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 6

Curricular guide with options for classes with or without computers

Overview

The Cyber Security lesson unit consists of three 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.

PowerPoint Review Lesson – This option provides the key unit concepts in a PowerPoint presentation format.

Unit Content

- Cyber Security and E-mail Protocols
- Risks of Spyware
- Spam Scams
- Cyber Security Review PowerPoint Lesson – covers key concepts from this unit

Unit Goals

Students will

- develop an understanding of proper e-mail protocol, and the necessity of using caution when opening e-mail to protect computer security
- identify the terms "virus", "worm", and "Trojan horse" as types of malicious code
- understand how malicious code is spread in e-mail
- understand the term spam and how it relates to e-mail
- 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
- understand the security risks associated with opening spam in e-mail
- 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 poster campaign using slogans developed in the lessons to inform others about cyber security issues.

Unit 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
- computer access for HTML activities (optional)
- student registration in mentor program at **www.isafe.org**
- optional: PowerPoint access for review lesson

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—Cyber Security and E-mail Protocols

Learning Objectives

- develop an understanding of proper e-mail protocol, and the necessity of using caution when opening e-mail to protect computer security
- inform others about cyber security issues

Match-up Game

Play the "Match-up Game" to demonstrate the many types of malicious e-mail and allow students to become familiarized with the various vocabularies related to this lesson.

Copy the vocabulary words and sample e-mails from the activity pages.

Directions:

- Announce that you are going to play a short game about e-mail.
- Explain that they will be given time to go around and try to find their match. Have the students choose partners. Pass out either a vocabulary word or an e-mail letter to each student pair. (Please note–there are 8 vocabulary terms. In large classes, this may cause some students to have duplicate vocabulary words and duplicate letters.)
- Inform students they have 5 minutes to walk around and find their match. They are to match the correct e-mail term with the example of the term in the letter.
- Note: It is not expected that all students will find their match or that they will understand all the terms.
- Discuss with students: which ones are correctly matched and which ones are not. Lead into a discussion of vocabulary terms.

Discussion 1

Discuss the results of the game.

- Inform students that e-mail is a form of communication. However, it has its own set of rules. Some reasons for this are harmful things like computer viruses.
- Initiate a discussion on viruses.
- Ask students how many have ever had their computer crash because of a virus?
- Ask students if they know how viruses are spread?
- Discuss some of the viruses they may have heard of.
- Inform students that one common method of obtaining a virus is by downloading an attachment from e-mail.
- Ask students what their own experiences with e-mail have been. What common issues, annoyances, etc. have they run into?

Peer-to-Peer Activity

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

With Computers

If working in a computer lab, allow students to access the HTML 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.
- Proceed to the Group Activity.

Without Computers

- Divide students into groups and pass out the reference pages on e-mail safety and malware (computer viruses). Students are to read over the pages and discuss the information.
- Discuss each item such as flaming and spamming to ensure students comprehend. Encourage the students to share personal experiences with spam and flaming.
- Proceed to the Group Activity.

Group Activity 

- Divide students into groups of four or five.
- Direct the students to students to think about what they have learned. Using this knowledge, students are to develop a top five list of e-mail rules to follow. It is suggested they also come up with a simple slogan to reinforce the necessity of e-mail rules.

Group Presentations 

Provide time for the student groups to present their rules and slogans, and discuss. Each group should briefly include the following during the presentation:

- Share their e-mail safety rules, and explain why they are important to remember.
- Share their slogan on e-mail safety.
- Explain how their slogan expresses e-mail safety.

Enrichment Activity

Upon conclusion of the unit, students use the lists and/or slogans created in these lessons to develop posters or webpages to spread these messages to others.

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".

ACTIVITY 1

Directions: Copy and cut out enough e-mail letters and vocabulary words so that each pair of students has one copy of either type.

Answer key:

Letter A: Incorrect Forward

Letter B: Flame

Letter C: Virus Extension

Letter D: Picture Attachment

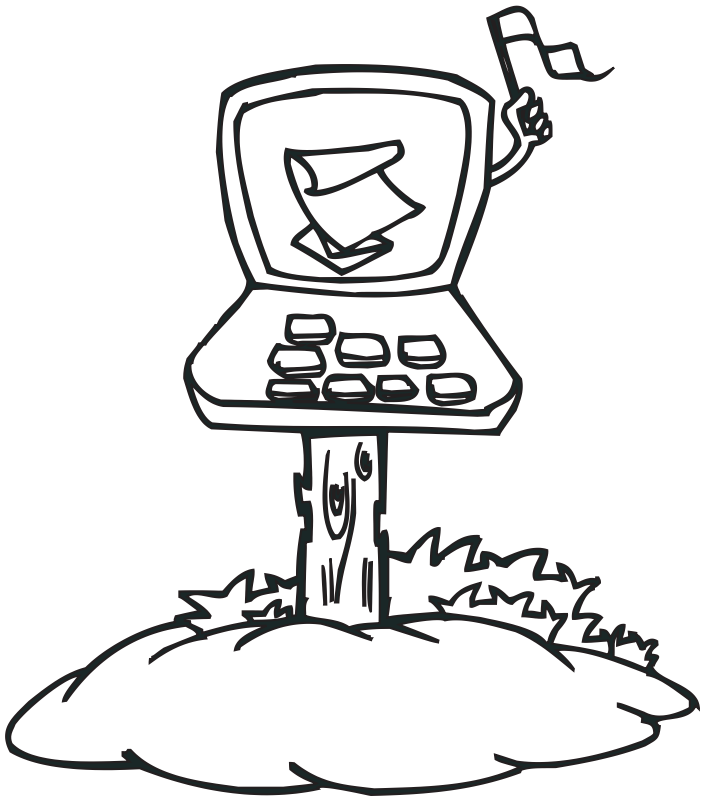
Letter E: Hoax

Letter F: Spam

Letter G: Reply

Letter H: Correct Forward

Vocabulary
Flame
Reply
Attachment
Virus Extension
Hoax
Spam
Correct Forward
Incorrect Forward



E-mail Letters

Letter A:

From: baseballpro@tampabay.rr.com
To: bigbog@yahoo.com
CC:
Subject: FW: Cool baseball trivia
Attachments:

Body:
Check out this cool site I got from a friend!
From: Ballplayer@aol.com
To: baseballpro@tampabay.rr.com; johnnyo@aol.com; devilraysfan@yahoo.com
Subject: Cool baseball trivia
Attachments:

Body:
Did you know that baseball has a rich history. You can find out more at this
Web site: http://www.crushquiz.com/trivia/directory/directory.asp?dir=Sports&dir2=Baseball

Letter B:

From: Jessicat@aol.com
To: Coolgirl@aol.com
CC:
Subject: Who do you think you are?
Attachments:

Body:
I can't believe you had the nerve to say hi to me after what you pulled off. JUST
WHO DO YOU THINK YOU ARE? Just you wait until I see you next time. I'd
Be afraid if I were you. I like that image – you always looking over your shoulder
Never knowing where I am. A person like you deserves fear.

-Your worst enemy

E-mail Letters

Letter C:

From: coolio@yahoo.com
To: jazzbeat@msn.com
CC:
Subject: Check out the cool game
Attachments: spybots.exe

Body:

This is a cool new game I just came up with. Download it and try it out.

- Coolio

Letter D:

From: Natedog@msn.com
To: havingfun@earthlink.net
CC:
Subject: Check out the picture
Attachments: goofy.gif

Hey –

Remember the party. Wait until you see how goofy you look eating your birthday

Cake. Check out the picture.

-Nate

E-mail Letters

Letter E:

From: justakid@aol.com
To: belindasmith@msn.com
CC:
Subject: Careful! Virus warning
Attachments:

Body:

Did you know that a very harmful virus has been circulating called the Black Death. It downloads and then thirty days later is causes your Computer to come up all black. You may already have it. Check your System files for lig.exe If it shows up erase it now. Please pass this on To your friends so they can protect their computers.

- A concerned net citizen

Letter F:

From: Junior@earthlink.net
To: whatsup@aol.com; barbiegirl@tampabay.rr.com; johnjohnson@msn.com; bayareaboy@aol.com
CC:
Subject: Pass this letter on
Attachments:

Body:

Hey guys – what's up. Pass this letter on to everyone you know so they know that

The mall is the place to hang out this weekend.

-Junior

E-mail Letters

Letter G:

From: bestfriend@yahoo.com
To: hanginout@aol.com
CC:
Subject: Reply
Attachments:

Body:

Hey girls what's up?
Well I'm not up to much of anything. How about you?
Are we still on for hanging out tomorrow night?
Yeah – my parents said I could go as long as I cleaned my room.

Catch you later
Your best friend

Letter H:

From: martianman@aol.com
To: martianman@aol.com
CC: happydays@yahoo.com
Subject: Baseball trivia -
Attachments:

Body:

I just got this site from a friend – check it out:

Body:

Did you know that baseball has a rich history? You can find out more at this Web site: http://www.crushquiz.com/trivia/directory/directory.asp?dir=Sports&dir2=Baseball

REFERENCE—E-mail Safety

E-mail is different than phone conversations, letters, or face-to-face meetings. These differences cause a new set of problems associated with this communication. Educate yourself on these e-mail no nos.

Flaming

Because e-mail is written and instantaneous, people find it easier to say things they might not otherwise say. Flaming is when you send a mean or hurtful e-mail. Flaming tends to happen frequently on the net because it's easy to write things without thinking them through. It's also easy to be misunderstood when writing e-mail messages, which can lead to a flame reply. Flaming can easily get out of control—if you get a flame message from someone, tell your parents or just delete it. Also, before you send an e-mail, think carefully about what you have said. Some things can be taken the wrong way—use emoticons to show people when you are joking.

Spamming

Spam is considered to be e-mail garbage. It is all that stuff you get and have to delete. Spamming is when you send junk mail such as jokes, hoaxes, urban legends, etc. to many people at once. You should never e-mail this type of stuff to people you do not know. And typically, even your friends don't want this stuff cluttering up their e-mail box.

Forwarding

E-mails should not be forwarded for several reasons.

1 – When you forward e-mail, you are giving out personal information such as the e-mail addresses of the person who sent it to you.

2 – Forwarding e-mail can also be considered spamming. Make sure the e-mail you send has a point. If you have to forward something—forward it to yourself and BCC: the people you want to also receive it. This gives them the body of the message without all the other personal information.

Hoaxes

There are a lot of stories, rumors, and urban legends circulating out there. Realize that not everything you receive in e-mail is true. Some examples are the e-mails that tell you to forward to ten friends and you'll receive money/gift certificates from a favorite store. Another harmful example is the e-mail that claims a virus may have been installed on your computer and you should delete a certain file.

Often this file is a necessary one for your computer. Make sure you delete these types of hoax e-mails and don't pass them on.

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:

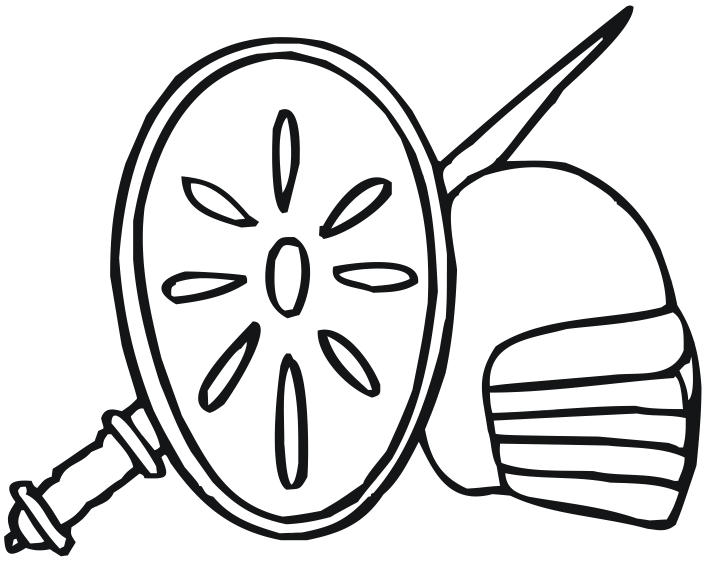
1. **Make sure a firewall is installed on your computer. If you aren't sure, ask your parents. A firewall prevents information from entering your computer without your permission.**

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

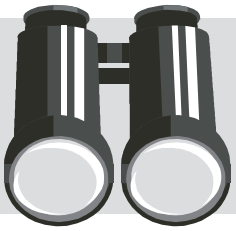
3. **Install anti-virus software on your computer, keep it updated, and most importantly—USE it.**

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.**



LESSON 2—Risks of Spyware



Learning Objectives

Students will:

- 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

Discussion

- Ask students if they have ever downloaded anything from online (games, papers, music, software, etc).
- Ask students if they have ever read a disclosure/privacy statement from an online Web site. Did they understand what they were reading?
- Ask students if they know the term spyware—and to self define it.

Activity

- Pass out the reference page.
- Break students into small groups.
- Have students read through the information and develop a list of types of Web sites that might install spyware on users' computers.
- Meet back as a large group and discuss the lists.
- Discuss possible ways to prevent or safeguard against the risks of spyware.
- Ask for examples from students of ways, if any, that they already deal with spyware

Concluding Discussion

- Review what spyware is and the necessity for precautions when downloading items online.
- 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.

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".

REFERENCE—Facts About Spyware

Spyware are programs that are typically loaded onto your computer without your knowledge when you download another program. These programs gather user information and report it back to a monitoring program—using your Internet bandwidth to do so.

Spyware can monitor a user's Web activity, scan files, create pop-up ads, log keystrokes, change the default page on the Web browser, and even gather personal information like password and credit card information.

Some signs you may have spyware including frequent pop-ups, your computer runs slowly, and your Internet is slower than usual.

Sometimes spyware is listed as "adware" in disclosure notices. So read carefully before downloading! In fact, many downloads can advertise no spyware—but that doesn't mean you aren't getting adware!

What Do You Do?

Keep your computer protected.

Follow the four steps to computer security and protection.

Step 1 – Use a firewall.

Step 2 – Update your operating system (OS) regularly.

Step 3 – Use virus-protection software.

Step 4 – Use spyware-protection software.

Remember: Virus- and spyware-protection software will only work if you use it.
Download a spyware-removal program: They can come bundled with virus protection and firewalls, or separately. You can do a simple Internet search to find a free program.

Read any and all agreements when you download software. A disclaimer about spyware could be hidden in the document language.

Choose your downloads carefully. Only download from reputable companies with posted disclosure statements.

Taking steps against spyware will help to:

- **keep your computer safe and secure**
- **keep your personal information private**

LESSON 3—Spam Scams

Learning Objectives

Students will:

- understand the term spam and how it relates to e-mail
- understand the security risks associated with opening spam in e-mail

Discussion

Guide a discussion centered on the following:

- Ask students how many have their own e-mail account.
- Ask students approximately how many e-mail messages they get a day/week.
- Ask students how many of those e-mail messages are messages they throw directly in the trash.
- Ask students if they know the term spam – and to self define it.
- Ask students what they know about safety/security risks in opening e-mail.

Activity

- Break students into small groups.
- Have students brainstorm additions to the lists of safety/security risks associated with e-mail created in the first lesson.
- Meet back as a large group and discuss the lists.
- Discuss possible ways to prevent or safeguard against risks on the lists.

Reference Page

- Pass out the reference page on Spam Scams to students.
- Read page as a class and discuss.
- If you have Internet access, have students go to **http://onguardonline.gov/spam.html** for additional information on spam.

Unit Enrichment Activity

- Allow students to meet back in their small groups. (Groups of 2-3 may work best. Or have students work individually)
- Hand out the Enrichment Activity page to students.
- Explain to students that they are going to conduct a poster campaign to educate others on e-mail security and the risks associated with spam.
- Have each student group design an educational poster on the topic.
- Share posters among classmates.
- Hang posters in school, library, community place, etc, or at a school event or parent meeting.
- Optional – hold a poster contest.

- Check out the Contest and Incentives link at **www.isafe.org**. i-SAFE periodically hosts poster contests, as well as other incentives for student projects.

Alternative for computer use

Follow the directions for posters above, but have students create webpages instead.

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.

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**.

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".

REFERENCE—Spam and Spam Scams

SPAM is a term commonly used for junk e-mail – that you didn't ask for. You might get SPAM in unwanted e-mail messages advertising a company or service. This form of junk mail is becoming more and more of a problem on the Internet. Most spam is received via mass e-mailing. However, other spam can be those annoying forwards you get in your in inbox from friends. Spam is just that – garbage e-mail that should remain unopened.

Combat against SPAM

1. Use an e-mail program that has a built in spam filter so you can delete messages automatically.
2. **DO NOT open spam** – it can alert the sender that you are a "real" e-mail address – opening yourself to the potential of more e-mails.
3. **DO NOT select the unsubscribe option** at the bottom of these e-mails. This is only confirming you are a live person. (This is for SPAM e-mail. Legitimate companies (companies you know and have signed up for) allow you to unsubscribe safely.

So how did they get my e-mail address?

You posted it somewhere! Be careful about where you post your e-mail address. Most companies will state if they can sell your information in their privacy policy. That online prize contest you entered or the free download you signed up for, etc. can put your e-mail on everyone's mailing list.

SPAM Scams

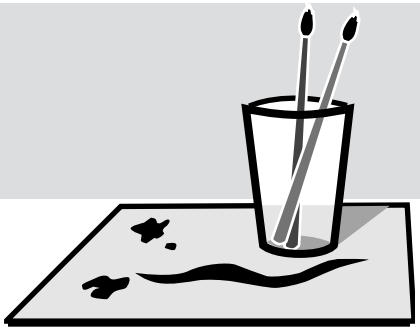
A lot of the spam involves scams, hoaxes, etc. Here are some of the most common types:

- Hoaxes: There are tons of hoax type e-mails circling the internet. These types of e-mails advise one not to flash your brights at night or be careful of kidney snatchers! They are a waste of time!
- Business opportunities: These e-mails offer ways to make money quickly—just remember if it is too good to be true—it probably is.
- Chain letters: You could get gift cards, money or more if you just forward this letter to everyone in your address book. Just not true!
- Health, diet, and drug scams: Want to buy pills, or lose weight quickly? You might receive several of these types of e-mails a day. Get rid of these!
- Illicit e-mail: Advertisements for inappropriate or illegal Web sites. Permanently delete!

Keep these types in mind as you open and read e-mail so you can stay safe and secure!

Go to http://onguardonline.gov/spam.html for more information on SPAM from the Federal Trade Commission.

REFERENCE—Poster Campaign



Directions:

You've become an expert on e-mail security now understand the safety and security risks associated with spam e-mail. However, there are many people out there who receive and open dangerous e-mail each and every day.

Help educate them by conducting a poster campaign.

Preparation

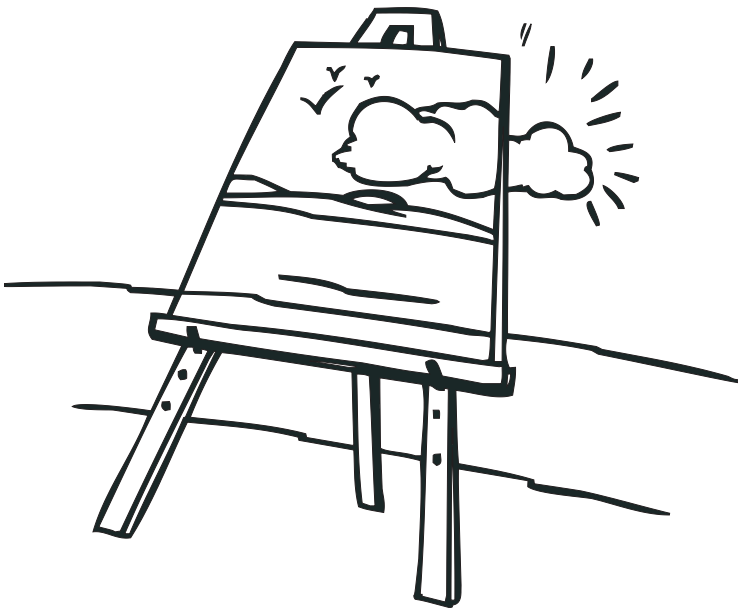
1. Research and decide on a group, event, or area that could benefit from posters on the topic spam.
   - Brainstorm—Where can you hang posters on this topic?
   - Some possibilities: Library, school hallways, cafeteria, mall, airport, etc.
2. Contact the group/person in charge of the areas you select to ask permission to hang posters.
3. Decide on number of posters needed.

Design Posters

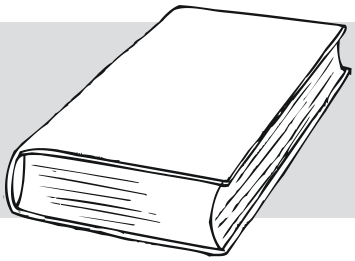
1. In groups or individually, design posters on the topic of electronic spam.
2. Consider the following:
   - Who is your audience?
   - What are key points they need to know?
   - Are there any unfamiliar vocabulary terms?
3. Make sure posters are informative and attractive.

Hang Posters

1. Have others "proof " posters to ensure no mistakes have been made.
2. Hang posters in a public area.



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".