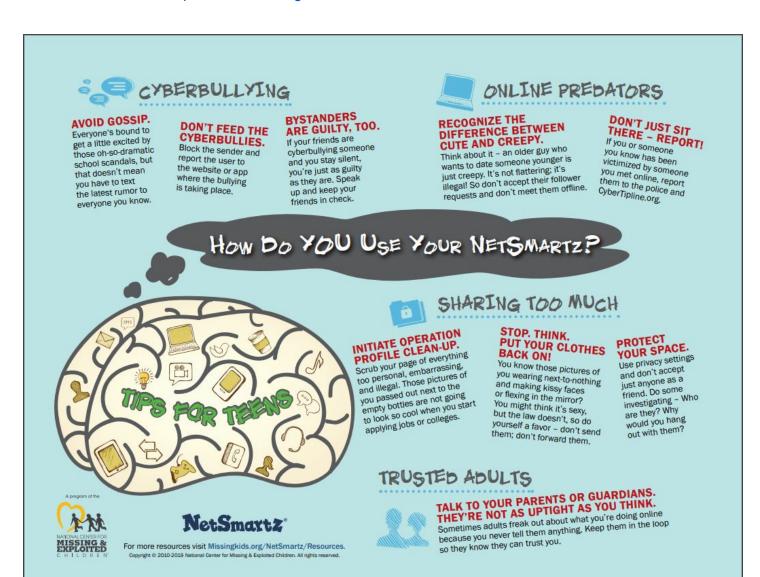
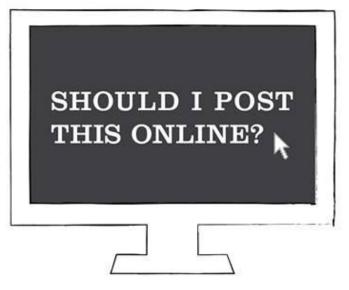
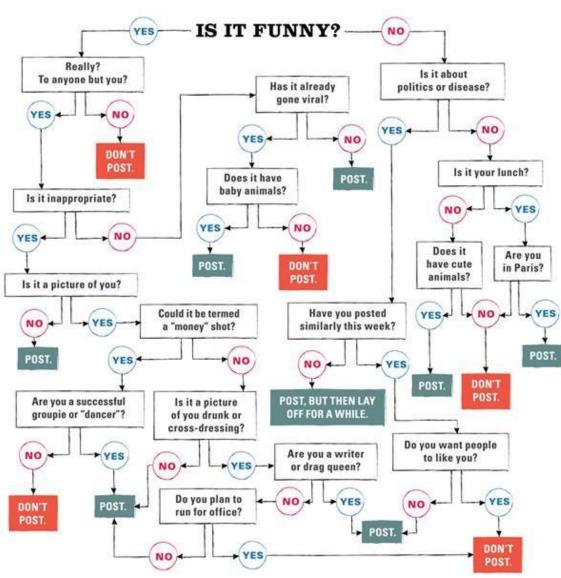
Online Safety Resources

Websites

- Internet Safety for Students: Elementary, Middle, and High School Students
 - https://www.philasd.org/educationaltechnology/teaching-and-learning/internet-safety/internet-safety-for-students/
- Internet Safety for Parents and Students:
 - https://kidshealth.org/en/kids/?search=y&q=internet-safety&datasource=kidshealthasection=parents teens kids&lang=english&start=0&rows=10
- Online Safety Tips for Students:
 - https://kidshealth.org/en/kids/online-id.html?ref=search







Top 7 Dangers of the Internet

1. Cyber Bullying

a. Nasty comments and verbal bullying can negatively impact a student's self-esteem and self-worth.

2. Cyber Predators

a. Not nice people lure student's to unsafe interactions in real life by playing into their insecurities and abusing their innocence.

3. Posting Private Information

 Student's sometimes do not understand social boundaries and will post personal identifying information (address or school), embarrassing stories, or inappropriate photos.

4. Phishing

 Emails from unknown people (cyber criminals) can sometimes be a link to a virus that destroys your computer or steals you personal information stored on the computer.

5. Cyber Scams

a. Children can fall for scams from cyber criminals, such as a free video game, but they have to put in credit card information in order to "reserve" the free game.

6. Downloading Malware

a. Similar to phishing scams, cyber criminals get students to download a program that slowly destroys your computer and steals your information.

7. No Delete Button

a. Things that happen online, stay online...forever. Students do not always have the mindset to consider future consequences and the things they post can hinder them later in life.

Source:

https://www.kaspersky.co.uk/resource-center/threats/top-seven-dangers-children-face-online



Personal Identifying Information

What is Personal Identifying Information?

Any data or information that can be used to identify an individual. Sharing personal identifying information can make it easy for people to find you in the real world, steal your information you saved on the computer, or use the information against you to make you feel bad about yourself.

What can I post?

- Jokes/funny videos
- Certain photos with parent permission
- Podcasts
- Showing off your hobbies, such as artwork, lego creations, creative activities
- Personal opinions or thought provoking quotes

What should I not post?

- Your real name
- Names of family members
- Your home address
- Your phone number
- Where you go to school
- Your friends' or family members' private information
- A photo of someone else, without their consent
- Where your parents work
- The name of your sports team

- Your passwords (Your parents are the only people that should know your password!)
- Any type of photograph (even of your pet!)
- Your current location (some phones have automatic GPS apps built in that may need to be turned off)
- Social Security number
- Parent's credit card numbers

If you're ever unsure if you should keep some information about yourself private, or if it's okay to share it with cyberfriends, ask your parents or another adult. Don't send pictures of yourself to anyone and don't agree to meet a cyberfriend in person without asking your parents first.



True or False Quiz

Test your knowledge!

1. Cyber Bullying is bad, but it isn't a big problem

a. False: Cyber bullying has become a bigger problem in recent years as more kids use social media. In fact, a recent poll showed that a third of kids between the ages of 12-17 have been victims of cyber bullying.



a. **False**: SafeSearch can filter out adult content, but it has to be turned on. But it can't protect you from sites, extensions and apps that may infect your computer.

3. Facebook checks a person's identity to make sure they are real.

a. **False**: All you need is a real email address to create a Facebook account. The name can be completely fake. Many people, including kids, also create more than one Facebook account. One with their real info and another with a false persona.

4. Mobile devices are safe from computer viruses and malware.

a. False: When smartphones and tablets first came out the risk for getting a virus or being affected by malware was low. But now crooks and hackers have learned how to crack them too. Rule of thumb: if it is connected to the Internet it can be harmed by malware. Also, there are some threats that only affect mobile devices. You're most at risk when you are on a public Wi-Fi connection.

5. You have to open something to get a computer virus.

a. False: A few years ago you had to open a file in order for a virus to infect the computer. Today, cyber criminals are programming malware to trick your computer into opening files automatically. You also don't have to download anything to get a virus. If your computer doesn't have malware protection just visiting the wrong site can give you a virus. Even with protection there are things called drive-by downloads that can sneak past safety software by looking like normal web traffic.

6. You can tell if your computer has a virus.

a. **False**: Nowadays computer viruses are programmed to stay under the radar. The tech criminals don't want you to know that they have infected your computer so they can collect your information for as long as possible.

7. Strangers don't really use the Internet to try to trick kids.

a. **False**: Strangers are online every day just like they are in the real world. In fact, the chances of running into them on the Internet are high. Cox Communications reports that 28% of kids have been contacted by a stranger online.

Source:

https://www.searchrpm.com/internet-safety-for-kids/kid-and-teen-resources/true-or-false-internet-safety-for-kids/kid-and-teen-resources/true-or-false-internet-safety-for-kids/kid-and-teen-resources/true-or-false-internet