INTERNET SAFETY

This lesson will help students identify and avoid situations that could threaten their safety on the Internet.

ISTE-NETS Student Standard 5: Digital Citizenship
- Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.

Goals:
To increase student knowledge of Internet safety
To aid the student in identifying dangers on the Internet
To build critical-thinking and decision-making skills relating to computer usage
To help students protect themselves from inappropriate behavior online

Advanced preparation:
The classroom teacher will need to make copies of the “Who Are You, Really?” and “What’s the Password?” pages.

<table>
<thead>
<tr>
<th>Activities</th>
<th>Materials Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Six Degrees of Information</td>
<td>None</td>
</tr>
<tr>
<td>What Would You Do?</td>
<td>“What Would You Do?” page (one per student)</td>
</tr>
<tr>
<td>How to build a great password</td>
<td>“What’s the Password?” page (one per student)</td>
</tr>
<tr>
<td></td>
<td>Pencils</td>
</tr>
</tbody>
</table>
Program Connection Information

Please use an external microphone (conference style) rather than the integrated one in the computer for the audio for your class and locate it centrally in the room. It can be difficult for the Greenbush teacher to hear the students using the computer microphone and therefore it reduces the interactive nature of the lesson. It is fine to use the computer webcam for your video source.

All classes will take place using Zoom desktop video. If your building is already set up to use a desktop video application with a computer, simply open a browser and enter https://zoom.us/j/3662120241 in the URL space. You may need to download Zoom launcher software (free download) if you don't already have it. This needs to be done in advance of the lesson.

If using a Polycom video conferencing unit (or any legacy type video conferencing unit) to connect to a ZOOM conference, make sure the unit is in "encrypted mode" then dial the following IP on the internet: 162.255.37.11 or 162.255.36.11 and once connected, they will ask for a MEETING ID: enter 3662120241 (for Sharon at Science Center).

It's always a good idea to touch base with your district technology facilitator prior to your program to make sure all systems/equipment are in place and operational and that there aren't any firewalls in place that might prevent you from connecting to Zoom.

Once you connect, you will enter a Zoom waiting room. Your Greenbush teacher will admit you into the final meeting room.

If you have questions, please call Sharon Bertolio at Greenbush, 620-724-6281, or email at sharon.bertolio@greenbush.org (best method of contact).
What Would You Do?

Scenario 1
You get a message request online from a stranger. “Hey! You seem like a fun person to hang out with. Let’s have some fun together! Can you add me to your friends list? –Jason”

Scenario 2
You get a text message on your cell phone from someone you don’t recognize. “Hey, this is Jen! Remember me from the summer?”

Scenario 3
After math class with Mrs. Beckstrom you get this message on your cell phone. “I’m Mark from your Math class with Mrs. Beckstrom. Did u understand the homework?”

Scenario 4
You get a message from someone you don’t follow. “Hey! Love your posts, you’re SO funny! Give me your phone number and we can talk more!”

Scenario 5
You get a chat from someone with whom you aren’t familiar. “I saw you in Math class today. U R CUTE! What is your address? I can come over 2 hang out.”

Scenario 6
You receive a message online. “Hey, I just met your friend Sam! She told me about you, would love to meet you. What’s your address?”
What’s the Password???

Here’s an idea for creating an extra-secure password.

Think of a fun phrase that you can remember. It could be your favorite song lyric, book title, movie catchphrase, etc.

- Choose the first letter or first two letters from each word in the phrase.
- Change some letters to symbols.
- Make some letters uppercase and some lowercase.

Here are some tips for creating passwords to safeguard your secrets.

**Strong passwords** are based on a descriptive sentence that’s easy for you to remember and difficult for someone else to guess.

**Moderate passwords** are passwords that are strong and not easy to guess by bad software, but could be guessed by someone who knows you.

**Weak passwords** commonly use personal information, are easy to crack, and can be guessed by someone who knows you.

- Use a unique password for each of your important accounts.
- Use at least eight characters.
- Use combinations of letters (uppercase and lowercase), numbers, and symbols.
- Don’t use personal information (name, address, email, phone number, Social Security number, mother’s maiden name, birth dates, etc.), or common words in your password.
- Don’t use a password that’s easy to guess, like your nickname, name of your school, favorite baseball team, etc.
- Don’t share your password with anyone other than your parents or guardian.

**My password idea is __________________**

(Do not use this password for any of your accounts now! It’s no longer a secret!!!)
Additional Lesson Resources
12 Resources for Teaching Digital Citizenship
Richard Byrne - FreeTech4Teachers.com

**Elementary School Resources**
Be Internet Awesome ([https://beinternetawesome.withgoogle.com](https://beinternetawesome.withgoogle.com)) is Google's new Internet safety curriculum for the 2017-18 school year. The Be Internet Awesome site features a game called Interland. The game is set in a virtual world that students navigate by correctly answering questions about Internet safety. The graphics of the game are great and there are some elements in which students navigate, but there is also a heavy reliance multiple choice questions in the game. The Interland game can be distributed through Google Classroom. G Suite administrators can push the game to the task bar on managed Chromebooks. There is a 48 page PDF containing lesson plans on each concept in the Be Internet Awesome curriculum that teachers can download for free. The curriculum is based five concepts: *Share with care, Don't fall for fake, Secure your secrets, It's cool to be kind, When in doubt, talk it out.*

Digital Passport ([http://bitly.com/ftdpp](http://bitly.com/ftdpp)) is an online program from Common Sense Media. The purpose of the Digital Passport program is to provide students in grades three through five with lessons and games for learning responsible digital behavior. Digital Passport uses videos and games to teach students about cyberbullying, privacy, safety and security, responsible cell phone use, and copyright. Students earn badges for successfully completing each phase of the Digital Passport program.

PBS Kids offers the Webonauts Academy ([http://pbskids.org/webonauts/](http://pbskids.org/webonauts/)) in which elementary school students can learn about safe online behaviors. When students have completed all of the Webonauts missions they will graduate from the Webonauts Academy. The educators tips page offers some practical suggestions for using Webonauts in the classroom or in a school library.
In an effort to teach children about potential dangers online and how to avoid them, the Council of Europe has offers a game called Through the Wild Web Woods (http://www.wildwebwoods.org). Through the Wild Web Woods is designed for students ages seven through ten to learn how to spot danger on the Internet and what to do when they do spot danger on the Internet. The game is available in twenty-four languages.

Professor Garfield is a free resource developed in part by the Virginia Department of Education. Professor Garfield teaches students how to be safe online, how to recognize and respond to cyberbullying, and how to decide if something is a fact or an opinion. These educational activities can be found in the free Professor Garfield apps; Online Safety (http://bit.ly/ftgarfield), Fact or Opinion (http://bit.ly/ftgarfield1), Cyberbullying (http://bit.ly/ftgarfield2). All of the free Professor Garfield iPad apps use the same format. The format is a set of comic strips that students read to learn about the issues the app is focused on. At the end of the comic strips students play some simple games to practice recognizing good online behaviors.

AT&T's Safety Land (http://bit.ly/ftatt) is a nice game through which kids learn and practice recognizing danger on the Internet. The game is set in the city of "Safety Land." As students navigate from building to building in Safety Land they are confronted with a series of scenarios and questions to respond to. If they respond correctly to each scenario they will capture the cyber criminal and send him to the Safety Land jail. Students who send the cyber criminal to Safety Land jail receive a certificate that they can print out.

**Middle School / High School Resources**

A Thin Line (http://www.athlonline.org/) is a digital safety education resource produced by MTV in collaboration with other media partners. The purpose of the site is to educate teenagers and young adults about the possible repercussions of their digital activities. A Thin Line offers a series of fact sheets about topics like sexting, digital spying, and excessive text messaging and instant messaging. A Thin Line gives students advice on how to recognize those behaviors, the dangers of those behaviors, and how to protect your digital identity. Students can also take a short quiz to practice identifying risky digital behaviors.

Own Your Space (http://bitly.com/ftmsft) is a free ebook designed to educate tweens and teens about protecting themselves and their stuff online. This ebook isn't a fluffy, general overview book. Each chapter goes into great detail explaining the technical threats that students' computers face online as well as the personal threats to data that students can face online. For example, in the first chapter students learn about different types of malware and the importance of installing security patches to prevent malware infections. The fourteenth chapter explains the differences between secured and unsecured wireless networks, the potential dangers of an unsecured network, and how to lock-down a network.
ThinkB4U (http://www.thinkb4u.com/) is a series of web safety videos and tutorials from Google and its partners. Using the "choose your own adventure" aspect of YouTube video editing, ThinkB4U offers interactive videos to educate viewers about things like protecting online reputations, avoiding scams, research and critical thinking, and responsible text messaging. ThinkB4U is divided into three basic sections; students, parents, and educators. Each section addresses nine different topics related to safe and responsible use of the Internet and cell phones. The sections include short videos about the topics, a short written lesson, and some interactive games on the topics of responsible use of the Internet and of cell phones. The Educators' section of ThinkB4U offers lesson plans from Common Sense Media and the National Consumer League. There are lesson plans designed for elementary school, middle school, and high school use.

Seven Digital Deadly Sins (http://sins.nfb.ca/#/Grid) is an interactive story produced by the National Film Board of Canada. The story contains seven chapters each containing short videos, essays, and polls. The videos and essays tell the stories of people suffering from digital sins like greed (illegally downloading media) and wrath (cyberbullying). After reading or watching the stories viewers can vote on questions about what they would do in similar situations. Seven Digital Deadly Sins does deal with some content, mostly in the section on lust, that you will want to screen before deciding if it is appropriate for the students in your classroom.

Creating and Protecting Strong Passwords

Whenever it is offered as an option, it is a good idea to use two-step or two-factor authentication on the online services you use. Google, Dropbox, Box, and many other cloud services offer this option. Two-step authentication means that just entering one password isn’t enough to log into a service. Learn about Google’s two-step authentication in this video https://youtu.be/zMabEyrPtRg and read about it in detail at http://bitly.com/ftgtwostep

Creating a strong password is the first step in securing your online accounts. Google offers good advice in this video https://www.youtube.com/watch?v=0RCSHfHHL_4