Accessing Information Online

This module will discuss the basics of safely accessing information online, including how to conduct safe and productive internet searches, how to assess whether a website is safe, whether information on a site is accurate, and how to be safe when downloading files.

can code communities

Orleans Digital Literacy Initiative

Internet Searches

Orleans Digital Literacy Initiative

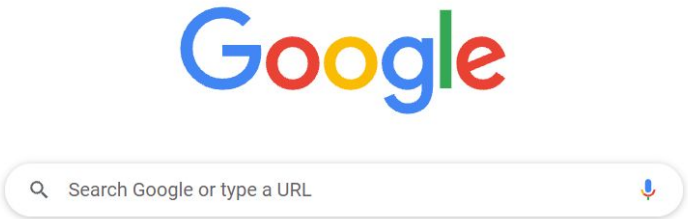
Safe and Productive Internet Searches

One important skill to have when working on the internet is how to search for resources and get information from trusted sources.

Orleans Digital Literacy Initiative

Google

Google is the most common search engine here in the United States. When accessing Google.com you are provided with a search bar that you can then use to search by using **keywords.**

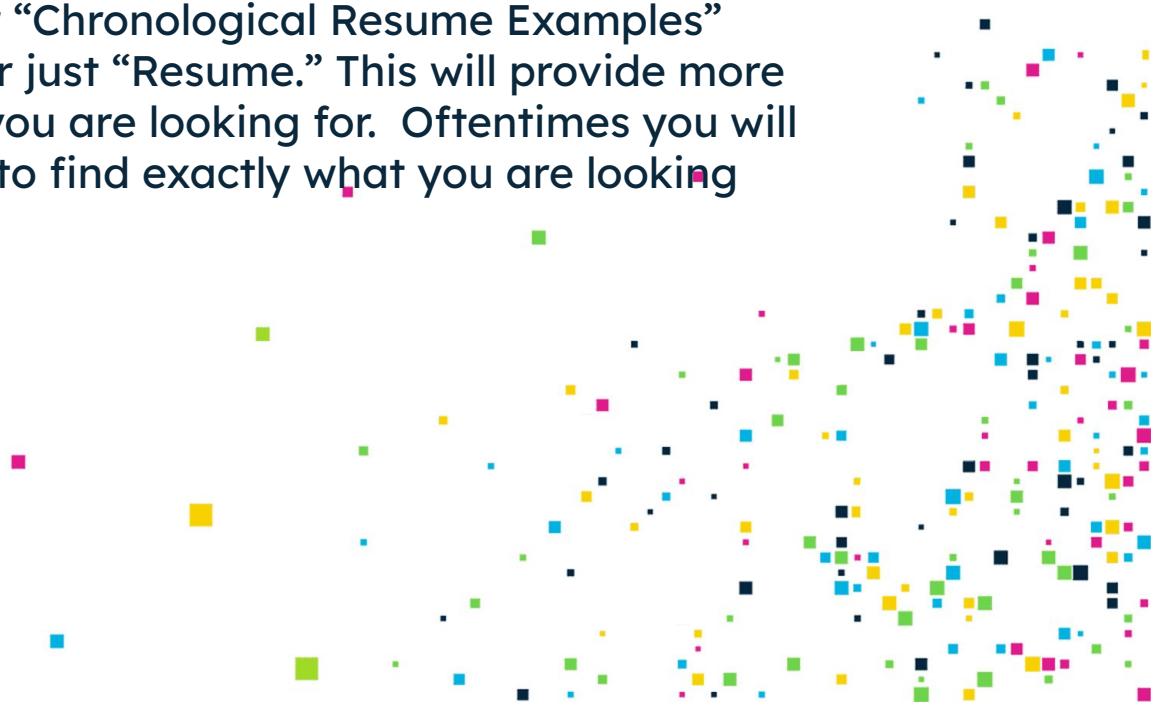


Keywords are words that describe the topic you are searching for. For example, if you are searching for examples of resumes, using a keyword search of “Resume Examples” will provide better results then just searching the word “Resume.”

Orleans Digital Literacy Initiative

Keywords

You want to make sure your keywords are specific enough, but not too specific. For example, if you want to search for examples of a chronological resume, search for “Chronological Resume Examples” instead of “Resume Examples” or just “Resume.” This will provide more specific search results for what you are looking for. Oftentimes you will need to make multiple searches to find exactly what you are looking for.



Orleans Digital Literacy Initiative

Other Search Engines

There are many other search engine options such as **DuckDuckGo** and **Microsoft Bing.** Bing is similar to Google, but is hosted and run by Microsoft. DuckDuckGo is built around privacy and does not save or sell your information. This can be helpful if you want to minimize tracking of your information online.

DuckDuckGo

Bing

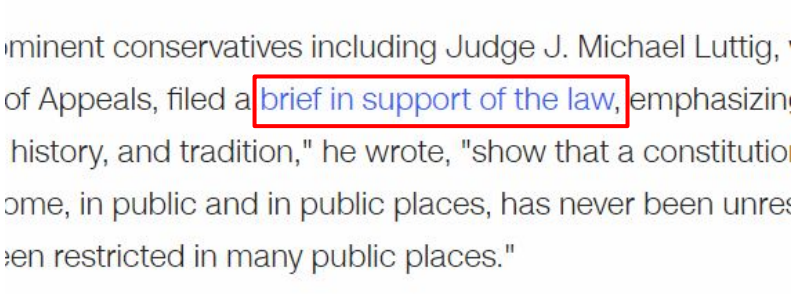
Orleans Digital Literacy Initiative

Is this Information Accurate?

Always see if the website provides a link or a citation that shows where the information is coming from. The biggest thing you can do to make sure information is accurate is using websites that reference validated sources.

CanCode Communities. (2021, October 29). *CanCode communities, Microsoft team up to introduce students to Tech Careers*. CanCode Communities. Retrieved November 2, 2021, from https://cancode.org/albanycancode/cancode-communities-microsoft-team-up-to-introduce-students-to-tech-careers/.

Example of a citation in an online article



Example of a link within an online article that will bring you to a citation.

Orleans Digital Literacy Initiative

Is this Information Accurate? (Continued)

Checking a website for spelling and grammar errors is a good way to quickly assess if the website is legitimate or potentially unsafe to use.

A good rule of thumb is to only visit trusted websites from sources such as major news outlets or websites from companies or organizations that you already know.

→ EVEN TRUSTED SOURCES MAY HAVE INACCURATE INFORMATION.

Questions to Ask When Conducting Web Searches

- ★ Is this website an unbiased source of information or do they have something to gain from sharing this information?
- ★ Can you find other sources that say the same thing and cite the same references?
- ★ Is this a well-known website? Does it cite known people or organizations?
- ★ Who runs this website? Is it an individual or an organization?
- ★ Does this website have a history of putting out false or misleading information?
- ★ Is this website making an offer that is too good to be true?
- ★ Is this something I need to click on?

Orleans Digital Literacy Initiative

Questions to Ask When Conducting Web Searches

- ★ Is the website easy to use?
- ★ Is there anything frustrating or weird about the website?
- ★ Are there a lot of pop-ups?
- ★ Is the website's spelling and grammar correct?
- ★ Who is the author of this website?
- ★ Where was the source published?
- ★ Why did the author create this website?

Orleans Digital Literacy Initiative

Sharing Information Online

Orleans Digital Literacy Initiative

Sharing Information Online

When posting information or data online, it is important to be aware of what you are sharing and the potential for misuse.

You should always be aware of the information and data you are sharing when you are posting to social media platforms, shopping online, signing up for accounts, and any time you enter your Personally Identifiable Information (PII) on a device.

Personally Identifying Information (PII) is any information that can be used to figure out who you are and potentially steal your identity. This includes your name, birthday, address, social security number, credit card information, and more.

Personally Identifiable Information

- ★ Make sure that files with PII are stored in places that your employer or organization wants them to be stored.
- ★ Make sure that files downloaded to your computer are erased to avoid being opened by individuals that should not be accessing them.
- ★ Make sure any files or images you store on a mobile device are saved in the correct places and are removed from any place that is unsecure, in case of loss or theft of the device.

Social Media Tips

Tips when using social media...

- ★ Be cautious of sharing too much
- ★ Adjust your privacy settings
- ★ Verify who you are connecting with
- ★ Do not share personal details
- ★ Remember what goes online, stays online
- ★ Keep passwords strong

Social Media Tip: There is a social media trend that is going around that creates a fun character name using things like your birth month, middle name, and the street where you live? Beware of this type of request to post/share: Your post could be used to collect information about you!
Best to sit this one out.

Orleans Digital Literacy Initiative

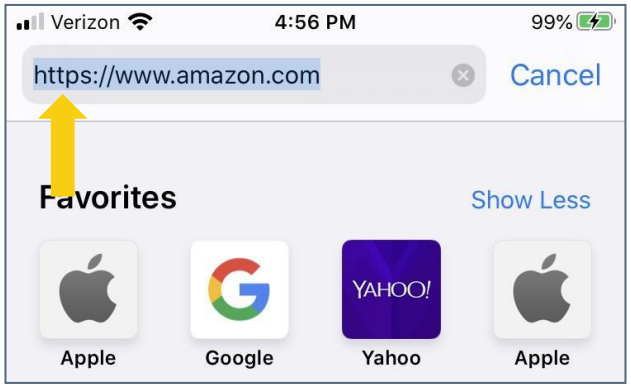
Searching with HTTP vs. HTTPS

Orleans Digital Literacy Initiative

Is this Website Secure?

There are two protocols for how information from your browser gets to a website and how information gets from the website to your browser.

HTTP stands for HyperText Transfer Protocol and **HTTPS** stands for HyperText Transfer Protocol Secure.



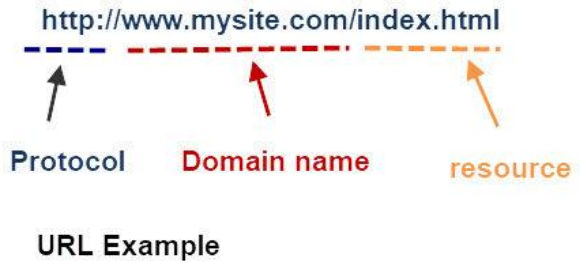
Amazon.com is using HTTPS

Orleans Digital Literacy Initiative

Searching with HTTP vs. HTTPS (Continued)

The main difference is that HTTPS is secure (encrypted) and HTTP is not. Someone who maliciously intercepts your data when you use HTTP can see or read what you have sent. Someone who maliciously intercepts your data when using HTTPS cannot see or read what you have sent.

You should never send any PII over HTTP. Only send it over HTTPS.
Never post PII to a shared drive like Google Drive or to a shared calendar space. PII should be shared only with those who need to know it.



The URL structure of an http: hosted website

Orleans Digital Literacy Initiative

Password Safety

Orleans Digital Literacy Initiative

Password Safety

Secure passwords go a long way toward keeping you safe online.

Orleans Digital Literacy Initiative

Password Do’s

Do create a unique password for each account you use.

Do use a random mix of numbers, letters, and symbols.

Do use a password manager to help you keep track of your unique passwords.

Do only submit your passwords to appropriate (secure) sites.

Orleans Digital Literacy Initiative

Password Don'ts

Do not use common phrases or personal information (i.e. a pet's name)

Do not write your passwords down.

Do not share your passwords.

Do not make short passwords.

Do not make a password that is easy to guess.

Do not keep the same password for a long time.

Do not store your password where it can be easily found.

Orleans Digital Literacy Initiative

Examples of Good & Bad Passwords

Examples of Bad Passwords	Examples of Good Passwords
Password	@H76cxgV90$$jKTsk
John2021	IegtDL2021!
03-21-1990	P3aS0up4me
Wizard22	nwso^d-scr23ap(hk3dh

Orleans Digital Literacy Initiative

Scams & Phishing

Orleans Digital Literacy Initiative

What is a Scam?

A scam is a term used to describe any fraudulent scheme that takes money or other goods from an unsuspecting person. Online scams have become very prevalent. While they used to be pretty obvious, they have become more sophisticated in recent years. Scams can be simple or more complex. They are similar in nature to phone scams. They can be found in email, websites, and on social media. Remember: If something seems too good to be true, it probably is!

Types of Scams

A **Donation Scam** is where a scammer pretends to be a charity so you will “donate” to it. However, you actually end up just giving the scammer your money.

Catfishing is when a scammer crafts a fake persona or identity in order to trick someone into giving them something they want.

A **419 or “Nigerian Letter” Scam** is a scam where the scammer asks to be sent an amount of money to cover some cost in order to award the recipient of the letter/email with a large sum of money.

An **Online Survey Scam** is a scam where a scammer offers usually either money or some good prize, like an iPad, but you have to fill out a survey. These surveys will often ask personal information, especially those found on security questions, to try and identify you and gain access to your accounts

Phishing

Scammers will use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, credit cards, or other accounts. Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.

Tactics Used in Phishing Scams

- ★ Scammers say they have noticed some suspicious activity or log-in attempts
- ★ Ask you to confirm your personal information
- ★ Ask you to click on a link to make a payment
- ★ Offer a coupon for free stuff

Orleans Digital Literacy Initiative

Pop-ups and Ads

Orleans Digital Literacy Initiative

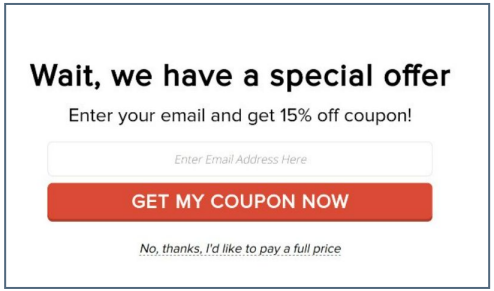
Pop-Ups and Ads

When you are using web browsers, you have to watch out for pop-ups and ads.

Pop-ups are windows (or text/graphic squares) that block you from viewing a website or something else until you close them. Pop-ups are advertisements, videos, or images that will pop up on the screen automatically on the page you are viewing. They are not a result of a click you make and many times are intended to grab your attention and make you click them. **Ads,** or advertisements, are things trying to get you to do something such as clicking and going to a shopping website. They can be malicious by either forcing you to click on something, collect information from you, or scam you.

Pop-Ups and Ads (Continued)

It is important to note that not all pop-ups and ads are malicious. The way to tell if a pop-up or ad is malicious is going to come down to the content. For example, a website asking for your email address for a newsletter may not be malicious. On the other hand, a pop-up saying “You won a free iPad!” or “Your computer has 20 viruses, clean now!” may be malicious.



Example of a pop-up advertisement

Safe Download Habits

Orleans Digital Literacy Initiative

Safe Download Habits

The most important safe downloading habit is only downloading files from trusted websites. Use the questions above to evaluate whether or not you should trust a website before downloading files onto your computer.

One red flag to watch for is a website that offers a download that has an advertisement that pretends to be a download button. In the image below, notice the blue triangle highlighted in yellow on the left above the green “Start Download” button. That icon signifies the button is actually an advertisement.

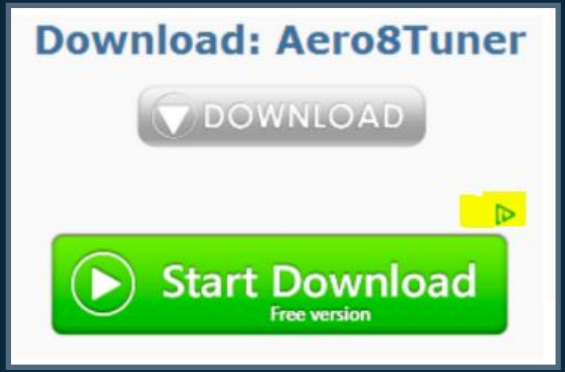


Image of a website ad with a download button

Orleans Digital Literacy Initiative

Safe Download Habits (Continued)

Always be aware and cautious of free options for things that you would usually expect to pay for. This is a sign that the file may not be safe. All of these online safety habits apply to not just downloading from sites on the internet, but also your email as well as other platforms that allow users to share files.

A good piece of general advice.

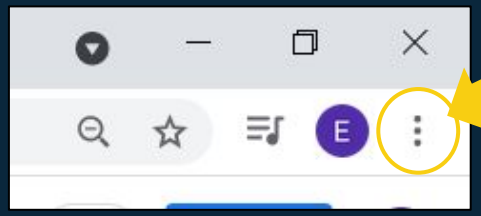
Trust your gut. If a website doesn't give you a good feeling, don't submit any sensitive information on it

Incognito Browsing

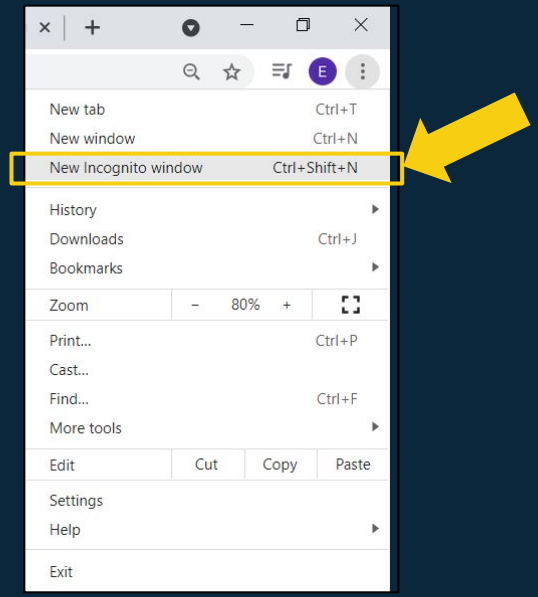
Orleans Digital Literacy Initiative

Incognito Browsing

When conducting web searches there are certain code snippets that are stored onto your computer such as **cookies** which are pieces of information that can be used to track information from your internet browsing history. Your **browsing history** is a record of the websites you have visited in the past. If you wish to block these cookies, you can use your browser's **incognito** mode. You can access your browser's incognito mode by clicking in the menu usually found in the top right corner of your browser and selecting "New incognito Window" or "New Private Window."



First step to opening a browser in incognito mode is to click the three dots on the right side of your browser



Next step is to choose "New Incognito window" which will open a new incognito window

Orleans Digital Literacy Initiative

Incognito Browsing

Using an incognito window means that you will not remain signed into any of your accounts, have targeted ads, or have the session show up in your browser history. This is a good way to keep your browsing sessions more secure on a shared computer.

Orleans Digital Literacy Initiative