

MODULE

14

# “let’s talk”

## SOCIAL MEDIA AND INTERNET SAFETY



### LEARNING GOALS

During this module, participants will:

- Recognize reliable sources of information online.
- Discuss considerations to make before posting on social media or sharing information online.
- Identify red flags for unsafe online situations.

## DEFINE THE ISSUE

The Internet and social media are ever-growing resources of information and social connections for many young people. What better place to turn for access to a variety of information? For answers to questions that are difficult to ask in person? For making new friends or strengthening friendships – locally and across the world? For advocating for issues that we care about? And much more.

While there are many benefits to the Internet and social media, there are also opportunities for negative or harmful experiences, such as hurtful or inappropriate advertisements and messages, cyber bullying, non-consensual sharing of images, recruitment and/or exploitation, fraud, and theft. While we can find valuable information and make or strengthen beneficial connections online, we must also evaluate information critically and be cautious about our actions.

The National Runaway Safeline (NRS) recognizes that young people routinely use the Internet and social media via cell phones, laptops, tablets, gaming consoles, etc. and firmly believes that the key to reaching young people and connecting them with support is to engage them in the places and spaces they already frequent. In fact, most young people that access NRS' programs and services cite that they learned about NRS through the Internet or social media. Data also shows that young people prefer to reach out to NRS via digital means.



NRS also recognizes that there are many experts in the field of Internet safety for youth – some of them are listed at the end of this module. This module incorporates some of the lessons about the Internet and social media that young people may receive in other areas of their life and includes example scenarios to practice these lessons.

## ICONS

For further details, see the Introduction Module.



## MODULE ACTIVITIES

	ACTIVITY	TIME	METHODOLOGY
	A. The Internet: Being a Critical User	15 minutes	Discussion/Activity
	B. Being Safe Online	15 minutes	Discussion/Activity
	C. Being Mindful of What You Share	15 minutes	Discussion/Activity
	D. Curating Your Online Image	15 minutes	Discussion/Activity



Total time required: **60 minutes**

## MATERIALS

- “Is This Legit?: How to Evaluate Website Sources” Handout
- “Is This Legit?: How to Evaluate Website Content” Handout
- “Tips to Avoid Internet Fraud” Handout
- “Keeping a Healthy Distance” Handout
- “Curating Your Online Image” Worksheet
- Blank Paper

## ACTIVITY 14A

### GETTING TO KNOW THE NET



15 minutes

**INTRODUCE** the topic of the Internet and social media.

**STATE** When used in a safe way, the Internet and social media can be a great place to learn, express yourself, keep in touch with friends, and even make new friends.

**ASK** How do you use the Internet and social media?

**WRITE** responses on poster paper or a chalk/dry-erase board. Examples might include the following:

- Using social media (e.g., Facebook, Threads, X (formerly Twitter), Instagram, TikTok, Snapchat, Reddit)
- Watching videos (e.g., YouTube)
- Messaging and chatting with friends
- Playing games
- Purchasing items (e.g., books, music, clothes)
- Keeping in touch with relatives
- School-related research
- Reading/watching the news
- Online journaling/blogging

**ASK** What do you enjoy most about these activities? How do you feel after?

**ALLOW** 1-2 participants to respond.

**ASK** Think about your experiences; how might they help you? How might these activities be harmful or cause stress?

**ALLOW** 1-2 participants to respond.



## ACTIVITY 14A CONTINUED

**STATE** As we've seen, the Internet and social media can serve many purposes. Many of them are beneficial. But it is important to recognize that not everyone on the Internet has the best of intentions. In fact, it is not uncommon to hear stories about people who have negative experiences or who are victimized through the Internet. For example, scams that ask you to submit personal information to win something or false advertisements for products or services where people lose money and/or have their credit card information stolen. Other situations include nude photos being shared that people did not give permission to share or individuals being coerced to leave home by people they met online who intend to cause them harm. Unfortunately, victimization through the Internet occurs more often than we realize.

The best way to avoid victimization on the Internet is to educate yourself about some basic ways to stay safe. We're going to spend the next few minutes learning some strategies to help us stay safe online.

Our first two handouts will focus on how to recognize reliable sources of information online.

**HAND OUT** "Is This Legit?: How to Evaluate Website Sources" Handout.

**STATE** The domain suffix of a website helps categorize sites according to their content. In most cases, .gov and .edu are the most useful for research and discerning factual information. However, we cannot find all the information we are interested in on .edu and .gov sites. The next handout will help us learn how to determine trustworthiness across domain suffixes.

**ASK** Do you have any questions about domain suffixes?

**HAND OUT** "Is This Legit?: How to Evaluate Website Content" Handout.

**STATE** Please take a minute or two and review the information on the handout.

**ALLOW** 1-2 minutes for participants to review.

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

**SELECT** a volunteer. Keep selecting volunteers until all items have been read.

**ASK** Do you have any questions or comments?

**DISCUSS** responses.

## IS THIS LEGIT? HOW TO EVALUATE WEBSITE SOURCES

**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	
<b>.com</b>	<b>Commercial site.</b> Originally used by websites intending to sell a product, .com is the most prevalent domain suffix in the U.S. and is used by a multitude of entities. Some websites require that you create a login name and password to purchase a product. Not always trustworthy.
<b>.edu</b>	<b>Educational Institution.</b> Used by elementary schools to universities, .edu contains materials and information that may be credible. However, students' personal websites are less likely to be credible.
<b>.gov</b>	<b>U.S. Federal Government.</b> The information posted from sites ending in .gov is considered to be from a credible source.
<b>.mil</b>	<b>Military.</b> This domain suffix is used by the various branches of the U.S. Armed Forces.
<b>.org</b>	<b>Nonprofit Organization.</b> Information on these sites may strongly advocate for specific issues and/or represent a specific point of view about a topic, such as human trafficking. These sites may solicit donations for their cause(s).
<b>.net</b>	<b>Network.</b> This domain is a catchall for sites, much like .com. Anyone can establish a website utilizing this domain suffix. Information from these sites should be given careful scrutiny.

## IS THIS LEGIT? HOW TO EVALUATE WEBSITE CONTENT

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

<b>Location of the Poster</b>	Are they in the place they are posting about?
<b>Network</b>	Who is in their network and who follows them? Do I know this account?
<b>Context</b>	Can the information be corroborated from other sources?
<b>Posting History</b>	Do they usually post about this topic? If so, what did past, or updated posts say? Do they fill in more details?
<b>Age</b>	What is the age of the account in question? Be wary of recently created accounts.
<b>Reliability</b>	Is the source of information reliable?

From The Sheridan Libraries at Johns Hopkins University. Retrieved 2023 from <https://guides.library.jhu.edu/evaluate/social-media>.

## ACTIVITY 14B

### BEING SAFE ONLINE



15 minutes

**INTRODUCE** the topic of social media.

**STATE** Social media can be a great way to stay connected with friends and family, promote issues we care about, and much more. However, we need to make sure we think critically about how we interact with people online for our safety and to mitigate any adverse consequences that a post, comment, picture or any other information shared could cause in the future. In the next activity, we will discuss how to respond to different online situations you may encounter.

**ASK** Have you ever received direct messages from someone claiming to be a friend that you later confirmed your friend did not send? How did you determine if it was fake or a scam? Use the activity worksheet to illustrate what this might look like on one of the platforms you use most.

**ALLOW** 4-5 minutes for participants to prepare their sketches.

**DISCUSS** responses.

Sample responses might include:

- The message did not come from the expected account, e.g., account included a long string of numbers
- Different tone
- The message included a link with little text to preface the message

**ASK** How do you respond to messages that you do not believe to be coming from someone you know?

**DISCUSS** responses.

Sample responses might include:

- Ignore it
- Check in with your friend to let them know they may have been hacked

**ACTIVITY 14B** →



## ACTIVITY 14B CONTINUED

**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. For example, it is not a safe practice to share your passwords with others or to reuse passwords on different sites.

You can find some more tips to avoid Internet fraud on the "Tips to Avoid Internet Fraud" handout.

**HAND OUT** "Tips to Avoid Internet Fraud" handout.

**STATE** Now, we are going to shift gears to talk about interacting with folks online that we have not met in person. We often have these interactions on gaming platforms and online discussion boards, but they also happen on more social media websites, including the more personalized ones where you can make your account private.

**ASK** How do you determine if a profile is real?

**ALLOW** 2-3 participants to respond.

**DISCUSS** responses.

Sample responses might include:

- You have mutual friends
- They have more than one post, generally a fully formed account
- The text in the posts makes sense and is not full of errors we wouldn't expect someone we know to make

**ASK** How do you set boundaries for relationships with people you have met online?

**ALLOW** 2-3 participants to respond.

**DISCUSS** responses.

Sample responses might include:

- Don't share private information
- Don't continue interactions if you feel uncomfortable
- Make sure you also have time interacting with people offline

**ASK** Do you have any questions or comments?

**DISCUSS** responses.

**STATE** If you experienced a situation online that made you feel unsafe, you can always call or text the National Runaway Safeline at 1-800-RUNAWAY or chat with them online at 1800RUNAWAY.org. They are there to listen and to help 24/7 and can connect you to other resources that may be able to assist as well.

## TIPS TO AVOID INTERNET FRAUD

### SAFETY TIPS

- **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 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 could find them. Don't share them with anyone.
- **Stay safe online.** Don't send sensitive information such as credit card numbers by email; 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.

From Internet Fraud, National Consumers League.  
Retrieved 2014 from <http://www.fraud.org/learn/internet-fraud>. Adapted with permission.

## ACTIVITY 14C

### BEING MINDFUL OF WHAT YOU SHARE



15 minutes

**INTRODUCE** the topic of digital footprint.

**STATE** We use the Internet in a lot of different ways. We share our opinions, photos, and videos across many different social media platforms. This can be a way to strengthen relationships and build communities online. When we share, we should think not only of our current relationships, but also of how sharing may affect our future. Your digital footprint includes all that you have posted, online purchases, and all the sites you have visited. We talked about this second aspect of digital footprint in the previous activity. The first part of your digital footprint, what you choose to share, we will talk about now.

**ASK** When you post on a discussion board, photo sharing app, gaming chat, or elsewhere online, how long do you think that post exists?

**ALLOW** 1-2 participants to respond.

**HAND OUT** “Considerations for Sharing” handout.

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

**SELECT** a volunteer. Keep selecting volunteers until all items have been read.

**ASK** What are some questions you might want to ask yourself before posting something online?

**DISCUSS** responses.

Sample responses might include:

- Does this post represent me well?
- What is my mood right now? Am I angry? Will I regret this later?
- What might a parent, teacher, and/or friend think?
- Is there anything in this post that could get me in trouble?
- How long will this post be up? Five years from now, if I saw this post again would I be okay with it or disappointed?
- What information am I okay with being accessible for the rest of my life?
- What would a future employer think?

## ACTIVITY 14C CONTINUED

**STATE** We also recognize that sometimes things get posted online that you did not post yourself or provide consent to be posted, most commonly nude photos or videos. These situations can be extremely emotionally challenging and potentially cause reputational harm, even though it's not your fault at all. It is important to know that the National Center for Missing & Exploited Children (NCMEC) has a service called **Take It Down** that helps remove or stop the online sharing of nudes that were taken of someone when they were under the age of 18. The service is free and it's anonymous, so you won't have to tell anyone it's you in the photo or video. The website is [takeitdown.ncmec.org](https://takeitdown.ncmec.org) and is included in the Resources section of this module.

If you are concerned about something else you shared online or even forget about the **Take It Down** resource, you can always call or text the National Runaway Safeline at 1-800-RUNAWAY or chat with them online at [1800RUNAWAY.org](https://1800RUNAWAY.org). They are there to listen and to help 24/7 and can provide you with the information for **Take It Down** and/or connect you to other resources that may be able to assist.

**ASK** Does anyone have any questions?

**DISCUSS** responses.

## CONSIDERATIONS FOR SHARING

### Be Careful What You Post.

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



### Be Careful Whom 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 how you can be safe.



### Be Careful What You Say.

Be careful what you say to others online. Would you say it to the person if they were standing in front of you and everyone was watching? How would you feel if someone said the same thing to you? Words hurt. You should also take threats made online seriously. Report bullying to a trusted adult.

## ACTIVITY 14D

### CURATING YOUR ONLINE IMAGE



15 minutes

**INTRODUCE** the topic of a brand and an image.

**STATE** A brand is something like a name, symbol, feature, or representation that distinguishes something from another. It can evoke a certain “vibe” or feelings. Social media influencers, for example, generally cultivate their own type of brand through the things they say, post about, type of followers they have, and/or type of companies or services they engage with or represent. Think about it: some are funny, others can be serious, some use their platforms for activism, others for fashion inspiration. But it is the combination of who they are, what they say or post, how they engage with followers or viewers and why they do what they do that make them individual personas or brands that can be largely distinguished from one another. They have their own unique online image.

This dynamic applies to non-influencers, for lack of a better term, too. It allows us to use the Internet and social media as tools to represent ourselves, highlight our unique qualities and strengths, and showcase skills for potential professional opportunities.

Now we are going to do an activity that puts this concept into practice.

**HAND OUT** “Curating Your Online Image” Worksheet.

**STATE** Think about a few things you’d like to share about yourself or how you’d like to represent yourself through your posts online. What is your brand? Write this on the back of the “Curating Your Online Image” worksheet. Then, use the front of the worksheet to sketch a post representing what that might look like. You can also describe it in words, like you might in a caption or write something as you would in a discussion board post, gaming profile, etc.

**ALLOW** 5-8 minutes for participants to create their post.

**ASK** Would anyone like to volunteer to show their post? What did you intend for your post to convey to others?

**ALLOW** 1-2 volunteers to share.

**ASK** Does anyone have any questions for our volunteers?

**DISCUSS** responses.

**STATE** Thank you for sharing. Everyone did a great job.

## CURATING YOUR ONLINE IMAGE

**FRONT:** Use the front of the worksheet to convey your brand. Sketch a post representing what that might look like. You can also describe it in words, like you might in a caption or write something as you would in a discussion board post, gaming profile, etc.

**BACK:** Write a few things you'd like to share about yourself or how you'd like to represent yourself through your posts online.

## HANDOUTS AND WORKSHEETS

- A. Is This Legit?: How to Evaluate Website Sources
- B. Is This Legit?: How to Evaluate Website Content
- C. Tips to Avoid Internet Fraud
- D. Considerations for Sharing
- E. Curating Your Online Image

## REFERENCES

Common Sense Education. (n.d.) Digital literacy & citizenship classroom curriculum. Retrieved 2014 from [http://www.cybersmartcurriculum.org/lesson\\_plans](http://www.cybersmartcurriculum.org/lesson_plans)

Internet Assigned Numbers Authority. (n.d.) Root zone database. Retrieved 2014 from <http://www.iana.org/domains/root/db>

Internet Education Foundation. (n.d.) Kids' Safety. Retrieved 2014 from <http://kids.getnetwise.org/>

National Runaway Switchboard. (2001). Runaway prevention curriculum for classroom and community educators. Chicago, IL: NRS.

University of South Carolina Upstate. (n.d.) Evaluating information – STAAR method: URL & what it can tell you. Retrieved 2020 from <https://uscupstate.libguides.com/c.php?g=257977&p=1721715>

## RESOURCES

AAP Family Media Use Plan is an interactive tool developed by the American Academy of Pediatrics (AAP). It includes a Media Time Calculator that can give a snapshot of how much time each child is spending on daily activities, such as sleeping, eating, homework, physical activity, and media use. It also includes AAP recommendations on screen-free zones, media manners, and much more (<https://www.healthychildren.org/English/family-life/Media/Pages/How-to-Make-a-Family-Media-Use-Plan.aspx>).

Child Safety Network offers information and resources on Internet and computer safety (<https://csn.org/category/safety/online-safety/>).

ConnectSafely is dedicated to educating users of connected technology about safety, privacy, and security. The website provides guides and resources for youth, families, and seniors, including family contracts and pledges ([www.connectsafely.org](http://www.connectsafely.org)).

Cyberbullying Resource Center has resources for educators, parents, and teens (<http://cyberbullying.us/>).

Enough Is Enough offers an Internet safety pledge for youth (<http://www.internetsafety101.org/youthpledge.htm>).

Internet Crime Complaint Center is a central hub for reporting cyber crime. It is run in by the Federal Bureau of Investigation (<http://www.ic3.gov>).



National Center for Missing & Exploited Children works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation. They provide resources to learn how to remove explicit content from various platforms. (<https://www.missingkids.org>).

National Runaway Safeline (NRS) works to keep America's runaway, homeless, and at-risk youth safe and off the streets. NRS operates the 1-800-RUNAWAY hotline and 1800RUNAWAY.org online services, including live chat, email and forums. NRS provides youth and families in crisis with support and access to resources 24 hours a day, 365 days a year (<http://www.1800RUNAWAY.org>).

NetSmartzKids is an interactive, educational safety resource from the National Center for Missing & Exploited Children created for children, parents, guardians, educators, and law enforcement. It uses age-appropriate, 3D activities to teach young children how to stay safe on the Internet (<http://www.netsmartzkids.org>).

OnGuardOnline.gov provides practical tips from the federal government to help you be safe, secure and responsible online. The website is managed by the Federal Trade Commission, in partnership with federal agencies. (<http://www.onguardonline.gov/>).

Stopbullying.gov provide information from various government agencies about what bullying is, what cyberbullying is, who is at risk, and how you can prevent and respond to bullying (<http://www.stopbullying.gov/>).

Take It Down is a free and anonymous service operated by the National Center for Missing & Exploited Children (NCMEC) that can help you remove or stop the online sharing of nude photos or videos that were taken of an individual when they were under the age of 18 ([takeitdown.ncmec.org](http://takeitdown.ncmec.org)).