

---

# HOMELAND SECURITY

## i-SAFE Lesson Plan

Suggested Grade Levels – Grades 7-12

Lesson guide with options for classes with or without computers

### Learning Objectives

Learners will

- apply knowledge and concepts learned in previously, 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

### 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](http://www.isafe.org), including the i-Mentor Training Network videos.

Learners will then engage in an enrichment activity which involves creating their own webquests on homeland security

### Materials / Preparation

- Computer access for CD webpage activities
- A copy of reference pages for each student
- A copy of activity pages for each student
- Student registration in mentor program at [www.isafe.org](http://www.isafe.org)
- *Optional:* PowerPoint presentation for this lesson is available on the CD for use as a student guide.

### Pre Assessment

If beginning the i-SAFE program with this lesson, administer the pre assessment online at [www.isafe.org](http://www.isafe.org) by clicking on the link, Assessments, prior to the lesson. To verify School ID#, login at [isafe.org](http://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](http://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](mailto:outreach@isafe.org). Your students will then be enrolled to receive information about sharing internet safety with other students and will be registered to participate in contests to win prizes.*

---

## 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 learned in previous lesson 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 the HTML activity provided on the i-SAFE CD. This activity should be completed in groups as a webquest. Links are all located on CD so access to the Internet is not necessary. Allow students to discuss the webquest, select roles, and divide up jobs. Open the HTML activity folder and start activity with the "Open Activity" file.
  - You are authorized by i-SAFE America 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 software 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.

### **Concluding Discussion**

- Review with students the successful tips they have developed for homeland security and cyber security
- Discuss why it is important to discuss this issue with others outside of the classroom.
- Encourage students to make a difference in their school when it comes to issues such as Cyber Security and Homeland security by registering at [www.isafe.org](http://www.isafe.org) for additional activities, materials, and support concerning this and other issues.
- Lead into a discussion about the Enrichment Activity.

### **Enrichment Activity**

Youth who participate in activities to share what they have learned about Internet safety are more likely to practice safe habits online. Additional lessons and support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. [www.isafe.org](http://www.isafe.org).

The creation of fun student activities can help other others become aware of cyber security risks. Students can receive additional information, materials and support to complete this project on their own from [www.isafe.org](http://www.isafe.org), including a downloadable student toolkit. Direct students to the

---

Kids and Teens section (X-Block) at [www.isafe.org](http://www.isafe.org) to access the i-Mentor Training Network's free online training module videos.

Using the format from the lesson, students will engage in an activity that will create awareness about what they have learned by creating their own webquest on the topic of Cyber Security and Homeland Security, and providing it for other students to learn from. Options include:

- Other grade level
- Different school
- Different class
- Or have all classes working on this project trade projects with each other.

### **Post Assessment**

Administer the post assessment online at [www.isafe.org](http://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](http://isafe.org), go to the "My Info" page and select "Find your school ID".

### **Contact us**

- We'd like to hear from you! E-mail [teachers@isafe.org](mailto:teachers@isafe.org) to share any unique ideas and/or experiences you had during implementation of this lesson.
- Students who participate in enrichment activities may be eligible for i-SAFE's monthly Most Valuable Mentor award – let us know about deserving students.

### **References**

The following sites were used in the design of this lesson.

- <http://www.us-cert.gov>
- [http://www.vaonline.org/internet\\_terrorism.html](http://www.vaonline.org/internet_terrorism.html)

---

# 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 nations 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.



**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.**

1.

---

---

---

---

2.

---

---

---

---

3.

---

---

---

---

---

Reference 1



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

*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 ye'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. Websites abound with propaganda for each and every cause. These websites 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.

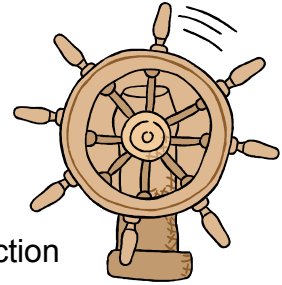
In this day and age, terrorists have the tools and means to launch cyber attacks and utilize the computer as a tool in their schemes. One only wonders when an attack will occur.

Well, I hope you learned quite a bit! It's easy to see how terrorists can use computers; we can only hope that they won't! Now share your answers with your group and know you are that much closer to the true treasure of knowledge.

---

Reference 3

Alrighty 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 than ever before.

---

Reference 4



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.