

INTERENT SAFETY AND RESPONSIBILITY – CYBER SECURITY

Note: This section can be taught by the technology teacher or classroom teachers with support from the librarian.

Contents:

1. Introduction and Essential Information
2. Required lesson
3. Additional lessons and activities
4. Additional Resources
5. Standards Alignment

1. Introduction and Essential Information

Identity theft, crashed computer systems, nagging computer viruses and spam email have all become a part of the online environment. As computer use continues to increase both at school and home, the risk of compromised security also increases. Criminals wishing to access personal information or hackers choosing to do harm to individual and networked computers have sophisticated methods for carrying out their crimes. At this time there are no simple, comprehensive solutions, but there are a number of behaviors and safe guards that individuals can put into place once they know about them.

The goal of this section on Cyber Security is to help students become aware of the potential risks, to identify ways they can protect themselves and to be able to apply those practices in their computer usage at home.

A list of basic terminology related to cyber security is included on the next page. If you would like a comprehensive list, go to the National Cyber Security Alliance's glossary at <http://www.staysafeonline.org/basics/glossary.html>.

2. Required Lesson

Material for this unit can be covered by using one of the following two presentations:

- Show the movie clip **Security: Malicious Code**. (13:42 minutes) **OR**
- Present the Powerpoint slideshow **Cyber Security** (17 slides).

PLUS:

Present the lesson **Smart E-mailing and IMing too!** (CyberSmart lesson at http://www.cybersmartcurriculum.org/lesson_plans/68_06.asp) This lesson teaches students to use caution when opening email from people they don't know. It also introduces students to spam and how to protect your computer against viruses. This lesson is included as a hard copy and on the disk as a PDF file called **Smart Emailing**.

Vocabulary for Cyber Security Lessons

File extension: a string of letters at the end of a file that indicates the type of file (.exe, .doc.)

Hacking: Breaking into a computer or network illegally.

Malicious code: computer code (programming) designed to do harm to a computer including viruses, worms and Trojan horses.

Phishing: Using a business name illegally in order to obtain information via email.

Spam: To send out unwanted and unsolicited mass e-mailings. They are often commercial advertising and inappropriate. These e-mails may contain worms, viruses or other malicious code.

Spim: Similar to spam, but sent via Instant messaging. It may also contain malicious code.

Steganography: (or “stego”) A technology that allows people to hide files within another file in order to transfer information secretly.

Virus: Computer programs that spread themselves by infecting files. They are usually spread through e-mail attachments.

Trojan horses: Computer programs that claim to do one thing but actually do another when downloaded.

Worms: Computer code that travels through networks via shared files and programs.

Spyware: A program that runs in the background to monitor computer activities without the user knowing it.

3. Additional activities:

1. **Risks of Spyware** (iSafe): Students learn about Spyware and what to do about it. They are encouraged to share the information through public service announcements. This lesson is included as a hard copy and as a PDF file called **5-8 Spyware Risks**.
2. **Private and Personal Information** (online CyberSmart lesson at http://www.cybersmartcurriculum.org/lesson_plans/68_01.asp) Students learn that some websites that look interesting may request private information in order to enter. Students create a collage of personal but not private, information. This lesson is included as a hard copy and on the disk as a PDF file called **Private and Personal Information**.
3. **Cyber Security Tips Brochure:** Students use the several websites to create brochures that they will share with their families. This lesson is included as a hard copy and as a Word document.
4. **“How Safe Are You?”** This online quiz created by the National Cyber Security Alliance can be used to determine how safe and secure your computer is. It would be an excellent homework assignment that students could do with their parents at home. The quiz can be found at <http://staysafeonline.org/basics/quiz.html>.

4. Additional Resources for Cyber Security Information:

Cyber Smart!

<http://www.cybersmart.org/home/>

Free curriculum and professional development is available to educators. All lessons and activities are tied to national standards. Well organized and helpful.

iSafe

<http://www.isafe.org/>

http://www.isafe.org/channels/sub.php?ch=ed&sub_id=media – *direct link to web casts*

Free curriculum, webcasts, and activities for educators, parents, students, and law enforcement agents are available online, print and CD. Student contests are available. It is cumbersome to navigate, but there are many quality resources and training opportunities. The webcasts are especially worthwhile.

National Cyber Security Alliance

<http://www.staysafeonline.org> –

This site is designed for home, school or business computer users. It provides free resources and information about how to protect yourself and your computers. The site has a comprehensive glossary of terminology related to all things related to the Internet.

5. Standards Alignment:

The lessons in this unit address the following ASD, state and national standards for libraries and technology.

ASD Library Standards and Alaska Content Standards for Library/Information Literacy

Standard E: A student should understand ethical, legal, and social behavior with respect to information resources.

Indicator 1: Use library materials and information resources responsibly.

ASD Technology Frameworks

Framework 3.0: Social, Ethical, and Human Issues

3.1.7: Identifies ways that telecomputing promotes a global community

3.1.8: Identifies examples and analyzes societal impact of advanced and emerging

technologies

3.2.1: Respects the privacy of others

3.2.4: Models ethical behavior and acceptable practice in use of technology and technological resources.

3.2.12: Discriminates between types of data as to which are public and private.

3.2.13: Demonstrates knowledge of safe and ethical procedures related to sharing personal information

Alaska Content Standards for Technology

Standard E: A student should be able to use technology responsibly and understand its impact on individuals and society.

Indicator 2: discriminate between responsible and irresponsible uses of technology;

Indicator 3: respect others' rights of privacy in electronic environments;

Indicator 7: integrate the use of technology into daily living;

Indicator 8: recognize the implications of emerging technologies.

ISTE National Educational Technology Standards

(International Society for Technology in Education)

Standard 2: Social, ethical, and human issues

A student who meets this standard should meet the following indicators:

--Students understand the ethical, cultural, and societal issues related to technology.

--Students practice responsible use of technology systems, information, and software.

Standard 4: Technology communications tools

A student who meets this standard should meet the following indicators:

- Students use telecommunications to collaborate, publish, and interact with peers, experts, and other audiences.
- students use a variety of media and formats to communicate information and ideas effectively to multiple audiences

AASL Information Literacy Standards for Student Learning

(American Association of School Librarians)

Standard 2: The student who is information literate evaluates information critically and competently.

- Indicator 1: Determines accuracy, relevance, and comprehensiveness.
- Indicator 3: Identifies inaccurate and misleading information.

Standard 3: The student who is information literate uses information accurately and creatively.

- Indicator 4: Produces and communicates information in appropriate formats.

Standard 8: The student who contributes positively to the learning community and to society is information literate and practices ethical behavior in regard to information and information technology.

- Indicator 3: Uses information technology responsibly.

Standard 9: The student who contributes positively to the learning community and to society is information literate and participates effectively in groups to pursue and generate information.

- Indicator 2: Respects others' ideas and backgrounds and acknowledges their contributions.
- Indicator 3: Collaborates with others, both in person and through technologies, to identify information problems and to seek their solutions.