




## 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](http://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.

# LESSON PLAN—Cyber Security and E-mail

## Suggested grade level 2

### Goal

Students will engage in a group discussion moderated by the teacher, to gain a basic understanding of what a computer virus is, how a virus spreads, the damage a virus can cause, and virus prevention techniques. Throughout the lesson, students will complete activities in an activity mini-booklet to express their ideas and reinforce concepts introduced.

*Note: In the early elementary grades it is suggested that the lesson on Cyber Community Citizenship be completed before any other i-SAFE lessons.*

### Materials / Preparation

A copy of the mini-booklet (pre-folded and stapled) and crayons, markers, or pencil for each student

### Assessment (Grades K – 2)

Post-assessments should be completed after implementation of the final i-SAFE lesson. Assessment instructions and Student Assessment questionnaire are located in the curriculum folder.

If ending the i-SAFE program with this lesson, administer the post-assessment online at [www.isafe.org](http://www.isafe.org) by clicking on “Surveys/Assessments” after to the lesson, and selecting the appropriate link. To verify school ID number, log in at [www.isafe.org](http://www.isafe.org), go to the My Info page, and select “Find Your School ID.”

### Lesson Outline

**Discuss communication and computer viruses in the cyber community, by providing open-ended questions to prompt discussion. Include the following:**

- Review: What is Cyberspace, and how do we get there? (The community that you go to every time you log onto the Internet.)
- Discuss the word communicate. How do we communicate in the community we live in? (Talk face to face, phone, send letters, intercom)
- Discuss the word “virus” as it applies to making people sick. (Don’t feel well, can’t do the things you normally do, because your body doesn’t feel well enough to work properly.)
- Correlate being ill with a virus to a computer becoming infected with a computer virus. (Destroys programs, computer doesn’t work right, computer fails) Activity Booklet: page 1
- Explain that computers can get computer viruses from e-mails with attachments. Activity booklet: page 2
- Explain the best way to keep a computer from catching a virus. (Never open an e-mail from someone without checking with a parent or teacher first.) Activity booklet: page 3

### Lesson Plan with Example Dialogue

Implement the lesson by following the example dialogue, or use it as a guide to cover the concepts presented in your own words. **Note: After each question, provide time for student responses.**

“Today i-Buddy is going to help you learn about how computers can get sick from the Cyber community. We are also going to learn about how to keep our computers from getting sick. We’re ready to get started. Remember, we are going to learn and use some words that some of you may not know, so be sure to let me know if you don’t understand a word.”

“E-mail messaging is a great way to communicate with someone you and your parents know. An e-mail is a letter that is sent over the Internet. When you are thinking about staying safe on the Internet, you are also helping to keep your computer safe! You know a lot about computers already.”

“Today I’ve got another story about i-Buddy to tell you, and a new i-Buddy activity booklet for you to work on.”

“The title of this booklet is called “A New Kind of Virus”. Write your name on the cover, and listen to the story.”



The next day they had to have a computer repair man come to the house. He had bad news for i-Buddy's family. He said the computer had a **virus** that had **infected** the computer. i-Buddy just didn't understand. The computer repairman explained to him that his computer was very sick, and that made i-Buddy very sad. He asked, 'What made the computer sick?' That's when i-Buddy learned about viruses."

**Question:** “How can people catch a virus, and what happens when they do?”

- When someone coughs or sneezes on you, you can catch a virus from their germs.
- When a person catches, or becomes infected with, a virus, he or she becomes ill.
- When you have a virus you can't do the things you normally do, because your body doesn't feel well enough to work properly.

**Resume story:** “i-Buddy didn’t know what a computer virus was so the computer repair man told him about them. He said that a virus is a type of computer program. He explained that a computer program is what makes the computer do things, like the game i-Buddy was playing. The game was a good kind of computer program. A virus is a very bad kind of computer program. It makes the computer ‘sick’. It destroys good programs. Sometimes the computer even stops working just like i-Buddy’s did, or sometimes it just does strange things, like make good programs disappear or not work right.”

©2010 i-SAFE Inc.

**Resume story:** “i-Buddy found out from his computer repair man that one way a computer can get a virus is from something called an e-mail attachment.

**Question:** “Does anyone know what **attachment** means?” (*Something that goes along with or is connected to something else*) “E-mail attachments are pictures or programs that can come along with an e-mail. Email attachments are like pictures that you mail along with a letter you have written. It’s fun to look at pictures on the Internet, but you need to check with an adult before you open an e-mail attachment because sometimes strangers attach computer viruses to e-mails. Then they send them out to make people’s computers sick! The viruses hide in the e-mail attachment.”

“Look at the bottom of page 1 of your booklet. Let’s read it together: ‘A virus can also make a computer sick’. Draw in something that shows what can happen to a computer when it catches a virus.”

**Question:** “What do you think it means when I say, ‘the virus hides?’” (*You can’t see it*) “That’s right! When a virus hides in an e-mail attachment, you can’t see it! Then if you open that attachment by clicking on it, the virus comes out of its hiding place and makes your computer sick! We say the computer catches the virus, just like when you catch a cold. Look at page 2 of your booklets. Can someone read it for us? Right, it says, a virus can hide in \_\_\_\_\_. What word can you write to finish that sentence?” (e-mail)

**Question:** “What do you think about somebody who would send a hidden virus to another person’s computer in an e-mail? Would a good citizen do this?” (No) “Sending a computer virus on purpose is really just the same as trying to break a computer with a hammer!”

**Question:** “Do you think there are any laws against sending computer viruses on purpose? Yes, there are laws against it. A person can go to jail for making a virus and sending it to other people!”

**Question:** “Do you know how to keep viruses away from your computer?”

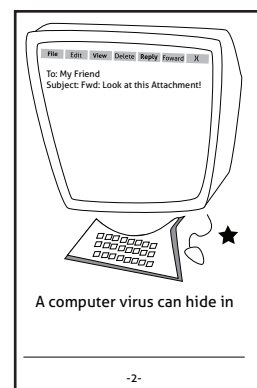
**Reinforce:** “The best way to keep your computer from catching a virus is to ask your parents or another adult to help you when you open up e-mail. And even when your parents do help you, don’t open up, or click on, an e-mail that has an attachment unless your parents were expecting to receive it. You can always use the phone to call the person who sent the e-mail, to make sure the attachment is safe before you open it. You will be a hero for your whole family if you prevent a virus from attacking your computer!”

**Question:** “What does the word prevent mean?” (Keep it or stop it from happening) “Read page 3, the back, of your booklets: ‘Be a hero! Prevent virus attacks!’ Draw a picture of yourself as a hero.”

**Conclude story:** “i-Buddy learned that the best way to make sure his computer doesn’t get sick is to never open an e-mail from someone he doesn’t know (a stranger), or an e-mail with an attachment. i-Buddy was so happy when his computer was finally fixed! Now he is very careful to remember what he learned about computer viruses. He wants all of his friends to know how to keep their computers healthy!”

### Review questions:

1. “What do we call something that can harm a computer or make it sick?”
2. “What can hide in an e-mail attachment?”
3. “What can happen to a computer that becomes infected with a virus?”
4. “What should you do if you receive an e-mail that has an attachment?”
5. “What is the best way to prevent computer viruses from infecting your computer?”



## **Empowerment in Action**

Tell the students that they now know a lot about computer viruses. Provide time to color the booklets. Tell the students to Go back to the cover and draw or write something that tells about what they have learned about computer viruses. Have the students take their booklets home to tell their families everything they learned today. Tell them their parents will be surprised at how Cyber smart they are.

## **Conclusion**

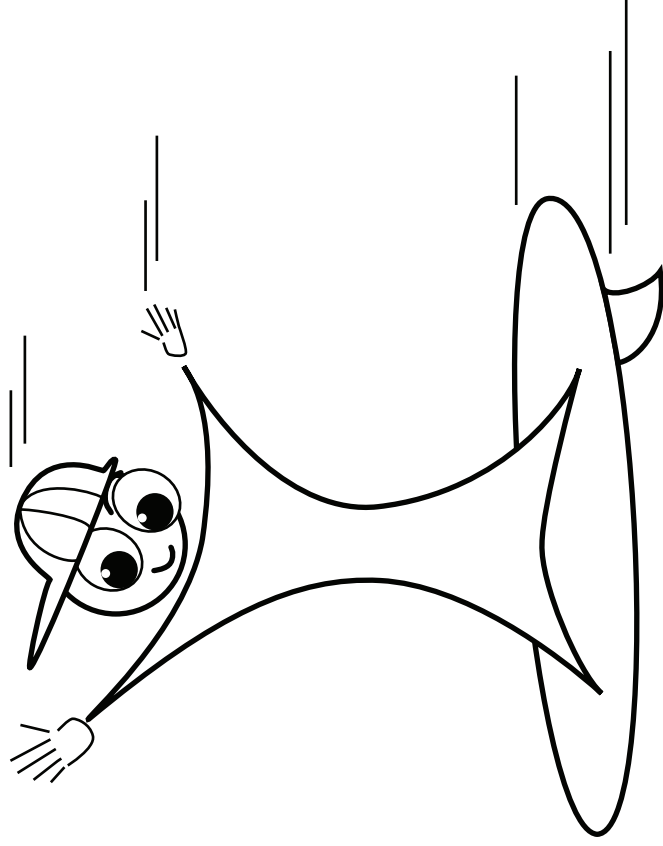
- Complete the Assessment activity if this is the last i-SAFE lesson to be implemented.
- Please submit photographs of students who create exceptional youth empowerment projects, for special recognition from i-SAFE. Photographs must be accompanied by corresponding personal release forms.

# LESSON ACTIVITY REPRODUCIBLES

## Instructions:

- Copy enough of the double-sided activity booklet pages for each student in the class.
- Assemble the pages using the page numbers as a guide, and fold along the center line.
- Staple the pages together to make a mini-booklet for each student.

Name: \_\_\_\_\_



**Be a hero!**  
**Prevent virus attacks!**

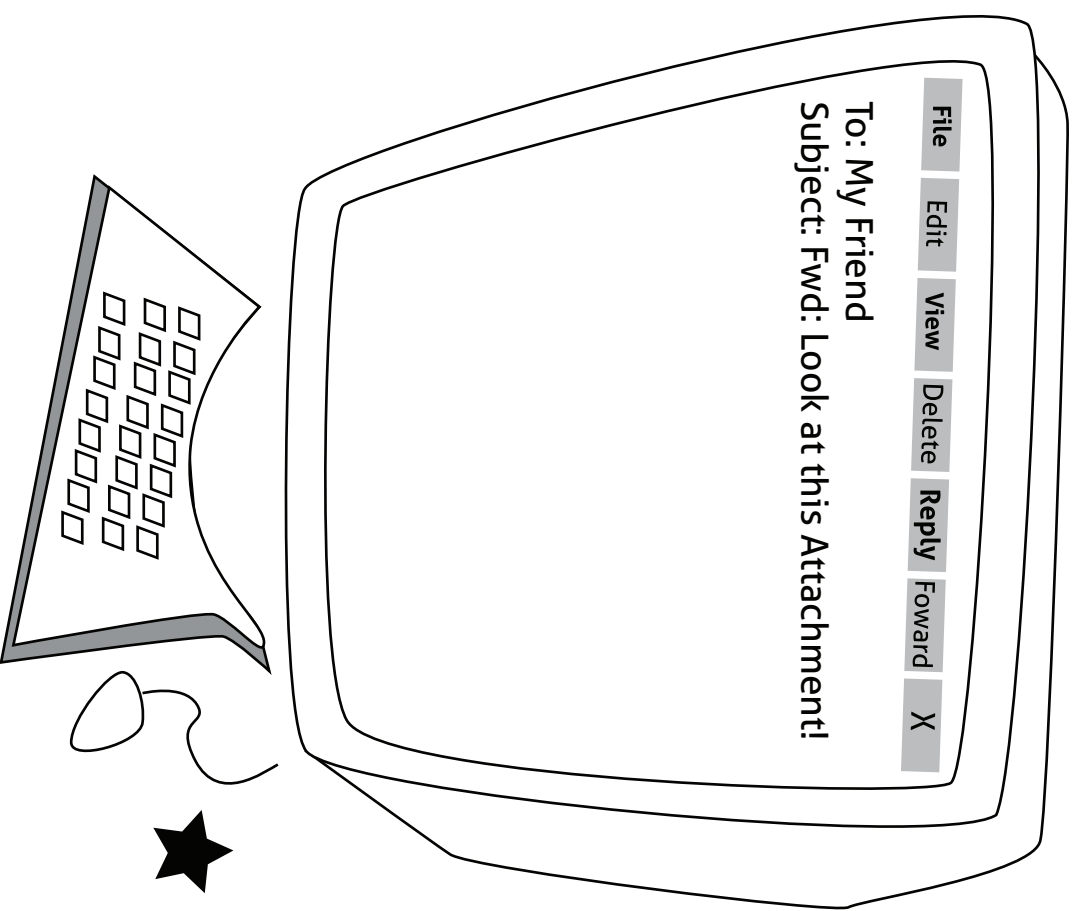
**i-Buddy Learns About  
A New Kind of Virus**

# When I have a virus, I feel

---

A virus can also make a  
computer sick!

-1-



A computer virus can hide in

-2-



# PARENT PAGE— Computer Security Action

## Malicious Code

### Introduction:

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, securely, make sure you know some basic maintenance skills and practice proactive prevention. Four essential elements must be addressed by PC users to keep their computers secure:

- firewall protection
- operating-system updates (Windows)
- malicious code
- spyware/adware

This action plan takes an in-depth look at malicious code and provides steps you can take to correctly maintain a secure computer and model good cyber-security behaviors for your children or students. Additional information about computer security is available at [www.isafe.org](http://www.isafe.org).

## Malicious Code

**Goal:** to be able to understand malicious code and the four steps to basic computer security protection

### Understanding It All:

1. **What:** Malicious code includes any programs (including macros and scripts) that are deliberately coded 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 malicious code that executes itself with the help of a user. 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, malicious code not only executes itself but attempts to make copies of itself from one place to another. For example: If your infected Word program attempts to access your e-mail account and e-mail itself to everyone on your address list, it is a worm.
  - **Trojan horse:** A Trojan horse cannot run on its own. It tricks the user into running the program by pretending 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.
2. **Why:** Malicious Code can be extremely harmful. Programs can change settings on the computer, delete files, slow down connection times, bog down e-mail, and more. One example is the ILOVEYOU worm/Trojan horse. It infected computers at more than half of the companies in the United States and even more in Europe. When it spread to a computer, it did two things: First, it overwrote files like jpegs (picture files would be overwritten with a copy of the worm so they could not be opened or recovered) on the hard drive. Second, 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 e-mail program, causing it also to bog down the Internet.

3. **When:** If not currently running virus-protection software, it is imperative that you obtain it. If running virus protection, make sure you update it frequently, as explained in the next step.

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