Internet Basics

ABOUT THIS CLASS

This class is designed to provide a basic introduction to accessing and navigating the internet (a.k.a. the "world wide web" or "the web"). Throughout the class, we will orient ourselves to the basic layout and functions of a web browser and learn to navigate the internet safely. We will also cover the basics of searching for information on the web. It is impossible in the short time we have to become proficient in even just the basics of using the internet, but it is my hope that this class will provide a good foundation for your future endeavors on the World Wide Web!

Course Objectives

By the end of this course, you will be able to:

- ✓ Connect to the internet
- ✓ Use an internet browser
- ✓ Navigate the internet safely
- ✓ Use a search engine to find information
- ✓ Save websites for easy access ("Bookmarks" & "Favorites")

This booklet will serve as a guide as we progress through the class, but it can also be a valuable tool for when you are working on your own. Any class instruction is only as effective as the time and effort you are willing to invest in it. I encourage you to practice soon after we have completed the class. There will be additional computer classes in the near future, and I am always available for questions during Tech Tuesdays (call to confirm the time).

Remember that the library has many additional books and resources to help you. Never hesitate to ask any of the Sisson Library staff to locate some resources for you.

Meg Wempe, Adult Services Librarian

Connecting to the Internet

Checking your Internet Connection

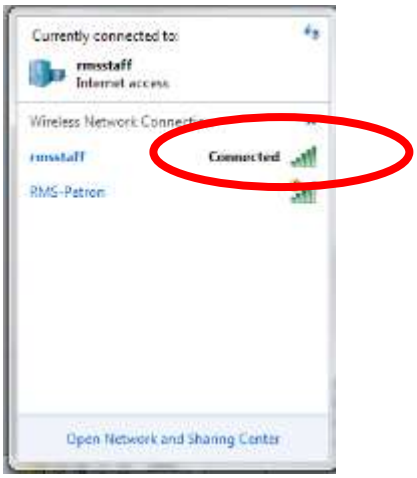
Before you can begin using the internet, you need to check to make sure you have an internet network connection, also called a LAN ("Local Area Network"). There are two ways to connect to the internet: **wired** and **wireless.**

Wired Connection: Wired LANs use Ethernet cables and network adapters and generally also require central devices like hubs, switches, or routers to accommodate more computers.[1]

Wireless (WiFi) Connection: WiFi is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections.[2]

Am I connected? On most PCs there is an icon in the notification area that gives the status of your internet connection:

Click on the bars to see your internet connection status:



[1] http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm

[2] http://en.wikipedia.org/wiki/Internet_access

If you are not connected, select the network you wish to connect to and enter the network password (if necessary). Many **public networks** do not require a password. These are called **open networks**. When using an open network know that, because they are "open," some of what you are doing online can be viewed by others. We'll discuss some safety tips later on.

Using an Internet Browser to Access the Internet

Once you have confirmed that you have a connection to the internet, you can log on to the internet via a **Web Browser**.

Web Browser: A web browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.[3] Simply put, a **browser** allows you to access and use the internet.

What browser can I use?

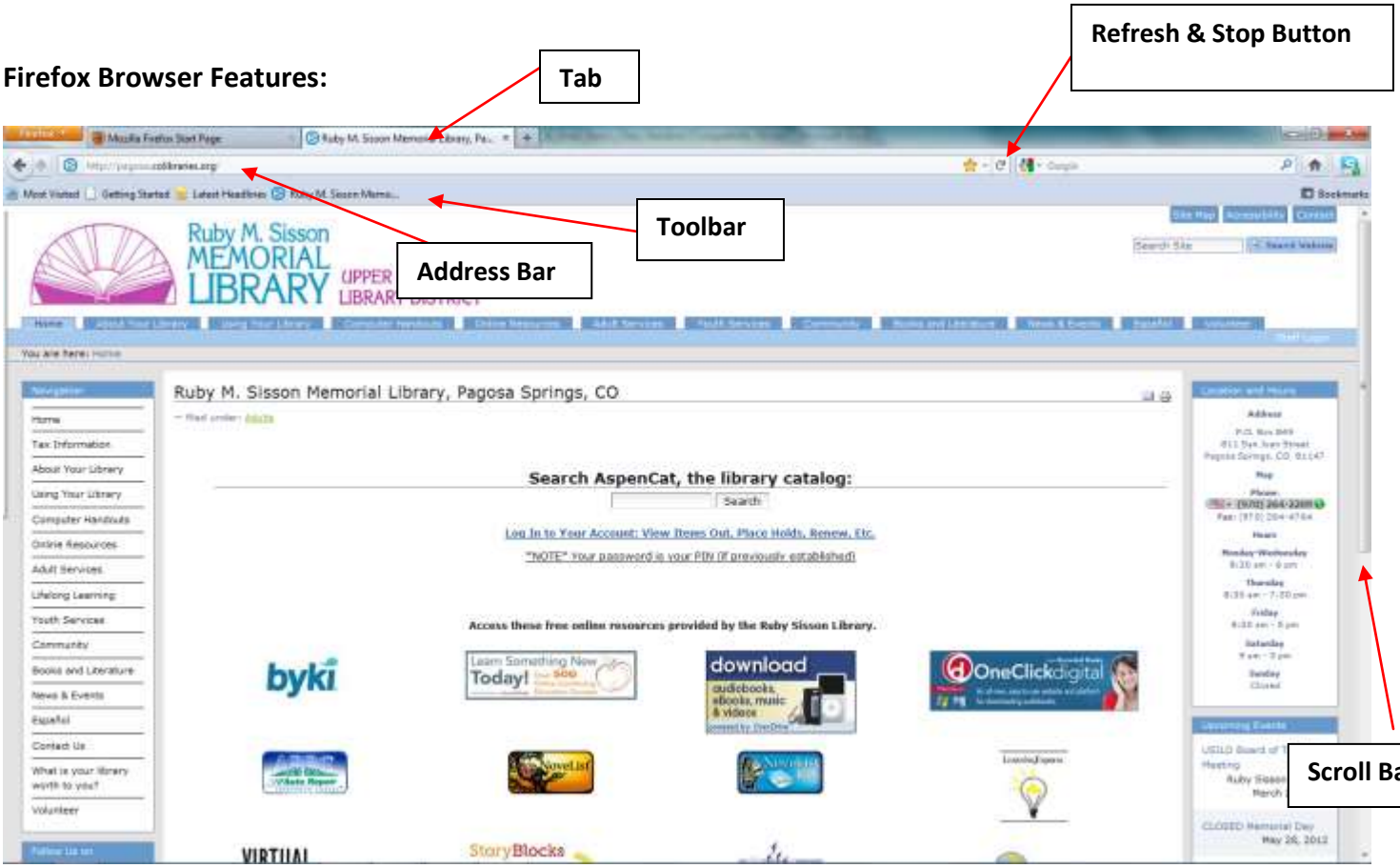
There are a range of browsers that are all free to use (most require that you download and install them prior to use.) Some of the most common browsers are:

- **Internet Explorer** (Microsoft)
- **Mozilla Firefox**
- **Safari** (for Macintosh Users)
- **Chrome** (Google)

All library computers have **Internet Explorer** and **Mozilla Firefox** already installed and ready to use. **Internet Explorer** is the most widely used browser due to its safety (which also means that it runs slower). **Firefox** is fast and user-friendly. We'll be using **Firefox**, though much of what we cover can be applied to most other browsers.

[3] http://en.wikipedia.org/wiki/Web_browser

Firefox Browser Features:



- The **Address Bar/Location Bar** – A box at the top of the browser window that displays the entire URL, or web site address. Also where you type a new address.
- The **Refresh and Stop Buttons** – located on the address bar line. These reload or stop a page load.
- The Links **Toolbar** – where shortcuts to your favorite websites are located.
- **Display Window** – that part of the browser that displays the content of the website you are visiting.
- **Scroll Bars** – navigation and directional bars located at the side (and sometimes bottom) of the display window that allow you to scroll down to see addition content.

- **Status Bar** – The box at the bottom of the browser window. This displays various pieces of information but mostly it shows the load speed and web site address of whatever address your mouse is hovering over.[4]
- **Tabs** —Different display windows open in the same browser.

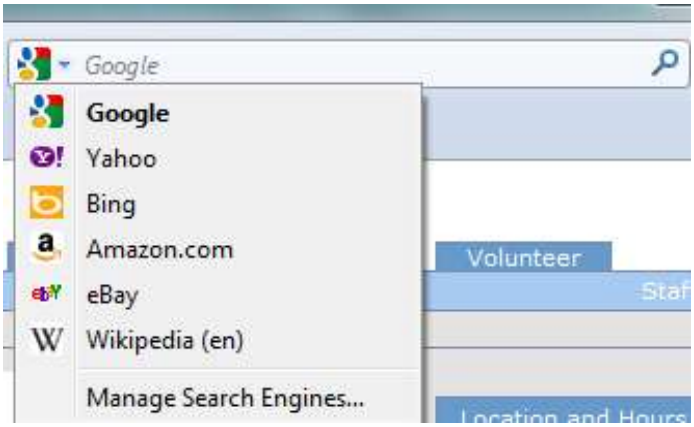
Searching the Web

To search the web, enter keywords and terms into a **Search Engine.** A **search engine** is designed to search for information on the World Wide Web. The information may consist of web pages, images, information and other types of files.[5]

Which search engine can I use?

- **Google**
- **Bing** (Microsoft)
- **Yahoo**

To begin a search in a search engine, you can either go to the website address of the search engine (such as **google.com**) or use can enter your terms directly into the search engine box in Firefox and then hit **enter** or click on the magnifying glass:



[4] http://www.ebpl.org/pdf/classdocs/BrowserBasics.pdf

[5] http://en.wikipedia.org/wiki/Search_engine

Knowing when a site is Secure

Using the internet is usually a very safe activity, but staying safe on the web requires acting responsibly and taking precautions. One of the easiest ways to know whether or not it is safe to enter personal information is checking to see whether a website is **secure.**

HTTP vs HTTPS

All website addresses use **http** or **https** at the start of their web address. HTTP stands for Hypertext Transfer Protocol. It's the first element you see in any URL and you can think of it as the language used to deliver information over the web. Most web browsers (including Internet Explorer) use an encrypted protocol called Secure Sockets Layer (SSL) to access secure webpages. These pages use the prefix HTTPS. The "s" stands for secure.

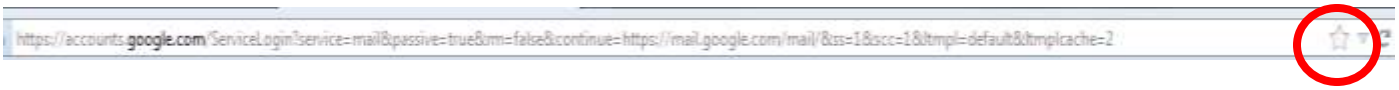
If you're just browsing the web and not entering any sensitive information, http:// is just fine. **However, on pages that you enter your password, credit card number, or other financial information, you should always look for the https:// prefix. If you don't see the "s," don't enter any information that you want to keep secure**.[6]

Favorites & Bookmarks (saving your favorite pages)

You can save your favorite websites (such as your email website, search engines, news sites, or the library's website) for easy access in the future by saving them to your **Bookmarks, Toolbar, Favorites,** or **Homepage.**

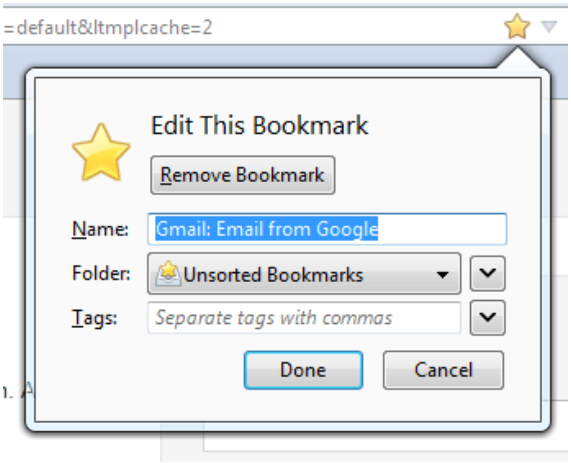
Bookmarking a site in Firefox:

Click on the Star at the end of **address bar:**



The star will then turn yellow, which means that the website is bookmarked. To edit (or sort) your bookmark, click the star again:

[6] http://blogs.msdn.com/b/securitytipstalk/archive/2011/04/04/http-vs-https-what-s-the-difference.aspx



From here, you can choose what to name the bookmark and where it is located (e.g. your bookmarks folder or on the toolbar at the top of your browser). You can also remove the bookmark, too.

Additional Safety Tips

Below are some additional safety tips for using the internet responsibly. The best mode of protection is to be cautious and vigilant—if you have any doubts about whether or not you should give out personal information, don't!

Eight Tips for Becoming Safe Online

1. Create stronger passwords.
2. Don't expose personal information.
3. Don't fall for Email scams.
4. Know who you're doing business with.
5. Be cautious with Email attachments.
6. Use software to avoid malware.
7. Be careful how much personal information you give away online.[7]

Beware of online fraud

According to the Federal Trade Commission, 31 percent of reported victims of identity theft are young people. Teenagers make attractive targets because they have good credit ratings and little debt, and they tend to be less savvy than adults about how to keep personal information secure.

Some things that your children should know in order to be smart consumers and avoid online fraud:

- Never share personal information. Don't give out personal information, such as your full name or hometown, in an instant message (IM) or a chat room unless you are certain of the identity of the person with whom you are chatting.
- Log off in public. If you use computers in a library or Internet cafe, log off completely before you leave. You don't know what software is installed on these computers or what it does and it might have keystroke tracking software installed.

[7] Criddle, Linda and Nancy C. Muir. *Using the Internet Safely for Seniors for Dummies*. Detroit: Gale Cengage Learning, 2009, pp. 13-14. (Available at the Ruby Sisson Library!)

- Create secure passwords and keep them secret. For more information see item 1 above.
- Use only secure sites. If your kids shop on the web, they should be sure the URL of any site where they enter financial information begins with https:// and features a yellow lock icon in the bottom right corner or a green address bar. They can click the icon or address bar to check the security certificate for the site.
- Recognize and report fraud. Teach your kids about the warning signs of identity fraud: preapproved credit card offers, calls from collection agencies, or unfamiliar financial statements. If your child suspects identity fraud, take action immediately to limit the damage. Contact their credit card company, banks, all three credit reporting agencies, and the police. Close any fraudulent accounts, and tell them to change their passwords for all online accounts. Keep records of all actions that you've taken.[8]

Don't type in credit card numbers or passwords

These measures provide some protection against casual hackers and identity thieves who prey on wireless networks. But if criminals are determined enough, they will eventually find a way to get around any security system.

If you want to be safe, avoid typing any sensitive information, such as your credit card number or any other financial information, while you use a public wireless network.

Tip: If you must enter credit card numbers while using a public wireless network, make sure there is a locked padlock icon at the bottom right corner of the browser window, and make sure the web address begins with https: (the "s" stands for secure).[9]

How to recognize scams

New scams seem to appear every day. We try to keep up with them in our Security Tips & Talk blog. To see the latest scams, browse through our fraud section. In addition, you can learn to recognize a scam by familiarizing yourself with some of the telltale signs.

Scams can contain the following:

- Alarmist messages and threats of account closures.
- Promises of money for little or no effort.

[8] http://www.microsoft.com/security/family-safety/childsafety-internet.aspx

[9] http://www.microsoft.com/security/online-privacy/public-wireless.aspx

- Deals that sound too good to be true.
- Requests to donate to a charitable organization after a disaster that has been in the news.
- Bad grammar and misspellings.

Popular scams

Here are some popular scams that you should be aware of:

Scams that use the Microsoft name or names of other well-known companies. These scams include fake email messages or websites that use the Microsoft name. The email message might claim that you have won a Microsoft contest, that Microsoft needs your logon information or password, or that a Microsoft representative is contacting you to help you with your computer. (These fake tech-support scams are often delivered by phone.)

Rogue security software scams. Rogue security software, also known as "scareware," is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure you into participating in fraudulent transactions. These scams can appear in email, online advertisements, your social networking site, search engine results, or even in pop-up windows on your computer that might appear to be part of your operating system, but are not.

What to do if you think you have been a victim of a scam

If you suspect that you've responded to a phishing scam with personal or financial information, take these steps to minimize any damage and protect your identity.

- Change the passwords or PINs on all your online accounts that you think might be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent email message.
- If you know of any accounts that were accessed or opened fraudulently, close those accounts.
- Routinely review your bank and credit card statements monthly for unexplained charges or inquiries that you didn't initiate.[10]

[10] http://www.microsoft.com/security/online-privacy/phishing-scams.aspx