremely harmful. Programs can change settings on the computer, delete files, slow down connection times, bog down email, and more. One example is the ILOVEYOU worm/Trojan horse. It infected computers at more than half of the companies in the US and even more in Europe. When it spread to a computer, it did two things: first it overwrote files on the hard drive such as .jpegs. Meaning picture files would be overwritten with a copy of the worm so they could not be opened or recovered; secondly it installed a Trojan horse designed to collect passwords and transmit them to a server in the Philippines. The ILOVEYOU program replicated by sending itself to every address in the email program, causing it to also bog down the Internet.

When is a good time?

If not currently running virus protection software it is imperative that you obtain a program. You can purchase one or download from the Internet. If running virus protection, make sure you update it frequently as explained in the next section.

***Tip: it is important to read reviews on virus software before purchasing. Try typing, “top rated anti-virus software” into a search engine to find reviews. One reason for this – the most popular anti virus software programs are not always the most effective. Virus designers write their programs to attempt to fool these programs. By choosing a newer or less known anti-virus software, you may actually be better protected as long as that software has adequate updates, etc.

How?

Anti-virus programs are an excellent form of protection, but they are only as good as the most recent update. Even if you updated your definitions the week before a virus comes out, you are at risk until you get the latest update that protects against that new virus.

Follow these steps:

STEP 1. Installing and keeping current a good anti-virus product is an important step in keeping your computer secure. Although this software is called anti-virus, most of these applications also protect against worms and Trojan Horses. Most anti-virus software now has the ability to checking incoming and outgoing email (through popular email programs like Outlook), to protect you against receiving or spreading unwanted computer problems through email. Since Word and Excel documents are such popular targets, most antivirus software also specifically interfaces with these for protection.

Check Now: Take a moment to see if you are running virus protection software. Go to Start: Programs: and browse through your program list. Many programs are available. Common anti-virus programs include those provided by Norton, Symantec, and Pc-Cillian. If you have one of these, open the program and familiarize yourself with it. When opened, many programs have an update button on the very first page.

STEP 2. The second step is to keep your anti-virus software definitions regularly updated. Most anti-virus software programs have a feature to automatically update your definitions periodically and it's good practice to set this to update at least once a week.

Check Now: Go into your virus protection software and familiarize yourself with the options. See how to update and whether regular updates can be scheduled.

STEP 3. Next, you should be very careful in opening email. If you get an email with an attachment from a sender you don't recognize, don't open the attachment. Even if the sender is someone you do recognize, if you aren't expecting an email with an attachment from him or her, if the wording of the subject or message seems strange for that person to send you, don't open it without first checking with him or her to verify it is legitimate.

STEP 4. For protection from Trojan horses, be careful if you download and install any software from the Internet. If you do, be sure you are always downloading it from a reputable site you can trust. Several sites offer reviews of the software you can download, read the reviews to see if other users have registered any complaints about Trojans or freeware in the software you are planning to install. Most major anti-virus software also now provides some protection against Trojan horses.

Self Check:

- I understand the importance of running Virus Protection Software.
- I have a Virus Protection Program running on my computer.
- I have run an update of my Virus Protection program.
- I have scheduled my Virus Program to run regular updates on its own.
- I know the basic difference between the various types of Malicious Code.

Reach Out...

...And make a difference. Are you trying to think of a way to reach people about the dangers of the Internet? Well, here it is. Why not **set up an information table** and give students and community members new ways to stay cyber safe?

Hand It Over

Set up a table at lunch, during study hall, at a school sports event, or after school to let students, teachers, and parents know how to play it safe online. Or, if you wanna do more than just letting those in your school know, **take your information table down to a local grocery store or mall** and let others in the community learn how to protect themselves online.



Get Started

Here are ideas to help you give the 411. It's up to you how you want to get the info out there.

- **Select a location.**
- **Fill out the Mentor Menu and let i-SAFE know the details.**
- **i-SAFE will send you brochures and tip sheets.**
- **Set up a table and electrical power.**
- **Make an i-SAFE poster or banner for your info table.**
- **Recruit some friends to help.**
- **Pass out brochures and tip sheets.**
- **Play the i-SAFE videos on a TV or laptop at the table for others to view.**
- **Get a PA system and play the i-SAFE Audio PSAs.**
- **Announce Safety Tips over the PA system.**
- **Conduct an Internet safety survey.**
- **Raffle off prizes.**
- **Hold a slogan or PSA contest.**

Contact mentors@isafe.org for assistance.



Maryland Mentors reach out to students and educators about the i-SAFE program at a youth conference.