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 Online Personal Safety Unit

Suggested Grade Level 6

Curricular guide with options for classes with or without computers

Overview

The "Personal Safety" lesson unit consists of five 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 five lessons to ensure all necessary information on online personal safety is covered.

Note: Lesson 4 of this unit briefly touches on online strangers, predators, and the grooming process. If appropriate to your students, the lesson "Predator Identification," available in the "Predator Identification" module for Gold subscribers, provides more in-depth coverage of this topic.

Unit Goals

Students will

- recognize ways personal information provided on the Internet can be used to harm the user
- make responsible choices in what they reveal online
- revise screen/user names and/or passwords to apply safety standards, if needed
- refuse to communicate with strangers who exhibit grooming tactics
- refuse to meet face to face with Internet strangers without the permission from parents
- recognize and report suspicious behavior by an online stranger to a trusted adult
- communicate in Cyberspace safely

Enrichment Goal

i-SAFE enrichment activities are 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**. Completion of this unit will prepare and guide learners to create and distribute brochures to create awareness about online personal safety.

Materials/Preparation

- online access to the i-SAFE assessments, if appropriate for this lesson
- a copy of "Be Smart Be Safe" activity pages for each student
- a copy of the teacher resource article
- a bingo card copy for each student
- a copy of the information game page, cut up as directed for group activity
- computer access to desktop publishing for creating a brochure or provided MS Word brochure template (optional for use in classrooms with computers)
- student registration in i-MENTOR program at **www.isafe.org**
- optional: PowerPoint presentation available 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** by clicking "Assessments" prior to the lesson. To verify school ID number, log in at **www.isafe.org**, go to the "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 may be completed at home. If you would like to register students yourself, simply go to **http://www.isafe.org/teachermentorprogram**, and fill out the information for your students. Then e-mail to **outreach@isafe.org**. Your students will be enrolled, receive information about sharing Internet safety with other students, and be registered to participate in contests to win prizes.*

LESSON 1—Safeguarding Your Identity While Online: Screen Names and Passwords

Learning Objectives

Students will:

- state the dangers in choosing an unsafe user name
- classify the types of personal information that should be avoided in constructing a safe user name
- assess the dangers in choosing an unsafe password
- identify strategies for making passwords safe
- demonstrate that they can choose a safe and secure password and user name

Peer-to-Peer Activity

Provide a copy of the reference/activity pages "Be Smart – Be Safe" for each student.

- Is a person really anonymous if they have provided personal information in a screen name?
- How can a safe screen/user name and/or password help you avoid danger on the Internet?

The reference/activity page will prompt students to create safe passwords using the strategies listed.

Discussion – Information Overview

- As a class, review the information found on the activity pages.
- Have each group address one or more of the questions and activity answers.
- Discuss any areas that are unclear.
- Discuss why non-identifying screen names and passwords are important.
- Make sure to cover the idea that in order to protect identity in the physical world, online screen/user names should never include personal or identifying information, including (but not limited to):
  - > first and/or last name
  - > address
  - > phone number
  - > date of birth (complete or partial) or age
  - > Social Security number
  - > e-mail address
  - > combinations of personal information, such as listed above
  - > combinations of personal information, such as listed above, plus descriptions like (but not limited to) gender, school name, favorite sport, favorite celebrity, family member names
- Go over the passwords created in the group. Discuss each one, and have students review to make sure that each follows the listed strategies. Emphasize that a password should:
  - > be lengthy, at least eight characters
  - > contain a combination of letters, numbers, and symbols
  - > be changed when its secrecy is in doubt
    - > **not** contain personal information
    - > **not** be shared

> **not** be easily guessed

> **not** be provided in an e-mail, even if requested

Group Activity

- Provide students with this list of screen names (write on the board or read aloud):
  > GTaylorplaysGuitar
  > carrie_lewis@gmc.net
  > REMforever
  > Miamisue13
  > canarielover
  > nymets29
  > brandonclassof09
  > wellesleygirl
  > namelessjester9
- Have students arrange the screen names in two lists to show those that contain identifying (or potentially identifying) information and those that do not.
  KEY:
  Contain Identifying (or Potentially Identifying) Information
  > andersonMJ (initials and last name)
  > carrie_lewis@gmc.net (e-mail address)
  > Miamisue13 (name, location, age)
  > brandonclassof09 (name and graduation year—tells age)
  > GTaylorplaysGuitar (initial, name, hobby)
  > wellesleygirl (location, gender)

  DO NOT Contain Identifying Information:
  > REMforever
  > canarielover
  > nymets29
  > namelessjester9
- Have each student create safe user names and passwords, which would be appropriate and non-identifiable on the Internet.
- List the safe screen names and passwords on the board.
- Ask students to think about whether the screen names and/or passwords they use could be made safer.

Conclusion

- Remind students that they need to avoid providing personal/identifying information while online.
- Encourage students to change their screen names or passwords, if needed, and discuss what they have learned with their parents.
- Remind students to register at **www.isafe.org** by clicking on "Create and Account" if they haven't done so already.

Be Smart Be Safe

The Internet 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 giving out private information. There are many out there who would like to know more about you for various reasons:

- They could want to harm you.
- They could want to steal from you.
- They could use information to conduct their own business either by selling your info or by using it in an illegal manner.

User ID/Screen name

A User ID is a nickname you select to identify yourself in e-mail, chats, etc.

- DO NOT USE personal information that can identify you, including:
  - > your real first and last name
  - > any part of your address
  - > your location (i.e. hilliegirl, HaverhillGuy)
  - > your telephone number
  - > your e-mail address
- Do not use an inappropriate suggestive name or word to describe yourself (i.e. sexyman42, hotbabygirl). You may attract the wrong kind of people.
- Do not use pornographic or obscene words.

Be careful that you don't combine pieces of personal information with other information that can be used to identify you or your location, such as in the screen name TSmith94Yankees.

Your Screen Name

Think about your own screen name. What does it say about you?

When you choose a screen name, you want something that allows you to remain anonymous, or unknown. Don't include personal information.

Secret Passwords

A password is a series of letters, numbers, and/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

A password is of no use to you if it is not a complete secret.

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

How to Create a Safe Password

A good password should . . .

- be lengthy, at least eight characters
- contain a combination of letters, numbers, and symbols
- be changed when its secrecy is in doubt
- not contain personal information
- not be shared
- not be easily guessed
- not be provided in an e-mail, even if requested

LESSON 2—Protecting Personal Information

Learning Objectives

Students will:

- comprehend that anyone met exclusively online is a stranger
- understand how indirect information can be used to identify someone
- recognize how to respond appropriately to Internet strangers
- understand risks of providing too much personal information in online profiles and forms

Read and Discuss

- Read the resource article located at the end of this less plan to the class.
- Have the group brainstorm how this could have been prevented.
- Have students answer the following questions:
  - > Why do students feel safe on the Internet?
    possible reasons: in own home, behind screen, anonymous, etc.
  - > What are some dangers on the Internet?
    possible answers: predators, thieves, bullying, bad sites, hate sites, etc.
  - > What are some good things on the Internet?
    possible answers: research, information, ability to find things, maps, directions, etc.
- Provide each student with a copy of the resource page, and select students to read the information to the class. Do the Identity Theft activity or read over the reference page together.
- Discuss and/or answer any questions about direct and indirect information.

Bingo Game

The following activity reviews and reinforces the concepts learned in this lesson and Lesson 1 of the personal safety unit. As you play the game, make sure to reinforce key lesson points, such as never revealing personal information online.

- "We've covered an enormous amount of information. Now you're going to have an opportunity to show how much you have learned. This activity is called 'REVIEW BINGO'."
- Distribute the "REVIEW BINGO" sheets, and ask students to read the directions with you. Then have students fill in answers on their bingo cards working alone, in pairs, or in small groups.
- When students finish filling out their bingo cards, announce: "Now I'll draw slips of paper that will have questions. These questions are answered by the words on your bingo square. After the question has been called, place a large check mark (or scrap of paper) in that bingo square. When you have checks in five boxes in a row or diagonal, call out "Bingo!" At that time, I will review with the class the correct answers to all of the questions asked and make sure your card was correct. Any questions?"
- As you play the bingo game, clarify and/or discuss terms or information that students find difficult.
- After winners have been identified, hold a brief discussion of the answers for squares not called in the activity.
- This game can be played multiple times or as time permits. If the game will be replayed, use colored paper or some other way to mark squares.

Wrap-Up Discussion

- Review with students the necessity of choosing anonymous screen names and passwords, and the importance of keeping one's identity safe and private.
- Reinforce that personal/identifying information should never be revealed online.
- Remind students that anyone met online is a stranger.

Resource Article

The following article is based on a compilation of several real stories about Internet safety issues.

Most teenagers and young adults these days have been online. Certainly there are plenty of good reasons to use the Internet—hanging out with friends, doing research, and playing games. Unfortunately, there is increasing danger involved in getting online.

Take Brittany for example. Brittany was a young teenager. She liked to hangout, play softball, and chat on the Internet, especially with Jason, the friend she met while online. Even though they had never met in person, she just knew Jason was her soul mate. He liked everything she liked, and they could always talk about softball. He knew her school and her team number. She had described the new uniforms to him.

Jason had reminded Brittany about being careful—to be careful about giving out personal information online. He cared about her and wanted her to be safe. As a matter of fact, he had reminded her so often that she tended to tune him out. To her, it wasn't like she chatted with anyone she didn't know! Besides, she never gave out her home address or phone number.

Brittany felt safe online. However, she wasn't fully aware of all of the dangers out there. Even without sharing her address, Brittany had supplied Jason with enough information in their conversations for him to be able to find her offline. And more importantly, Jason had built a trusting relationship with her, even though they had never met.

Fortunately, Brittany's friend was, in reality, a 35-year-old law-enforcement officer who was involved with the prevention of Internet crimes. Establishing an Internet relationship with Brittany was used to show how easy it is for people on the Internet to get information that can potentially put others—especially young people—in danger.

Demonstrations like this one have been used across the country to show that only until you know what the dangers are, and know how to protect yourself, can you be assured that you will have a great time online, and still be safe.

REFERENCE PAGE—Who knows WHAT about You?

Know about indirect information solicitation

Sometimes people can find out all about you "indirectly" – by piecing bits of seemingly unrelated information together. For example, indirect information about your school, activities, etc., could lead someone to figure out where you live. Be aware of what you say at all times, and where you say it online –

Watch out for communication dangers…
… on the Web

- POP-UPs – You are a WINNER! Surfing the Web often provides lots of pop-ups offering free merchandise, contests, and survey forms to fill out. Information you provide can be used to create e-mail spam and will make MORE pop-ups!
- Web sites you visit – Some Web sites ask you for private information before you can access their stuff. Make sure you ask your parents before giving anyone private information on online forms.
- Your own Web site – Many young people now have their own Web sites or social networking pages. Be cautious about what information you display.

…in E-mail

- Spam – many companies advertise via e-mail and ask for more information about you. Do not respond to these e-mails – DELETE them!
- 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.
- Remember the sender of an e-mail may not be someone you know – don't send personal information, photographs, etc.

…when Chatting, IMing, or Gaming

Instant communication can result in revealing information you wouldn't normally reveal. This can leave you open to harm.

- 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 about yourself. Eventually you will have said enough.
- Private chats aren't always private – when you meet offline friends online in a private chat room, be careful. Others can often enter and lurk (watch what you are saying about yourself).

Directions

Using the word sheet, fill in the squares of the bingo card below. Mix up the words so that your card isn't the same as someone else's. The teacher will read out questions. The answers to these questions are those words you used to fill in the bingo squares. Find the correct answer and mark it off. You have Bingo if you get five in a row. Raise your hand or call out Bingo when you do!

Internet Safety Bingo				
		FREE		

Bingo Vocabulary

Directions

Use the following twenty-four words to fill in the squares on your bingo chart. Remember to mix up the order of the words – you don't want your chart to look like anybody else's. Then to play the game, listen carefully as the teacher reads out questions. Try to locate the correct answer to the question and mark it off on your bingo chart. When you get five in a row horizontally, vertically, or diagonally – call out Bingo!

Vocabulary:

1. LMSmith14
2. Singin4fun
3. Chat
4. Pop-ups
5. Address
6. Password
7. Spam
8. Delete
9. Trusted adult
10. Indirect
11. Stranger
12. Screen name
13. Online form
14. IM
15. 19#He%d2
16. Personal Information
17. Online
18. Picture
19. Your own webpage
20. Change it
21. False
22. True
23. Unsafe
24. Anonymous

Teacher Resource Page—BINGO Terms and Definitions

1. This is an example of a screen name that is considered inappropriate.
   LMSmith14
2. This is an example of an appropriate screen name.
   Singin4fun
3. This is a way to communicate online.
   Chat
4. Providing information on these will give you spam e-mail and more of these.
   Pop-ups
5. This is one piece of information, which is considered private or personal.
   Address
6. You should never tell this information to anyone or even write it down.
   Password
7. This refers to unwanted garbage e-mail
   Spam
8. You should do this when you receive unwanted e-mail.
   Delete
9. When you feel you or a friend are in danger from someone from the Internet you should report it to a
   Trusted adult.
10. This refers to the kind of information that is gained through knowing things like a school mascot, concerts, etc.
    Indirect
11. A person you have only met on the Internet is a
    Stranger.
12. An online nickname is also known as a
    Screen name.
13. Ask a parent before you fill out one of these.
    Online form
14. The well-known abbreviation for Instant Messaging is
    IM.
15. This is an example of a safe password.
    19#He%d2

16. First or last names, phone number, and birth date are all examples of

    Personal Information.

17. Do not meet or phone people you meet

    Online.

18. It is dangerous to send this or post this online.

    Picture

19. You should be careful about personal information you put here.

    Your own webpage

20. What should you do if you think someone knows your password?

    Change it

21. True or false: It is a good idea to give your phone number to people you meet online.

    False

22. True or false: It is a good idea to keep your parents or guardians informed of online interaction.

    True

23. A screen name containing your zip code, your school name, and your last name is **Unsafe**.

24. If your screen name/user ID contains personal information, you are NOT

    Anonymous.

LESSON 3—Identity Theft

Goal and Objectives

Introduce students to the concept of identity theft and the risks associated with revealing private information online. Students will:

- Understand the concept of identity theft.
- Understand the security risks associated with revealing private information online.
- Develop an action plan for dealing with identity theft that can be shared with parents.

Materials

- Resource Page and Student Activity Page – Make copies for students in class
- Internet access (Recommended) to **http://onguardonline.gov/idtheft.html and www.isafe.org**

Discussion

- Ask students how much time they spend online.
- Ask students if they have ever visited a Web site asking for personal information.
- Ask students if they frequently reveal things like name, birth date, etc online.
- Ask students if they have ever bought items online.
- Ask students if they know the term identity theft – and to self define it.
- Ask students to discuss how identity theft can affect a person. Who is most vulnerable?

Activity

- Break students into small groups.
- Have students attempt to answer the following questions in their groups:
  - > What are steps you can take to protect your personal information?
  - > If you discover your identity has been compromised or a credit card number used illegally, what should you do and whom should you contact?
  - > What steps can you take to be prepared "just in case something does happen?"
- Meet back as a large group and go over discussion results.

Reference Page

- Pass out the reference page to students.
- Read reference page as a class and discuss.

If you have Internet access have students go to **http://onguardonline.gov/idtheft.html** for additional resource information from OnGuardOnline.

Activity

- Pass out the student activity page and read as a class.
- Allow students to meet back in their small groups. (Groups of 2-3 may work best. Or have students work individually.)
- Have students develop an action plan – a checklist of what to do if one suspects their identity is stolen.
- Share checklists.
- Develop an opportunity to share lists and information on identity theft with parents.

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:

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Give it out only if absolutely necessary or ask to use another identifier.
- 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 ftc.gov/idtheft.

Student Activity Guide—Identity Theft

Activity 1

In addition to the reference page, use other resources as available to you to research identity theft.

- In your groups design a checklist to guide you in the process of protecting your identity if you ever think it might have been stolen.
- Some items not to forget:
  - > Contact Credit Card Companies
  - > Contact Consumer Reporting Agencies: Examples: Transunion, Equifax, and Credit Data Services
- What else can you come up with? Make sure to put it in a logical order!

Activity 2 – Parent Presentation

Chances are you aren't as likely to be a victim of identity theft as your parents are when they are online – especially now that you've been educated! Think about it – you are in a better position than most to educate parents on the issues you've been learning about.

Use what you have learned about identity theft to create an informative presentation for parents or others at your school. Design and develop your parent presentation:

- What information do you consider "critical" when it comes to identity theft for parents to know?
- What information can make an impact on how parents participate online?
- Use the student activity page and content learned from this lesson to start to develop content for your presentation.
- Develop an action plan – a checklist of what to do if one suspects their identity is stolen.
- Share checklists. At your parent night, hand out copies of your checklist so parents will know what to do if they are ever a victim of identity theft.

Make arrangements with school faculty to share your parent presentation at a regularly scheduled school event such as an open house or PTA meeting.

Need more information?

i-SAFE has some pretty amazing materials available to you as you plan your parent presentation at the i-MENTOR Training Network.

You can watch a video just for students and receive training on how to reach out

1. Go to **www.isafe.org** and log in.
2. If not registered, click on "Create an Account."
3. Access the X-BLOCK and select the i-MENTOR Training Network.
4. Select the module: Parent Presentation.
5. Watch the training video – take notes.

LESSON 4—Online Strangers, Predators, and the Grooming Process

Learning Objectives

- Define an online stranger as anyone met exclusively online.
- List safety rules/advice of behavior toward strangers in the physical community that also apply to behavior toward strangers in Cyberspace.
- Recognize steps in an online predator's grooming process.
- Recognize how to respond appropriately/safely to Internet strangers.

Introductory Discussion

- Ask how many students use the Internet, and how many go online alone.
- Ask what they like to do online.
- Ask if it is their intention to talk to adults while online.
- Ask how they know if someone is their age when online.

Peer-to-Peer Activity

Information Activity Directions:

- Provide each student with a question cut from the information activity page.
- Tell students that each has a unique question. They are to try to get that answer from five different students without asking the question directly. They cannot simply come out and ask. They will have one minute to prepare their thoughts and questioning procedure.
- Direct the players to pair up (at teacher discretion). Inform students that they have one minute to negotiate conversation and find the answer to their question.
- Have students change partners five times, allowing one minute per each grouping.
- Ask students to raise their hands if they found it easy or if they got their answers. Ask how they got their answer without asking the question. Discuss some of the strategies used to uncover answers.
- Ask who had a difficult time, and have them explain why. Ask if some people resisted giving information. Did this make the assignment more difficult? Would it also make it difficult for someone online to find information?
- Use the information game to show that people can find out things in indirect ways. Explain that some people do this online and use the information they gain to pretend to be your friend.
- Explain that it may be easier to get direct information on the Internet because it is through writing.

Discussion

Guide students into a discussion about the concept that anyone met exclusively online (not a known friend from the physical community) is a stranger.

- Ask students to define the term "stranger."
- Ask students to list common advice/rules concerning strangers in the physical world.
- Explain to students that those rules also apply online. All people MET exclusively online are strangers. Nothing is really known about these people.

Define "online predator"

- Explain that some people lie about who they are and what they want on the Internet for various reasons. Sometimes it is to steal an identity or to bully. Other times it is to meet children and teens to form an inappropriate relationship. These people are known as "online predators."
- Ask students if they know what the word "predator" means. Take their answers and try to form a definition.
- Relate their answers to online predators by reinforcing the following: A predator is one who stalks or uses lies, secrecy, or stealth, to get close enough to another person in order to easily hurt or harm them.
- Ask students if they know what the word prey means. Take their answers and try to form a definition.

Define "prey"

- One who is a victim or is vulnerable to victimization by a predator is prey.
- Relate the concept to the online environment.

Minimize danger

- Inform students that there are things they can do to minimize the danger and the chances of becoming prey to an online predator.
- These safety precautions include choosing a safe screen name, not revealing information on the Internet, and carefully choosing with whom to communicate.
- Inform students that no matter what, it is important to tell an adult if they feel uncomfortable online or are approached by someone who discusses inappropriate things or wants to meet them offline.

Group Activity

Hand out the reference pages on the grooming process.

Review steps in the grooming process.

(1) SIMILAR INTERESTS

An online predator will establish a relationship by discussing common interests, likes, and dislikes with the intended victim. This leads to a feeling of familiarity and a friendship. A predator can find potential prey to begin a relationship by searching online profiles and screen names for interesting topics, such as particular sports or hobbies, as well as birth dates or ages. Once the grooming process starts, the victim feels like he or she really knows the predator. It is difficult to consider this "friend" a "stranger."

Reinforce: If you have only communicated with someone online, you cannot be sure if the person is who he/she claims to be. People online are not always who they say they are. It is very easy for anyone to feel like he or she knows someone online when it is not really true. A predator uses this concept to his/her advantage.

(2) TRUST

A predator will want to listen to anything the victim wants to talk about. This tactic is used to build trust. For example: If you are being victimized, the following might be a typical scenario. If you have a bad day at school or at home, he will be sympathetic. He will tell you that he understands. You will begin to believe that this person really cares about you.

Reinforce: The longer people "talk" and share online, the more the victim will come to believe that this online person is no longer a stranger but actually a friend. Soon a sense of trust is developed in this false friend. A predator uses this to try to separate the victim from his or her true friends and family.

(3) SECRECY

As the relationship progresses, a predator will usually ask the victim to keep the friendship secret from others. He/she may explain that other people, especially parents, won't understand how you (the victim) can be such good friends with someone who you met on the Internet. This approach gives the predator confidence that it will be more difficult for an adult to step in and protect the victim.

Reinforce: This type of behavior is a very important warning sign. Anytime an online "friend" asks to keep the relationship a secret, recognize this as a warning, and report it to a trusted adult. A true friend would not need to keep the relationship a secret.

(4) BREAK DOWN BARRIERS

Once the predator has built a trusting relationship he or she will continue to break down barriers in order to achieve the ultimate goal of a face-to-face meeting. One way this is accomplished is by sending pictures that may at first make the victim feel uncomfortable. This often happens because kids and teens are naturally curious about many things. Predators prey on that curiosity and continue to feed it so that the victim will not be afraid. This is done by gradually sending more and more pictures and other inappropriate material so that the victim becomes less sensitive to things that normally would make him/her uncomfortable.

Reinforce – It is normal to be curious, but students should know that it is against the law for anyone to send pictures of people (of any age) without their clothes on to someone they know is under 18 years old. This criminal action must be reported to a trusted adult and/or law enforcement.

Discuss with the students that if anyone sends them pictures or any other material that make them feel uncomfortable for any reason–please tell a trusted adult (parent, teacher, law enforcement officer).

(5) MAKE THREATS

Sometimes, but not always, a predator will threaten the (victim). A predator may threaten in different ways to keep the victim from telling an adult. One tactic is to use a reverse threat.

Example: Imagine you are a victim. A predator will tell you that if you tell anyone, he or she will tell your parents about your relationship, then your parents will be really mad at you and may take away your computer or ground you. The predator may tell you that he or she knows where you live and can harm you or your family.

Reinforce (1): Students need to know that if anyone ever threatens them, online or offline, they need to tell a trusted adult. The ultimate goal of an Internet predator is always to get the victim to meet with him or her in person.

Reinforce (2): As intelligent young people, they may believe they can never be tricked by an adult they meet online. But the fact is, criminals make it their business to devise ways to deceive them.

Wrap-Up Discussion

- Review and reinforce the concept with students that anyone met online is a stranger.
- Have students name the steps a predator uses to groom a potential victim.
- Reinforce: It is important to never reveal personal information online and have safe screen names so as to not be targeted by strangers online.
- Reinforce: It is important to report behavior by a stranger online that makes them uncomfortable, asks for personal information, or requests a face-to-face meeting.
- Ask students to give reasons why knowing about the grooming process can make them more confident users of Internet communications.

Information Activity

Directions

Duplicate one or more pages (35 questions to a page) so that each student will have 1 question.

Cut out questions on solid lines, and pass out 1 to each student.

Do you have a dog?	How tall are you?	What size shoe do you wear?
Do you have a cat?	What is your worst fear?	If you could be an animal – what animal would you be?
What is your favorite color?	What is your best memory?	What type of music do you like?
What is your favorite food?	How would you describe yourself?	What do you do most on a computer?
Where would you like to go on vacation?	What is your favorite subject in school?	What chores do you have?
How many brothers do you have?	What do you do on the weekends?	What is your phone number?
How many sisters do you have?	What is your favorite holiday?	Who was your favorite teacher?
What hobbies do you have?	How old are you?	What is the name of your school?
What is your favorite movie?	Who is your favorite actress/actor?	What is your favorite television show?
What is your favorite song?	What is your favorite book?	What city do you live in or near?
Who is your hero?	What is your favorite ice cream flavor?	What is your least favorite subject in school?
What sports do you like?		
What would you like to be when you grow up?		

The Grooming Process

How can you be sure who you're talking to online? Internet predators use what is known as the grooming process to create seemingly safe online relationships and then betray that friendship by attempting to break down barriers and cause harm.

Online predators find their "prey" by going to chat rooms where young people gather or by searching online profiles for a specific type of victim.

Predators use a process to "groom" their victims, which usually follows this pattern:

(1) Establishes similar interests through chatting or instant messaging. This leads to more private communication like e-mail and phone calls.

(2) Builds trust. A predator counts on the fact that establishing so much in common with an online friend will lead to a trusting relationship. A predator is hoping that you will develop such a trust that you will separate yourself from your true friends and family.

(3) Keeps it a secret. It is a predator's goal to keep the friendship a secret from others. Engaging in a secret friendship like this leaves you vulnerable.

(4) Breaks down barriers. A predator works on the trust that has been established and may break down barriers further by exposing you, the victim, to pictures or materials that may at first make you uncomfortable. This is a common tactic because kids and teens are naturally curious about many things. The more a victim is exposed to, the less he or she will feel that it is wrong.

(5) Makes threats. Sometimes, but not always, a predator will make threats to the intended victim to keep the relationship a secret. Online threats are against the law. Think about it: Would a real friend threaten you or your family with harm?

(6) Meets face to face. The ultimate goal of an Internet predator is to get the intended victim to meet with him or her in person. You may believe that you can never be tricked by someone you meet online, but remember that predators make it their business to learn tactics to deceive their prey. NEVER meet anyone in person who you only know online.

Best Advice

Online friendships can be fun, but always consider what kind of information you are sharing.

If you notice that one of your online friendships is following the grooming process pattern, proceed very cautiously. There is no reason for an online friend to want to have a secret relationship with you and/or to force you to meet in person.

Let your friends and family know about people you meet online, and tell someone immediately if you are threatened or feel uncomfortable about anything that is said or sent online.

LESSON 5—Online Personal Safety Review and Action

Learning Objectives

- Define the 4 Rs of Internet safety.
- Identify others who could benefit from personal safety information and why.
- Apply knowledge of online personal safety to develop and distribute brochures on online safety.

Discussion

Use the reference half-page about the 4 Rs to review what has been learned in this unit.

- RECOGNIZE techniques used by online predators to groom and deceive their victims.
- REFUSE all requests for personal information, to keep the relationship secret, or to meet anywhere.
- RESPOND assertively. Log off, exit the program, or turn off the computer.
- REPORT suspicious or dangerous contact that makes you feel uncomfortable.

Review: Have students list types of personally identifying information, including:

- name
- age
- birth date
- Social Security number
- address
- phone number
- gender
- school name
- e-mail address

Ask students to state why it is risky to reveal this type of information online.

Be sure to cover that it can be used by others to harm us. Examples:

- cyber predators
- cyber bullies
- identity theft
- spam

Review with students what they should do if presented with the following scenarios:

- What should they do if a Web site they want to enter requests any of this information?
- What should they do if they are presented with a profile for IM or chat that requests this information?
- What should they do if they are talking to someone online who requests this information?

Emphasize that they should NEVER reveal information online without their parent's permission. However, with a parent's help, they may be able to safely fill out necessary forms and/or profiles.

Engage students in a discussion of the following:

- Prior to receiving this Internet safety information, were they making mistakes online in revealing personal information?
- Do they know others who could benefit from online personal safety information?
- Why is online safety an important message for their peer group?
- Should adults like teachers and parents have access to this type of information?
- Why? (Adults are especially at risk for identity theft when putting personal information on the Internet.)
- Name some good ways to relay this information to others?

Peer-to-Peer Activity

To accommodate different classroom environments, choose one of the following options: for classrooms with computers or for classrooms without computers.

Advise students that they are now going to participate in an activity to disseminate information about staying safe online to others. Divide students into small groups. Provide students with copies of the brochure activity handouts.

With Computers

Students access their choice of a desktop-publishing program for making brochures. (A sample template with instructions for completing a brochure in MS Word is included with your curriculum materials.)

- Students design a brochure to provide information about personal safety.
- Students incorporate information from activity sheets and discussions.
- Print brochure.
- Proceed to Discussion 3.

Without Computers

- Provide students with materials to make a brochure (paper, markers, crayons, etc.).
- Students design a brochure to provide information about personal safety.
- Students incorporate information from activity sheets and discussions.
- Proceed to Discussion 3.

Discussion 3

- Students present their brochures to the class.
- As a class, decide which brochure is the most informative and creative.
- Make plans to copy the brochure and distribute. (Another option is to have multiple brochures utilizing all brochures students have created.)
- Where will the brochure have the most impact? Distribute at lunch, in library, with report cards, etc.
- Plan a distribution day.

Wrap-Up Discussion

- Guide students in a discussion about what they have learned and why Internet safety is important. Be sure all areas are addressed, including:
  - > choosing a screen name

> choosing a password

> not revealing information

> consequences of actions

- Discuss ways in which students can distribute brochures. Suggestions: Hand out at lunchtime, send home with students, set up booth with brochures at open house, etc.
- Discuss why it is important to discuss cyber safety issues with parents.
- Encourage students to make a difference in their school when it comes to cyber safety Issues by registering at **www.isafe.org** for additional activities, materials, and support concerning this issue.
- 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 support for students, teachers, and parents on Internet safety topics are available from i-SAFE Inc. at **www.isafe.org**.

Student directions:

- Finalize plans for brochure copying and distribution.
- Ask your teacher to submit an Implementation Plan by going to their My Info page and select "Brochure Distribution."
- Additional materials may be ordered from i-SAFE for this activity, if desired.
- Direct questions about implementing enrichment activities to **outreach@isafe.org**.
- Additionally, i-SAFE provides the i-MENTOR Training Network training videos to help students implement enrichment activities. These short videos provide specific "how-to" information about accomplishing i-SAFE outreach activities. Access the i-MENTOR Training Network by clicking on "Kids and Teens" at **www.isafe.org**.
- Distribute the brochures.
- Let i-SAFE know how your activity went. E-mail **outreach@isafe.org**.

Post-Assessment

Administer the post-assessment online at **www.isafe.org** by clicking on "Assessments" if this is your last lesson for i-SAFE. To verify school ID number, log in at **www.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** to share any unique ideas and/or experiences you had during implementation of this unit.

REMEMBER the 4 R's

www.isafe.org

RECOGNIZE

Recognize techniques used by online predators to deceive, groom, or intimidate their victims.

Grooming techniques to encourage an eventual face-to-face meeting:

- Establishes Similar Interests
- Builds Trust
- Encourages Secrecy
- Breaks Down Barriers
- Makes Threats

REFUSE

Refuse all requests for personal information, to keep the relationship secret, or to meet in person.

Refuse to provide personal information by phone or e-mail if you didn't initiate the communication.

RESPOND

Respond assertively by exiting the program, logging off, or turning off the computer.

REPORT

Report any suspicious or dangerous contact that makes you feel uncomfortable to a trusted adult.

REMEMBER the 4 R's

www.isafe.org

RECOGNIZE

Recognize techniques used by online predators to deceive, groom, or intimidate their victims.

Grooming techniques to encourage an eventual face-to-face meeting:

- Establishes Similar Interests
- Builds Trust
- Encourages Secrecy
- Breaks Down Barriers
- Makes Threats

REFUSE

Refuse all requests for personal information, to keep the relationship secret, or to meet in person.

Refuse to provide personal information by phone or e-mail if you didn't initiate the communication.

RESPOND

Respond assertively by exiting the program, logging off, or turning off the computer.

REPORT

Report any suspicious or dangerous contact that makes you feel uncomfortable to a trusted adult.

Brochure Creation and Distribution

Grab people's attention and educate them at the same time!

Your Goal Should You Choose to Accept It:

You've been learning about Internet Safety – Now its time to make sure your peers, parents, and faculty understand the issue also.

Materials/Preparation

- Background knowledge on Internet safety concepts
- Computer with Internet access (recommended)
- Materials of choice for developing brochures (Desktop Publishing program, paper, etc.)
- A means to copy brochures for distribution

The Plan

Take a minute and think about the following – the questions will help guide you in your brochure creation.

- Review what you know about personal safety on the Internet.
- Who will this information most benefit? How can you make sure they read it?
- What information is critical when it comes to understanding how to safely and securely interact online?
- How can you grab people's attention and make them listen to your important message?

Develop and distribute brochures

- Decide who the target audience for the brochure distribution will be—example: parents, students, public at large (or even all three!)
- Design a brochure, or a series of brochures, to relay information on your topic
- Use materials of choice to create brochures
- Make plans to copy the brochure(s) and distribute
- Figure out where the brochure will have the most impact – plan distribution there (i.e. distribute in cafeteria at lunch, after a Parent Open House, During a Faculty meeting, etc.) Make sure you have permission for your distribution.
- Copy brochures
- Plan a distribution day
- Distribute brochures

Verification

Let i-SAFE know. Briefly document your success with this project and e-mail to **outreach@isafe.org**. Include dates the work was done and a copy of the finished product if possible.