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.

LESSON—Risks of Spyware

Suggested grade level 5-6

Lesson Guide

This lesson focuses on the issues of spyware and adware, including definitions and examination of the risks of downloading items that are potentially bundled with spyware.

Goal and Objectives

Introduce students to the term spyware and the risks of downloading items potentially bundled with spyware. Students will:

- understand the term spyware and the types to which it applies
- understand the security risks associated with downloading items online
- understand how personal information may be compromised via spyware
- engage in an activity to reinforce concepts by sharing information with others

Materials

- a copy of the reference page for each student in the class
- a copy of the activity page for each student group

Procedures

Discussion

Ask students how much time they spend online.

- Ask students if they have ever downloaded anything from online (games, papers, music, soft ware, 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 define it.
- Ask students if there are safety/security risks in downloading items.

Activity

- Break students into small groups.
- Have students brainstorm a list of safety/security risks associated with downloads online.
- 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 to students.
- Read and discuss the reference page as a class.

Developing Public Service Announcements (PSAs)

- Allow students to meet back in their small groups. (Groups of two to three may work best. Or have students work individually.)
- Hand out the activity page to students.
- Have each student group develop a PSA informing others about the possibility of spyware and adware bundled into downloads.
- Share PSAs among class.
- Discuss ways to broadcast the PSAs outside of the classroom.

Review

- Review what spyware is and the necessity for precautions when downloading items online.
- Discuss why it is important to share cyber security issues with others and how to be proactive in dealing with them.

- Take the parent page home and help your families learn about the risks of spyware.
- Broadcast PSAs over the school's public-address system, during assemblies, and/or on school news broadcasts; or create videotapes for distribution.

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

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 include 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 soft ware 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 soft ware. 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**

ACTIVITY

Spyware Activity Guide Developing a Public Service Announcement

You've learned a lot about spyware and adware. You might even call yourself an expert! Now it's time to educate others. You'll be developing Public Service Announcements (PSAs)—educational "commercials"—to educate others about how to guard against spyware and adware.

Preparation

1. Share examples of PSAs on other topics you are familiar with. For examples about internet safety (in English), visit **www.isafe.org**.
2. Find a media outlet within your school.
3. Brainstorm: Where can PSAs be played in your school? (Some possibilities include closed circuit TV or school cable system, student radio broadcasts, or PA Announcements.)
4. Think outside the school: Find a media outlet.
5. Brainstorm: Where can PSAs be played in your city? (Some possibilities include over the radio, on a local news station, over the PA at a baseball game.) What new ones can you come up with?

Develop and Deliver PSAs

1. Based upon the media outlet, select media type—audio, video, or live.
2. Write a script that pertains to your topic and presentation style (audio, video, etc.).
3. Record the PSA (unless doing it live).
4. Edit the PSA with original music, if desired, and titles.
5. Provide PSA through the selected media outlet.

PARENT PAGE—Spyware

Spyware! These days, spyware can cover any number of malicious programs. The term originally was defined as soft ware that was loaded without knowledge on a computer to monitor Web activities. Today, it is easier to label most spyware as "malware" to cover the wide range of harm it can do to a computer.

So how does spyware/malware get loaded onto your computer?

Typically, these malicious programs are loaded without your knowledge when you accept web page components, download soft ware like games, use mp3 players, search toolbars, or use freeware and shareware, etc. Additionally, subscribing to certain online services, such as file-sharing servers, can also load spyware/malware onto your computer. Always look at the user licence agreement for anything downloaded or purchased online to see if it mentions installation of third-party software.

What Can Spyware/Malware Do?

The list of activities for these invasive programs is extensive. Not only can they monitor Web activities and send information back to others, spyware/malware has been known to do the following:

1. deliver pop-up advertising while Web browsing
2. spam you with advertising e-mail
3. slow down your connection
4. steal your personal information (via keystroke logging)
5. send your address book information out
6. hijack your browser, and redirect you to advertising or a fake web page
7. use your computer as a server to host sending out spam, broadcasting porn, etc.
8. slow down and even crash your computer

Prevention of Spyware/Malware

What can you do to protect yourself and your computer? Follow these steps in order for maximum protection.

1. Maintain a firewall on your computer.
2. Update your computer operating system (OS) regularly.
3. Install and use virus protection on your computer regularly.
4. Install and use a spyware-removal regularly, at least once a week.

Other Tips

- Read licencing agreements and user agreements for everything you use, buy, or download online.
- Stay knowledgeable about the latest threats of spyware and malware.
- Make sure you can restore your computer by having all soft ware disks and for installation—back up any and all files just in case. Someday, you may have to reformat your hard drive to completely clean out spyware.