

INTERNET & CYBER SAFETY

Internet & Cyber-Safety is a two hour course designed to familiarize students with web browser basics, search engines, and search strategies. Ethical and safety concerns will also be considered.

Objectives:

- Define Internet and World Wide Web
- Describe the difference between Internet and World Wide Web
- Define basic Internet terminology
- Describe web browsers and their uses
- Identify screen components of Internet Explorer
- Students will identify the basic parts of the world wide web
- Discuss security issues on the internet
- Discuss ethical issues with respect to internet use
- Identify the components of a URL
- Students will learn to understand what the different parts of search results suggest about the content of the pages they offer
- Apply the principles of evaluation to Web sites
- Students will use and compare search strategies using Boolean and operator search modifiers
- Students will understand the importance of strong passwords
- Define “networks”- 2 or more computers connected by cables, telephone lines, radio waves, satellites, or infrared light beams
- Define “internet” - a global network of networks with billions of connected computers
- Define “World Wide Web” - the system we use to access the internet
- Define “Web Browser” – the type of program we use to access the World Wide Web

- Review screen components of Internet Explorer from the top down.

Title Bar:

Minimize:

Restore:

Close:

Address Bar:

.....

Back & Forward Buttons:.....

.....

Tabs:

.....

Status Bar:

.....

- Define “**Hyperlink**” – a command embedded in text or an object which, when clicked, will open another file, take you to another place in the same file or to a new location on the internet.

.....

.....

- Define “**URL**” (Uniform Resource Locator) or Web Address – the global address for documents and other resources on the internet.

.....

.....

- Define “**Search Engine**” – a program that searches documents / web pages for a particular word or set of words and returns a list of pages containing those words and/or set of words.

.....

.....

Internet Search Tips

- **Every word matters.** Generally, all the words you put in the query will be used.
- **Search is always case insensitive.** A search for [new york times] is the same as a search for [New York Times].
- Generally, **punctuation is ignored**, including @#\$%^&*()=+[]\ and other special characters.
- **Keep it simple.** If you're looking for a particular company, just enter its name, or as much of its name as you can recall. If you're looking for a particular concept, place, or product, start with its name. If you're looking for a pizza restaurant, just enter pizza and the name of your town or your zip code. Simple is good.
- **Think how the page you are looking for will be written.** A search engine is not a human; it is a program that matches the words you give to pages on the web. **Use the words that are most likely to appear on the page.** For example, instead of saying [my head hurts], say [headache], because that's the term a medical page will use.
- **Describe what you need with as few terms as possible.** The goal of each word in a query is to focus it further. Since all words are used, each additional word limits the results. If you limit too much, you will miss a lot of useful information. The main advantage to starting with fewer keywords is that, if you don't get what you need, the results will likely give you a good indication of what additional words are needed to refine your results on the next search. For example, [weather Cancun] is a simple way to find the weather and it is likely to give better results than the longer [weather report for Cancun Mexico].
- **Choose descriptive words.** The more unique the word is the more likely you are to get relevant results. Words that are not very descriptive, like 'document,' 'website,' 'company,' or 'info,' are usually not needed. Keep in mind, however, that even if the word has the correct meaning but it is not the one most people use; it may not match the pages you need. For example, [celebrity ringtones] is more descriptive and specific than [celebrity sounds].

(Some of these tips were copied from <http://support.google.com/websearch/bin/answer.py?hl=en&answer=134479> on April 13, 2012. Although sourced from Google, they also apply to searches using any search engine.)

INTERNET SCAVENGER HUNT

- When did William Barret Travis write his famous letter from the Alamo?
Answer:
- What are the words of the Pledge of allegiance to the Texas State Flag?
Answer:
- Who was the “Bandit Queen of Dallas?”
Answer:
- Who declared the “hook ‘em horns” the official UT hand symbol in 1955?
Answer:
- Where was Lyle Lovett born?
Answer:
- Where is the museum for East Texas Culture located?
Answer:
- What was the name of the school in Rusk Country where a natural gas leak led to an explosion, killing 319 students and teachers.
Answer:
- What town was the Edwards County seat from 1883 – 1891?
Answer:
- What is the estimated number of songs with Texas or Texas places in the titles?
Answer:
- What is the Texas State Shell?
Answer:
- The King Ranch is bigger than what state?
Answer:
- Where was Sam Houston born?
Answer:
- What children’s book was set in Camp Green Lake Texas?
Answer:

How to Evaluate a Web Page

- **Purpose:** Why was the page created? To:
 - Inform
 - Entertain
 - Advertise or Sell a product or service
 - Influence views, beliefs, elections
 - Provide up-to-the-moment news
 - Personal enjoyment
- **Sponsor/Owner:** On what type of Internet provider or organization does the page reside?
 - Government agency
 - Educational
 - Business/Company
 - Association: Professional, Trade, Entertainment
 - News bureau: television, newspaper, radio
 - Personal (Individual)
- **Organization and Content:** Is the page organized and focused? Is it well designed? Is the text well written? Are the links relevant and appropriate? Are the links evaluated?
- **Bias--political or issue stance** (of the author or sponsor): Most web pages have an inherent bias that will impact the way information is conveyed on them. Is the author or sponsor:
 - left/liberal?
 - right/conservative?
 - center?
 - a political action group or association?
 - a business?
- **Date of Production/Revision:** When was the web page produced? When was it last revised? How up-to-date are the links? Are the links still viable?
- **Usefulness:** Is the web page relevant to your search?
- **Authority/Author** Who is responsible for the page? Is the author an expert in this field? What else has he/she written or produced? Does the author provide an e-mail address? How accurate is the provided information? Is a bias evident?
- **Audience:** To what type of reader is the web page directed? Is the level appropriate for your needs? Is the page for:
 - general readers?
 - students (elementary, high school, college, graduate)?
 - specialists or professionals?
 - researchers or scholars?
- **Coverage:** Does the page cover the topic comprehensively, partially or is it an overview?
- **Illustrations:** Are the graphics clear in intent, relevant and professional looking? Do the graphics add to or enhance the content?
- **Security** Are security and/or encryption systems employed when necessary?

WEBSITE EVALUATION RUBRIC

[HTTP://WWW.LOC.GOV/EXHIBITS/LEWISANDCLARK/LEWISANDCLARK.HTML](http://www.loc.gov/exhibits/lewisandclark/lewisandclark.html)

WEBSITE # 1	1	2	3	4	5
Purpose					
Sponsor/Owner					
Organization and Content					
Bias--political or issue stance					
Date of Production/Revision					
Usefulness					
Authority/Author					
Audience					
Coverage					
Illustrations					
Security					

NOTES:

.....

[HTTP://WWW.UNMUSEUM.ORG/UNMAIN.HTM](http://www.unmuseum.org/unmain.htm)

WEBSITE # 2	1	2	3	4	5
Purpose					
Sponsor/Owner					
Organization and Content					
Bias--political or issue stance					
Date of Production/Revision					
Usefulness					
Authority/Author					
Audience					
Coverage					
Illustrations					
Security					

Internet Basics Terminology

Adware: A malicious code that displays unsolicited advertising on your computer.

Blog: A personal or professional journal kept on a Web site which is updated frequently. Blogs generally have a theme and can be private or public.

Chat room: An online site used for social interaction, usually based on a topic or theme, where people with shared interests can “chat” with others.

Content filtering: Allows you to block internet access to certain types of content.

Cookie (also referred to as a Tracking cookie, browser cookie, HTTP cookie) : Cookies are small pieces of text stored that a web browser places on a user’s computer.

Cyberbully, cyber bullies, cyberbullying: Bullying that occurs online.

Cyber crime: Criminal activity that targets computers or uses online information to target real world victims.

Download: Transfer material from a server or remote computer to your computer.

Email Signatures: this is a block of text added at the end of emails. It often contains your full name, possibly your Job description, location, phone number, an inspirational thought etc.

File sharing: Refers to the ability to store files either in a central place that can be shared with as few as one other person, or publicly.

Freeware: This is software that is owned and copyrighted, but that the owner is giving away for free.

Identity theft: Stealing someone’s identity in order to impersonate them.

Malware: stands for Malicious softWare and is an umbrella term that includes any type of harmful code – “trojans”, “worms”, “spyware”, “adware”, etc that infiltrate a computer without consent of the computer user and are designed to damage the computer, collect information, or allow your computer to be subverted and used remotely to send spam etc.

Phishing: the attempt by people to impersonate a business in order to trick you into giving out your personal information.

Posting: Means to upload information to the web

Scam: to con, cheat, trick, swindle, others.

Shareware: Shareware is method of product advertising that lets you 'try before you buy'. This type of software can be downloaded from the Internet or may be distributed as a CD and can be used free of charge.

Social networking: Refers to a category of Internet applications to help connect friends, business partners, or other individuals together using a variety of tools

Spam: Unsolicited e-mail attempting to sell you something. Also known as junk mail.

Spyware: is stealthy software that leverages your Internet connection to collect information about you without your knowledge or consent and sends it back to whomever wrote the spyware program. Like adware it is often installed when you download 'freeware' or 'shareware' programs. Spyware may be looking for your banking information, personal information, etc. It is illegal and pervasive.

URL: (Uniform Resource Locator) refers to a unique internet address of a file or destination. To find a particular site or document you type the URL into the browser window and the browser will bring up that particular address.

Virus: a computer program which can duplicate itself and spread from one computer to another.

Web Page: a document on the web. Each web page has a unique URL.

Web Site: a group of related web pages.

Web Server: computers connected to the Internet that host web sites.

11 Tips for Safe Online Shopping

These tips have been abbreviated for the sake of space. Read the full text at <http://www.pcmag.com/article2/0,2817,2373131,00.asp>

1. **Use Familiar Websites:** Start at a trusted site rather than shopping with a search engine.
2. **Look for the Lock:** Never ever, ever buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least. You'll know if the site has SSL because the URL for the site will start with HTTPS:// (instead of just HTTP://). An icon of a locked padlock will appear, typically in the status bar at the bottom of your web browser, or right next to the URL in the address bar.
3. **Don't Tell All:** No online shopping store needs your social security number or your birthday to do business. When possible, give the least amount of information possible.
4. **Check Statements:** Go online regularly and look at electronic statements for your credit card, debit card, and checking accounts. If you see something wrong, pick up the phone to address the matter quickly.
5. **Inoculate Your PC:** You need to protect against malware with regular updates to your anti-virus program.
6. **Use Strong Passwords:** We like to beat this dead horse about making sure to utilize strong passwords, but it's never more important than when banking and shopping online.
7. **Think Mobile:** There's no real need to be any more nervous about shopping on a mobile device than online. The trick is to use apps provided directly by the retailers, like Amazon, Target, etc.
8. **Avoid Public Terminals:** Hopefully we don't have to tell you it's a bad idea to use a public computer to make purchases, *but we still will. If you do, just remember to log out every time you use a public terminal, even if you were just checking email.*
9. **Privatize Your Wi-Fi:** If you do decide to go out with the laptop to shop, you'll need a Wi-Fi connection. Only use the wireless if you access the Web over a virtual private network (VPN) connection.
10. **Count the Cards:** Gift cards are the most requested holiday gift every year, and this year will be no exception. Stick to the source when you buy one; scammers like to auction off gift cards on sites like eBay with little or no funds on them.
11. **Know What's Too Good to Be True:** Skepticism, in most cases, can go a long way toward saving you from a stolen card number.

Social Networking Safety Tips (from AARP)

Social networking websites such as MySpace, Facebook, Twitter and Windows Live Spaces are services people can use to connect with others and to share information such as photos, videos and personal messages. As the popularity of these social sites grows, so do the risks of using them.

1. **Use caution when you click links** that you receive in messages from your friends on your social website. Treat links in messages on these sites as you would links in email messages.
2. **Know what you've posted about yourself.** A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, home town, high school class or mother's middle name.
3. **Don't trust that a message is really from who it says it's from.** Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out.
4. **To avoid giving away email addresses of your friends, do not allow social networking services to scan your email address book.** When you join a new social network, you might receive an offer to enter your email address and password to find out if your contacts are on the network. The site might use this information to send email messages to everyone in your contact list or even everyone you've ever sent an email message to with that email address. Social networking sites should explain that they're going to do this, but some do not.
5. **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.
6. **Be selective about who you accept as a friend on a social network.** Identity thieves might create fake profiles in order to get information from you.
7. **Choose your social network carefully.** Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card.
8. **Assume that everything you put on a social networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.
9. **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the Web.
10. **Think twice before you use social networking sites at work.**
11. **Talk to your kids about social networking.**