Browsing the Internet and Staying Safe: Seniors Session (2)

Instructor: Daniel Chong **Email: dchong@mybpl.org**

What Is An Internet Browser?

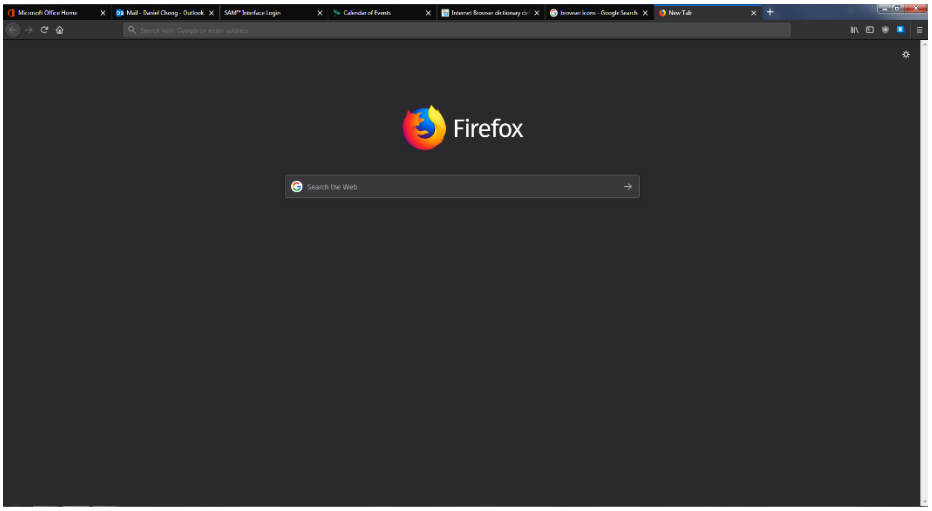
Before we can start surfing the web, we first must be able to connect to it. The standard way of doing this is by connecting through an Internet Browser. To define an internet browser we can say it is: "A software application used to locate and display Web pages." Two of the most popular browsers today are Google Chrome and Microsoft Edge (New Internet Explorer) with Mozilla's Firefox bringing up the third largest market share. If you are using a Mac, then the default browser is called Safari.

All the different browsers work in the same basic way. When we double [left] click on the icon* (Seen Below) on our desktop, it will bring up the home page that we have set or a blank page that we can then search or enter a destination directly to.

Navigating Our Browser

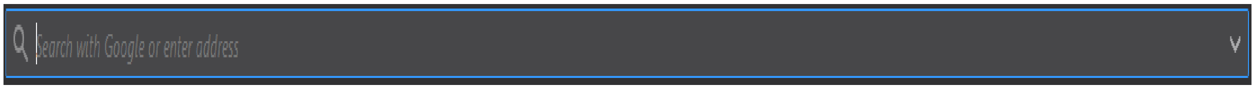
The landing page, or first thing that opens when we run the browser, can be changed to whatever we'd like. Depending on the browser you have installed the landing page will be different, but usually it is some sort of search engine or news such as yahoo's front page.

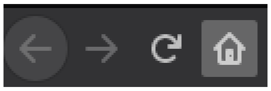
It will look similar to below.


Microsoft Office Home
Mail - Daniel Chong - Outlook
SAM™ Interface Login
Calendar of Events
Internet Browser dictionary def
browser icons - Google Search
New Tab
Search with Google or enter address
Firefox
Search the Web

From this page we can go anywhere on the internet. First let’s break the page down into its parts to better understand the User Interface.

The most important part of any web browser will be the URL bar. This is the bar that is located at the top of the screen, just below where our tabs live and just above the main body of the page. Here we can enter in a web address, such as google.com and be redirected there or we can do a search and be directed through whatever search engine we have set as our default.





To the left of our search bar, we can see that we have to arrows. These are our navigation buttons. They will allow us to take one step, forwards or backwards, in our session history. Your session history is just any pages that you have opened in that instance of your browser session.

Next to the arrows, we have the refresh button (circular arrow). This will allow us to refresh a page to get the most recent iteration of that website. For example if we are reading articles on the New York Times website and we want to see if there are any new articles, we could hit the refresh button and the newest ones would appear.

Finally we have a button that looks like a house, this is our home button and it will simply take us back to whatever our landing page is.

To the right of the navigation bar, we have our tools section. Most commonly this will hold things that we can use to make our life easier, such as our bookmarks and extensions. You will also find your settings here, in Firefox and Chrome they are three lines or dots, and in Internet Explorer it is a gear. Click on this and you will find a myriad of settings to customize and change, which will be easier to follow along with in class and take notes on things you would like to change.

Follow Along

Setting Up and Using Email

Many conversations happen over email, and today having one is almost critical. From staying in touch with loved ones, to signing up for an Amazon account we can use an Email address to do a multitude of things.

Luckily setting one up is very easy!

There are many different providers such as Gmail, Yahoo Mail, Hotmail, AOL, and so on. Choose one that fits your needs, most of them have the same basic framework of how they work.

Today we will set up a Gmail account and go through the basics of using it, such as sending an email, checking an email, and signing up for something and verifying the email address.

Follow Along

Cloud Storage

I'm sure that we have all at least hear about this new thing called the "Cloud," and while it can seem confusing at first it is actually rather simply idea. The basic idea behind the Cloud is storage.

When computers first came into the home in modern PCs they had physical storage on what was called disks. This allowed us to save our files and come back to them later.

This Photo by Unknown Author is licensed under CC BY

As technology advanced and the internet evolved, we found that we could send files over the internet to be stored somewhere else other than our actual computer hard drive. This is what the Cloud is.

The cloud is a collection of servers at a remote location that allow us to send data to be stored within those servers. Popular Cloud Services are: Google Drive, OneDrive and Dropbox. OneDrive is the standard cloud service from Microsoft that comes on all Windows 10 machines, it is free with a premium version offering unlimited storage. This same service plan follows for all Cloud Services, free for limited storage and premium for unlimited.

Luckily most of these Cloud Services offer a large amount of free space, so unless you are using it exclusively for all your storage you will most likely not run out of space.

To start using one of these services just make and account (it is usually tied to an email address) and start saving files. It works just like a regular save, except instead of “saving” it you are instead uploading it.

Follow Along

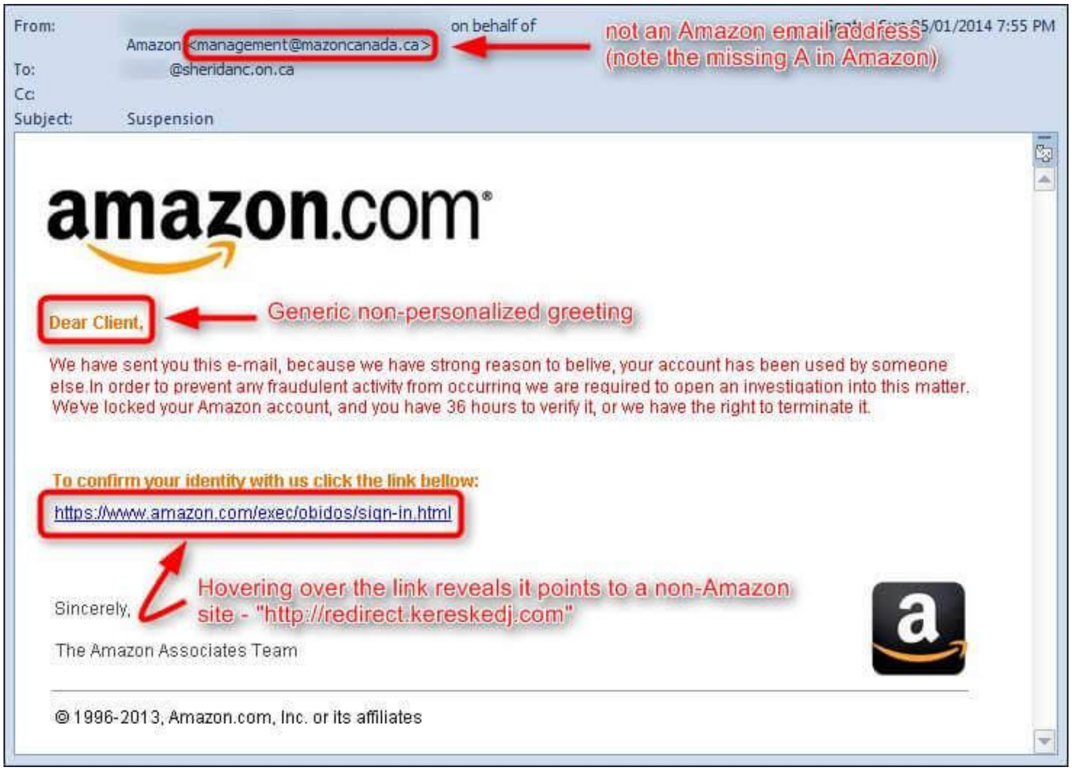
Email Phishing and General Malware

As with all things good, there is always someone who tries to take advantage, and with computers it is no different. One of the most common ways people try to take advantage of each other over the internet are scams that fall under the category of Email Phishing.

When we make an email account and sign up for services the service provider gets access to our email account NAME. This is put on a list and sometimes it is stolen (and then sold on the Black Market) in a data breach or the company sells it for a profit. When this happens, criminals are able to get a hold of these email lists and then send out scams to all the accounts on that list. This is called Email Phishing.

Email Phishing can be defined as any scam or nefarious action taken over email, with the goal of getting as much personal information about you as possible with the hope of stealing your identity. Popular ways people do this is by sending out emails that look like they are from legitimate businesses to try and get you to sign in to your account associated with that information.

Luckily Phishing can be easy to spot. As seen in the image below.



From: [redacted] on behalf of Amazon <management@mazoncanada.ca> 5/01/2014 7:55 PM
To: [redacted]@sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address
(note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Other uses of Email Phishing can be to get you to click on a link that takes you to a nefarious website that will do what is called a “Drive-By Download” and this will stealthily install some sort of program onto your computer that will collect information. Be it a keylogger or ransomware it can and will be detriment to your system, but again, luckily as it is easily spotted, most of this malware can be removed from your computer.

Removing and Preventing Malware

If you have a Windows computer, you already have a default and competent anti-virus in Windows Defender. There are many other solutions out there, such as BitDefender, Norton, McAfee and Avira, but for standard reasons the Windows De fender will catch most if not all malware.

If something did get through, I encourage you to download a program called, Malwarebytes. This is a second opinion scanner, which we use here at the library, and it offers a free and a pro version. The free version will scan on command, while the pro version will scan in the background. For our needs the free version will do. If you ever think your computer is compromised, simply double click on the desktop icon (blue M) and hit the green, “Scan Now” button in the middle. This will perform a virus scan and when its done we will have the option to review, quarantine and delete all potentially unwanted programs it may find.

Browser Add-ons

On top of an anti-virus, we can install browser add-ons which enhance and protect our browser in real-time. Many of these are free and lightweight programs developed for the community, by the community.

The 3 I suggest using are called:

1. Ublock Origin
2. Privacy Badger
3. HTTPSEverywhere

With these three activated, you will not experience adds, your computers browser can no longer be tracked via third parties, and you will have a secure internet connection to whatever website you are visiting IF they offer HTTPS.

While adding these programs is purely optional, they do offer more protections. Nothing can beat yourself though, common sense is the best antivirus. So remember, if it looks sketchy, it probably is sketchy!