

SOCIAL MEDIA AWARENESS

- Remember that anything you post, comment, or like will be collected and analyzed by the service you are using, and those “insights” will be sold to or shared with other companies.
- Avoid commenting on posts marked public, these comments can be easily collected and analyzed.
- Monitor what people post and say about you, and check if it’s public. Contact and ask them to restrict access on public posts about you.
- Only accept friend requests from people you know, and consider asking them a question only they would know the answer to before accepting. Imposters use fake friend requests to snoop on you and your family, usually for criminal purposes.

(back)

FACEBOOK SETTINGS GUIDE

On a desktop/laptop, go to: <https://www.facebook.com/settings>

Sorry up front – Facebook has a LOT of settings.

GENERAL ACCOUNT SETTINGS

From the General Account Settings page:

- **Review Name and Username.** Recommend you use the name people know you by. Using something different won't confound anyone researching you, and may draw unwanted attention your way. If you do use another name, ensure your username doesn't reveal your real name.
- **Review Contact and Ad Account Contact.** If you are changing your email to a more private provider, this is where you do it.

Next, **go to Security and Login** on the left menu.

SECURITY AND LOGIN

From the Security and Login page:

- **Review "Where you're logged in."** You may need to click "see more." Review the devices. If there are any old devices, click the three vertical dots to the right of them and select "Log Out." If you one of them is not your device and you don't know why it's there, select "Not you?"
- **Next, change password.** Click the edit button next to "change password" and change your password to a strong password generated by your password manager.
- **Set up 2FA.** To the right of "use two factor authentication," click the edit button. Choose Authentication App -> add new App. Scan the QR code with your app or copy/paste the shared secret. Once it's saved in your app, tap continue, enter the six-digit code from your app to confirm.
 - o Next go to "Show Codes" to the right of "Recovery Codes." Copy and paste these somewhere safe (e.g. Standard Notes encrypted note, your password manager's notes section (not ideal), or print them out and keep them somewhere safe (...like a safe).
 - o If you have SMS as a backup method enabled, **disable it.**
- **Review authorized logins.** Below change you password, tap the view button next to "authorized logins." Remove any old devices, third party apps or devices, or anything you don't know what it is.
- **Ensure "get alerts about unrecognized logins" is on.**
- You can optionally "choose 3 to 5 friends to contact if you get locked out." If you're locked out, your friends will each get a code. You need all of the codes to unlock your account. It's a pretty secure recovery method. Five friends is best.

Next, **go to Your Facebook Information** on the left menu.

Facebook Settings (front)

Social Media Settings Guide – The Complete Digital Privacy Checkup Checklist – May 2020

YOUR FACEBOOK INFORMATION

From the Your Facebook Information page:

- * Click view button to the right of "**Off-Facebook Activity**"
 - o Click "Clear History" button on the right, and confirm.
 - o Below that, click "More Options."
 - o Click "Manage Future Activity." When the menu pops up, click the blue "Manage Future Activity" button.
 - o **Next to "Future off-Facebook activity," change the toggle to off.**
 - o When the menu pops up, click the blue "turn off" button.

Next, return to the settings menu and **go to Privacy** on the left settings menu.

PRIVACY

From the Privacy page:

- * Next to "who can see your future posts?" ensure it says "Friends." If it does not, click "Edit" and change to Friends.
- * Next to "Limit the Audience for Old Posts on your Timelines," click "Limit Past Posts" on the right. Tap the "Limit Past Posts" button, and then when the popup menu displays, "Limit Past Posts" button again.
- * Under "How People Find and Contact You" edit each one as follows:
 - o "Who can send you friend requests?" **Friends of Friends.** This helps prevent scammers from posing as your friends to friend you.
 - o "Who can see your friends list?" **Friends.** Your friends list contains a lot of information about who you know and work with, and can be used for deep research into your life.
 - o "Who can look you up using the email you provided?" Anything but everyone – suggest **only me.** The more you lock this and the next setting down, the harder it will be for scammers to friend you – your email and phone are widely available through stolen databases.
 - o "Who can look you up using the phone number you provided?" Anything but everyone – suggest **only me.**
 - o "Do you want search engines outside of Facebook to link to your profile?" **No.**

Next, **go to Timeline and Tagging** on the left settings menu.

TIMELINE AND TAGGING

From the Timeline and Tagging page, review settings. **Recommended settings:**

- "Who can post on your timeline?" **Friends or Only Me.**
- * "Who can see what others post on your timeline?" **Friends.**
- * "Allow others to share your posts to their stories?" **Off.**

- "Hide comments containing certain words from your timeline?" You can use this to somewhat restrict what people say about you. For example, if you're a NYPD police officer and want to minimize comments connecting you to police you might have "police, FOP, cop, NYPD." Just know that you're also giving Facebook information about what you find sensitive.

- * "Who can see posts you're tagged in on your timeline?" **Friends or Only Me.**

- "When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?" **Friends or Only Me.**

- Review posts you're tagged in before the post appears on your timeline?" **On.**

- Review tags people add to your posts before the tags appear on Facebook?" **On.**

Next, **go to Stories** on the left settings menu.

STORIES

From the Stories page, set all to "Don't Allow."

Next, **go to Location** on the left settings menu.

LOCATION

* **On the Location Settings page, ensure Location History is off.**

Next, **go to Blocking** on the left settings menu.

BLOCKING

On the Blocking page, review settings. **Restricted List** lets you add people who you are friends with who you don't want to see most of your activity.

Next, **go to Face Recognition** on the left settings menu.

FACE RECOGNITION

* **On the Face Recognition page, set Face Recognition to No.** This will prevent Facebook from collecting and using your facial data.

Next, **go to Public Posts** on the left settings menu.

PUBLIC POSTS

* **On the Public Posts page, set "Who Can Follow Me?" to Friends.** If you have a connected Twitter account, recommend you disconnect it.

Next, **go to Apps and Websites** on the left settings menu.

APPS AND WEBSITES

* **On the Apps and Websites page, recommend you turn off Apps, Websites, and Games.** If you have websites that you use for Facebook single sign-on logins, you should first go to those websites and either create an account/password with the same email you use for Facebook, or delete the account.

Facebook Settings (back)

Social Media Settings Guide - The Complete Digital Privacy Checkup Checklist - May 2020

REVIEW NOTIFICATIONS SETTINGS

You can review and change your notification settings by going to Notifications on the left menu.

REVIEW PROFILE AND COVER PHOTOS

Click your Profile Picture/Name in the top right of the screen.

- * **Review your cover photo.** This photo is always public. If it was taken at a location that you don't want to be public (e.g. your house, friends/relatives' house, work), then change it to another photo (or remove the EXIF information if you know how to do that). Avoid photos with family that could be used to identify your family members. Click "edit cover photo" to change.

- * **Review your profile photos.** Your primary profile photo is always public. **As with the cover photo, minimally ensure this photo was not taken at a place that would reveal a location you don't want public, like your home.** The best course is to choose a photo that does not show your likeness or that of any of your family, an avatar or similar, instead.

- o To change it, click your profile photo, and then "Update Profile Picture." Select a new photo.

- o You also want to review your old profile photos. Click your profile photo again and then click "View profile picture."

- In the top right, there are three dots. Click them and then click "Edit Audience." This does not change who can see your photo (everyone), but does let you limit who can see likes and comments on it. **Set to Friends or Only Me.**

- **Click through your profile photos and change the audience on each one to Friends,** or delete them. These photos will be limited to only your friends.

Now, back to your main profile page. If you have a bio, you should probably delete it. **Next, click "Edit Profile."**

- Review and edit this information as you see fit.

- Scroll to the bottom and click "Edit your About Info."

- * **Work through each of the categories on the left (e.g. Work and Education, Places You've Lived, etc) and review the associated information in the right pane. Here's what you're looking to do:**

- o Remove any unnecessary information.

- o For the information you keep, check who it is shared with by click the three dots on the right. **At most, share with Friends.**

- o **Keeping your birthdate/year on your profile is a bad idea.** It can help someone steal your identity.

- * **Now, scroll down and review all of your friends. Remove any that you don't know, or that seem suspicious.** Don't be afraid to ask them questions only that person would know to verify they are who they claim to be.

LINKEDIN SETTINGS GUIDE

On a desktop/laptop, go to: <https://www.linkedin.com/psettings/account>

ACCOUNT SETTINGS TAB

Under the **Login and Security** heading:

- **Review/update login settings.** Update/change your email address, set a new password with your password manager, and check devices that remember your password (review this list and remove any old, unused, or unknown devices).
- **Enable two-step verification.** Click "change" to the right of "two-step verification," and **turn it on.** Follow steps to select "authenticator app," as your method and add the authentication token to your app of choice. Next, get the recovery codes and save them someplace safe (either encrypted or offline).

Under the **Site Preferences** heading:

- **Review: Name, Location, and Industry.** Click "change" to the right of "Name, Location, and Industry." All of this information is generally public (you can control this some, see later settings).

Under **Partners and Services** heading:

- **Review connected accounts and services.** Recommend you unlink all accounts and services (Microsoft, third party, Twitter).

Under the **Account Management** heading:

- **Consider hibernating or deleting your account.** Unlike Facebook, only about a quarter of Americans have a Facebook account. You don't have to have one. If you're happy with your current job, in this section you can either hibernate or delete your account. Hibernation is a good option if you expect to look for a new job in the future, but not right now. If you choose to hibernate or delete your account, you're done. If not, continue.

Next, click the **Privacy Tab** at the top of the page.

PRIVACY TAB

Under the "**How others see your profile and network information**" heading:

- * **Edit: your Public Profile.** Click "edit your Public Profile." If your profile is public, this view will show you what *anyone searching on the internet* will see when they click your profile.
 - o **Click "edit your custom URL" in the top right.** This is the web address for your profile. **Remove any reference to your name;** it's best just to type a string of 6-12 random numbers and letters. Click the "Save" button when you're done.
 - o Before editing content, go to down to the "Edit Visibility" header on the right. **Recommend:** set "your profile's public visibility to off."
 - If you did that, you're done with this section, if not: set profile photo to "only first degree connections," and then scroll down to toggle off headline, summary, articles and activity, current experience, past experience, education, and groups to your comfort level (recommend all toggled off: remember, this is for *anyone* to see).
 - Return to privacy settings tab.
- **Edit: who can see your email address.** Click "who can see your email address." **Recommend:** set to "Only visible to me." If people want to contact you, they can message you in LinkedIn.
 - o Set toggle to "No." Set the "allow your connections to download your email in their data export?" toggle to no.
- **Edit: who can see your connections.** Click "who can see your connections." **Recommend:** set to "only you." Your other option is "your connections," but this is a huge group – people connected to you (1st), people connected to them (2nd), and people connected to them (3rd). LinkedIn is a big game of six degrees of Kevin Beacon. Your connections reveal a lot about who you are, what you do, who your family is, etc.
- **Edit: viewers of this profile also viewed.** **Recommend:** set to "No."
- **Edit: who can see your last name.** **Recommend:** last initial (second option). Your connections (all 1st, 2nd, and 3rd level connections) will still see your full name, but people completely unconnected to you will only see your last initial.
- * **Edit: representing your organization and interests.** Set to "No."
- * **Edit: profile visibility off LinkedIn.** Set to "No."
- * **Edit: Microsoft Word.** Set to "No."

Under the **"How others see your LinkedIn activity"** heading:

- **Edit: Profile/Story Viewing Options.** For these two settings, choose either "private profile characteristics" or "private mode." If you're a LinkedIn subscriber, the clear option is "private mode" because you can remain anonymous and still see who has viewed your profile. If you're not a subscriber and select "private mode," you lose the ability to see who has viewed your profile.
- **Edit: Manage active status.** Recommend: Your connections or no one. This can be used to monitor your habits and activity.
- **Review: (1) Share job changes, education changes, and work anniversaries from profile; (2) Notify connections when you're in the news; and (3) Mentions or tags by others.** Recommend: set all to "No."

Under the **"how LinkedIn uses your data"** heading:

- **Edit: Manage who can discover your profile from your email address.** Recommend: "Nobody." Your email is effectively public because of data leaks and thefts, and can be used by scammers and others to pretend to be a connection and connect with you.
- **Edit: Manage who can discover your profile from your phone number.** Recommend: "Nobody." For the same reasons as your email.
- *** Review: Sync Contacts.** Review and remove any synced contacts — do not sync contacts. Syncing contacts gives Microsoft a metric ton of information on your friends, family and colleagues and their addresses, phone numbers, and emails.
- *** Review: Sync Calendar.** Remove any synced calendars, and do not sync calendars. Like contacts, this is a lot of information to give away about you and your activities.
- **Review: Salary data on LinkedIn.** Recommend: delete any salary data.
- **Clear: Search history.**
- **Review: Personal demographic information.** Recommend: click "remove all information."
- *** Edit: Social, economic, and workplace research.** Toggle off.

Review all items under the **"Job seeking preferences"** and the **"Blocking and hiding"** headings.

Next, click the **Ads Tab** at the top of the page.

ADS

**** Review every item on this page and set all of them to "no" or unclick all boxes. ****

When you're done, click the **Communications Tab** at the top of the page.

COMMUNICATIONS

Review every item on this page based on your preferences and comfort levels.

For "Research Invites," set to "No."

FINALLY, REVIEW YOUR PROFILE

Go to your profile by clicking your profile picture in the top right of the screen, and then "View Profile."

- *** Review your profile photo.** **Ensure this photo was not taken at a place that would reveal a location you don't want public, like your home.** Or, if you know how, you can use a tool to remove the EXIF data.
- Review and edit your profile with an eye to what you're willing/comfortable sharing. Think about how a criminal or other adversary might see and use this information as you review it.

INSTAGRAM SETTINGS

FIRST A HEADS UP

Before we go into the settings, you should be aware that Instagram is inherently dangerous from a privacy perspective. Most commonly, people post photos and videos from their daily activities. This can provide a potential adversary with a lot of information about your lifestyle, interests, family and friends, their facial recognition data, where you live, where you frequent, and more. While Instagram seems to strip EXIF (e.g. location) data from photos posted to Instagram, Facebook, Instagram's parent company, certainly has access to all of that information. So be careful. If you're a member of Gen Z or a younger millennial, you probably can't completely abandon Instagram without attracting attention to yourself or losing the ability to monitor what's posted about you there. If you're not in that demographic, consider walking away and deleting your account.

Now, on a desktop/laptop, go to:

<https://www.instagram.com/accounts/edit/>

EDIT PROFILE

Start by reviewing your profile:

- * **Name.** Change your name to either an alias or just your first name. Don't use your full name.
- * **Username.** Change your username to something without your name in it, e.g. "AtomicBlossom."
- **Remove bio information.**
- * **Uncheck "Similar Account Suggestions."** Uncheck the box at the bottom that says "Include your account when recommending similar accounts people might want to follow."
- **Hit Submit button.**

If you're not sure if you want to delete your Instagram account or not and want to see what it's like without it, you can temporarily disable it by clicking the "temporarily disable my account" link to the right of the submit button.

Next, go to **Change Password** tab on the left menu.

CHANGE PASSWORD

On the change password tab, you can, well, change your password. Set a new secure password generated by your password manager.

Next, go to **Apps and Websites** tab on the left menu.

APPS AND WEBSITES

Review. Recommend; unlink any apps or websites listed here.

Instagram Settings (Twitter on opposite side)

Social Media Settings Guide - The Complete Digital Privacy Checkup Checklist - May 2020

Next, go to **Email and SMS** tab on the left menu, review and then **Push Notifications** tab.

EMAIL AND SMS AND PUSH NOTIFICATIONS

Review these two tabs. You can manage your notifications.

Next, go to the **Manage Contacts** tab on the left menu.

MANAGE CONTACTS

- * **Delete/Disconnect any synced contacts.** Syncing contacts gives Facebook a metric ton of information on your friends, family and colleagues and their addresses, phone numbers, and emails.

Next, go to the **Privacy and Security** tab on the left menu.

PRIVACY AND SECURITY

Under Account Privacy heading:

- * **Check "Private Account."** If this setting isn't checked then everything you post is public.
- **Uncheck "Show Activity Status."** This can be used by adversaries to track your online patterns and activity.
- * **Uncheck "Allow Sharing."** If you leave this checked, it effectively allows anyone to bypass your privacy and open your posts up to anyone.
- **Review comment settings.** This page can be used to add keywords that automatically hide any comments that contain them. You can put your last name, for example, to hide any comment that mentions your last name, or any other identifying information you don't want the world to associate with your Instagram account. Just be aware that you are also telling Facebook what information you believe is sensitive.
- **Set "Photos of You" to add manually.** This lets you control what gets associated with your profile (it doesn't let you control what people choose to post of you).
- **Turn on Two Factor Authentication.** Click the "edit two factor authentication settings" link. Set up two factor authentication. Instagram requires you first set up text message authentication, but you can then add an authentication app as another method.

HOW TO PERMANENTLY DELETE YOUR INSTAGRAM ACCOUNT

You can permanently delete your Instagram account by going here:

<https://www.instagram.com/accounts/remove/request/permanent/>

TWITTER SETTINGS

TWITTER TIPS

Like Reddit (below), Twitter accounts don't need to be associated with your name. If you just like lurking on Twitter, you can set a very private profile and use it to read tweets. If you're going to engage in Tweeting, try to separate your Twitter identity from your real one. Some tips:

- Use a username (your @) that is not affiliated with your name, is not used on other services, and would not be something someone who knows you would guess might be you.
- Avoid tweeting information that could be used to identify you.
- To further minimize a username's association with you, register using an email alias that doesn't contain your name and that you don't use elsewhere.
- If you have a Twitter account associated with your name, or if you post things that might identify you, at least make your account private.

Now, on a desktop/laptop, start by going here:

<https://twitter.com/settings/account>

ACCOUNT SETTINGS

Under Login & Security header:

- **Review username**, and change as desired.
- If you don't have a phone number attached to your account, add one for extra account security. You can use a virtual number (i.e. Google Voice) if you want to keep your account anonymous.
- **Change email and password as appropriate**. Use your password manager to set a new complex password.
- **Click Security**.
 - o **Check "password reset protect."** Follow prompts to enable it.
 - o **Next enable Two Factor Authentication**. Click the tab for Two Factor Authentication and then check the box for "authentication app." Follow the prompts to set it up with your token app of choice. Then return to the account tab.
- You can delete your Twitter account by clicking "Deactivate your account" at the bottom of this menu. Your account will be deactivated for 30 days and then Twitter will start deleting it.

Next, click the **Privacy and Safety** tab on the left hand side of the page.

PRIVACY AND SAFETY

Under Privacy and Safety and Tweets headers:

- * **Check "protect your tweets" box.**

Twitter Settings (Instagram on other side)

Social Media Settings Guide - The Complete Digital Privacy Checkup Checklist - May 2020

- * **Click "Location information" tab**

- o **Ensure "add location information to my Tweets" is unchecked.**
- o **Click "delete all location information"** and confirm. Return to the Privacy and Safety menu.

- * **Click "photo tagging" tab**

- o **Ensure "photo tagging" is turned off.** Return to the Privacy and Safety menu.

Under Direct Messages header:

- **Uncheck "Receive messages from anyone."**

- **Check "quality filter."**

- Review "read receipts" and choose your preference.

Click "discoverability and contacts" tab

- Under discoverability, **recommend you uncheck both boxes** (let people find you by email or your phone number).
- * **Click "manage contacts"**
 - o **Turn off any contact syncing that is set up.**
 - o **Click "remove all contacts" and confirm.** Return to the Privacy and Safety menu.

Review settings under safety header.

- ** **Click "personalization and data" tab.**

- At the top, toggle off "personalization and data"
- Check to see that all of the boxes are unchecked.

Review the other settings tabs.

LAST, REVIEW YOUR PROFILE

Visit: https://twitter.com/i/flow/setup_profile

Follow the menu to review your profile photo, background photo, and bio. **This information is all public.** Recommend you use an avatar or other image instead of a profile, and avoid using photos taken at a place associated with your without removing EXIF information.

REDDIT SETTINGS

FIRST, SOME REDDIT TIPS

Reddit can be hypothetically anonymous. While the company can almost certainly identify you through your IP addresses, devices, etc, your presence on the platform can be refreshingly private when managed properly. To achieve this:

- Choose a username that is not affiliated with your name, is not used on other services, and would not be something someone who knows you would guess might be you.
- Avoid posting about anything that could be used to identify you. If you want to post things like that, create a separate username for those posts (many Reddit apps let you use/manage multiple accounts). Think of each username like an identity.
- To further minimize a username's association with you, register using an email alias that doesn't contain your name and that you don't use elsewhere.
- To minimize the data Reddit collects on you while still getting a lot of functionality, **use a third-party app**. Apollo is both an improvement over the default Reddit app, and more private.
- Be aware that if you use Reddit for a number of years, the combination of your posts, comments, and subscribed subreddits can probably be used to identify you.

Now, on a desktop/laptop, go to:

<https://www.reddit.com/settings>

ACCOUNT SETTINGS

- **Update your email and password** as appropriate. Set a new complex password with your password manager.
- **Ensure your account is not linked to Twitter.** Disable/unlink if it is.

You can deactivate your account by clicking the red "deactivate account" at the bottom of the page.

Next, click **Profile** tab at the top of the page.

PROFILE SETTINGS

- * **Reddit profiles are public and completely optional.**
Recommend: delete anything here.
- * **Ensure "content visibility" and "active in communities visibility" are unchecked.**

Next, click **Privacy and Security** tab.

PRIVACY AND SECURITY SETTINGS

* Under "privacy" header, review and untoggle/deselect all options.

Under the "advanced security" header:

- **Turn on "Use two-factor authentication."** Follow prompts to set up your chosen authentication app for 2FA.

REVIEW OTHER TABS

Review the other tabs to set notification, and chat preferences.

THE COMPLETE PRIVACY CHECKUP CHECKLIST

This checklist is for those who want to go all the way and complete the entire Checkup.

It's task-organized to help you get there efficiently.

STEP ONE: SECURE DEVICES & REDUCE COLLECTION

☐ **Complete device settings checklists for your devices** (iOS/iPadOS, Android, Windows, MacOS).

☐ Ensure your devices are encrypted using strong diceware passwords (instructions in guides)

Diceware word lists: [here](#), [here](#), and [here](#).

☐ Ensure auto-update is enabled for all devices and applications.

☐ Ensure your Windows PCs are minimally protected with Windows Defender (avoid Kaspersky). Consider a total security suite for all of your devices.

☐ Enable WiFi calling on your phone if it's part of your cell phone plan.

☐ **Switch to [Signal Messenger](#)** for a more secure alternative than traditional phone calls and SMS messages.

☐ **Recommended: install the latest version of Mozilla Firefox and set to default;** follow [Firefox checklist](#) to restrict tracking. Alternately, install [Brave](#).

☐ Complete settings checklist for your browser ([Firefox](#) or [Brave](#)); install browser extensions (see guide).

☐ Review and delete unnecessary browser extensions.

☐ Set default browser to DuckDuckGo or Startpage and start searching privately.

☐ **Use an encrypted DNS service** (e.g. Cloudflare 1.1.1.1), see browser configuration guides for Firefox and Brave.

☐ Acquire, download and use a paid, privacy-oriented, VPN service, especially on a public network, or use Cloudflare's free WARP service.

STEP TWO: DECIDE & GET SERVICES

Now is the time to decide what services you want to use. Most importantly, are you changing to a more private email provider like [ProtonMail](#) or [Tutanota](#)? If you are, do this now. Also, decide what app you're going to use for 2FA.

☐ **Get a 2FA token app if you don't already have one.** If you have one and want to switch, now is also the time to get one. Microsoft Authenticator or LastPass Authenticator is recommended so you can securely back up your tokens.

☐ **Consider changing to private alternatives.** If you're switching email, create your new email account so you can move your accounts to it later. Enable 2FA on it. If your new email service allows you to create email aliases, create some to separate the email you use to communicate with people and those you use for accounts/logins.

☐ **Set up and use a password manager** ([Dashlane](#), [LastPass](#), [1Password](#), [KeyPassXC](#)), using a strong diceware password and enabling two factor authentication to protect it. If you didn't set a strong password for your email, go back and do this now – go crazy, many providers let you use 30-, 40-, 50-character passwords that will never be broken (you don't have to type them in anymore).

☐ **Consider switching to a more private cloud storage provider like [Sync](#) or [Tresorit](#).** Enable 2FA.

STEP THREE: LOCKDOWN SOCIAL MEDIA

☐ **Double-check privacy settings for social media accounts** to restrict public information and sharing. Change any old public posts to private (just friends). See [Social Media Settings Guide](#) for a walk-through of Facebook, LinkedIn, Instagram, Twitter, and Reddit settings.

For each social media service:

☐ Check profile photos and replace photos taken in revealing locations with others, or delete and replace with an avatar or non-identifying photo.

☐ Review and delete unnecessary or revealing details in your social media profiles.

☐ Review your friends and remove suspicious accounts or people you don't know.

☐ Consider deleting social media apps from your devices and using the website instead (you can still have the icon on your home screen/app drawer).

☐ California/EU/Nevada residents (or those pretending to be...): exercise your right to request these companies not sell your data.

☐ Enable 2FA for each site, set a strong password from your password manager, and change your account email to your new, more-private, email account.

STEP FOUR: SECURE YOUR ONLINE DATA

☐ **Comb through your account, app, and service settings for every account you have to restrict data-sharing,** following the [Privacy Settings Checklist](#).

☐ Take this opportunity to delete any old or unused accounts (www.justdeleteit.xyz).

☐ California/EU residents (or those pretending to be...): exercise your right to request companies not sell your data for the services you use or to delete your accounts/data.

☐ Enable 2FA for each site where it is available, set a strong password from your password manager, and change your account email to your new, more-private, email account. Consider giving fake answers to security questions.

☐ Avoid single sign-ons (e.g. login with Facebook, Amazon, or Google) – Apple single sign-on is okay. If you currently use single sign-ons, the walkthroughs for Facebook, Amazon, and Google discuss how to turn them off.

☐ **Place credit freezes at credit bureaus:**

☐ **Equifax:** <https://www.freeze.equifax.com>

☐ **Experian:**
<https://www.experian.com/freeze/center.html>

☐ **TransUnion:** <https://www.transunion.com/credit-freeze>

☐ **Sign up for a breach monitoring service** (e.g. [Firefox Monitor](#)) or full identity protection service.

STEP FIVE: SECURE YOUR HOME NETWORK

☐ **Secure your home router:**

☐ Consider replacing a router provided by your service provider with one you own.

☐ Set a strong password on your home network router.

☐ Ensure your home router's firmware is up-to-date, and if available, set it to auto-update.

☐ Set your home router to deny external/remote administration or configuration; disable UPnP.

☐ Ensure your home WiFi network is secured using WPA2 encryption (WEP and WPA are easily cracked), and uses a strong password.

☐ **Change default passwords for any other device connected to your network** (e.g. cameras) and ensure they are up-to-date.

☐ **If you have a secure WiFi guest network, segregate internet-of-things devices onto your guest network** (e.g. cameras, digital assistants).

STEP SIX: CHANGE YOUR HABITS

☐ **Be careful about the devices you buy and services you use, and avoid devices and services from Chinese companies.**

☐ **Get in the habit of turning off Bluetooth and WiFi when you're not using them.**

☐ **Don't plug your devices directly into public USB ports to charge them without a data blocker.**

☐ **Discuss and share this guide with your friends, family, and coworkers.** If you're savvy, offer to help them with some of the more difficult actions. You can do this while you're sharing your new email address, if you created one.

OPTIONAL: CLEAN UP YOUR ONLINE DATA TRAIL

☐ **Consider completing the [Database Removal Checklist](#)** to clean up your online presence with data providers and data brokers and start with a new slate.

CONGRATULATIONS! YOU HAVE TAKEN CONTROL OF YOUR PRIVACY. NOW KEEP IT.

☐ **Set a calendar reminder to review social media settings every 3 months.**

☐ **Set a calendar reminder to conduct an annual checkup:**

☐ Review your password manager for accounts you no longer use and close/delete them to protect your data from breaches that haven't been discovered/announced.

☐ Change passwords.

☐ Revisit privacy settings and options for your devices and services you use.

☐ **Become engaged in privacy issues.**

WINDOWS 10 CONFIGURATION GUIDE

Configure Windows 10 to Harden it from Attacks and Reduce Tracking

OVERVIEW

Altogether, this guide will help you to significantly protect both your privacy and your data. **If you don't care to do everything, that's your call, but at least complete [General Privacy Settings](#), [Activity History](#), [Location](#), and [Diagnostics & Feedback](#).**

A handful of settings can go a long way to making your device both much more secure and private.

This guide also seeks to balance usability with privacy and security. **For most users, changing these settings won't impact your use.** In instances where changes might impact some users, it will be explained. While everything here matters, red stars (*) denote critically important settings for privacy.

All settings can be found in Windows Settings. You get there by clicking the bottom left Windows/start menu, then clicking the settings gear icon. If you have difficulty finding a setting, you can search for it in the bottom left search bar.

Open Windows Settings, and get started:

GENERAL PRIVACY SETTINGS (ADS)

From Windows Settings, click Privacy (a lock icon).

**** On the main privacy page, switch off all four general privacy settings** (let apps use advertising ID, let websites provide locally relevant content, let windows track app launches, and show me suggested content). **While they're all important, the first setting (let apps use advertising ID), lets advertisers track your use of Windows applications.**

ACTIVITY HISTORY

Next, from the Privacy settings menu, select **Activity History** from the left menu.

**** Activity History.** Uncheck both boxes (store my activity history on this device, and send my activity history to Microsoft). **These settings allow Microsoft to track all of your activity on Windows (including websites visited and apps used).**

If you are logged in using a Microsoft Account, there will be a toggle switch under a header **"Show Activity from these Accounts."** Toggle it off.

Finally, click the "clear history" button.

** LOCATION

Next, on the left menu in Privacy Settings, click **Location**.

**** Location.** Location services are ~80% of your device privacy, or lack thereof. **Most people can disable location services on their PC altogether and have no impact to usability.** You may need to occasionally enter in a zip code or an address instead of having it auto-populate, it's a small price to pay for significantly better privacy.

To completely disable Location, click the "change" button under the "allow access to location on this device" header, and toggle off Location. Unlike other operating systems, Windows does not allow you to fine tune what data is used to determine your location, so this strongly recommended for privacy.

*** Next, click the "clear" box** under the "Location History" header.

If you disabled Location, then you're done with this section. If not, continue:

- *** Review the apps/services below "choose which apps can use your precise location."** Be extremely judicious about what apps you grant access to your location.

** DIAGNOSTICS & FEEDBACK

From the same privacy settings menu, select **Diagnostics & Feedback** on the left menu.

- **** Under Diagnostic Data, select the "Basic" radio button.** The alternative, "Full," provides Microsoft detailed information on your browsing habits and use of your computer.

- *** Switch off all three toggles** (improve linking and typing, tailored experiences, and view diagnostic data).

- **** Click the "delete" box under "Delete Diagnostic Data."** This will delete all data collected to this point.

- Under "feedback frequency," use the drop down to change to "never."

- Under "recommended troubleshooting," use the dropdown to change to "only fix critical problems for me." Again, this setting potentially allows detailed information to be sent to Microsoft about your computer and usage when there's an error.

SPEECH/INKING AND TYPING

Next, visit the “speech” and “inking and typing menus on the left menu in privacy settings, and disable both. If you’re one of the very few people who use Cortana, you must keep speech enabled to continue using it.

OTHER PRIVACY SETTINGS

Next, from the same privacy settings menu, review each item on the left menu below Location. Review each and either turn off each completely or revoke access to any apps that don’t seem to have a clear reason for the information. Be particularly mindful of:

- **** Contacts. Sharing contacts with an app is dangerous.** Most apps heavily abuse the privilege by uploading your contacts to the parent company and sharing and selling them to advertisers – not just the names, but the numbers, emails – everything. **Avoid sharing them with social media applications, in particular.**
- Most users can safely disable most of these completely without affecting their usability. **To completely disable an item click the “change” box at the top, and then toggle the service off.**
- **The following services ARE used by most people, and shouldn’t be turned off completely unless you don’t use them:** camera (video calls), microphone (video calls), background apps (general use), documents, pictures, videos, file system.

When you’re done with that, return to the main settings menu; you can click the back arrow in the top left.

UPDATE & SECURITY

Next, from the main Settings menu, select **Update & Security**.

- Click “Advanced Options.” From the advanced options menu, **toggle on “Receive updates for other Microsoft products when you update Windows” and “Update Notifications.”** Then go back by clicking the back arrow in the top left.
- Click the “Check for updates” box. Install any available updates.

WINDOWS SECURITY

Next, from the Updates & Security settings, click **Windows Security** on the left menu.

- **Ensure all items have a green check next to them** (virus & threat protection, account protection, firewall & network

protection, app & browser control, and device security). Visit any item that is not checked and follow prompts to correct.

Next, return to the main settings menu.

WI-FI SETTINGS

Next, from the main settings menu, select **network & internet**. Then select **Wi-Fi** from the left menu.

- **Enable Random Hardware Addresses.** Depending on your version, this will either be available below the list of Wi-Fi networks as a toggle, or in a submenu under “advanced options” in the same place.
- **Review saved Wi-Fi networks.** From the Wi-Fi settings screen, select “manage saved networks.” **Remove/forget any old/unused/public networks.**

Next, return to the main settings menu.

ACCOUNT SETTINGS (LOGIN)

From the main settings menu, select **Accounts**. Then, **click sign-in options on the left.**

- *** Review sign-in options.** Set a new strong diceware password if you have not yet done so. You can use Windows Hello (face or fingerprint) if available, these are secure sign-in options. You can also set a login PIN for faster login (not recommended if traveling to a high-risk country). PINs should be at least 6 characters – check the box to use a PIN that includes letters. PINs are local to your device – they can only be used to gain access to your computer if you physically have the computer (unlike a password, which can be used remotely).

- Under Privacy, **toggle off “show account details such as my email address on the login screen.”**

Return to the main settings screen.

CORTANA

From the main settings menu, select **Cortana**. **If you don’t use Cortana, switch all off.** Otherwise, **review and turn off the last toggle (use Cortana even when my device is locked).**

Return to the main settings screen.

SEARCH

From the main settings menu, select **Search**. **Toggle off all toggles** (Microsoft Account, Work or School Account, My Device History, My Search History.)

- Click the “clear my device history” box.

ENCRYPT YOUR PC

Unfortunately, Windows PCs do not have an easy out-of-the-box encryption option. That's a problem because your data is completely unprotected if your device falls into the hands of a thief or customs inspector. There are two main ways to encrypt a Windows PC – with Microsoft's Bitlocker (Windows Pro only), and with VeraCrypt, a free, open-source, encryption tool. For most people, VeraCrypt is probably the best option – both for ease and availability (most people don't have Windows Professional). If Bitlocker is available, and your computer is equipped with a Trusted Platform Module (TPM), then Bitlocker does provide the most seamless way to encrypt.

VeraCrypt:

Here's a guide to encrypting your system drive with VeraCrypt: <https://www.howtogeek.com/howto/6169/use-truecrypt-to-secure-your-data/>

Bitlocker

You can check if your PC has a TPM by typing "tpm.msc" in the search bar and selecting the TPM app. If there is information on a TPM version, you have a TPM. If it doesn't, you can still use Bitlocker if you wish, guide below. Your PC must also have Windows 10 Professional or Enterprise, you can check by typing "about my PC" in the search bar, select the app, and scroll down to "Windows Specifications." If it says Windows 10 Pro, you're ready to go.

- This guide describes how to enable Bitlocker with a TPM: <https://www.dell.com/support/article/en-us/sln302845/how-to-enable-or-disable-bitlocker-with-tpm-in-windows?lang=en>
- This guide describes how to enable Bitlocker without a TPM: <https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/>

In either case, you want to encrypt the entire drive, not just used space.

1.1.1.1 APP

As of this writing, Cloudflare's 1.1.1.1 WARP service was in closed beta testing for desktops. When it's available for broader download/install, it's a good solution to force all of your computer's connections through encrypted DNS and encrypt your traffic so that your internet service provider cannot see what you're up to on the internet.

TURN OFF/ON BLUETOOTH AND WI-FI

Both Bluetooth and Wi-Fi are typically in the Action Center, available by clicking the bottom right of the screen (notifications). Tap the icon and turn them off/on.

If the Bluetooth icon is not in the Action Center, you can turn it off by going to windows settings -> devices -> Bluetooth and toggling it off there.

FACTORY RESET

Backing up and factory resetting a Mac or PC is much more complicated and time consuming than for a mobile device like an iPhone. For this reason, it's best to just buy a cheap computer if you need a computer when traveling to a high-risk country.

To back up your computer, such as for a trip with it to a high-risk country, you'll need a portable hard drive that has at least as much space as you have used on your computer, and you can follow the guide here:

<https://www.windowcentral.com/how-make-full-backup-windows-10> - you want to create a system image.

To securely erase and factory reset your PC, here's another guide: <https://home.bt.com/tech-gadgets/computing/windows-10/how-to-wipe-your-pc-with-windows-10-11364002707321>

SOCIAL MEDIA SETTINGS GUIDE

This guide will walk you through changing your social media settings.

There are walk-throughs for [Facebook](#), [LinkedIn](#), [Instagram](#), [Twitter](#), and [Reddit](#) settings on the following pages.

REVIEWING SOCIAL MEDIA SETTINGS

Social media settings change constantly, so as you work your way through your social media settings, when reviewing social media settings:

- **Be on the lookout for any new options** not mentioned here.
- **It's best just to work your way through every menu**, as settings are often hidden in unexpected places.
- **For most services, the desktop website version offers the most options**, so that's where you should start.

This guide provides walk-throughs for [Facebook](#), [LinkedIn](#), [Instagram](#), [Twitter](#), and [Reddit](#). A * will denote a setting that is critically important to your privacy. **Comb through the menus of any other social media services you use for similar settings** (e.g. Snapchat, Goodreads, Pinterest, etc).

Settings in this guide are based on the desktop website version of each site, both because the web version has the most options and to avoid needing to have multiple guides for each service.

For each social media service:

- ☐ **Double-check privacy settings for social media accounts to restrict public information and sharing.**
- ☐ **Change any old public posts to private (just friends).**
- ☐ **Check profile photos** and replace photos taken in revealing locations with others, or delete and replace with an avatar or non-identifying photo. Please don't use your kids.
- ☐ **Review and delete unnecessary or revealing details** in your social media profiles.
- ☐ **Review your friends and remove suspicious accounts or people you don't know.**
- ☐ **Consider deleting social media apps from your devices and using the website instead** (you can still have the icon on your home screen/app drawer – instructions in right column).

In the following guides, a * denotes a setting that is critically important to your privacy.

MAKE YOUR OWN APP

Social media apps are notorious for devouring as much information about you, your devices, and how you use them as you can.

You can stop this by using the mobile web page version instead. How to do it:

iOS/iPadOS (Safari only):

- Open Safari and go to the service's webpage (e.g. <https://facebook.com>). Log in.
- Tap the Share icon at the bottom (a square with an arrow pointed upward).
- Scroll down to "Add to Home Screen"
- Type the name of the service (e.g. Facebook) above where the web address is.
- Tap "Add" in the top right.

Android OS - Firefox:

- Launch Firefox and go to the service's website (e.g. <https://facebook.com>). Log in.
- Tap the menu icon.
- Tap "Page."
- Tap "Add to Home Screen."

Android OS – Brave:

- Launch Brave and go to the service's website (e.g. <https://facebook.com>). Log in.
- Tap the menu button.
- Tap "add to home screen."

DON'T LINK ANYTHING TO SOCIAL MEDIA

Lots of apps and websites want you to link your social media account to them. Don't. They want this because it's a way to better track and get more information about you.

(front)

SOCIAL MEDIA AWARENESS

- Remember that anything you post, comment, or like will be collected and analyzed by the service you are using, and those “insights” will be sold to or shared with other companies.
- Avoid commenting on posts marked public, these comments can be easily collected and analyzed.
- Monitor what people post and say about you, and check if it’s public. Contact and ask them to restrict access on public posts about you.
- Only accept friend requests from people you know, and consider asking them a question only they would know the answer to before accepting. Imposters use fake friend requests to snoop on you and your family, usually for criminal purposes.

(back)

FACEBOOK SETTINGS GUIDE

On a desktop/laptop, go to: <https://www.facebook.com/settings>

Sorry up front – Facebook has a LOT of settings.

GENERAL ACCOUNT SETTINGS

From the General Account Settings page:

- **Review Name and Username.** Recommend you use the name people know you by. Using something different won't confound anyone researching you, and may draw unwanted attention your way. If you do use another name, ensure your username doesn't reveal your real name.

- **Review Contact and Ad Account Contact.** If you are changing your email to a more private provider, this is where you do it.

Next, **go to Security and Login** on the left menu.

SECURITY AND LOGIN

From the Security and Login page:

- **Review "Where you're logged in."** You may need to click "see more." Review the devices. If there are any old devices, click the three vertical dots to the right of them and select "Log Out." If you one of them is not your device and you don't know why it's there, select "Not you?"

- **Next, change password.** Click the edit button next to "change password" and change your password to a strong password generated by your password manager.

- **Set up 2FA.** To the right of "use two factor authentication," click the edit button. Choose Authentication App -> add new App. Scan the QR code with your app or copy/paste the shared secret. Once it's saved in your app, tap continue, enter the six-digit code from your app to confirm.

- Next go to "Show Codes" to the right of "Recovery Codes." Copy and paste these somewhere safe (e.g. Standard Notes encrypted note, your password manager's notes section (not ideal), or print them out and keep them somewhere safe (...like a safe).

- If you have SMS as a backup method enabled, **disable it.**

- **Review authorized logins.** Below change you password, tap the view button next to "authorized logins." Remove any old devices, third party apps or devices, or anything you don't know what it is.

- **Ensure "get alerts about unrecognized logins" is on.**

- You can optionally "choose 3 to 5 friends to contact if you get locked out." If you're locked out, your friends will each get a code. You need all of the codes to unlock your account. It's a pretty secure recovery method. Five friends is best.

Next, **go to Your Facebook Information** on the left menu.

Facebook Settings (front)

Social Media Settings Guide – The Complete Digital Privacy Checkup Checklist – May 2020

YOUR FACEBOOK INFORMATION

From the Your Facebook Information page:

- * Click view button to the right of "**Off-Facebook Activity**"
 - Click "Clear History" button on the right, and confirm.
 - Below that, click "More Options."
 - Click "Manage Future Activity." When the menu pops up, click the blue "Manage Future Activity" button.
 - **Next to "Future off-Facebook activity," change the toggle to off.**
 - When the menu pops up, click the blue "turn off" button.

Next, return to the settings menu and **go to Privacy** on the left settings menu.

PRIVACY

From the Privacy page:

- * Next to "who can see your future posts?" ensure it says "Friends." If it does not, click "Edit" and change to Friends.
- * Next to "Limit the Audience for Old Posts on your Timelines," click "Limit Past Posts" on the right. Tap the "Limit Past Posts" button, and then when the popup menu displays, "Limit Past Posts" button again.
- * Under "How People Find and Contact You" edit each one as follows:
 - "Who can send you friend requests?" **Friends of Friends.** This helps prevent scammers from posing as your friends to friend you.
 - "Who can see your friends list?" **Friends.** Your friends list contains a lot of information about who you know and work with, and can be used for deep research into your life.
 - "Who can look you up using the email you provided?" Anything but everyone – suggest **only me.** The more you lock this and the next setting down, the harder it will be for scammers to friend you – your email and phone are widely available through stolen databases.
 - "Who can look you up using the phone number you provided?" Anything but everyone – suggest **only me.**
 - "Do you want search engines outside of Facebook to link to your profile?" **No.**

Next, **go to Timeline and Tagging** on the left settings menu.

TIMELINE AND TAGGING

From the Timeline and Tagging page, review settings. **Recommended settings:**

- "Who can post on your timeline?" **Friends or Only Me.**
- * "Who can see what others post on your timeline?" **Friends.**
- * "Allow others to share your posts to their stories?" **Off.**

- "Hide comments containing certain words from your timeline?" You can use this to somewhat restrict what people say about you. For example, if you're a NYPD police officer and want to minimize comments connecting you to police you might have "police, FOP, cop, NYPD." Just know that you're also giving Facebook information about what you find sensitive.

- * "Who can see posts you're tagged in on your timeline?" **Friends or Only Me.**

- "When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?" **Friends or Only Me.**

- Review posts you're tagged in before the post appears on your timeline?" **On.**

- Review tags people add to your posts before the tags appear on Facebook?" **On.**

Next, **go to Stories** on the left settings menu.

STORIES

From the Stories page, set all to "Don't Allow."

Next, **go to Location** on the left settings menu.

LOCATION

* **On the Location Settings page, ensure Location History is off.**

Next, **go to Blocking** on the left settings menu.

BLOCKING

On the Blocking page, review settings. **Restricted List** lets you add people who you are friends with who you don't want to see most of your activity.

Next, **go to Face Recognition** on the left settings menu.

FACE RECOGNITION

* **On the Face Recognition page, set Face Recognition to No.** This will prevent Facebook from collecting and using your facial data.

Next, **go to Public Posts** on the left settings menu.

PUBLIC POSTS

* **On the Public Posts page, set "Who Can Follow Me?" to Friends.** If you have a connected Twitter account, recommend you disconnect it.

Next, **go to Apps and Websites** on the left settings menu.

APPS AND WEBSITES

* **On the Apps and Websites page, recommend you turn off Apps, Websites, and Games.** If you have websites that you use for Facebook single sign-on logins, you should first go to those websites and either create an account/password with the same email you use for Facebook, or delete the account.

Facebook Settings (back)

Social Media Settings Guide – The Complete Digital Privacy Checkup Checklist – May 2020

REVIEW NOTIFICATIONS SETTINGS

You can review and change your notification settings by going to Notifications on the left menu.

REVIEW PROFILE AND COVER PHOTOS

Click your Profile Picture/Name in the top right of the screen.

- * **Review your cover photo.** This photo is always public. If it was taken at a location that you don't want to be public (e.g. your house, friends/relatives' house, work), then change it to another photo (or remove the EXIF information if you know how to do that). Avoid photos with family that could be used to identify your family members. Click "edit cover photo" to change.

- * **Review your profile photos.** Your primary profile photo is always public. **As with the cover photo, minimally ensure this photo was not taken at a place that would reveal a location you don't want public, like your home.** The best course is to choose a photo that does not show your likeness or that of any of your family, an avatar or similar, instead.

- o To change it, click your profile photo, and then "Update Profile Picture." Select a new photo.

- o You also want to review your old profile photos. Click your profile photo again and then click "View profile picture."

- In the top right, there are three dots. Click them and then click "Edit Audience." This does not change who can see your photo (everyone), but does let you limit who can see likes and comments on it. **Set to Friends or Only Me.**

- **Click through your profile photos and change the audience on each one to Friends,** or delete them. These photos will be limited to only your friends.

Now, back to your main profile page. If you have a bio, you should probably delete it. **Next, click "Edit Profile."**

- Review and edit this information as you see fit.

- Scroll to the bottom and click "Edit your About Info."

- * **Work through each of the categories on the left (e.g. Work and Education, Places You've Lived, etc) and review the associated information in the right pane. Here's what you're looking to do:**

- o Remove any unnecessary information.

- o For the information you keep, check who it is shared with by click the three dots on the right. **At most, share with Friends.**

- o **Keeping your birthdate/year on your profile is a bad idea.** It can help someone steal your identity.

- * **Now, scroll down and review all of your friends. Remove any that you don't know, or that seem suspicious.** Don't be afraid to ask them questions only that person would know to verify they are who they claim to be.

LINKEDIN SETTINGS GUIDE

On a desktop/laptop, go to: <https://www.linkedin.com/psettings/account>

ACCOUNT SETTINGS TAB

Under the **Login and Security** heading:

- **Review/update login settings.** Update/change your email address, set a new password with your password manager, and check devices that remember your password (review this list and remove any old, unused, or unknown devices).
- **Enable two-step verification.** Click "change" to the right of "two-step verification," and **turn it on.** Follow steps to select "authenticator app," as your method and add the authentication token to your app of choice. Next, get the recovery codes and save them someplace safe (either encrypted or offline).

Under the **Site Preferences** heading:

- **Review: Name, Location, and Industry.** Click "change" to the right of "Name, Location, and Industry." All of this information is generally public (you can control this some, see later settings).

Under **Partners and Services** heading:

- **Review connected accounts and services.** Recommend you unlink all accounts and services (Microsoft, third party, Twitter).

Under the **Account Management** heading:

- **Consider hibernating or deleting your account.** Unlike Facebook, only about a quarter of Americans have a Facebook account. You don't have to have one. If you're happy with your current job, in this section you can either hibernate or delete your account. Hibernation is a good option if you expect to look for a new job in the future, but not right now. If you choose to hibernate or delete your account, you're done. If not, continue.

Next, click the **Privacy Tab** at the top of the page.

PRIVACY TAB

Under the "**How others see your profile and network information**" heading:

- * **Edit: your Public Profile.** Click "edit your Public Profile." If your profile is public, this view will show you what *anyone searching on the internet* will see when they click your profile.
 - o **Click "edit your custom URL" in the top right.** This is the web address for your profile. **Remove any reference to your name;** it's best just to type a string of 6-12 random numbers and letters. Click the "Save" button when you're done.
 - o Before editing content, go to down to the "Edit Visibility" header on the right. **Recommend:** set "your profile's public visibility to off."
 - If you did that, you're done with this section, if not: set profile photo to "only first degree connections," and then scroll down to toggle off headline, summary, articles and activity, current experience, past experience, education, and groups to your comfort level (recommend all toggled off: remember, this is for *anyone* to see).
 - Return to privacy settings tab.
- **Edit: who can see your email address.** Click "who can see your email address." **Recommend:** set to "Only visible to me." If people want to contact you, they can message you in LinkedIn.
 - o Set toggle to "No." Set the "allow your connections to download your email in their data export?" toggle to no.
- **Edit: who can see your connections.** Click "who can see your connections." **Recommend:** set to "only you." Your other option is "your connections," but this is a huge group – people connected to you (1st), people connected to them (2nd), and people connected to them (3rd). LinkedIn is a big game of six degrees of Kevin Beacon. Your connections reveal a lot about who you are, what you do, who your family is, etc.
- **Edit: viewers of this profile also viewed.** **Recommend:** set to "No."
- **Edit: who can see your last name.** **Recommend:** last initial (second option). Your connections (all 1st, 2nd, and 3rd level connections) will still see your full name, but people completely unconnected to you will only see your last initial.
- * **Edit: representing your organization and interests.** Set to "No."
- * **Edit: profile visibility off LinkedIn.** Set to "No."
- * **Edit: Microsoft Word.** Set to "No."

Under the **"How others see your LinkedIn activity"** heading:

- **Edit: Profile/Story Viewing Options.** For these two settings, choose either "private profile characteristics" or "private mode." If you're a LinkedIn subscriber, the clear option is "private mode" because you can remain anonymous and still see who has viewed your profile. If you're not a subscriber and select "private mode," you lose the ability to see who has viewed your profile.
- **Edit: Manage active status.** Recommend: Your connections or no one. This can be used to monitor your habits and activity.
- **Review: (1) Share job changes, education changes, and work anniversaries from profile; (2) Notify connections when you're in the news; and (3) Mentions or tags by others.** Recommend: set all to "No."

Under the **"how LinkedIn uses your data"** heading:

- **Edit: Manage who can discover your profile from your email address.** Recommend: "Nobody." Your email is effectively public because of data leaks and thefts, and can be used by scammers and others to pretend to be a connection and connect with you.
- **Edit: Manage who can discover your profile from your phone number.** Recommend: "Nobody." For the same reasons as your email.
- *** Review: Sync Contacts.** Review and remove any synced contacts — do not sync contacts. Syncing contacts gives Microsoft a metric ton of information on your friends, family and colleagues and their addresses, phone numbers, and emails.
- *** Review: Sync Calendar.** Remove any synced calendars, and do not sync calendars. Like contacts, this is a lot of information to give away about you and your activities.
- **Review: Salary data on LinkedIn.** Recommend: delete any salary data.
- **Clear: Search history.**
- **Review: Personal demographic information.** Recommend: click "remove all information."
- *** Edit: Social, economic, and workplace research.** Toggle off.

Review all items under the **"Job seeking preferences"** and the **"Blocking and hiding"** headings.

Next, click the **Ads Tab** at the top of the page.

ADS

**** Review every item on this page and set all of them to "no" or unclick all boxes. ****

When you're done, click the **Communications Tab** at the top of the page.

COMMUNICATIONS

Review every item on this page based on your preferences and comfort levels.

For "Research Invites," set to "No."

FINALLY, REVIEW YOUR PROFILE

Go to your profile by clicking your profile picture in the top right of the screen, and then "View Profile."

- *** Review your profile photo.** **Ensure this photo was not taken at a place that would reveal a location you don't want public, like your home.** Or, if you know how, you can use a tool to remove the EXIF data.
- Review and edit your profile with an eye to what you're willing/comfortable sharing. Think about how a criminal or other adversary might see and use this information as you review it.