



MODULE 13: Internet Safety And Fun

Learning Goals

During this module, participants will:

- ◆ Learn how to determine the appropriateness and validity of the content of websites.
- ◆ Understand how to protect themselves against Internet fraud.
- ◆ Brainstorm how to establish healthy boundaries in Internet-based relationships.

MODULE 13: INTERNET SAFETY AND FUN

DEFINE THE ISSUE

In September of 2001, the National Runaway Switchboard added “Internet relationship” to its list of issues identified during crisis calls. Since then, the Internet has frequently been discussed in calls dealing with runaway youth. Whether it is a parent who wonders how to access a runaway child’s email account to check activity or a youth who considers leaving home to stay with someone they met online, the Internet plays a large role in many of our calls.

While we at NRS recognize the dangers that may face youth online—from online predators to online bullying to identity theft—we cannot ignore the fact that the Internet is an ever-growing resource of information and social connections for many youth. What better place to turn for answers to questions that are difficult to ask in person? For networking with people across the globe? For access to every sort of information?

NRS recognizes that using computers at home and in school is routine today. We also recognize that there are many “experts” in the field of Internet safety for children and adolescence—some of them are listed at the end of this module. Module 13 incorporates some of the lessons about the Internet that youth may receive in other areas of their life. Participants will use real life scenarios to practice these lessons.

ICONS:

For further details, see the Introduction Module.



MODULE 13: INTERNET SAFETY AND FUN

MODULE ACTIVITIES

ACTIVITY	TIME	METHODOLOGY
A. Getting To Know The Net	15 minutes	Discussion/Activity
B. Tips To Avoid Internet Fraud	10 minutes	Discussion/Activity
C. Keeping It Real While Playing It Safe On The Internet	20 minutes	Discussion/Activity



Total time required: **45 minutes**



MATERIALS

- ◆ Poster paper or chalk/dry erase board
- ◆ Markers or chalk
- ◆ 3 x 5 note cards or blank pieces of paper for each participant
- ◆ "Is This Legit?: How To Evaluate Websites, Page 1" handout
- ◆ "Is This Legit?: How To Evaluate Websites, Page 2" handout
- ◆ "Tips To Avoid Internet Fraud" handout
- ◆ Copy and cut "Internet Role Play Scenarios" handout
- ◆ "Keeping A Healthy Distance" handout



Consider showing the curriculum companion film "1-800-RUNAWAY".



If you'd like to incorporate an Internet safety pledge in this module, see examples at www.webwisekids.org and www.netsmartz.org/resources/pledge.htm.



MODULE 13: INTERNET SAFETY AND FUN

ACTIVITY 13A. GETTING TO KNOW THE NET

15 minutes



- INTRODUCE** the topic of the Internet.
- STATE** *When used in a safe way, the Internet can be a great place to learn, to express yourself, and to keep in touch with friends.*
- ASK** *How are you personally involved with the Internet?*
- WRITE** responses on poster paper or a chalk/dry erase board. Examples might include the following:
- Email with friends/relatives
 - Instant-messaging (IM-ing)
 - Chatting with friends
 - School-related research
 - Reading/watching the news
 - Looking up directory information (e.g., WhitePages.com; YellowBook.com)
 - Using online social networking sites (e.g., MySpace.com; Facebook.com; Xanga.com; etc.)
 - Online journaling/blogging
 - Buying stuff (e.g., books, music, clothes)
- STATE** *As we've seen, the Internet can serve many purposes. Everyday more people rely on it. Unfortunately, not everyone on the Internet has the best of intentions. In fact, we often hear stories about people who are victimized through the Internet. For example, computer viruses are spread through emails, and people scam others out of money through false advertisements on websites. In more extreme cases, we hear of people being abducted by others they've met through the Internet. Unfortunately, victimization through the Internet occurs more often than we realize.*
- The best way to avoid becoming a victim on the Internet is to become educated on some basics. We're going to spend the next few minutes becoming more Internet savvy.*
- HAND OUT** "Is This Legit?: How to Evaluate Websites, Page 1" worksheets.
- ASK** *Would someone like to volunteer reading the first item on the worksheet?*
- SELECT** a volunteer. Keep selecting volunteers until all items have been read. A copy of the worksheet is shown below:



Common Domain Suffix	Description
.com	Commercial site. Websites that are sometimes intended to sell a product. Some websites require you to create a log-in name to purchase a product. Not always trustworthy.
.edu	Educational Institution. Educational institutions, from elementary schools to universities. Material from a department or research center at the educational institution may be credible. However, students' personal websites are less likely to be credible.
.gov	US Federal Government. The information posted from sites ending in .gov is considered to be from a credible source.
.mil	Military. This domain suffix is used by the various branches of the US Armed Forces.
.org	Non-profit Organization. Information on these sites may strongly advocate specific points of view like being Pro-Life versus Pro-Choice, or may solicit for donations.
.net	Network. This domain is a "catch-all" for sites that don't fit into any of the domains listed above. Information from these sites should be given careful scrutiny.

STATE *Let's assume you're browsing websites using a web browser like "Internet Explorer," "Safari," "Mozilla Firefox" or "Netscape." Every site that you view will have its own web address that ends in one of the domain suffixes (or simply, "domains") listed on the "Is It Legit?" worksheet.*

ASK *What domains have you seen with the different endings we've just reviewed?*

ALLOW 2-3 minutes for responses. Examples might include the following:

- www.amazon.com, www.ebay.com, www.google.com, www.yahoo.com
- www.ucsf.edu, www.yale.edu, www.depaul.edu
- www.cdc.gov, www.firstgov.gov, www.whitehouse.gov
- www.navy.mil, www.army.mil, www.af.mil
- www.1800RUNAWAY.org, www.redcross.org, www.nationalsafeplace.org
- www.youthcourt.net, www.sbcglobal.net

ASK *What do you suppose is the purpose of these domain suffixes?*

ALLOW 1-2 participants to respond.



PROVIDE The correct answer, if necessary: To categorize sites according to their content.

ASK *A movie theatre's web address would likely end with what domain?*

ALLOW 1-2 participants to respond.

PROVIDE The correct answer, if necessary: Site would likely end with .com because it's a business.

STATE *Good job. Now I'd like us to spend another few minutes going over some basic guidelines that will help determine whether the content of a website can be trusted.*

HAND OUT "Is This Legit?: How to Evaluate Websites, Page 2" worksheets.

STATE *Please take a minute or two and review the information on the handout I just gave you.*

ALLOW 1-2 minutes for participants to review the handout.

ASK *Would someone like to volunteer reading the first item on the worksheet?*

SELECT a volunteer. Keep selecting volunteers until all items have been read. A copy of the worksheet is shown below/on the next page:

- Does the website give credit to a specific author?

Anyone can publish anything on the web. So, it's important to know who is responsible for the information on the website. What are the author's credentials? Is he or she an expert in the topic?

- How up-to-date is the website? (Including links to other websites)

Outdated information may be incorrect or incomplete, so it's important to know when the information on the website was compiled. Responsible website creators (also called Webmasters) will state when the website was last updated at the bottom of the screen. If a website has links to sites that are no longer active, you may also want to question whether or not the website is up-to-date.



- Are you confused by who owns the website?

Sometimes web addresses can be long and appear not to make much sense. The best way to find out who is responsible for the site is to truncate, or cut down, the address to its "root." The root is the very beginning of the web address that usually ends in a domain suffix. For example, the root address of the National Runaway Switchboard is 1800RUNAWAY.org

- How does the information listed on the website compare with other similar websites?

Comparing information from one website with other information sources can help you avoid relying on information that may be incorrect.

ASK

DISCUSS

Do you have any questions or comments?
responses.



MODULE 13: INTERNET SAFETY AND FUN

ACTIVITY 13B. TIPS TO AVOID INTERNET FRAUD

10 minutes



HAND OUT

a 3 x 5 card or blank sheet of paper to each participant.

STATE

I'd like you to write the following information on the card/paper I just gave you. Please write:

- Full name
- Address
- Telephone number (including cell phone number)
- Name of school (if applicable)
- Social Security number
- Date of birth and age
- Height and hair color
- Any extracurricular activities (e.g. sports teams, clubs, jobs)
- Email address and password (if applicable)

COLLECT

the cards or pieces of paper. Ask the following questions as needed to promote discussion (some may have been raised during the activity).

ASK

- *Thank you for writing down the information. Is there anyone who didn't write down all the information I asked for? Why?*
- *Did anyone question why I was asking for this information? If yes, at what point did you start to have questions?*
- *Who wrote down all of the information? Why?*
- *What do you think could happen to this information if it ends up in the hands of the wrong person?*

DISCUSS

responses.

SHRED/TEAR

the cards or pieces of paper. **DISCARD** them so they cannot be retrieved.

STATE

We should all be careful with the information we give people either in person, over the phone, or on the Internet. This information is very valuable and can cause harm if it lands into the hands of an untrustworthy individual or company.



STATE

Internet fraud has become a problem in the U.S. and worldwide. Typically, Internet fraud occurs when you share important information about yourself with a source you believe is legitimate but isn't.

The best way to prevent Internet fraud is to keep your personal information private unless you can guarantee that the individual or website is legitimate.

The personal information I had you write down should be kept private and confidential.

What are some other forms of identification should you keep private and confidential?

DISCUSS

responses. Examples include the following:

- *School name*
- *Pictures*
- *Debit/credit card numbers*
- *Bank account number*
- *Driver's license/State ID card number*

STATE

You all came up with some great ideas for information that should be kept private. Let's find out which are most important to keep private.

HAND OUT

"Tips to Avoid Internet Fraud" worksheets.

ASK

Would someone like to volunteer to read the first item on the worksheet?

SELECT

a volunteer. Keep selecting volunteers until all items have been read. A copy of the worksheet is shown below:

Guard your financial information. Provide your credit card or bank account number only when you are actually paying for something.

Keep your social security number confidential. It's the key that unlocks your identity. Don't give it to anyone unless you're sure who it is and why it's necessary to provide it.

Beware of imposters. Be suspicious if someone contacts you claiming to be from a company that you do business with and asks you to provide information they should already have. Before responding, contact the company directly to confirm that the call or email is from them.

Memorize your passwords and PIN numbers. Don't leave them in your wallet or on your desk where someone else could find them.



Stay safe online. Don't send sensitive information such as credit card numbers by e-mail; it's not secure. Look for clues about security on websites (in the form of an icon that resembles a padlock). At the point where you begin to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shttp." Your Internet browser may also show that the information is being encrypted, or scrambled, so no one who might intercept it can read it. But while your information may be safe in transmission, that's no guarantee that the company will store it securely.

OTHER TIPS TO AVOID FRAUD WHILE YOU'RE OFFLINE

Keep your U.S. mail safe. Your U.S. mail contains account numbers and other personal information. Collect it promptly from your mailbox and ask the post office to hold it if you're going away. Send bill payments from the post office or a public mailbox, not from home.

Lock it up. Keep your personal information locked up at home, at work, at school, and other places so others won't have easy access to it.

Check your credit reports regularly. If you find accounts that don't belong to you or other incorrect information, follow the instructions for disputing those items.

STATE

So far, we talked about becoming more knowledgeable about websites and finding out how to avoid fraud that could affect you legally or financially. We're going to switch gears and begin to talk about how to avoid other types of fraud that can lead to more physical harm.

ASK

Do you have any questions or comments?

DISCUSS

responses.



MODULE 13: INTERNET SAFETY AND FUN

ACTIVITY 13C. KEEPING IT REAL WHILE PLAYING IT SAFE ON THE INTERNET

20 minutes



- INTRODUCE** the topic of healthy Internet relationships.
- STATE** *People of all ages are turning to the Internet to connect with other people worldwide. People connect through shared perspectives and interests or as a means of feeling valued.*
- A great aspect of the Internet is that we can be anonymous when we interact with others through social networking websites like MySpace.com or chat rooms. However, the anonymity of the Internet is also one of its most dangerous aspects - especially if we find ourselves chatting with people who don't turn out to be who they say they are.*
- We're going to do some role playing now.*
- ASK** *Who would like to volunteer reading for the two roles in our role play?*
- SELECT** 2 volunteers.
- SELECT** which of the 3 scenarios to use.
- GIVE** one volunteer SCENARIO A, which he or she will read to him or herself and then act out. The other volunteer participant will get SCENARIO B, which he or she will read aloud and act out.
- STATE** *The role play will take place aloud, but it is meant to be an on-line conversation.*
- ALLOW** volunteers to review their scenarios, then give them 1-2 minutes to act out the role play.
- ASK** *After seeing this role play, what are your reactions?*
- DISCUSS** responses.
- ASK** *What would you do in this person's situation?*
- DISCUSS** responses.
- ASK** *What would you have done to prevent being in this situation?*
- DISCUSS** responses.
- ASK** *What were some of the bad decisions, if any, that were made throughout this situation?*
- DISCUSS** responses.



STATE *According to a popular website where people can meet and socialize, there are some important tips to remember when meeting people on the Internet.*

HAND OUT "Keeping A Healthy Distance" worksheets.

ASK *Would someone like to volunteer to read the first item on the worksheet?*

SELECT a volunteer. Keep selecting volunteers until all items have been read. A copy of the worksheet is shown below:

Be Careful What You Post. Anyone with access to a computer can see the information or pictures you post online. This means your friends, teachers, boss, and even your parents! Carefully consider what you post, including your address or location, screen names, and other identifying information.

Be Careful Who You Trust. One captivating thing about the Internet is its anonymity. It's a place where people can be who they want. You may think you know someone based on their personality, profile, or picture, but they may actually be someone entirely different. Use caution when getting to know someone online. And always be careful when meeting an online friend in person. Consider what ways you can be safe.

Be Careful What You Say. Teasing and bullying online is just as bad as it is in person. And some of it is even illegal. Report negative behavior to a trusted adult or to the authorities (police, teacher, Webmaster).

ASK *Do you have any questions or comments?*

DISCUSS responses.

STATE *If you'd like to visit a youth-friendly resource online, go to the National Runaway Switchboard's website at <http://www.1800RUNAWAY.org> or www.switched-onmag.org.*



MODULE 13: INTERNET SAFETY AND FUN

SUMMARY

STATE

- *The Internet can be a great place to learn, to express oneself, and to keep in touch with friends.*
- *The kind of source responsible for the ownership of a website can help us decide if it is trustworthy.*
 - *Sites with extensions of .com or .net may or may not be trustworthy.*
 - *Sites that end in .gov and .edu are usually trustworthy.*
 - *Sites with .org endings often advocate for a particular point of view, such as www.1800RUNAWAY.org.*
- *Other indicators that a website is legit are when the site:*
 - *Credits a specific author*
 - *Is up to date*
 - *Clearly indicates who owns it*
 - *Compares with similar sites*
- *Tips for avoiding Internet fraud include:*
 - *Guarding credit card, banking, and social security numbers*
 - *Being suspicious of people asking for information they should already have*
 - *Keeping PINs and passwords private*
 - *Never sending sensitive information in an e-mail*
 - *Keeping U.S. mail safe*
 - *Checking credit reports*
- *While we can trust most people we meet online, we should still be careful in what we post, who we trust, and what we say.*



MODULE 13: INTERNET SAFETY AND FUN

HANDOUTS AND WORKSHEETS

- A. Is This Legit? : How To Evaluate Websites, Page 1
- B. Is This Legit? : How To Evaluate Websites, Page 2
- C. Tips To Avoid Internet Fraud
- D. Internet Role Play Scenarios
- E. Keeping A Healthy Distance

REFERENCES

Cyber Smart offers a curriculum addressing the interconnected challenges and solutions involved in responsible and safe technology use (http://www.cybersmartcurriculum.org/lesson_plans).

Generic Top Level Domains (n.d.) Retrieved 2006 from <http://www.iana.org/gtld/gtld.htm>

(Borrowed and adapted with permission from) The **National Consumers' League's Fraud Center: Internet Fraud Tips** (n.d.) Retrieved 2006 from <http://www.fraud.org/tips/internet/idtheftavoid.htm>

National Runaway Switchboard (2001). *Runaway Prevention Curriculum For Classroom and Community Educators*, Chicago, IL: NRS

NetSmartz411 is an online resource for learning about Internet safety, computers, and the web. It also offers a pledge for youth to take on internet safety (<http://www.netsmartz.org>).

Web Wise Kids is a website for youth that equips youth to make wise choices online. It also offers a pledge for youth to take on internet safety (<http://www.webwisekids.org>).

RESOURCES

BlogSafety.com is where parents, teens, educators, and experts discuss and learn about safe blogging and social networking (<http://www.blogsafety.com>).

Child Safety Network offers information and resources on internet and computer safety (<http://www.csn.org/index.jsp>).

Enough Is Enough emerged in 1994 as the national leader on the front lines to make the Internet safer for children and families (<http://www.enough.org>).

GetNetWise is a public service that offers resources needed to make informed decisions about the use of the Internet (<http://www.getnetwise.org>)



Internet Crime Complaint Center is a vehicle to receive, develop, and refer criminal complaints regarding cyber crime run in partnership with the FBI and the National White Collar Crime Center (<http://www.ic3.gov>).

i-SAFE Inc. is a website that offers safety education dedicated to protecting the online experiences of youth everywhere (www.i-safe.org).

National Runaway Switchboard is the federally-designated national communication system (hotline and website) for runaway and homeless youth. Youth and family members call 1-800-RUNAWAY or access the website to work through problems and to find local help (<http://www.1800RUNAWAY.org>).

NetSmartz® is an interactive, educational safety resource from the National Center for Missing & Exploited Children® and Boys & Girls Clubs of America for children, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet (<http://www.netsmartzkids.org>).

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help be on guard against Internet fraud, secure computer information, and protect personal information (<http://onguardonline.gov/index.html>).

Safe Teens offers information and resources for teens and parents on internet safety (<http://www.safeteens.com>).

Stay Safe Online provides free and non-technical cyber security and safety resources to the public so consumers, small businesses, and educators have the know-how to avoid cyber crime (<http://www.staysafeonline.info>).

WiredSafety provides resources, information, and education to Internet and mobile device users of all ages (<http://www.wiredsafety.org>).



IS THIS LEGIT? :

HOW TO EVALUATE WEBSITES

Page 1

Directions: Refer to this guide when you're trying to determine what kind of source is responsible for the ownership of a website.

DOMAIN SUFFIXES	
Common Domain Suffixes	Descriptions
.com	Commercial site. Websites that are sometimes intended to sell a product. Some websites require you to create a log-in name to purchase a product. Not always trustworthy.
.edu	Educational Institution. Educational institutions ranging from elementary grades to the university. Material from a department or research center at the educational institution may be credible. However, students' personal websites are less likely to be credible.
.gov	US Federal Government. The information posted from sites ending in .gov is considered to be from a credible source.
.mil	Military. This domain suffix is used by the various branches of the US Armed Forces.
.org	Non-profit Organization. Information on these sites may strongly advocate specific points of view like being Pro-Life versus Pro-Choice, or may solicit for donations.
.net	Network. This domain is a "catch-all" for sites that don't fit into any of the domains listed above. Information from these sites should be given careful scrutiny!

Need to talk? Call us.
 1-800-RUNAWAY
National Runaway Switchboard
www.1800RUNAWAY.org



IS THIS LEGIT? :

HOW TO EVALUATE WEBSITES

Page 2

Directions: Refer to these guidelines to help you determine whether or not the content of a website is fact or fiction.

Does the website give credit to a specific author?

Anyone can publish *anything* on the web. So, it's important to know who is responsible for the information on the website. What are the author's credentials? Is he or she an expert in the topic?

How up-to-date is the website? (Including links to other websites)

Outdated information may be incorrect or incomplete, so it's important to know when the information on the website was compiled. Responsible website creators (also called Webmasters) will state when the website was last updated at the bottom of the screen. If a website has links to sites that are no longer active, you may also want to question whether or not the website is up-to-date.

Are you confused by who owns the website?

Sometimes web addresses can be long and appear not to make much sense. The best way to find out who is responsible for the site is to truncate, or cut down, the address to its "root." The root is the very beginning of the web address that usually ends in a domain suffix. For example, the root address of the National Runaway Switchboard is 1800RUNAWAY.org.

How does the information listed on the website compare to other websites with similar content?

Comparing information from one website with other information sources can help you avoid relying on information that may be incorrect.

Adapted with permission from **The CyberSmart! Education Company**,
www.cybersmartcurriculum.org/lesson_plans

Need to talk? Call us.
1-800-RUNAWAY
National Runaway Switchboard
www.1800RUNAWAY.org



TIPS TO AVOID INTERNET FRAUD

Guard your financial information. Provide your credit card or bank account number only when you are actually paying for something.

Keep your social security number confidential. It's the key that unlocks your identity. Don't give it to anyone unless you're sure who it is and why it's necessary to provide it.

Beware of imposters. Be suspicious if someone contacts you claiming to be from a company that you do business with and asks you to provide information they should already have. Before responding, contact the company directly to confirm that the call or email is from them.

Memorize your passwords and PIN numbers. Don't leave them in your wallet or on your desk where someone else could find them.

Stay safe online. Don't send sensitive information such as credit card numbers by e-mail; it's not secure. Look for clues about security on websites (in the form of an icon that resembles a padlock). At the point where you begin to provide your financial or other sensitive information, the letters at the beginning of the address bar at the top of the screen should change from "http" to "https" or "shhttp." Your Internet browser may also show that the information is being encrypted, or scrambled, so no one who might intercept it can read it. But while your information may be safe in transmission, that's no guarantee that the company will store it securely.

OTHER TIPS TO AVOID FRAUD WHILE YOU'RE OFFLINE

Keep your US mail safe. Your US mail contains account numbers and other personal information. Collect it promptly from your mailbox and ask the post office to hold it if you're going away. Send bill payments from the post office or a public mailbox, not from home.

Lock it up. Keep your personal information locked up at home, at work, at school, and other places so others won't have easy access to it.

Check your credit reports regularly. If you find accounts that don't belong to you or other incorrect information, follow the instructions for disputing those items.

ADAPTED WITH PERMISSION FROM THE **NATIONAL CONSUMERS LEAGUE'S FRAUD CENTER**,
www.fraud.org

Need to talk? Call us.
1-800-RUNAWAY
National Runaway Switchboard
www.1800RUNAWAY.org



INTERNET ROLE PLAY SCENARIOS

SCENARIO 1A: You are a member of a hate group. You're trying to draw in this new kid that's visited your webpage without scaring him/her off immediately. Use any convincing tactic you can to get him/her to meet up with you at school.



SCENARIO 1B: You have been grounded by your parents for getting in some legal trouble with your friends. You're not supposed to speak with those friends anymore—how realistic is that? You convinced your parents to allow you to keep your computer in your room because you've got a report you're working on and you need the Internet. Little do they know that you're chatting with some new people you've met. Hey, at least it's not your old friends, right?



SCENARIO 2A: You are a senior at East High School. You've met someone cool online and really want to meet up with him/her in person. You don't mean to come off as creepy, but you are really trying to pressure him/her into meeting you.



SCENARIO 2B: You are a new student at West High School and you're in your sophomore year. It's been hard to make friends part way through the school year. Plus, everyone seems to know each other from elementary and middle school. You've met someone who seems really neat online, but your parents won't let you date yet. You'd kinda like to meet up with this person, but you need to figure out a way to do it so your parents won't know.



SCENARIO 3A: You want people to sign this online petition about this so-called popular girl at school who you hate. She's made your life miserable by spreading rumors about you and your family, teasing you when the teacher isn't looking, and hitting on the person you like though she'd never go out with him. You will do anything—and say/write anything—to make people sign on.



SCENARIO 3B: Your parents finally got fast Internet at home and you're kind of new to the whole thing. You come across a student page for your school and notice something about a petition about a girl in your class. You're curious, so you click on it...



Need to talk? Call us.
1-800-RUNAWAY
National Runaway Switchboard
www.1800RUNAWAY.org



KEEPING A HEALTHY DISTANCE

- **Be Careful What You Post.** Anyone with access to a computer can see the information or pictures you post online. This means your friends, teachers, boss, and even your parents! Carefully consider what you post, including your address or location, screen names, and other identifying information.
- **Be Careful Who You Trust.** One captivating thing about the Internet is its anonymity. It's a place where people can be who they want. You may think you know someone based on their personality, profile, or picture, but they may actually be someone entirely different. Use caution when getting to know someone online. And always be careful when meeting an online friend in person. Consider what ways you can be safe.
- **Be Careful What You Say.** Teasing and bullying online is just as bad as it is in person. And some of it is even illegal. Report negative behavior to a trusted adult or to the authorities (police, teacher, Webmaster).

safety

Need to talk? Call us.
1-800-RUNAWAY
National Runaway Switchboard
www.1800RUNAWAY.org



Module 13: Internet Safety and Fun Pre and Post-Activity Worksheet

Initials:

Directions: Please put your initials at the top of the page and circle "pre" if you are taking the test before class or "post" if you are taking the test after class. Answer the following questions to the best of your ability!

What is your **gender**: _____ **Race/ethnicity**: _____ **Age**: _____

- _____ is a common Internet domain suffix for an educational institution.
 - .gov
 - .com
 - .edu
 - .mil
- Responsible webmasters will make sure a legit webpage is _____.
 - pretty
 - up-to-date
 - colorful
 - confusing
- What type of personal information is **NOT** always safe to give online?
 - Age or birthday
 - Address
 - Social security number
 - All of the above
- Which of the following **is** a way to avoid internet fraud?
 - memorize passwords and PIN numbers
 - send a credit card number through email
 - give a full address over instant messaging
 - give any information such as full name, phone number and social security number
- It is safe** to meet anyone in person that I meet online because people are always who they say they are.
 - True
 - False
- What does .com stand for?
 - corporate site
 - company site
 - community site
 - commercial site
- "Internet Explorer", "Safari", "Mozilla Firefox" are examples of _____.
 - a webmaster
 - computer code
 - web browsers
 - none of the above
- The purpose of a domain is to _____.
 - track where you are
 - make you type more
 - categorize the content
 - network with the computer
- Some of the ways we can be involved with the internet are _____.
 - journaling or blogging
 - instant messaging
 - e-mailing
 - all of the above
- The best way to protect yourself on the internet is to learn about the basics of the "net".
 - True
 - False

