

GETTING STARTED

Step #1 – Introduction (Whole Group)

Time: 5-10 minutes

Simple goals for introduction:

- Let students know who you are and what you have come to discuss
- Find out what students already know about responsible online behavior
- Peak students' interest in the topics you will be covering

A good way to engage students is to start your presentation with probing questions, rather than simply standing in the front of the class and lecturing to the students. **You do not have to ask each of the following questions. These are simply provided as tips to get you started.**

Possible Introduction Flow:

- Provide your name and the company you represent. Ask if the students have ever heard of your company?
- “Can anyone tell me what they think our company does and why our job is important to computer users today?”
- Briefly and simply describe your company and some of the things you do in your role. (It may also be a good idea to talk about what steps you had to go through to get a job like yours---This can be a subtle way to peak student interest in exploring technology careers.)

Possible Probing Questions:

- How many of you like to use the Internet?
- How many of you use it everyday?
- Where are some places you use the Internet regularly? (Call on students as they raise their hands. This will give you an idea of how many students have home computers and use it regularly at their own home, and how many use it at a public place like a library or at school.)
- What kinds of things do you regularly do when using the Internet? (Examples; homework, email, socialize with friends, send pictures to far away family members)
- For those of you that have a computer in your house, where does your family keep the computer?
- Do you have special rules for using the computer and the Internet?
- What are some of those rules?

Transition to Whole Group Lesson:

- “Wow! You guys know a lot!” My job as a Security Specialist for (Google, Symantec, Microsoft) is to help people understand how to use the Internet responsibly and safely to protect themselves and their computer. This is so important that we are working with an organization from Washington DC called the National Cyber Security Alliance to help make sure that students at every grade level understand how to stay safe and act responsible while using the Internet.”

Step #2 (Whole Group Lesson) **Becoming A Smart Digital Citizen** **By Using the WWW Decision Tool & C3 Concepts**

Approximately 15 Minutes

Write the following words on the classroom chalkboard or whiteboard - Cyber Safety, Cyber Security, Cyber Ethics - spaced apart and with room to write underneath each heading.

Make an additional column with the heading: “ Things I do in Cyber Space” (online)

- Make sure students understand that cyber space is just another word for the “online” world they are participating in when they use the Internet.

Explain to students that because actions in cyber space can often make ourselves and our computers vulnerable we have to understand tools and take precautions to become smart digital citizens who act responsibly online, protect their computer wisely, and follow all safety rules.

Asks students to define each term the best they know how and raise hands to share thoughts about what each term means.

Things I Do In Cyber Space (Online)

Cyber Safety: _____

Cyber Ethics: _____

Cyber Security: _____

Key Objectives:

1. Students will understand that “cyber” is another word for the “online” world they are participating in when they use the Internet.
2. Students will understand that whatever they post or send into cyber space can often be viewed just as easily from strangers in another part of the world as their classmate who lives a few blocks away. Ask students who they think sees the information they post when online.
3. Students will understand the three key components of the C3 Concepts and how to use the WWW Decision Tool to make wise choices and behave responsibly while online.

C3 Definitions- Provide Definitions and Collect Student Feedback:

1. *Briefly Review Cyber Safety-*

-“Responsible rules and behaviors designed to keep individuals safe whenever connected to the Internet.”

-Ask students:

- “What are some examples of “safety rules” your parents ask you to follow while using the Internet?” List answers under appropriate column on the chalkboard.
- “Why do you think these are important to follow?”

2. *Briefly Review Cyber Ethics-*

- “Cyber-Ethics is informal code of positive conduct used whenever some is using the Internet.”

-Ask Students:

- Examples of wise and poor Internet use choices and discuss with students
- Strategies for being a good digital citizen who behaves ethically online.

3. *Briefly Review Cyber Security –*

-“The protection of information and computer systems and networks while connected to the Internet.”

-Ask Students:

- What are some common strategies that people use to protect their computer and personal information?
- What are some security tips users should know to keep their computer safe and protect their personal information whenever they go online?

WWW Decision Tool

Now that you have explained the C3 Concepts to students and helped them think about how their regular Internet activities fit under these three important headings, the next step is to provide students with an internal “tool” or “decision checklist” to help reinforce strategies to behave responsibly, and remain safe and secure during all Internet activities.

The internal “WWW Decision Tool” is a good reminder to protect your personal information and remain in the drivers seat with how much information you share with others when online.

(Review With Students)

W –Who is asking for this personal information?

W –What information is being requested?

W – Why do they need this personal information?

Read the following scenario out loud to students to help them practice the WWW Decision Tool and how to approach the scenarios they will analyze while working in small groups. Ask students to recall what the WWW stands for and how it can serve as a reminder to Scott about thinking critically before releasing any personal information online. Discuss the ethics issues this scenario involves with following school rules and respecting school property, as well as the security risks associated with “free” downloads.

After brief discussion with the students, explain that they will now work in small groups to act as “Security Specialists” and solve other cyber-scenarios.

Sample Scenario #1 – Security/Ethics-Potential Viruses From Free Downloads

Scott is a Fourth Grade student at Honors Elementary School where his class is doing research in the school’s computer lab on ways to stay safe and secure while online. The computers at school are all connected to the same network, which holds student’s personal information. During Scott’s research on the Internet that day he receives several pop-up ads offering free iPhones with 12 months of free mobile services including text

messages if you accept the free trial subscription of “TechIsCool” online magazine. Scott knows the school’s Acceptable Use Policy is very clear about not downloading anything on school computers to protect the network. He knows he shouldn’t, but he wants an iPhone so badly and doesn’t want to miss the opportunity to get the phone for free. Scott clicks on the link offering the free download. Scott gets suspicious when he starts getting additional pop-up ads asking for detailed personal information. He returns to the StaySafeOnline website and reads all about the potential harm in accepting free downloads. Scott changes his mind, doesn’t provide personal information, and returns to his research on cyber security.

Please use your knowledge of the WWW Decision Tool and C3 Concepts to identify the red flags that Scott almost passed by in the hopes of getting a free phone.

Step#3

Small Group Reinforcement Lessons

Solving C3 Scenarios Using the WWW Decision Tool

10 Minutes Group Work

10 Minutes Reporting Out to Class

Instruct students that they will be working in groups of four or five to solve a scenario that highlights a C3 issue. (For larger classes you can divide students into groups of up to six.) Explain that they will be working as members of a team to provide the best answers to the questions provided on their Recording Sheet. There are Team Roles for certain members of each team including a Team Reporter that will read your scenario to the entire class and report your team’s answers and responses when you are done.

WRAP UP:

Go around the room and call on each team’s reporter to read their scenario and report the team’s answers.

After each group has shared their responses, collect the Scenarios and Reporting Forms and instruct students to go back to their individual desks.

TIPS:

- ★ Before students begin their work, ask if anyone has any questions about what they will be doing with their team.
- ★ While students are working in their teams, walk around the classroom to monitor student activity, prompt students when necessary to think critically, and encourage all students to participate and contribute to the team's efforts.
- ★ Do not hand out Scenarios, vocabulary term sheets, or Reporting Forms until students are in their groups and you are ready for them to begin working.
- ★ Tell students they have only 10 minutes to assign team roles, read the scenario, discuss, and record responses to the questions on the reporting form. They must work together to quickly and critically work through all of the questions.

Step #4

Individual Take Home Assignment

This Assignment Should Take Students Approximately 50 Minutes

Assignment:

- ★ Think critically about what you know about cyber security and issues individuals, schools and companies face when connected to the Internet. Using one full page, respond to the following two questions. Apply all of the knowledge you now know about cyber safety, cyber ethics, and cyber

security and the importance of behaving responsibly, ethically, and wise while online.

1. Who do you think is responsible for making sure the Internet is safe and secure for everyone? (Think about local police, government agencies, individual users, etc.) If the government is involved, who should be most responsible? - Be sure to thoroughly explain your answer. (Hint: Review the National Cyber Security Alliance website – www.staysafeonline.org - for one Federal agency leading these efforts.)

2. What do you see as the most common issue surrounding the use of the Internet and other mobile technologies (such as cell phones and PDA's) with your friends and classmates? Now that you are more aware of the three-tiered approach to Internet education, what would you recommend teachers and administrators do to better prepare students to be safe and responsible while online? - Be sure to thoroughly explain your answer.