Title: Online Safety Basics

Objectives

To increase students' awareness of the risks involved in inappropriate conduct, contact, and content used through the Internet and cell phones.

Time frame to Complete

60 minutes

NRS EFL

4

Stackable Cert. Documentation	*Technology*	*Study / Life skills*	*EL-Civics*	*Career Pathways*	Police	Paramedic	Fire Rescue	Medical Asst.	EKG / Cardio	Phlebotomy	Practical Nursing	Healthcare Admin	Pharmacy Tech	IMT	AMT	HVAC	Welding	Other:					
	X	X																					

Standard(s) Addressed in Lesson

Read for Understanding

Benchmark(s) Addressed in Lesson

R.4.3. Apply decoding skills (for example, multi-syllabic words) to read words.
R.4.8. Understand meaning of some specialized content vocabulary (for example, "constitution").

Materials

Booklet – "Net Cetera: Chatting with Kids About Being Online" This is a free publication available from the Federal Trade Commission. A preview is available online at http://www.youtube.com/watch?v=mypHId8vOJw To order multiple copies, go to www.bulkorder.ftc.gov The book is also available in Spanish.

Internet access

Learner Prior Knowledge

Activities

Step One Present the lesson objective by reading/explaining pgs. 4 and 5 of the book introduction.

Step Two Direct students to glossary. Read and clarify definitions for the following vocabulary from glossary: cyberbullying and sexting.

Step Three Pre-select internet sites that give examples of cyberbullying. One example that may be effective is http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D_Jackson/examples.htm.

Step Four Have students go to the pre-selected sites and read the examples.

Step Five Read pages 14-21 in the book (the pages are double spaced and large font so this is not too lengthy). Teacher can simplify and clarify word meanings, if needed.

Step Six Group discussion/questions

Assessment/Evidence

Group discussion and responses to lesson

Adaptations for Beginning Students

Adaptations for Advanced Students

More advanced students could also read the section in the book about Phishing (pp 26-27) or Texting (p 33) and explain the guidelines for such practices to the class.

Teacher Reflection/Lesson Evaluation

This is a 45-page booklet and it contains useful information for teaching the risks involved in inappropriate conduct, contact and content used through the Internet and cell phones. The book can be a significant resource for developing lessons and is also a valuable and free resource to parents. Many of our adult students may be totally unaware of the socialization and communication methods used by their children.

This lesson was created by Middletown ABLE.

INTRODUCTION

The internet offers a world of opportunities.

People of all ages are:

- posting video from mobile devices
- building online profiles
- texting each other from their mobile devices
- creating alter egos in the form of online avatars
- connecting with friends online they don't see regularly in person
- sending photos to friends
- broadcasting what they're doing to hundreds of people

Chat room – An online space where you can meet and exchange information through messages displayed on the screens of others who are in the "room."

COPPA – The Children's Online Privacy Protection Act; it gives parents control over what information websites can collect from their kids under 13.

Cyberbullying – Bullying or harassment that takes place online; includes posting embarrassing pictures or unkind comments on a person's profile or sending them via instant message or email.

Firewall – Hardware or software that blocks unauthorized communications to or from your computer; helps keep hackers from using your computer to send out your personal information without your permission.

GPS – "Global Positioning System," a global navigation satellite system that is used in cars or phones to determine location and provide directions.

Hacking – Breaking into a computer or network by evading or disabling security measures.

Instant messaging (IM) – Enables two or more people to chat in real time, and notifies you when someone on your buddy list is online.

Intellectual property (IP) – Creative products that have commercial value, including copyrighted property like books, photos, and songs.

Limited user account – An online setting that grants someone access to some of the computer's functions and programs, but allows only an administrator to make changes that affect the computer.

Malware – Short for "malicious software"; includes viruses and spyware that steal personal information, send spam, and commit fraud. (See Badware.)

Password – A secret word or phrase used with a user name to grant access to your computer or protect sensitive information online.

Patch – Software downloaded to fix or update a computer program.

Peer-to-peer (P2P) file-sharing – Allows you to share files online—like music, movies, or games—through an informal network of computers running the same sharing software.

PDA – "Personal Digital Assistant," can be used as a mobile phone, web browser, or portable media player.

Personal information – Data that can be used to identify you, like your name, address, birth date, or Social Security number.

Phishing – When scam artists send spam, pop-ups, or text messages to trick you into disclosing personal, financial, or other sensitive information.

Privacy settings – Controls available on many social networking and other websites that you can set to limit who can access your profile and what information visitors can see.

Profile – A personal page you create on a social networking or other website to share information about yourself and communicate with others.

Security software – Identifies and protects against threats or vulnerabilities that may compromise your computer or your personal information; includes anti-virus and anti-spyware software and firewalls.

Sexting – Sending or forwarding sexually explicit pictures or messages from a mobile phone.

Smart phone – A mobile phone that offers advanced capabilities and features like a web connection and a portable media player.

SMS – "Short Messaging Service," technology that allows text messages to be sent from one mobile phone to another.

Social networking site – A website that allows you to build a profile and connect with others.

Spyware – Software installed on your computer without your consent to monitor or control your computer use.

Texting – Sending short messages from one mobile phone to another.

Tween – A child between 8 and 12 years old.

User name – An alias used with a password to grant access to accounts and websites.

Video calling – Internet services that allow users to communicate using webcams.

Virtual world – A computer-simulated online "place" where people use avatars—graphic characters—to represent themselves.

Virus – Malware that sneaks onto your computer—often through an email attachment—and then makes copies of itself.

Webcam – A video camera that can stream live video on the web; may be built into the computer or purchased separately.

SOCIALIZING ONLINE

Social networking sites, chat rooms, virtual worlds, and blogs are how teens and tweens socialize online. Kids share pictures, videos, thoughts, and plans with friends, others who share their interests, and sometimes, the world at large.

Socializing online can help kids connect with friends, and even their family members, but it's important to help your child learn how to navigate these spaces safely. Among the pitfalls that come with online socializing are sharing too much information, or posting pictures, video, or words that can damage a reputation or hurt someone's feelings. Applying real-world judgment and sense can help minimize those downsides.

What can you do?

Remind your kids that online actions can reverberate.

The words they write and the images they post have consequences offline.

Explain to your kids why it's a good idea to post only information that they are comfortable with others seeing.

Some of your child's profile may be seen by a broader audience than you or they are comfortable with, even if privacy settings are on. Encourage your child to think about the language they use online, and to think before posting pictures and videos, or altering photos posted by someone else. Employers, college admissions officers, coaches, teachers, and the police may view your child's posts.

Remind your kids that once they post information online, they can't take it back.

Even if they delete the information from a site, they have little control over older versions that may exist on other people's computers and circulate online.

Use privacy settings to restrict who can access and post on your child's profile.

Some social networking sites, chat rooms, and blogs have strong privacy settings. Talk to your kids about these settings, and your expectations for who should be allowed to view their profile.

Review your child's friends list.

You may want to limit your children's online "friends" to people they actually know.

Talk to your teens about avoiding sex talk online.

Research shows that teens who don't talk about sex with strangers online are less likely to come in contact with predators. In fact, researchers have found that predators usually don't pose as children or teens, and most teens who are contacted by adults they don't know find it creepy. Teens should not hesitate to ignore or block them.

Know what your kids are doing.

Get to know the social networking sites your kids use so you know how best to understand their activities. If you're concerned that your child is engaging in risky online behavior, you may want to search the social sites they use to see what information they're posting. Are they pretending to be someone else? Try searching by their name, nickname, school, hobbies, grade, or community.

Encourage your kids to trust their gut if they have suspicions.

Encourage them to tell you if they feel threatened by someone or uncomfortable because of something online. You can then help them report concerns to the police and to the social networking site. Most of these sites have links for users to report abusive, suspicious, or inappropriate behavior.

Tell your kids not to impersonate someone else.

Let your kids know that it's wrong to create sites, pages, or posts that seem to come from someone else, like a teacher, a classmate, or someone they made up.

Create a safe screen name.

Encourage your kids to think about the impression that screen names can make. A good screen name won't reveal much about how old they are, where they live, or their gender. For privacy purposes, your kids' IM names should not be the same as their email addresses.

Help your kids understand what information should stay private.

Tell them why it's important to keep some things—about themselves, family members, and friends—to themselves. Information like their Social Security number, street address, phone number, and family financial information—say, bank account or credit card numbers—is private and should stay that way.

SEXTING

Sending or forwarding sexually explicit photos, videos, or messages from a mobile phone is known as "sexting." Tell your kids not to do it. In addition to risking their reputation and their friendships, they could be breaking the law if they create, forward, or even save this kind of message. Teens may be less likely to make a bad choice if they know the consequences.

CYBERBULLYING

Cyberbullying is bullying or harassment that happens online. It can happen in an email, a text message, an online game, or comments on a social networking site. It might involve rumors or images posted on someone's profile or passed around for others to see, or creating a group or page to make a person feel left out.

Talk to your kids about bullying. Tell your kids that they can't hide behind the words they type and the images they post. Hurtful messages not only make the target feel bad, but they also make the sender look bad—and sometimes can bring scorn from peers and punishment from authorities.

Ask your kids to let you know if an online message or image makes them feel threatened or hurt. If you fear for your child's safety, contact the police.

- **Read the comments.** Cyberbullying often involves mean-spirited comments. Check out your kid's page from time to time to see what you find.
- **Don't react.** If your child is targeted by a cyberbully, tell them not to respond. Bullies usually are looking for a reaction from their target. Instead, encourage your child to work

with you to save the evidence and talk to you about it. If the bullying persists, share the record with school officials or local law enforcement.

- **Protect their profile.** If your child finds a profile that was created or altered without his or her permission, contact the company that runs the site to have it taken down.

- **Block or delete the bully.** If the bullying involves instant messaging or another online service that requires a "friends" or "buddy" list, delete the bully from the lists or block their user name or email address.

- **Help stop cyberbullying.** If your child sees cyberbullying happening to someone else, encourage him or her to try to stop it by not engaging or forwarding anything and by telling the bully to stop. Researchers say that bullying usually stops pretty quickly when peers intervene on behalf of the victim. One way to help stop bullying online is to report it to the site or network where you see it.

- **Recognize the signs of a cyberbully.** Could your kid be the bully? Look for signs of bullying behavior, such as creating mean images of another kid.

- **Keep in mind that you are a model for your children.** Kids learn from adults' gossip and other unkind behavior.