Evaluating Web Pages/Dangers of the Web

OBJECTIVE: Upon completion of the **Evaluating Web Pages/Dangers of the Web** component, you will be able to:

- Put into practice evaluation guidelines, including currency, accuracy, objectivity, and authority, when viewing and utilizing Web pages.
- Have information to help you avoid common email phishing scams and social networking problems with your awareness of Internet safety precautions.

It is important to evaluate Web pages very carefully. Since Web pages can be published by anyone, certain Web pages may contain false, hurtful, or inaccurate information. Use the four criteria below for evaluating Web pages.

**Currency**

- Are there dates on the Web page to tell:
  - When the page was written?
  - When it was placed on the Web?
  - When it was last revised?
  - **CAUTION:** Undated or outdated material is no better than anonymous material. Avoid using it.

**Relevance**

- The importance of the information for your needs.
- Does the information relate to your topic or answer your question?
- Who is the intended audience?
- Is the information at an appropriate level (i.e. not too elementary or advanced for your needs)?
- Have you looked at a variety of sources before determining this is one you will use?
- Would you be comfortable citing this source in your research paper?

**Authority**

- Is it clear who wrote the information, and do they provide a list of qualifications and a contact link?
- Is there a link to the institution or organization that sponsored the Web page?
- Is there a way to verify the legitimacy of the sponsor?
- Can you get to the root Web site?
- Is there a link provided to send comments or suggestions to the author?
- **CAUTION:** Avoid using anonymous information on Web pages.

**Accuracy**

- Are the sources clearly listed?
- Is the information free of grammatical errors?
- If there are charts or graphs, are they clearly labeled and easy to read?
- If there any evidence of biasness?
- Are your hopes for the Web page causing your interpretation of the page to become biased?
SUGGESTION: Look for the “About Us” link to find out more about the investors or creators of the Web page.

Purpose

- What are the objectives or goals of the Web page? Does the Web page meet those objectives or goals?
- How detailed is the Web page’s information?
- What is the tone of the Web page? Is it a satirical page or spoof, or is its focus serious or academic?

Also… remember that Web pages are written for different types of audiences. Some Web pages may be appropriate for research or a school paper. Other Web pages are meant for viewing by children or the general population. It is important to determine the audience for a Web page.

Dangers of the Web

Social Networking Tools

Did you know?...

- That social networking Web sites such as Facebook are a rapidly growing component of the Web?
- On these Web sites, as well as blogs and personal Web pages, students and others post information about themselves and their interests.
- Potential employers, schools, and other entities are “Googling” and viewing MySpace.com, Facebook, and other Web pages for background checks?
- Posting information about bad habits (i.e., drinking, gambling, use of illegal drugs, etc.), posting provocative photographs, or making negative statements about your job, your teacher, and others may impact your ability to find a job and have legal ramifications.

Steven Rothberg of College.Recruiter.com, during a 2006 NBC Nightly News interview, stated that a posting on the Web may “be out there forever.” He advises to only post information online that you “would feel comfortable sharing with your grandmother.”


Remember…

- People online are not always who they seem to be. Someone posting to a Web site as a 19-year old student may in reality be a 44-year old sexual predator.
• Anything posted on the Web can become public information.

• Even if you set a privacy setting on your Web page, sending a message to anyone (even if not specified in your settings), may allow that person to view your Web page.

• It is essential to use safety precautions when posting anything to the Web. These precautions include:
  ▪ Do not include any personal information such as your home address and your telephone number on a Web page.
  ▪ Do not give out detailed information about your activities.
  ▪ Do not meet in person with someone you “meet” online. If you do, meet in a public place and take a friend as backup. Be very, very cautious.
  ▪ Use the privacy features on a Web site. They are not 100% secure but can prevent some issues.
  ▪ Do not ever post anything on a Web page that you may be embarrassed about in the future. Do not post anything that could harm you in your career, personal, or school life.
  ▪ Report any user abuse that you may find on the Web.

E-Mail Phishing and Scams

Unscrupulous people and con artists may send unsolicited emails. For example, a common scam is the following:

An email is sent explaining that their money is tied up in another country and, if you will help them by sending a small amount of money for fees or providing bank account access, etc., you will be receive a large amount of money in return. If you fall for this scheme, the con artist(s) gets your money plus possible access to your bank account.

Some scams are easy to detect; others are more difficult to recognize. Phishing is one way in which thieves are able to steal money or someone’s identity.

What is Phishing?

According to the Federal Trade Commission (FTC), “phishers” send an email or pop-up message that claims to be from a business or organization that you may deal with. The message may ask you to “update,” “validate,” or “confirm” account information.” You are given a link to a website “that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information.” In this way, if you respond to a bogus site, the phishers “steal your identity and run up bills or commit crimes in your name.” (http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm). These phishing emails and pop-ups are very tricky, often look very official, and may be hard to detect.
Ways to Protect Yourself from a Phishing Attack

1. Do not reply to an email or pop-up message that asks for personal or financial information. Do not click on the link that may be provided in the email. Do not call the phone number that is provided in the email.
   ♦ If you are concerned, contact that business or bank directly – use a phone number that you know to be correct or open a new web browser and type in the company’s email address yourself. Do not cut and paste the link from the email to the Internet browser.

2. Do not open any attachments related to the email. This could cause a virus, spyware, or other software to be loaded on your computer, creating havoc on your computer and/or allowing your personal information to be leaked.

3. Use anti-virus software, but remember nothing is foolproof. (Sullivan University has anti-viral and firewall protections, but occasionally a hoax email comes through).

4. Do not email personal or financial information if at all possible. Try to buy online from companies that you trust. Always go to the companies’ web address and look at the web address carefully – for example, numbers in the front of a web address usually indicate a scam (for example, http://134.555/www.ebay.com is not a valid web address). If you have begun (initiated) a transaction with a company or organization and need to use credit card information, checking information, etc., look for “indicators that the website is secure,” such as https in the website name (again, nothing is foolproof, so always use caution).

5. Review credit card and bank account information frequently.

If you receive a phishing email