



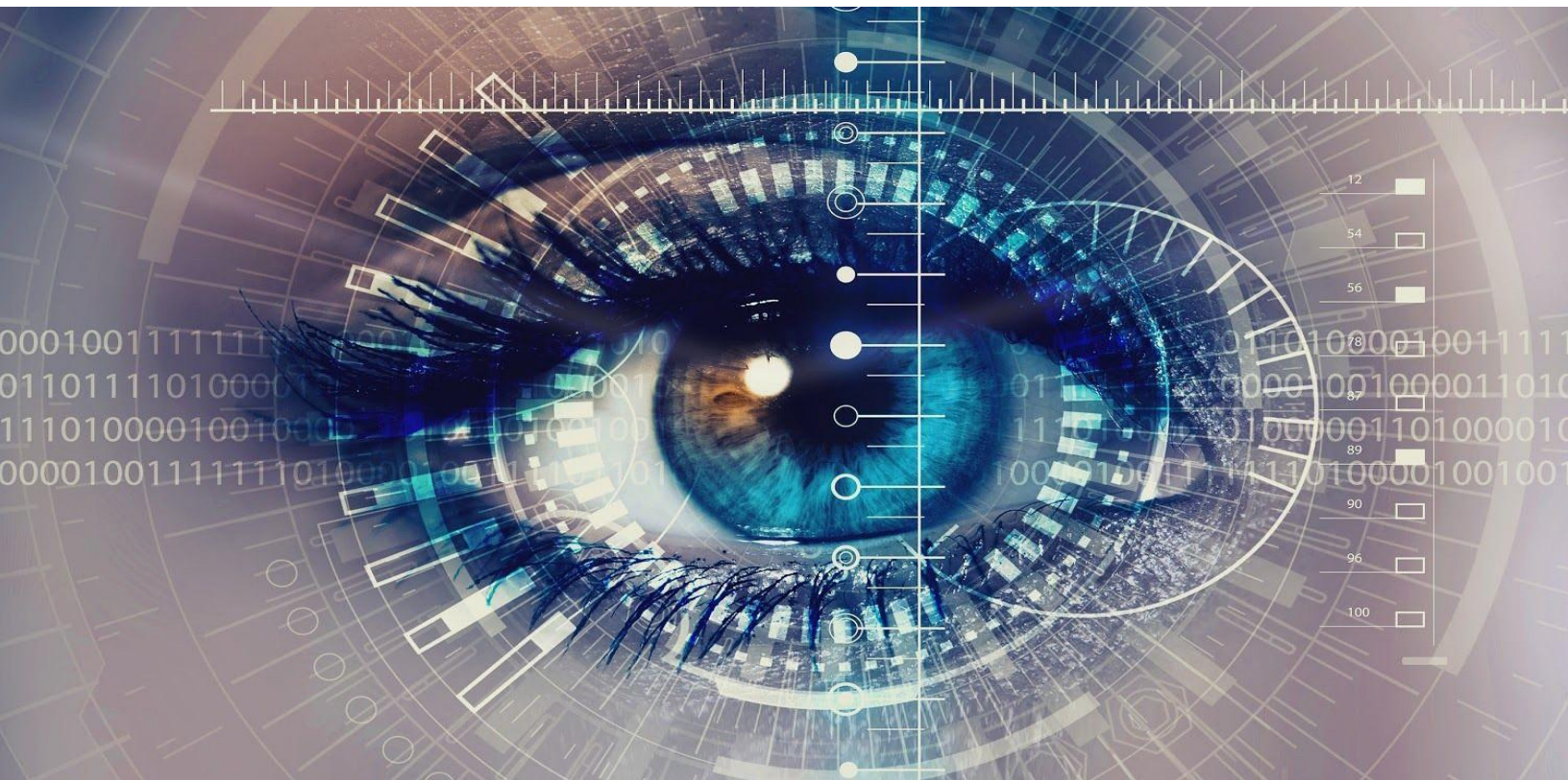
**HUMAN-i**  
INTELLIGENCE SERVICES, INC.

Suite 111, Fort Langley,  
BC, V1M 2R4  
+1 (604) 764-1469  
[team@human-i.org](mailto:team@human-i.org)

Social Media Privacy & Security

Best Practice 11/21





## Introduction

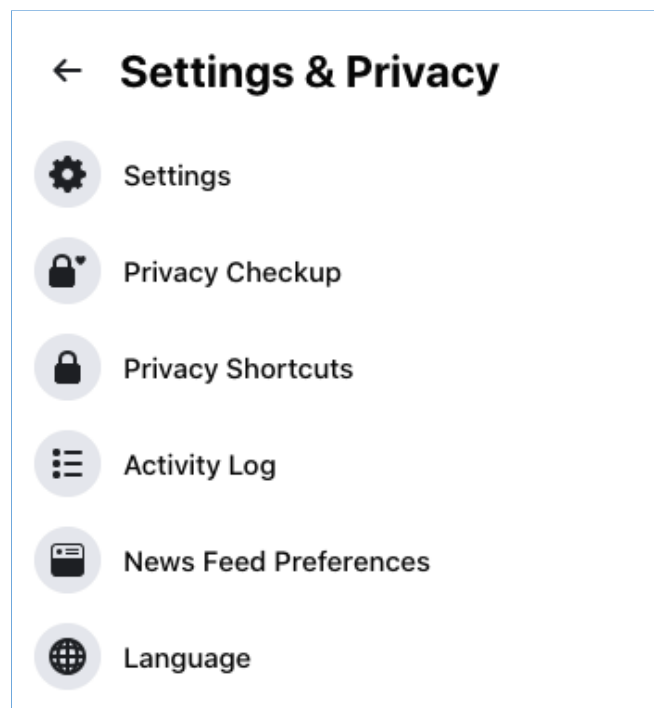
Our routine use of social media, email and apps means that we are constantly dispersing fragmented pieces of personal information across the internet and exposing ourselves to a variety of risks. Many of these programs explicitly state their intentions to share our information with others, while others do little to protect our information from theft or inappropriate use.

This document is designed to be a supplement to in-person training and presents the basic structure and function of popular social media platforms and apps including best practices with respect to safety and privacy from first contact onward. It also highlights how easy it can be to locate your personal information across platforms despite available safety measures being correctly followed, and how users can protect themselves, their family, their organization and their data from vulnerability and exposure.

# Privacy & Security Settings for Social Platforms:

## Facebook:

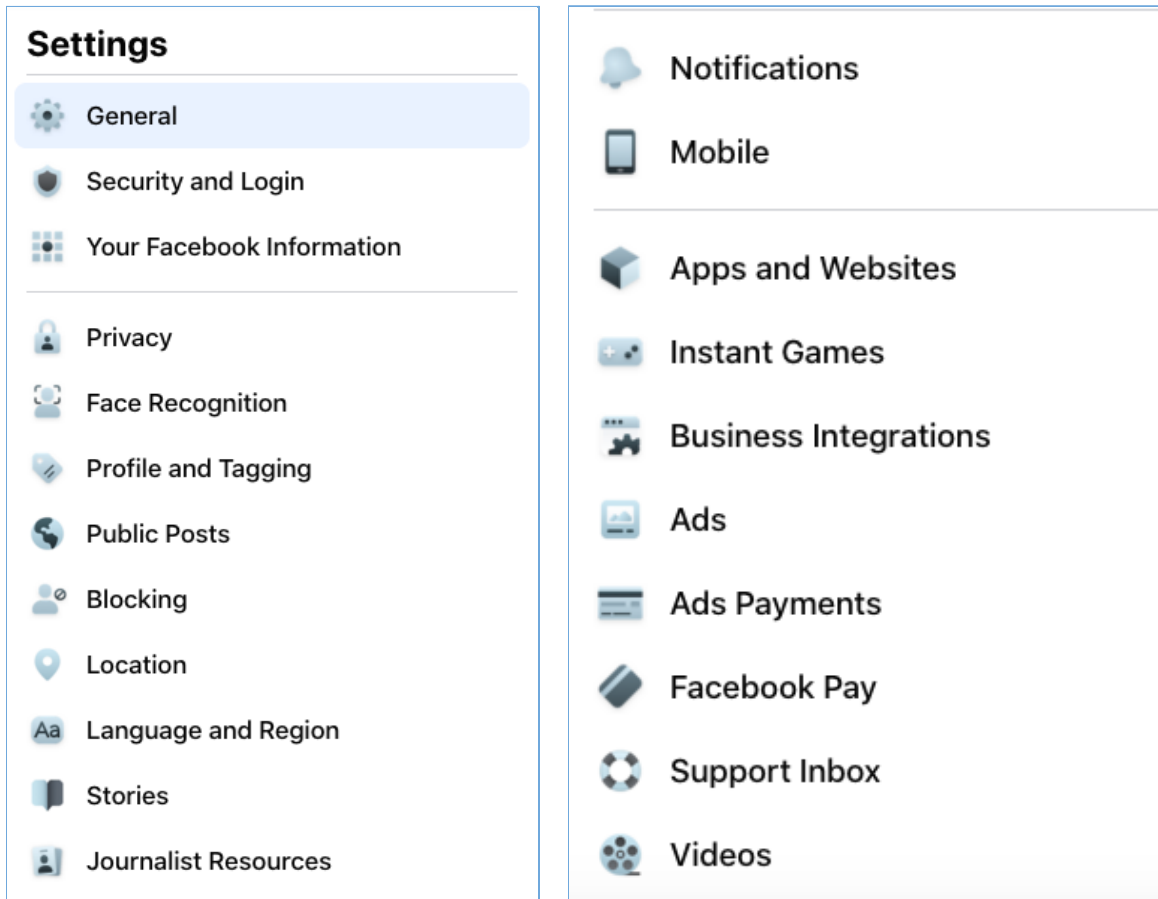
The main Privacy and Security settings can be found under the triangular “down” arrow on the far right of the main Facebook navigation bar at the top of the home screen, under Settings. The initial menu displayed provides some initial privacy checks and shortcuts and is a helpful starting point centred around an intuitive interface. Consider carefully the implications of settings around data privacy, security and convenience such as 2-factor authentication and password reset mechanisms.



Once these menu items have been completed, go to the main Settings menu to apply other privacy and security settings for your account and profile, including tagging, visibility, notifications and advertising. With respect to the menu items shown in the screenshots below, best practice for highest security is advised as follows:

Under Location - Location history should be set to **Off**

Under Face Recognition - Set to **No**



Mobile allows you to explore the option of associating a cell phone number with your account - which is to improve advertising and reset your password, however, enabling this option has the potential to decrease account security and is NOT RECOMMENDED.

To reduce public exposure to personal information, the settings shown below are recommended and are the most robust currently available. Easy to understand explanations are available under each section and it is important to work through each setting methodically, and regularly, to ensure each setting is current and meets privacy and security needs.

Be aware that Facebook changes its privacy and security settings frequently, therefore regular review of all sections is recommended to ensure desired settings are maintained.

### Login

- 🔑 **Change password**  
 It's a good idea to use a strong password that you're not using elsewhere [Edit](#)
- 👤 **Save your login info**  
 It will only be saved on the browsers and devices you choose [Edit](#)

### Two-Factor Authentication

- 🛡️ **Use two-factor authentication**  
On • We'll ask for a code if we notice an attempted login from an unrecognized device or browser. [Edit](#)
- 📱 **Authorized Logins**  
 Review a list of devices where you won't have to use a login code [View](#)
- 📦 **App passwords**  
 Use special passwords to log into your apps instead of using your Facebook password or login codes. [Add](#)

### Setting Up Extra Security

- 🔔 **Get alerts about unrecognized logins**  
On • We'll let you know if anyone logs in from a device or browser you don't usually use [Edit](#)
- 👥 **Choose 3 to 5 friends to contact if you get locked out**  
 Your trusted contacts can send a code and URL from Facebook to help you log back in [Edit](#)

## Privacy Settings and Tools

---

**Privacy Shortcuts**    Check a few important settings  
 Quickly review some important settings to make sure you're sharing with the people you want.

---

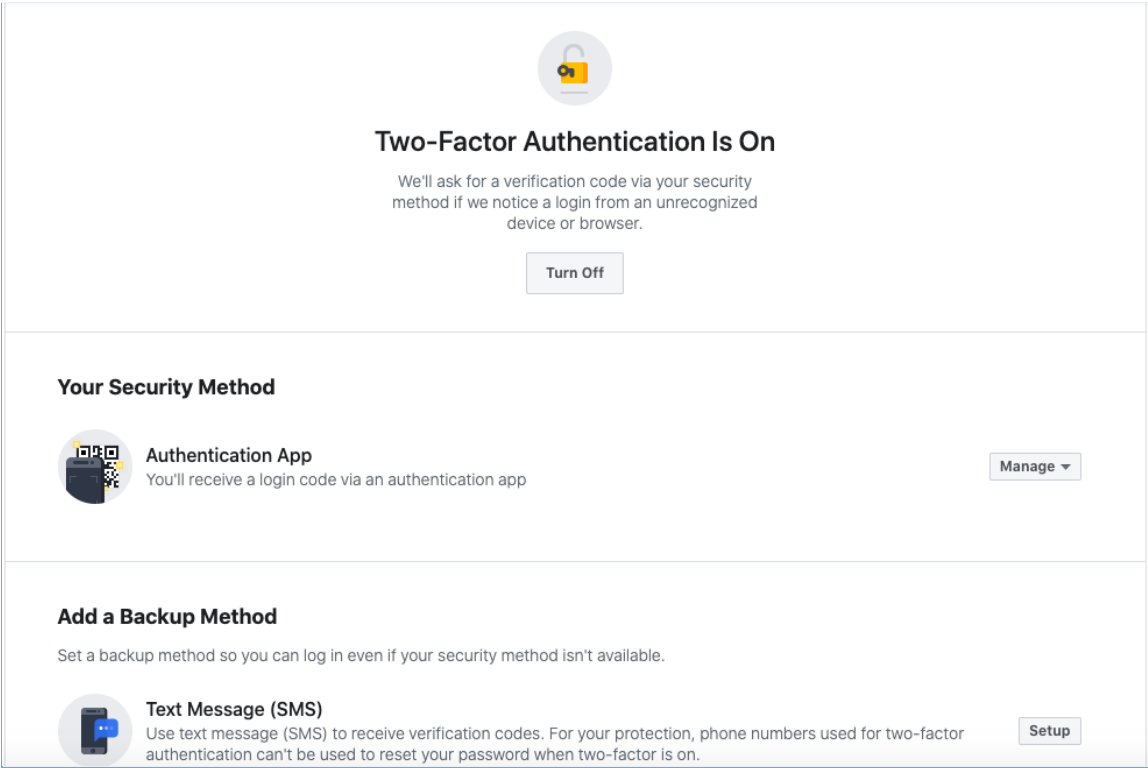
**Manage your profile**  
 Go to your profile to change your profile info privacy, like who can see your birthday or relationships.

---

**Learn more with Privacy Basics**  
 Get answers to common questions with this interactive guide.

<b>Your Activity</b>	<p>Who can see your future posts? <span style="float: right;"><b>Friends</b> <a href="#">Edit</a></span></p> <hr/> <p>Review all your posts and things you're tagged in <span style="float: right;"><a href="#">Use Activity Log</a></span></p> <hr/> <p>Limit the audience for posts you've shared with friends of friends or Public? <span style="float: right;"><a href="#">Limit Past Posts</a></span></p> <hr/> <p>Who can see the people, Pages and lists you follow? <span style="float: right;"><b>Public</b> <a href="#">Edit</a></span></p>
<b>How People Find and Contact You</b>	<p>Who can send you friend requests? <span style="float: right;"><b>Friends of friends</b> <a href="#">Edit</a></span></p> <hr/> <p>Who can see your friends list? <span style="float: right;"><b>Only me</b> <a href="#">Edit</a></span></p>

Two-factor authentication (2FA) is recommended for each social media site and email account. Facebook enables 2FA either through SMS messaging or through the use of the Authenticator App, which can be used to verify multiple accounts on a variety of apps. The Authenticator App must be downloaded onto a mobile device and then synced using a scanned QR code (not as complicated as it sounds). As with most 2FA, with the exception of email, access to your mobile device will be required to log into your account on each subsequent occasion. If a phone number is used for 2FA on Facebook, care must be taken to ensure the phone number is not also used as a password reset mechanism as this can be viewed publicly, albeit partially, and can be a potential security risk.



Followers and Friends on Facebook are not the same and require different privacy settings. It is recommended that users switch notifications on to alert you to comments on your posts, or follows by people not in your Friends list.

## Public Post Filters and Tools

---

**Who Can Follow Me** Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Friends ▾

Each time you post, you choose which audience you want to share with.

This setting doesn't apply to people who follow you on Marketplace and in buy and sell groups. You can manage those settings on Marketplace.

[Learn More](#)

---

**Public Post Comments** Who can comment on your public posts? Friends Edit

---

**Public Post Notifications** You can get notifications when people who aren't your friends start following you and share, like or comment on your public posts. Turn these notifications on for Public ▾

---

**Public Profile Info** Who can like or comment on your public profile pictures and other profile info? Friends Edit

---

**Off-Facebook Previews** Enable previews when your Public Group posts are shared off of Facebook. Previews may include your username, your profile image and any other content from your original post. Off ▾

Facebook allows you to view and to some extent, control the apps and third parties which have access to your data. They match your profile to information received from third party apps to provide personalized information and advertising to you either based on other advertisements you've clicked through or websites or services you've used outside of Facebook. While you cannot prevent Facebook using your information in this way as it is a condition of the terms of service, you can control the information Facebook collects about you and how it uses it to profile you and direct advertising to you based on your preferences and information provided (see screenshots below).

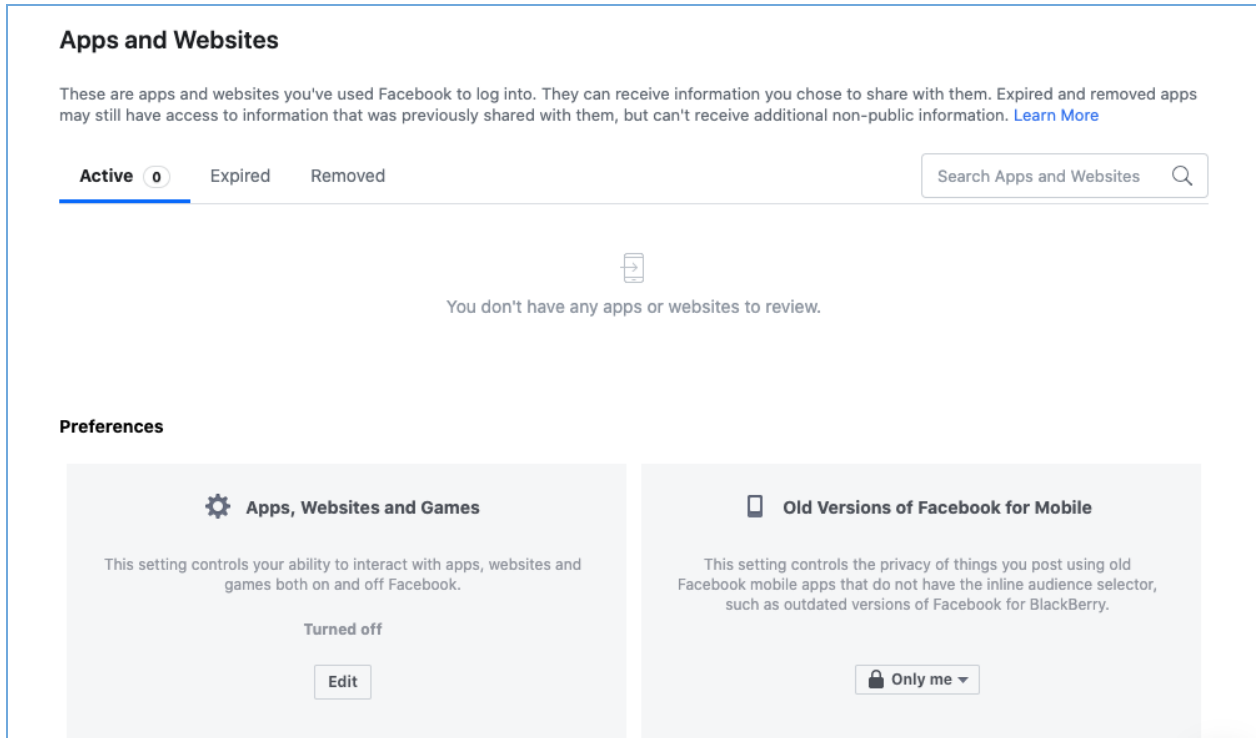
### Ad Preferences

- Advertisers
- Ad Topics
- Ad Settings**

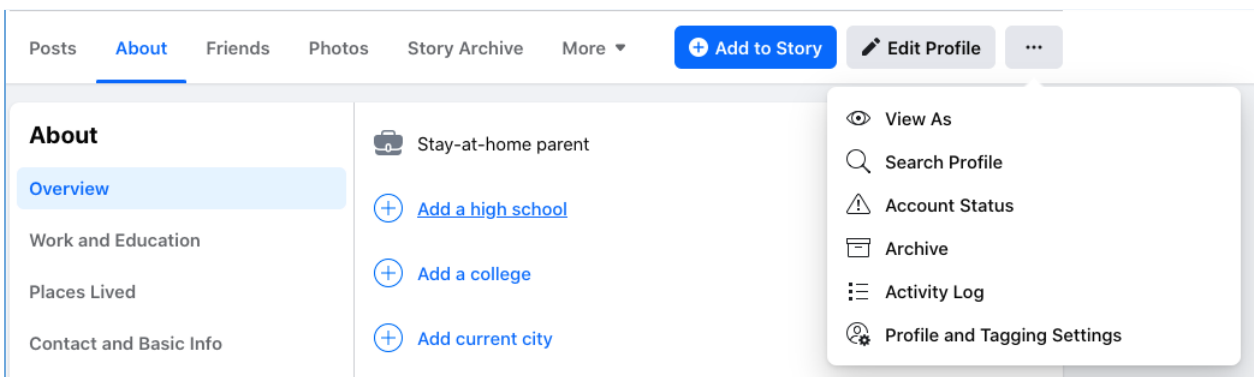
your activity on websites off of Facebook to decide which ads to show you.

#### Manage Data Used to Show You Ads

- Data about your activity from partners** Personalized ads based on your activity on other websites, apps or offline >
- Categories used to reach you** Profile information, interests and other categories used to reach you >
- Audience-based advertising** Advertisers using your activity or information >
- Ads shown off of Facebook** How advertisers can reach you through off-Facebook ads >
- Social Interactions** Who can see your social interactions alongside ads? >



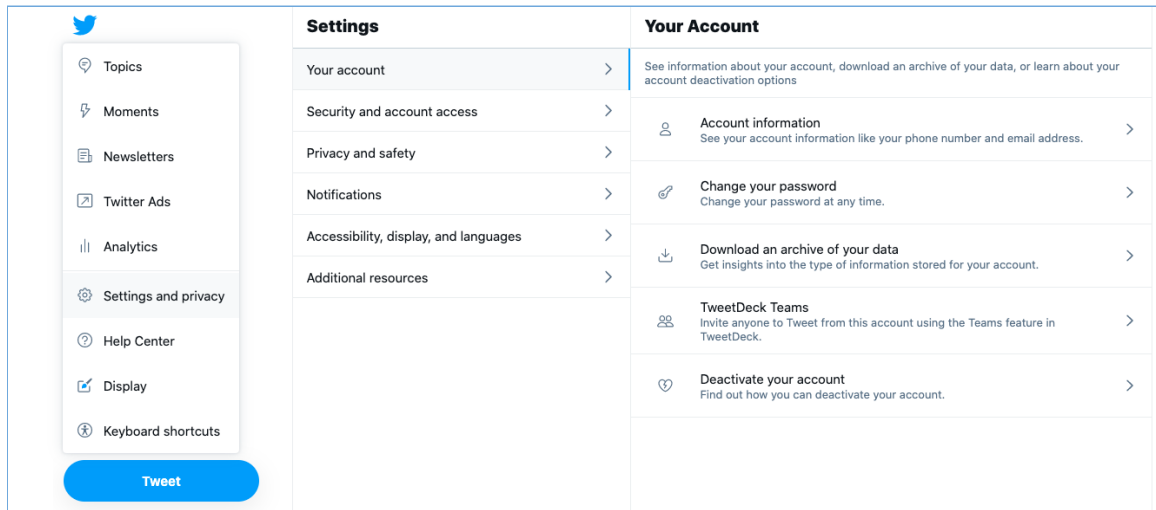
Users can also access privacy settings and data controls using menu items revealed by clicking the 3 dots at the right of the section at the top of your timeline:



Methodically click through each of these links to control the privacy and access for each type of content. Settings are reasonably intuitive and allow you to control what other people can post, and view, about you. Some of these settings will return you to the main Privacy and Settings Menu and some may require you to re-enter your password.



# Twitter:



Twitter provides a reasonably intuitive Settings and Privacy menu which is found under the More tab on the left of the screen under the main menu. A broad range of privacy and security options are available, as well as control over advertising and linked accounts.

Clicking through the Account tab at the top of the menu allows users to set up Two-Factor Authentication (2FA) via text message or mobile app.







It also allows users to configure a backup code in the event you lose your device and cannot receive a 2FA code, as well as providing temporary passwords if you would like to use your Twitter account to log into a secondary app, or vice versa. It should be noted that if you choose to use your phone number to reset your password, this will be partially visible to anyone attempting to reset your password maliciously and used in conjunction with the password reset settings on other social media accounts, could represent a security risk.

We recommend that users periodically check the current and past sessions to ensure all devices accessing the account are known and authorized, and as with all social media accounts, the password should be unique and changed frequently.

Settings	← Security
Your account >	Manage your account's security.
Security and account access >	<b>Two-factor authentication</b>
Privacy and safety >	Help protect your account from unauthorized access by requiring a second authentication method in addition to your Twitter password. You can choose a text message, authentication app, or security key. <a href="#">Learn more</a>
Notifications >	Two-factor authentication >
Accessibility, display, and languages >	
Additional resources >	<b>Additional password protection</b>
	Enabling this setting adds extra security to your account by requiring additional information to reset your password. If enabled, you must provide either the phone number or email address associated with your account in order to reset your password.
	Password reset protect <input checked="" type="checkbox"/> <a href="#">Learn more</a>

Under the Privacy and Safety tab there are many options to limit the exposure of your tweets, along with your physical location, your personal information and how easy it is for others to find and contact you.

The remainder of the Twitter settings are simple and intuitive; again, work through them methodically, selecting the level of privacy that you are comfortable with.

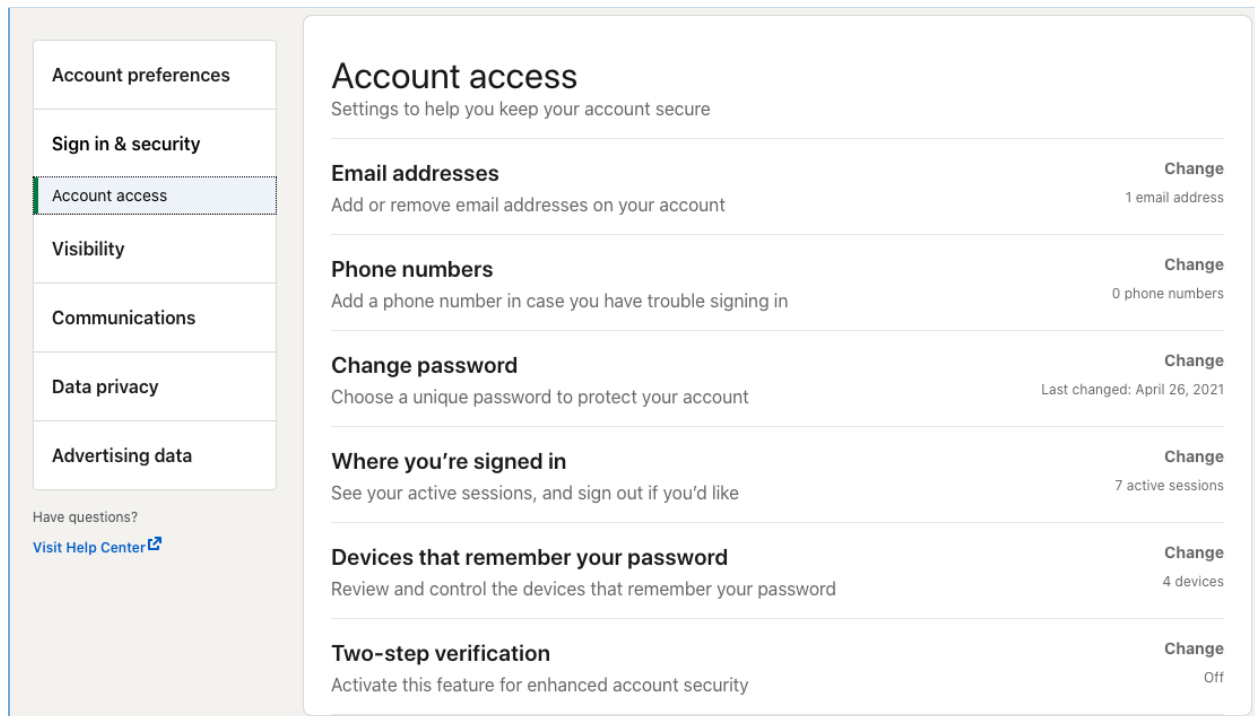
Settings	Privacy and safety
Your account >	Manage what information you see and share on Twitter.
Security and account access >	<b>Your Twitter activity</b>
Privacy and safety >	 <b>Audience and tagging</b> Manage what information you allow other people on Twitter to see. >
Notifications >	
Accessibility, display, and languages >	 <b>Your Tweets</b> Manage the information associated with your Tweets. >
Additional resources >	
	 <b>Content you see</b> Decide what you see on Twitter based on your preferences like Topics and interests >
	 <b>Mute and block</b> Manage the accounts, words, and notifications that you've muted or blocked. >
	 <b>Direct Messages</b> Manage who can message you directly. >
	 <b>Discoverability and contacts</b> Control your discoverability settings and manage contacts you've imported. >
	<b>Data sharing and off-Twitter activity</b>

# LinkedIn

Although often under-utilized, LinkedIn Privacy and Security settings provide extensive options for protecting private data and also is the most transparent of the popular social platforms.

The Settings and Privacy main menu is located in the drop-down menu under your name on the main navigation bar, along with the settings to manage Posts and Activity.

The language is simple and intuitive and there are 6 sections on the right of the page which allow users to navigate between various privacy and security menus. As per Facebook and Twitter, work through these methodically, selecting the settings that meet your personal requirements.



The screenshot shows the LinkedIn 'Account access' settings page. On the left is a navigation menu with the following items: Account preferences, Sign in & security, Account access (highlighted), Visibility, Communications, Data privacy, and Advertising data. Below the menu is a link to the Help Center. The main content area is titled 'Account access' and includes a subtitle 'Settings to help you keep your account secure'. It lists several settings, each with a 'Change' link and a count of items:

- Email addresses:** Add or remove email addresses on your account. 1 email address.
- Phone numbers:** Add a phone number in case you have trouble signing in. 0 phone numbers.
- Change password:** Choose a unique password to protect your account. Last changed: April 26, 2021.
- Where you're signed in:** See your active sessions, and sign out if you'd like. 7 active sessions.
- Devices that remember your password:** Review and control the devices that remember your password. 4 devices.
- Two-step verification:** Activate this feature for enhanced account security. Off.

LinkedIn provides the most versatile settings for degrees of connections and public accessibility of all the social networking platforms. Much of your information can be restricted to connections or network only, both within and outside of the platform, which instructs search engines how to index and display your data.

**Edit your custom URL**  
Personalize the URL for your profile.  
www.linkedin.com/in/julieclegg1 [✎](#)

**Edit Content**  
This is your public profile. To edit its sections, update your profile.  
[Edit contents](#)

**Edit Visibility**  
You control your profile's appearance for people who are not signed in to LinkedIn. The limits you set here affect how your profile appears on search engines, profile badges, and permitted services like Outlook.  
If you have added a LinkedIn creator card to your profile, then unselecting Public or hiding photos, headline, summary, or articles & activity will remove this feature from your profile.  
[Learn more](#)

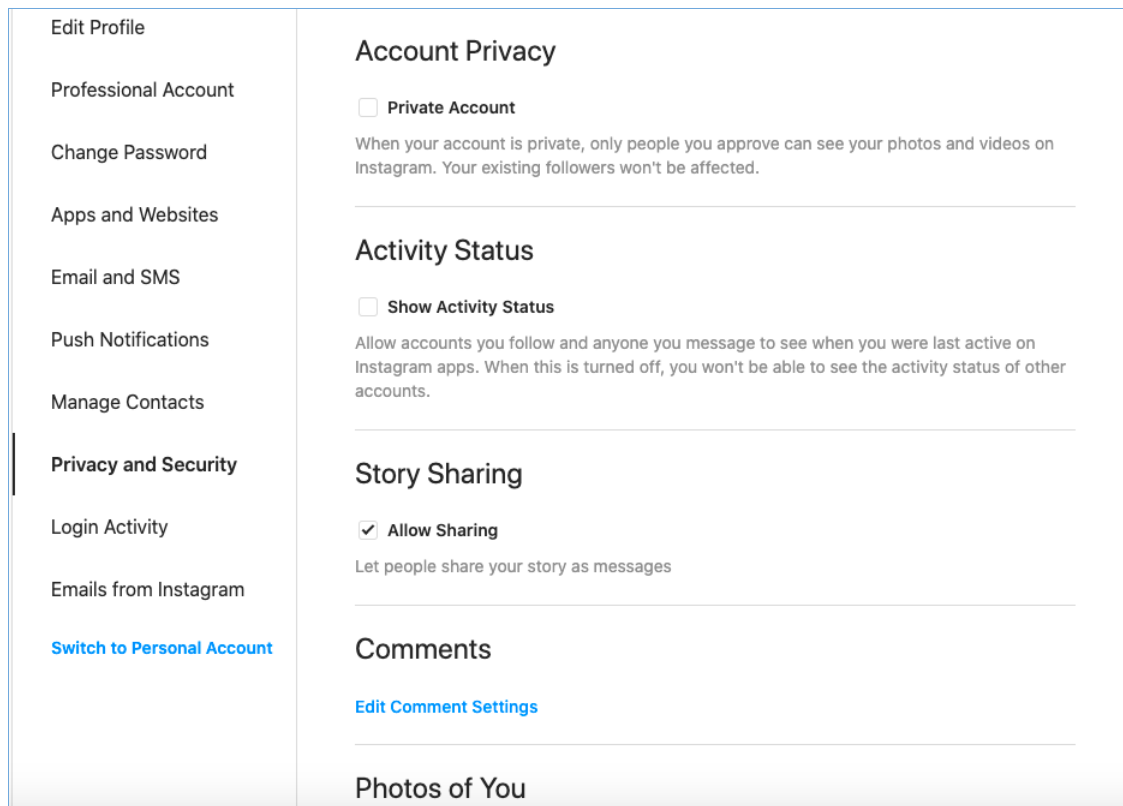
Your profile's public visibility  On

While LinkedIn offers versatility over your visibility and data security, their privacy practices are not as robust and there are several free browser add-ons and external applications which are able to scrape LinkedIn data and use it to automate subscriptions to mailing lists and access provided information such as phone number and postal codes, even if this information is hidden from public view.

It is recommended that only public information is input into LinkedIn, even within the private areas (with the exception of private messages), so as to maintain privacy and security. Locations, personal contact information, private events and other linked applications should be removed where possible.

# Instagram

The Privacy and Security settings of Instagram are very straightforward and can be found under Settings by clicking through the user's profile image. The options differ based on whether these are accessed using the desktop or mobile app, however, they are straightforward and self-explanatory.



Two-Factor Authentication can be activated either via text message or mobile app, along with all previous logins, user names used, locations, password changes and other account activity.

It is recommended that personal Instagram accounts are set to Private with filters activated for comments and tagged images. As with most other social media platforms, login activity allows users to ensure their account is not being accessed by another device or user.

Instagram does not provide partial password reset data, therefore if anyone attempts to reset the password on an account, the account holder will be notified via email.

# Social Media Privacy & Security Checklist

- Use a unique (or for-purpose) email address for each social media account to prevent breached information being exposed or linked in deep web databases.
- Do not add a phone number to an account unless it is solely to enable 2FA and ensure that restriction is put in place via the security settings.
- Change each password every 6 months and use a unique password for each account.
- Regularly check where you are currently logged in to ensure each login is attributable to you and not another person or device gaining unauthorized access to your account.
- Enable two factor authentication (2FA) on all accounts to prevent unauthorized entry including SIM swapping or cloning attempts.

Privacy & Security Actions	Facebook	Twitter	LinkedIn	Instagram
Unique email address				
Phone number removed or restricted				
Last password change				
Unique password				
Login alerts or restrictions				
Password reset protection				
2 Factor Authentication				
Friends and connections restricted				
Photos and videos restricted				
Account visibility protected				