Orleans Digital Literacy Initiative

Social Media Basics

This module will discuss using the various social media platforms safely, including privacy settings and personal information.
We will also talk about internet permanence and digital footprint.

Social Media Platforms

Social media is made up of websites and applications that allow users to create and share content or to participate in social networking. There are a variety of social media software platforms available for use and they all have somewhat similar features in varying forms for different audiences or uses. Some of the most commonly used platforms are listed below.

Twitter

Twitter is a software platform available as a web and mobile application where people post short messages called **tweets**. Twitter users can be mostly anonymous or use personas/characters to set up their accounts.

Instagram (IG)

Instagram is a software platform available as a web and mobile application where users create posts that consist of images and captions. People usually post as themselves.

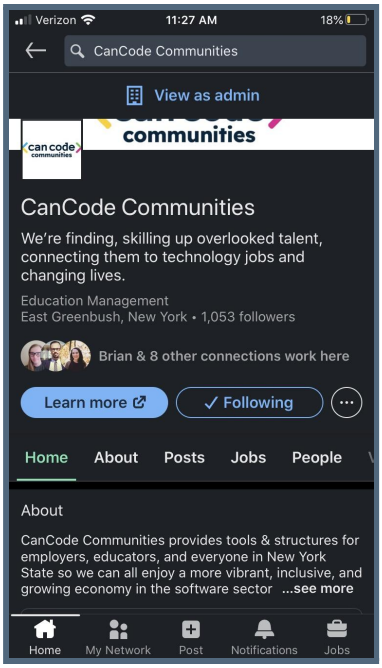
Facebook

Facebook is a software platform available as a web and mobile application where people can post messages or images and have a network of friends. Facebook also has the option to join groups on various topics. For example, if you are involved in a local activity, you can join or create a group around that topic.

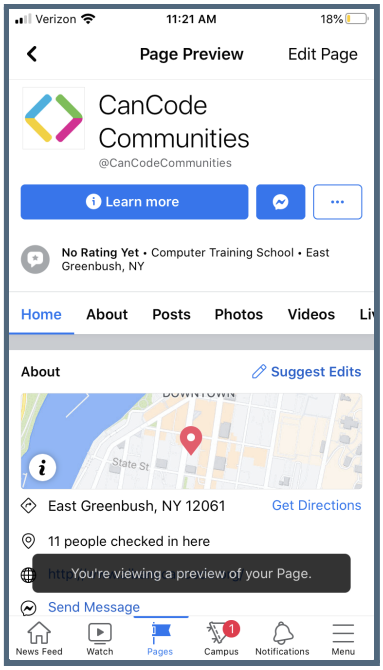
LinkedIn

LinkedIn is a software platform available as a web and mobile application for career-focused social interactions. Users have the ability to share a resume, build business connections, find jobs, and share posts.

In addition to the individuals who use these platforms, businesses will use them to reach a variety of people, by setting up a profile that describes their business and provide more information and contact resources to connect with the business.



CanCode Communities LinkedIn Page



CanCode Communities Facebook Page

Privacy Settings

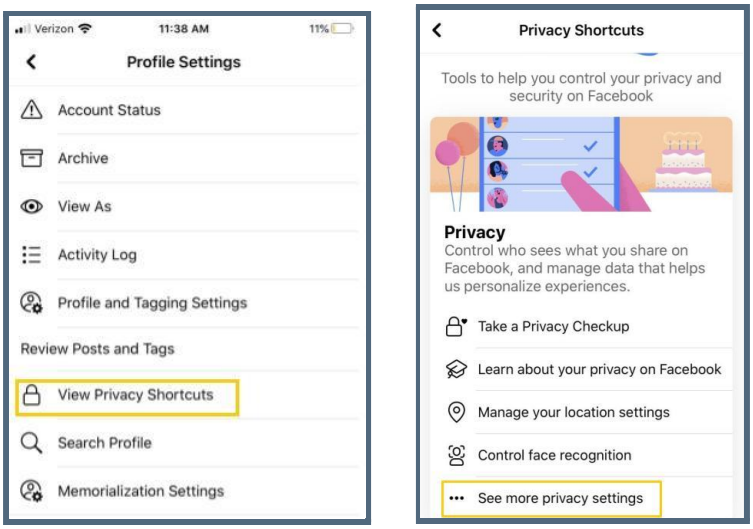
All social media platforms have **privacy settings**. These control what parts of your profile other people can see and who can find you on the platform. What and how you control it will depend on the platform you are using.

Facebook

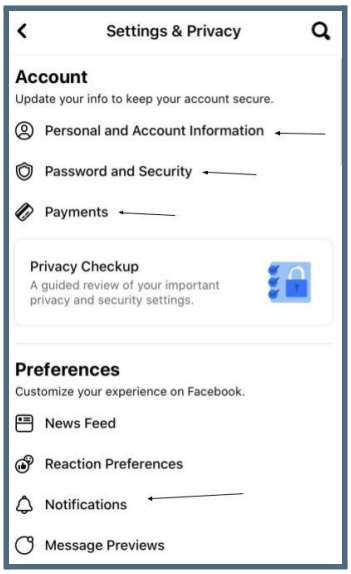
On Facebook you can control who sees your posts and your profile. You can set things to be Public, Friends of Friends, Friends, and Private. You can also choose who can send you messages or friend requests or even find your profile. The best way to check your privacy settings is using an **incognito** browser and looking at your profile.

> An incognito browser is a private version of your browser that does not save passwords, search history, ad tracking or any personal information.

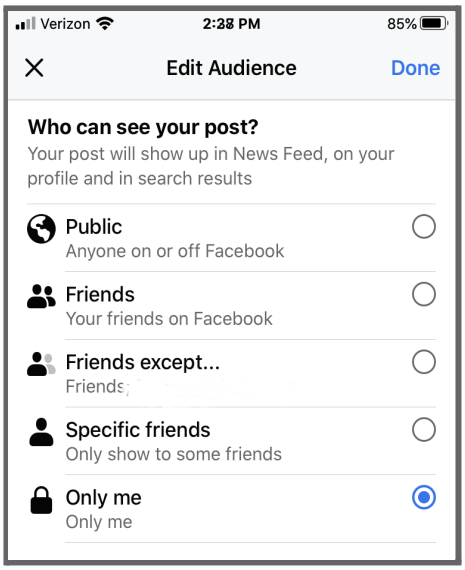
→ It is recommended that you set up your profile to only be visible to your friends.



Go to 'View Privacy Shortcuts' and then 'See more privacy settings'



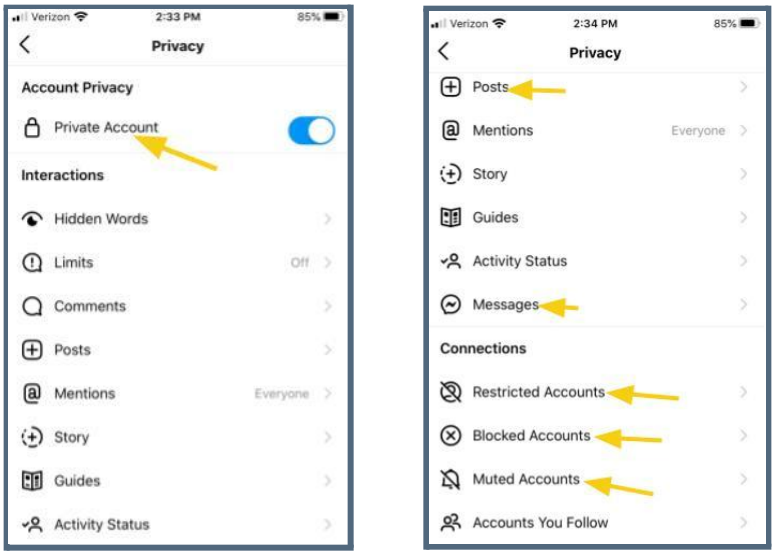
Settings and privacy in Facebook



Privacy Settings for who can see your posts on Facebook

Instagram

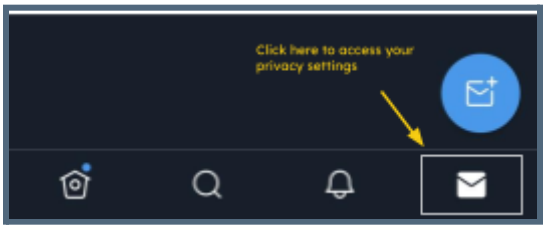
On Instagram you can control who sees your posts, profile, and your stories. You can set your profile to public or private. You can control who looks at your Instagram stories by going into your Account Privacy and choosing these options. Instagram also allows you to block or restrict other accounts from viewing your profile.



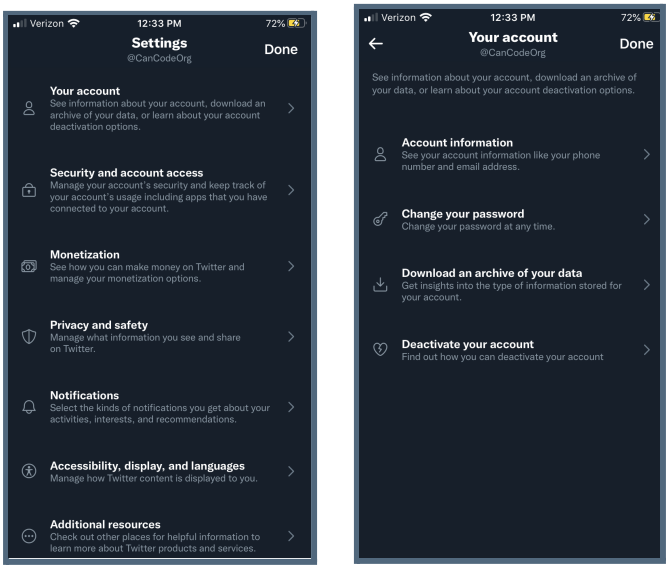
Account Privacy Settings on Instagram

Twitter

On Twitter you can control who sees your posts and profile. Like Instagram, you can set your profile to public or private. You can also control who can mention your profile in tweets. Additionally, Twitter also allows you to block other accounts from seeing or accessing your profile.



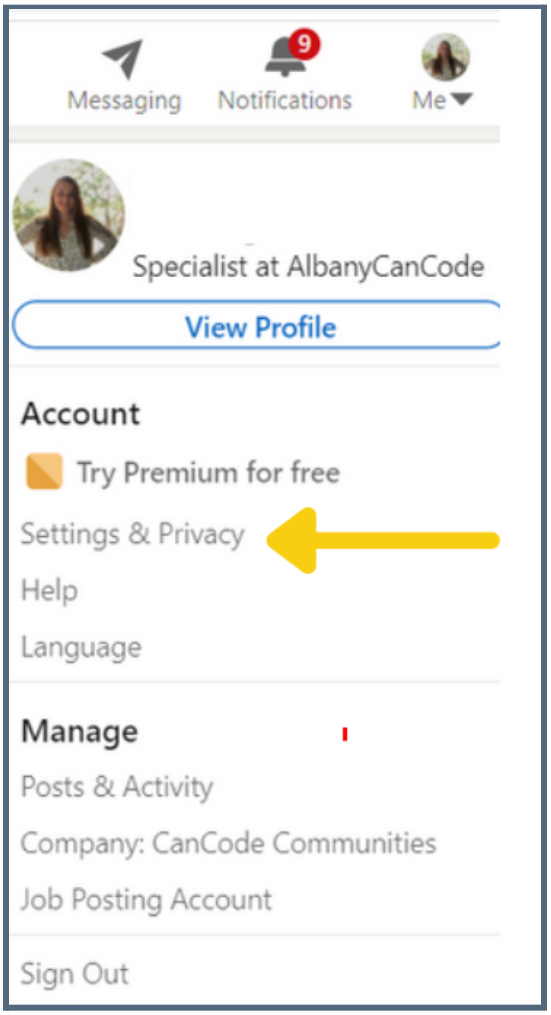
Click on the envelope to access your privacy settings



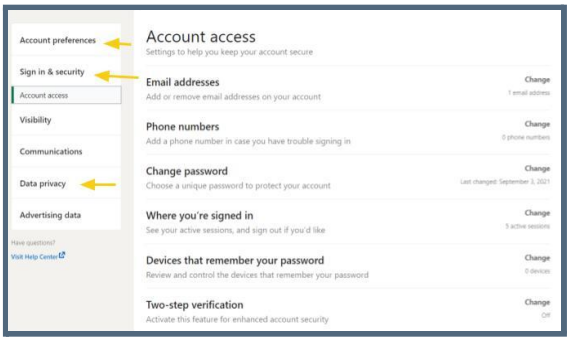
Privacy Settings in Twitter

LinkedIn

On LinkedIn you can also control who sees your posts and profile. LinkedIn is slightly different from other social media platforms because you have to connect with someone to have access to their profile. You can control who can mention your profile in their status updates and you can unmention yourself from a status update. Additionally, LinkedIn also allows you to block other accounts from seeing or accessing your profile.



Drop down menu to access your account setting



Settings and Privacy Menu on LinkedIn

Your Digital Footprint

Your **digital footprint** is the record of all the data you have put out online. This includes things you have intentionally shared, like a social media post or email, as well as data that has been recorded about you such as your **IP address**.

What is an IP address?
An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. To find your IP address click on Settings, then Network and Internet, and then WiFi. Click on the Network you are connected to and scroll down to find your IP address. It will look similar to 192.168.1.11

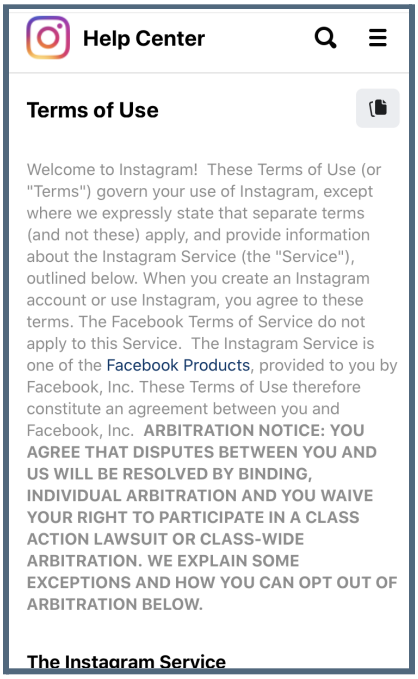
An example of an IP address

Terms of Service

Makers of Social Media apps and websites require you to agree to **Terms of Service** (ToS) before you can use an application. A Terms of Service Agreement, also known as a **Terms of Use** or **Terms and Conditions**, is a legal agreement between you and the corporation that makes and owns the application.

You may also be required to agree to **Community Guidelines** in order to use certain apps. These guidelines lay out the rules for the use of the application. They cover both acceptable and unacceptable use of the application.

It is strongly suggested that you read these items carefully before you agree to accept them. These agreements will often include information about how the company that makes the application or runs the website will be using your personal information as well as waivers of liability.



Example of Instagram's Terms of Service

Think Before You Post

It is important to keep in mind that your online presence is permanent. While you may delete a post or an image from social media, it has already been shared and will always exist in some form on the servers of the social media company. This is because anyone who saw it can save it and share it without your permission. Additionally, the social media companies keep a history of user posts and interactions that are very difficult to destroy. Once an account is opened, it is near impossible to ever get the information you have shared removed from the servers it has

been stored on. You must always assume that once you have shared something out on the internet, you no longer have control over it.

What you put online will often be people's first impression of you, so think carefully about what you want to share. Many platforms have the ability to make things public or private. When something is public, it can be seen or shared by anyone. Only share something publicly if you are okay with that. Many employers research a candidate's social media in the hiring process, so remember to keep that in mind when sharing publicly on your platforms.

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

Personal Information

When posting or giving 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 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.

- ★ 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.

Most people know not to post important things, like their social security number or a password, but even things that seem harmless can be used against you. For example, maybe it's your Mom's birthday so you create a Facebook post saying "Happy Birthday, Mom!" Now someone may have

your password and username and possibly the answer to one of your **security questions**. If one of your security questions for your bank account was your Mom's birth date, a person could have access to one of your accounts and make fraudulent transfers in your bank account. The lesson is to be aware of what information is protecting your accounts and what you are sharing.

A **Security Question** is a question that is asked when you set up an account. It will be used if there is an issue signing into your account or if you forgot your password. It will also be used to verify your identity, if needed.

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!