

Staying Safe Online

Session Overview

This session invites high school students to explore ways to recognize danger on the internet.

Session Schedule

- Welcome and Community Builder 15 minutes
- Introduction to the Issue 15 minutes
- Understanding the Issue 15 minutes
- Short Break 10 minutes
- Exploring the Issue 30 minutes
- Addressing the Issue 30 minutes
- Closing Comments and Prayer 5 minutes

Learning Outcomes

- The participants will explore ways to maintain their privacy and safety while online.
- The participants will evaluate their current level of online safety and explore ways to become safer while online.

Preparation

- Gather the following items:
 - ▶ Computer with large screen or connected to an LCD projector or television monitor. You will also need Internet access.
 - ▶ *Tracking Teresa* video from the NetSmartz website (<http://www.netsmartz.org/resources/reallife.htm>)
 - ▶ Newsprint and markers
 - ▶ Copies of resource 1, *How Safe Are You*, one for each participant
 - ▶ Pencils or pens, one for each participant

- On newsprint write the following acronyms:

DVD	SCUBA	AD
ATM	IQ	ISBN
MC	PI	PIN
PS	PR	SOS
SPF	TIP	JK
TBD	VIP	RIP
CD	LOL	TGIF
TTYL	DJ	TMI
BCC	UV	LCD
CEO	WWW	CIA
FBI	JPEG	NCAA

Welcome and Community Building (15 minutes)

1. Welcome the participants and invite them to divide into small groups of 5 to 6 people. Provide each group with a sheet of newsprint and a marker. Refer the groups to the listing of acronyms posted on the newsprint you prepared earlier. Let the groups know that the rules to this game are simple, the team with the most defined terms at the end of the designated time - wins. Tell the groups that they have only a few minutes to determine what each common acronym stands for. Instruct them to write acronyms and the corresponding definition on the newsprint provided. Let them know they will have no more than 7 minutes. Then start the game.
2. Call time when 7 minutes has expired and then provide the participants with the correct definitions for each. The table below offers the corresponding response to each acronym:

DVD	Digital Video Device
SCUBA	Self Contained Underwater Breathing Apparatus
AD	Anno Domini
ATM	Automated Teller Machine
IQ	Intelligent Quotient
ISBN	International Standard Book Number
MC	Master of Ceremonies
PI	Private Investigator
PIN	Personal Identification Number
PS	Post Script
PR	Public Relations
SOS	Save Our Souls
SPF	Sun Protection Factor
TIPS	To Insure Prompt Service
JK	Just kidding
TBD	To Be Determined
VIP	Very Important Person
RIP	Rest in Peace
CD	Compact Disk
LOL	Laugh Out Loud
TGIF	Thank God It's Friday
TTYL	Talk to You Later
DJ	Disc Jockey
TMI	Too Much Information
BCC	Blind Carbon Copy
UV	Ultra Violet
LCD	Liquid Crystal Display
CEO	Chief Executive Officer
WWW	World Wide Web
CIA	Central Intelligence Agency

FBI
JPEG
NCAA

Federal Bureau of Investigation
Joint Photographic Experts Group
National Collegiate Athletic Association

3. Ask each group to total up the number of correct acronyms they guessed, and invite everyone to acknowledge the winning team with a round of applause.

Introduction to the Issue (15 minutes)

1. Ask the participants the following questions and invite a few responses. Note the responses to both questions on separate sheets of newsprint.
 - a. Besides the creation of a "new language" what are some of the other benefits of Internet access and communication?
 - b. What are some of the risks of Internet access and communication?
2. Invite the participants to gather with their small group members. Ask each person to think of two interesting statements about themselves that are true. Also ask them to come up with one statement that is believable but not true. Allow a few minutes for the participants to do some thinking.
3. Invite the participants one at a time in their small groups to share their three statements. Note that it is the task of the remaining group members to determine which two statements are true and which is not. Have the groups proceed until everyone has shared their statements and the guessing has been completed.
4. Proceed by offering the following session introduction:
 - a. Even though many of you know one another it is likely that some (if not all) of you were not always able to correctly guess which of your group's member's statements was false. So how can we expect to know when someone we communicate with online is telling the truth? Even though we might think we know someone well online, we really have no way of knowing whether the person is telling the truth or has our best interest in mind.
 - b. It's true that the Internet provides some awesome benefits to each of us, the benefits some of you mentioned earlier as well as others not mentioned. But there are also risks, and dangers

that we can encounter when we are online. Consider these statistics.

- In January of 2005 in Lafayette, Louisiana, a 16-year-old girl was attacked by a 37-year-old man who read her profile on a popular social networking site and tracked her down at her after-school job. (Myers, J.C. "Teens' MySpace Website a Boon for 'Predators.'" Times Argus. February 13, 2006).
 - 64% of all teens say that teens do things online that they wouldn't want their parents to know about (Family, Friends & Community: Protecting Teens Online, Amanda Lenhart. March 17, 2005. Pew Internet & American Life Project. December 12, 2005).
 - Almost one in eight youth ages 8-18 discovered that someone they were communicating with online was an adult pretending to be much younger (Internet safety: Realistic Strategies & Messages for Kids Taking More and More Risks Online. Polly Klaas Foundation. February 17, 2006).
 - One-third of youth ages 8-18 have talked about meeting someone they have only met through the Internet (Omnibuzz.Research. Nationwide Poll of Teens and Tweens. Polly Klaas Foundation, December 21, 2005).
 - 30% of teenage girls polled by the Girl Scout Research Institute said they had been sexually harassed in a chat room. (Girl Scout Research Institute. The Net Effect: Girls and New Media. 2002).
 - One third of Internet users age 10-17 were exposed to unwanted sexual material (University of New Hampshire. Online Victimization of Youth: Five Years Later. National Center for Missing and Exploited Children. August, 2006).
 - Authorities say teens are finding trouble in the social networking environment where millions of people, can in seconds, find out where they go to school, learn their interests, download their pictures and instantly send them messages ("Teens Putting Themselves at Risk Online." Associated Press. *USA Today* 5 February 2006).
- c. This is why we really must pay attention to the kinds of conversations and contact we engage in while online. We must also be mindful of the kind information we give out about ourselves.

- d. During our time together today, we'll be exploring the issue of online safety, and how to be more diligent about keeping safe from people, and companies who seek to manipulate, mislead, and harm us.

Understanding the Issue (15 minutes)

1. Invite the participants gather around the computer monitor or television screen. Let them know that they are about to view a videos which highlights how easy it anyone can become a target or online manipulation, exploitation and crime.
2. Watch the video.
3. Ask the participants the following questions, inviting a few to respond aloud:
 - a. What was most surprising to you about the video?
 - b. Based on the information presented in the video, how many of you can confidently say that you are using safe internet practices?

Exploring the Issue (30 Minutes)

1. Invite the participants to gather with their small group members. Tell them that you will be reading a few case scenarios and their task will be to discuss possible solutions to each situation. Note that the small groups will have a few minutes to discuss possible solutions and then will be invited to share with the entire group their ideas.
2. Read aloud each scenario. Throughout the process, give the groups about 5-7 minutes to discuss possible solutions, and then invite each group to offer aloud a few of the solutions they have determined. Continue this process until all scenarios have been read and discussed. (Note below each scenario is a listing of possible solutions suggested by the Center for Missing and Exploited Children. If these suggestions are not included in the ones determined by the participants, be sure to note them as options as well).

Scenario #1: Karli recently made a posting on a newsgroup that included her full name, telephone number, and E-mail address. After listening to the Internet safety lesson given by her teacher, she realizes that she probably doesn't want that information posted online. What should she do?

Solution: Karli should first tell her parents or guardian. Together they should check with the newsgroup and see if they can remove her posting. If not, they should contact the newsgroup administrator, and ask the administrator to remove Karli's posting.

Scenario #2: Bryce is opening a new e-mail account and trying to come up with his e-mail address. He is 17; plays on both the school and city baseball teams; plays drums in a band; and is a huge Yankees fan, especially since he lives in New York. What would be a good e-mail address for Bryce? What should he avoid including in his e-mail address or screen name? Why?

Solution: Bryce should not use his first or last name in his e-mail address or screen-name since these are obvious identifiers. He should not include his age or birth year either. He may wish to have a name associated with his love of baseball, but shouldn't include his team name or the school or city for which he plays, nor give any other clues about where he lives. He also might want to consider names that involve his interest in music as long as he doesn't include the name of his band or any other information that could enable someone he doesn't know to discover his identity.

Scenario #3: Rachel has had a really rough time this past year. It seems like no one is there for her anymore. Feeling lonely, Rachel has been spending a lot of time online. She met a girl named Cristina there. Rachel feels like she and Cristina have a lot in common. Cristina is always so sympathetic and a great listener. Just last night Cristina mentioned that she would be in Rachel's hometown in a week and suggested that they meet. Rachel thinks that would be a lot of fun. Why not finally meet this person she has gotten to know so well? Cristina trusts her — Cristina has told her everything from her shoe size to where she shops to her favorite music to where she lives and what her parents do for a living. Cristina doesn't understand why Rachel has to be so protective of her personal information. Rachel agrees to meet with Cristina, but now she is having doubts. What should she do?

Solution: First of all, Rachel has no proof that Cristina is who she says she is. It is easy online to pretend to be a teenager even if in reality you are a middle-aged man. Rachel has good reasons to have her doubts. She should not meet Cristina and immediately tell her parents what has been going on.

Scenario #4: Jeremy is a huge fan of baseball cards. Through a baseball-card site, he has become friends with another baseball-card fan named

Thomas. Both Thomas and Jeremy live in the same city, and they decided online that they should meet in person so that, rather than having to type about their different card collections; they can compare and trade them in person. Jeremy knows that it is a bad idea to meet someone in person he only knows online, but he is certain Thomas is harmless. What should he do?

Solution: Jeremy should tell his parents about the situation. If they decide it is okay to try to meet, Jeremy's parents should call Thomas' parents. If the meeting still seems okay after that conversation, Jeremy's parents should go with Jeremy to meet Thomas and his parents in a public place such as a popular park. To avoid this type of situation in the future, Jeremy is better off meeting people to trade cards through organized events.

(The above scenarios and solutions are taken from the *Tracking Teresa* session for high school students found at www.netsmartz.org. ©1998 and 2003, National Center for Missing & Exploited Children.)

Addressing the Issue (30 minutes)

1. Once again, provide each group with a blank sheet of newsprint and a marker or two. Ask the groups to spend some time discussing and determining at five to ten practical guidelines for staying safe online. Allow about 10 minutes for them to complete this task.
2. Gather the groups and invite each to share a few of their ideas. If any of the following ideas are suggested, be sure to include them in the overall discussion:
 - Make sure your screen names does not reveal too much about you; for example, your screen names should not include clues to your real name, age, hobbies, or other information that predators can use.
 - Keep personally identifiable information private. That includes your name, school, social security number, address, age, birthday, phone number, and the names of your friends or family members.
 - Be careful where else you put information that is publicly accessible, such as school and personal web sites, and friends' web sites.
 - Watch what information you share indirectly, such as your school mascot, when your favorite band played in the area,

or any other information predators could use to figure out where you live.

- Chat online only with people you know in the real world, such as friends from school and community groups, or members of your family. Remember if don't know someone in the real world, you don't know them.
- Don't break the rules for someone. If someone seems too good to be true, they usually are. Always remain in control of the situation.
- If you think that you are being harassed or stalked, never reply to the harasser. Make sure you let an adult know what's going on. And if you're really afraid, report it to your parents and then to the police.
- Remember that just because someone gives you their personal information or sends you an e-mail, it doesn't mean that you have to give them your information.
- Never get together with someone you "meet" online.

(Adapted from www.teenangels.org)

3. Distribute a copy of resource 1, *How Safe Are You?* and a pen or pencil to each participant. Let them know that the handout will help them evaluate their own online practices. They may complete the evaluation either on their own or in pairs. Encourage them to be completely honest, even if some of their online practices have not always been smart or safe. The goal of the activity is for them to evaluate their current practices and set up making a plan to change those that are not safe. Let them know that they will not be required to share their evaluation with anyone (other than their partner, if one was chosen). Allow about 10 minutes for them to complete this task.

Closing Comments and Prayer (5 Minutes)

1. Offer a summary of the session using your own observations of the time together. You might also invite one or two participants to share their own reflections.
2. Conclude by inviting the participants to bow their heads in prayer and then pray the following prayer aloud.

God of the Universe, Lord of all time and space,
Your almighty Word leapt down from the farthest starry
Heavens to save us from slavery in Egypt

And to fashion us into a holy people of truth and justice.
The finger of your almighty power casts out evil
And restores order to the jumbled chaos of this fragile world.
Your Incarnate Word enters everything human,
Speaking parables of comfort to the needy
And those held captive by fear
And inviting disciples to proclaim good news everywhere.

Bless again this day the mysterious computer
Which awaits your power and [our] human effort.
Grant wisdom, knowledge and a clear memory to [our]
mind[s] as [we] sit before this new creature of your infinite
power.

Bless [our] heart[s] with endless patience whenever needed.
Guide [our] hands that [we] may be your faithful servant in
every key [we] press.
Enable [our] limited efforts to bring glory to your Name
and blessings to your people everywhere.

Delete [us] not from your Kingdom and save [us] from all fear
and from all error of sin and ignorance.
[We] whisper this prayer, mindful of the needs of all through
the power of your Word and the life-giving energy of your
Spirit.

Amen.

Written by Most Reverend Richard J. Sklba and accessible at
www.archmil.org/ourfaith/praycomputer.asp

Additional Resources for Exploring the Issue of Online Safety

www.cybersmart.org. This site develops curricula and training programs designed to help educators empower students to take full advantage of computers and the Internet. The site contains Internet safety information for students, parents, and educators, and includes lesson plans, activity sheets, downloadable posters, and safety tips.

www.getnetwise.com. This site is a resource for parents to educate themselves and their children about how to use the Internet safely.

www.missingkids.com. This site provides information on general child safety and Internet safety for children, parents, educators, law enforcement, and the community.

www.safeteens.com. This site provides tips, advice, links, and suggestions to help make the online experience fun and productive.

Resource 1

How Safe Are You?

Does your screen name reveal too much about you? (i.e, your real name, age, hobbies, school, town, or other information that can be used to harm you)

yes no

Are any of the following pieces of information about you posted anywhere online? (i.e., your name, school, social security number, address, age, birthday, phone number, and the names of your friends or family members)

yes no

Is any information publicly accessible, from other internet sites such as school web sites and friends' web sites?

yes no

Do you share information such as your school mascot, when your favorite band played in the area, or any other information someone could use to figure out where you live?

yes no

Do you chat online with people you do not know in the real world?

yes no

Have you ever given out personal information about yourself to someone you have not met -face-to-face?

yes no

If you answered "yes" to even one of the above questions, you need to rethink your Internet interactions. Below write down the action steps you will take to become a safer Internet user.

Action:

Action:

Action: