IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE
COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS
TWELFTH EDITION, MARCH 2021

BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

HOW TO USE THIS GUIDE

The Identity Awareness, Protection, and Management (IAPM) Guide is a comprehensive resource to help you protect your privacy and secure your identity data online.

The IAPM Guide is divided into chapters detailing key privacy considerations on popular online services, mobile apps, and consumer devices available in the market today. Each section provides you with tools, recommendations, and step-by-step guides to implement settings that maximize your security. The guide is updated periodically.

While some of the chapters in the IAPM Guide deal with technical issues, they do not require a technical background to follow.

The U.S. Department of Defense creates this guide to provide recommendations for readers to keep their identities private and secure online. Please note the information presented here is subject to change.

HIGHLIGHTS FROM THE TWELFTH EDITION!

- A newly consolidated Online Dating chapter
- A newly revamped Video Communications chapter
- Contents updated with the latest mobile operating systems:
  - iOS (v. 14.3) and Android (v. 11)
- Updated chapters, including:
  - Facebook
  - Instagram
  - LinkedIn
  - TikTok
  - Twitter
  - Google Account
  - Messaging Apps
  - Photo Sharing & Storage
  - EXIF Data Removal
  - Video Communications
  - Smartphones
  - Traveling with Smartphones
  - Identity Theft Prevention
  - Securing Home Wi-Fi Network

USEFUL LINKS AND RESOURCES

A Parent's Guide to Internet Safety	https://www.fbi.gov/resources/parents
The Balance: Identity Theft 101	https://www.thebalance.com/identity-theft-basics-4073614
Privacy Rights Clearinghouse	http://www.privacyrights.org/privacy-basics
HTTPS Everywhere	https://www.eff.org/https-everywhere
Securing Your Web Browser	https://www.us-cert.gov/publications/securing-your-web-browser

DISCLAIMER:

TABLE OF CONTENTS

WHY IS IDENTITY PROTECTION A CONCERN?

YOUR DATA IS EVERYWHERE

Everything you do creates a stream of data

PERSONAL	FINANCIAL	BIOMETRIC	BEHAVIORAL
• Name • Birth Date • Work, Education, and Address History • Family and Friends • Likes and Interests	• Credit Cards • Bank Accounts • Digital Wallets • Online Payments • Purchase history	• Face Recognition • Voice Recognition • Fitness Tracker Data • Device Authentication • DNA Analysis	• Browsing History • Social Media • Relationships • Interactions with Devices and Sensors • Location Tracking

YOUR DATA IS VALUABLE

• The 21st-century world is based on trading personal data, instead of money, for convenience or utility.

• Online companies collect your data to develop targeted ads and sell them. Digital advertising was worth $365 billion worldwide as of March, 2020.[1]

• On the criminal side, personal data is worth a lot of money. Personally Identifiable Information (PII) sells for $1-1,000 dollars on the Dark Web, where criminals sell it in bulk.[2]

When you trade your data for a service, you are not the customer.

YOU ARE THE PRODUCT

YOUR DATA IS UNPROTECTED

• The United States has no centralized, formal legal structure to protect your data.

Data Cannot Be Truly Deleted Once It's Out There

• Companies can and do share data with each other, so you don't know who might take over your data. 91% of users install mobile apps without reading the Terms of Service, which often allow for data sharing.[3]

• Biometric data is everywhere. Even a picture of your face in the wrong hands could put you at risk.

• Hacks are constant. Your data could have already been stolen.

YOUR DATA CAN BE DANGEROUS

• Any single piece of data can be innocuous, but it becomes a three-dimensional digital profile when tied to other sources. Advertising firms, public records companies, or cyber criminals can gather and link bits and pieces of your personal data together.

• Identity theft can waste time and hurt consumers financially.

• Oversharing online can lead to personal embarrassment or professional consequences.

• Online behavior can reveal patterns of life that can lead to physical risk in the real world.

WHAT CAN YOU DO ABOUT IT?

EDUCATE YOURSELF

- 74% of people are unaware that Facebook develops profiles of users' interests.[4]
- Knowing the risks puts you ahead of most people.
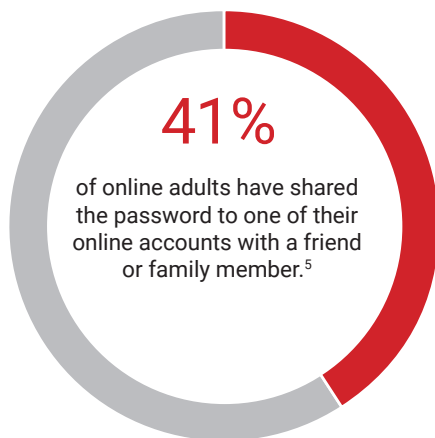- The IAPM Guide is a great start. Look at the Table of Contents page for more information sources.

REVIEW TERMS OF SERVICES
and stay up-to-date with privacy updates and changes.

PROTECT YOURSELF

- Use caution before agreeing to share your information. Think before you click.
- Learn how to tell the legitimate from the illegitimate.

- When in doubt, opt out.
- Threats to your identity constantly change. Monitor your credit and online accounts, and keep your software and devices up-to-date.

Be proactive about identity security. Only share PII with people or companies you trust.

41% of online adults have shared the password to one of their online accounts with a friend or family member.[5]

39% of online adults say that they use the same (or very similar) passwords for many of their online accounts.[6]

25% of online adults admit that they use less secure passwords, because simpler passwords are easier to re-member than more complex ones.[7]

STRIKE THE RIGHT BALANCE

DON'T PANIC!
Your identity and privacy can still be protected.

- Social media and apps are useful, but make sure you use them safely.
- Before using a product or sending your PII to someone, ask yourself if it is providing enough of a benefit to be worth the risk.
- If your identity has already been stolen, you still have time to react and recover.
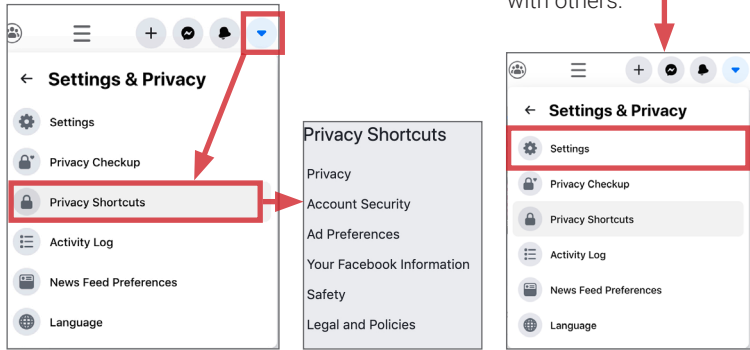
FACEBOOK

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure you recognize all the logged-in devices and locations.
- Remember that even if you restrict your data from public view, Facebook still has access to your data and may share it with third parties.

MAXIMIZING YOUR FACEBOOK PRIVACY

Facebook provides shortcuts to privacy settings that limit what others can see in your profile.

From the top drop-down menu on your computer, navigate to **Settings & Privacy > Privacy Shortcuts** to change your basic privacy.

For more extensive and granular control, go to **Settings**. Click through each tab to control how your personal information is shared with others.

RECOMMENDED SETTINGS
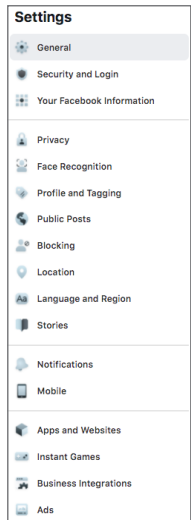
The (1) Security and Login, (2) Your Facebook Information, (3) Privacy, (4) Face Recognition, (5) Profile and Tagging, (6) Public Posts, (7) Blocking, (8) Location, (9) Stories, (10) Ads, and (11) Apps and Websites tabs contain settings for concealing personal information. Use the settings displayed below to maximize your security online. Facebook interactions (e.g., likes, posts) have been used to behaviorally profile individuals. Minimize the amount of personal information you share by limiting your interactions.

1 The **Security and Login** tab contains settings to protect your login credentials, monitor attempted and successful logins, and recover your account in the event of a lockout. Use **Where You're Logged In** to monitor login activity and end inactive sessions. Navigate to **Setting Up Extra Security > Get alerts about unrecognized logins** and **turn ON** alerts.

2 Use the **Your Facebook Information** tab to view, transfer, or download your data, and to deactivate or delete your account. Under **Off-Facebook Activity**, navigate to **Manage Your Off-Facebook Activity**, **Clear History**, and **Manage Future Activity** to control how Facebook tracks and shares your information outside of its platform. This section also contains shortcuts to your **Activity Log** and an informative **Managing Your Information** tab addressing common Facebook and Instagram data management topics.
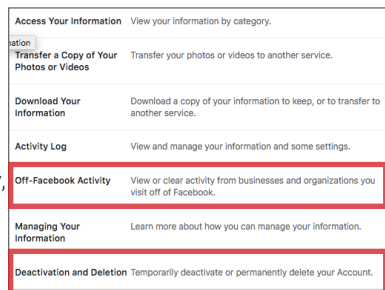
3 Use the **Privacy** tab to control who can search for you, contact you, and see your activity. Restrict sharing settings throughout. Under **Your Activity > Use Activity Log**, review past posts individually and limit the audiences for each entry. Use **Limit Past Posts** to retroactively change the settings of all **Public** posts to a **Friends** only audience.
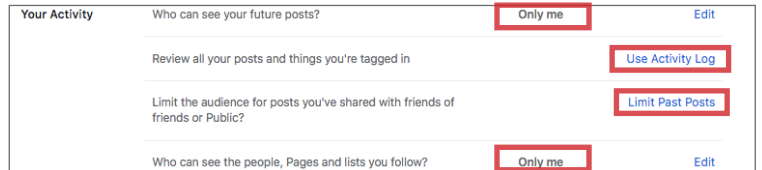
4 Under **Face Recognition Settings,** disable face recognition by setting this function to **No**. This prevents Facebook from searching and matching your face against all photos and videos uploaded to its database.

5 **Profile and Tagging** controls how others interact with your profile and posts. Restrict sharing settings and enable review capabilities throughout. Select **View As** to preview what others can see on your profile.
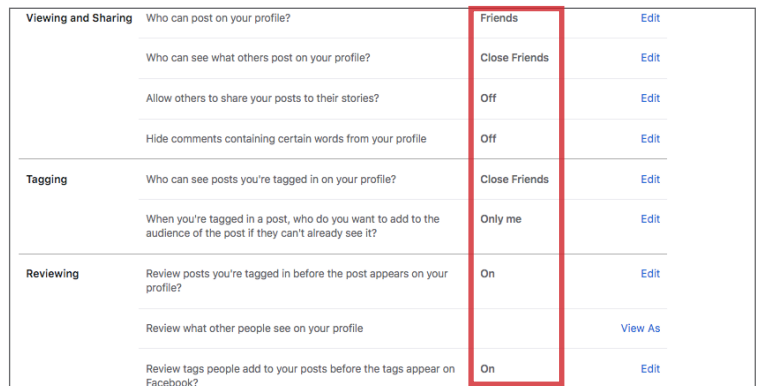
6 Followers are people outside your **Friends** network who interact with content you share publicly. Your **Public Posts** are streamed on their News Feeds. To prevent this, set **Who Can Follow Me** to **Friends**. Restrict **Public Post** and **Public Profile Info** settings as shown.
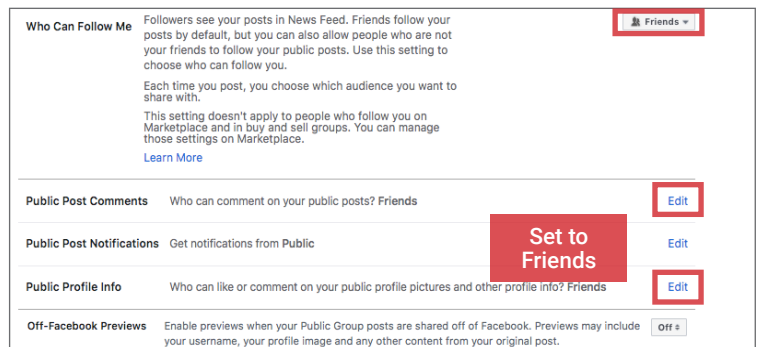
7 Use the **Blocking** tab to restrict select users from seeing your posts, and to block users, messages, invites, and pages.
Use **Block apps** to prevent apps from obtaining your non-public information through Facebook.
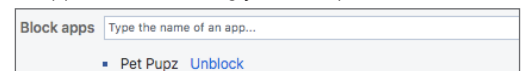
RECOMMENDED SETTINGS CONTINUED

8 Facebook uses your device to obtain and store location data. Under **Location Settings**, ensure your **Location History** is OFF. Use **View your Location History >** ⋯ **> Delete all Location History** to remove stored data.

> ⓘ Learn more
> ⚙ Location Settings
> 🗑 Delete this day
> 🗑 Delete all location history

9 Use the **Stories Settings** tab to limit other users from sharing your stories. Set both **Sharing Options** to **Don't allow.**

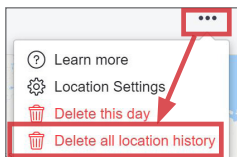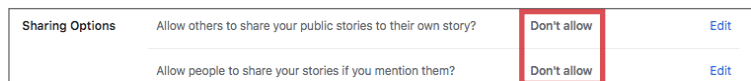| Sharing Options | Allow others to share your public stories to their own story? | Don't allow | Edit |
| | Allow people to share your stories if you mention them? | Don't allow | Edit |

10 Use the **Ads** tab to limit Facebook from tracking and using your data for advertising. Under **Ad settings > Manage Data Used to Show You Ads**, navigate through each section and **toggle OFF** data usage settings.

Under **Social Interactions**, restrict visibility to **Only Me.**

Ad Preferences
- 🎯 Advertisers
- 📋 Ad Topics
- ◉ Ad Settings

11 Using Facebook as a login method for other apps or sites enables those services to access your Facebook data. Use the **Apps and Websites** tab to examine and manage **Active, Expired,** and **Removed** permissions.

Limit unnecessary access.

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

Toggle OFF

FACEBOOK PROFILE PAGE

The Facebook profile page contains tabs that allow users to add information about themselves, view friend lists, and post text, photo, and video entries to their profiles. General audience settings reside within these tabs. Use the guidelines below to maximize your security while interacting with these features.
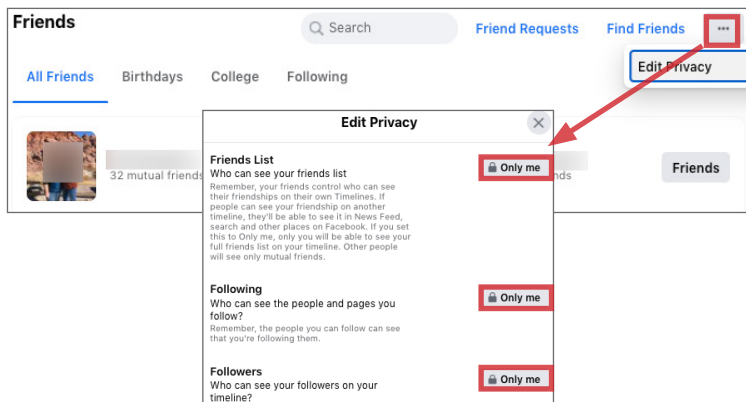
ABOUT

Avoid entering personal data in the **About** section unless required by Facebook. This information is mostly optional and contains data fields including **Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships, Details About You,** and **Life Events**. Use audience settings to change the mandatory fields to **Friends** or **Only Me**.
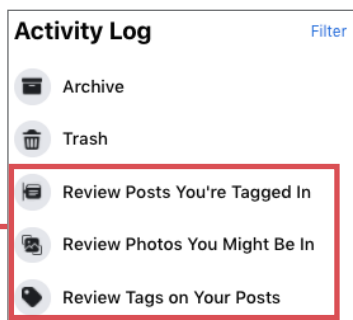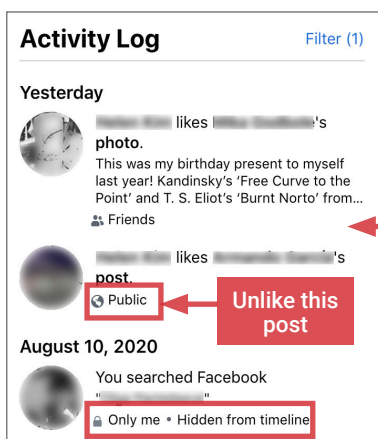
About
- Overview
- Work and Education
- Places Lived
- Contact and Basic Info
- Family and Relationships
- Details About You
- Life Events

Places Lived
Current City
Washington D.C.
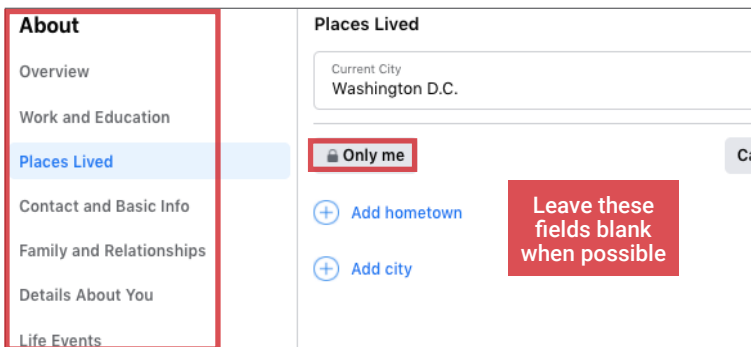
🔒 Only me

Leave these fields blank when possible

⊕ Add hometown
⊕ Add city

FRIENDS

The **Friends** tab provides a searchable list of all your Facebook Contacts. Click ⋯ **> Edit Privacy** to restrict access to your **Friend List** and **Following** settings; set these fields to **Friends** or **Only Me**.

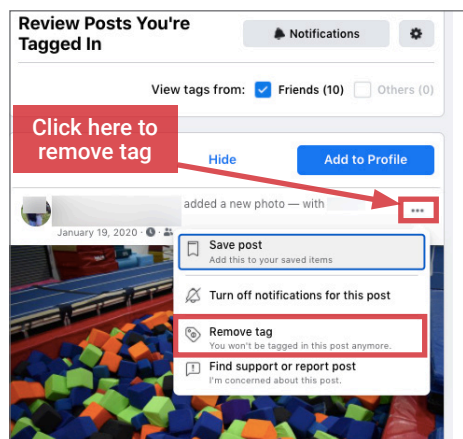**Friends** · Search · Friend Requests · Find Friends · ⋯
All Friends · Birthdays · College · Following
Edit Privacy
32 mutual friends · Friends

Edit Privacy
Friends List
Who can see your friends list
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. — 🔒 Only me

Following
Who can see the people and pages you follow?
Remember, the people you can follow can see that you're following them. — 🔒 Only me

Followers
Who can see your followers on your timeline? — 🔒 Only me

ACTIVITY LOG

Activity Log · Filter (1)

Yesterday
▢ likes ▢'s photo.
This was my birthday present to myself last year! Kandinsky's 'Free Curve to the Point' and T. S. Eliot's 'Burnt Norto' from...
👥 Friends

▢ likes ▢'s post.
🌐 Public — Unlike this post

August 10, 2020
You searched Facebook "▢"
🔒 Only me • Hidden from timeline

Activity Log · Filter
- 🗄 Archive
- 🗑 Trash
- ▤ Review Posts You're Tagged In
- ▤ Review Photos You Might Be In
- 🏷 Review Tags on Your Posts

The **Activity Log** (**Profile > ⋯ > Activity Log**) chronologically displays all your activities on Facebook, including your posts, photos and posts you are tagged in, your likes and reactions, comments on other people's posts, and searches.

Review your Activity Log weekly and **Remove** or **Hide** tags, likes, and comments from posts and photos you no longer want to be associated with on Facebook. **Always untag, unlike, or remove comments from other people's posts where the privacy setting is set to Public.**

Review Posts You're Tagged In · 🔔 Notifications · ⚙
View tags from: ☑ Friends (10) ☐ Others (0)

Click here to remove tag

Hide · Add to Profile
added a new photo — with
January 19, 2020 · ⋯
- 🔖 Save post — Add this to your saved items
- 🔕 Turn off notifications for this post
- 🏷 Remove tag — You won't be tagged in this post anymore.
- 🚩 Find support or report post — I'm concerned about this post.
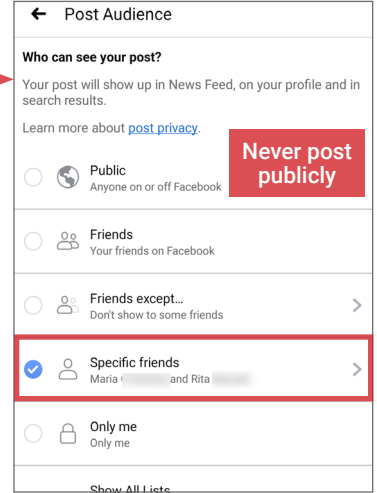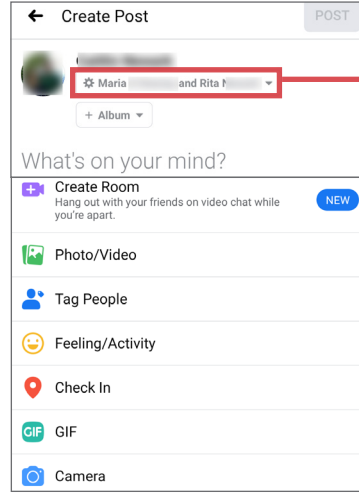
FACEBOOK

POSTING TO FACEBOOK

Facebook allows you to post a new status, upload photos, or check in to locations using the **What's on your mind?** prompt. The icons highlighted at the bottom of the prompt are shortcuts for adding further personal information to each post. Several shortcuts may pose a significant risk to your privacy and should be used sparingly. Follow the guidelines outlined in this section to avoid over-sharing your information.
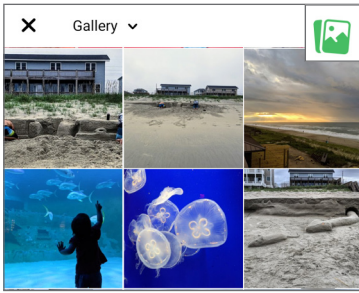
Add to your post

SELECTING YOUR PRIVACY

For every post, Facebook allows you to select the audience through the **Post Audience** tab beneath your name. For maximum privacy, select **Specific friends** with whom you would like to share your post. Never make your posts available to the public.

Create Post · POST

What's on your mind?

Create Room
Hang out with your friends on video chat while you're apart. · NEW

Photo/Video

Tag People

Feeling/Activity

Check In

GIF

Camera

Post Audience

Who can see your post?

Your post will show up in News Feed, on your profile and in search results.
Learn more about post privacy.

Never post publicly

Public
Anyone on or off Facebook

Friends
Your friends on Facebook

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

Specific friends
Maria and Rita

Only me
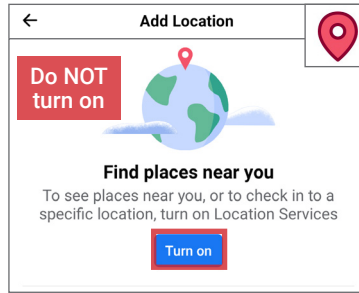Only me

Show All Lists

ADD PHOTOS/VIDEOS

Avoid posting photos to your Timeline. These photos can often be viewed from your contacts' profile pages and can be saved and shared without your knowledge or consent.

TAG PEOPLE
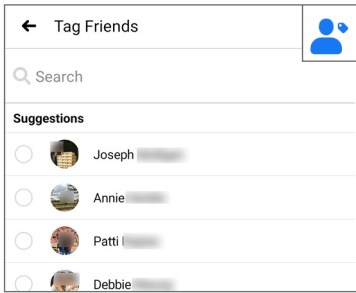
Tagging friends in posts extends the visibility of your post and profile to your friends' networks. Limit the number of tags you add to your Facebook posts.

CHECK IN

Add Location

Do NOT turn on

Find places near you
To see places near you, or to check in to a specific location, turn on Location Services.

Turn on

Never disclose your location in a Facebook post. Doing so allows Facebook to record your whereabouts and allows others to see when you are away from home.

LIVE VIDEO

If you choose to go live, limit your audience
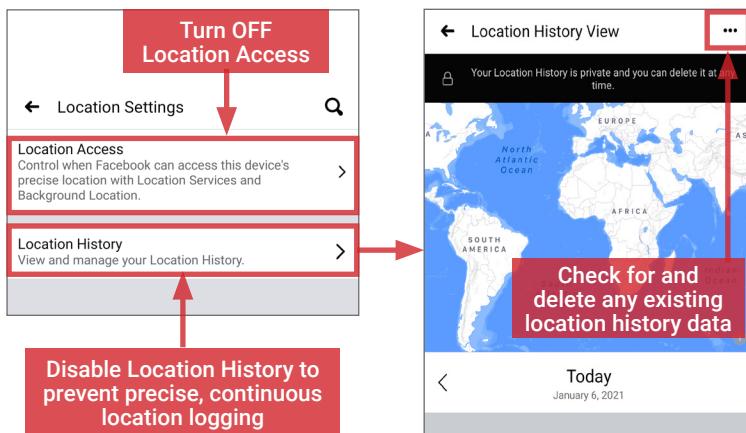
Tap to add a description

Start Live Video
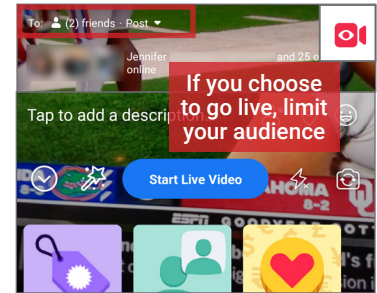
Avoid posting live videos. Videos are hard to vet for potentially harmful data and may lead to legal repercussions if others believe a video compromises their privacy.

LOCATION SETTINGS

When enabled, Facebook's location services tag location data to your posted or shared content, personalize your ads, and help you find nearby places of interest. Facebook uses these features to continually track your precise location and build a detailed map of your location history.

Avoid giving Facebook access to your location. Navigate to **Settings > Privacy > Location** to configure your location settings as shown below.
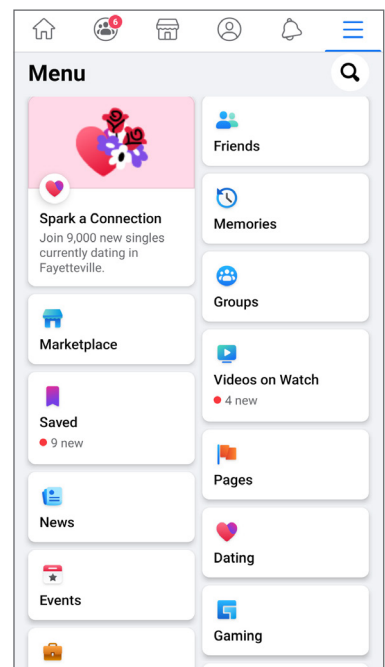
Turn OFF Location Access

Location Settings

Location Access
Control when Facebook can access this device's precise location with Location Services and Background Location.

Location History
View and manage your Location History.

Disable Location History to prevent precise, continuous location logging

Location History View

Your Location History is private and you can delete it at any time.

EUROPE
North Atlantic Ocean
AFRICA
SOUTH AMERICA
ASI...

Check for and delete any existing location history data

Today
January 6, 2021

ADDITIONAL FEATURES

In an effort to attract users and keep them engaged, Facebook offers several services within its platform, including **Dating, Events, Facebook Pay, Games, Jobs,** and **Marketplace**, among others. Facebook also offers several specialized apps such as **Facebook Gaming, Facebook Local,** and **Messenger**. Engaging with these Facebook services and apps increases the risk of your personal profile data being exposed to the public or unknown individuals. It also increases the likelihood that more personal data (e.g., your financial information for Facebook Pay) will be introduced to the Facebook environment.

Always check for and configure service-specific privacy and security settings if you decide to use these features.

Menu

Spark a Connection
Join 9,000 new singles currently dating in Fayetteville.

Marketplace

Saved · 9 new

News

Events

Friends

Memories

Groups

Videos on Watch · 4 new

Pages

Dating

Gaming

FACEBOOK MOBILE SETTINGS

Facebook Mobile settings closely resemble those of the website. Settings you implement carry across both the web and mobile app. From the ☰ icon in the navigation panel, select **Settings & Privacy > Settings**. Navigate tabs within the **Security**, **Privacy**, and **Ads** sections to implement settings shown below.

Security and Login

Where you're logged in — See all

Google Pixel 3 · Old Fields, WV, United States
Facebook app · Active now

Windows PC · Old Fields, WV, United States
Chrome · 5 minutes ago

Review your active sessions and devices frequently to spot unauthorized activity

Change password
It's a good idea to use a strong password that you're not using elsewhere

Turn ON

Setting Up Extra Security

Get alerts about unrecognized logins
We'll let you know if anyone logs in from a device or browser you don't usually use — On

Use two-factor authentication
Use your phone as an extra layer of security to keep other people from logging into your account. — On

Choose 3 to 5 friends to contact if you get locked out
Your trusted contacts can send you a URL from Facebook to...

Turn ON two-factor authentication

← **Privacy Settings**

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.

Your Activity

Who can see your future posts?
Only me

Limit who can see past posts

How People Find and Contact You

Who can look you up using the email address you provided?
Friends

Who can look you up using the phone number you provided?
Friends

Do you want search engines outside of Facebook to link to your profile?
No

Ads
Review how we use data to make the ads you see more relevant.

Ad Preferences
Control how data influences the ads you see, and learn more about how our ads work.

Privacy
Control who sees what you do on Facebook, and how data helps us personalize experiences.

Privacy Settings
Control who can see your posts and content, as well as who can search for you.

Face Recognition
Choose whether we recognize you in photos and videos.

Timeline and Tagging
Decide who can interact with you and your posts on Facebook.

Public Posts
Manage who can follow you, and who can comment on your public posts.

Blocking
Review people you've previously blocked.

Location
Manage your location settings.

Active Status
Show when you're active.

Data about your activity from partners
...based on your activity ...apps or offline

...reach you
...interests and other categories used to reach you

Audience-based advertising
Advertisers using your activity or information

Ads shown off of Facebook
How advertisers can reach you through off-Facebook ads

Social Interactions
Who can see your social interactions alongside ads?

Show when you're active

You'll still ...in ...you turn off the sett... or Facebook. You will... ...are active or recent...

Navigate to: Ad Preferences > Ad Settings > Manage Data Used to Show You Ads

Toggle all OFF

Toggle OFF in both Facebook Mobile & Messenger (if using) to ensure full effect

IPHONE SETTINGS

iPhones can be configured to control how your data is shared while you are using the Facebook app. From the iPhone's **Settings**, scroll down to the **Facebook** tab to review and adjust Facebook's access to your data, such as **Location**, **Photos**, **Camera**, and **Microphone**. **Toggle OFF** all permissions at all times unless required on a case-by-case basis.

Settings

- Drive
- **Facebook**
- Gmail
- Google
- Google Calendar
- Google Maps
- Google Photos
- Grubhub
- Hangouts
- HUJI
- Instagram

‹ Settings **Facebook**

ALLOW FACEBOOK TO ACCESS

- Location — Never ›
- Photos — Never ›
- Microphone
- Camera
- Siri & Search — Siri & Suggestions
- Notifications — Banners, Badges
- Background App Refresh
- Cellular Data

When in Low Power Mode, background app refresh is disabled.

FACEBOOK SETTINGS

Disable all permissions

Toggle OFF

ANDROID SETTINGS

Android phones can be configured to protect your personal data while you are using the Facebook app. Navigate to **Settings > Apps & notifications > See all apps > Facebook** and select **Permissions** to review and adjust Facebook's access to your data. **DENY** all permissions unless required for a specific, limited-time use case (e.g., uploading a photo).

← App info

Facebook

Open — Uninstall — Force stop

Notifications
~0 notifications per week

Permissions
No permissions granted

Storage & cache
325 MB used in internal storage

Mobile data & Wi-Fi
No data used

← App permissions

Facebook

ALLOWED
No permissions allowed

DENIED
- Calendar
- Camera
- Contacts
- Location

DENY access for each category

DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT

Deactivate Account
Deactivating your account is temporary. Your account will be disabled and your name and photos will be removed from most things you've shared. You'll be able to continue using Messenger.

Delete Account
Deleting your account is permanent. When you delete your Facebook account, you won't be able to retrieve the content or information you've shared on Facebook. Your Messenger and all of your messages will also be deleted.

Continue to Account Deletion

Deactivating a Facebook account removes your name and photos from posts that you have shared. Navigate to **Settings > Your Facebook Information > Account Ownership and Control > Deactivation and Deletion** and select **Deactivate Account** to temporarily suspend your account until the next login. Some information may remain visible, such as your name in someone else's friends list and messages you have exchanged with other users.

To delete your account, navigate to **Deactivation and Deletion**, as shown above. Select **Permanently Delete Account**, and follow the prompts to confirm. Deletion begins 30 days after request submission, at which point your data is no longer accessible to other users. Facebook may take up to 90 days to fully remove your shared content and may privately retain certain account information. To protect your long-term privacy, remember to **deactivate or delete your Facebook account and the Facebook app (if using) when the service is no longer needed**.

INSTAGRAM

INSTAGRAM - DO'S AND DON'TS

- Don't connect your Instagram account with your other SNS profiles (e.g., Facebook, Twitter, Tumblr). It increases your account's discoverability.
- Only accept follow requests from people you know and trust. Assume that ANYONE can see, save, and forward photos you post.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images that clearly show your face. Select pictures of yourself taken at a distance, at an angle, or wearing sunglasses.
- Don't embed your posts with hashtags (e.g., #foodie, #caturday), as hashtags increase your posts' visibility and make them searchable by others.
- Remember that even if you restrict your data from public view, Instagram still has access to your data and may share it with third parties.

OVERVIEW

Instagram is a photo-sharing app for uploading personal pictures and videos. With over 1 billion monthly active users in 2020, it is currently the sixth most popular social networking service (SNS) worldwide.[8,9]

Instagram's parent company is Facebook, which acquired the app in April 2012.[10] While they operate as two distinct platforms, the user can sync their activities and experience in both.

Instagram accounts can be either **public** or **private**. Content posted on public Instagram accounts is indexed by search engines and can be viewed by anyone, including non-Instagram members. Posts made on private accounts are only shared with followers that have been approved by the account owner. **It is recommended that you keep your personal Instagram account set to private at all times.**

natgeo

Liked by yamashitaphoto and others
natgeo Photo by @renan_ozturk | Ushishir Island, the crown jewel of the Kuril Islands in the North Pacific. As one... more
View all 1,525 comments
dzalcman Whew, that color!
December 2

INSTAGRAM MEDIA FORMATS

Instagram supports three different media formats for upload, storage, and sharing:

- **Stories** are real-time, temporary video or photo posts which are not automatically saved to your profile page. New stories are designated with a pink-purple circle around your profile page and are viewable for 24 hours.

- **Videos** can be shared in a single post or as a video series. The best video formats are **MP4** and **MOV**.

- **Photos** can be shared in a single post or as a photo series. Instagram supports a maximum resolution of 1080x1080 pixels. Larger photos are automatically downsized during upload. The aspect ratio must be set between 1:91:1 (landscape) and 4:5 (portrait).

Stories
_.siamarie   heyjoo_lee   guerrillafe...

Videos
WATCH
Videos You Might Like
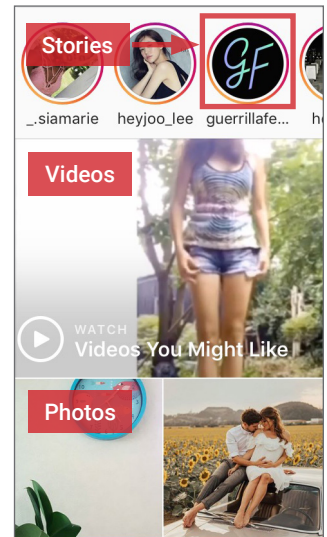
Photos

ACCOUNT REGISTRATION - PRIVACY TIPS

1
Sign up to see photos and videos from your friends.

DO NOT use your Facebook account for sign up or log in.

SIGN UP   LOG IN

Enter your email

Log In with Facebook

2
Name and Password
Add your name so friends can find you.

Full Name ← **Full Name is NOT REQUIRED during registration. Do not share.**

Password ← **Choose a complex password and change it every 3 months.**

Next

3
Find People to Follow
To help people connect on Instagram, you can choose to have your contacts periodically synced and stored on our servers. You pick which contacts to follow. Disconnect anytime to stop syncing.

Learn More

DO NOT allow contacts access.

Cancel

Allow Access

Getting Started

MANAGING YOUR INSTAGRAM PROFILE

Cancel   Edit Profile   Done

Choose a profile photo that doesn't include your face or a location you frequent.

Change Profile Photo

Don't reveal your name, birth date, or other personally identifiable information (PII) in the username. Choose something not linked to your ID.

Don't reveal your full name in the Name field. It can be left empty (or you can insert an emoji!).

Name   🙂
Username   rhdurjxieidkidid
Website   Website
Bio   Bio

Do not link a personal website or add Bio information.

DIRECT MESSAGING FEATURES

Today 9:11 AM

▶ Photo

Senders are notified when recipients screen capture ONE-TIME, TEMPORARY messages.

A few others haha

▶ Photo

▶ Photo

Oh jeez

Double tap to like

Share a temporary photo or video in a DM
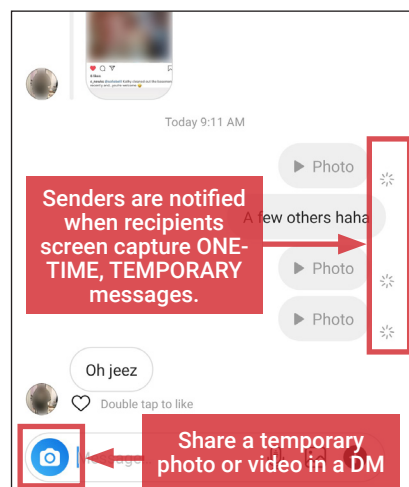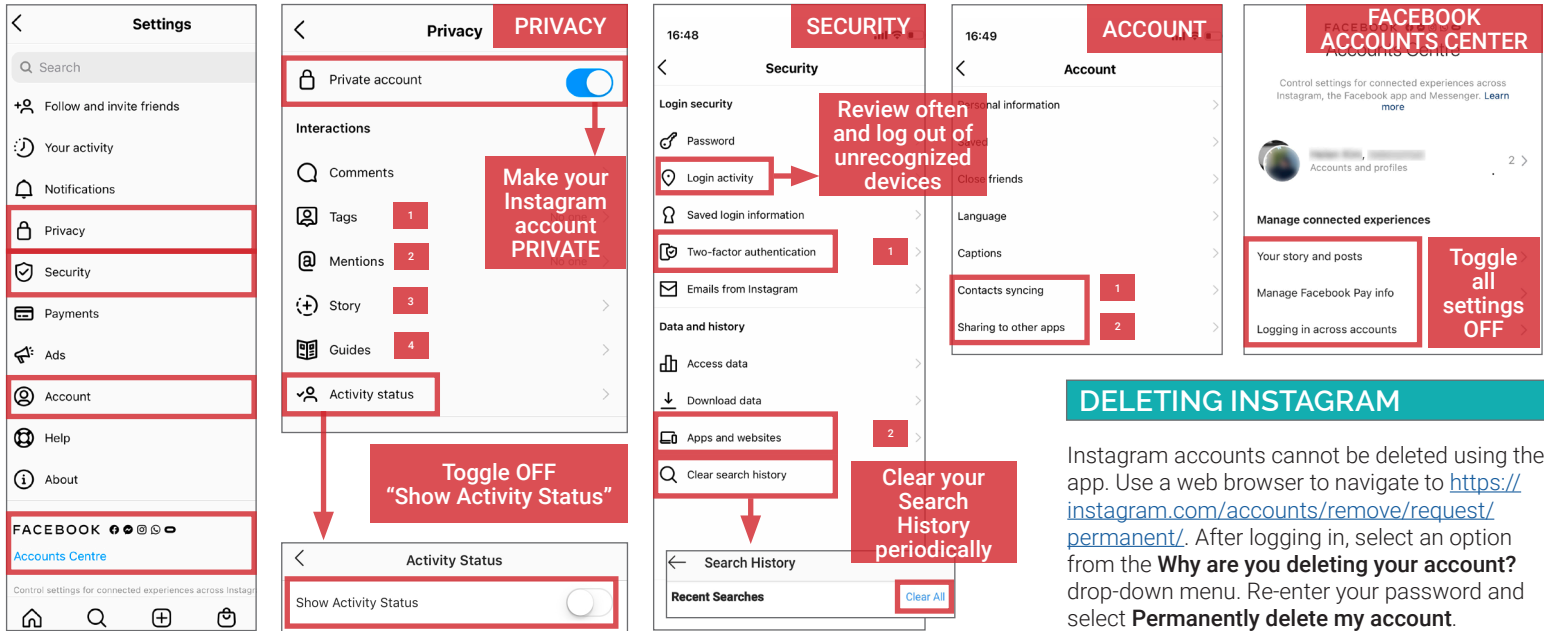
Direct Messages (DMs) allow users to communicate privately in the app. With DMs, users can send texts, photos, videos, and audio messages. They can also share public Instagram stories and posts. Much like Instagram posts, users have the option to send DMs as a **temporary** or **permanent** message. The recipient has the option to replay temporary messages one time.

If the recipient screen captures a temporary message, the sender is notified via a push notification, and a blinking shutter icon appears next to the captured message.

NAVIGATING INSTAGRAM SETTINGS

Go to your **Profile** and tap the ☰ icon (top-right corner) to access **Settings**. Apply the settings under **Privacy**, **Security, Account**, and **Facebook Accounts Centre** as shown to control the visibility of your content and minimize the amount of personal information you share with Instagram and third-parties.

Settings
- Search
- Follow and invite friends
- Your activity
- Notifications
- Privacy
- Security
- Payments
- Ads
- Account
- Help
- About

FACEBOOK
Accounts Centre

Control settings for connected experiences across Instag

PRIVACY

Privacy
- Private account ⬤
- Interactions
  - Comments
  - Tags [1]
  - Mentions [2]
  - Story [3]
  - Guides [4]
  - Activity status

Make your Instagram account PRIVATE

Toggle OFF "Show Activity Status"

Activity Status
- Show Activity Status ○

SECURITY

16:48
Security
- Login security
  - Password
  - Login activity
  - Saved login information
  - Two-factor authentication [1]
  - Emails from Instagram
- Data and history
  - Access data
  - Download data
  - Apps and websites [2]
  - Clear search history

Review often and log out of unrecognized devices

Clear your Search History periodically

← Search History
Recent Searches   Clear All

ACCOUNT

16:49
Account
- Personal information
- Close friends
- Language
- Captions
- Contacts syncing [1]
- Sharing to other apps [2]

FACEBOOK ACCOUNTS CENTER

Accounts Centre

Control settings for connected experiences across Instagram, the Facebook app and Messenger. Learn more

Accounts and profiles   2
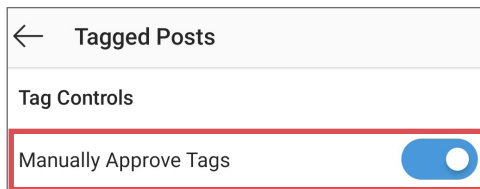
Manage connected experiences
- Your story and posts
- Manage Facebook Pay info
- Logging in across accounts

Toggle all settings OFF

DELETING INSTAGRAM

Instagram accounts cannot be deleted using the app. Use a web browser to navigate to https://instagram.com/accounts/remove/request/permanent/. After logging in, select an option from the **Why are you deleting your account?** drop-down menu. Re-enter your password and select **Permanently delete my account**.

PRIVACY

1, 2 Under **Privacy** > **Tags** and **Privacy** > **Mentions**, set **Allow Tags From** and **Allow @mentions From** to **No One**. Additionally under **Tags**, **toggle ON Manually Approve Tags** to review when others tag you in photos, videos, and stories before they become associated with your Instagram profile.
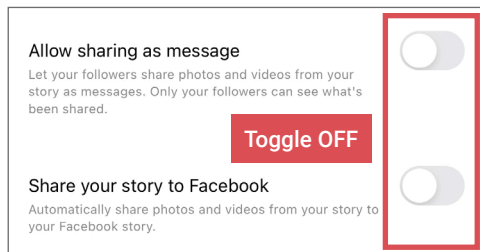
← **Tagged Posts**
Tag Controls
Manually Approve Tags ⬤
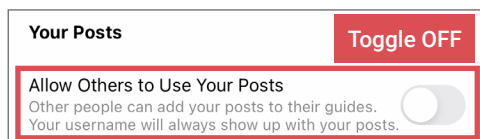
3 Navigate to **Privacy** > **Stories > Sharing** and **toggle OFF** all options as shown.

Allow sharing as message
Let your followers share photos and videos from your story as messages. Only your followers can see what's been shared. ○

Toggle OFF

Share your story to Facebook
Automatically share photos and videos from your story to your Facebook story. ○

4 **Toggle OFF Allow Others to Use Your Posts** to prevent other users from sharing your Instagram content with others.
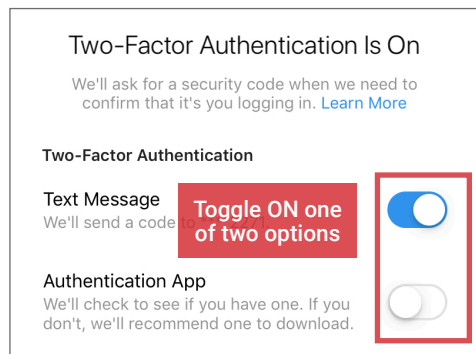
Your Posts   **Toggle OFF**
Allow Others to Use Your Posts
Other people can add your posts to their guides. Your username will always show up with your posts. ○

SECURITY

1 Under **Security** > **Two-Factor Authentication,** enable two-factor authentication on Instagram to protect your account against identity theft and takeovers.

Two-Factor Authentication Is On
We'll ask for a security code when we need to confirm that it's you logging in. Learn More
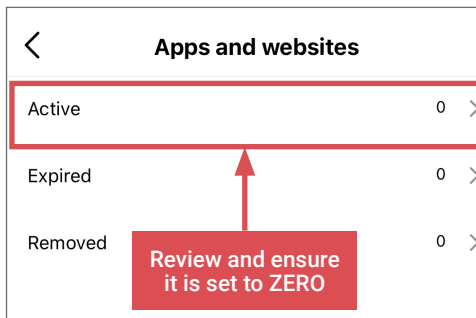
Two-Factor Authentication

Text Message
We'll send a code to   **Toggle ON one of two options** ⬤

Authentication App
We'll check to see if you have one. If you don't, we'll recommend one to download. ○

2 Under **Security > Apps and Websites**, you can see a list of all third-party apps with access to your Instagram account data. Review the list frequently and remove them as needed to prevent them from accessing your data in the background.
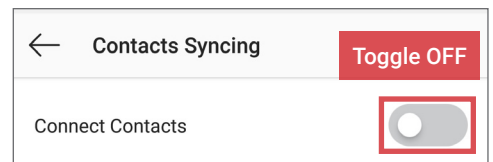
← **Apps and websites**
Active   0 >
Expired   0 >
Removed   0 >

Review and ensure it is set to ZERO

ACCOUNT
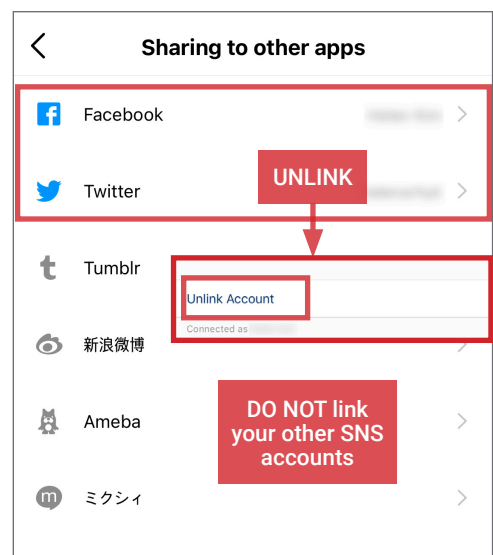
1 Under **Account** > **Contacts Syncing, toggle OFF Connect Contacts** to prevent your phone contacts from syncing with Instagram.

← **Contacts Syncing**   **Toggle OFF**
Connect Contacts ○

2 Review which SNS accounts you may have connected with your Instagram account under **Account** > **Sharing to other apps**. If there are linked accounts, unlink each one by clicking on the SNS link and choosing **Unlink Account**.

← **Sharing to other apps**
- Facebook >
- Twitter >   **UNLINK**
- Tumblr
  - Unlink Account
  - Connected as
- 新浪微博 >
- Ameba >
- ミクシィ >

DO NOT link your other SNS accounts

LINKEDIN

SOCIAL NETWORK - DO'S AND DON'TS

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see and share information you post regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all the logged-in devices and locations.
- Remember that even if you restrict your data from public view, LinkedIn still has access to your data and may share it with third parties.

MANAGING YOUR LINKEDIN PRESENCE

LinkedIn is a professional networking service with 772 million members worldwide.[11] It is mainly used to connect employers who create job postings and job seekers who share their resumes and Curricula Vitae (CVs). Users typically maintain profile pages outlining professional and educational achievements, and establish networks with others who report similar interests and backgrounds. They can also identify personal areas of expertise, skills, and interests. Since 2016, LinkedIn has been a subsidiary of Microsoft.[12] Follow the recommended settings to limit exposing your personal data without foregoing LinkedIn's many useful features.

Manage your Settings & Privacy
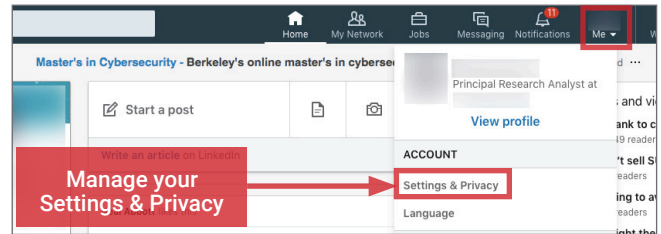
NAVIGATING LINKEDIN SETTINGS

1 Account preferences

2 Sign in & security

3 Visibility
- Visibility of your profile & network
- Visibility of your LinkedIn activity

4 Communications

5 Data privacy

6 Advertising data

From the home page, click on the drop-down menu **Me** icon on the top panel and navigate to **Settings & Privacy**. From this page, you can access granular privacy controls.

LinkedIn provides privacy settings under six following areas: (1) Account preferences, (2) Sign in & Security, (3) Visibility, (4) Communications, (5) Data Privacy, and (6) Advertising data. Apply the settings shown on the following two pages to ensure that your profile and activities are visible only to the people of your choosing.

1 ACCOUNT PREFERENCES

Navigate to **Settings & Privacy > Account preferences** and implement the following recommendations to minimize how your data is tracked and repurposed through LinkedIn.

Under **Site Preferences**, set the visibility of your profile photo to **Connections** or **No One**. Also, disable **the Viewers of this profile also viewed** feature, as it increases the chance of your profile being suggested to other members.

Show profile photos Choose whether to show or hide profile photos of other member	**Set to My Connections or No One**	Change Connections
Feed preferences Customize your feed		Change
Viewers of this profile also viewed Choose whether or not this feature appears when people view your profile	**Turn OFF**	Change No
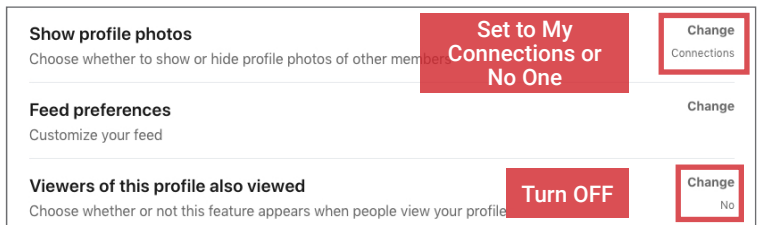
Under **Sync options**, disable if you are currently syncing your calendar or contacts with LinkedIn

Sync calendar Manage or sync calendar to get timely updates about who you'll be meeting with	**Disable Syncing**	Change
Sync contacts Manage or sync contacts to connect with people you know directly from your address book		Change
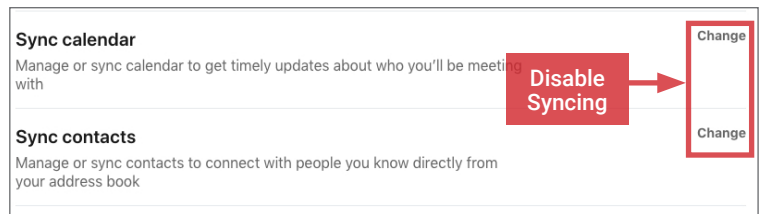
Review **Partners and Services** section monthly to see which services and apps you've given access to your LinkedIn data. Remove permissions from services that you no longer use or require.

Partners & services Services you've connected your LinkedIn account		
Microsoft View Microsoft accounts you've connected to your LinkedIn account	**DO NOT connect to Twitter or Microsoft**	Change 0 connected accounts
Twitter Manage your Twitter info on your LinkedIn account		Change Not connected
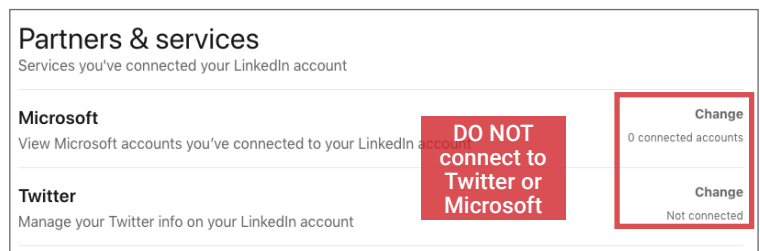
2 SIGN-IN & SECURITY

Navigate to **Settings & Privacy > Sign-in & Security**. Under **Account Access**, you can review which devices and sessions are currently active on LinkedIn. Review frequently and log-out of sessions that you are no longer using, remove passwords from devices where they are automatically stored, and activate two-step verification to secure your account from potential account takeovers.

Where you're signed in See your active sessions, and sign out if you'd like	**Review and log out of inactive sessions**	Change 2 active sessions
Devices that remember your password Review and control the devices that remember your password	**Set to 0**	Change 0 devices
Two-step verification Activate this feature for enhanced account security	**Turn ON**	Change On

CLOSING YOUR LINKEDIN ACCOUNT

If you no longer require LinkedIn, visit **Settings & Privacy > Account preferences > Account management > Closing account** and confirm your decision. Account deletion is permanent after 20 days.

LINKEDIN SETTINGS CONTINUED...

3 VISIBILITY

Under **Visibility**, implement the settings as shown to minimize how your provile and activity is visible on LinkedIn and other public search engines.

Visibility of your profile & network
Make your profile and contact info only visible to those you choose

Profile viewing options Choose whether you're visible or viewing in private mode	Change / Private mode
Story viewing options Choose whether you're visible or viewing in private mode	Change
Edit your public profile Choose how your profile appears	Your profile's public visibility — Off
Who can see or download your email address Choose who can see your email address on your profile and in approved apps or download it in their data export	Change
Who can see your connections Choose who can see your list of connections	Change / Only you
Who can see your last name Choose how you want your name to appear	Change / Abbreviated
Representing your organization and interests Show your name and/or profile information with other content shown on LinkedIn?	Change / No
Profile visibility off LinkedIn Choose how your profile appears via partners' and other permitted services	Change / No
Profile discovery using email address Choose who can discover your profile if they haven't connected with you, but have your email address	Change / Nobody
Profile discovery using phone number Choose who can discover your profile if they haven't connected with you, but have your phone number	Change / Nobody

Turn your public profile visibility OFF

Set to Private Mode

Set to No

Set to Only visible to me

Set to Only you

Set to Abbeviated

Set to No

Set to No

Set to Nobody

Set to Nobody

Visibility of your LinkedIn activity
Make sure your network only sees the activity you choose to show

Manage active status Choose who can see when you are on LinkedIn	Change
Share profile updates with your network Choose if your network is notified about key updates from your profile	Change / No
Notify connections when you're in the news Choose if your network is notified when you've been mentioned in an article or blog post	Change / No
Mentions or Tags Choose whether other members can mention or tag you	Change / No
Followers Choose who can follow you and see your public updates	Change / Connections

Set to No one

Set to No

Set to No

Set to No

Set to Connections

4 COMMUNICATIONS

Minimize the following three settings under the **Communications** tab.

Who can reach you
Manage who you'd like to get communications from

Invitations to connect Choose who can connect with you	Change / Imported contacts
Invitations from your network Choose what invitations you'd like to receive from your network	Change / On
Messages Allow select people to message you	Change / InMail
Research invites Choose if you want to get invites from LinkedIn to participate in research	Change / No

Messaging experience
Choose how would you like LinkedIn to customize your experience

Read receipts and typing indicators Turn on read receipts and typing indicators	Change / Off

Set to Imported contacts

Set to No

Set to Off

5 DATA PRIVACY

Navigate to **Settings & Privacy > Data Privacy > How LinkedIn uses your data > Get a copy of your data** to receive and review a comprehensive report of your past activity and network information. After review, revoke access when possible to data you no longer want to share with Linkedin.

Getting a copy of your data   Close
See your options for accessing a copy of your account data, connections, and more

Your LinkedIn data belongs to you, and you can download an archive any time or **view the rich media** you have uploaded.

○ Download larger data archive, including connections, contacts, and your account history. **Learn more**

○ Want something in particular? Select the data files you're most interested in.

☐ Articles   ☐ Connections

6 ADVERTISING DATA

The **Advertising Data** tab details the types of information Linkedin uses from your profile and activities to create personalized ads on your behalf. Review this tab carefully and opt-out of detailed tracking when possible to minimize sharing personal details with LinkedIn and its third-party partners.

Profile data for personalizing ads Choose how ads appear to you	Change / No
Interest categories See more relevant ads, such as job ads, based on your and similar members' activities on LinkedIn and Bing	Change

Set to No

Set to No

Data collected on LinkedIn
Choose what type of data you would like LinkedIn to use to show you more relevant ads

Connections Choose whether your connections can be used to show you relevant ads	Change / No
Location Choose whether your location can be used to show you relevant ads	Change / No
Demographics See more relevant ads based on your demographic data	Change / No
Companies you follow See more relevant ads, such as job ads, based on companies you follow	Change / No
Groups Choose whether the groups you've joined can be used to show you relevant ads	Change / No
Education See more relevant ads, such as job ads, based on your education	Change
Job information See more relevant ads, such as job ads, based on your job info	Change
Employer See more relevant ads, such as job ads, based on your company information	Change

Set to No

Uncheck all listed items

Third-party data
Choose how you'd like data from your activity off LinkedIn to be used to show you more relevant ads

Audience insights for websites you visit Choose if your data can be used anonymously by third party websites you visit to help them better understand their audiences	Change / No
Ads outside of LinkedIn Choose if you want to see relevant ads on websites and apps outside of LinkedIn	Change / No
Interactions with businesses Choose how your information given to businesses is used to show you relevant ads	Change / No
Ad-related actions Choose if your actions on ads can be used to understand and report aggregate ad performance	Change / No

Set to No

TIKTOK

TIKTOK - DO'S AND DON'TS

- Don't connect your TikTok account with other SNS profiles (e.g., YouTube). Connecting increases your account's discoverability.
- Only accept follow requests from people you know and trust. Assume that ANYONE can see and forward videos you post and record copies.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging videos that clearly show your face. Select videos of yourself taken at a distance, at an angle, or wearing sunglasses.
- Don't embed your posts with hashtags (e.g., #flashback, #quarantine). Hashtags increase your posts' visibility and make them searchable by others.
- Remember: even if you restrict your data from public view, TikTok still has access and may share it with third parties or the Chinese government.[14]

OVERVIEW

TikTok is a video-sharing social networking service (SNS) and entertainment platform owned by ByteDance, an Internet technology company headquartered in Beijing, China. TikTok encourages users to record, share, and react to short videos as a form of creative expression. It also encourages users to download, edit, and reshare videos posted by other users. TikTok became popular in the U.S. in 2018 after merging with Musical.ly (a Shanghai-based music video-sharing SNS) and hosts 800 million monthly active users in 2020.
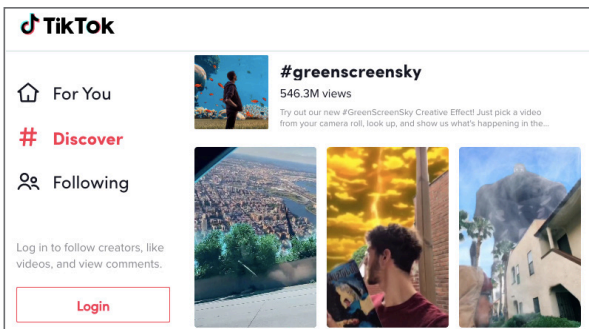
TikTok is primarily used as a mobile application but is also accessible via a web browser. TikTok accounts can be **public** or **private**. Content posted on public accounts is indexed by search engines and can be viewed by anyone, including non-TikTok users. Posts made on private accounts are shared with followers that have been approved by the account owner. Regardless of privacy settings, TikTok has access to all users and may share it with third parties. It is recommended that you **keep your TikTok account set to private at all times.**

In 2019 and 2020, the U.S. Department of Defense released guidance recommending that personnel delete TikTok from personal electronic devices due to data security concerns.[13] U.S. Military branches have also banned the installation and use of TikTok on government-issued mobile devices. **Before installing and using TikTok, check with your employer for relevant regulations, restrictions, and usage guidelines.**

ACCOUNT REGISTRATION

1 | **Sign up for TikTok**

Create a profile, follow other accounts, make your own videos, and more.

- Use phone or email
- Continue with Facebook
- Continue with Google
- Continue with Twitter
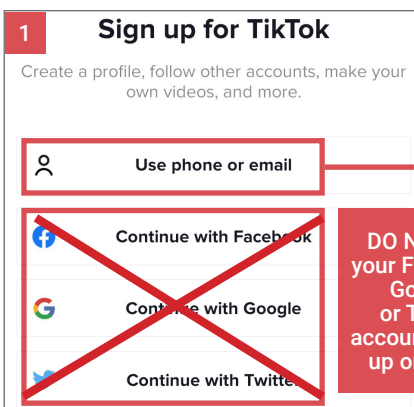
DO NOT use your Facebook, Google, or Twitter account to sign up or log in.

2 | **Sign up**

Phone | **Email**

Sign up with a secondary email address.

Email address

By continuing, you agree to TikTok's **Terms of Use** and confirm that you have read TikTok's **Privacy Policy**.

Next

DO NOT reveal your name, birth date, or other personally identifiable information (PII) in the username. Choose something not linked to your identity or other online accounts.

3 |

Create username

You can always change this later.

✔

Sign up

MANAGING YOUR TIKTOK PROFILE

Choose a profile photo or video that doesn't include your face or a location you frequent.

@_____ 🔒

0 Following | 0 Followers | 0 Like

Edit profile 🔖

You can make liked videos public in Privacy settings ✕

← **Edit profile**

📷 Change photo | 🎥 Change video

Name | user_____ >
Username | _____ >
tiktok.com/@_____ 📋
Bio | Add a bio to your profile >
YouTube | Add YouTube to your profile >

Cancel | **Name** | Save

Name
user_____ ⊗

Set your username?
You can change your username once every 30 days.

CANCEL | SET USERNAME

Use an anonymized Name and Username, such as a string of characters, numbers, or emojis.

DO NOT add a Bio or link other SNS accounts.

POSTING TO TIKTOK

Video editing tools and add-ons

BRINGING OUTSIDE IN

NEW DECOR
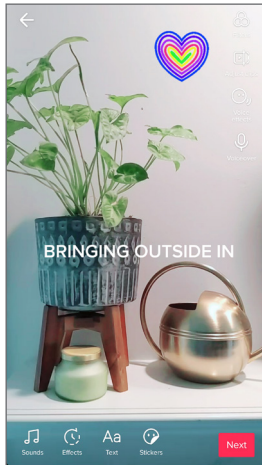
It is challenging to control personal data disclosure in videos.

When recording videos for TikTok, avoid capturing your face and voice, as well as those of friends and family members. Do not record videos in familiar locations such as your home or workplace.

When posting, limit the visibility and searchability of your content through the following steps:

- Restrict viewership to approved Followers.
- Disable comments and collaboration (**Stitch, Duet, and React**) features as shown at right.
- Avoid using hashtags or detailed descriptions.
- Avoid tagging friends.

Post

Describe your video

#Hashtags   @Friends

Select cover

Who can view this video — Followers >

Allow comments — **Toggle OFF**

Allow Stitch, Duet, and React

Save to device

Drafts   Post
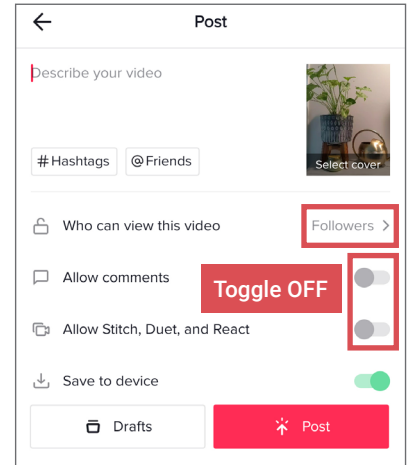
NAVIGATING TIKTOK SETTINGS

To access settings, go to your **Profile** and tap the ⋮ icon [top right]. Apply the **Settings and privacy** configurations shown below to control the visibility of your videos and minimize the amount of personal information you share with TikTok and third parties.

Settings and privacy

ACCOUNT

- Manage account **1**
- Privacy **2**
- Security **3**
- Balance
- TikCode
- Share profile

CONTENT & ACTIVITY

- Push notifications
- App language
- Content preferences
- Digital Wellbeing
- Family Pairing **4**

SUPPORT

Find additional privacy and security information here.

- Report a Problem
- Help Center
- Safety Center
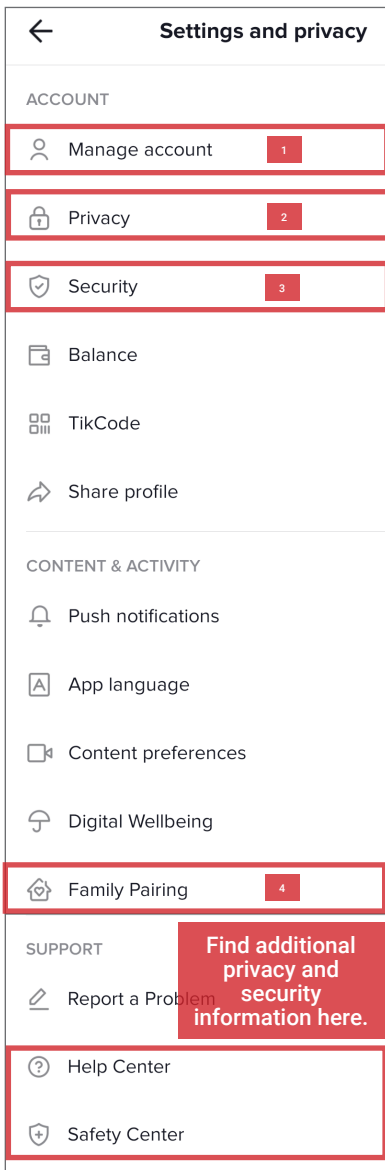
1   MANAGE MY ACCOUNT

If you decide to stop using TikTok, navigate to **Manage my account** > **Delete account** and complete the verification process to confirm your decision.

3   SECURITY

Navigate to the Security section and apply the following settings:

- Under **2-step verification,** follow the prompts to enable additional security settings.
- Use **Manage Devices** to monitor devices accessing your TikTok account**.**
- **Toggle OFF Save login info.**

4   FAMILY PAIRING

TikTok is popular with young users and provides parental content control options.

To set up an account for a young user, navigate to **Settings and privacy** > **Family Pairing** and follow the prompts.

This feature allows a parent to link with a child's account via QR code in order to control app viewing time, content exclusion, and messaging functionality.

Family Pairing

Who is using this TikTok account?

Parent   **Teen**
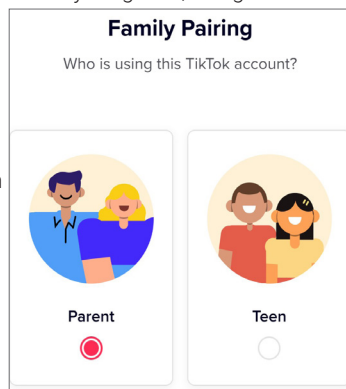
Parents can also configure spam filtering and keyword filtering by visiting **Settings and privacy > Privacy > Comment filters** and adjusting filtering settings as desired.

2   PRIVACY AND SAFETY

Navigate to **Privacy** and apply the following settings:
- **Toggle ON Private account** to limit public access to your content and your liked videos.
- **Toggle OFF Suggest your account to others** to prevent TikTok from sharing your profile.
- Turn OFF **Find your contacts**.
- **Toggle OFF Ad authorization** to prevent advertisers from featuring your videos.
- Under **Safety,** apply settings as shown below.

Private account

With a private account, only users you approve can follow you, and browse your videos (in Following, For You, and profile). Your account can still be found in search results or as a suggestion.

Privacy

Find your contacts   **Toggle OFF**   Off

PERSONALIZATION AND DATA

Personalization and data

Ad authorization
Allow third-party advertisers to use your videos in ads.   **Toggle OFF**

SAFETY

Allow your videos to be downloaded   Off

Who can send you direct messages   Friends

Who can Duet with your videos   Only me

Who can Stitch with your videos   Only me   **Restrict to Friends or Only me**

Who can view your liked videos   Only me

Who can comment on your videos   Friends

Comment filters   On

TWITTER

SOCIAL NETWORK - DO'S AND DON'TS

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all the logged-in devices and locations.
- Remember that even if you restrict your data from public view, Twitter still has access to your data and may share it with third parties.

OVERVIEW

Twitter is a social networking and micro-blogging site that hosts 187 million daily active users as of 2020.[15] Twitter allows users to post short entries to their profiles and follow updates from other accounts. On average, Twitter users post approximately 500 million entries per day from both the website and mobile app.[16] For most, Twitter is used as a source to discover breaking news developments and stay up-to-date on current events or friends' recent whereabouts. Should you choose to maintain a Twitter account, use this book's recommendations to enhance your privacy.

TWITTER PROFILES

Profile pages can be operated by individuals, corporations, or other organizations. Regardless of who maintains the account, each individual profile is labeled with a unique username known as a Twitter Handle (e.g., @google). Handles allow other users to locate profiles and mention them in posts.

Twitter profiles are intended to contain some of the account owner's personal data, and may include:

- A short biography or personal description
- The user's primary location
- A link to a personal website, blog, or other SNS profile
- Birth date
- Date of Twitter account creation
- Number of followers
- Number of accounts followed
- Number of Tweets

If you opt to use Twitter, minimize the amount of personal information shared on your public profile.

POSTING TO TWITTER

A Twitter entry is referred to as a **Tweet**. Tweets can be composed of photos, videos, links, polls, or short text entries, limited to 280 characters. Tweets are public, indexed, and searchable, unless protected by the user. Many users never Tweet, choosing only to follow persons or topics of interest.

Tweets display the profiles of those who interacted with the posted content. Limit your interactions to better control your profile's reach.
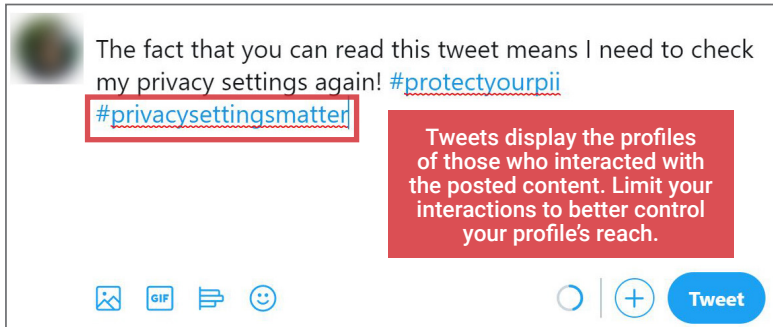
Mentions (@username) are used to tag other users or accounts in a Twitter update. Tags create a link to the mentioned individual's profile. When a public user mentions a private Twitter account, the link to the profile of the private account becomes visible to the public.

Hashtags (#topic) are used to highlight key topics in individual posts. When a hashtag is posted by numerous users across the network, the hashtag becomes a **trending topic** of conversation. Trending topics are advertised on Twitter and extend the reach of posts and profiles. Tweets with hashtags are searchable within the Twitter search engine.

When a Tweet is published, other Twitter users are able to interact with it through the icons highlighted to the left. Interactions inlcude **Replies, Retweets, Likes,** and additional Tweet sharing or saving options.

- **Replies** - Replies are text responses to another user's Tweet. The Reply prompt automatically mentions the author of the original Tweet within the text of the reply.

- **Retweets** - Retweets are used to forward other users' Tweets to a user's personal followers. Retweets always retain a link back to the original poster's profile page.

- **Likes** - Likes are used to show endorsement of another user's post. A list of entries liked by a single user appears directly within that user's Twitter profile page.

MAXIMIZING YOUR TWITTER PRIVACY

Settings

- Your account
- Security and account access
- Privacy and safety
- Notifications
- Accessibility, display, and languages
- Additional resources
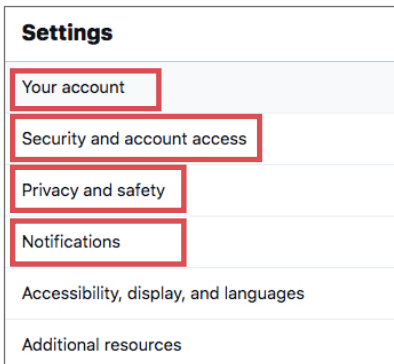
Access Twitter's settings using the panel located at the left side of your home screen. Click **More > Settings and privacy** and navigate to pages containing customizable security options.

Maximize account security and privacy by configuring your settings as shown on this page.

NOTIFICATIONS SETTINGS

Notifications alert you when others interact with your profile or content. For maximum security, navigate to **Settings > Notifications > Push/SMS/Email notifications** and **toggle ON** notifications. Under **Related to you and your Tweets**, check the boxes to receive email alerts regarding **Direct messages** and **Tweets pushed/messaged/emailed to you**.

← **Email notifications**

Email notifications — **Toggle ON**

Get emails to find out what's going on when you're not on Twitter. You can turn them off anytime.
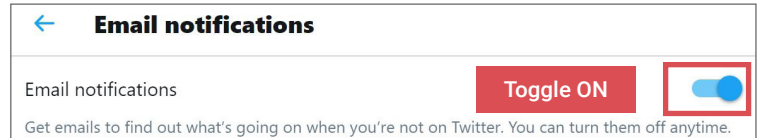
ACCOUNT & SECURITY SETTINGS

The **Settings > Your account** page provides Twitter account customization options. While Twitter is designed to make user contents reach as many audiences as possible, the setting provides options to limit your content to only people of your choosing. The most important thing to maximize your privacy on Twitter is to set **Your account** private. To do so, navigate to **Settings > Your account > Account information > Protected Tweets.**
- Check the box for **Protect your Tweets** to ensure posts are only displayed to your followers.
- **Toggle Photo tagging OFF** to prevent other users from tagging you in their photos and tweets.

Manage what information you allow other people on Twitter to see.

Protect your Tweets — **Check box to set Private**

When selected, your Tweets and other account information are only visible to people who follow you. Learn more

Photo tagging Off — **Turn OFF**
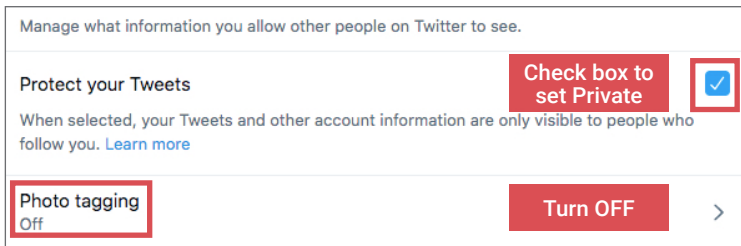
For maximum login security, navigate to **Settings > Security and account access > Security** page:
- Enable **Two-factor authentication**.
- Enable **Additional password protection**.

Navigate to **Your account > Account information > Username** to update your Twitter handle. Use an anonymized handle that does not divulge any key personal information (e.g., full name, birth date).

← **Change username**

Username
C�_____

Use a nickname, initials, or pseudonym. Don't reveal your full name inside the username
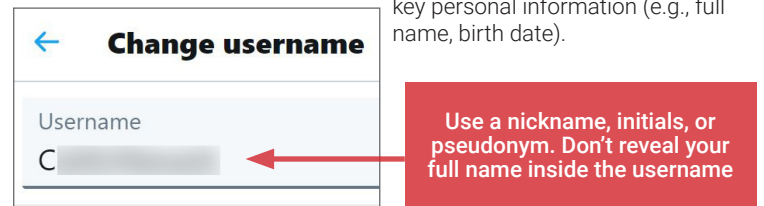
To deactivate your Twitter account, visit **Account > Deactivate your account** and follow the prompts to confirm. The deletion process begins 30 days after request submission, and takes up to one week for completion.

← **Deactivate account**

Caitlin ____
@C_

This will deactivate your account

You're about to start the process of deactivating your Twitter account. Your display name, @username, and public profile will no longer be viewable on Twitter.com, Twitter for iOS, or Twitter for Android.

Deactivate
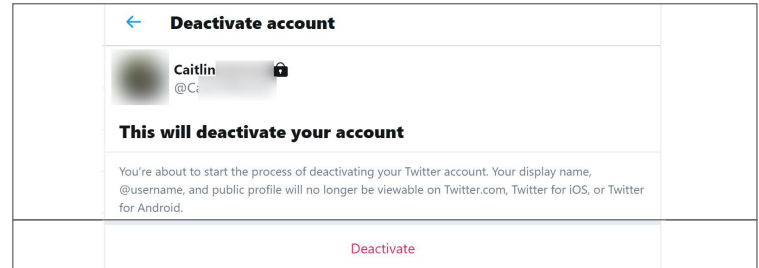
PRIVACY AND SAFETY

Twitter provides two privacy controls for how it accesses user's location data. First, navigate to **Settings > Privacy and safety > Your Tweets > Add location information to your Tweets** and implement settings as shown.

← **Add location information to your Tweets**

Click to clear location data from your Tweets

If enabled, you will be able to attach ~~location information~~ to your Tweets. Learn more

Add location information to your Tweets — **Uncheck box**

Remove all location information attached to your Tweets
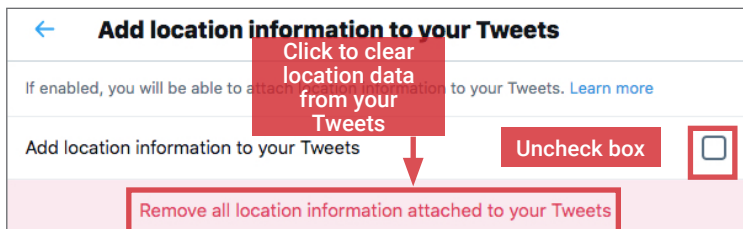
Second, navigate to **Settings > Privacy and safety > Your Tweets > Data sharing and off-Twitter activity > Location information**.

← **Location information**

Manage the location information Twitter uses to personalize your experience.

Personalize based on places you've been

Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, Twitter may also personalize your experience based on other places you've been.

Uncheck the box to disable Twitter from personalizing your account based on your location

The **Privacy and safety > Data sharing and off-Twitter activity** page details how Twitter accesses and shares your data with its third-party business partners for advertising purposes. Go through each section as shown and implement the following recommended settings:
- Uncheck the box to disable **personalized ads**
- Uncheck boxes for both settings to disable **Off-Twitter tracking**
- Uncheck the box to disable Twitter from **sharing data with its partners**

Data sharing and off-Twitter activity

Ads preferences
Manage your ads experience on Twitter. — **Uncheck box**

Off-Twitter activity
Manage how Twitter uses your online activity ~~and websites you visit, to personalize your experience~~ — **Uncheck both boxes**

Data sharing with business partners
Allow sharing of additional information with Twitter's business partners — **Uncheck box**

Location information
Manage the location information Twitter uses to personalize your experience.

GOOGLE ACCOUNT

GOOGLE ACCOUNT - DO'S AND DON'TS

- Closely track all Google products and services you own and use, and review your usage habits frequently—do they still provide you with absolutely necessary functions? If not, remove, deactivate, or unsubscribe as needed to limit what Google collects about you.
- If possible, use an email address that does not reveal your full name or potentially identifying information (e.g., birth date) when using Google services.
- Avoid using profile photos that reveal your face, and do not share personal identifiers (e.g., last name and current city) on your Google profile.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Remember that even if you restrict your data from public view, Google still has access to your data and may share it with third-parties.

OVERVIEW

Click on your profile icon > Google Account
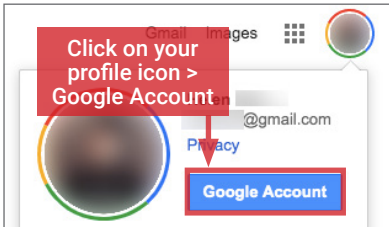
Google Account settings encompass all privacy and security controls for Google-operated services, including:
- Apps and websites, such as Search, Gmail, Calendar, Maps, Google Photos, and YouTube.
- Operating platforms, such as the Android OS and Chrome browser.
- Products and devices, like the Pixel phone, Google Home, and Google Ads built into third-party services.

Due to the ubiquity of these services, the consolidated data and activities across all Google services can reveal a highly unique and individualized profile of your online identity. Therefore, it is imperative to review your Google Account settings frequently to prevent unwanted exposure and sharing. Use the recommended settings below to minimize the amount of personal data collected and shared by Google.

MINIMIZING DATA COLLECTION AND SHARING ON GOOGLE
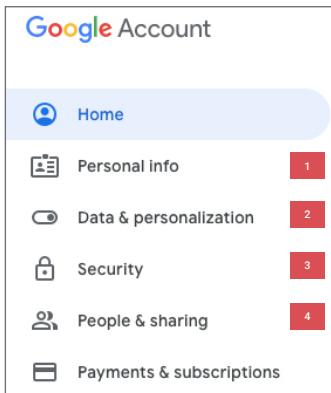
Access your Google Account settings from web or mobile browsers at www.myaccount.google.com. From the home page, you can access granular privacy controls.

The (1) Personal Info, (2) Data & personalization, (3) Security, and (4) People & sharing tabs contain settings for controlling how Google collects and uses your data. Use the recommended settings in the next two pages to maximize your privacy while interacting with Google's services.

1 PERSONAL INFO

This page contains settings for controlling how your basic information, such as name and profile photo, appears across all Google products and services. Click on **Go to About me** at the end of the page to implement the following changes.

Profile and Cover Photos are always PUBLIC.

Do NOT use photos that directly expose your face or your family members.

Abbreviate your last name

Set all fields to Hidden

Review all photos associated with your Google Account. Set visibility to Only Me or Limited when possible
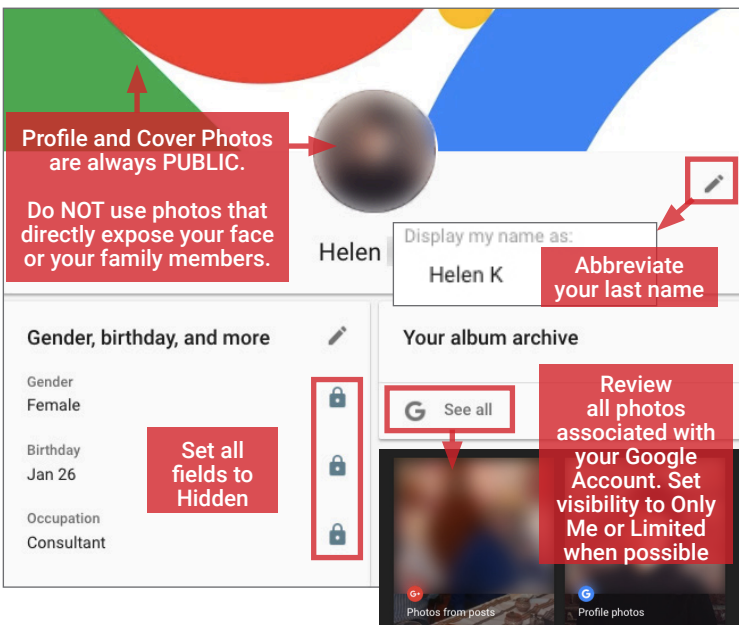
2 DATA & PERSONALIZATION

The **Data & personalization** page contains settings for controlling what Google can do with personal data collected from your activities across all Google products and services. The collected personal data range from browsing and location history to voice & audio activity. Under **Activity controls**, ensure all activity and history tracking are **Paused** for your Google Account. Activity and history tracking are used for personalization purposes and do not impact your ability to access Google's services and features..

Set ALL to Paused
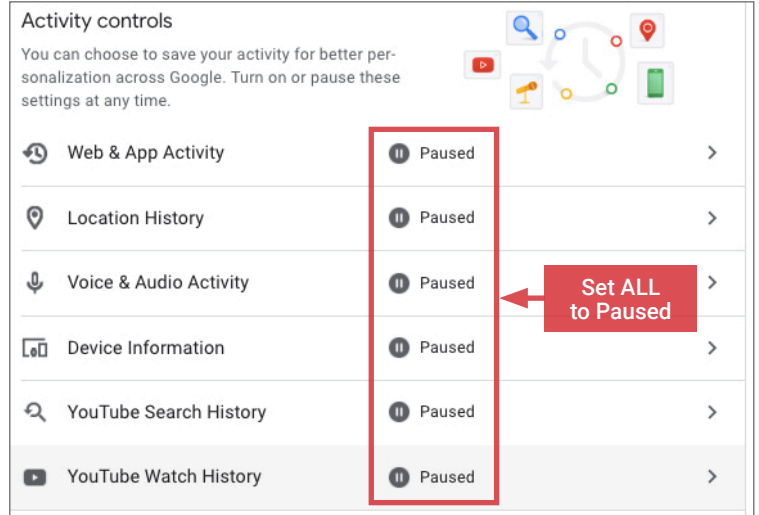
Turn OFF Ad Personalization to limit Google from using your online activities to compile a consumer profile of you to sell ads with third-party advertisers.
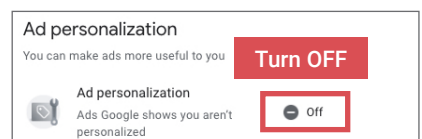
Turn OFF

Navigate to: General preferences for the web > Search Settings > Private results

DO NOT use private results

2 DATA & PERSONALIZATION - CONTINUED

Activity and Timeline displays a chronological archive of your activities on Google services, including a mapped history of your locations based on information from Google Maps and smartphones. Review items; remove all sensitive locations and info.

Activity and timeline
See the activity saved in your account and the places you've been, or delete any or all of your past activity.

> **Remove all items you do not want breached**

My Activity
Rediscover the things you've searched for, read, and watched

Timeline
See where you've been based on your Location History

3 SECURITY

The **Security** page contains settings to protect your login credentials and devices, monitor attempted and successful logins, and recover your account in the event of a lockout. Follow the recommended settings below to maximize your Google Account's security.

Signing in to Google

Password	Last changed Dec 23, 2008
2-Step Verification	On
App passwords	None

> **Update your password every 3 months**

> **Turn ON 2-Step Verification**

Third-party apps with account access
You gave these sites and apps access to some of your Google Account data, including info that may be sensitive. Remove access for those you no longer trust or use. Learn about the risks

Slack
Has access to Google Contacts
REMOVE ACCESS

> **Remove access from third-party apps you no longer use**

5 signed-in devices

Mac -
, NJ, USA · This device

's iPhone
United States · 3 hours ago

's iPad
United States · Jul 16

Sign out
Don't recognize this device?

's iPad
United States · Jul 4

> **Review your signed-in devices frequently**

> **Sign out of old devices you no longer use**

4 PEOPLE & SHARING

The **People & Sharing** page contains information about people you interact with on Google's services; and controls for how your information is shared and displayed. Immediately disable the following two settings.

Location sharing
You aren't sharing your real-time location with anyone on Google

Manage location sharing

> **NEVER share your real-time location with anyone. If you are doing so, disable access IMMEDIATELY**

Share recommendations in ads
You can choose to show your name, profile photo, and activity in shared endorsements in ads to help others find things you're interested in

Shared endorsements in ads   Off

> **Turn OFF**

ADDITIONAL PRIVACY SETTINGS

Use the **Privacy Checkup** tool from your account's home page to verify the desired privacy settings have been applied. Use the following settings shown below to control the visibility of your phone number, photos, and activities on YouTube.

Help people connect with you

(714) 2   -2

☐ **Better sharing on Google**
Enable video calling, share photos, and get notifications through Google services when people send photos & more to this number.

If turned off, you'll get SMS notifications instead.

☐ **Help people identify you via this number**
People who have this number will be able to see your name & photo, and identify things you've posted on Google services like reviews on Maps & comments on YouTube.

> **Navigate to: Home > Privacy Checkup**

> **Uncheck**

Manage your Google Photos settings

Group similar faces
Auto group photos by matching faces to better search, manage, and share.
☐ Learn more

> **Toggle OFF**

Remove geo location in items shared by link
Affects items shared by link but not by other means. ☐ Learn more

> **Toggle ON**

Manage what you share on YouTube

Likes and subscriptions
You can share your liked videos, saved playlists, and subscriptions with other YouTube users.

☑ Keep all my liked videos private
☑ Keep all my saved playlists private
☑ Keep all my subscriptions private

> **Check ALL to keep your activities private**

Your YouTube activity feed
You can choose to automatically have your public YouTube activity show up in your channel's activity feed. Don't worry, we'll never share information about activity on private videos.
☐ Learn more

☐ Post to feed when I add a video to a public playlist
☐ Post to feed when I like a video
☐ Post to feed when I save a playlist
☐ Post to feed when I subscribe to a channel

> **Uncheck ALL to limit sharing to your YouTube feed**

DELETING A GOOGLE SERVICE OR ACCOUNT

Delete a Google service
You can delete a specific Google service from your account, like YouTube or Gmail

Delete a service

Delete your Google Account
You can permanently delete your Google Account and all your services and data, like emails and photos

Delete your account

Under the **Data & Personalization** page, navigate to **Download, delete, or make a plan for your data** to make your selection. If you would like to delete your account for a specific Google service, such as YouTube or Gmail, choose **Delete a Google service**. If you would like to shut down your Google account—and all its associated services, choose **Delete your Google Account**. For both options, Google will prompt you to download your data associated with the account before completing the deletion.

HEALTH APPS & FITNESS TRACKERS

OVERVIEW

A **fitness tracker** (a.k.a. activity tracker) is a popular consumer device or application used for monitoring and recording a person's fitness-related metrics such as distance walked or run, calorie burn, heartbeat, and quality of sleep. It is usually a type of **wearable biosensor**, an electronic device worn on the body as an accessory, equipped with sensors that convert biological elements into a signal input. Fitness trackers have reached mainstream adoption worldwide, with user penetration rate hitting 11.8% of the US population in 2020.[17] The most common fitness tracker form factor is a wristband intended to measure physical activity and body functions throught the 24-hour cycle.

Most wearables are used for fitness, wellness, and sleep tracking. All fitness trackers come with an accompanying smartphone or desktop app that provide useful insights and metrics. Although physical sensors in most fitness trackers are similar, the algorithms that interpret outputs are unique to vendors. User health and fitness data is transmitted via a Bluetooth, Wi-Fi, or near-field communication (NFC) connection to a computing device.

HOW PEOPLE TRACK HEALTH & FITNESS

Most users track and analyze their health and fitness data in one of the three following ways:

- **Native apps**: Native fitness-tracking apps are part of the smartphone's operating system (OS). They are developed by smartphone manufacturers, and analyze movement and inputs from the smartphone. They are the least privacy-invasive and accurate of the options. Examples include **Apple Health** and **Samsung Health**.
- **Hardware-independent apps**: Hardware-independent fitness-tracking apps aggregate inputs from different fitness-tracking devices and smartphones to create a comprehensive profile of a user's health and activities. These apps are device and hardware-independent, relying on user input data as well as data linked from other physical trackers using custom application programming interfaces (APIs). Examples include **Google Fit** and **MyFitnessPal**.
- **Hardware-dependent apps**: Hardware dependent fitness-tracking apps accompany and analyze data from a specific brand of wearable fitness tracker. Hardware and the accompanying app are developed by the same company. They provide the most comprehensive and accurate monitoring of your health and fitness, as the accompanied hardware is expected to be worn by the user at all times. Examples of this are **Fitbit** and **Garmin Connect**.

The type of fitness tracker you choose depends on your budget and comfort level with sharing physical and activity data with the technology provider. The privacy considerations for each service is outlined below.

HEALTH & FITNESS APP	OS	FITNESS DATA INPUT SOURCES	THIRD-PARTY DATA SHARING	BUILT-IN SNS LINKS	IDENTITY DATA	DEFAULT SHARING
APPLE HEALTH	iOS only	iPhone, Apple Watch, third-party apps (e.g., FitBit)	Shares health and fitness data with other iOS apps	None	Name, birth date, weight, height, emergency contacts	Private
SAMSUNG HEALTH	Android only	Android devices; third-party fitness trackers, medical sensors, scales	Shares health and fitness data with partner apps	None	Email address, birth date, gender, height, weight	Private
GOOGLE FIT/ WEAR OS	Android, iOS	Android devices, third-party apps and devices, Google Fit apps and devices	Shares health and fitness data with connected apps and devices	None	Email address, gender, height, weight, high-accuracy location	Private
myfitnesspal	Android, iOS	Compatible with many popular health apps (e.g., Garmin Connect, Fitbit, Strava, Glow)	Shares data with other health apps (e.g., Apple Health, Garmin Connect)	Facebook	Name, email address, profile photo, location, zip code, height, gender, weight, birth date	Private
fitbit	Android, iOS, Windows	Fitbit fitness trackers	Shares data with compatible third-party apps	None	Name, display name, birth date, gender, height, weight, place	Varies by data type
GARMIN	Android, iOS, Windows	All Garmin fitness trackers and smart watches	Shares fitness data with any apps using Garmin Connect API	No direct link to SNS; can share activities as web links	Name, profile photo, location, gender, height, age, birth date	My Groups and Connections

APPLE HEALTH
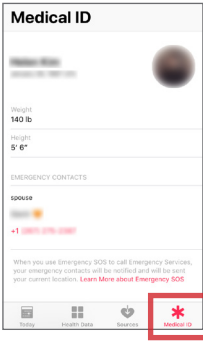
The Medical ID option shares personal data and is not required to access app features. Do not create one, or delete one if you already have one. If you already created Medical ID, navigate to the **Medical ID** tab at the bottom:

- Select **Delete Medical ID** at the bottom.
- If you wish to maintain Medical ID, **toggle OFF Show When Locked**.

SAMSUNG HEALTH

Navigate the upper-right drop-down menu to **Settings**.

- Under **General** select **Password > Set password** to protect your Samsung Health data.
- Under **Advanced, toggle OFF Together** to keep your data private.

Use the upper-right **profile icon** to access your profile page. Do not add a photo or a **Nickname**.

GOOGLE FIT

In Fit, navigate to **Profile > Settings**:

- Under **Google Fit Data**, use **Manage your data > Manage data** to **Clear All Data** or specifically delete **Activities** and **Location** data.
- Under **Activity tracking**, **turn OFF Track activity metrics** (steps and distance) when not needed. Disable **Use your location** to prevent movement mapping.

Android Users: navigate to **Settings > Apps & notifications > Advanced > App Permissions > Location > Fit** and **toggle OFF location permission** to prevent Google Fit from precisely mapping your daily activities, which may reveal sensitive information about your whereabouts.

MYFITNESSPAL

Navigate to the **More** tab **> Settings > Sharing & Privacy**. Implement data-protective settings suggested below. Do not link your Facebook account.

FITBIT

Use the profile card icon in the upper right to navigate to **Account**. Under **Privacy & Security**:

- Select **Privacy**. Review all **Personal Info** categories and adjust each category to **Private**.
- Select **Security and login > Manage Account Access** to periodically review the devices accessing your account.
- Select **Manage Data > Manage Third Party Apps** to revoke access of connected apps. Use **Manage Data > Delete Account** to remove your Fitbit data and profile when no longer in use.

GARMIN CONNECT

Navigate to the **More** tab **> Settings > Profile & Privacy**

- Set your Garmin profile and activities to **Only Me**.
- **Toggle OFF** all personal data shown on your profile.
- Navigate to **Data**; **Opt Out** and **Toggle OFF** the following optional settings.
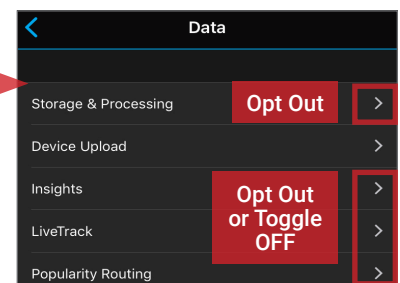
MESSAGING APPS

MESSAGING APPS - DO'S AND DON'TS
- Only establish and maintain contact with people you know and trust. Do not accept chat requests from unverified numbers or IDs.
- Do not send messages you do not want copied, screenshot, or re-posted by another user.
- Use all available PIN, password, and privacy protection options. Change passwords every three months to enhance security.
- Do not link your app to your social networking services (SNS) (e.g., Facebook, Twitter), or permit the app to use your location.
- Provide the minimal amount of identity data required to register and use the app.
- Ensure that your contacts take similar security precautions. Review your contacts often.

WHAT ARE MESSAGING APPS?

Messaging apps, which operate over cellular or Wi-Fi networks, employ security features to protect users' communications from surveillance by third parties. Protected communications commonly include text and photo messaging, voice and video calling, and interactive media (e.g. GIFs, emojis, etc.). These apps can be downloaded from your device's native provider (e.g., Android Play Store or iPhone App Store), and often only permit users to communicate with others who have installed the app. Some messaging apps afford users greater protection against eavesdropping by concealing the users' identities or making message content indecipherable to anyone except the intended recipient(s). As a result, using messaging apps may potentially offer users two layers of security: anonymity and data security.

- **Anonymity**: Messaging apps do not connect personally identifying information to messages and often require zero or limited identity data for account registration. They often offer private or public messaging to pseudonymous profiles and messages that expire after an allotted time.
- **Data Security**: Messaging apps protect private messages and account information through specific encryption methods, account settings, desktop support, or storing a limited collection of user data on the app provider's servers.

VULNERABILITIES

As with any digital communication, your personal data and messages are potentially at risk of being compromised. Though often anonymous and encrypted, secure messages and their senders' identities are susceptible to the following vulnerabilities:

- App providers may collect user data, contact lists, and usage information, and hold this information for an indefinite length of time. Some of this information may identify devices or users, and may be shared with affiliates and third parties.
- Messages not encrypted from end-to-end are susceptible to interception and decryption. However, **apps that claim to employ end-to-end encryption may have errors in their software that leave app users and their devices vulnerable to hacking through remote code execution, such as media file injection or malicious links.** Physical possession of the device is not needed for a bad actor to gain control of it.
- Failing to secure your device creates opportunities for unauthorized access. Screenshots or photos of communications also allow data leakage.
- App providers may elect to log user data for an indefinite amount of time. Data logging can enable the recovery of older communications.
- **App companies that retain a server-side ability to decrypt user communications data may share the information with law enforcement agencies in countries where the app company operates.** Additionally, in many countries, especially those with authoritative regimes, judicial or administrative orders are not necessary to seize data in a server within their reach, geographically or technically.

CHOOSING THE RIGHT MESSAGING APP

As a whole, messaging apps afford users enhanced privacy. However, users may place themselves at unwanted risk if they do not take the time to research app capabilities and take proper precautions. Four common messaging apps are profiled in this chapter for representative purposes.

SERVICE	DESCRIPTION	IDENTITY DATA	ENCRYPTION FEATURES	LINKAGES
Facebook Messenger	*Parent Company*: Facebook, Inc.	*Sign up*: Facebook Account OR Phone number/name/contacts *Optional*: Photo	Optional end-to-end encryption via Secret Conversations mode *Encryption Type:* Open Whisper System's Signal Protocol	*Social Networks:* Facebook, Instagram *Device Permissions:* Contacts, Phone, SMS
WhatsApp	*Parent Company*: Facebook, Inc.	*Sign up*: Phone number *Optional*: Name, photo	End-to-end encrypted in-app communications (messages, voice/video calls) *Encryption Type*: Open Whisper System's Signal Protocol	*Social Networks:* Facebook (WhatsApp business accounts only) *Device Permissions:* Contacts, Microphone, Storage
Signal	*Parent Company*: Signal Foundation	*Sign up*: Phone number, profile name *Optional*: Name, picture	End-to-end encrypted in-app communications (messages, voice/video calls) *Encryption Type:* Open Whisper System's Signal Protocol	*Social Networks:* None *Device Permissions:* Contacts, Phone, Storage
GroupMe	*Parent Company*: Microsoft	*Sign up*: Name, phone number or email *Optional*: Name, picture	**No encryption**	*Social Networks:* Facebook, Twitter *Device Permissions:* Phone, Location, Storage

FACEBOOK MESSENGER

Facebook Messenger allows users to exchange messages, photos, videos, stickers, audio content, stories, files, voice and video calls, and set up group meeting rooms with other Facebook and Instagram users. Messenger offers optional end-to-end encryption for message and voice message conversations supported by Open Whisper System's Signal Protocol.
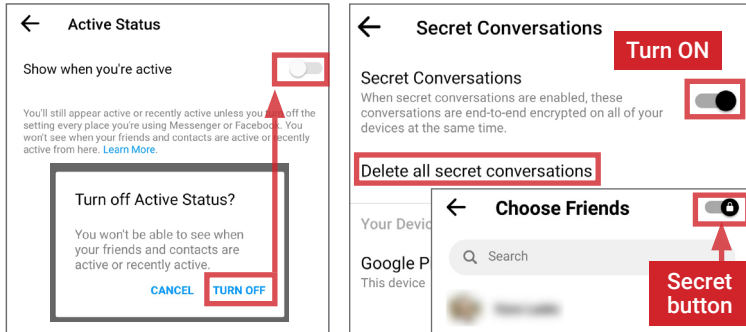
Tap your profile photo to access settings. Under **Profile > Active Status**, **turn OFF Show when you're active.** When starting a new chat, **toggle ON** the **Secret** button [lock icon, upper right] before selecting the recipient. To use the expiring message feature, tap the clock icon in the text box and set the timer.

- Consider using a secondary phone number to create a Messenger account that is not linked to your Facebook or Instagram account.
- Do not link Messenger with your SMS conversations or device contacts
- Always use **Secret Conversations**, and periodically delete conversations.
- If using the **Create Room** feature for group meets, tap the pencil icon [upper right] and set **Who Can Join Automatically** to **People you invite**.

WHATSAPP

WhatsApp provides end-to-end encryption for messages and voice and video calls using Open Whisper System's Signal Protocol. Group messaging can include up to 256 participants, while voice/video calls support up to 4 users. The Broadcast List option enables a user to send the same direct message to up to 256 recipients, rather than using Group Chat. WhatsApp is owned by Facebook, and announced plans to begin sharing user data (including phone number, profile data, and status messages, among others) with Facebook for targeted advertising purposes by February 2021.[19]
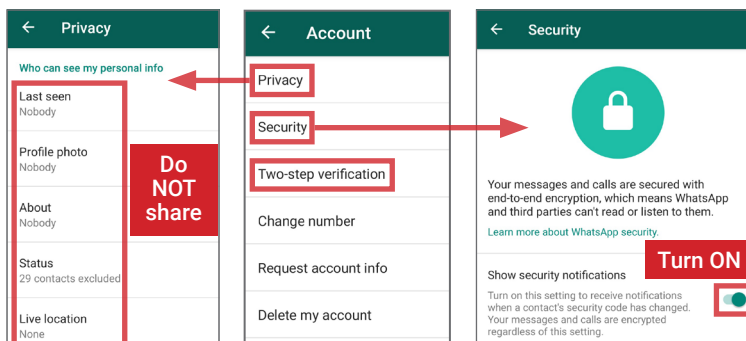
Visit **Settings > Chat > Chat backups** to disable video and chat backups.

To maximize security, go to **Settings > Account** and apply the following options**:**
- Under **Privacy,** set **Who can see my personal info** options to **Nobody.** Do not share your **Status** or **Live location** information.
- Under **Security**, enable **Show security notifications** to view changes in contacts' security codes.
- Enable **Two-step verification** to prevent outside access.
- Periodically delete all conversations.

SIGNAL

Signal supports end-to-end encrypted communication using Open Whisper System's Signal Protocol. iPhone users can only use Signal to communicate with other Signal users; Android users can contact anyone through the app, but messages with non-Signal users are unencrypted.

In 2018, Signal rolled out a unique **Sealed Sender** feature that also encrypts message sender/recipient information.[18] The app does not collect user metadata or automatically store messages when you backup your device.

Tap the "**...**" icon [upper right] to select **Settings > Privacy** and apply the following options:

- Enable **Screen Lock** and set the inactivity timeout to a short interval.
- Enable the **Screen Security** and **Incognito keyboard** features to limit opportunities for information collection.
- Under **Communication**, toggle on **Always relay calls** to ensure communications do not reveal your IP address.
- Under **Sealed Sender**, enable **Display indicators**
- Under **Signal PIN**, enable **Registration Lock.**
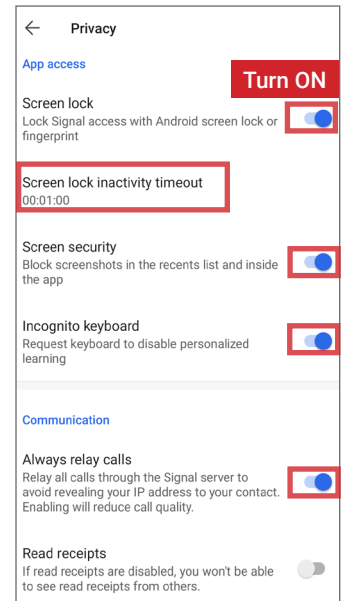
Visit **Settings > Storage > Clear message history** after each completed communication, or set **Keep messages** to 30 days. Never turn on chat backups.

GROUPME

GroupMe is a New York-based mobile messaging app launched in 2010 that was acquired by Microsoft in 2011.[20] GroupMe has 10.75 million active monthly users as of September 2019.[21] Users can register for an account by linking their existing Facebook, Apple, or Microsoft accounts, or with a phone number or email address. Participants in groups can receive and send messages over SMS without registering for a GroupMe account.

GroupMe has a simple settings interface with minimal security and privacy controls.

Navigate to **Settings** and toggle off **Send read receipts for DMs**. Next, tap your profile picture and:

- Enable **Use two-step verification**
- Turn off **Enable sharing**
- Never link your GroupMe to Facebook or Twitter

Note that GroupMe does not use encryption. As a result, user data collected through GroupMe is transmitted unencrypted and can be visible to unintended recipients. This means that the content of communications, as well as the membership and names of groups, can be disclosed to unintended parties.
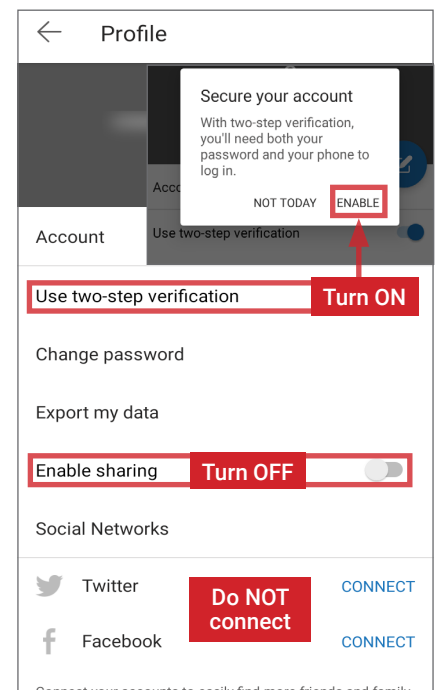
MOBILE WALLETS

MOBILE WALLETS - DO'S AND DON'TS

- Use all available PIN, password, and biometric protection options.
- Turn on notifications and regularly monitor transaction history for unauthorized payments.
- Only transfer money to people or merchants you know and trust, and establish a maximum transaction limit to prevent large purchases and transfers.
- Do not link your mobile wallet application to a social networking service (SNS) (e.g., Facebook, Twitter).
- Link a bank account only to cash-out; delete bank account information once the cash-out process has been completed.
- Before signing up, always research if a mobile wallet service provider has a good or bad track record in handling users' privacy and data.

WHAT ARE MOBILE WALLETS?

Mobile wallets allow you to link credit cards, debit cards, and bank accounts to complete one or both of the following transaction types:

- **User to friend**: Allows you to transfer money to a friend using their email address or phone number. Money is stored in a balance within the mobile application. You can use this balance for further transfers or deposit it into your bank account.
- **User to merchant**: Allows you to pay for goods and services online or at the point-of-sale using a QR code or near field communication (NFC) chip. You can pay by selecting a specific card, account, or existing balance, if available.

Most mobile wallets from different companies do not interact with each other; for example, you cannot transfer money from Google Wallet to a friend with Venmo. Given that different mobile wallets perform distinct functions, you may choose to maintain multiple wallets.

BENEFITS OF MOBILE WALLETS

Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile device.

On most smartphones, fingerprints can be used as a purchase authentication method, enhancing your security over a physical credit or debit card.

RISKS OF USING MOBILE WALLETS

Consolidating multiple cards into a single app increases your risk of exposure. Physically losing possession of your phone may allow an unauthorized user to make payments with any linked card or account. Unauthorized users will also have access to consolidated transaction logs, exposing a wide range of your financial habits and activities.

Most wallets are also accessible through a web browser. Although cards may physically be in your possession, unauthorized access to your online wallet account will expose your personal information and activity. It also puts your money at risk for theft.

Some mobile wallets offer social features, such as an activity feed of friends' transactions or the option to post transactions to Facebook. Without strict privacy settings, social features expose your activity and potentially even your whereabouts.

CHOOSING THE RIGHT MOBILE WALLET

You should consider the following questions when choosing a mobile wallet:

- What operating system do you have?
- Are you transacting with your friends or paying merchants?
- What security features do you require?
- Do you want social options? Do you want the ability to limit social options?

Six of the most popular mobile wallet services are outlined below.

SERVICE	OS	TRANSACTION TYPE	REQUIRED IDENTITY DATA	SECURITY OPTIONS	SNS LINKS	DEFAULT VISIBILITY
Cash App	iOS, Android	User to friend, User to merchant	Phone or email, full name, zip code, $Cashtag (unique payment name)	PIN	None	$Cashtag (can be hidden)
Pay	iOS	User to friend, User to merchant	Full name, billing address, shipping address, email, phone number, debit/credit card data	Fingerprint or face required for transactions	Send money directly to contacts using iMessages	None
G Pay	iOS (in-store payments not supported), Android, browser	User to friend, User to merchant	Full name, email, bank account, debit/credit card data	PIN, fingerprint	None	None
venmo	iOS, Android, browser	User to friend, User to merchant	Full name, email, phone number, bank account or debit/credit card data	Password, PIN, fingerprint	Facebook (optional), internal social features	Friends (can set to private)
PayPal	iOS, Android, browser	User to friend, User to merchant	Nationality, full name, email, address, phone number, bank account data or credit/debit card data	Password, fingerprint	None	Private

SQUARE CASH APP
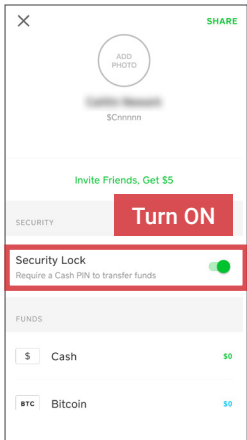
Navigate to **Settings** in the upper left portion of the home screen:

- Require **Security Lock** to transfer funds.
- Under **Personal,** add your **Email Address** or **Mobile Number** for account verification.
- Under **Notifications**, enable **push and email notifications**.
- Under **Privacy, toggle Cash.me** to **OFF.**

Users can link cash to a custom Visa debit card available through the app, or purchase/sell Bitcoin to use in transactions. An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

APPLE PAY (IPHONE ONLY)
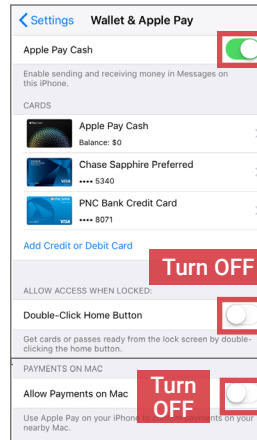
In the iPhone **Settings** > **Wallet & Apple Pay** menu, add/remove credit or debit cards you wish to use with Apple Pay.

- **Toggle Apple Pay Cash ON** to enable direct money transfers with your contacts.
- **Turn OFF Double-Click Home Button** to limit access to Apple Pay when your phone is locked.
- **Turn OFF Allow Payments on Mac** to minimize risks of an unauthorized person making a purchase on your computer.

Enable both PIN and fingerprint/face ID protections for your iPhone's lock screen. Use both options to ensure extra security.

GOOGLE PAY

Navigate to your **Google Account** (circular icon, upper right corner) > **Security > Signing into Google > Google Account PIN** to create a PIN to approve purchases and complete transactions in G Pay. Also enable **2-Step Verification**.

In the G Pay app:
- Navigate the dropdown menu to **Settings > Sending money** and **toggle ON Require a confirmation** to enable your **PIN** during transactions, or enable **Fingerprint.**
- Under **Settings > Notifications,** turn **ON** notifications for purchases and transactions.

Android users: Navigate to **Google Pay Settings > General > Location Settings** and **toggle OFF Use location**.

iPhone users: Navigate to your phone's **Settings** > **Privacy** > **Location Services** and set Wallet location access to **Never**.
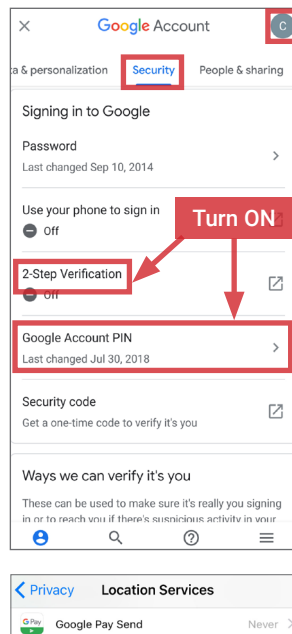
VENMO

Navigate the dropdown menu to **Settings > Account**:

- Under **Privacy**, select **Private**.
- Navigate to **Notifications > Push Notifications** and enable push notifications for all **Payments** and **Activity** options.
- Under **Friends & Social**, do not connect Facebook or Phone Contacts.

Under **Settings > Security:**
- Enable **PIN Code & Fingerprint.**
- Review **Remembered Devices** regularly to check for suspicious log-ons.
- Complete the one-time **Identity Verification** process to help prevent fraudulent use of your account.
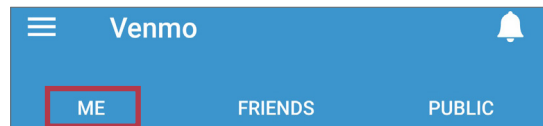
Monitor your transaction activity by selecting the **ME** tab at the top of the home screen.
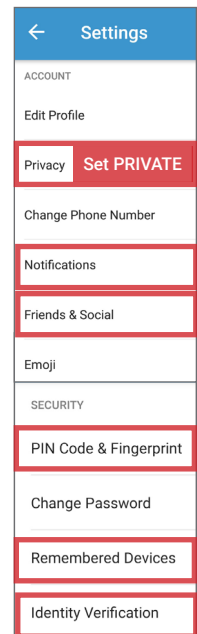
PAYPAL

Log in to PayPal using your browser and navigate to **Settings > Account:**
- Do not provide SSN or Passport numbers.

In **Settings > Security**:
- Configure **Security questions** and **2-step verification.**
- Keep the **One Touch for auto login at checkout** feature turned OFF.
- Monitor **Permissions you've given** to apps and sites you use, and remove unnecessary access.
- Review account **Activity** routinely to monitor for suspicious activity.

Under **Notifications**, enable all **Payments** notifications.

> **Security questions**
> For your protection, please choose 2 security questions. This way, we can verify it's really you if there's ever a doubt.
> **2-step verification**
> Add an extra layer of security to your account by using a one-time security code in addition to your password each time you log in.
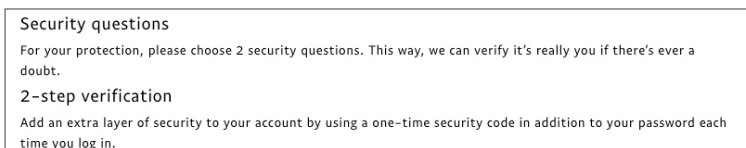
In the mobile app: Under **Settings > Login and Security**, **toggle OFF Stay logged in for faster checkout** to prevent account information from being accessed prior to login. PayPal can now be linked with Google Pay.

MOBILE WALLETS - BEST PRACTICES

To protect yourself while using mobile wallets, use the following guidance:

- Avoid accessing mobile wallets on public Wi-Fi networks.
- Use privacy settings to restrict the social features of mobile wallets, so only you can see account activity.
- **Turn ON** transaction alerts to receive email or text notifications of any transaction.
- Routinely review your transaction history to check for any unusual activity.
- Only provide personal or financial information that is required for mobile wallet use.
- Restrict permissions to your device contacts and settings.
- When possible, set transaction limits (e.g. $100) to prevent large unauthorized transfers from your account.
- Never send or receive money from strangers or unverified accounts.

ONLINE DATING SERVICES

ONLINE DATING SERVICES - DO'S AND DON'TS

- Do not link online dating profiles to your social networking or photo sharing services (e.g., Facebook and Instagram).
- Avoid using usernames and profile photos that appear on other social networking services (SNS).
- Do not include information unique to you (e.g., last name or place of work) in your public profile data or messages.
- If possible, upgrade your account to a paid version; paid accounts often offer more control over who can see your profile and what data is visible.
- Always read and take the time to understand the site's Terms and Conditions before agreeing to register an account.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

OVERVIEW

Online dating services and apps are used by individuals looking to develop a personal or romantic relationship with others. While each service is unique, dating platforms typically ask users to maintain a public profile containing photos of themselves and personal information. Profiles are often searchable through the site and, at times, may be pushed to users who share common interests or locations. User data may also be featured in online ads or social networking sites (SNS). If you join a dating service, use the recommendations in this chapter to help protect your online dating profiles and associated personal data.

COMMON THREATS FROM DATING SERVICES

Dating services and apps present unique threats to users in comparison to other SNS. Dating sites encourage interactions between unacquainted individuals, collect extensive personal information that is used to match compatible individuals, and have few methods of verifying the accuracy of users' claims. Before participating in online dating, consider the following threats to your personal data:

- Services often use detailed questionnaires to pair like-minded individuals, allowing the services to collect targeted information about users' lifestyles.
- Many services encourage users to connect an SNS to their profile or require them to supply face photos to help verify the account's legitimacy.
- Matches may request personal contact information (e.g., phone number or SNS) and wish to communicate outside the dating service platform.
- Catfishing—a form of social engineering that uses a fake online persona to glean information from unsuspecting, real individuals—is common among dating services and can lead to identity theft, financial exploitation, character defamation, and other online scams.

SELECTING A DATING SERVICE

Dating services are designed to pair individuals based on common interests, values, lifetime achievements, lifestyles, or other personal factors. As a result, users often divulge more personal information within a dating service than they would feel comfortable sharing on other social networking services (SNS) such as Facebook. Prior to registering an account, examine the types of data collected by each dating service of interest, research how the service works, and consider any ways in which the service links to your other online profiles or personal devices (e.g., smartphone permissions). Then select the service that best fits your privacy needs.

REGISTRATION

Dating services ask users to provide varying degrees of personal information in order to set up and begin using an account. Research what types of information will be requested during registration, and take the following steps to help protect your overall online privacy:

Phone number: If possible, register with a secondary mobile or electronic phone number rather than your primary number. This will help limit linkages between your dating account and other online accounts.

Email address: Create a unique email address for each dating account you register. This will help limit linkages between your dating account and other online accounts.

Username: Usernames should not represent your true name or include numbers related to your identity (e.g. your birth date). Select a unique username that is distinct from any other account you have registered online.

Questionnaires: Many dating services ask users to answer questions in order to be matched with potential partners. These are important for the service's functionality, but may request highly personal or sensitive information. Use discrimination when completing questions and, where possible, avoid providing highly detailed answers.

Example question:

> Should the government require children be vaccinated for preventable diseases?

Device Permissions: Limit dating app device permissions at first use.

PROFILE DATA

The examples below display optimal ways to populate common identity fields requested as part of a user profile. Limit publicly visible profile information wherever possible. Note that some dating services provide more granular privacy controls as part of a paid account subscription.

Name: If permitted, do not provide your full name, or opt to use an abbreviated display name.
- Jennifer Vident (Use "Jen" or "Jen V.").

Email address: Create a unique email address for each dating account.

Biographical details: Provide high-level biographical details.
- Job: Media analyst (Use "Consultant").
- Education & Degree: Consider omitting these fields if you attended a small school or hold an uncommon degree (these details make it easier for people to research you online).

Location: Select a large metropolitan area or nearby zip code instead of your home location.
- Hackensack, NJ (Use "New York, NY").

Photos: Many dating services require at least one face photo. For additional photos, select ones that do not clearly show your face or distinguishable landmarks near your frequent locations. Use unique photos that don't appear in your other online accounts.

USING DATING SERVICES

Dating services employ a variety of methods to pair users, including: analysis of questionnaire responses, user location, mutual SNS connections, or mutual profile interest. It is common for users to try multiple dating services. Be sure you understand how your selected service(s) work, and to track any changes in how your services operate. Consider the following usage tips:

- Always examine a service's **privacy and account security settings** before you engage with matches. Many services offer website and app access; settings can vary depending on the interface. Dating apps are likely to require specialized device permissions (e.g., Location, Media storage) that should be restricted unless the app is in-use.
- Services typically provide a way to digitally communicate with matches. Consider using **in-service communication tools** to thoroughly vet matches before disclosing personal contact information. Never share personal information such as your home address or financial account data online.
- Use caution when selecting a dating service that operates as part of a SNS (e.g., Facebook Dating). These services link to one or more of your SNS profiles and can expose a greater degree of personal data.
- Dating services may offer the ability to increase your profile's visibility across the dating platform, linked SNS, or the Internet, by allowing your profile to be used in ads, or by paying an additional fee. Do not use these features.
- **Suspend or deactivate** your dating service profile when it's not in use.
- **Delete** your data and account when the dating service is no longer needed, and uninstall the dating app from your device. If needed, search the service's help or FAQ sections for instructions on permanent account deletion.
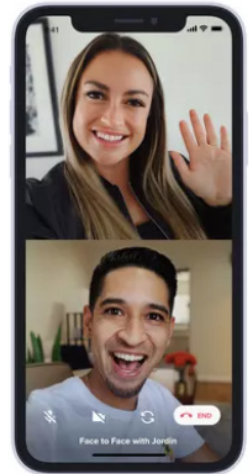
The following sections examine two dating services in order to illustrate the variety of features and privacy settings available to users. Readers are encouraged to look for and configure similar settings in whatever dating services they use.

BUMBLE

Bumble is a location-based dating service that pairs users with potential romantic matches or friends. Bumble includes a photo-verification process to ensure users match their profile pictures.

Opt to register with Bumble using a secondary phone number rather than your Facebook account. Do not connect your Instagram, Spotify, or other online accounts.

Navigate to your **Profile** and tap the **pencil icon** [lower right of your profile photo] **> Edit profile** to view and adjust your profile information, following the recommendations provided in the Profile Data section. Ensure you are comfortable with what profile information is shown to other users.
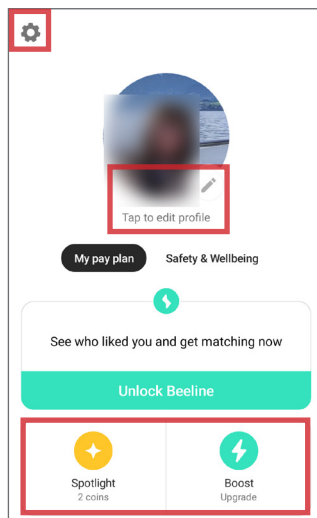
Navigate from **Profile** > **gear icon** [upper left] to access your **Settings**:
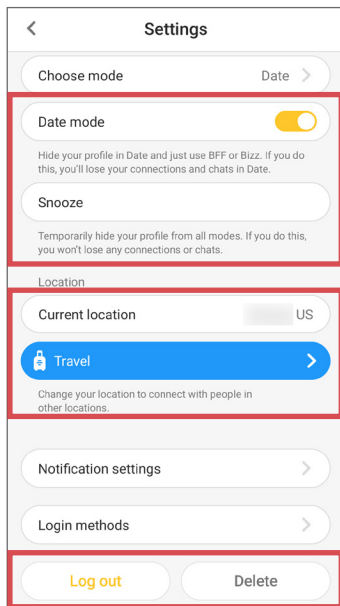
- Use the **Date mode** or **Snooze** features to temporarily hide your profile when you are not actively using the service.
- Remember that your **Current location** reveals your whereabouts. Consider using the **Travel** feature to set your location to a nearby city or zip code rather than using your home location.
- Scroll to the bottom of the Settings screen to **Log out** or **Delete** your account when it is no longer needed.

Do NOT use the **Spotlight** or **Boost** features offered on the Profile screen; these increase the visibility of your profile in a manner you cannot fully control.

TINDER
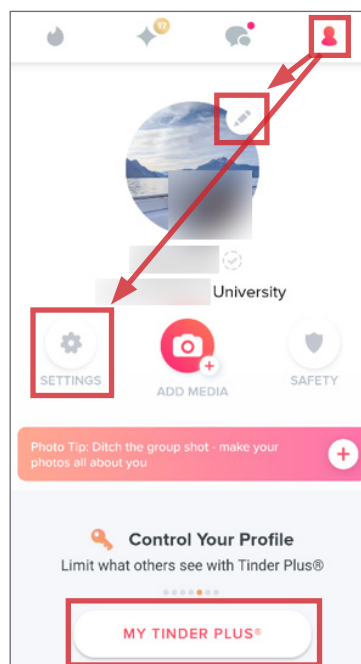
Tinder is a dating service that pairs users with potential romantic matches using location, mutual social networking service (SNS) connections, and common interests.

Register with Tinder using a secondary phone number rather than your Facebook or Google account. Do not connect your Instagram, Spotify, or other online accounts.

Tap the red avatar icon [upper right] to navigate to your **Profile**. Tap the **pencil icon** [upper right of your profile photo] to view and adjust your profile information, following the recommendations provided in the Profile Data section. Ensure you are comfortable with what profile information is shown to other users.

Navigate from **Profile** > **Settings** [gear icon] to access **Settings**:

- Remember that your **Location** reveals your whereabouts. Adjust **My Current Location** to a nearby city or zip code rather than using your home location. Consider adjusting your device permissions to only grant Tinder access to your location when using the app.
- **Toggle OFF Show me on Tinder** to temporarily hide your profile.
- Scroll to the bottom of the Settings screen and select **Delete Account** when it is no longer needed.
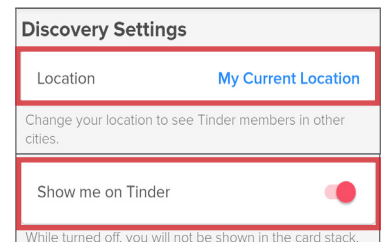
Tinder offers additional privacy controls through the at-cost **My Tinder Plus** subscription. This subscription allows users to control who sees their profile (e.g., only people the user has liked), and to limit the visibility of their age and location data.

PHOTO SHARING AND STORAGE

PHOTO SHARING AND STORAGE - DO'S AND DON'TS

- Only share photos with people you know and trust. Assume that ANYONE can see, save a copy, and forward photos you post online.
- Ensure your family and friends take similar precautions with their photos; their privacy settings can expose you to unwanted parties.
- Avoid posting or tagging images that clearly show your face. Select pictures of yourself taken at a distance, at an angle, or wearing sunglasses.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.
- Remove EXIF (Exchangeable Image File Format, or photo metadata) and location data from the photos you upload whenever possible.
- Limit the visibility of the photos to only your account or to accounts that you approve individually.

OVERVIEW

Photo sharing services (PSS) are online photo albums that store, organize, and share your digital photos; many social networking services (SNS) such as Facebook and Twitter also function as photo sharing services. PSS provide a convenient way to share photos, but can expose you to privacy risks if you do not take proper precautions. This chapter explains how you can control the security settings of six popular photo sharing services to protect your privacy.

SERVICE	PRIMARY USE	PRIVACY OPTIONS?	SHARE EXIF?	LOCATION OPTIONS	ALLOW REPOSTING?	GOOGLE INDEXED?
Snapchat	Share temporary photo & video messages known as "Snaps"	Everyone, My Friends, Custom	Yes	User location tracked by default; disabled with Ghost Mode feature	No	No
iOS Photos	Organize and share photos from Apple devices	Private (able to share album/images)	No	Locations on photos tracked by default; no option to remove info	No, but photos can be downloaded once shared	No
Google Photos	Automatically back up, organize, share photos from smartphones	Private (able to share albums/images and tag your Google contacts)	Yes	Can tag location to photos; geolocation tracking if enabled	No, but photos can be downloaded once shared	No, but the service is owned by Google
flickr	Share photos within grouped user environments	Public, Private, Contacts, Family, Friends	Yes	Can tag location to photos, can embed location in EXIF data	Yes	If Public (can opt out)
imgur	Share and comment on photos	Public, Hidden (images viewable with direct URL), Secret	No	None (can add location to photo description)	Yes	If Public
Pinterest	Share concepts and ideas using images	Public, Private (with Secret Boards)	No	None (can add location to photo description)	Yes	If Public (can opt out)

SNAPCHAT

Snapchat allows users to send temporary photo and video messages ("Snaps") to one another. Snaps can only be viewed once by the intended recipient(s) and are set to expire within 1 and 10 seconds.

Tap your profile photo icon and then **Settings > Who Can...**:

- Set **Contact Me** to **My Friends**.
- Limit **View My Story** to **My Friends** or **Custom**.
- Tap **See My Location**. Turn on **Ghost Mode** and toggle OFF **Allow friends to request my location**.
- Tap **See Me in Quick Add** and toggle OFF the box to avoid being recommended as connection to other users.
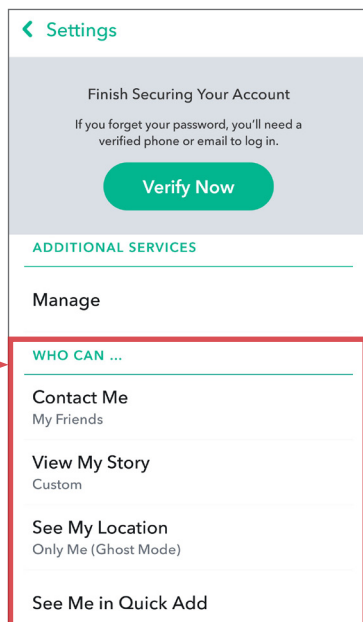
Under **Additional Services** > **Manage** > **Maps**, toggle OFF **Share Usage Data**.

IOS PHOTOS

iOS Photos is an intelligent photo organizer and sharing tool exclusively for Apple users. It is the default photo app on all iOS devices and comes pre-installed on Macs, iPhones, and iPads. It cannot be removed or uninstalled.

iCloud Photo Sharing is a feature allowing users to create private albums from photos and share with their contacts. To share photos from your Apple device, navigate to **Settings > Photos**:

- **Shared Albums**: Toggle ON.

When photos are shared with contacts who do not use iCloud, the app creates a link to a public website with the shared photos which anyone can see and access. Users can also post to SNS, messengers, and other photo sharing apps directly from iOS Photos.
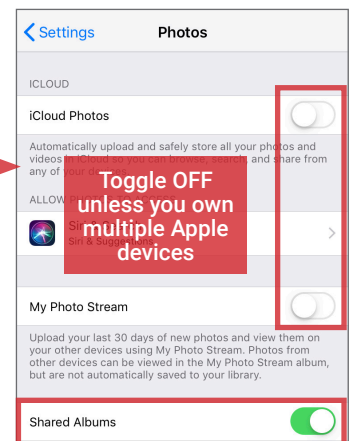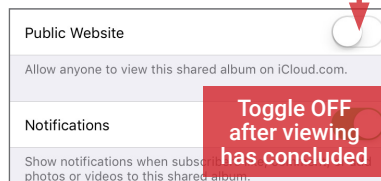
iOS Photos doesn't provide a privacy control for managing location data in photos. If you are concerned, process your photos through EXIF removal tools (see pg. 26-27) before sharing them.

PINTEREST

Pinterest is a site where users can upload, categorize, and share images called Pins on dedicated pages called Pin Boards. To maximize your privacy on Pinterest, make the following modifications to your account settings.

Go to ⋯ > **Edit settings > Account Basics** and make the following changes:

- Under **Search privacy**, toggle ON **Hide your profile from search engines**.

Under **Personalization**, toggle OFF the following selections:

- **Use sites you visit to improve which recommendations and ads you see**: toggle OFF.
- **Use information from our partners to improve which recommendations and ads you see**: toggle OFF.

Search privacy
🔴 Hide your profile from search engines (ex: Google). **Learn more**

Personalization
⚪ Use sites you visit to improve which recommendations and ads you see • Learn r
⚪ Use information from our partners to improve which recommendations and ads yo

Search history
Clear Recent Searches Remove things you've recently searched for from search
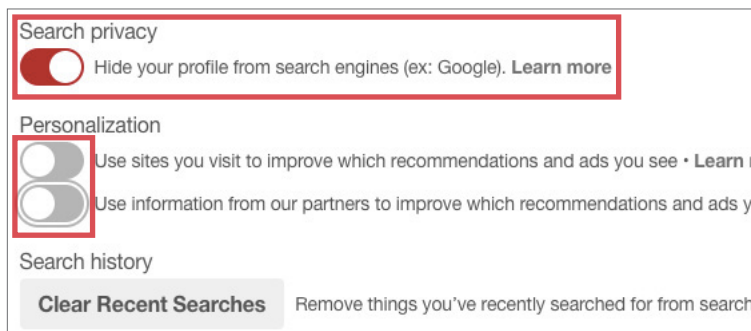
When you make a new Board in Pinterest, toggle the **Secret boards** option ON to keep your pins private.

Name | **Privacy Concerns**

Secret
Learn more 🔴 | **Toggle ON**
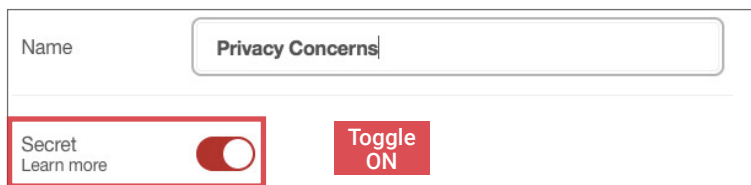
IMGUR

Imgur allows users to share photos or albums with anyone using a customized URL and easily post their photos to other sites such as Reddit and Facebook. By default, Imgur strips all EXIF data from the photos you upload. However, you still need to make a few modifications to your account settings to maximize privacy.

Hover over your username (top right) and select **Settings** from the drop down menu to make the following changes:

- When creating a new album, select **Hidden** to make albums accessible by URL only, or **Secret** so album is visible only to you.
- **Comment mentions**: check this box to receive notifications when you are mentioned in a comment.
- Use the **Security** tab to review account activity sessions.

Create an album
Album Title (optional)
Select Hidden or Secret to maximize privacy
Alb
⚪ Public ⚪ Hidden ⚪ Secret
This album is hidden from your account page, but is still accessible with the direct URL.

Current sessions
Current or recently active sessions involving your account. Sign out o password, or contact support.
● 50.110.235.148
Chrome 67.0.3396.99 on Windows
sign out
● Imgur Desktop Site 📱
Security log
Important events involvi **Monitor Activities**
Action
7 minutes ago logged in (with password)

FLICKR

Flickr, acquired by SmugMug in April 2018, supports 90 million monthly active users.[23] It offers free and paid accounts for photo sharing and editing. To maximize your privacy, click your avatar in the upper right corner and select **Settings** from the drop down menu. This takes you to the **Account settings** page.

Make the following changes under the **Privacy & Permissions** tab for **Global settings** and **Defaults for new uploads**:

Global settings	
Who can download your images (including originals)?	Only you
Largest shared image size	Best display size
Allow others to share your stuff	No
Who can add you to a photo?	Only you
Allow your stuff to be added to a gallery [?]	No
Hide your EXIF data [?]	Yes
Hide your stuff from public searches [?]	Yes, on flickr.com and 3rd-party sites
Hide your profile from public searches	Yes
Who can see what on your profile	• Email address: Only you • Real name: Your friends and family (• Current city: Your friends and family (n/a) Edit your IM names, real name, or current city

Under the **Sharing & Extending** tab, do NOT connect your account to SNS.

Personal Information | Privacy & Permissions | Emails & Notifications | Sharing & Extending
Share Flickr photos to other sites
Post from Flickr directly to Facebook, Twitter, your favourite blogs and more. Just set up a connection between Flickr and your favourite services, and voilà!
📘 Facebook — connect
🐦 Twitter — connect
📋 Tumblr — connect
Do NOT connect
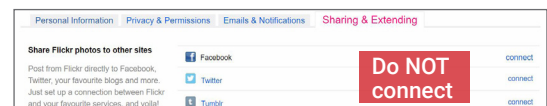
GOOGLE PHOTOS

Google Photos, the default photo app on Android devices, is a photo sharing, storage, and organizational tool with more than 1 billion active users.[22] It seamlessly connects with Gmail to allow easy online photo sharing via albums and public URLs. In addition to location tagging, Google Photos uses face recognition to group similar faces and encourages photo organization by faces contained in the photos.

Make the following changes to your account settings to minimize the degree of personal data shared and collected by Google, and maximize your privacy. Open the Google Photos app on your smartphone or browser and navigate to **Settings**:

- Go to **Group similar faces** and **TURN OFF** face grouping.
- Under **Sharing,** turn ON **Remove geo location**.
- Under **Google Apps**, select **Google Location settings** and turn OFF **Use location**.

Google Location settings
Photos uses location info to improve your experience, like auto organization & search
Turn OFF

Remove geo location
From photos & videos that you share by link, but not by other means 🔵
Turn ON

Turn off face grouping?
All face groups for your favorite people will be removed
KEEP ON | **TURN OFF**

EXIF DATA REMOVAL

EXIF DATA

Exchangeable Image File Format (EXIF) is a standard format for storing and exchanging image metadata. Image metadata is included in a captured image file and provides a broad range of supplemental information. Some social networks and photo-sharing sites, such as Flickr, Google Photos, and Instagram, have features that share EXIF data alongside images. Others, including Facebook and Twitter, do not share EXIF data but may utilize the information internally. EXIF data is stored as tags, some of which reveal unique identifying information.

CATEGORY	IMPORTANT TAGS	IDENTITY IMPLICATIONS
Geolocation	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photo sharing sites, including Google Photos and Flickr, publicly display image GPS coordinates on a map.
Timestamps	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
Camera	Make, Model, Serial Number	A unique serial number identifies the device used to capture an image or sets of images.
Authorship	Artist, Owner Name, Copyright	Links images with a name or organization.
Image Summary	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about those captured in the image by providing additional content regarding persons and locations.

Limiting EXIF data, especially geolocation information, before distributing image files can help protect your identity from overexposure. This should be done in two stages: 1) preventing your smartphone from storing the identifying EXIF data in image files, and 2) removing existing EXIF data from image files using an EXIF removal application.

PREVENTING THE CAPTURE OF GEOLOCATION DATA

- Taking a screenshot of a photo from a phone running an operating system newer than iOS 7 or Android Jelly Bean will create **a brand new image that contains no EXIF data**. To take a screenshot on an iOS device, simultaneously press the lock and volume-up buttons; with a Galaxy or Note, press the power and home buttons simultaneously, or swipe your hand from left to right across the screen; with a Google Pixel, simultaneously press and hold the lock and volume down buttons for 2 seconds.
- Turn off geolocation data capture using your smartphone's camera application [shown below]. Note that photos taken in airplane mode still contain geolocation data.
- When uploading or sharing photos, remember that EXIF data and image quality have no correlation. Lower quality images still contain EXIF data.

IOS (V. 14.3)

Turn off iOS location services to ensure images captured with the native iPhone camera app will not contain any geolocation EXIF data.

1. Select the **Settings** app and navigate to **Privacy** > **Location Services.**

2. Turn off location services altogether, or disable location specifically for the iPhone's Camera application.

3. Return to the **Settings** app and navigate to **Privacy** > **Photos**.

4. Disable permissions for other apps to access photos already stored in your iPhone's Camera Roll by setting to **None** or **Selected Photos**. Do not allow third-party apps access to all photos.
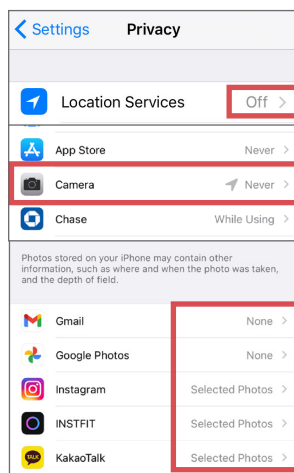
ANDROID (V. 11)

Turning off location storage in the Android Pie camera application prevents captured images from containing EXIF data.

1. Open the **Camera** app and select the down-arrow icon [top center] to access the camera menu.

2. Tap the **white gear icon** [bottom right] to access **Settings**.

3. Under **General**, toggle OFF **Save location**.
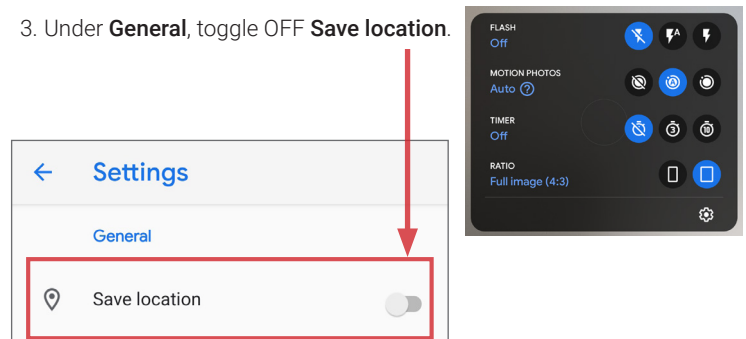
EXIF REMOVAL SOFTWARE

Several EXIF removal software applications and programs exist. Some are free and some charge. The following are examples of how the programs work.

EXIF VIEWER LITE BY FLUNTRO

EXIF Viewer LITE is a free, iOS app where you can view, delete, and edit EXIF data of images stored on your Apple devices. The app can also remove or edit EXIF data on multiple photos at once. The full version of the EXIF Viewer is available for purchase.

Toggle OFF Overwrite setting and toggle ON Delete Original image after creating to permanently delete EXIF
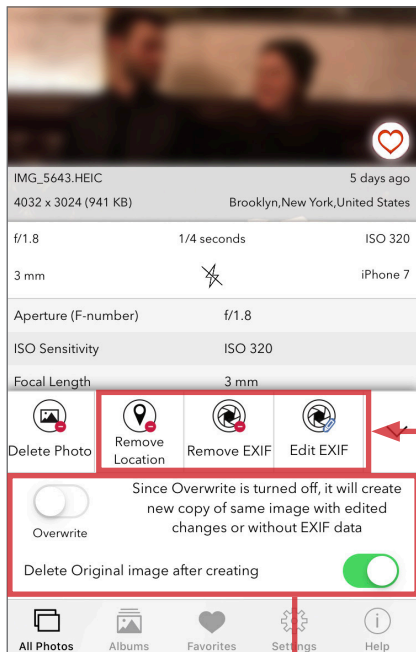
1. Download the EXIF Viewer Lite from the **App Store.**

2. Open the NoLocation app and select photo(s) to view all their available EXIF data. From here, you can:

   • Select **Remove Location** to quickly remove location data on your photos. Other EXIF data will be preserved.

   • Select **Remove EXIF** to strip all the available EXIF data from your photos.

   • Select **Edit EXIF** to change the EXIF data on your photo by editing its date, time, and location.

3. Finalize changes by approving the app to make changes to your photos.

PHOTO EXIF EDITOR - METADATA EDITOR

Photo EXIF Editor - Metadata Editor is one of several free apps that deletes EXIF data from image files stored on your Android devices.
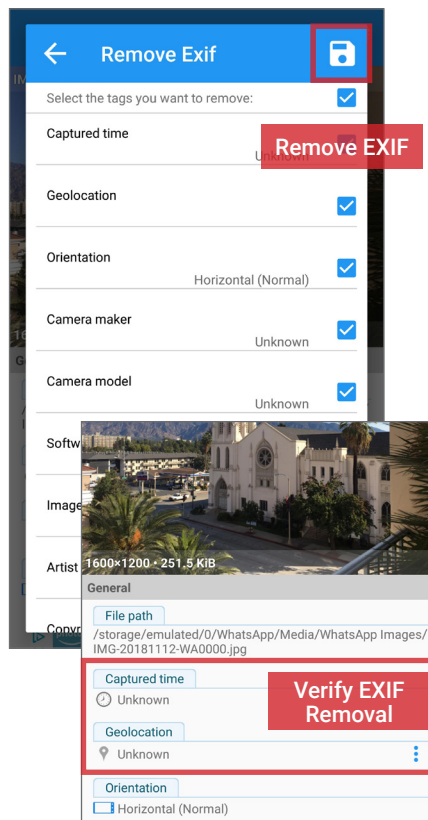
1. Download Photo EXIF Editor from the **Play Store** and allow media access permissions.

2. Open the Photo EXIF Editor app and select **Photos**.

3. Navigate your device gallery and select an image.

4. Tap the EXIF Erasure icon on the upper right corner, select all tags for removal, and tap the save icon. Scroll down to review whether EXIF data has been removed; you can make manual adjustments to certain fields if desired.

5. An EXIF-free image file with an updated date and time stamp will be saved in place of the original, which can then be shared using your Gallery or SNS apps.

VIEWING AND REMOVING EXIF DATA ON OS X

Use the **ImageOptim** application (available at http://imageoptim.com) to remove EXIF data on your OS X computer.

1. Open the ImageOptim application.

2. Drag the photos selected for EXIF removal into the application window and wait for a green check mark to appear next to the file name.
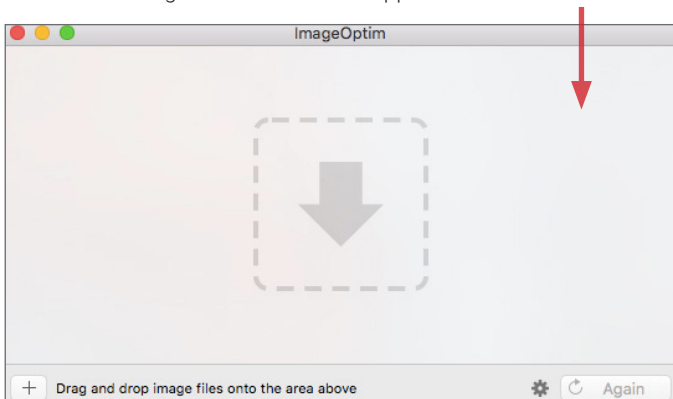
3. Check that the EXIF data has been removed by right-clicking the image and selecting **Get Info**. EXIF data is listed under **More Info**.

VIEWING AND REMOVING EXIF DATA IN WINDOWS

Use the Windows 10 operating system on your computer to verify EXIF data has been successfully removed.

1. Navigate to an image in File Explorer, right-click the image, and select **Properties**.

2. In the **Properties** window, select the **Details** tab.

3. Most EXIF data, including geolocation, can be located in the **Details** tab if they are embedded inside the image file.

4. Windows 10 also allows system administrators to remove all EXIF data from the selected image by clicking the **Remove Properties and Personal Information** link.
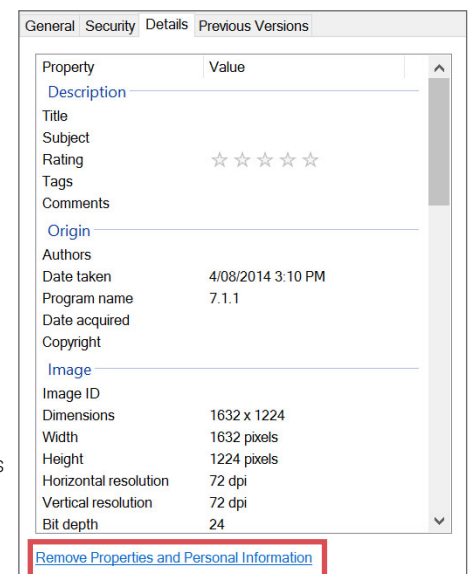
VIDEO COMMUNICATIONS

VIDEO COMMUNICATIONS - DO'S AND DON'TS

- Determine the features you need. Video communication services range from free smartphone apps to full-featured enterprise subscription systems.
- Video communications services are not considered secure for transmitting sensitive data. Use discretion when sharing information via video calls.
- Evaluate the security and privacy features offered by each service you use. Configure settings to limit how much of your personal data is shared.
- Prevent strangers from being able to discover your phone number or profile by implementing the most restrictive privacy settings after signing up.
- If possible, do not link your video communications accounts to social networking services (SNS).
- Ensure your friends and family members take similar precautions; their video calling behavior can expose your personal data.

WHAT ARE VIDEO COMMUNICATION SERVICES?

Video communications services transmit real-time video data between users using cameras (e.g., a webcam or smartphone), device microphones, and a Wi-Fi or cellular network connection. They are increasingly popular for personal communications, as well as for use in remote work and educational settings. Many are available for free, while several offer premium features (e.g., call recording) with paid subscriptions. Video communications services support three general use cases:

- **User to use**r: An individual video calls another user. Popular services include FaceTime, Viber, and Skype.
- **User to group (group calls):** An individual video calls several users. Popular services include Zoom, Google Meet, and MS Teams.
- **User to public (live streaming)**: An individual streams a live video feed to a wide audience, typically via a social networking service (SNS) or streaming service. Popular services include YouTube Live, Periscope, and Twitch.

BENEFITS

Video communications services offer users:

- A low- or no-cost method for keeping in touch (when used over Wi-Fi).
- An engaging communication experience that includes audio data, visual data, and rich media elements such as photo-sharing, file-sharing, GIFs, and emojis.
- Numerous service options with specialized features such as video call encryption, call screening, and call recording.
- The ability to use one account across multiple devices (e.g. personal laptop, smartphone, and tablet).

DISADVANTAGES

Video communication services present several potential disadvantages:

- Video communications require charged/functional hardware and an Internet or cellular network connection.
- A poor network connection can result in low-quality video calls.
- Using additional security features such as call encryption may lower performance.
- Video communications conducted over cellular networks may result in high data usage and account overages.
- Callers and recipients typically must use the same service.
- Video communications services do not typically connect to traditional mobile numbers or emergency services.
- Video communications services are subject to bugs, disruptions, and malware that may impact service quality.

USING VIDEO COMMUNICATIONS SERVICES

The table below outlines common vulnerabilities and related best practices for using video communications services. The following page outlines a selection of common services in order to further illustrate the variety of security features and privacy settings available for consumers.

VULNERABILITY	BEST PRACTICES
Services may track, store, and share your data with third parties (e.g., advertisers). Your service usage behavior can be used to profile you.	• Review a service's privacy policy and terms of service prior to first use and after any updates. • Only grant necessary device access permissions. • Limit services from saving data to your device. • If possible, avoid linking your SNS or other online accounts. Video calls conducted through SNS (e.g., Facebook Messenger) may collect gratuitous amounts of user data.
You can be contacted by strangers or spam accounts.	• Set your account to private and limit the ways others can look you up (e.g., via email address). • Turn on call screening, and only accept video calls from people you know.
Your account can be hacked.	• Password-protect your accounts and enable to two-factor authentication if possible. • Promptly install security and service updates. • Monitor where you're signed in to check for unauthorized access. • Periodically delete your conversations and remove unnecessary contacts. • Always deactivate or delete your account when it's no longer needed.
Unwanted parties can join or snoop on your call.	• Use end-to-end call encryption, if possible. • Set a meeting password for your group calls and lock the call once all participants have joined. • Verify contacts' identities prior to engaging with them.
Your video calls may leak sensitive personal data including your face, voice, and surroundings (including cohabitants and personal space).	• Be mindful of your surroundings when engaging in video calls. • Limit background exposure of your personal spaces, or use a virtual background. • Remember that bugs or glitches can reveal your private communications. Video content can be recorded; use discretion when sharing sensitive information.

CHOOSING A VIDEO COMMUNICATIONS SERVICE

The table surveys some of the popular video communication services. They are included in this book to illustrate the variety of features and privacy settings available for consumers.

SERVICE	COMPATIBLE OS	BEST USES
Skype	iOS, Android, macOS, Windows, web	File sharing, screen sharing, document collaboration, video calls
MS Teams	iOS, Android, macOS, Windows, web	File sharing, screen sharing, document collaboration, video calls for enterprises
zoom	iOS, Android, macOS, Windows, Linux	Encrypted group audio/video meetings and calls, live streaming video, screen sharing (web)
Google Meet	iOS, Android, web	Encrypted one-to-one or group audio/video calls, live streaming video, screen sharing (web)
FaceTime	iOS, macOS	Encrypted audio calls, video calls, and messages; voice memos
Rakuten Viber	Android, iOS, Linux, macOS, Windows, Linux	Encrypted audio calls, video calls, and text messages; group chat up to 250 people.

ZOOM CLOUD MEETINGS

Settings

BASIC

Meeting

Contacts

Chat

General

My Profile

Profile Photo

Account   @gmail.com

Display Name   Caitlin

Personal Note   Not Set

Update Password   **Leave these fields blank**

Department   Not Set

Job Title   Not Set

Location   Not Set

Use Fingerprint ID

Navigate to **Settings** [wheel icon, lower right. Under **My Profile**:
- Do not complete any optional fields. Do not add a profile photo.
- Scroll to the bottom and **toggle ON Use Fingerprint ID** if available.
- Use the **Sign Out** link at the end of this screen when you are no longer using the app.

Under **Meeting**:
- Set your default microphone and video settings as shown at the right.
- Scroll down and select **Keep Virtual Background For All Meetings.**

Navigate to **Contacts > Phone Contacts Matching** to disable this feature.

Meeting Settings

Auto-Connect to Audio   Off *

Always Mute My Microphone

Always mute my microphone when joining a meeting

Always Turn Off My Video

Always turn off my video when joining a meeting

Mirror My Video   **Toggle ON**

Always Show Video Preview

Always show video preview dialog when joining a video meeting

SKYPE

Sign out

Caitlin
My Microsoft account

Invisible

Share what you're up to

Bookmarks

MANAGE

Skype profile

Skype to Phone
Call phones at affordable rates

Skype Number
Get a second number

Settings

Privacy

SEARCH

Appear in search results

Tap your profile icon:
- Do not add a profile picture.
- Set your activity status to **Invisible**.
- Do not share a status.

Settings

Account & Profile

General

Appearance

Calling

Messaging

Notifications

Contacts

Under **Settings,** navigate to:
- **General** and toggle OFF Share location with Bing
- **Calling** and **toggle OFF Answer incoming calls automatically**
- **Messaging** and toggle OFF Read receipts

Next:
- Navigate to **Settings > Contacts** and **toggle OFF** Sync your contacts.
- Navigate to **Contacts > Privacy** and **toggle OFF Appear in search results.**

FACETIME

+1 (714)   **Choose ONE**

@gmail.com

FaceTime Live Photos

Navigate to **Settings** > **FaceTime**.

- Choose how others can reach you on FaceTime. Only enabling one option.
- **Toggle FaceTime Live Photos** to **OFF.**

GOOGLE MEET

Google Meet is a feature of your Google account and offers few specialized settings. Refer to the **Google Account** chapter for more information on how to control personal data in Google's environment.

Adjust your **device permissions** to allow Meet to take pictures and record video when the app is in use.

Navigate to the **three-bar icon** [top left]. Under **Settings, toggle OFF Send more diagnostic info** to limit information-sharing with Google.

Google Meet

Settings

Send feedback

Help
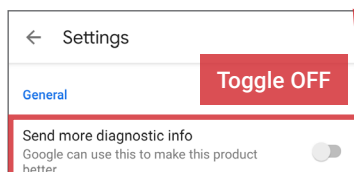
Allow Meet to take pictures and record video?

While using the app

Only this time

Deny

Settings   **Toggle OFF**

General

Send more diagnostic info
Google can use this to make this product better.

VIRTUAL PRIVATE NETWORK (VPN)

VIRTUAL PRIVATE NETWORKS (VPN) - DO'S AND DON'TS

- Select a VPN provider that allows you to protect multiple devices; some services limit the number of devices you can run on a single private network.
- Review your VPN Terms of Service (ToS) thoroughly to ensure your web traffic, stored data, and personally identifiable information (PII) are protected.
- Monitor your Internet speeds after connecting to a VPN; overburdened VPN servers can slow connections.
- Enable the kill switch option of your VPN service; whenever you are disconnected from a server, Internet is also disconnected as a safeguard.
- Before making your selection, always research whether a VPN provider has a good or bad track record in handling user privacy.
- Remain vigilant once you have chosen a VPN service provider; be on the lookout for software upgrades and periodic changes in the ToS.

WHAT IS A VPN?

A virtual private network (VPN) is a private network that extends across a public network or the Internet, allowing users to surf the web privately, safe from outside view. When a VPN is activated, incoming web traffic is routed through a secure, remote server equipped with firewalls and data encryption tools.
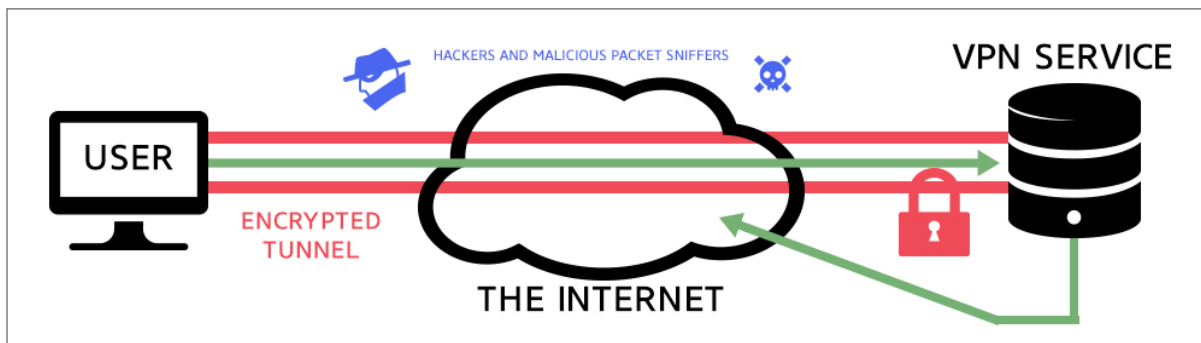
For the average user, VPNs offer an added layer of identity protection by concealing network and location data and shielding PII from potential hackers and identity data brokers. While a VPN is enabled, Internet traffic and session data are looped through a remote server with data encryption before reaching the requested website's server. Three common use cases for VPN technology are described below:

- **Business –** Companies use VPNs to allow access to intranet sites and secured files with off-site employees.
- **Residential –** More households are establishing VPNs at home to keep their family's PII, browsing history, Internet Protocol (IP) address, and location data secure from malware and malicious websites.
- **Mobile –** As an increasing number of users access the web using their phones, mobile apps providing VPN access are becoming popular. However, VPN does not mask location or other session data from apps to which the user has previously permitted access.

VPN BENEFITS

- The VPN tunnel, a private connection established between your device and the remote server, shields your PII from outside view.
- VPN services typically include: data encryption, IP address protection, ad blockers, and kill switches. Ad blockers remove unwanted advertisements, while a VPN kill switch automatically cuts your connection during service interruptions. These features ensure that your session is protected on both the browser and server level.
- VPNs shield PII in worst-case scenarios by encrypting user data and decreasing the risk of identity exposure against data theft and malicious attacks.
- VPN users can route web traffic through servers in other countries. This offers unique benefits, such as allowing users to view country-specific content that is normally blocked in their physical location.

VPN VULNERABILITIES

- VPNs can cause a reduction in Internet connection speed. The tunneling effect of most VPN services creates a connection lag.
- VPN service providers will have access to your username, password, session data, and some PII. Review your service's ToS frequently to ensure that the company is not sharing or selling your data with third-party partners and vendors.
- VPNs often use servers located in other countries; privacy laws vary among countries, so your data may be at greater risk when connecting to servers located in places with lenient privacy laws.
- Some VPN providers, especially free ones, come with monthly data caps. Make sure the plan you choose includes sufficient bandwidth for your needs.
- VPNs are not fool-proof in protecting your privacy online; they are subject to hacks and data breaches like all other digital services.

CHOOSING THE RIGHT VPN SERVICE PROVIDER

The easiest way to establish and connect to a VPN from home is by using a reputable service provider. Your selection will depend on your specific usage requirements, physical location, and device type. Before committing to a particular provider, consider:

- Can the service be loaded onto multiple devices? Can the service be used on all devices simultaneously?
- Is the software or app compatible across different operating systems, if needed?
- Are there any data restrictions in place? Does the VPN service provider guarantee complete anonymity?
- What level of data encryption is offered? Does the service provider keep server logs?
- Where is the VPN provider located? Choose a provider based in a country with no data retention requirements or practices.

Most providers offer paid and free versions of their service. Be aware that the free option comes with limits such as bandwidth caps, the number of accessible servers, and the number of devices allowed per VPN.

HOW TO ESTABLISH AND CONNECT TO A VPN

After selecting your VPN provider, install the VPN software and begin your protected browsing session. Using VPN software will require you to login each time you wish to make a connection. Most services require a basic username/password combination for authentication. Additional security features, like use of an alphanumeric authentication key, are used for account recovery or password resets. Some free trials may not require registration. The following is an example of how VPN programs work.

1 Create an account with your chosen VPN service provider.

2 Download and install the selected VPN program. If you are using a mobile device, locate the app in the App Store or Google Play Store.

FREE PROXY   HELP   FREE DOWNLOAD

3 Open the program on your device and sign in. VPNs can be run indefinitely; however, if you logout of the program or shutdown your device, you will need to login again.

CyberGhost

Username

Password

Login

☐ Keep me logged in

Please enter a username and a password

Your Username:

Username

Usernames should contain at least 6 characters. Allowed are letters (a-z, A-Z), numbers (0-9), dashes (-), underscores (_), and points (.)

Your Password:

Password

Server

⊙ 🇩🇰 Denmark

⊙ 🇫🇮 Finland

⊙ 🇫🇷 France
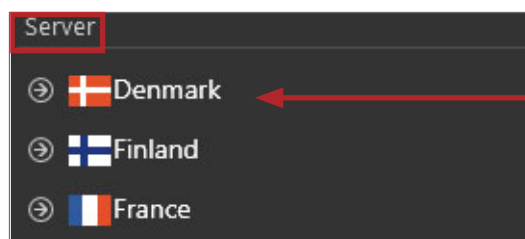
4 Choose your target server by country or region and establish a connection.

5 Once the connection has been established, allow the program to run in the background of your device. The VPN service dashboard gives you information about the new IP address, server location, and connection duration.

6 Disconnect from the chosen server when ready, removing the protection from your device. Login is required every time you want to reconnect to a VPN.

STOP ANONYMOUS SURFING

Miami
SERVER LOCATION

107.183.242.45
YOUR IP HAS BEEN REPLACED BY CYBERGHOST.

UNITED STATES

00:00:09
TIME

You are currently protected

✔ Hidden IP ✔ 107.183.242.45-Miami-S03-I03 ✔ Military Grade Encryption ✔ No Logs

WINDOWS 10 - DO'S AND DON'TS

- Before using Windows 10, adjust the default factory settings; they are set to maximize data collection across all Microsoft apps and programs.
- Immediately review and adjust Cortana's default privacy setting to prevent Microsoft from collecting gratuitous personal data.
- Only approve suggested system updates or Express Settings after reviewing the Terms of Service.
- Review data permissions of all apps installed on your computer every three months. Apps you never interact with can still access your Windows data and collect your user statistics and patterns for analysis.
- Ensure that your anti-virus software, VPN, and web browsers to are up-to-date and functional.

OVERVIEW

Windows 10 is the most recent version of the Microsoft's operating system. It includes a new browser, varied login protocols, a digital assistant, and default settings that collect and send usage data to Microsoft. The programs in Windows 10 are more interconnected than previous versions and require new sets of user data and input to function, such as additional account fields, access to the lock screen, and contact lists. This means Windows 10 collects and uses personal data in new ways compared to previous iterations. Follow the recommended settings below to avoid sharing an unnecessary amount of personal information with Microsoft. Note also that Windows 10 PCs may include pre-installed software that exposes user devices to hacking. Review and uninstall any unnecessary programs and apps, or consider reformatting new devices to limit risk.

CORTANA - WINDOWS' INTELLIGENT PERSONAL ASSISTANT

Cortana is a voice-enabled intelligent personal assistant created by Microsoft. It is accessible at the bottom left of your computer screen, and appears as a circle icon or search box. When activated, Cortana assists you in searching the web, creating alarms, managing contacts, and writing emails and messages. To fully function, Cortana must access your Microsoft email address, geolocation data, microphone, calendar, user metadata, and computer settings.
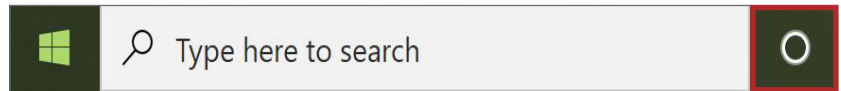
Using Cortana with the default factory settings will leave your PII exposed. It is recommended that you **disable Cortana** during most normal usage scenarios. If you choose to use Cortana for special use cases, follow the recommended settings in this chapter to maximize your privacy.

CORTANA SETTINGS

1 On your home screen, click on the **Start Menu** (represented by the Windows icon located in lower left corner of the home screen), and navigate to **Settings > Cortana > Talk to Cortana** and configure the settings depicted below.

Cortana
Cortana language, permissions, notifications
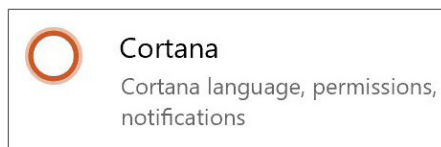
2 Under **Settings > Cortana > Permissions**, click **Manage the information Cortana can access from this device**.

Talk to Cortana
Permissions
More details

Permissions
Manage what you permit Cortana to do, see, and use.
Manage the information Cortana can access from this device

Home
Find a setting
Cortana
Talk to Cortana
Permissions
More details

Talk to Cortana

Microphone
Make sure Cortana can hear m

Check the microphone
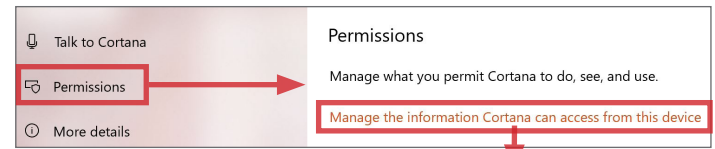
Toggle OFF Hey Cortana to prevent Cortana from listening anytime the computer is on.

Hey Cortana
Let Cortana respond to "Hey Cortana"
Off
Cortana uses more battery when this is on.

Keyboard shortcut
Let Cortana listen for my commands when I press the Windows logo key + C
Off

Don't enable Cortana functionality when your computer is locked. This permission creates a hole in your computer's security.

Lock Screen
Use Cortana even when my device is locked
Off
To get Cortana tips on the lock screen, choose Picture or Slidesh as your background in Lock Screen Settings.

Manage the information Cortana can access from this device

Permissions
Manage what Cortana can see and use.

Location
Off
When you let Cortana collect and use your location and location history, Cortana can remind you at places you choose, help you find directions, and keep you posted on what's up nearby.

Contacts, email, calendar & communication history
Off
Cortana can help keep you on time and prepared for meetings, suggest reminders to help you follow up on your commitments, help track your packages and flights, and more when you let Cortana collect and use information like your contacts, calendar details, and content and communication history from messages and apps.

Browsing history
Off
If you let Cortana collect and use your browsing history, Cortana can offer personalized suggestions on Microsoft Edge websites.

When you turn off any option, Cortana stops collecting and using that data. To delete what Cortana's already learned, go to Cortana's Notebook > About me, and sign out.

Speech privacy settings

Privacy Statement

Toggle OFF all permissions to prevent Cortana from seeing and using your Location, Contact, Email, Communication, and Browsing data.

To delete previously collected data, return to the home screen and click the Cortana icon. Navigate to Cortana's Notebook (notebook icon located on the left of the Cortana panel) > About me, and sign out.

ADJUSTING WINDOWS 10 PRIVACY SETTINGS

Managing the privacy settings on Windows 10 is the only way to control what information is collected, stored, and shared by Microsoft. The following steps will show you what Windows has access to and how you can maximize your data security.

1 Navigate to Windows 10's privacy settings by clicking **Start Menu > Settings > Privacy**.

> 🔒 Privacy
> Location, camera, microphone

2 Under the **General** heading, modify the options as shown below in order to secure your computer and PII.

🏠 Home

Find a setting 🔍

Privacy

Windows permissions

🔒 General
🗩 Speech
🗐 Inking & typing personalization
🗐 Diagnostics & feedback
🖳 Activity history

General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app activity (Turning this off will reset your ID.)
◯ Off

Let websites provide locally relevant content by accessing my language list
◯ Off

Toggle OFF all privacy options

Let Windows track app launches to improve Start and search results
◯ Off

Show me suggested content in the Settings app
◯ Off

3 Under **Privacy > Speech,** turn **OFF Online speech recognition** to prevent the collection of voice data.

🏠 Home

Find a setting 🔍

Privacy

Windows permissions

🔒 General
🗩 Speech

Speech

Online speech recognition

Use your voice for dictation and to talk to Cortana and other apps that use Microsoft's cloud-based speech recognition. Microsoft will use your voice data to help improve our speech services.

If you turn off online speech recognition, you won't be able to speak to Cortana or use dictation. However, you can still use the Windows Speech Recognition app and other speech services that don't rely on Microsoft's cloud-based services.

◯ Off **Toggle OFF**

4 Under **Privacy > Inking & typing personalization,** turn **OFF Getting to know you** to prevent the collection of typing and handwriting data.

🏠 Home

Find a setting 🔍

Privacy

Windows permissions

🔒 General
🗩 Speech
🗐 Inking & typing personalization

Inking & typing personalization

Getting to know you

Use your typing history and handwriting patterns to create a local user dictionary that makes better suggestions for you.

When this is switched off your personal typing and inking dictionary will be cleared. Typing suggestions and handwriting recognition using the system dictionary will continue to work.

◯ Off **Toggle OFF**

View user dictionary

7 Microsoft automatically enables numerous app permissions, including access to your device location, camera, microphone, communications logs, and your account information, among others. Carefully examine each category listed under **Privacy > App permissions**. When in doubt, **toggle OFF** all permissions that are not essential to your device usage. Where possible, clear historical data periodically.

For example, **toggle OFF Location** access, and only allow essential apps (e.g. Maps) access to your location data. Clear location history periodically.

5 Under **Privacy > Diagnostics & feedback**, opt to send only **Basic** device information to Microsoft. **Toggle OFF Improve inking & typing recognition** and **Tailored experiences.** This page also contains an interface to **Delete diagnostic data**. Delete your diagnostic data periodically.

🏠 Home

Find a setting 🔍

Privacy

Windows permissions

🔒 General
🗩 Speech
🗐 Inking & typing personalization
🗐 Diagnostics & feedback
🖳 Activity history

App permissions

🚶 Location
📷 Camera
🎤 Microphone
🎙 Voice activation
💬 Notifications
🗐 Account info

Diagnostics & feedback

Diagnostic data

Choose how much diagnostic data you want to send to Microsoft. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of which option you select, your device will be equally secure and will operate normally. Get more info about these settings

Set to BASIC

◉ Basic: Send only info about your device, its settings and capabilities, and whether it is performing properly.

◯ Full: Send all Basic diagnostic data, along with info about websites you browse and how you use apps and features, plus additional info about device health, device activity, and enhanced error reporting.

Improve inking and typing

Your current Diagnostic data setting prevents inking and typing data from being sent to Microsoft.

Send inking and typing data to Microsoft to improve the language recognition and suggestion capabilities of apps and services running on Windows.

◯ Off **Toggle OFF**

Tailored experiences

Let Microsoft offer you tailored experiences based on the diagnostic data setting you have chosen. Tailored experiences are personalized tips, ads, and recommendations that enhance Microsoft products and services for your needs.

◯ Off **Toggle OFF**

6 Under **Privacy > Activity history**, uncheck both boxes to prevent Windows from collecting your activities and syncing that data to the cloud. **Toggle OFF Show activities from these accounts**. Scroll down and use **Clear activity history** to periodically delete your activity data.

🏠 Home

Find a setting 🔍

Privacy

Windows permissions

🔒 General
🗐 Speech, inking, & typing
🗐 Diagnostics & feedback
🖳 Activity history

App permissions

🚶 Location
📷 Camera
🎤 Microphone
💬 Notifications
🗐 Motion

Activity history

Jump back into what you were doing with apps, docs, or other activities, either on your PC or your phone.

UNCHECK both boxes

☐ Let Windows collect my activities from this PC

☐ Let Windows sync my activities from this PC to the cloud

Review the Learn more and Privacy statement for info about activity history, what happens when you send your activity history to Microsoft, and how we respect your privacy.

Show activities from accounts

These are your accounts on this PC. Turn them off to hide their activities from your Timeline.

🟦 Microsoft **Toggle OFF** ◯ Off

Clear activity history

Clear history for **Periodically clear activity history**

Clear

Manage my Microsoft Account activity data

SMARTPHONES

SMARTPHONES - DO'S AND DON'TS

- Protect your device with a strong alphanumeric password. Pattern locks can be strong but have a greater risk of being compromised.
- If available, enable hard-disk encryption on your device. iPhones and Android devices with recent OS upgrades may enable encryption by default.
- Limit accessing sensitive information from the lock screen, including call logs, emails, text messages, and voice assistant functions (Siri, Google Now).
- Malicious emails and texts can infect your phone with malware. Avoid messages with links from unknown parties; regularly run antivirus software.
- Cameras and microphones can be remotely activated; as a precaution, remove batteries before discussing any sensitive information.
- If available, restrict permissions to limit the personal data apps can access. Review what data (e.g., location) apps collect before downloading.

PROTECTING YOUR SMARTPHONE FROM PHYSICAL ACCESS AND MALWARE RISKS

Use these settings and recommendations to minimize security risks and protect your personal data. Feature availability can vary by OS version and device.
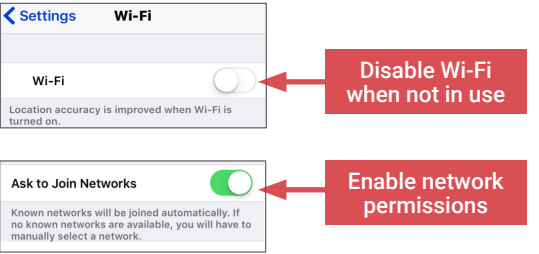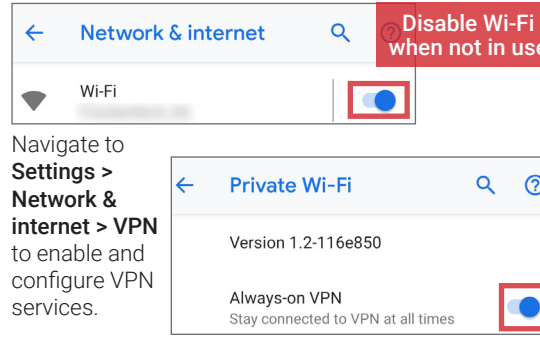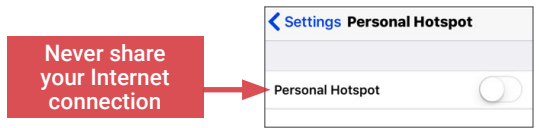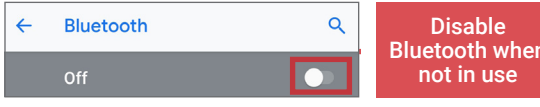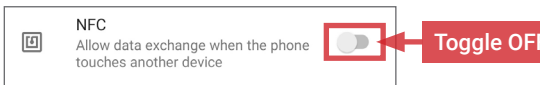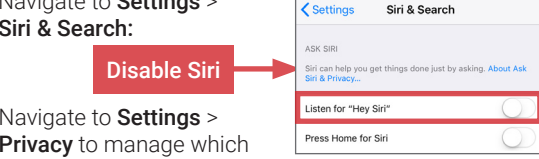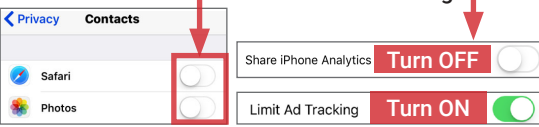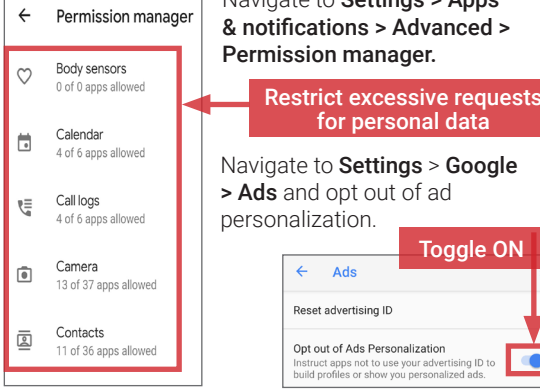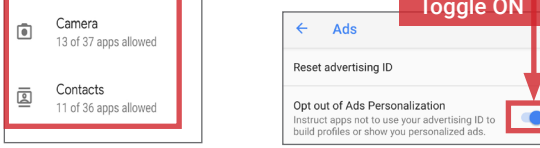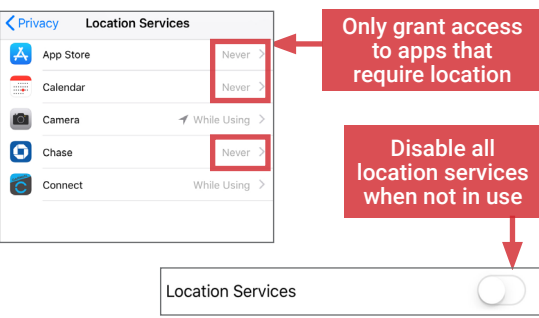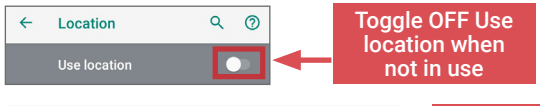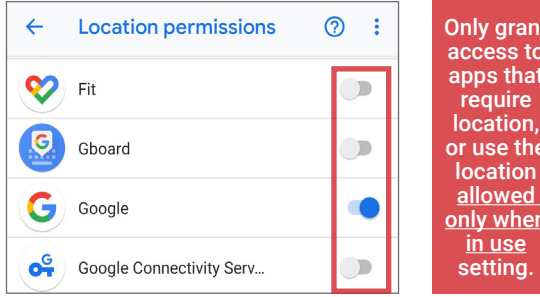
RISK SCENARIO	IPHONE (V. 14.3)	ANDROID (V. 11)
SMARTPHONE IS PHYSICALLY ACCESSED BY SOMEONE WITHOUT YOUR CONSENT To prevent unauthorized access, set up a strong alphanumeric passcode or PIN at least eight digits long. Fingerprints, face recognition, and pattern locks may be strong, but they present greater risks to your identity when compromised. To secure your SIM card, set up a SIM PIN lock. When set, no one else can use your SIM to make calls or use cellular data.	Navigate to **Settings > Face ID & Passcode** **Always use BOTH FaceID and passcode. Do not use FaceID alone.** **Block access to phone data when locked** **Turn ON Erase Data after 10 failed attempts** Settings — Face ID & Passcode; Turn Passcode Off; Change Passcode; Require Passcode — Immediately; ALLOW ACCESS WHEN LOCKED: Today, Notifications View, Siri; Erase Data — Erase all data on this iPhone after 10 failed passcode attempts.	Navigate to **Settings > Security > Screen lock.** **Use a PIN, pattern lock, or biometrics** **Go to Screen lock > ⚙ > Lock after screen timeout and set time period** DEVICE SECURITY; Screen lock — PIN; Pixel Imprint — 3 fingerprints set up; Smart Lock. Screen lock — Lock after screen timeout (5 seconds after timeout, except when kept unlocked by Smart Lock); Power button instantly locks (Except when kept unlocked by Smart Lock).
SMARTPHONE IS LOST/STOLEN Use apps that allow you to locate, lock, and erase data on your phone remotely. If a stolen phone is later recovered, the device should be considered compromised. Get a new SIM card for the device. Perform a hard-reset, erasing all files, settings, accounts, and software. Change the passwords of any linked accounts.	Install **Find My** from Apple. Find My Apple Free; Devices — iPhone This iPhone — With You. Capabilities: • Remote lock. • Erase data. • GPS locator. • Sound alarm. • Send text message to phone. • Backup data through iCloud storage.	Install **Google Find My Device.** Google Find My Device — Google LLC; Tools; #4 Top Free; INSTALL. Capabilities: • Locate device by GPS. • Remote lock. • Erase data. • Sound alarm. • View network, battery status, and hardware details.
SMARTPHONE IS INFECTED WITH MALWARE Your smartphone can be infected with malware by clicking links in emails or texts, visiting malicious websites, downloading apps or photos from bad actors, or connecting to a compromised device. Use browsers that enable ad- and script-blocking. Download third party security apps to check for and prevent malware from compromising your data.	Install a malware monitoring app, such as **Lookout.** While iOS is not readily susceptible to viruses, use this app to monitor the system for malicious activity. Capabilities: • Monitor malicious activities in apps. • Check OS and apps to ensure they are up-to-date. • Missing device alert & locator.	Install a malware monitoring app such as **AVG Antivirus.** AVG AntiVirus — UPGRADE; SCAN; Scan now for hidden threats! Capabilities: • App, file, Wi-Fi, & website scanner. • Text and call blocker. • App lock. • Remote lock. • Erase data remotely. • GPS locator. • Kill slow tasks. • VPN. • Encrypts private photos.

RECOMMENDATIONS TO MINIMIZE PHYSICAL ACCESS AND MALWARE RISKS

- Immediately install smartphone operating system updates and security patches. Keep all apps updated to maximize protection.
- Never jailbreak or root smartphones. Jailbroken/rooted phones allow malicious apps to bypass device security protocols and alter device software.
- Only install apps from the official Apple or Google Play store. On Android, ensure **Settings > Lock screen & security > Unknown sources** is turned **OFF**.
- Record IMEI number to identify device if lost/stolen. iPhone: **Settings > General > About**. Android: **Settings > About device > Status > IMEI information**.
- Wipe data on device before discarding, donating, recycling, or selling it. Transfer SIM card to new device or destroy it.
- Change passwords on your phone frequently (approximately every 3 months) to maximize security.

WIRELESS PROTECTION AND APP SECURITY SETTINGS

Smartphones communicate personal data across a variety of networks and apps. Follow these steps to best protect your identity data in one of the following four common smartphone use case scenarios. The availability of suggested settings may vary by OS version, device manufacturer, and model.

USE CASE	IPHONE (V. 14.3)	ANDROID (V. 11)
CONNECTING TO WI-FI NETWORKS Information transmitted via public Wi-Fi networks can be intercepted by third parties. Avoid using public wireless networks, and always use a VPN client, such as Shrew Soft VPN (http://www.shrew.net) to encrypt your mobile activities.	Navigate to **Settings** > **Wi-Fi:** **Disable Wi-Fi when not in use** — **Enable network permissions** — Navigate to **Settings** > **VPN** to enable and establish a VPN connection.	Navigate to **Settings > Network & internet > Wi-Fi:** **Disable Wi-Fi when not in use** — Navigate to **Settings > Network & internet > VPN** to enable and configure VPN services.
CONNECTING VIA BLUETOOTH Bluetooth and NFC involve the wireless communication of two devices within close geographical proximity. When Bluetooth is enabled, hackers may be able to exploit the connection to access your calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and NFC and disable these features when they are not in use.	Navigate to **Settings** > **Bluetooth** to disable services. **Disable Bluetooth when not in use** — Navigate to **Settings** > **Personal Hotspot** to disable broadcasting your private Internet connection. **Never share your Internet connection**	Navigate to **Settings** > **Connected devices** to establish and enable **Bluetooth** and **NFC** connections. **Disable Bluetooth when not in use** — **Near Field Communications (NFC)** enables smartphones to transfer data when devices touch. **Toggle OFF** when feature is not in use. **Toggle OFF**
DATA RETAINING APPS Downloaded apps frequently collect personal information to sell to advertisers or third-party data aggregators. Native applications such as Siri and Google Assistant may also collect user data, including device information or audio recordings. Many devices allow users to restrict the personal information or permissions that apps can access. Set strict limits to protect personal information.	Navigate to **Settings** > **Siri & Search:** **Disable Siri** Navigate to **Settings** > **Privacy** to manage which specific data each app accesses from your phone. Navigate to **Settings** > **Privacy**—apply following settings under **Analytics** and **Advertising.** **Turn OFF** — Share iPhone Analytics **Turn OFF** — Limit Ad Tracking **Turn ON**	Navigate to **Settings > Apps & notifications > Advanced > Permission manager.** **Restrict excessive requests for personal data** Navigate to **Settings** > **Google > Ads** and opt out of ad personalization. **Toggle ON**
APPS USING REAL-TIME LOCATION Many apps request permission to track your real-time location. Avoid granting permission to these apps when possible, and turn off all location tools when they are not in use. Additionally, pictures taken with smartphones may retain location information inside their EXIF data, and location will be shared along with the photos once they are uploaded to a website or SNS. One exception to this rule is with device-locating apps for loss and theft such as **Find My** or **Find my device**.	Navigate to **Settings** > **Privacy** > **Location Services:** **Only grant access to apps that require location** **Disable all location services when not in use**	Navigate to **Settings** > **Location:** **Toggle OFF Use location when not in use** **Only grant access to apps that require location, or use the location allowed only when in use setting.**

✈ TRAVELING WITH SMARTPHONES

TRAVELING WITH SMARTPHONES - DO'S AND DON'TS

- Bring a dedicated loaner device when you travel overseas; do not bring your primary smartphone.
- Make sure your device is running the latest software; this will help protect you against any new technical vulnerabilities.
- Assume that all information on your device can be compromised while traveling in a foreign country; leave sensitive information off of your phone.
- Use a VPN to protect your phone when accessing Wi-Fi networks in a foreign country.
- Use anti-virus services to ensure that your phone is protected from malware.
- Password-protect your device and set your phone to lock automatically when not in use.

ENSURE THAT YOUR PHONE'S SOFTWARE IS UP-TO-DATE

Ensure that the software on your smartphone is up-to-date. This will offer you the latest protection against newly-discovered technical vulnerabilities.

iPHONE (V. 14.3)
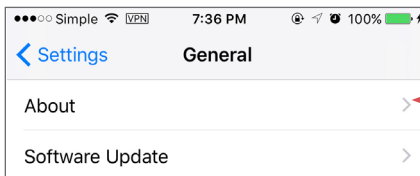
Go to Settings > General > Software Update. Check to see if your software is up-to-date.

If your software is not up-to-date, your iPhone will prompt you to download the latest software.

ANDROID (V. 11)

Go to Settings > System > Advanced > System update to view system status
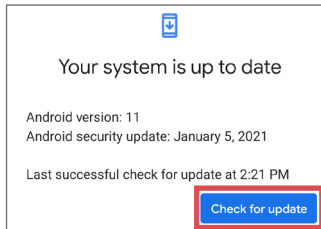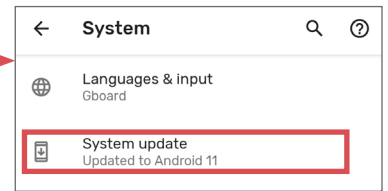
Confirm current software is up-to-date. If not, follow Android prompts to download and install the latest software version and security update.

PROTECT YOUR PHONE AGAINST MALWARE

Like a computer, your phone is vulnerable to malware and malicious apps. Use anti-virus apps to ensure that your phone is protected.

iPHONE (V. 14.3)
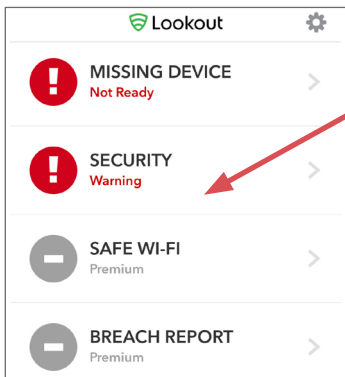
Lookout for iPhone is an option. Go to Security to see if your phone has any malicious apps.
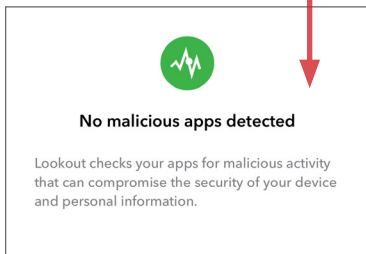
ANDROID (V. 11)
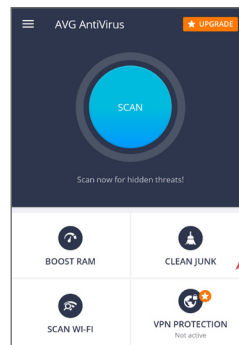
AVG Antivirus Free is available for Android. Click Scan to check your smartphone for viruses.

AVG also offers Wi-Fi network scanning and VPN Protection.
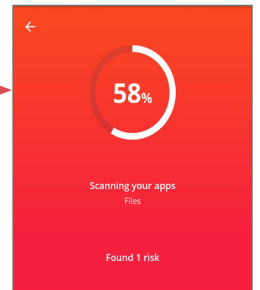
SET YOUR PHONE TO LOCK AUTOMATICALLY AND SET A COMPLEX SCREENLOCK PASSWORD

In case you lose your device, you want your smartphone to lock automatically to prevent physical access. Use a complex password to protect your phone.

iPHONE (V. 14.3)
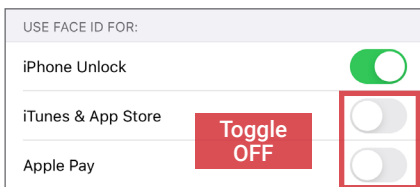
Go to Settings > Face ID & Passcode. Disable Face ID for sensitive options, such as App Store, Apple Pay, and Password AutoFill.
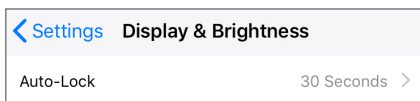
Go to Settings > Display & Brightness > Auto-Lock. Set the Auto-lock to 30 seconds.

ANDROID (V. 11)
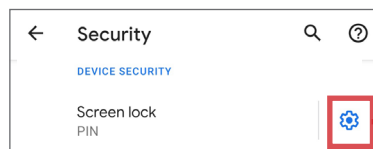
Go to Settings > Security > Screen lock to enable device protection. Choose between pattern, PIN, password, or biometric lock.
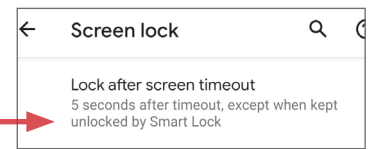
Go to Screen lock settings > Lock after screen timeout, and select a short timeout period.

DISABLE WI-FI AND BLUETOOTH

Disable **Wi-Fi** and **Bluetooth** on your smartphone when you are not using them; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware.

iPHONE (V. 14.3)

Go to Settings > Wi-Fi. Turn Wi-Fi OFF.

Go to Settings > Bluetooth. Turn Bluetooth OFF.

ANDROID (V. 11)

Go to Settings > Network & internet > Wi-Fi. Turn Wi-Fi OFF when not in use.

Go to Settings > Connected devices > Connection preferences > Bluetooth. Turn Bluetooth OFF.

USE VPN ON WIRELESS NETWORKS

Virtual Private Networks—or **VPNs**—allow you to extend a private network across a public network such as public Wi-Fi. Using a VPN will make it more difficult for malicious individuals to eavesdrop on your Internet traffic. Use a VPN service such as SurfEasy VPN or Avast SecureLine to protect yourself.

iPHONE (V. 14.3)

Use widely available VPN services such as **SurfEasy,** and **Avast SecureLine** VPN for iOS to protect yourself when connecting to Wi-Fi during travel.

ANDROID (V. 11)

Use VPN services such as **SurfEasy for Android** to protect yourself when connecting to Wi-Fi during travel.

RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

Find My app and **AVG AntiVirus** can locate lost phones, wipe data remotely from lost phones, and provide contact information to return a lost device.

iPHONE (V. 14.3)

Use the Find My app to recover lost or stolen iPhone, iPad, and Macbooks

Immediately activate Lost mode and erase the device upon loss or theft

ANDROID (V. 11)

Use anti-theft features (e.g., those available with the AVG AntiVirus Free app) to set a lock screen message, recover lost or stolen Android smartphones using Google Maps, and wipe data remotely from the device and SD content card

IDENTITY THEFT PREVENTION

IDENTITY THEFT PREVENTION - DO'S AND DON'TS

- Create a unique password for each of your accounts and devices to limit the risk of having multiple accounts compromised at once.
- Change your login passwords on a regular basis, and don't store them in your email or cloud storage services, which a hacker can potentially access.
- Keep your computer up-to-date by installing the latest versions of the operating system and anti-virus software protection.
- Avoid sharing sensitive information such as credit card or Social Security Numbers through texts, emails, or chats.
- Never use public networks to conduct online financial transactions. Remember to log out of personal accounts opened on public devices.
- Ensure that all communications involving online financial transactions are sent through an SSL encrypted connection ("https://").

IDENTITY THEFT - BACKGROUND

Identity theft is currently one of the fastest-growing crimes in America. In 2018, 60 million Americans were affected by identity theft and the total value losses in 2019 reached $16.9 million.[24] On average, each victim spends 100 to 200 hours over a six-month period trying to resolve an identity fraud issue.[25] While the common conception is that identity thieves are online scammers, evidence indicates that up to 50% of all reported cases involve theft committed by a neighbor, co-worker, or family member.[26] Most identity theft cases can be resolved with minimal long-term impacts if they are caught early.

TYPES OF IDENTITY THEFT AND WHAT'S AT RISK

Identity theft occurs when one individual fraudulently uses another's personal information for financial or personal gain. Though the motives behind identity theft may differ, disseminating sensitive or potentially harmful information places your identity and financial assets at risk.

SENSITIVE DATA

- Social Security Number
- Driver's License Number
- Credit Card Number
- Bank Account Number
- Birth Certificate
- Tax Information
- Employee Identification Number

POSSIBLY HARMFUL

- Pets' RFID Numbers
- Utility Account Numbers
- Residential History
- Unsolicited Credit Offers

WHAT DOES IDENTITY THEFT LOOK LIKE?

Pie chart:
- Credit Card Fraud — 30%
- Employment or Tax-Related Fraud — 19%
- Other Identity Theft — 15%
- Phone or Utilities Fraud — 12%
- Bank Fraud — 11%
- Loan or Lease Fraud — 7%
- Government Documents or Benefits Fraud — 6%
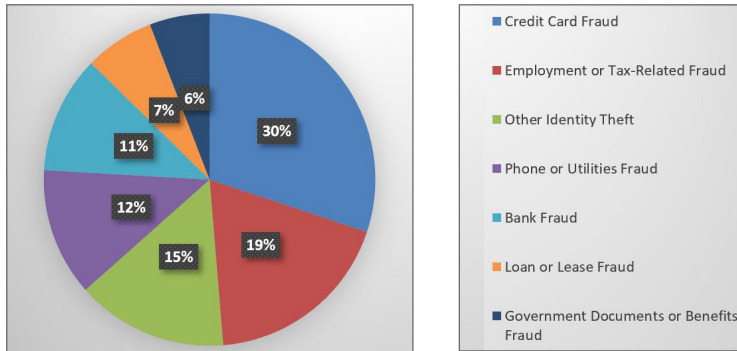
*Source: Network for Identity Theft Types by # of Reports, Federal Trade Commission, *Consumer Sentinel Network Data Book 2017* (March 2018)

IDENTITY THEFT TYPES

- Financial
- Insurance
- Medical
- Criminal
- Driver's License
- Social Security
- Synthetic
- Child

AGE OF VICTIMS

- < 19 years: 4%
- 20 to 39 years: 29%
- 40 to 59 years: 32%
- 60+ years: 35%

FAKE WI-FI NETWORKS

Fraudsters may establish fake Wi-Fi hotspots to mimic public Internet access points. Avoid communicating personal and financial information over public Wi-Fi connections, and do not access any unsecured networks.

Do NOT use unsecured Wi-Fi Connections

Linksys Extender Setup - 3B1

NETGEAR53
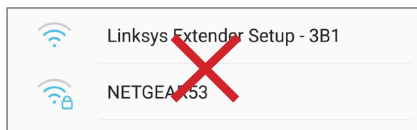
SNS MINING

Sharing personal information may allow another individual to apply for a line of credit using your identity, or send targeted phishing scams. Avoid sharing home addresses and birth dates on social networking service (SNS) profiles, and never disclose any of the sensitive information.

PHISHING SCAMS

Phishing scams are among the most popular techniques for acquiring personal information. The information gleaned from phishing scams can be used to open fraudulent accounts or assume control of existing accounts. The model below outlines the common identifiers of a phishing email.

1. Non-descriptive senders or mismatched email addresses (e.g., the "From" and "Reply-To" addresses do not match).
2. Unprofessional subject titles.
3. Phrases demanding the user to share personal information to prove their identity.
4. Threats to close accounts without compliance or immediate actions.
5. Absence of company logo within the email header.
6. Presence of grammatical or spelling errors.
7. Emails containing links to other pages or attachments may contain malicious scripts to install malware.

> **1** **From:** Payment Services <XXXXX@XXXX.XXX>   **5**
> **Reply-To:** <XXXXXXX@XXXX.XXX>
> **Date:** Mon, 23 Nov 2014 12:34:13 -0700
> **2** **Subject:** Suspicious Account Activity!
>
> This message is to inform you that your account has exhibited unusual activity within the past 24 hours and has since been locked for security purposes. In order to verify ownership of your account you must respond to this email with the following information:
>
> **3** Name:
> Email:
> Account Number:
> Social Security Number: **6**
>
> **4** Failure to verify your account information may result in forfeiture of funds. To see a summary of your account activity, open the attached documents or visit our Security Center.   **7**

SIGNS OF IDENTITY THEFT

Credit scores can be damaged or ruined with identity theft. However, damages can be reduced significantly if caught early. Bank statements should be checked weekly, while each of the three credit reports (Equifax, Experian, and TransUnion) should be checked once per year. The following occurrences may indicate a stolen identity:

- Errors appearing on bank and credit card statements.
- Errors appearing on credit reports.
- Financial accounts flagged for suspicious activity.
- Debt collectors calling to inform about delinquent debts.
- Problems filing insurance claims.
- Fraud alerts activated on credit cards.

Score	Rating	Details
850–700	**BEST** HIGHER CREDIT SCORE	• Most favorable interest rate • Lower monthly lease or loan payment • Higher likelihood of qualifying for the lease or loan • Access to incentives offered by the manufacturer or seller
650–450	LOWER CREDIT SCORE	• Higher down payment may be needed • Co-signor may be necessary • You may not be able to qualify for the loan at that amount that means a less expensive purchase may need to be considered.
400–300	**WORST** VERY LOW CREDIT SCORE	• Credit may be denied altogether

850-750 Excellent* | 749-720 Very Good* | 719-660 Good* | 659-580 Fair* | 579-500 Poor* | 499-300 Very Poor*

*General credit score ranges. Ranges may vary slightly by lender

IDENTITY THEFT PROTECTION SERVICES

Select companies offer services to monitor customers' credit scores and to protect their personal information online. Each company works with creditors to identify fraudulent activity and restore a customer's reputation. Most packages also offer financial reimbursements for significant personal losses. Individuals should still follow best practice guides to prevent the compromise of identity data during online activity. The table illustrates features for different tiers of identity theft protection services.

IDENTITY MONITORING SERVICE TYPES	SSN	BANK ACCOUNT	CREDIT CARD	MEDICAL FRAUD	PUBLIC & COURT RECORDS	COMPUTER SECURITY OFFERINGS	CREDIT REPORTS	FINANCIAL COVERAGE
Basic	✓	✓	✓		✓		Annually	Up to $1 Million
Comprehensive	✓	✓	✓		✓	✓	Annually	Up to $1 Million
Most Comprehensive	✓	✓	✓	✓	✓	✓	Quarterly	Up to $1 Million

RESOLVING IDENTITY THEFT

Place an Initial Fraud Alert
Call one of the three credit report companies listed below and request that an initial fraud alert be placed on your credit scores. The alert lasts for 90 days and prevents any new lines of credit from being opened in your name without a form of verifiable identification. Placing an initial fraud alert entitles you to a free credit report from each of the three credit report companies. Also, consider freezing your credit to prevent creditors from accessing your credit reports. Credit freezes can be implemented for a fee (between $5.00 to $15.00) and are enabled by calling each of the three credit reporting agencies listed below. Credit freezes remain active until the individual who requested the credit freeze contacts the credit agencies and instructs them to unfreeze the reports.

Request Your Credit Scores
Use sites like www.annualcreditreport.com or www.creditkarma.com to request free copies of your credit scores. Look for inconsistencies within your credit reports and send letters to each of the three credit reporting companies explaining the misuses. Then, contact the fraud department of each business that reported a fraudulent transaction. Close any financial accounts that were opened without your permission or which show unauthorized activity.

Create an Identity Theft Report
File an online complaint with the Federal Trade Commission (FTC) at www.ftc.gov/complaint and a police report outlining the details of the theft. If the police are reluctant to file a report, present them with the **FTC's Memo to Law Enforcement**, which is available at www.IdentityTheft.gov. Together these documents make up an identity theft report and can be used to remove transactions or obtain information about the accounts misused by an identity thief.

EQUIFAX®	experian™	TransUnion®
1-888-766-0008	1-888-397-3742	1-800-680-7289

KEEPING YOUR KIDS SAFE ONLINE

KEEPING YOUR KIDS SAFE ONLINE - DO'S AND DON'TS

- One family member's unsecured privacy and sharing settings can expose personal data from the rest of the family.
- Ensure kids only establish and maintain connections with people you know and trust. Review their connections often.
- Assume that ANYONE can see any information kids post and share regarding their activities, whereabouts, and personal life.
- Avoid posting or tagging images of you and your family that clearly show your faces. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post smartphone photos and ensure kids don't use their face as a profile photo; use cartoons or avatars instead.
- Use secure browser settings when possible, and monitor your child's browsing history to ensure that you recognize all access points.

OVERVIEW

Online engagement can potentially expose children to cyber-bullying, influence operations, pornography, drug and alcohol usage, and violence. Children are at risk not only from exposure to inappropriate content posted by others on the Internet, but also from exposing their personal information to strangers on social networking services (SNS). The following web browser settings, add-ons, and software downloads are available to restrict or monitor a child's activities online, potentially supporting efforts to foster healthy online activity.

MICROSOFT EDGE SETTINGS

To view child safety options, login to your Microsoft account upon opening the browser and click on **Family Safety.** From this page, you can register accounts for your children and customize their Internet browsing settings. The Family Safety settings can be only accessed with a Microsoft account.

PARENTAL CONTROLS

Adjust how your children can use the computer. Allow or block specific programs and websites, and set personalized restrictions.

PASSWORDS

Create a username/password for your child's account that only you know.

TIME RESTRICTIONS

Set a time frame of acceptable computer use for your child.

GOOGLE CHROME SETTINGS

To ensure your child's safety when using Google Chrome, download Blocksi from the Chrome Store to add child safety settings to the browser.

ADVANCE SETUP

Configure filters to allow, block, or warn users of certain content types. Select the **>** next to each filter category to set more granular restrictions.

FILTERS

YouTube Filter - filters YouTube channels and videos.
Content Filtering - identifies specific words in webpages to prevent access.
Black/White List - allows users to add specific URLs to block or allow.

TIME RESTRICTIONS

Set a time frame of acceptable computer use for your child.

FIREFOX SETTINGS

STANDARD FIREFOX: Select **Tools > Options > Privacy & Security** to block sites with malicious content. Under **Tracking Protection > Use Tracking Protection to block known trackers**, select **Always**. For **Send websites a Do Not Track signal**, select **Always**.

FOXFILTER FOR FIREFOX: To set parental controls, download the FoxFilter add-on. Once installed, users are allowed to set keywords to block or permit specific sites, and set sensitivity settings.

FAMILY SAFETY SERVICES

Free and paid services are available for monitoring your children's online activities. The representative software options listed below can be effective in restricting or monitoring content that your child tries to access.

CAPABILITIES	MICROSOFT FAMILY SAFETY	NET NANNY	NORTON 360 DELUXE
Image monitoring	Windows 8+	✓	
SMS message monitoring		✓	✓
Contacts monitoring	Windows 8+	✓	✓
Block sites option	✓	✓	✓
Allow sites option	✓	✓	✓
Report user activity	✓	✓	✓
User access requests to admin	✓	✓	✓
Time restrictions	✓	✓	✓
Game restrictions	✓	✓	
Paid service		✓	✓
Remote access notifications	✓	✓	✓
Lock safe search	Windows 8+	✓	

NORTON 360 DELUXE

Norton 360 Deluxe is comprehensive service that offers online family monitoring features along with Norton Security protection. It allows parents to track which websites children visit and filter harmful content, including profanity, sexual content, violence, drug and alcohol use, weapons, and hate sites. Parents can use this tool to conduct web, time, search, social network, mobile app, text, and video supervision; review activity history; remotely lock devices; use GPS to track device location; and receive email alerts, on an unlimited number of family devices.

Norton 360 Deluxe identifies SNS profiles that children maintain and allows supervisors to see what kids are sharing with the public (e.g., name, age, profile picture, etc.). It also prevents children from sharing personal information including phone numbers, Social Security Numbers, and email addresses.

MICROSOFT FAMILY SAFETY

Activate this free service from your Microsoft account (https://www.account.microsoft.com/family/). The service provides basic content filters along with reports on programs and websites accessed by each account.
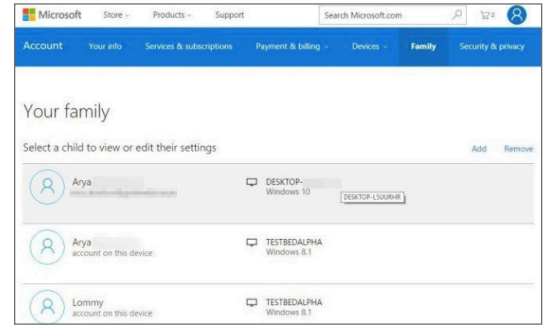
Adults can set individualized settings for each account and view their child's requests to access blocked content each time they log in.

NET NANNY

Net Nanny is a type of service that both restricts and monitors content from computer programs, instant messengers, SNS, and web browsing applications. It is installed onto the desktop and provides granular settings for filtering and reporting potentially harmful content online.
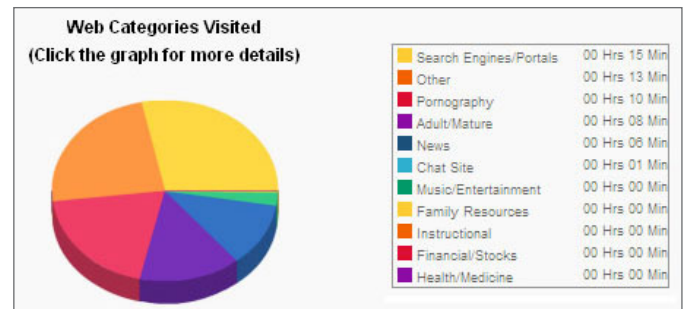
Parents can respond to their child's permission requests remotely from a mobile app or computer in real time. Additional settings include blocking applications, Internet connections, proxy servers, blogs, and chat rooms. Net Nanny displays an extensive list of SNS and instant messengers as well as 35 categories of potentially harmful content to screen.
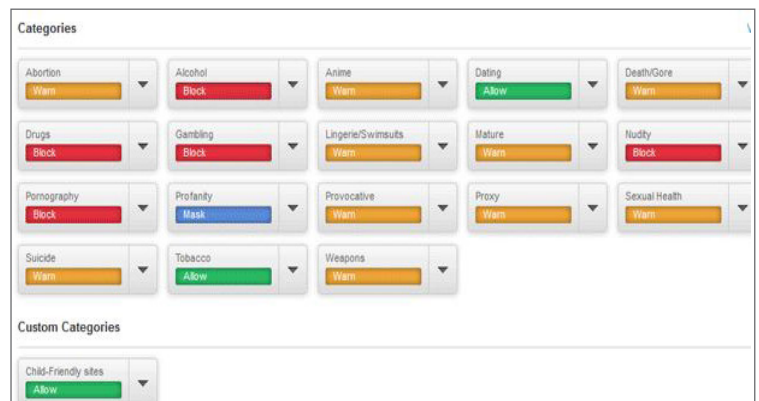
Net Nanny also provides time-based Internet usage restriction capabilities for each user profile.
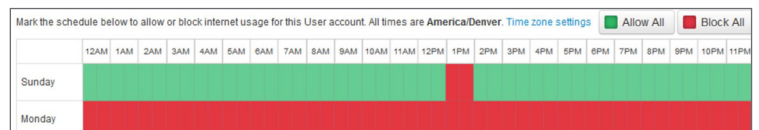
ONLINE REGISTRATION

ONLINE REGISTRATION - DO'S AND DON'TS

- Remember: even if you restrict your data from public view, online services still have access to your data and may share it with third parties.
- Avoid filling in optional identity fields for online profiles; only provide the minimum required identity information.
- Never give online services access to your Social Security Number (SSN).
- Do not upload or sync your existing phone, email, or SNS contacts with an online service.
- After completing the registration process, remove any non-essential identity data from your personal profile that was required during sign-up.
- Configure privacy settings to protect your identity information immediately after registering an online profile.

IDENTITY DATA IN ONLINE ACCOUNTS

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Social networking services (SNS) and online retailers and service providers request a variety of personally identifiable information (PII) from users during account creation and operation. The following sections provide an overview of common identity elements that are collected, tracked, and shared through account registration processes. It is recommended that you limit sharing these types of PII as much as possible.

FIRST AND LAST NAME

First and last names are mandatory for many online accounts. When possible, use your initial or a nickname instead of your full name, especially if your name is uncommon.

First name	Last name

MOBILE PHONE NUMBER

Services may ask to verify your identity using a mobile phone number. Consider using an alternative method to verify accounts, or signing up with a secondary mobile number (e.g., a online number dedicated for registration).

Enter Your Phone Number

US +1 ▾

EMAIL ADDRESS

Email accounts are ubiquitous in online registration. Consider creating a unique email address for each account you register.

Sign up

Email address

SOCIAL LOGIN

Services may allow users to sign up through SNS accounts (e.g., Twitter or Facebook) by importing your existing SNS account login data. Sign up with an email address instead.

Continue with Facebook

Continue with Google

Continue with Twitter
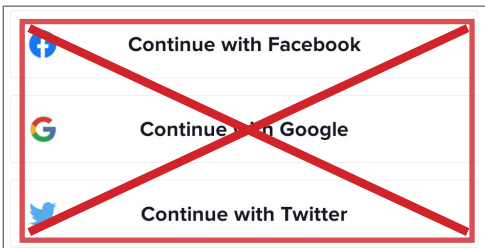
USERNAME

Usernames are unique to each account and identify individuals within an online network. When creating a username, do not include personally identifiable information (PII), such as your name or nickname, location, or birthday. Do not use the same or similar usernames across multiple accounts.

Set your username?

You can change your username once every 30 days.

CANCEL   SET USERNAME

> Do not use the same password or username across multiple accounts. Ensure that your passwords are complex and unique by including numbers and special characters.

⊕ Add a workplace

🎓 Studied at

Leave these fields blank whenever possible.

⊕ Add current city

⊕ Add hometown

⊕ Add a relationship status

📞 Mobile

RELATIONSHIP / ORIENTATION

With the exception of online dating services, relationship status and sexual orientation are almost always optional data fields. If possible, refrain from sharing this data.

Gender
○ Female ○ Male ○ Custom ❓

GENDER

Gender is commonly requested during registration. Whenever possible, avoid making a distinction when signing up.

✕ Gender	✓
Female	○
Male	○
Custom	○
Prefer Not to Say	⦿

EMPLOYMENT INFORMATION

With the exception of professionally-oriented SNS, company and employment information are often optional data fields. When providing work information, be as generic as possible (i.e., only provide the industry in which you work, rather than a specific job title). Do not identify your employer or share your physical work location.

LOCATION

Location information is required at varied levels of granularity depending on the service. Your street address, city, state, ZIP code, time zone, and/or country may be requested. Online services may also request your hometown or prior living locations. During sign up, only provide the most generic location required by the service, or consider entering a nearby ZIP code or metropolitan area. Do not share prior locations.

BIRTH DATE

Birth dates are used to verify the user's age and customize age-appropriate content and services. This information is sometimes published on the profile and can be removed retroactively. Don't share your full birth date unless it's required.

Birthday
Jun ⇅ 30 ⇅ 1995 ⇅ ❓

ONLINE REGISTRATION AND VERIFICATION PROCESSES

The data required during registration varies by service; review the mandatory personal fields prior to registering an account with the service. Note that some services may seek to verify the legitimacy of your account through phone, email, or other identity verification techniques.

1. Enter required identity fields on the registration page(s). Avoid supplying more information than required.

Create a New Account
It's quick and easy.

First name | Last name
Mobile number or email

2. Consider using dual-factor authentication to add an additional layer of security to your account. Dual-factor authentication requires the user to verify an attempted login via email, text message, or an automatically generated code.

token is:
556584
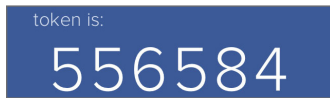
When possible, use an application such as Authy 2-Factor Authentication or Okta that automatically generates a login code, instead of providing your mobile phone number for dual-factor authentication.

3. If necessary, complete any required challenge-response tests (e.g. a CAPTCHA) to verify you are a human user rather than a "bot"--an automated software program.

I'm not a robot — reCAPTCHA Privacy - Terms
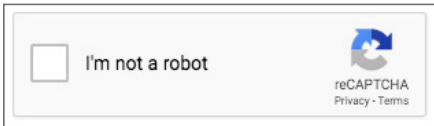
4. Confirm your account via email, if possible. Avoid using mobile phones or other identity verification procedures in order to prevent further dissemination of your data.

Enter the code from your email

Let us know this email belongs to you. Enter the code in the email sent to   .

FB- 37362

To complete registration, follow the confirmation link sent to your email address, or enter the code emailed to you.

Send Email Again

Update Contact Info | Continue

5. Access your newly created account once it is confirmed. Review your populated personal identity data fields and remove any non-required information. Adjust your privacy and security settings to limit personal information-sharing and visibility.

f Facebook

Your account has been created —
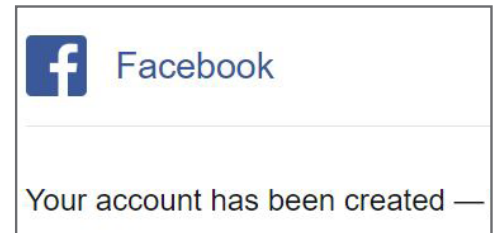
HOW ACCOUNT INFORMATION IS USED ONLINE

During account registration, online services may request several pieces of personal information. This data is used to enhance a user's experience within the service's site or mobile app, personalize content, track and deliver user rewards (e.g., coupons, points), and support online marketing and advertising.

Regardless of privacy settings, the personal information you associate with an account can be accessed by the service. The service may further share your data with unknown third parties. To learn more about how your information may be used, stored, protected, and shared, check the service's Terms of Service or Privacy Policy prior to registering an account.

ACCOUNT DEACTIVATION

1. If you plan to temporarily stop using

Deactivate Account
Deactivating your account can be temporary.
Your profile will be disabled and your name and photos will be removed from most things you've shared. You'll be able to continue using Messenger.

a service, check your account settings or search the account support page to determine if deactivation is available. Deactivation limits personal data sharing and account searchability.

2. Remember to sign out of your account on all devices, including your computer, tablet, smartphone, smartwatch, and any others. Disable or uninstall the service's app from your linked device(s).

Account
Hello,

Privacy
CA privacy rights
CA do not sell my info
CA supply chain act
Terms

○circle.
$432.91 lifetime savi
60 available votes

Sign out
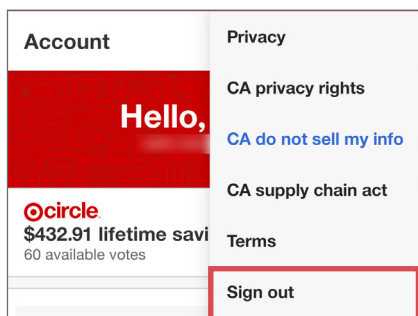
ACCOUNT DELETION

1. If you plan to permanently stop using a service, search your account settings or the help section to determine how to delete the account. Deletion procedures vary by service and require you to complete multiple actions, such as emailing your deletion request to a customer service representative. Note that some services require an extended time period (e.g., 90 days) to remove your account fully; your personal information may remain accessible during this time.

♪ TikTok

Results for 'Delete'

Showing **3** support topic results.

Delete a video

Delete your account
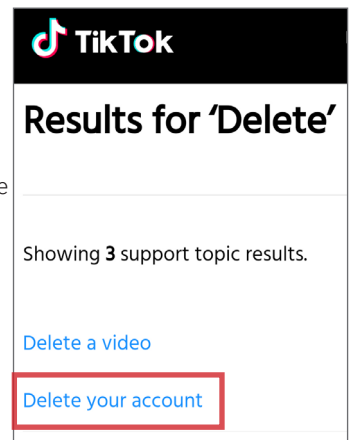
2. Disable or uninstall the service's app from all linked mobile device(s).

OPTING OUT OF DATA AGGREGATORS

OPTING OUT OF DATA AGGREGATORS - DO'S AND DON'TS

- Conduct research to see what records each data aggregator has collected about you and your loved ones before opting out.
- Some data aggregators may have information about you and your family under multiple listings; you may need to repeat the removal processes described below for each listing.
- Have ALL the required information prepared before you begin the removal process.
- Follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- Encourage family members and cohabitants to remove their records from data aggregators as well.

DATA AGGREGATORS - HOW TO LOCATE YOUR INFORMATION ONLINE

Data and identity aggregators collect and catalogue information about individuals through a combination of public records collection and extensive web indexing and crawling. Search for your name, names of family members, email addresses, phone numbers, home addresses, and social networking service (SNS) usernames and URLs using Google. Once you have located information that you want removed, record your findings to facilitate the removal process. Please note the information presented here is subject to change.

OPTING OUT INSTRUCTIONS BY SERVICE - OVERVIEW

Many data aggregators offer online opt out forms, while others require hard-copy forms to be mailed or faxed along with proof of identity (e.g., a copy of a driver's license). Removing your records from data aggreggators can be a time-consuming process, but opting out lowers the risk of providing access to your personal information to strangers online.

Data aggregators frequently change online opt-out procedures. Online methods often require your email address, so consider creating a disposable email account specifically to use in opt-out procedures. Monitor your inbox and spam folder to ensure you receive all emailed opt-out instructions and confirmations. Note the timeframe required for data removal, and check the aggregator site after the removal time period has passed to ensure your information is no longer searchable. Given the number of data aggregators that may catalogue your data, it may be helpful to create and update a tracking sheet to guide your removal processes.

CONFI-CHEK.COM

PeopleFinders, PublicRecordsNow, PrivateEye and Veromi are all owned by the same parent company: **Confi-Chek.com**. Each subsidiary has a different opt-out procedure:

Opt out of PeopleFinders and PublicRecordsNow by visiting https://www.peoplefinders.com/manage. Enter your information and select **Find My Listing**. Find your record, and select **This is me > opt out my info**. Check all three boxes under **Security Check**, and select **Continue**.

Opt out of PrivateEye by visiting: https://www.privateeye.com/static/view/optout/. Complete the online form. After completion, you will be automatically redirected to PrivateEye partner sites.

Opt out of PublicRecordsNOW by visiting https://www.publicrecordsnow.com/static/view/optout/. Enter your information and select **Opt out.**

Opt out of visiting https://www.veromi.com/help. Scroll to **How do I remove myself from these records?** (entry 20) and follow the instructions to submit a written records removal request.

Veromi by Veromi

INTELIUS

Intelius owns, or is affiliated with, the following people search websites: Classmates.com, DateCheck, iSearch, LookUpAnyone, Peopleconnect.us, PeopleLookup, PhonesBook, PublicRecords, Spock, USSearch, and Zabasearch.

Some of these aggregators use the opt-out interface depicted below, found at https://www.intelius.com/optout. To opt out:

- Search for your record.
- Click **Select & Continue**.
- Enter a confirmation email address.
- Complete the CAPTCHA.
- Check your email and copy/paste the link provided in order to complete your request (should process within 72 hours of confirmation).

For Intelius aggregators that do not use this common opt out format, visit the help section of each website and search for opt out instructions under Privacy and Opt Out topics.

OPTING OUT INSTRUCTIONS CONTINUED...

BEEN VERIFIED

BeenVerified allows you to opt out at: https://www.beenverified.com/f/optout/search.

Search for your name in ALL STATES, and click the listing(s) relevant to you. Enter your email address, complete the CAPTCHA, and click **Send Verification Email**. Follow instructions in the verification email to complete de-registration.

SPOKEO

To opt out of Spokeo, first find your listing, then visit Spokeo's opt out page: www.spokeo.com/optout.

Enter the URL of your listing, complete the CAPTCHA, and enter your email. Click **Remove This Listing**.

Your listing will be removed in 2-3 days.

PEOPLESMART

Visit https://www.peoplesmart.com/optout-go:
- Search for your record(s).
- For each relevant record, click **That's The One**.
- Under **Who are you opting out?** select **Yourself**.
- Enter your confirmation email address.
- Complete the CAPTCHA.
- Click **Send Verification**.
- Check your email to complete the opt out process.

Complete Details

That's The One
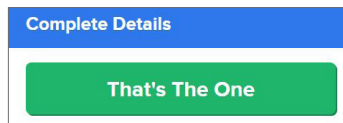
Your listing will be removed in 2-3 days.

INSTANTCHECKMATE

To opt out of InstantCheckMate, follow the instructions at: https://ww.instantcheckmate.com/opt-out.

Select **Remove This Record**. Enter your email address, complete the CAPTCHA and select **Send Confirmation Email**. Click **Confirm Opt Out** inside the email you receive, and InstantCheckMate will begin processing your opt out request, which can take up to 48 hours.

PEEKYOU

Fill out the PeekYou opt out form at: www.peekyou.com/about/contact/optout/index.php.

Under **Actions,** select **Remove my entire listing**. Paste the numbers at the end of your profile's URL in the **UniqueID** field, and complete the CAPTCHA. You will receive an initial email confirming you've sent in your opt-out form and a second email in a few days or weeks to tell you it has been deleted.

WHITEPAGES

First, locate your information on Whitepages by searching your name. Then visit https://www.whitepages.com/suppression_requests. Click **View Details** and copy the URL address associated with your profile(s). Enter the URL of the relevant profile(s) in the Opt-out form and click **Opt-out > Remove me > I just want to keep my information private**.
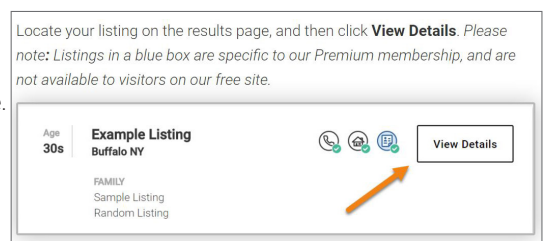
Locate your listing on the results page, and then click **View Details**. *Please note: Listings in a blue box are specific to our Premium membership, and are not available to visitors on our free site.*

| Age 30s | **Example Listing** Buffalo NY |
| FAMILY | Sample Listing Random Listing |

View Details

Verify your identity with a phone call; enter your phone number and you will immediately receive an automated call from Whitepages. Use your touchscreen to enter the four-digit verification code provided via the opt out form. For further details, visit:

https://support.whitepages.com/hc/en-us/articles/115010106908-How-do-I-edit-or-remove-a-personal-listing-

PIPL

Pipl is a people search engine and no longer offers a direct information removal option. Instead, Pipl recommends you remove your personal information from the source websites it lists under your name; once data is removed from the source website, it should no longer appear in Pipl results.

For further information, visit: https://pipl.com/help/remove/ .

Can I remove my information from the search results?
If you prefer that a certain link will not be shown on pipl.com you should act to remove the page from the source website (you can see the details of the source website next to each result item); once the data is removed from the source, a link should no longer appear in our results page.

SECURING HOME WI-FI NETWORK

SECURING HOME WI-FI NETWORK - DO'S AND DON'TS

- Use an ethernet cable instead of a Wi-Fi connection when possible; disable the wireless network when it is not being used for an extended period.
- Use the most up-to-date hardware and operating systems to maximize your connecting devices' security options.
- Turn on automatic updates for your network devices' firmware or periodically check for updates on the network devices' websites.
- Determine whether you have a router and modem, a hybrid router-modem, or just a modem to best secure your network.
- Enable your devices' firewall and implement strong encryption to block various techniques used by unauthorized individuals to access your network.
- Secure mobile devices that can access your home network; establish screen locks to ensure that stolen devices cannot reconnect to your network.

OVERVIEW

Home wireless networks allow users to connect multiple devices to a single, remote Internet network. While wireless technology makes it easier for users to access the Internet, it also opens the door to new security threats not present in hard-wired connections. Failure to take the proper precautions when configuring your home wireless network may leave your personal information and Internet traffic susceptible to unauthorized individuals. Use the recommendations outlined in this book to secure your home wireless network and better protect your privacy.

WI-FI NETWORK BASICS

A home wireless network consists of a modem, a router, and a selection of personal electronic devices. Unlike Local Area Networks (LAN)—networks requiring all devices to be linked together via network cables—a home wireless network broadcasts radio waves from a router to allow wireless devices to communicate with one another. When the router receives communications from personal devices, the data is then passed through a hard-wired connection to the modem and onto the Internet service provider.
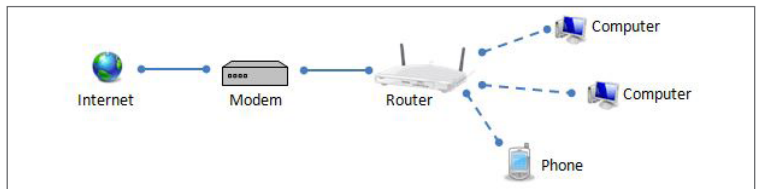
Depending on your particular Internet Service Provider (ISP), geolocation, and Internet package, you may not own all the hardware components of a home wireless network. Technology advancements enable some companies to sell router-modem hybrids, reducing the number of necessary devices. In other scenarios, some ISPs establish relationships with residential complexes so that everyone in a building must use their service and thus, don't provide routers.

If you have a router, you must first gain access to your router to initiate the necessary security settings. To select or review your router's security settings, enter the router's IP address (usually found on a sticker on the back of the device) into any web browser's URL bar. Next, enter the default username and password for your router into the prompt. If you are unaware of your default IP address, password, or username, reference http://www.routeripaddress.com to determine your router's specific details. Even without a router, you can use the information in this chapter to secure your wireless network.

PREVENTING THIRD-PARTY ACCESS TO YOUR WI-FI NETWORK

Some ISPs, such as Comcast XFinity or Verizon FiOS, offer roaming Wi-Fi hotspot services, which allows users to access the Internet on their mobile devices at faster speeds than normally available. These services often use bandwidth from the in-home wireless networks of nearby subscribers. If your ISP offers this type of service, **call the company directly to opt out.**

WHAT TO DO IF YOU SUSPECT YOUR NETWORK HAS BEEN COMPROMISED

Following the recommendations outlined in this book will significantly reduce your home network's chances of becoming compromised. However, it is wise to periodically check if there has been any unauthorized activity on your network. Within the router's web interface, locate the section that identifies the devices connected to your network (e.g., Attached Devices, DHCP Clients Table, Connected Devices, etc.). If you see an unknown device accessing your network, end the connection, and consider contacting your Internet service provider to determine if your network was compromised. If you determine that your network was accessed without authority, **immediately change the usernames and passwords to the wireless network and administrative login pages** If your network was compromised, the hacker may have been able to see your Internet traffic and gain access to your login credentials or other personal data. You willl need to secure all of your online accounts by changing their passwords.

WI-FI SETTINGS OVERVIEW

Follow these steps in order to secure your home wireless network and prevent third-party hackers, neighbors, and scammers from accessing your personal data. The settings in this book apply whether you have a router or not. For router-specific instructions, go to https://routersecurity.org/.

CHANGING DEVICE/ACCOUNT LOGIN SETTINGS

Whether you have a router or simply a modem, your ISP account comes with a default username and password setting, (e.g., Username = "Admin" and Password = "Password") so that anyone can login to their settings for the first time. Once you have logged into your device settings, by going through your ISP or reading your devices' manual, change the defaults to enable additional security. Usernames should not represent your name, home address, or any other personal identity data. Passwords should be unique, alphanumberic combinations with at least 12 characters.
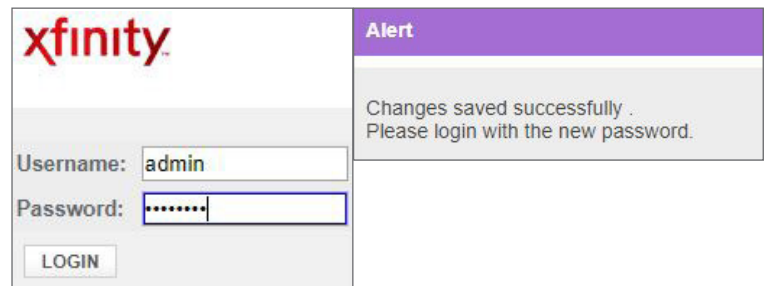
CREATING A NETWORK NAME AND PASSWORD

The Service Set Identifier (SSID) field is used to change the personalized name of your wireless network. Your wireless network name should not reveal any personally identifying information. Your network password—or Pre-Shared Key (PSK)—is the password that you use to connect to the Internet and it is distinct from the password that you use to login to your router. Your PSK password should also be long and complex.

CHOOSING A STRONG ENCRYPTION

To maximize the security of your network, select WPA2-PSK (AES) as your primary security mode, if possible. WPA2 is the strongest form of encryption used to protect wireless networks, while AES is an encryption standard trusted by government organizations to protect sensitive information. The table below shows available encryption types and their associated strengths. Make sure to combine strong encryption protocols with the additional security of a password. This will make it less likely that outsiders can eavesdrop on your Internet activities.

ENCRYPTION	PRIVACY STRENGTH
WPA2-PSK (AES)	Maximum
WPA2-PSK (TKIP)	Minimal (older devices only)
WPA-PSK	Weak or None
WEP	Weak or None

MAC ADDRESS FILTERING

MAC address filtering allows the administrator to create a list of approved devices that can access the network. Devices not on this list are denied access or have to request it from the administrator. MAC addresses are not discoverable through the settings; search for ways to retrieve your personal devices' MAC addresses based on their operating systems.

MAC Address Filtering cannot verify users, only the device accessing the network

Limit the number of MAC addresses you approve to maximize network security.

MONITORING CONNECTED DEVICES

Once logged in, navigate to **Connected Devices** to monitor the devices connected to your wireless network. Check this table often to ensure that only authorized individuals use your Internet. Common signs of unauthorized use include slowed speeds and sudden disconnections.

DISABLE HYBRID ROUTER SETTINGS

In the case of a hybrid router-modem, you can disable the internal router settings. For basic Internet use, a router-modem combo will suffice, but a dedicated modem offers additional security settings, parental controls, and hosting abilities. The ability to enable Hypertext Transfer Protocol Secure (HTTPS) encryption, which makes it more difficult for unauthorized individuals to access your network traffic, is one difference. **Enable Bridge Mode** to turn off router functionality and setup your own.

SETTING UP A FIREWALL

A firewall is a network security system that controls incoming and outgoing network traffic based upon predetermined security rules. The firewall can block a number of methods commonly used by unauthorized individuals to compromise and access networks. Always enable firewall settings to secure your home network. Use the maximum security settings available whenever possible.

INDEX

REFERENCES

1 https://www.statista.com/outlook/216/100/digital-advertising/worldwide#market-revenue

2 https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

3 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf

4 http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/

5 http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

6 http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

7 http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

8 https://techcrunch.com/2018/06/20/instagram-1-billion-users/

9 https://ourworldindata.org/rise-of-social-media

10 https://ourworldindata.org/rise-of-social-media

11 https://news.linkedin.com/about-us

12 https://news.microsoft.com/announcement/microsoft-buys-linkedin/

13 https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html

14 https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084

15 https://www.statista.com/statistics/970920/monetizable-daily-active-twitter-users-worldwide/

16 https://business.twitter.com/

17 https://www.statista.com/outlook/319/109/wearables/united-states

18 https://techcrunch.com/2018/10/29/signal-sealed-sender-feature-messaging-security/

19 https://arstechnica.com/tech-policy/2021/01/whatsapp-users-must-share-their-data-with-facebook-or-stop-using-the-app/

20 https://www.businessinsider.com/what-is-groupme

21 https://www.statista.com/statistics/350461/mobile-messenger-app-usage-usa/

22 https://www.theverge.com/2019/7/24/20708328/google-photos-users-gallery-go-1-billion

23 https://expandedramblings.com/index.php/flickr-stats/

24 https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis

25 https://www.economist.com/finance-and-economics/2017/09/14/how-to-protect-yourself-against-the-theft-of-your-identity

26 https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf