



# TAKE CONTROL OF Your Facebook Security & Privacy

Facebook is huge. Almost a quarter of the world population is considered active on the platform. It has changed the way people communicate, and for better or worse it has become a major part of the lives of so many people. Whether you love, hate, or are just indifferent about Facebook (no judgement here), it's worth configuring and locking down your account to control what others can see about you.

We'd be willing to wager that most readers of this document understand that, for the most part, if you want to control your privacy online, you need to limit what you put online. At least, that's a big part of privacy. Unfortunately, with mobile devices, location sharing, and machine learning, services are able to collect a lot of information that you aren't directly giving it voluntarily.

In this document, we are going to discuss how you can take control of your personal information. We will also break down Facebook's privacy settings to help you gain control over your personal identity while using the social network.

Presented By: Directive | Revised: November 2019

## **Statement of Confidentiality**

What follows is simply the result of analysis and a review of solutions available. The contents of this document are provided "AS IS". This information could contain technical inaccuracies, typographical errors and out-of-date information. This document may be updated or changed without notice at any time. Information presented is believed to be from reliable research and sources and no representations are made by Directive as to another cited parties' information for accuracy or completeness.

Copyright © 2019 Directive. All rights reserved.

## About Directive

Directive serves as a resource for businesses who need support for their information technology, as well as a consultant who can assist them in managing it. As a result, we can help you improve each and every aspect of your business operations with advanced IT solutions. For a selection of our core services, see the rest of this page, or visit our website at <https://www.directive.com>.



### MANAGED IT SERVICES

To help reduce amount of time and resources lost due to technology related issues and downtime, our managed IT services take a proactive approach to technology maintenance. By remotely monitoring your network and data constantly, potential issues can be detected and remedied before they result in an interruption of daily operations.



### SECURITY SOLUTIONS

Businesses of all sizes and in every industry need to respect the need for comprehensive security. We offer a wide scope of services to protect your company and its data, including content filtering, antivirus and antimalware, firewall, phish testing, and many others. We'll keep you secure so you can focus on being productive.



### NETWORK CARE

Your business' network is its backbone, supporting operations and allowing different parts to stay communicative. Controlling how files and folders can be accessed and shared, and setting policies that dictate how the network can be used are key functions. An organized and efficient network is key to your success - we can help you get there.



### BUSINESS CONTINUITY

Business continuity planning is about more than just backing up your company's data. It's about your company's ability to recover from a catastrophic event. Directive offers reliable data backup solutions and the expertise to assist you with your business continuity and disaster recovery preparations.



### EMAIL HOSTING + PROTECTION

Whether you'd prefer to have us host your email, or you want to keep it in-house, we offer solutions to help keep your business safe and its email managed. With spam protection and email filtering on your side, you can be confident that your email is working for your business.



### TECHNOLOGY SUPPORT

For businesses that rely on technology, a critical element of an IT strategy is finding the right tech support. From implementation and configuration to after hours end-user technology emergencies, we are there to assist you with your technology needs whenever you or your employees need them.

## MAKING SENSE OF FACEBOOK'S PRIVACY SETTINGS

# “Should I Just Quit Facebook?”

You don't need to jump ship, but you do need to control what information is shared.

We're going to leave the ultimate decision up to you, but regardless of how you feel about social media and Facebook in general, there are plenty of pros and cons to being an active Facebook user. Let's go over them and the history of Facebook regarding user privacy.

### What are the Pros?

There's the obvious stuff - Facebook is a great platform to communicate with friends, colleagues, and family. Facebook Messenger is a pretty feature-rich instant messenger with group chat capabilities. Many businesses and organizations use Facebook as one of their main platforms to communicate with clients and customers, either through Facebook pages or Facebook groups. Plus, businesses can run fairly cost-effective targeted advertisements through Facebook with better accuracy than most other ad platforms.

### What are the Downsides?

Privacy. All of the information we punch into Facebook goes to Facebook. It helps Facebook learn about us. Facebook watches how you interact with posts and what you scroll through. After hours and hours of this, year after year, like after like, Facebook really starts to figure out who you are, maybe even more than you think you are letting on. It uses this information to help target ads and curate the posts you see in your timeline.

As we've seen historically, Facebook has also done some pretty shady things with our personal data. Without going too deep into any particular topic, here are a few quick privacy-related examples to refresh your memory:

Facebook had a feature where companies could track purchases by Facebook users and notify their friends of what had been bought, often without consent.

2007

Facebook had a bug that exposed the email addresses and phone numbers of 6 million Facebook users.

2013

It was revealed that Facebook had a massive 50 million user data breach, knew about it, but did nothing until it started to make them look bad.

2015

Facebook was charged by the FTC for allowing private information to be made public without warning. Facebook was essentially letting third-parties access user information without consent.

2011

Facebook decided that Facebook apps shouldn't have access to all the private user data that they want, meaning it was pretty much a free-for-all until then. This leads up to the infamous Cambridge Analytica scandal.

2014

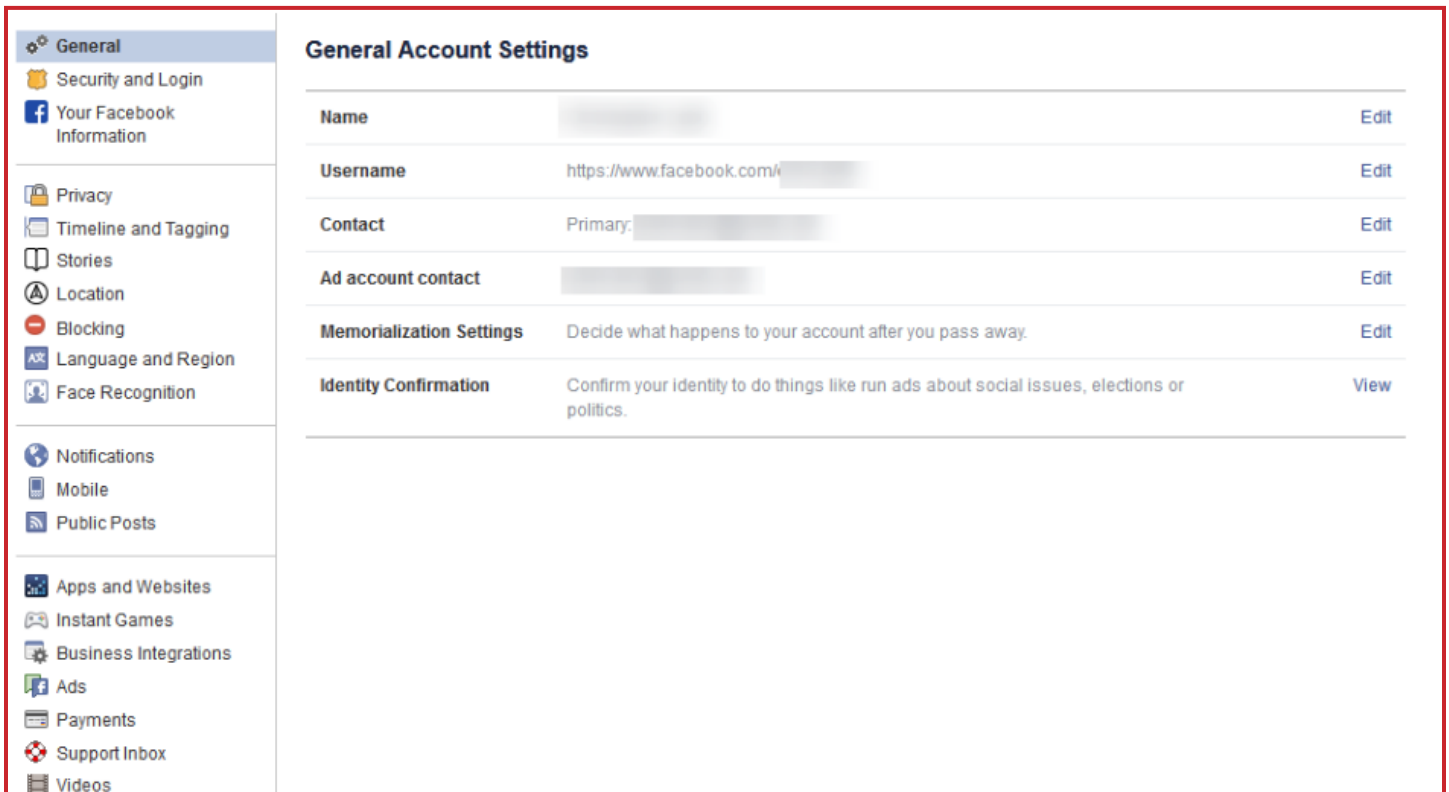
Facebook ran an experiment to see if they could make users depressed by delivering depressing content. It turned out that yes, they can.

2018

## TAKE CONTROL OVER YOUR FACEBOOK SECURITY SETTINGS AND 2FA

# Making Sense of Facebook's Security and Privacy Options

Let's log in and take a look at how we can gain control over your information. Log in to **Facebook.com** and click the little down arrow on the top right. Then click **Settings**. If you ever get lost during this guide, you can get back to where you need to be by coming back to this point. We're going to spend quite a bit of time here. Let's start with a little general housekeeping.



The screenshot shows the Facebook 'General Account Settings' page. On the left is a navigation menu with categories: General (selected), Security and Login, Your Facebook Information, Privacy, Timeline and Tagging, Stories, Location, Blocking, Language and Region, Face Recognition, Notifications, Mobile, Public Posts, Apps and Websites, Instant Games, Business Integrations, Ads, Payments, Support Inbox, and Videos. The main content area is titled 'General Account Settings' and contains the following settings:

Setting Name	Value	Action
Name	[Redacted]	Edit
Username	https://www.facebook.com/[Redacted]	Edit
Contact	Primary: [Redacted]	Edit
Ad account contact	[Redacted]	Edit
Memorialization Settings	Decide what happens to your account after you pass away.	Edit
Identity Confirmation	Confirm your identity to do things like run ads about social issues, elections or politics.	View

## Verify the General Account Settings are Correct

Make sure you own and control all of the email accounts tied to your Facebook account. This is just good practice for all of your online accounts - every ecommerce site, every social network, every service you sign up for - if any account is tied to an older email address that you don't check anymore or don't have access to, you'll have a hard time getting back into the account if something were to happen. the outage experience downtime, and cannot perform their jobs as effectively without their working equipment.

## Security & Login: Find Out Where You've Logged into Facebook

Click **Security and Login** on the right.

First, Facebook will show you all of the recent devices logged into your account. It will show you approximately where geographically the device was, the browser used, and when it was last active. Obviously, if you see something suspicious here, you should **change your password** right away (the options for that are directly below). Additionally, you can click the **3-dot icon** on the right next to any login and log that device out.

The screenshot displays the Facebook 'Security and Login' settings page. On the left is a navigation menu with options like General, Security and Login, Your Facebook Information, Privacy, Timeline and Tagging, Stories, Location, Blocking, Language and Region, Face Recognition, Notifications, Mobile, Public Posts, Apps and Websites, Instant Games, Business Integrations, Ads, Payments, Support Inbox, and Videos. The main content area is titled 'Security and Login' and features a section 'Where You're Logged In'. This section lists several active sessions:

- Windows PC** (Firefox) - Active now
- Samsung Galaxy Note 10+** (Messenger) - 3 hours ago
- Windows PC** (Firefox) - 15 hours ago
- Samsung Galaxy Note 10+** (Facebook app) - 16 hours ago
- Windows PC** (Firefox) - October 10 at 10:44 AM
- Samsung Galaxy Note 8** (Messenger) - September 4 at 9:43 AM
- Samsung Galaxy Note 8** (Facebook app) - September 4 at 9:43 AM

At the bottom of the list, there is a 'See Less' link and a 'Log Out Of All Sessions' button.

## If It's Been a While, Take a Moment to Change Your Password

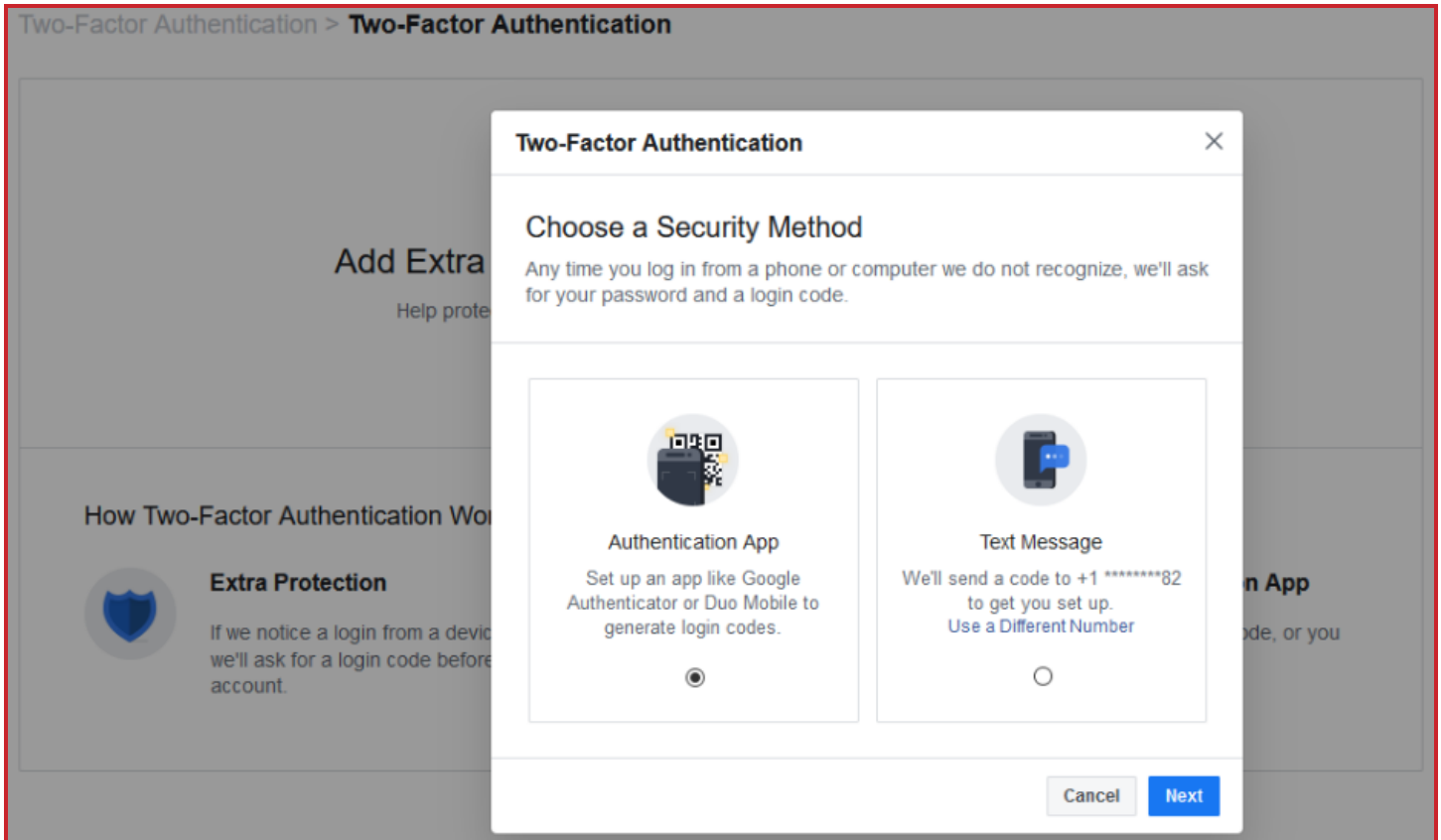
While we're here, it wouldn't hurt to create a new Facebook password. You should consider doing this across all of your accounts regularly (at least every 6-to-12 months, but more often for critical accounts like your bank and email).

Just as a reminder, you can get there by clicking on the **down arrow** on the top right of Facebook, going to **Settings**, and clicking **Security and Login**.

**MAKE SURE TO NEVER USE THE SAME PASSWORD  
FOR TWO DIFFERENT ACCOUNTS ONLINE.**

## Enable Two-Factor Authentication

Directly below the password options are settings for two-factor authentication (2fa). This adds additional security to your account in case your password gets stolen. Select **Use two-factor authentication** and click **edit**. Facebook will take you to a page that walks you through setting it up. From there, click **Get Started**. You will be given two Security Methods. We recommend understanding both options before choosing one.



### Option 1 - Authentication App

This lets you use a third-party authentication app like Google Authenticator or Duo Mobile to generate the login code. This is a little bit more secure, but it does require you to have access to the mobile device that the authenticator app is installed on.

### Option 2 - Text Message

Facebook will send a code to your phone number. You'll want to make sure your phone number is accurate and can receive texts. This isn't as secure as using an authentication app, because it is technically possible for a hacker to intercept your text messages, but it's definitely better than nothing.

*Continue reading to learn how to set these up!*

## How to Set Up Two-Factor Authentication

Depending on the option you choose, Facebook will walk you through the next steps to verify and enable two-factor.

### **Authentication App:**

To set this up, open the **Google Authenticator** or **Duo Authenticator** or **LastPass Authenticator** on your mobile device. It makes the most sense to use the authenticator app that you use for other accounts, but if you don't have one, and you have a Google account, use Google Authenticator.

Then, from Facebook on your computer (see the above screenshot), select **Authentication App** and click **Next**.

Facebook will give you a square barcode called a QR code to scan. In your **Authenticator App**, add a new account (typically there is a + icon to tap) and scan the QR code. Once scanned, the app will generate a 6-digit number to use. Facebook will ask for a **Confirmation Code**. Type in the 6-digit number and you'll be set.

### **Text Message:**

Setting this up is simple, once you choose Text Message and click **Next**, Facebook will text you a code. Type that code into Facebook and you'll be set.

Depending on the option you choose, Facebook will walk you through the next steps to verify and enable two-factor.

## Add a Backup

Once two-factor authentication is set up, Facebook will give you an option to **Add a Backup**. If you choose to set up two-factor with an **Authentication App** then Facebook will allow you to set **Text Message** 2FA as a backup, and vice versa. It's not a bad idea to set up the other method as well, just in case. Lots of online accounts offer 2FA, and some of them (like Google, Microsoft, and Amazon) will give you backup options as a way of giving you an alternative way in in case your primary method of 2FA isn't available. Let's say you were using text messages for your 2FA and you get forced into a situation to change your cell phone number. You'd be in a difficult situation if you didn't have a backup option.

Facebook also lets you grab **Recovery Codes** (by the way, Google does this too, so if you have a Google account or use Gmail, it's a good idea to get all of this set up over there as well).

Back on the [Two-Factor Settings page](#), under **Add a Backup**, there is an option for **Recovery Codes**. Click **Setup**, and Facebook will pop up a window telling you about recovery codes, and click **Get Codes**. Facebook will give you 10 recovery codes that you can use in an emergency to get back into your account. These codes basically work as one-off 2FA codes, so you'll need to know your Facebook password and one of these 10 codes to get back into your account.

Remember, these recovery codes can only be used once. You can request 10 new codes at any time by going back to the **Two-Factor Settings** page, but you can't use the same code twice. It's also very important that you keep them in a safe place, but not make it clear to anybody what they are. Write them down on an index card with a big "F" written in the corner and keep it in your wallet.


## Setting Up Extra Security

Back in the **Security and Login** area of **Facebook's Settings**, scroll down to **Setting Up Extra Security**.

This area allows you to get alerts sent to you when a new device or browser is used to log into Facebook. It's pretty straight forward, you can even define additional email addresses if you want. You can also have those notifications sent to you via Facebook Messenger, SMS, or as a Facebook notification. We definitely recommend at least having it set up to email you.

**Setting Up Extra Security**

---

 **Get alerts about unrecognized logins** Close

**On** • We'll let you know if anyone logs in from a device or browser you don't usually use

---

Get an alert when anyone logs into your account from an unrecognized device or browser.

**f Notifications**

Get notifications

Don't get notifications

---

**Messenger**

Get notifications

Don't get notifications

---

**✉ Email**

Email login alerts to [redacted]

Don't get email alerts

---

[Add another email or mobile number](#)

---

[Save Changes](#)

Below that option, you can choose **3 to 5 Friends** to Contact if you get locked out. If you set this option up, make sure you only put in people you can trust. Also, it might be a good idea to only add a contact who you feel takes their security seriously. Otherwise, turn off this option.

We realize this has been a lot, but by setting up 2FA and controlling who and what device has access to your Facebook account, you are taking a big step in controlling your online identity. We encourage you to take time to review all of your social media, bank accounts, online shopping accounts, email accounts, and other services you are signed up with to prevent unauthorized access.



## MAKING SENSE OF FACEBOOK'S PRIVACY SETTINGS

# Facebook's Privacy Options

If you are like many, you might not love everything that has to do with Facebook, but you probably do benefit from having a massive social platform that you can use to communicate with friends, family, fans, clients, and prospects. Privacy is more important than ever.

Let's log in and take a look at how we can gain control over your information.

**Log in** to your Facebook account on your desktop. On the top right, there is a small **down arrow**. Click it and go to **settings**.

From there, click **Privacy**.

Privacy Settings and Tools			
<b>Your Activity</b>	Who can see your future posts?	Public	<a href="#">Edit</a>
	Review all your posts and things you're tagged in		<a href="#">Use Activity Log</a>
	Limit the audience for posts you've shared with friends of friends or Public?		<a href="#">Limit Past Posts</a>
<b>How People Find and Contact You</b>	Who can send you friend requests?	Everyone	<a href="#">Edit</a>
	Who can see your friends list?	Only me	<a href="#">Edit</a>
	Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.		
	Who can look you up using the email address you provided?	Friends	<a href="#">Edit</a>
	Who can look you up using the phone number you provided?	Everyone	<a href="#">Edit</a>
	Do you want search engines outside of Facebook to link to your profile?	Yes	<a href="#">Edit</a>

## Breaking Down Facebook Privacy Options

Facebook generally lets you set privacy options for a few different groups of people:

<b>Public</b>	Anyone can see this information, even if they are not Facebook friends, and even if they aren't signed into Facebook. In theory, this means search engines and other online entities can see your information as well.
<b>Friends</b>	Only people you are Facebook friends with can see the information.
<b>Friends Except...</b>	Filter out some friends or specific user-created groups from seeing certain information. For example, you can create a group called "employees" and put your employees who have added you on Facebook in it. Then you can lock down some content and forbid those friends from seeing it.
<b>Only Me</b>	None of your friends can see the information, and that it is strictly between you and Facebook. Still, don't share anything that you wouldn't want getting out there.

You can also choose specific Facebook friends who can see certain content, if you wish. Let's take a look at each option. Fortunately, Facebook does a pretty good job explaining these in plain English.

- ⇒ **Who can see your future posts?** This option allows you to set the default privacy setting on future Facebook posts. You can always manually change it on a per-post basis, this just sets the standard.
- ⇒ **Review all your posts and things you're tagged in.** If you click **Use Activity Log** you'll be able to scroll through your entire timeline and manage permissions of your previous posts. This is also where you'll find posts that you've been tagged in from friends.
- ⇒ **Limit the audience for posts you've shared with friends of friends or Public?** If you click **Limit Past Posts**, you can quickly lock down all of your past posts by changing them from **Public** to **Friends** only. Careful though, Facebook doesn't let you revert this very easily. If you decide you wanted your posts to be public, you'd need to go through them by hand to change the privacy settings.
- ⇒ **Who can see your friends list?** This is definitely one you should lock down. You don't need everyone in the world seeing who your Facebook contact list is. Setting this to **Only me** will keep that information private from Facebook Users.
- ⇒ **Who can send you friend requests?** You can either set this to **Everyone** or **Friends of friends**. This is one of the few cases where it probably doesn't hurt to leave it set to everyone.
- ⇒ **Who can look you up using the email address you provided?** You can decide if the general public can find you on Facebook via your email address. For most of us, we probably don't need that, so locking this down to **Friends** or **Only me** is probably a good call.
- ⇒ **Who can look you up using the phone number you provided?** Again, you probably don't need the public using this, so setting it to **Friends** or **Only me** will give you more control over your identity.
- ⇒ **Do you want search engines outside of Facebook to link to your profile?** Although Facebook doesn't really control how Google, Bing, and the other search engines work, you can dissuade your Facebook profile from being indexed by the search engines with this option. If your personal brand is important and you want people to be able to find your profile when Googling your name, keep this set to **Yes**.

## Control How Others Interact with Your Facebook Profile

Still under Facebook's Settings area, click Timeline and Tagging on the left. These settings let you choose whether or not others can post content to your timeline, and who can see this content.

Timeline and Tagging Settings			
Timeline	Who can post on your timeline?	Only me	Edit
	Who can see what others post on your timeline?	Friends	Edit
	Allow post sharing to stories?	On	Edit
	Hide comments containing certain words from your timeline	Off	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Friends	Edit
	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	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	Friends	Edit
Review	Review posts you're tagged in before the post appears on your timeline?	Off	Edit
	Review tags people add to your posts before the tags appear on Facebook?	Off	Edit

Let's take a look at each option regarding your Facebook timeline and the Facebook tagging feature. Facebook breaks these down pretty well.

- ⇒ **Who can post on your timeline?** You can choose **Friends** or lock it down to **Only me** so nobody can post to your profile.
- ⇒ **Who can see what others post on your timeline?** If you choose **Friends** for the above option, you should definitely lock down who can see it. Setting this to **Friends** will limit who sees your friend's post, and **Only me** will prevent a Facebook friend from hurting your reputation.
- ⇒ **Allow others to share your posts to their stories?** Facebook breaks this one out pretty clearly - if you post something publicly, do you want friends to be able to share it? This is how good content gets shared around Facebook, so you may want to leave this **enabled**.
- ⇒ **Who can see posts you're tagged in on your timeline?** Friends can tag you in a Facebook post, but you can control who can see it. If you want to hide your personal life or have some rambunctious Facebook friends, you may want to set this to **Only me** or at least lock it down to just **Friends**.
- ⇒ **Review posts you're tagged in before the post appears on your timeline?** You'll be able to vet the content you are tagged in, but remember, if Jack tags you in a post, all of Jack's friends will be able to see it before you get a chance to review it. You should definitely set this to **on**.
- ⇒ **Review tags people add to your posts before the tags appear on Facebook?** Definitely set this to **on**.

## Managing Public Posts

Still in the **Settings page** of Facebook, click **Public Posts** on the left-hand side.

### Who Can Follow Me

Followers are sort of like one-sided friends. It might be somebody who sent you a friend request that you chose to ignore. If you want the general public to be able to see your posts and follow you, set the option to **Public**. If you want to only allow **friends** to see your post, change this setting to Friends.

### Public Post Comments

This is where you choose who can comment on your public posts. You can lock this down to just Friends, or Friends of Friends if you wanted a bit of a wider berth.

### Public Profile Info

Some parts of your Facebook profile are available for the general public (your name and profile image, for example). Do you want just anyone to be able to comment on your profile image or other biographical information? Locking this down to **Friends** or **Friends of Friends** is usually a good idea.

## Want Facebook to Know Where You Are?

Facebook can track your location history. They don't share that data to your friends, but... honestly we couldn't find a whole lot of reasons why Facebook wants to collect this data other than to serve you targeted ads. We hope that's all it is used for, but it's better to be safe.

From the Facebook **Settings page**, click **Location** on the left-hand side. You can **View your Location History** to see what Facebook already knows about you. In order to turn the feature off, you need to log into the mobile app.

### *On Your Facebook App:*

1. Tap the **3-bar hamburger icon** on the top right. Then scroll down and tap **Settings & Privacy**, and then **Privacy Shortcuts**. You'll find a whole new area with security settings and documentation on how Facebook lets you control your identity.
  2. Look for **Manage your location settings** which should be on screen without needing to scroll down.
  3. Tap **Location Access** and turn off **Location History**. Tap **Location Services** and turn "Use Location" to off.
  4. You'll also see an option for Background Location. You might need to go back a step on your phone to get to it. You'll want to turn that off as well, if it isn't already.
  5. **Let's go ahead and delete your location history too.\*** Again, from the Facebook mobile app, tap the **3-bar hamburger icon** on the top right. Then scroll down to **Settings & Privacy** and then **Privacy Shortcuts**.
  6. Choose **Manage your location settings** and tap **View Your Location History**.
  7. Facebook will prompt you for your password.
  8. Tap the **3-dot** settings icon on the top right.
  9. Tap **Delete all location history**.
- \*Keep in mind, if you post a photo that tags your location, or check in to a public place, you might be granting Facebook access to your location data again!**

## Apps and Websites That You've Connected to Facebook

One last thing - some websites and applications will let you log in via Facebook. For example, **Spotify** will let you create an account with your Facebook account, and the dating app **Tinder** will use your Facebook profile image for your Tinder profile.

This is fine, if you've locked down your Facebook account and are protecting your login with two-factor authentication and a secure password, and you are controlling the data that you give to Facebook, then these other applications aren't going to be much of an issue.

However, it is worth auditing the applications and websites you've given access to your Facebook. If you don't use something anymore, or you don't recognize something, it's best to revoke its access.

Google has a similar feature. You can access it by logging in to your Google account and go to their [security settings](#).



### *For Facebook, From Your Computer:*

1. Tap Click the down arrow icon on the top right and choose settings.
2. Then click Apps and Websites on the left-hand side.
3. Review the Active apps and remove any that you no longer need.
4. Be sure to check the Expired tab on the top as well. These apps are still technically attached to your account, but they haven't been used recently.
5. You can click on each app and website to see what information is shared.

## Was That Overwhelming?

Protecting your data and your identity is important. If you are looking to protect your business, don't hesitate to reach out to us. Give us a call at **607.433.2200** or visit us on the web at <https://www.directive.com/>

# Focus On Your Business Not Your Technology

*Interested in a **FREE** Managed IT Consultation?*

Visit: <https://www.directive.com/free-it-consultation>  
or call us at **888-546-4384** now!