GUIDE TO CYBER SECURITY FOR PROTECTIVE MOTHERS

Retaining Access to Critical Accounts:
Tip Sheet

Escaping an abusive intimate partner is an incredibly difficult emotional and physical process. The tip sheet below is focused on taking some of the guesswork out of securing digital accounts abusers may maintain access to after a victim has already escaped. Accounts that an abuser can use to continually harass or stalk their victim.

Remember, these abusers typically have **low levels of sophistication but high levels of intimate knowledge**. That means they know what you would choose for a password.

So, let's get started by answering a few questions — and making a list of:

- Social media accounts both the victim and the abuser share;
- Bank accounts, food delivery services, such as UberEats, car sharing services, such as Lyft, and shopping, such as Amazon, that store a victim's current address.
- Critical services – email, cell phone provider (AT&T, Verizon, or T-Mobile), social media services — the victim uses.

(**Important note:** This cheat sheet doesn't contain instructions for how to rotate credentials for — or access to — IoT devices. But, **it's important that you do so for devices both the victim and the abuser have access to**.)

Once we have that inventory, **let's begin taking control of those accounts step-by-step, treating them as if the abuser still has access**:

Step 1: Change The Locks

If a victim isn't already using one, now is an excellent time to start using a password manager like LastPass. Here are the steps to start:

1) **Install Browser Extension (Chrome; Firefox)**
2) **Create an Account**
3) **Add Recovery Cell Phone Number**
4) **Sign-Into Browser Extension** •••|
5) **Add LastPass to Your Phone**

Once a victim is using a password manager, now is the time to rotate your passwords. You'll want to use your password manager to generate strong passwords for your accounts.

Here are some direct links to security pages across popular accounts:

"Change password..."

- **Router: Change SSID (WiFi Network Name) and Admin Password**
- **Google:** Click the "change password" button on Google's **guide**.
- **Yahoo:** Sign in to the **security page** to change your password.
- **Outlook:** Follow the steps in Microsoft's **guide**.
- **Facebook:** Go to the **Security & Login** page to change your password.
- **Linkedin:** Visit the **Change Password** page.
- **Instagram:** Visit the **Change Password** page.
- **Twitter:** Visit **the Password settings page**.
- **Apple: Change Password** on Apple's account page.
- **Amazon: 'Login & Security'** on 'Account' page
- **Venmo: 'Change Password'**
- **Paypal: "Update"** your "**Password"**

ProTip: LastPass isn't your only option; the **Freedom of the Press Foundation** has a handy guide on **choosing a password manager.**

Step 2: Close the door.

By now, you've regained access to your accounts, but an abuser may — unbeknownst to their victim — still may be logged in. Many services allow you to sign out every logged-in device, and you'll want to do that right away.

"Log out of ALL active sessions..."

- **Google:** The first pulldown allows you to sign out other sessions at **Security checkup**.
- **Yahoo:** Look through **Account Activity** and click sign out on all the other sessions.
- **Twitter:** Click the button that says "Log out all other sessions" at **Active Sessions.**
- **Instagram:** Click each session and then click "Log out" on **Login Activity.**

- **Facebook:** Click “See More” and then “Log out of all sessions” at the bottom of the expanded list at **Security and Login**.
- **LinkedIn:** Check **Where You’re Signed In** and click sign out on all other sessions.
- **Apple:** Remove unknown devices on the **Devices page**.
- **Amazon:** Manage and deregister devices on this **‘Devices’** page.
- **Venmo:** See “**Sessions**”
- **Paypal: (Make sure to change your password)**

Next, check your **recovery email** and **phone number** in a victim’s accounts to ensure that they’ll have access to both, and remove any that they don’t recognize.

“Settings…”

- **Google:** Check the “Ways we can verify it's you” in the **Security** dashboard.
- **Yahoo:** Click on the recovery email or phone number in the **Security dashboard to** change.
- **Twitter:** Check “Your Account” in **Settings.**
- **Instagram:** Check the **Settings** for your account.
- **Facebook:** Check your **mobile settings** (**to ensure that your information is correct**) and **account settings.**
- **LinkedIn:** Visit the **security dashboard** and check the email addresses and phone number sections.
- **Apple:** See your **Account** page.
- **Amazon:** See “**Login & Security**”
- **Venmo:** **Check “Email Address” and “Phone Number”**
- **Paypal:** Check your **“Phone Number(s)” and “Email”**

After you’ve done that, you’ll want to look carefully at the list of services that have access to your account. It is pretty standard for apps like slack to have access to your google account, for example, but now is the time to clean out any services that you don’t actively use. Visit each of the following and remove any connected services you don’t recognize.

“Apps with access…”

- **Google**: Check Third-Party **apps with access.**
- **Twitter**: See **Connected Apps**
- **Instagram**: Check **Apps and Websites**
- **Facebook:** Check **Apps and Websites**
- **LinkedIn:** Check **Permitted Services**
- **Apple:** Check **Manage apps and websites.**
- **Venmo:** See “**Apps Linked**” at the bottom of the page.

- **Paypal:** Manage and Remove **‘Permissions’** you’ve given to separate accounts

Step 3: Add another lock

You’ll want to make sure that you’re using two-factor authentication for your accounts as well. While you may have set your phone number as an authentication method, it is much safer to use a two-factor functionality in Lastpass or a dedicated app like **Google Authenticator** (**Android**, **iOS**) or **Authy** (**Android**, **iOS**, **Desktop**).

“Multi-Factor Authentication…”

- **Google:** Go to the two-step **verification page.** Click the blue-button in the upper right.
- **Yahoo:** Follow **Yahoo's** guide.
- **Outlook:** Follow Microsoft’s **Guide**
- **LastPass, Personal Account:** Follow the **Two-Factor Authentication Instructions**
- **Facebook:** Visit **Security Settings** to enable
- **Instagram:** Visit **Two-Factor Authentication** in your browser, not the app.
- **LinkedIn:** Enable **Two-Factor Authentication**
- **Twitter:** Enable ‘Password Reset Protect' in **Security Settings**//Enable 'Password Reset Protect')
- **Apple:** Visit the **Security** page to enable two factor
- **Amazon: ‘Login & Security’** on ‘Account’ page
- **Venmo:** Relies on SMS, One-Time-Codes sent by Default. (**Make sure to take the extra step securing your cell phone account, below, to ensure access.**)
- **Paypal: “Update”** your “**Two-Factor-Authentication”** setting

As an extra step, you can also prevent abusers from cloning your number by locking down your SIM card so no one can take over your phone number except you. **Several critical services like Facebook allow users to reset their passwords using a registered phone number.**

These are instructions for how to add 'extra security to your carrier's account, **most often in the form of a four-digit PIN, to make it exceedingly difficult to port your number:**

- **Verizon** (NumberLock)
- **AT&T Instructions**
- **Sprint Instructions**
- **T-Mobile Instructions**
- **Cricket Instructions**
- **GoogleFi: Gmail/Google Account** Add 2FA and Strong Unique Password

FYI: If you're having trouble — just call your carrier!

While you're at it, **Facebook** and **Google** have checkups that will walk you through the most common settings related to your privacy and security. **It's always good to check them every once in a while to make sure your comfortable with these settings.**

Additional Resources:

- **HackBlossom's EXCELLENT Guide on 'DIY Cybersecurity for Domestic Violence'**
- **Stop Stalkerware (Resources by Country)**
- **Apple: Device and Data Access When Personal Safety is at Risk**

Supplemental iOS Advice:

Now that we've taken steps to secure a victim's accounts. It's important to review that person's devices — particularly their smartphones — for lingering software meant to spy on them.

As a first step, disable location tracking on a victim's smartphone. That means turning off native apps, such as iOS' 'Find My Phone,' and going through settings that share a device's location with social media accounts, such as Facebook.

Next, consider turning off unknown callers on your iPhone in **Settings > Phone > Silence Unknown Callers.** (This will mute phone calls from numbers that you don't have saved in your phone, and can become annoying.)

Consider downloading this tool — which costs $3 in the Apple App Store and contains supplemental guides and a full iOS Security Toolkit

> **iVerify, Trail of Bits (Download it inside the App Store)**

This piece of that toolkit is especially helpful for redacting additional location information that accompanies iPhone photos:

> ***iVerify MetaData Extension Instructions (Stripping Data From iPhone Photos)*:**
>
> *iVerify includes a share extension that strips metadata from your photos and videos. Photos and videos taken on your device include additional data such as the time and date, GPS location, camera specs, and other details you may want to remove before sharing.*
>
> *Learn to strip metadata*
>
> 1) *Choose an image or video in the Photos app that you'd like to share.*
> 2) *Press the Share button.*
> 3) *Scroll to the bottom and choose Share without Metadata from the actions list.*
> 4) *Metadata will be removed and you will be prompted to share the photo again, now with its metadata stripped.*
>
> *Note: The extension only strips metadata that has a potential impact to privacy. Some metadata remains, such as photo orientation.*

Privacy Settings:
Tip Sheet

Privacy Settings: Facebook
Privacy Settings: Google
Privacy Settings: Instagram
Privacy Settings: Twitter
Privacy Settings: TikTok
Privacy Settings: LinkedIn
Privacy Settings: Venmo
Bonus: Setting Up A Second, Secure Phone Number

Once an abuser no longer has access to their victim's account, we may want to make that victim is generally more difficult to find over social media — either by obscuring their personal profiles or filling real profiles with fake information.

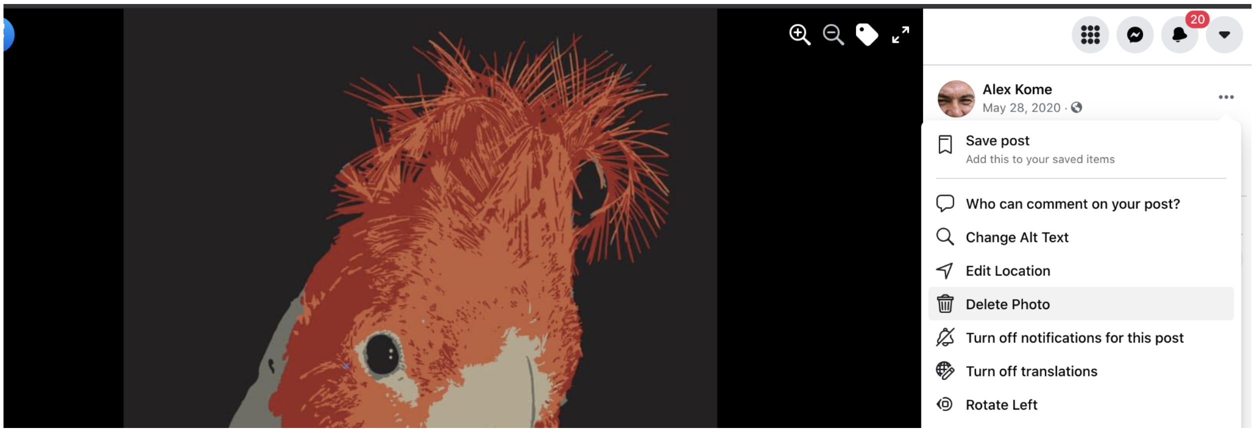
Please be aware that services frequently change their settings and new features, some of the settings belo may have changed.

Facebook:

The social network makes it difficult to keep your photos and personal information private. But, we want to take the guesswork out of that process, so stop whatever you're doing, take about 15-minutes out of your day, and follow along:

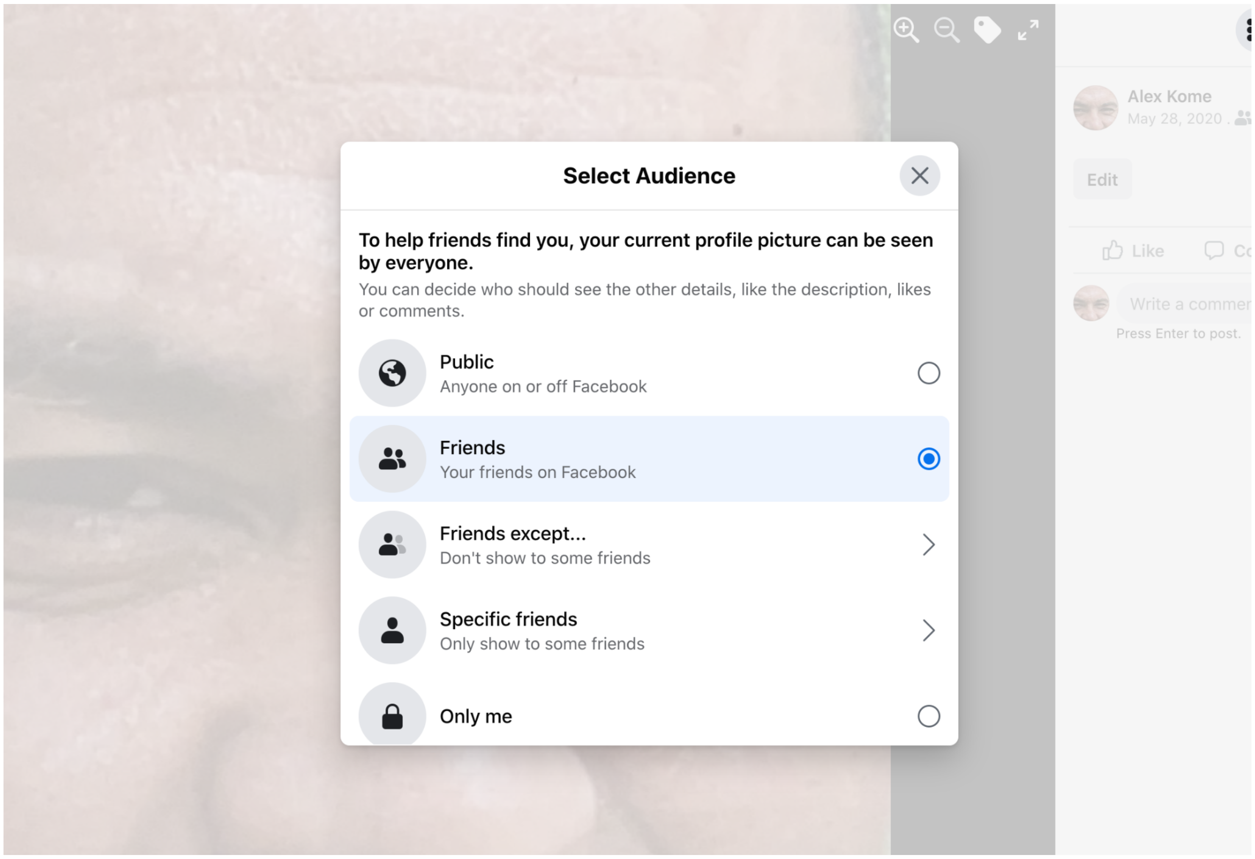
Step 1: Kill your cover photos; they're always public

If you're uncomfortable with people you don't know seeing the comments and likes left by your friends, delete all of the photos in your cover photo album. They're only allowed to be public — 🌍.



Then, go through your albums, photos, and posts, click on the 👥 icon to the right of the date the content was published to choose who can see it.

Finally, make sure your profile photo is only viewable by your friends 👥 , this will stop others from discovering people close to you through your comments and likes.



Select Audience

To help friends find you, your current profile picture can be seen by everyone.

You can decide who should see the other details, like the description, likes or comments.

○ Public — Anyone on or off Facebook

● Friends — Your friends on Facebook

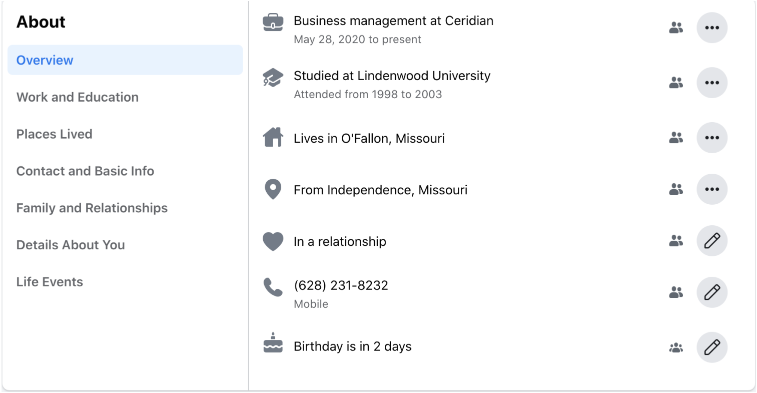
Friends except... — Don't show to some friends

Specific friends — Only show to some friends

○ Only me

Step 2: Suppress your 'About' section

Make the “**About**” information on the Facebook profile page private or for “**Friends**” only



Business management at Ceridian
May 28, 2020 to present

Studied at Lindenwood University
Attended from 1998 to 2003

Lives in O'Fallon, Missouri

From Independence, Missouri

In a relationship

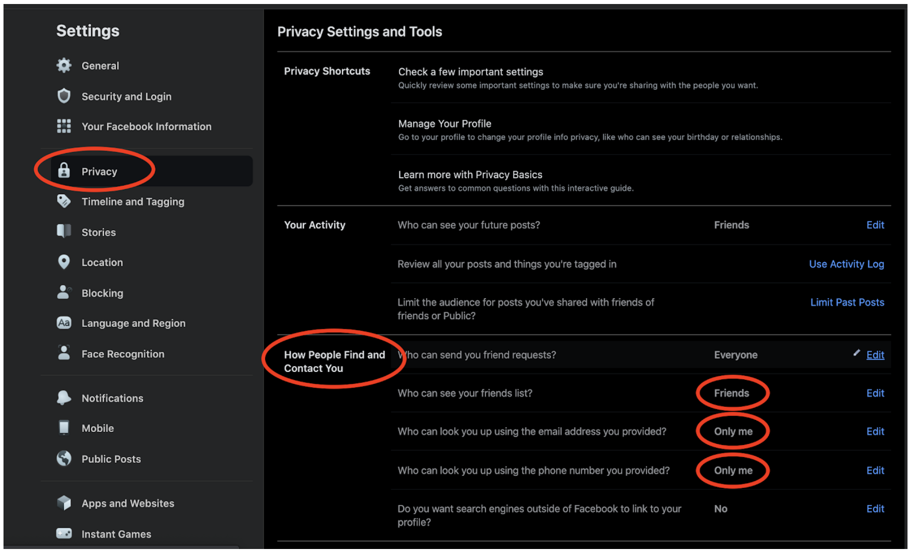
(628) 231-8232
Mobile

Birthday is in 2 days

Click through Overview, Work and Education, Places Lived, Contact and Basic Info, Family and Relationships, Details About You, and Life Events to make sure you’re not exposing any of that information publicly: 🌐.

Step 3: Limit your past posts and make your friends list private

Sign in to your account and visit **Privacy Settings** to ensure you're comfortable with who can send you friend requests; who can see your friend's lists; and who can look you up using the email address you registered with your account, among other choices. Also make sure to click “**Limit Past Posts**” to erase old posts that may still be public.



Privacy Settings and Tools

Privacy Shortcuts

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

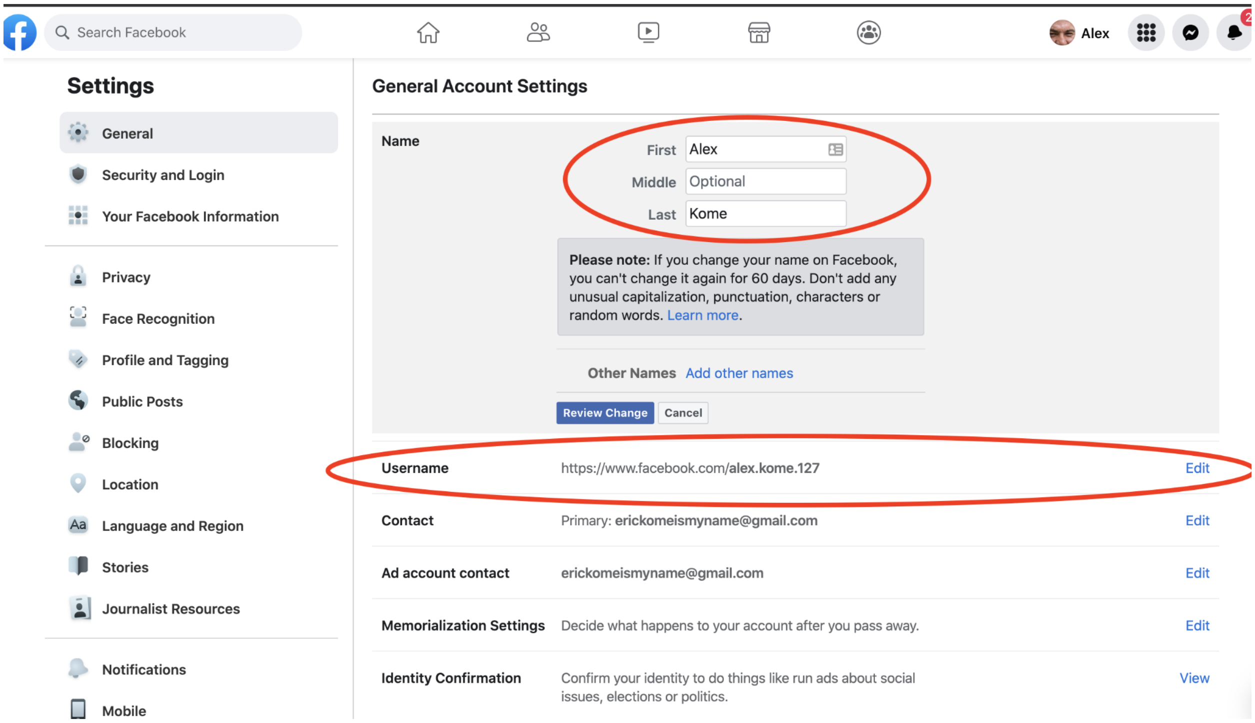
Manage Your Profile
Go to your profile to change your profile info privacy, like who can see your birthday or relationships.

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

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How People Find and Contact You	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list?	Friends	Edit
	Who can look you up using the email address you provided?	Only me	Edit
	Who can look you up using the phone number you provided?	Only me	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

Step 4: Change your real (and user) name

Changing your name and your username on your personal profile makes it more difficult for people outside your immediate community to find you.



General Account Settings

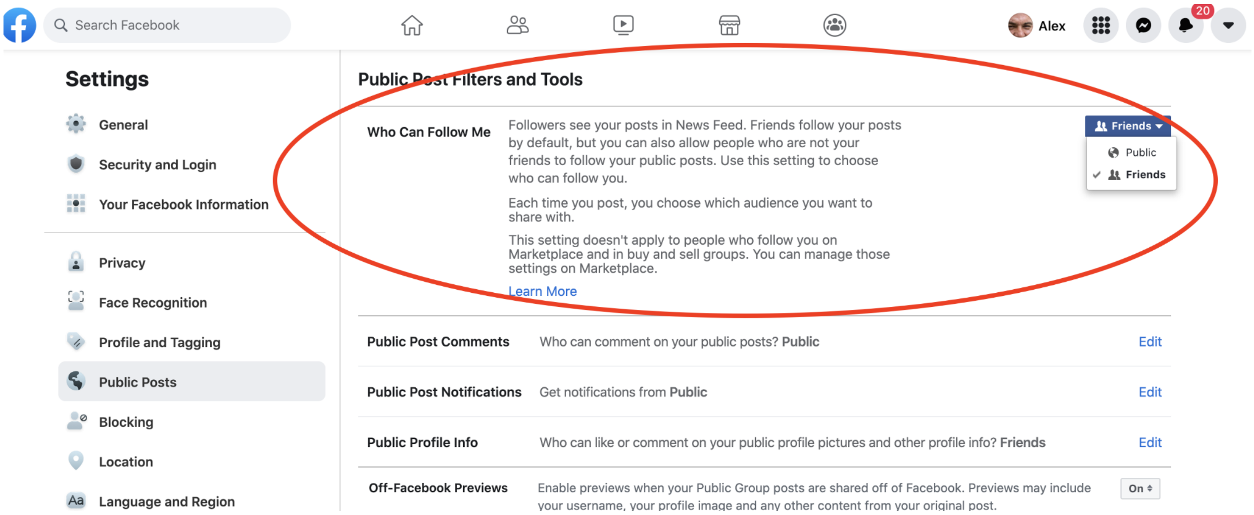
Name — First: Alex; Middle: Optional; Last: Kome

Please note: If you change your name on Facebook, you can't change it again for 60 days. Don't add any unusual capitalization, punctuation, characters or random words. Learn more.

Other Names: Add other names

Username	https://www.facebook.com/alex.kome.127	Edit
Contact	Primary: erickomeismyname@gmail.com	Edit
Ad account contact	erickomeismyname@gmail.com	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

Additionally, turn off people's ability to "**Follow**" you:



Public Post Filters and Tools

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

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

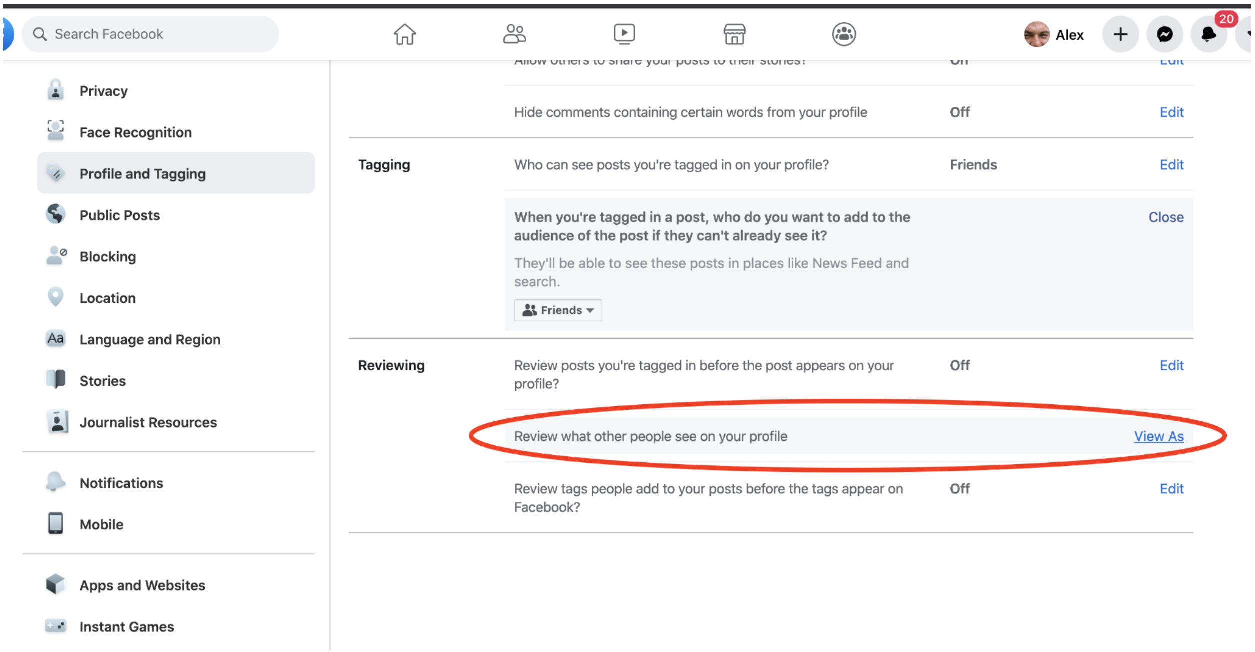
This setting doesn't apply to people who follow you on Marketplace and in buy and sell groups. You can manage those settings on Marketplace.

Learn More

Public Post Comments	Who can comment on your public posts? Public	Edit
Public Post Notifications	Get notifications from Public	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit
Off-Facebook Previews	Enable previews when your Public Group posts are shared off of Facebook. Previews may include your username, your profile image and any other content from your original post.	On

Step 5: Have a friend — who you aren't Facebook friends with — look at your profile to see what's still public.

After all this, you should go and view your account using the "**Review what other people see on your profile**," feature



Allow others to share your posts to their stories? Off Edit

Hide comments containing certain words from your profile Off Edit

Tagging

Who can see posts you're tagged in on your profile? 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? Close

They'll be able to see these posts in places like News Feed and search.

Friends

Reviewing

Review posts you're tagged in before the post appears on your profile? Off Edit

Review what other people see on your profile View As

Review tags people add to your posts before the tags appear on Facebook? Off Edit

Another way to ensure the most personal parts of your profile aren't exposed to the public is to have a friend (preferably, someone who you aren't friends with on Facebook) look at your now privacy-hardened profile to check the efficacy of your work.

Google

Three quick tips:

- **Make sure you're not sharing your location with anyone you don't know:** https://myaccount.google.com/people-and-sharing
- **Remove your personal information from your profile:** https://myaccount.google.com/profile
- **Turn off view history in google docs, sheets, and slides:** https://support.google.com/docs/answer/7378739?visit_id=637535159404412820-908897253&p=docs_analytics&rd=1

Instagram:

Keeping your Instagram private is an all-or-nothing activity. Set your account to private from the Instagram app on your Android or iOS device:

- Go to your profile, then tap ⚙ .
- Tap Settings.
- Tap Privacy > Account Privacy.
- Tap next to Private Account to make your account private.

Set your account to private on your computer or mobile browser. Go to instagram.com on your computer or mobile browser:

- Click ⚙ , then click ☰.
- Click Privacy and Security.
- Below Account Privacy, click to check the box next to Private Account.

But, if you want to go a step further to obscure your identity, take a tip from privacy-conscious high schoolers and decouple your real name from the pictures you post by creating a finsta — short for a fake Instagram profile.

Twitter:

- Go to Twitter's **Privacy Settings**.
- Uncheck the "**Add Location Information to my Tweets**" feature
- "**Delete all location information**," from your existing tweets.
- Go to Twitter's **Security Settings** and check the "Password reset protect," feature. Twitter's account reset flow displays partial phone numbers and email addresses, by default, that can help an abuser verify a victim's current contact information.

Going a step further, generally, be mindful not to interact with brands on Twitter in public. Only DM them, directly. And, if you want to make your account private, check the "Protect your Tweets" option within Twitter's **Privacy Settings**.

TikTok:

Even though you can access TikTok in the browser, you'll need to open the smartphone app to make your account private:

1. Go to your profile page and select the three-dot icon — ••• — in the top-right corner.
2. Select Privacy and Safety.
3. There, toggle the switch for "Private Account."

You can also select who can send you comments and direct messages, as well as who can duet one of your videos. Additionally, you can limit your contact with strangers by using the "Friends" setting.

LinkedIn:

The goal of changing your LinkedIn profile is to either redact a victim's current job and location, or throw off an abuser and make them think their victim is living somewhere they aren't:

- View the users' profile once logged in.
- **Click** ✎ at the top right of the first section of the users' profile
- **Delete the user's current location,** or change the location to a location where the user doesn't actually live.
- **Click** ✎ to the left of each individual job — and **redact the users' job history to obscure their current location.**

Venmo:

You can access Venmo's privacy settings from your smartphone:

- Open iOS or Android application
- Go to **Settings**
- **Tap on 'Privacy'**
- Make all transactions '**Private**' and "**visible to sender and recipient only**"
- Underneath **'More**'; Click '**Friends List**' and then select **'Private'.**

You can equally do this in the browser, here

Bonus: Setting Up a Second, Secure Phone Number

We've had our cell phone numbers — at least many of us have — since high school. And those numbers can be used to pivot to discover more pieces of information about us, including our home addresses and relatives' names through social media sites and people search engines.

With that in mind, you should consider setting up a way to contact you that doesn't involve a 10-digit-number.

1) **Register a separate phone number.** This can be done for free over services like **Google Voice** — which can be paired with a throwaway email account; a desk phone; a phone number from an online calling service, such as Skype; or a cheap prepaid SIM card.

2) **Register your new number with Signal.** We like Signal, because it contains a cryptographic feature called Forward-Perfect Secrecy, which protects past sessions against future compromises of keys or passwords.

That means that if anyone happens to get a hold of your Signal account and re-registers it on a new device, they won't be able to view past messages. (If you already have a Signal account on an existing device and are unwilling to delete it, you may have to purchase a new device to just house that Signal account — read the "**Picking a Device for Your Second Signal Number**" on **this Intercept article**.)

3) **Add a Registration Lock.** You can do that on your device through these settings:
   iPhone users: *Click Settings > Privacy > Registration Lock > Enabled*
   Android users: *Click Settings > Privacy > Registration Lock > Enabled*

   This will stop anyone from registering your throw-a-way number with Signal, even if you lose access to your Google Voice, Skype, or prepaid SIM number.

Remember, don't give out your real cell phone number to people you don't know!