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 2—Proactive Protection Online

Learning Objectives

Students will:

- become experts on the topics of screen name choice, password choice, consequences of online interactions, resources for help, online relationships, and maintaining privacy when online
- be able to select safe screen names and passwords
- be able to interact safely online
- know the resources available if a victim of an online issue

Review

Have students review some of the issues that came up during the survey discussion and true-life script presentation (Your Online Safety: Understanding the Issues lesson).

Peer-to-Peer Activity

The remainder of the lesson will be spent examining in-depth information by student groups on staying safe online. Each group will become an expert on their topic and will present to the rest of the class. Choose one of the following options for classrooms with computers or for classrooms without computers to accommodate different classroom environments.

Decide whether students will work as one large group or in several smaller groups.

With Computers

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 following procedures may be combined as a large group activity, if desired.

Students divide into workable groups. There should be one group for each topic:

- Screen Names and Passwords
- Privacy Online
- Online Interaction
- Consequences
- Resources
- Include separate topic on Identity Theft if desired

Assign each group a topic, and give each group its topic reference sheets. Have each group read through its reference sheets and discuss in groups. Each group will create a short presentation to educate the rest of the class on its expert topic.

Create presentation (with computers)

- Use PowerPoint (or other presentation software), and design a minimum of two—maximum of five—slides to explain and educate others on the topic. Students may feel free to use i-SAFE artwork and graphics in their slide shows.
- Have groups be prepared to present their topic using their PowerPoint slides to the rest of the class.

Presentation (with computers)

- Each group will present for its topic. If done as a one-group project with slides, divide slide presentation among class members.
- After each group has presented, discuss the information as a class.

Create presentation (without computers)

Students divide into workable groups. There should be one group for each topic:

- Screen names and Passwords
- Privacy Online
- Online Interaction
- Consequences
- Resources
- Include separate topic on Identity Theft if desired

Assign each group a topic, and give each group its topic reference sheets. Have each group read through its reference sheets and discuss in groups. Groups should then create overheads, posters, or other presentation props to illustrate the important points. Groups should also write a coordinating script. Have groups be prepared to present their topic using their prop and script to the rest of the class.
Once completed, proceed to presentation.

Presentation (without computers)

- Each group will present for its topic. If done as a one-group project, divide props presentation among class members.
- After each group has presented, discuss the information as a class, review the props, and offer suggestions on improving the presentation.

Wrap-Up Discussion

1. Review with students the necessity of choosing anonymous screen names and passwords.
2. Reinforce that personal/identifying information should never be revealed online.
3. Remind students that anyone met online is a stranger.

Expert Group—Screen Name/ID & Passwords

Directions

In your expert group, read and discuss the information provided on this reference sheet. When finished, brainstorm at least two rules, which represent the information you have learned. Remember: You are responsible for becoming the expert on this topic. You will be required to share this information with your base group.

User ID/Screen Name

A user ID or screen name is a "nickname" you select to identify yourself in e-mails, chats, etc.

Choose one that contains letters and numbers.

Realize that someone may already have the user name you want. Attempt to make yours unique.

DO NOT USE personal information such as:

- -your real first name
- -your real last name
- -your location (i.e., hilliegirl, HaverhillGuy)
- -your zip code
- -family or friend names
- -a suggestive name or word (i.e. sexyman69, hotbabygirl)
- -pornographic or obscene words

Do use:

- -a nickname (for example: sunshine, shortstuff)
- -something that relates to a favorite hobby, musical group, or movie (i.e., Cheering4u, LinkinParkFan, Matrixmad)
- the current year added to the end of the name if someone is already using the name you want (i.e., shortstuff-10)
- a second letter at the end of your nickname (i.e., ddancer instead of dancer)
- For added security, always opt NOT to add your name or nickname to any sort of member directory.

Password

A password is a series of letters, numbers, or symbols used to log you in to a computer system. Passwords are used to access e-mail, join chat rooms, etc. They are usually between six and eight characters long.

Password Security

1. Don't tell anyone your password.
2. Don't write your password down anywhere.
3. When you decide on a password, make sure it can't be guessed.
4. Make sure no one is standing near you when you enter your password.
5. If you think there's even a chance someone else might know your password, change it.

Password FAQs

Why is password security important?

Many people like to "crack" codes and use e-mail, etc., for their own use. Some of these people may even be your friends or people you go to school with. Once in, they can do awful things to your stuff and to the stuff of other people.

How can I tell if my password can be guessed?

People who crack codes use computer programs to do so. Your password is encrypted, meaning it is changed into new numbers/codes once entered into the system. So no one can just take a look or break into a system to get it. Instead, they use computer programs to encrypt letters and numbers in an attempt to match your password.

To attempt every possible combination would take forever. Instead, obvious combinations are tried. Many people choose a password based on something personal like their name, address, Social Security number, phone number, etc. The program tries these first. Next the program tries all the words in the dictionary forward and back. This only takes several minutes. This is why it is unwise to choose a common word like "friend" as a password.

So what are you supposed to do if you can't write it down and it can't be a word or familiar thing?

There are tricks to creating a good password that can't be guessed yet can be remembered. **Here's one of the tricks**: Take a phrase you like and will remember. Now use the first letter of each word. Add any appropriate capitalizations, punctuation, and other character manipulations.

For example: "Three blind mice, see how they run" would end up as "3bm,shtr."

Expert Group—Privacy Online

Directions

In your expert group, read and discuss the information provided on this reference sheet. When finished, brainstorm at least two rules, which represent the information you have learned. Remember: You are responsible for becoming the expert on this topic. You will be required to share this information with your base group.

Online identity

The Internet is an arena of information. However, it is not anonymous. When you sign on, others have access to you. Your e-mail address, screen name, and password serve as barriers between you and others. You need to maintain this barrier by not including private or personal information in an online identity.

There are many people out there who would like to know more about you for a variety of reasons:

1. They could want to harm you.
2. They could want to steal from you.
3. They could use information to conduct their own business, such as selling your info or using it in an illegal manner.

If you are under 13, the Children's Online Privacy Protection Act (COPPA) applies to you. It requires commercial Web site operators to get parental consent before getting your personal information. It is hoped that this law will help stop Web site owners who might misuse information they collect from you.

For those older than 13: You still need to be careful.

When surfing the Internet, chatting, or e-mailing, stay safe by remembering:

- **Never give out your first or last name, your parents' names, your home address, your phone number, your birth date, etc.**
- **Don't tell anyone your password.**
- **Be careful to whom you tell your screen name and user ID.**
- **To prevent SPAM, use a different screen name from your e-mail address. View a Web site's privacy policy to understand how they can use the information you give them.**
- **Ask for parental permission before giving information out.**
- **You should be able to participate in most online activities without giving out information.**
- **Log off if personal information is asked for.**
- **When you receive an e-mail that is inappropriate, delete it and report it. Don't ask to be removed or click on the removal button—that informs spammers that yours is a real e-mail address, and they will send more!**
- **Don't give out other people's names or e-mail addresses—you want to protect them also.**
- **Don't register for contests or fill out information to download software.**
- **Understand that people aren't always who they claim to be. Don't give out information to anyone claiming to be from the Internet company, etc.**
- **E-mail is not always private, so don't put anything in there you would not want to see broadcasted.**

Expert Group—Online Interaction

Directions

In your expert group, read and discuss the information provided on this reference sheet. When finished, brainstorm at least two rules, which represent the information you have learned. Remember: You are responsible for becoming the expert on this topic. You will be required to share this information with your initial group.

The Web

These days, it's difficult to get your schoolwork done without using an Internet search engine. There are lots of great sites on the Web with useful information. You can find books, games, and pictures—anything you want. However, there are risks associated with searching the Internet.

Watch out for . . .

- **Inappropriate Sites** – There are some sites you should not go to. They can be inappropriate, hate-filled, or upsetting. When you accidentally come across a site you know you shouldn't be in, close out of it quickly. Click on the X in the upper right-hand corner of the screen, or if you still have trouble, try logging off completely or rebooting.
- **Faulty-Information Sites** – Don't trust everything you read without double checking and checking references.
- **Private Information** – Some Web sites ask you for private information before you can access their stuff. Don't give it out, and ask your parents if you have further questions about it.
- **Your Own Web Site** – Many teens now have their own Web sites. However, you have to be careful about what information you display.

E-Mail

Watch out for . . .

- Spamming – Many companies advertise via e-mail. They try to entice you to purchase items, visit inappropriate sites, etc. Delete these e-mails.
- Be careful when you reply to an e-mail. You are including your e-mail address, and you don't know where it will go from there.
- Inappropriate, offensive, angry e-mail should be reported to your Internet provider.
- Remember: The sender of an e-mail may not be someone you know. Don't send personal information, photographs, etc.

Chatting and IM

Chatting and instant messaging (IM) allows you to engage in real-time "conversation" with people around the world. You type what you want to say, and then everyone can see it. Some chat rooms have specific interests, such as an actor or music group. Some chat rooms are moderated, meaning there are people watching the conversation, who step in to guide or enforce rules.

The monitor can't, however, prevent you from going off to a private chat area with a person who might do you harm or keep you from typing information that could put you in danger.

Be Safe.

- Keep online interaction online. Don't agree to meet or phone people met online.
- Don't give out personal information. Be careful about indirectly saying too much, such as naming a school mascot, game times, etc. Eventually, you will have said enough.
- Keep your parents or guardians informed of online interaction.
- Use chat rooms that are moderated.
- Be suspicious of someone who wants to be your friend and tries to turn you against your parents, teachers, or friends. That's not what friendship is all about.
- Private chats aren't always private. When you meet offline friends online in a private chat room, be careful. Others can lurk in your conversation—listen to private conversations between you and your known friends.

Social Networking

Social Sites, Newsgroups, Forums, Blogs, and Bulletin Boards

Social-networking sites, as well as traditional online forums and newsgroups, are all places where you can read posted files, download or upload files, or post your own messages. Posted messages remain there even after you leave. You can find an individual or a group on almost any topic, and they are a great way to get involved in an area of interest.

THINK before you POST.

- The biggest risk is including personal information in postings. Don't reveal anything identifying about yourself.
- Realize that by posting to some types of bulletin boards, you are making your e-mail address public.
- Groups that are illegal or want to spread hateful messages may try to get you involved if you post contact information.
- Realize that anything you post online may be difficult to undo.

Expert Group—Consequences

Directions

In your expert group, read and discuss the information provided on this reference sheet. When finished, brainstorm at least two rules, which represent the information you have learned. Remember: You are responsible for becoming the expert on this topic. You will be required to share this information with your initial group.

Introduction

People tend to feel invincible and protected when they are on the Internet. They feel safe and secure because they are sitting at a computer, safe and sound in their home. It is difficult for them to imagine all the possible dangers lurking out there. However, there are consequences for lax behavior on the Web. Some are annoying; others are quite serious and dangerous.

Possible Consequences

1. Many exchange photos with people they have met online. This is dangerous for two reasons: It allows the other person to recognize you, and you lose control over how your photo might be used or altered by another person. You might not like what happens and be powerless to do anything about it. For example: A photo of your face could be placed on another person's body, etc.

2. When you freely use your e-mail address, you are advertising to others that this is a valid address to e-mail to. The likelihood for spam e-mail or other unwanted mailings increases dramatically.

3. Many people chat and instant message online. Do you know that anyone can access a chat and anyone can search and look at a chat or IM profile? What are you advertising to total strangers? The more information you give freely to others, the more tools they have to break down your defenses. You open yourself up to cyber stalking, harassment, and other types of victimization by someone who may want to harm you.

4. When you post something on an online bulletin board, you cannot erase it. Whatever is written is there for everyone to see, whenever they want to see it. This can lead to embarrassment or loss of privacy.

5. Entering a credit card number and/or Social Security number, name, and address information, etc., on an unsecured Internet site can lead to monetary theft and worse: identity theft.

Experts Group—Resources

Directions

In your expert group, read and discuss the information provided on this reference sheet. When finished, brainstorm at least two rules, which represent the information you have learned. Remember: You are responsible for becoming the expert on this topic. You will be required to share this information with your base group.

When Problems Occur

On the Internet, there are varying degrees of offense, just as there are in real life. Some things are mere annoyances, such as junk e-mail or spam. Other things rise above being annoyances and become illegal, such as child luring or child pornography. There is a proper place to report annoyances, just as there is a way to report the more illegal crimes.

A general guideline for reporting Internet wrongdoing is to get the help of a trusted adult to determine if law enforcement should be called.

Any type of threat of physical harm is illegal and must be reported.

1. Call the local police and ask if they have a department affiliated with Internet Crimes Against Children (ICAC). If they do, go through that department.

2. Simultaneously, file a report with the Cybertips hotline at 1-800-843-5678.

Online criminal actions that should be reported:

1. **Cyber Bullying** – You feel you are being bullied, harassed, and/or threatened online.

2. **Cyber Stalking** – You feel you are being victimized by a hateful or obsessive person.

3. **Child Luring** – You feel you are in danger or someone you know is in danger of falling prey to a predator.

4. **Inappropriate Material Sent to a Minor** – Pornographic or other inappropriate material is being sent to you via online communication (e-mail, etc.).

Expert Group—Identity Theft

Identity theft is a serious crime that costs American consumers billions of dollars and countless hours each year. It occurs when someone uses your personal information without your permission to commit fraud or other crimes. While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk. The Federal Trade Commission (FTC) encourages consumers to Deter, Detect and Defend to help cut down on identity theft.

Deter

Deter identity thieves by safeguarding your information:

1. Shred financial documents and paperwork with personal information before you discard them.
2. Protect your Social Security number. Give it out only if absolutely necessary or ask to use another identifier.
3. Don't give out personal information via the phone, mail or the Internet unless you know who you are dealing with.

Detect

Detect suspicious activity by routinely monitoring your financial accounts and billing statements. Be alert to signs that require immediate attention, such as: bills that do not arrive as expected; unexpected credit cards or account statements; denials of credit for no apparent reason; and calls or letters about purchases you did not make.

Defend

If you think your identity has been stolen, here's what to do:

1. Contact the fraud departments of any one of the three consumer reporting companies (Equifax, Experian, TransUnion) to place a fraud alert on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. You only need to contact one of the three companies to place an alert.

2. Close the accounts that you know or believe have been tampered with or opened fraudulently.

3. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or, at the very least, the number of the report, to submit to your creditors and others who may require proof of the crime.

4. File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps officials learn more about identity theft and the problems victims are having so that they can better assist you.

To learn more, visit www.ftc.gov/idtheft.