2016 NATURE Summer Camp
CYBER SECURITY

Description:

Most internet users would like to learn more about cyber security. Many lack an understanding of the common dangers that could occur online. Among parents, many lack confidence that their child is safe when using the internet. With the ever-expanding use of the internet, education is critically needed to address safe computer habits, particularly among students who use and adopt new technologies more quickly than their parents.

Cyber security involves more than putting small barriers in place, such as using anti-virus software and knowing to delete spam. It requires a wall of defenses. Cyber security education must be thorough to help students keep themselves safe from the wide range of threats and dangers online.

Education must address three subject areas: cyber ethics, cyber safety, and cyber security (National Cyber Security Alliance). If any one of these areas is missing, students will lack the knowledge to fully protect themselves.

Consider each of these areas separately:
• Cyber Ethics: Students learn to make decisions in a way that shows respect for others and for others' safety while online. The topics in this area include an understanding of the acts and consequences of cyber crime and unethical behavior, such as hacking and cyber bullying.
• Cyber Safety: Students become aware of the predators, spammers, and cyber bullies who may be online. They learn to recognize traps and dangers and then respond to them effectively or report them to authorities.
• Cyber Security: Students learn about attacks on their computers that may cause damage or steal information, such as identity or financial data. They learn about malware, spam, and identity theft, and how to protect themselves and their computer.

State Standards:

9-12 RU.1
9-12 RU.4
9-12 RU.5
9-12 RU.6
9-12 RU.10
9-12 RU.11
9-12 RU.12

Objectives:

• raise students' awareness on the cyber security threats and measures of safety for protection and prevention
• impact positively the online behavior of students when using online and offline applications
• raise students' awareness on the consequences of cyber crime and reckless online behavior

Education Standards:

• Assess students comprehension of the cyber security, cyber safety, and cyber ethics terminology and concepts introduced in each lesson
• Assess students' awareness of the threats associated with using online applications
• Assess students' awareness of the measures of protection to ensure cyber safety
• Assess how students apply cyber safety concepts to real-life situations

Schedule:

9:00 – 9:30	Cultural Connection
9:30 – 10:00	Cyber Security Powerpoint Introduction
10:00 – 10:30	Activity 1 (Email)
10:30 – 11:15	Activity 2 (Online Communication)
11:15 – 12:00	Activity 3 (Cyber Ethics)
12:00 – 12:45	LUNCH
12:45 – 1:30	Activity 4 (E-Commerce)
1:30 – 2:30	Activity 5 (Online Games)
2:30 – 3:00	Session Wrap-up

Activity 1: Email

Learning Objectives:
>Introduce new cyber security words and definitions related to email.
>Help students to recognize cyber threats when receiving an email.
>Raise awareness of the consequences of cyber threats related to email.
>Reinforce ways that students can protect themselves online through responsible behavior when handling email.

Definitions
Email – electronic mail, the transmission of messages over communications networks.
Spam – electronic junk mail
Scam – fraudulent scheme to make a quick profit.
Attachment – a file attached to an email message.
Hyperlink – a link to a web page address in Hyper Text Markup Language (HTML).
Cyberbully – someone who uses the internet to harass, intimidate, embarrass, or demean others
Phishing – using fake web sites to trick you into giving away personal information

Email, short for electronic mail, refers to sending, receiving, and storing mail using an internet-based communication medium. To send and receive an email, you need to subscribe to an email service or be provided with one by work or school. Email service subscription is usually free, provided you have access to the internet. Microsoft (Hotmail), Yahoo (Yahoo mail) and Google (Gmail) are all well-known free email service providers. Subscription normally requires you to complete a registration process. You should be sure to read the email provider terms and conditions carefully and make certain you agree to them prior to establishing your account. Email Security Threats Email viruses and worms are common. If you haven't yet received one, chances are good you will.

The following list offers steps you can use to help decide what to do with every email message you receive with an attachment. You should only read a message that passes all of these tests:
• The Know test: Is the email from someone you know?
• The Received test: Have you received email from this sender before?
• The Expect test: Were you expecting email with an attachment from this sender?
• The Sense test: Do email sender ID, contents described in the subject line, and attachment filename make sense? For example, would you expect the sender – for instance, your mother – to send you an email message with the subject line "Here you have, ;o)" that contains a message with attachment "AmerDiab.jpg.vbs?" A message like that probably doesn't make sense. In fact, it happens to be an instance of the Amer Diab worm, and reading it can damage your system.
• The Virus test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program.

To ensure safety from cyber crimes and threats when handling and using emails, be aware of and abide by the following safety guidelines:

1. Security

   A. Maintain and update your computer anti-virus, anti-spyware, and firewall programs regularly.

   B. Use caution in opening email attachments.

   C. Never open email with a subject title you don't understand.

   D. Delete advertisement email and do not respond to it.

   E. Set your spam filter or junk mail filter to block images and automatically send suspected spam and junk mail to the spam filter. Most email programs have a feature in their "options" menu you can use to filter email.

   F. Don't open email asking you to unsubscribe from electronic news letters or groups you did not subscribe to.

2. Safety

   A. Set a strong password that does not include any personal information or information others can guess, like your birth date or Social Security number. Change your password frequently. A strong password is a phrase consisting of letters, numbers and symbols.

   B. Archive your email in folders for easy access and retrieval.

   C. Backup the information you receive in email you consider important on a disk or drive.

   D. Lock your computer when not in use. Others could access the information exchanged on your email account.

   E. Be aware that schools have the right to view any email account and information exchanged on its machines and network.

   F. Share with your parents any information you read and see that makes you feel uncomfortable.

3. Privacy

   A. Never provide confidential information in an email. Text written in an email is similar to a text sent on a postcard or a letter sent without an envelop. Any one who handles this post card could read your message.

   B. Use caution when providing information on an electronic form to register for an email account.

   C. Make sure your user ID does not include your first or last name.

4. Email handling vows

   A. Never believe information exchanged in email.

   B. Never arrange to meet someone in person whom you only know through email.

   C. Never write inappropriate or threatening emails.

   D. Never write an email when angry or upset. Treat others with respect as you would like to be treated.

   E. Never delete email that carry threats and harassment or be silent when noticing one. F. Never share passwords with friends, only with your parents if needed.

   G. Never download songs, images, or files sent as an attachment or link unless expected from a family member or school.

   H. Never hack into another person's email account for entertainment, as it is a cyber crime punishable by the law. ¾ Never share files and images protected under the copyright law without the permission of the author and the publishing agency.

Scenario – Read the following scenario and answer the questions below:

Brian is a ninth-grade student. The school he is attending implemented an email system to encourage students to contact their teachers with questions and inquiries after school hours. Brian used the email system frequently and would check his email on a daily basis. One day, Brian received an email from a sender he did not recognize, but since his friends use aliases for their online identity, he thought it may be one of them. The subject title of the email was "Math got easier." Brian opened the message right away. The message read, "the attached is a list of equation answers." Brian opened the attachment, which was almost blank. After few attempts, Brian closed the email and attachment and shut off his computer, which had crashed. Next day in school, Brian's friends asked him about the attachment he sent them. Brian was surprised. He didn't recall sending them a message with an attachment. He was really surprised when the principle called him to his office and inquired about the spam he sent to every teacher and student with an email account on the school's server, almost crashing it.

Scenario Questions:

1. What is spam?

2. Mention three cyber safety violations committed by Brian?

3. How would Brian limit spam in his email account?

5. List three things could Brian do to protect his computer and email from cyber threats.

6. What do you think happened to Brian?

Lesson Questions:

1. Define the following terms:
    a.) email

    b.) spam

    c.) scam

    d.) hyperlink

    e.) phishing

2. Provide an analogy for each:
Example: an email is similar to a post card

a.) spam is similar to

b.) online line phishing is similar to

c.) firewall is similar to

d.) online viruses are similar to

3. List the five-point test prior to reading an email and opening an attachment.

1-

2-

3-

4-

5-

4. Provide a cyber safety violation example for the following online behavior:
Example: receiving an email with a subject title "You won a trip for four" – opening the email and attempt to respond to it

a.) opening an email attachment

b.) forwarding an email

c.) responding to an email sent by some one angry with you

d.) sending an email with class mates pictures

"I got a tool to remove malicious malware..."

<u>Activity 2:</u> Online Communication (Chatrooms, Instant Messaging, and Text Messaging)

Definitions – Use online resources to define the following terms.

1. Chatroom

2. Text

3. Short messaging service (SMS)

4. Cyberbullying

5. Routers

6. Password

7. User ID

8. Internet protocol (IP) address

9. Alias

People use chatrooms, instant messaging, and text messaging for various reasons, such as:

- Communicate with friends and family members
- Meet new friends online
- Express opinions
- Discuss school projects and homework
- Exchange music files, movie clips, art work, links, and pictures
- Attend virtual training and learn new skills
- Meet a requirement for a distance learning class (high school level)
- Learn about new subjects, such as language, culture, or geography
- Search for dates
- Harass and cyberbully others
- Learn about cultural and musical events

Although many people depend on chat and text messaging to communicate with their friends and peers, few are aware of the dangers and risks they might face by not paying attention to the security aspects of using online chat. Some of the risks people could face on chat include the following:

- Identity theft – Sharing personal information in a chatroom could lead to identity theft by malicious individuals.
- Viruses and malware – One can accidently download a virus or malware from a chatroom, sent by other chatroom users or hidden in an advertisement.
- Harmful links – Links shared on a chatroom could lead the user to come across sites with inappropriate adult content, gambling, or sites meant to defraud users.

• Predators – Predators join chatrooms to collect personal information about young adults, teenagers, and children. The information they collect could lead a predator to seek the physical location of the child or teenager and cause them harm. Predators work to gain victim's trust and attachment slowly. Once a predator has gained the victim's trust, they could request them to behave in an inappropriate way, or ask to meet with them at the victim's home alone, or at another location.
• Intruders – Through a link or malware sent to the chatroom user's computer, intruders could gain access to that user's computer and information.
• Compromising personal information – Personal information, including pictures posted on the chatroom site, could be accessed by any chatroom member.
• Cyerbullying and harassment – Cyberbullys use chatrooms to demean, harass, and oppress others by posting harmful information, comments, and pictures on a public forum about an individual or a group.
• Excess time spent in a chatroom – adolescents may spend many hours in chatrooms, almost to the point of addiction. This takes time away from engaging in other important tasks and activities. Too much time in chatrooms can have a negative social effect as well, leading away from physical interaction with people and towards isolation.

Scenario – Read the following scenario and answer the following questions.

Jennifer was thrilled to join an instant messaging service her friends used every day. Since they use a private chat-room, Jennifer decided to take a digital picture of herself and add it to the chatroom under her user name. Every now and then, she and her friends would use a webcam to see one another while chatting. At the end of one conversation, one of her friends stayed to chat with her. Jennifer's friend was asking many personal questions, which was unusual. Then she expressed admiration for Jennifer's beauty. Jennifer was not comfortable with the remarks her friend was making. Her friend also insisted that they both should use the webcam to see one another while chatting. When Jennifer turned on her webcam, her friend said that her own webcam was not working. Hearing this, Jennifer turned her webcam off and excused herself to go do homework. The next day at school, Jennifer saw the friend she was chatting with the day before. To her surprise, her friend said to the whole group that she had been visiting a relative with her parents and younger brother, which was the reason why she was not able to join the chat a day before. When Jennifer asked her about the identity of the person using her chat user ID, the friend had no clue. The friend had an elder brother and sister who were at home, but she was not sure if either of them knew her user ID and password.

Scenario Questions

1. What do you think happened next? Why do you think so?

2. What online chat threats did Jennifer encounter?

3. What online chat risks did Jennifer take?

4. Who, in your opinion, was chatting pretending to be Jennifer's friend? Explain why you think so.

5. If you were in Jennifer's situation, what would you have done differently?

6. What should Jennifer do next?

7. If you were Jennifer's parents, what chatroom rules would you set

Log on to Carnegie Cyber Academy
www.carnegiecyberacademy.com
Then click on "Fun Stuff," click on "game archives," and play the Packet the Rabbit game, which will introduce you to how an IP address works

Activity 3: **Cyber Ethics**

Definitions – Use internet resources to define the following terms.

1. Internet etiquette or "netiquette"

2. Misinformation

3. Social network or virtual community

4. Blog

5. Cyber bully

6. Hacker

Log on to Carnegie Cyber Academy
www.carnegiecyberacademy.com
Then click on "Fun Stuff" and play Betty's Netiquette Quiz game to see if you are good cyber citizen.

Read the following 4 Scenarios and answer the question after each.

Scenario 1: Putting privacy and identity in jeopardy
Scott sat down at his brother's computer while he was out because he wanted to check his email and surf the web. To Scott's surprise, his brother had not logged out of his computer, and he had left the window open that displayed his email account. It was tempting for Scott to think he could send an email from his brother's account as if he were his brother. Also, Scott could see that his brother had been emailing a friend whom his parents had forbidden him to see.

1. What could go wrong in this situation?

2. What should Scott do next?

3. Lesson learned?

Scenario 2: Sharing confidential information over the web

Frank was looking forward to working during the summer so he could save money for college. He applied for many positions in offices where he could learn something about the business world. When he was finally offered a job, however, Frank was not satisfied with it. He used time at work to send out more job applications from his email account. He also used IM on his computer at work to complain about his boss to his friends. After two weeks, Frank was fired for misuse of company resources. His boss was extremely angry, and refused to recommend him for other positions.

1. What went wrong in this situation?

2. Lesson learned?

Scenario 3: Cyber bullying

Jack loved his new digital camera, and he tried to take it everywhere he went, including to his sister's dance class. During dance class, he took a picture of his sister as she fell. The photograph caught her in an embarrassing position. Jack thought the photo was funny and forwarded it to a few of his friends. Some of the friends then forwarded it to others who went to their school. When Jack's sister arrived at school later that week, to her horror, the photograph had been printed and passed around the school. She felt humiliated.

1. What went wrong in this situation?

2. Lesson learned?

Scenario 4: Posting misinformation

Randy was part of a web design club at school, and updating the school's website was part of the club's activities. One day, he volunteered to post the soccer team's schedule to the website. The club president told Randy to call the soccer coach to obtain the schedule information, but Randy was in too much of a hurry. He wanted to finish the task and go home in time to watch his favorite television show. Instead of calling the soccer coach, he used a search engine to look for the schedule. He found a blog by one of the team's players that had a schedule of games, and Randy used the blog's information. The following weekend, many people at the school were confused or upset. The schedule Randy had posted on the school's website was from two years ago! The information was completely incorrect, causing some parents and soccer fans to miss the first game of the season.

1. What went wrong in this situation?

2. What could Randy have done differently?

3. Moral of this story?

Activity 4: E-Commerce

Definitions – use your online resources to define the following terms

1. e-Commerce

2. e-Tailing

3. Electronic data interchange (EDI)

4. Business applications

5. Business-to-business (B2B)

6. Private information

7. Phishing

8. Authentication

9. Encryption

10. ATM

11. PIN

Scenario – Read the following scenario and answer the following questions.

Keith travels often for work, so he opened a bank account for his elder son Chris, a sixteen year old in eleventh grade. Keith provided Chris with a debit card and a credit card in case Chris could not reach him and his wife and there was an emergency need for cash. Chris felt empowered having a large sum in his bank account. He could not wait to share the information about his bank account with his friend Roy. Chris went to Roy's house, where he and Roy surfed the internet to purchase a signed T-shirt they had wanted for a while. After selecting the T-shirts and finalizing the purchase, both printed their receipts after checking the item number and price. They also double checked that the shipping information showed Chris's correct house address so he could receive the shipment. Five days later, Chris received a phone call from the shipping company, asking that he confirm the name, address, and order number. Chris provided the necessary information and was excited to know their T-shirts would be arriving nine days later. Nine days passed after the confirmation call and Chris did not receive the T-shirts. He called the company and was told that the shipment was on the way and would take two more weeks for the shipment to arrive. To Chris astonishment his father came home angry about a large amount of money that was charged against Chris's new bank account.

Scenario Questions

1. What do you think happened next? Why?

2. Do you think Chris and Roy charged large sums of money? Why?

3. Who, in your opinion, charged Chris's bank account? Why?

4. What cyber crime did Chris fall victim to?

5. What did Chris do wrong?

6. What did Keith do wrong?

7. List three unsafe behaviors that Chris did.
   a.
   b.
   c.

8. List three safe behaviors Chris did.
   a.
   b.
   c.

True or false:

1. Young adults are the fastest-growing demographic among online shoppers.

2. E-Tailing is retail online shopping.

3. Phishing is when you buy an item that does not exist.

4. Anti-virus and anti-spyware software has nothing to do with online shopping.

5. If a bank calls to confirm a transaction, you should provide all the information they are asking for.

6. An ATM PIN is your personal identification number assigned to access your account from an ATM machine.

7. Fraud in online shopping is when someone gets hold of your bank account or credit card number to make online purchases.

8. The availability of pre-paid credit cards is limiting teenagers from making online purchases.

9. Make sure to carry your PIN number on a piece of paper along with your ATM card.

10. Use a strong password when creating an online form.

11. There is no need to save the merchandise receipts once your receive items you have purchased.

12. Pay attention to the items purchased prior to finalizing the payment.

13. If you don't know how to operate an ATM machine, ask the person behind you in line to show you how.

14. A breach of your privacy occurs when a company collects personal information about you when you visit their website.

15. Buying and selling stocks and trading items online is a fun activity to do with friends.

16. Check your bank account regularly to monitor financial transactions.

<u>Activity 5:</u> Online Gaming

Definitions – use your online resources to define the following terms

1. Multi-user games

2. Cyber predator

3. Identity theft

4. Intruder

5. Copyright infringement

6. Griefer

Educate yourself about game ratings and abide by them. Ratings are usually marked on the back of the game box or listed in a review of online games.

What do the following game ratings indicate?

EC
E
E 10+
T
M
AO
RP

Scenario – read the following scenario and answer the following questions.

Steve received an electronic game machine containing eight games as a gift from his grandfather. Steve was very happy for the generous gift and could not wait to link his game to the internet and to the TV to play. One of the games was played by the majority of his friends. He called his friends and asked them to meet him online, and then, after he connected his game machine to the TV screen and connected it to the internet, he created an avatar to represent himself. He gave the avatar a catchy name, Squantaqua. Steve and his friends played for hours every day. When Steve passed all the levels he could, he linked to the internet through his game machine to download a new stage. Steve filled out a form and paid for the game via a credit card given to him by his father for use in an emergency. After downloading the new stage, Steve found to his dismay that he could not run the game and furthermore, his game machine stopped working. To make matters worse, his friends told him that it looked to them like he was still playing in the game using his avatar for two more days when his machine was not working.

Scenario Questions

1. Please provide an ending for this scenario.

2. What didn't Steve do?

3. What would you do differently if you were in Steve's position?

4. Can you list seven safety guidelines Steve should follow in online game play?

5. In your opinion, what happened to Steve's game machine?

From the Carnegie Cyber Academy website:
www.carnegiecyberacademy.com
click on the "Fun Stuff" tab to play the Cyber Defense Quiz game.