Lesson Skill: Summarizing information

Strand Reading--narrative nonfiction

SOL 6.5
7.5
8.5

Materials

- Copies of the attached KWL Chart worksheet
- Copies of the attached essay *Do You Value Your Privacy?* by Jared Pierce

Lesson

1. Tell students they will read a short essay about privacy and the Internet. Have them brainstorm what they know about the topic by taking notes on the KWL Chart worksheet. As they generate information, have them categorize it and speculate about what they might learn from the reading. This activity will encourage students to exercise critical thinking and analysis skills. If necessary, model such categorizing by thinking aloud while combining and classifying information.
2. Have students generate a list of topic-related questions they want answered as they read and record the questions in the center column of the worksheet.
3. Have students read the essay, pausing from time to time to try to answer the questions listed in their What I Want to Know column and recording the answers in the What I Learned column. Usually, these are either facts or broad concepts expressed in short sentences.
4. Discuss with the class what they learned. Review the questions raised before reading to determine whether all have been answered. Because students may have questions that are not answered in the essay, this activity should serve as an impetus to find and discuss the answers by research and/or communication with others.
5. Encourage students to map and/or summarize the information from their What I Learned list.

Do You Value Your Privacy?

By Jared Pierce

Do you value your privacy? Most everyone does, but few know how careless they are with it. The Internet has made keeping your private information safe more difficult. You can shop online and sign up for services that make life easier, such as e-mail accounts and online banking. These services are simple, but you may not even realize how much time they save you. With the ease of use for these services comes an increased need to send your personal information through the Internet. How does one stay safe in this online world? The following will answer questions you may have about Web site authenticity and ways to keep your private information private.

How can you be sure Web sites are legitimate? A good indicator is what they have at the bottom of their home page. Sites that allow themselves to be checked by an outside source will have a link on the bottom of the page to that source. The two most common outside sources are TRUSTe and BBBOnline, which stands for the Better Business Bureau online. These two sources will have the site turn in information to see whether it meets certain standards. If it does, it receives certification and is typically a site you can trust. Keep in mind that these labels can be applied by clever cyber criminals to create the illusion you are viewing a safe site. Check with the particular source listed at the bottom of the page to see if the page is authentic before giving the site any of your personal information.

When verifying the authenticity of a site, be sure to note the exact ending of the site's address as well. Domain names will typically end in *.org, .gov, .edu, .com.,* or *.net.* Sites ending in *.gov or .edu* are usually the safest. To obtain these endings, a site must be associated with the government or an academic institution. The ending *.org* is typically used by organizations but does not verify whether they are legitimate or not. If a site ends in *.com* or *.net*, it is either paid for or gained freely. Often, cyber criminals will create site names similar to something familiar to fool users into giving away personal information. Be sure to know if the actual site you want to visit ends in *.com* or *.net.* Knowing the difference can keep you out of lot of trouble.

If you are confused about how to look up a site to see if it is legitimate, perhaps the best tool to use is *whois.net.* This site will tell you who owns the site in question, when it was updated, whether it is secure, and more necessary information. You do not have to understand the cyber jargon a site uses. All you need to know is that the site is registered and can be trusted with your personal information.

On occasion, you may receive an e-mail asking you to update your personal information. Most sites do not require you to update information unless you are making a purchase and they are verifying that the information they have is still up-to-date. However, cyber criminals will use a common scam known as *phishing*. They send out e-mails looking like they came from a genuine site and asking you to update your personal information. If you respond, they can use this information to access your credit card accounts and charge them at will. So, don't do it! Don't respond!

If you keep these safety tips in mind, your chances of falling prey to cyber crooks will drop. Keeping track of who knows your personal information is very important to online safety. You may not have a bank account at this time, but careless online purchasing or browsing habits now could continue when you do get an account. Remember, you are not the only one at risk when a cyber criminal manages to gain access to your computer. Everyone who uses that computer and has at some point left personal information there is in danger. Develop a healthy caution now about trusting Internet sites with your personal information, and you will be better off in the future.

KWL Chart

What I Know	What I Want to Know	What I Learned
Categories of Information:		