The Leader in e-Safety Education

Terms of Use

Clicking on the "Agree and Print" button (below) means that I agree that:

- i-SAFE© lessons may NOT be shared with other educators (e.g., faculty or staff) in any school or district which is not currently covered by your school's or district's Subscription and License Agreement.
- i-SAFE© lessons may NOT be duplicated for any reason except for your classroom use.
- i-SAFE© lesson hand-outs may be printed for students ONLY for your current classroom use.

Duplication, sale, resale and any other form of unauthorized use of i-SAFE copyrighted materials is prohibited and, therefore, a violation of law.

(I understand and agree to above Terms of Use)

Agree and Print

Student assessments are an important component of i-SAFE. When beginning the i-SAFE program with these lessons, i-SAFE strongly encourages educators to administer the pre-assessment online at **http://auth.isafe.org/selftest/index.php**.

To verify a School ID#, login at **www.isafe.org**, go to the My Info page and select "Find your school ID."

Upon completing the i-SAFE lessons, please direct your students to take the online post-assessment. Assessment data can be used by your school/district as a reliable measurement of its Internet safety education policy.

i-SAFE Cyber Security Unit

Suggested Grade Level 8

Curricular guide with options for classes with or without computers

Overview

The Cyber Security lesson unit consists of four separate lessons combined into one unit. The unit can be completed as one longer lesson, or divided at the lesson component sections indicated into shorter lessons. Complete all these lessons to ensure all necessary information on cyber security is covered.

Unit Goals

Students will:

- develop an understanding of malicious code and proper e-mail protocol
- understand the necessity of using caution when opening e-mail to protect computer security
- understand the term peer-to-peer networking (P2P)
- understand the security risks associated with P2P networks
- share the knowledge about P2P networks and their security risks with others
- apply knowledge and concepts such as hacking, steganography, malicious code (i.e. viruses and worms), to information on cyber terrorism
- be able to identify and comprehend the utilization of the Internet in cyber terrorism and cyber warfare
- be able to identify and comprehend security prevention techniques
- read and understand the school action plan in regards to security threats
- inform others about cyber security issues

Enrichment Goal

i-SAFE enrichment activities are designed to 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**.

Enrichment Activity

Completion of this unit will prepare and guide learners to create a Public Service Announcement informing others about the 4 key prevention processes that will keep a computer secure.

Materials / Preparation

- online access to the i-SAFE assessments, if appropriate for this lesson
- copies of the reference pages for each student
- copies of the activity pages for each student
- optional: computer access for HTML activities
- student registration in mentor program at **www.isafe.org**
- optional: PowerPoint presentation for this lesson is available for use as a student guide

Pre Assessment

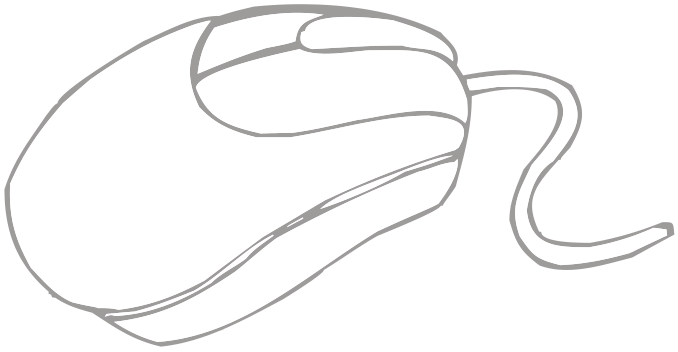
- If beginning the i-SAFE program with any lesson in this unit, administer the pre assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go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

Post Assessment

- If ending the i-SAFE program with any lesson in this unit, administer the post assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID".

Mentors

All students participating in the i-SAFE curriculum are considered i-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.



LESSON 1—Point of Attack: Malware

Learning Objectives

Students will develop an understanding the issues surrounding malware and secure e-mail protocol, and the necessity of enabling computer security functions to ensure computer security.

Activity 1

KEWL Chart Sections 1 and 2

Put the KEWL chart up on an overhead, or reproduce on a chart or board. This chart will guide discussion on malware such as viruses, worms, and Trojan horses. Teacher should initiate and lead discussion on these topics.

If the students are familiar with a KEWL chart (a chart in which you list what you Know, what you Want to learn, what you Learned, and how to Spread your knowledge), compare i-SAFE's "KEWL" chart with it. (KEWL is a popular term, meaning "cool" used in online communication.)

Section: K – What do you Know?

Begin by questioning the students on what they know about viruses, worms, and Trojan horses. List their appropriate answers in the K column of the chart. This column forms a foundation of what the students currently know about harmful viruses, worms, and Trojan horses. Most should be familiar with viruses and be able to give basic information.

Sample questions and answers:

Q. What is a computer virus?

A. A program that attacks your computer and causes problems.

Section: E – Expand your Knowledge

Question students on where their knowledge is lacking. What more do they feel they should know about viruses, worms, and Trojan horses to protect themselves and their computers?

Sample question and answer:

Q. What else would you like to learn about viruses, worms, and Trojan horses? Do we really understand how to prevent infection?

A. How can I prevent getting my computer "sick"? What are worms? What are Trojan horses? Why should I care?

Peer-to-Peer Activity

Once the first two columns of the KEWL chart are completed, students are ready to learn about computer viruses.

Choose one (1) of the following options: for classrooms with computers or for classrooms without computers, to accommodate different classroom environments.

With computers

If working in a computer lab or classroom with computers, allow students to access the overview activity on their computers. Students can work individually, in pairs, or in small groups. Allow your situation to dictate guidelines.

- You are authorized by i-SAFE to reproduce the files in any way appropriate for providing individual computer access in your learning environment, such as CD, disk, hard drive copies, or network availability.
- This activity walks students through the concepts of viruses, worms, and Trojan horses. It explains how these are spread and how to prevent infecting a computer. When finished with the lesson, students enter a scenario game. They are asked to choose how they would react to various situations.

Call for students to end the activity after 15-20 minutes and return to the KEWL chart.

Without computers

- Divide students into groups and pass out the Activity pages. Each group should receive activity pages which describe e-mail etiquette and virus terms, and the mock scenario activity page. Students are to read over the information; then, based on their new knowledge, each group should discuss each scenario and decide what they believe the correct action would be.
- Call for students to end the activity after 15-20 minutes and return to the KEWL chart.

Return to KEWL chart – Sections 3 & 4

Using what students have learned from their group work, they will finish the KEWL chart as a class.

Section: W – What have You Learned?

Now that students have covered viruses, worms, and Trojan horses, ask them what they have learned from their information pages and the scenarios. Check the "what you want to know" questions.

Sample question and answer:

Q. What do we know worms, viruses, and Trojan horses?

A. Viruses can be gained by downloading e-mail attachments. Worms affect computer networks. It isn't safe to download items on the Internet without proof —they can be Trojan horses.

Q. Name the 4 key prevention processes (in order) that will keep a computer secure:

A. 1. Use a firewall

2. Keep your operating system updated
3. Use anti-virus soft ware
4. Use Anti-spyware soft ware

**Make sure all key concepts presented and the critical attributes of viruses, worms, and Trojan horses are covered. Scenarios Answers: 1. a; 2. b; 3. b; 4. c; 5. b; 6. a (this is an illegal action)*

Section: L – Leading others in learning

This section allows students to identify ways to own the knowledge they have learned. By spreading knowledge to others, students continue their own learning. In this column allow students to brainstorm ways to spread knowledge. Informs students that they will be given the opportunity to lead others in learning a the conclusion of this unit.

Sample questions and answers:

Q. How can we spread what we have learned?

A. Talk to parents about what learned. Give presentations to others, design posters, incorporate peer-to-peer communication, etc.

Activity 2 - Crossword Puzzle

Pass out copies of the Crossword puzzle activity page. Have students complete the puzzle to review what they have learned. Work in pairs if desired.

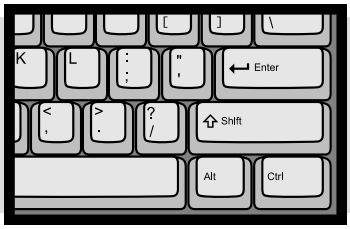
Concluding Discussion

- Review with students what malicious code is and the necessity for precautions when online.
- Discuss why it is important to discuss cyber security issues with others and how to be proactive in dealing with it.
- Review the 4 key steps to computer security.

KEWL Chart – Cyber Security

K Know	**E** Expand Knowledge	**W** What was Learned	**L** Lead Others in Learning

ACTIVITY—Scenarios



Directions

In your groups, read each scenario and decide which option you would choose. Think about why.

Explain why.

1. You receive an e-mail with the attachment fun.exe:
   a. Delete the message immediately
   b. Open the attachment
   c. Forward the message to all your friends.

2. You are out browsing Web sites, and one person's personal webpage has a simple game available to download.
   a. Download and play the game
   b. Keep looking—it could be a Trojan horse
   c. Tell all your friends about it.

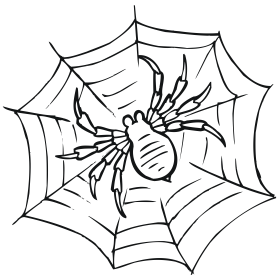
3. Your best friend told you he was sending you an attachment—you get the e-mail and you:
   a. Download the attachment
   b. Save the attachment to your computer and then open it
   c. Delete it.

4. A company sends you an irritating e-mail every day—you take the following action:
   a. Forward it to everyone in your mailbox so they will know what it feels like.
   b. Click on the "Take me off your list" link at the end of the e-mail—you've had enough!
   c. Report it to you Internet Service Provider

5. You like writing code and have come up with a clever one that forwards itself to everyone in the e-mail address book—and when opened says "I Win" you should:
   a. Send it to your friends, they'll get a laugh out of it.
   b. Forget about it
   c. Post it to your Web site for others to see.

6. A friend sent you a movie file he just downloaded from a P2P network. Before you open the file you should:
   a. Delete it
   b. Scan it with anti-virus software
   c. Burn it to CD

ACTIVITY—Don't Get Bit by the Bug



Crossword Vocabulary

Shift
Replicate
Reputable
Spam
Trojan horse
Virus
Worm
Malicious Code
Program
Exe
Vbs
Steganography
Hacking
Attachment

Across

2. This file extension stands for visual basic.
4. One common virus extension.
5. Written instructions in a computer language.
6. You should hold this key and delete to completely erase e-mail.
9. These are codes that claim to be one thing but do something else.
12. Sending out mass mailings.
13. This explains the purpose of a file.

Down

1. These harmful items use a computer network to spread.
2. A harmful program that piggybacks on others.
3. Games and software should only be downloaded from _____ companies.
7. This is a technology that allows people to embed or hide data inside of other files like documents (.doc), pictures (.gif, .bmp, .jpeg), or music files (.wav, .mpeg).
8. Programs written for a bad or destructive purpose.
10. The process of breaking into a computer or a network.
11. Trojan horses are unable to do this - unlike viruses or worms.

REFERENCE—Malicious Programs

Malware – Malware are programs, such as worms and viruses, that include malicious code—code written with the intent to harm, destroy, or annoy. "Code" is a term for the language(s) computer programs are written in—the "code" tells the computer what and how to do things. Malware can attach to e-mail and carry out their programming which can cause computers to work improperly.

A **Virus** is a computer program that spreads itself by infecting files. Viruses are dangerous and can shut your computer down. While there are many ways to get a virus, the most common is through downloading e-mail attachments.

- There are consequences for creating or spreading a virus. You can be prosecuted as a criminal.

Worms also include malicious code. Worms work through networks. They travel through shared files and programs and can bring down an entire system.

Trojan horses are another type of malicious code. These are programs that claim to do one thing but actually do another when downloaded. For example, you download a game but instead the program wipes out your hard drive.

Spyware A program running in the background to monitor your computer activities. Frequently downloaded without you knowing it, they can monitor your web browsing and cause pop-ups.

Prevention Tips

Here are some things you can do to keep your computer safe and keep it from being a threat to other computers:

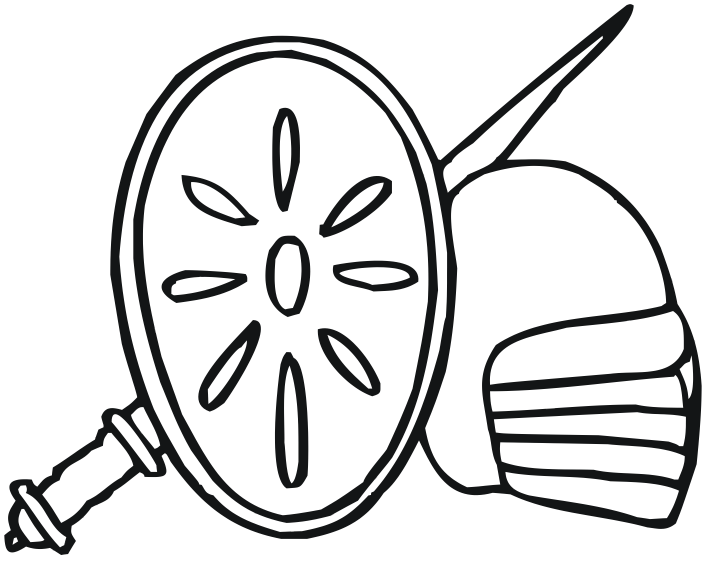
1. Make sure a firewall is installed on your computer. If you aren't sure, ask your parents. A firewall prevents information from entering your computer without your permission.

2. Keep your computer updated (download updates for your operating system regularly)

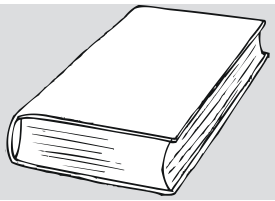
3. Install anti-virus software on your computer, keep it updated, and most importantly—USE it.

4. Install anti-spyware software on your computer and run it periodically.

5. E-mail that has been forwarded "FW:" or has an attachment with the suffix of ".exe," ".scr," or ".vbs." should be considered a red flag for possible virus infection. If you do want to open an attachment, scan it through the virus software first. To do this, save all attachments before opening them.



REFERENCE—Other Terms to Know



Spim: Mass Instant Messages or to send out mass IMs (like spam in e-mail).

File extensions: A string of letters at the end of a file name that explain the purpose of a file. For example, hello. doc - .doc is the file extension. It explains the file is a document. .exe is an executable file – meaning it does something. SCR stands for script and .vbs stands for visual basic, which is a programming language.

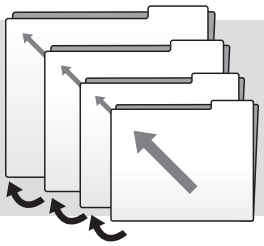
Attachment: Something is attached to the e-mail. It can be a document, a picture, or a program.

Steganography: This is also known as stego. This is a technology that allows people to embed or hide data inside of other files like documents (.doc), pictures (.gif, .bmp, .jpeg), or music files (.wav, .mpeg). The real message is hidden. It is believed that terrorists, drug traffickers, corporate raiders, and hackers use this way to communicate secretly. It is for this reason you shouldn't forward messages. You never know what the message really says and if it is altered, your name will be on it.

Hacking: The process of breaking into a computer or network. One example is that of a Boston teenager who hacked into the phone company's computer system and caused it to crash. This type of offense is criminal, AND YOU will be prosecuted!

Phishing: Using a business name without permission to send out an e-mail asking for personal information. Never respond to these type e-mails. They will typically use the information for illegal purposes. They are "fishing" for a victim—thus the term phishing.

LESSON 2—Security Risks of P2P File Sharing



Learning Objectives

Students will:

- understand the term peer-to-peer networking (P2P)
- understand the security risks associated with P2P networks
- share the knowledge about P2P networks and their security risks with others

Discussion

Guide a brief introductory discussion about peer-to-peer (P2P) networks.

- Ask students if they have ever heard of or used peer-to-peer networks. Some examples of "former" networks include Napster, Blubster, and Grokster.
- Ask students who have used these networks what they are commonly used for (common uses: downloading illegal music, movies, software, etc.)?
- Ask students to define the term peer-to-peer networks. Have students think about what the name means in relation to how computers interact with others. (Typically users download software from a P2P site, which creates a shared folder on the hard-drive that can be accessed by any other member of the network. That means anybody, in any country, anywhere in the world, who has a computer and Internet access, can access the computer in your home and make illegal unauthorized copies of the music and anything else contained in that location, thus the peer-to-peer name). The software program simply allows the user to search and find a particular computer with which to connect.
- Ask students to brainstorm potential security risks associated with using peer-to-peer networks

Reference

Pass out a copy of the "P2P Security Risks" page to each student or place information on a board or overhead. Go over the page together and discuss the following:

- Ask students if they have ever downloaded anything (games, papers, music, software, etc) from a Web site or peer-to-peer network.
- Ask students if they read the disclosures before downloading P2P software.
- Ask students what type of security protections P2P networks have.
- Explain, P2P networks open a computer to many different security risks.

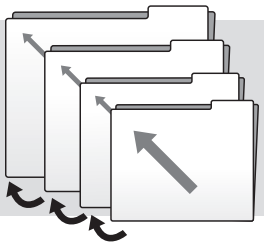
Activity

- Break students into small groups.
- Have them develop a top ten list of security risks associated with P2P networks.
- Meet back as a large group and discuss the lists.
- Discuss possible ways to prevent or safeguard against the risks of using P2P.
- Ask for examples from students of ways, if any, that they already deal with spyware or malicious code.

Review

Review the 4 key steps for computer security and have students tell how this applies to P2P networks.

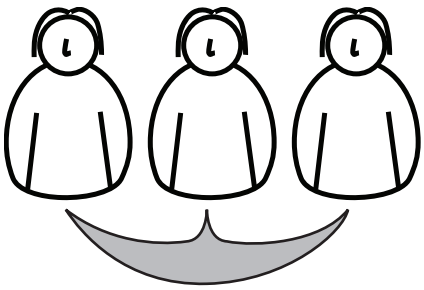
REFERENCE—Understanding Peer-to-Peer Networking



Downloading music from the Internet became popular when millions first used Napster to download their favorite songs rather than trekking to a store to buy the CD. Although Napster has now transitioned to a legal download service, most peer-to-peer (P2P) networks are primarily used to illegally download music, movies, and software.

So just what is P2P networking? P2P software running on individual machines allows computers to communicate directly with one another rather than through a central server such as hosted through a Web site. With P2P software you can allow anyone in the world to copy files directly from your own computer. This could be a single file, a whole folder, or even your entire hard drive.

Unknowingly, you may be sharing more than you think or would ever want to.



Like an Internet search engine, P2P software allows a user to type in a search term. The search will pull up files that use that term from any computer currently connected to the Internet running the same P2P software. You can then select the files you want to download; you could be downloading files from a computer in China, or nearly anywhere in the world.

While P2P is legal and can be fun to use, there are definite dangers associated with it. For one thing everything offered via P2P may NOT be legal. File-sharing over P2P networks also puts the user at risk for contracting a computer virus that's attached to one of the transferred files. Spyware is a serious concern in the P2P environment. Many P2P networks auto install spyware on your machine—you won't even know it's there.

Peer to Peer: Know the Malicious Code Dangers

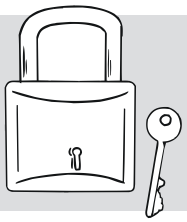
- **Viruses**—when downloading a shared file, there is the danger of downloading a computer virus or Trojan horse onto your computer. These viruses can cause all kinds of problems, such as erasing all the files on the hard drive or the automatic sending of pornographic e-mails to all of your friends in your mail directory. The worst part is that virus protection software works on the Internet and e-mail, but doesn't protect you while you run P2P software.
- **Spyware**—many of the P2P programs automatically install spyware on your computer as part of the installation process. These spyware programs can range from a simple nuisance to a true invasion of privacy. They can cause numerous pop-up ads and banners to appear, or install tracking programs that view your usage patterns, and more. If you notice that you are getting numerous annoying pop-up messages, the odds are that you may have a P2P filesharing program installed on your computer.

Spyware: Are You Aware?

Most illegal P2P networking software now comes entangled with all types of spyware and adware. To download a P2P program you must automatically accept the inclusion of this other "software." In addition, removal of spyware or adware often causes the P2P software to stop working. So what is the big deal about a little spyware or adware?

1. You are being spied on. The spyware and adware snoop on your behavior and transmit information over the Internet to third parties. This can include private data such as your computer's IP address and credit card numbers.
2. Spyware and adware cause your system or network to run slower. The constant transferring of information uses up bandwidth and computer resources.
3. It's annoying. Spyware and adware can cause frequent pop-up ads and other annoying hassles while online or surfing the Internet.

LESSON 3—Homeland Security



Learning Objectives

Students will:

- apply knowledge and concepts such as hacking, steganography, malicious code (i.e., viruses and worms), to information on cyber terrorism
- be able to identify and comprehend the utilization of the Internet in cyber terrorism and cyber warfare
- be able to identify and comprehend security prevention techniques

Discussion 1

- Review with students the idea that the Internet is a cyber community. Discuss some of the ways community rules can be broken or abused.
- Ask students to think of events (terrorism events) that have threatened or succeeded to create harm or destruction, that have happened in and to the United States such as September 11, the War on Terrorism, etc.
- Ask students if the Internet could be utilized as a potential weapon either by terrorists or other governments?
- Introduce the concepts of cyber terrorism:
  > The execution of a surprise attack by a sub-national foreign terrorist group, or individuals with a domestic political agenda, using computer technology and the Internet to cripple or disable a nation's electronic and physical infrastructure. Also to be considered is a physical attack aimed at the Cyber infrastructure that would also result in down time. Either way the goal is to increase panic, fear and confusion.
- Introduce the concept of cyber warfare:
  > The use of computers and other devices to attack an enemy's information systems as opposed to an enemy's armies or factories.
- Discuss how concepts such as hacking, steganography, malicious code (i.e., viruses and worms) have an impact on cyber terrorism or cyber warfare.
- Cover all relevant vocabulary and issues pertaining to each. Option—write on the board or have the students write down the definitions of the following terms.
  > Terrorism: The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons.
  > Cyber Community: a group of people connected through online interaction.
  > Infrastructure: The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons.
  > Target Hardening: Making targets more resistant to attack or more difficult to remove or damage.
  > Briefly discuss how protecting a cyber target from terrorism is like protecting a physical target like a power plant or a water treatment plant. What are the differences?
- Discuss how student participation in developing cyber security strategies is in effect participation in Cyber Target Hardening.
- Discuss how the infrastructure of the United States is largely reliant on computers to work effectively and the possible consequences to the infrastructure of a cyber attack.

Peer-to-Peer Activity 

Select an option: With Computers or Without Computers.

With Computers

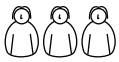
- Students should access a the HTML activity. This activity should be completed in groups as a webquest. You don't need the Internet to access this activity. After extracting the files to a folder on your computer, the activity will be locally available. Open the HTML activity folder and start activity with the "Open Activity" file.

  > You are authorized by i-SAFE to reproduce the files in any way appropriate for providing individual computer access in your learning environment, such as CD, disk, hard drive copies, or network availability.

- The first page of the activity provides an introduction to the webquest and its goals. Students will learn more about cyber warfare/terrorism by conducting a quest using the i-SAFE provided webpages. In the second part of the quest, each group is to come up with three guidelines that can be used to combat cyber terrorism by students and others in the community.
- Students should work through the quest, process, resources, and conclusion section of the activity. When finished, they should access a word processing or publication soft ware to type up their information for presentation.
- Proceed to Peer-to-Peer Activity Extension.

Without Computers

- Divide students into groups of three. Hand them the Activity Sheet with directions and goal orientation of the activity.
- Students should choose their job role and divide up tasks.
- Students will then conduct the quest using activity pages provided on the topic they select.
- Students will meet back in groups to share information learned and design their presentation. Part of the presentation is coming up with three guidelines that can be used to combat cyber terrorism by students and others in the community.
- Proceed to Peer-to-Peer Activity Extension

Peer-to-Peer Activity Extension 

- The groups should present the information they learned during the quest to the class.
- Have students discuss what they read and learned from the activity. Refer back to the concepts in the beginning discussion.
- Discuss each group's guidelines, and as a class, come up with five guidelines that can be used to combat cyber terrorism by students and others in the community.
- Reinforce the concept that by participating in cyber security, students are an active part of homeland security.

REFERENCE 1—What's in a Definition?

Okay, Mateys, let's see if we can define cyber terrorism. Don't just skim this article though! I'd read carefully if I were you. This article has lots of definitions for it, and you have to decide for yourself what the correct one is. Pay close attention—some articles have answers to more than one question.

At first glance, the term cyber terrorism seems easy to define. After all you and I are familiar with the Internet and you also have an idea of what terrorism is. You've lived through September 11. However, while you might know what cyber means and what terrorism means when put together it is much more difficult to define. The old saying "One man's terrorist is another man's freedom fighter" shows that defining terrorism is very subjective. That means what one person thinks is a terrorist may be another person's hero.

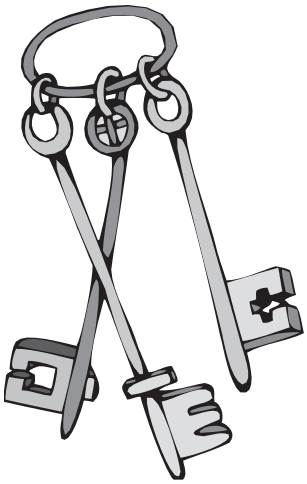
When one realizes how unclear the definition of terrorist is, one can see why this could get even more confusing in the cyber world. If one uses the most broad definition of terrorism: "the calculated use of violence (or threat of violence) against civilians in order to attain goals that are political or religious or ideological in nature; this is done through intimidation or coercion or instilling fear," and applies this definition to the cyber community, a wide range of activities can now be concluded to be cyber terrorist acts.

Here, let me explain better: Is an e-mail bomb an example of activism or cyber terrorism? What if the e-mail bomb was written by a 17-year-old-college student who was trying to state his political views. This action caused intimidation, coercion, etc and was used to attain goals that are political in nature. However, not many people would consider a 17-year-old a terrorist. Now think about this: if an Al Qaida member conducted it, this same action would take on new meaning because of the history or the group and previous terrorist activities.

Let's take a look at how some other people defined cyber terrorism. Read these carefully. Each one is a little different. Is there one you agree with?

- Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term cyber terrorism, defined cyber-terrorism as the convergence of cybernetics and terrorism.
- Mark Pollitt, special agent for the FBI, offers a working definition: "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents." This version of definition was offered by a police chief: "Cyber-terrorism – attacking sabotage-prone targets by computer—poses potentially disastrous consequences for our incredibly computer-dependent society."
- The media often use the term cyber-terrorism in a different manner altogether: "Canadian boy admits cyber terrorism of his family: Emeryville, Ontario (Reuter)—A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday."
- A renowned expert Dorothy Denning defined cyber terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives." R. Stark from the SMS University defines cyber-terrorism as "any attack against an information function, regardless of the means."

Wow—those definitions are very different from one another! According to them, any computer attack from site defacing to computer pranks can be considered cyber terrorism. However, such broad definitions do not adequately address the true idea of cyber terrorism and don't show a difference between cyber crime and terrorism. Instead the simple definition of cyber terrorism can be the *use of information technology and means by terrorist groups and agents*—with an understanding that terrorist groups and agents are those who have been identified as such through traditional definitions of terrorism.



Finally, a suggestion can be made that instead of the broad indefinable term cyber terrorism, one can use the term information warfare. This takes into account both legitimate and terrorist organizations using the cyber scene to conduct war. I hope you got all that! It can be confusing but it is important to understand what cyber terrorism is in order to prevent attacks. Now take your answer back to your group—hopefully you've found one answer to your scavenger quest and are that much closer to your treasure!

REFERENCE 2—New Frontiers for Terrorists

Aye, Mateys. I've been known as the terror of the open sea! Ye be trying to find my treasure I know. Well, I'll aid ye a little. Read this entire article carefully or ye may miss something important. I'll not be telling the answers though—those you'll have to find for yourself.

The computer has become a powerful tool for use by anyone. The Internet has opened new boundaries and frontiers. Communication, expression of ideas, information, all are available nearly instantaneously. However, as you can imagine, such a powerful tool can be used for bad things too. Computers can be vulnerable to viruses, worms, Trojans, hacking, etc. As Americans rely more and more on computers the possibilities and opportunities for abuse abound.

In this day and age computers are vulnerable to terrorism as well. Cyber terrorism can occur in many ways. Terrorists can use the computer as a tool, a place for evidence, or as a target for attack. With such opportunities available how will the United States prepare?

When online it is easy to see one manner in which computers are being utilized by terrorists. Web sites abound with propaganda for each and every cause. These Web sites attempt to spread their messages, raise funds, and target attacks or resistance movements against governments. Where once such groups would have encountered open opposition, restrictions, etc, now they have an open forum for spreading their word and seeking support.

Terrorists also utilize the Internet in many of the same ways any other person would– for information gathering. With so much info available at the click of a few buttons, the Internet has made intelligence gathering a simpler process. Additionally, by using hacking techniques, sensitive, classified, and other government data becomes available. With this type of information, planning and performing terrorist attacks is made easier.

Finally, computers can be used by terrorists as a point of attack. This is perhaps the most frightening of all scenarios. With so many people so dependent on computers and Internet, such an attack could be crippling. Think about it: computers are used at banks, to run phone systems, to route 911 calls, to guide computers, in hospitals, etc. Such attacks on computers can be made in many ways. One could hack into a system and remove, alter, or destroy data. Such interference could result in denial of service, outages, or other widespread downtime. Another attack format could be to flood the system with e-mails, greatly slowing down service or causing the system to crash so legitimate users cannot access the system. By similar means viruses, worms, or Trojans can be launched to create large-scale destruction and down time. We have only to use our imaginations to see how the Internet could be used as a tool by terrorists.

But has the Internet actually been used in such a manner by terrorists? One can find stories online of items where credit has been given to terrorists or subversive groups.

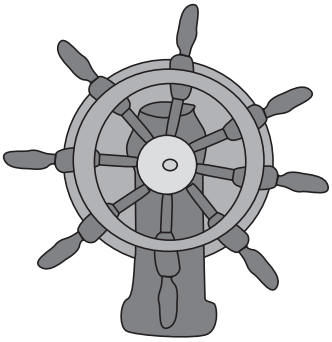
For example, the use of the computer as a tool can be seen by the Tamil Tiger terrorists. They hacked into Sheffield University in England in 1997 for propaganda and fund raising. They utilized legitimate user Ids and passwords of some of the academics in the university and sent e-mails under this cover around the world asking for donations to a charity in Sri Lanka. Successful utilization of the computer for this type of undercover propaganda and fund raising effort has proved to be successful. In addition, recent denial of service attacks on eBay, Yahoo, and CNN have been suggested to be the work of terrorists although this cannot be confirmed.

In this day and age, terrorists have the tools and means to launch cyber attacks and utilize the computer as a tool in their schemes. One only wonders when an attack will occur.

REFERENCE 3—Cyber Security and You

Alright now! It's time to take the wheel and set sail to see how we can help. What steps can you and I take to protect against a cyber attack? Read on and let's find out. Read all carefully though—there is lots of info here.

Do you know that you can do your part to protect your country? Protection against a cyber terrorist attack begins at home. Ensuring that your personal computer is secure could play a crucial role in protecting the national Internet infrastructure. Attacks of all kinds can take advantage of home computers. Denial of service, virus and worms, all make use of the home computer and can cause untold damage and downtime nationally. However, by taking a few simple steps average home computer users (meaning you) can have safe, protected computers and do their part to protect the United States.



First and foremost—use virus protection software. More importantly, update the software periodically. This will help protect your computer against viruses. Without frequent updates you leave your computer vulnerable—new viruses emerge at an alarming rate and old software offers no protection for a new virus.

Second—use some common sense when dealing with e-mail. The easy rule to follow is don't open e-mail if you don't know who it is from. Special care should be taken when dealing with attachments. With attachments, it is best to (1) know the person sending the message, and (2) to be expecting it. Suspicious e-mails should always be deleted or questioned further. Other dangerous e-mails could contain hyperlinks. These should also be treated with extreme caution. Remember—it's better to delete if you aren't sure!

The third way to protect your computer is to carefully choose passwords. Choosing passwords that are difficult to guess makes it more difficult for terrorist infiltration or utilization of accounts. Another good idea is to use separate passwords for various accounts so that if one is discovered, the other accounts won't be compromised. When making a password, make sure it has at least 8 characters—both numbers and letters. Also, keep it meaningless: not a word, date, etc.; for example Tmp2Ab78. This ensures that computer programs are unable to easily crack the code. Finally, ensure that passwords are secure by regularly changing them and by never giving them out to others.

Another important protection measure is a firewall. A firewall acts as a wall between your computer and the outside world. You can utilize a software firewall for a personal computer or a hardware firewall if protecting many computers. Firewalls work by filtering material from the Internet. Good material is allowed access while potentially dangerous material is denied. This keeps outside sources out of your computer and provides a higher level of protection against hackers.

Understanding the risks of file sharing is also important. Many times computers link to share files, music, movies, etc. However, when open to sharing, your computer is also open to attack. Thus it is best to turn off file sharing and only utilize it when absolutely necessary. This will ensure that you don't invite strangers unknowingly into your computer. A sixth safety measure is to disconnect from the Internet when not in use. When connected to the Internet, the connection not only allows you out to explore it allows others in and opens your computer to hackers, viruses, etc. By simply disconnecting, you remain protected when not utilizing the computer.

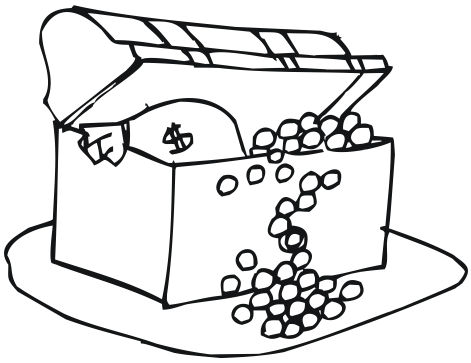
Updating computer patches is another important security measure. Software companies periodically release updates and patches when bugs or operating errors are discovered. These bugs could pose as a weak point or a way to enter; however, patches and updates fix these problems. Often you can set your computer up to download and install patches periodically if you forget to check.

Finally make sure that others using your personal computer understand how to protect it. A weak link can result in infection, hacking, or other security breach.

By following these security measures, you not only protect your personal computer, but also the Internet infrastructure. Like a chain, removing a link weakens the overall length. By removing your computer from future attacks, you weaken the attack overall. Play your part in fighting cyber terrorism with these simple steps.

Now take what you've learned back to your group and share! You've learned another important part of the knowledge and are closer to the treasure then ever before.

REFERENCE 4—A Nation's Response



Now you know what cyber terrorism is, how it can occur and how you can help prevent it. It's time to take a look at what the government is doing to protect you. Learn all and share with your group to complete your quest successfully.

The government has taken many steps to protect our country against future terrorist attacks. At airports there is extra security. News stations monitor our safety status. However, what have they done to protect our computers from a cyber attack? The government protection plan takes several different formats, and extends beyond just prevention to proactive strategies for minimizing damage from cyber attacks.

The first area the government is concentrating on enhancing is raising the security level in order to ensure prevention of damage. This includes taking a risk measurement to see what areas are weak and working to enforce those areas.

Critical areas such as government computers, critical response systems like 911, etc. will be checked and double-checked to continually raise the security level of each. This might mean upgrading firewall protection, virus software, etc.

Another area targeted for improvement by the government to prevent the success of cyber terrorism is the communication between the government and private sector. The private sector has resources and people to aid the government in prevention, responses, and basic sharing of information. Together the government and private sector can also make information available to the public to prevent attacks.

The private sector will also be incorporated into response scenarios. As the government determines how best to handle cyber terrorism scenarios, the private sector will be consulted and included. This will help strengthen the response capabilities of both as they cooperate to prevent foreseen dangers and deal with unforeseen ones. In addition to these efforts, the government will work to establish the basics of information security. They will train personnel, conduct research and development, survey application, etc. Perhaps most importantly, laws and regulations will be developed as a countermeasure to cyber terrorism. These will enable prosecution of those within the United States and aid in prevention overall.

Finally, the United States government will develop international contacts and cooperation. Since it is assumed many cyber attacks will occur across national borders, it is understood that international cooperation will be needed to prevent, apprehend, and prosecute the criminals.

All of these measures are important but the government understands that protection needs to occur first with the people and their personal computers. It has set up a National Cyber Alert System with tips targeted at aiding the home and corporate user and geared toward instruction on security. The Alert System also has Security Bulletins targeted toward technical audiences, which outline security issues, vulnerabilities, potential impact, patches, and ways to work around to mitigate risks.

Finally the new Security System includes Security Alerts, which provide real-time information on security issues so people know what is going on, and the risks currently available. Its amazing the many levels the government is working at to prevent attacks on our computer system. Take this information back to your group and share! You're on your way to claiming the ultimate treasure of full knowledge.

ACTIVITY—Seek and You Shall Find

Directions:

You and your mates will be on a scavenger quest not for treasure but for priceless knowledge. Plan wisely how you will divide up tasks—will one read, one write, one present? Or perhaps each take a question and divide up the articles? It's your choice but choose wisely—there is a time limit and a goal. But remember the pirate's advice—no answer is ever completely correct—you'll have choices in your answers. Think and discuss what you have seen and read. Then use your brains, Mateys, to come up with your own answers. You'll have to discuss what you've seen, read, and answered so be PREPARED!!

The Treasure List:

1. Provide a definition of Cyber Terrorism.

2. What are three ways a Terrorist might use a computer?

3. What is one example of a terrorist attack using a computer?

4. What steps are being taken by the U.S. Government to protect the nation from cyber terrorist attacks?

5. How might an American citizen unknowingly aid a cyber terrorist in their efforts to do harm?

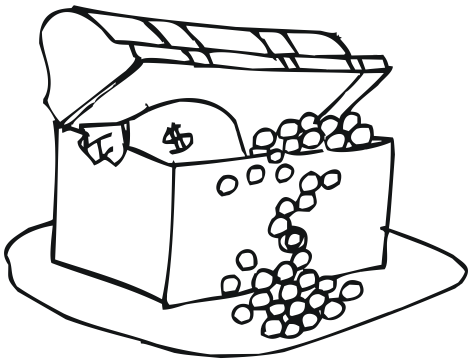
6. What steps can we take to protect our nation's computer infrastructure?

Design Guidelines

Ok! Now that you've found the treasure, it's time to utilize that knowledge. As a group come up with three guidelines which can be used to combat cyber terrorism by you and others in the community. Think carefully and creatively.
Later you will share these with your classmates and make a class list.

1. _____
2. _____
3. _____

Don't forget to discuss your answers with your group mates! Make sure you understand them and can discuss them with the rest of the class.



LESSON 4—National Student Watch

Learning Objectives

Students will develop a comprehensive understanding of their schools action or disaster plan in response to homeland security threats, and the means of relaying information concerning threats.

Introduction

Instructor information: In this day and age, students are often the best defense against any attack, from a student or a terrorist, occurring. They are aware when a fellow student is planning something. They know their environment and when a suspicious package suddenly shows up. They are the ones in the chatrooms who might catch wind of something.

So why not include them in the planning, educate them on the dangers, and watch, as they become a part of Homeland Security.

For more information on this critical topic, please visit: **www.ed.gov/emergencyplan/**

This is a government maintained site with information on developing an action plan, guidelines for action plans, and preventative measures to be put in place.

Materials

Student copies of the school's disaster action plan

Lesson Introduction

Read the introductory story to the class.

- Have students take time to think about some of the items mentioned in it.
- Open a discussion about the story.

Discussion 1

Engage the learners in a brief discussion in which they define the terms Homeland Security and identify, explain, and analyze the dangers involved to schools. Guide the discussion to cover the following:

- What was the introductory story about?
- What are terrorists? Why might schools be a target?
- What is Homeland Security? Why should we as students be concerned?
- How can schools be made safer places for students?
- What is a school action plan? Does my school have an action plan?
- What are some items in a good action plan?
- As students how can we be a line of defense in keeping our school safe?

  > Do we often hear things online, in chats, IMs, on Web sites, etc that should be relayed to officials?

Create student groups of 3 or 4 to complete the following project.

Activity

Hand out a copy of the school's action plan to each group.

- Students are to read through the action plan and familiarize themselves with it.
- In groups, the students should discuss the action plan and brainstorm any areas of weakness.
- Chart the plans strengths and weaknesses.
- Proceed to Discussion 2.

Discussion 2

Provide time for each student group to present their strengths and weaknesses chart, and discuss. Each group should briefly include the following during the presentation:

- Share their charts.
- Discuss what they learned from the assignment.

Ask students what other ways they can prepare and ensure their school is safe.

- What should they do/who should they contact if their hear rumors, spot something unsafe, etc.

Unit Enrichment Activity

Discussion

- Discuss why it is important to discuss cyber security issues with others and how to be proactive in dealing with it.
- Ask students who they think would benefit from this information and why.

Activity
Create Public Service Announcement (PSA)

- Allow students to meet back in their small groups. (Groups of 2-3 may work best. Or have students work individually)
- Hand out the activity page to students.
- Have each student group develop a Public Service Announcement informing others about the 4 key steps for computer security (They may wish to research additional information on installing firewalls, etc. for this activity).

Broadcast

- Share PSAs among class.
- Discuss ways to broadcast the PSAs outside the classroom.

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

Additional lessons and support for students to go peer-to-peer on Internet safety topics are available through **www.isafe.org**.

Documentation

- Please submit photographs of students who create exceptional youth empowerment projects, for special recognition from i-SAFE. Photographs must be accompanied by corresponding personal release forms.
- We'd like to hear from you! Send an e-mail to **teachers@isafe.org** to share any unique ideas and/or experiences you had during implementation of this lesson.

Post Assessment

- If ending the i-SAFE program with any lesson in this unit, administer the post assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID".

Public Service Announcements – PSA

Grab people's attention and educate them at the same time!

Your Goal

Explore the safety issues involved with cyber security and develop a public service announcement to educate others about the risks of, and legal alternatives to, piracy.
The PSA can be audio, video, or live. Part of the project is locating a broadcast medium.

Materials/Preparation

- background knowledge on cyber security terminology and issues
- computer with Internet access (recommended)
- materials of choice for developing PSA (video, audio, etc.)
- obtain cooperation with school media outlet, radio, TV, or other broadcast medium

Issues

Take a minute and think about the following before you decide how to present your information.

- How can Internet Safety PSAs be of service to others?
- What information do you consider "critical" when it comes to information about security?
- Who is this information "critical" for?
- How can you grab people's attention and make them listen to your important message?
- Based on what you know about the issues, what information will be most beneficial?

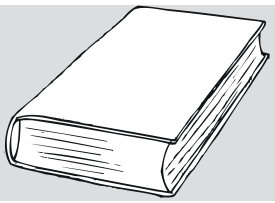
Preparation

1. Find a Media Outlet – will it be at your school or in the larger community?
2. Brainstorm—where can PSAs be played in your school or in your city?
   - Some possibilities: over the school PA system, at assemblies, over the radio, on a local news station, over the PA at a baseball game. What new ones can you come up with?
3. If going outside of the school, contact the media outlets to develop a cooperative agreement for broadcasting the PSAs.
   - Contact the media outlet before preparing your PSA to get their specific requirements regarding length, format, etc.
   - Be prepared on your topic so you can "sell" them on the idea over the phone.

Develop and Deliver PSA

1. Based upon media outlet—select media type—audio, video, or live.
2. Write the script that pertains to your topic and presentation style (i.e. audio, video, etc.).
3. Record the PSA (unless doing it live).
4. Edit the PSA with original music and titles.
5. Provide PSA through the selected media outlet.
6. Let i-SAFE know about your success. E-mail **outreach@isafe.org**.

Cyber Security Review PowerPoint Lesson Guide



Materials

Computer access to view PowerPoint presentation

Pre Assessment—if beginning the i-SAFE program with this lesson

- 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. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID."

Learning Objectives

Students will:

- develop an understanding of malicious code and proper e-mail protocol
- understand the necessity of using caution when opening e-mail to protect computer security
- examine necessary components of an acceptable use policy (AUP)
- understand the security issues involved in using P2P file sharing
- understand the term spyware and the types of programs it applies to
- understand the security risks associated with downloading items online
- understand how personal information may be compromised via spyware
- identify how to be secure at school and follow AUP guidelines
- examine security risks of peer-to-peer networks
- be able to identify and comprehend security prevention techniques
- inform others about cyber security issues

Presentation Overview

This presentation of 27 slides provides information on cyber security and its associated issues, and enables specific student discussions. The format also provides easy integration of teacher-initiated discussions on any of the topic concepts.

The presentation reviews the following topics:

- malicious code
- viruses
- worms
- Trojan horses
- Spyware
- Prevention information
- Acceptable Use Policies
- Peer-to-peer network risks
- enrichment activity

Discussions

Slide 4 – What types of security threats are students familiar with? Ask them what they have seen and had experience with.

Slide 9 – How do you know if your computer is "infected" – students brainstorm how they are aware of security issues on their computer.

Slide 12 – Asks students to think about how their computer could get infected in the first place.

Slides 24-26 – Asks students to brainstorm about AUPs, why schools need them, why students need to understand more about them, what they should contain, etc.

Enrichment Activity

See detailed instructions in the unit overview and lesson plans for each grade level.

Post Assessment – if ending the i-SAFE program with this lesson

- If ending the i-SAFE program with this lesson, administer the post assessment online at **www.isafe.org** by clicking on the link, Assessments, prior to the lesson. Students will need to know the i-SAFE School ID# to obtain access.
- To verify School ID#, login at **www.isafe.org**, go to your "My Info" page and select "Find your school ID."