IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS

EIGHTH EDITION, MARCH 2019

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 two-page chapters detailing key privacy considerations on the most popular online services, mobile apps, and consumer devices available in the market today. Each chapter provides you with tools, recommendations, and step-by-step guides to implement settings that maximize your security. The guide is updated twice a year, in March and September.

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

The US Department of Defense creates this guide as a public service, and hopes this guide will help readers keep their identities private and secure.

TABLE OF CONTENTS

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 Right 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:

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this guide. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third-party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only.

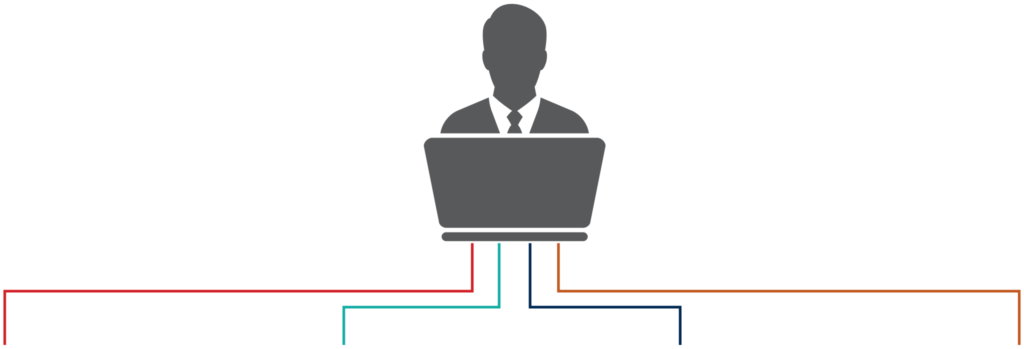
Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government.

DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

WHY IS IDENTITY PROTECTION A CONCERN?

YOUR DATA IS EVERYWHERE

Everything you do creates a stream of data



PERSONAL

- Name
- Birthdate
- Work, Education, and Address History
- Family and Friends
- Likes and Interests

FINANCIAL

- Credit Cards
- Bank Accounts
- Digital Wallets
- Online Payments
- Purchase history

BIOMETRIC

- Face Recognition
- Voice Recognition
- Fitness Tracker Data
- Device Authentication
- DNA Analysis

BEHAVIORAL

- 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 $266 billion worldwide in 2018.[1]
- On the criminal side, personal data is worth a lot of money. PII sells for $1-1,000 dollars each 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 can pose risks.
- Hacks are constant. Your data has probably already been stolen.

YOUR DATA CAN BE DANGEROUS

- Any piece of data alone can be innocuous, but tied to other sources, it becomes a three-dimensional image of you that can pose a threat. Advertising firms, public records companies, or criminals can link disparate information about you 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.

[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

WHAT CAN YOU DO ABOUT IT?

EDUCATE YOURSELF

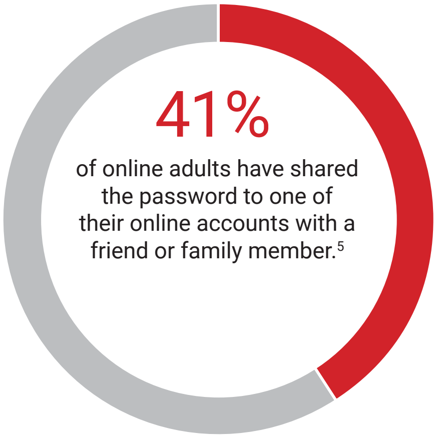
- 74% of people are unaware that Facebook develops profiles of users' interests.[4]
- Knowing the risks puts you ahead of most people.
- The IAPM Guide is a great start. Look at the Table of Contents page for more information sources.

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

PROTECT YOURSELF

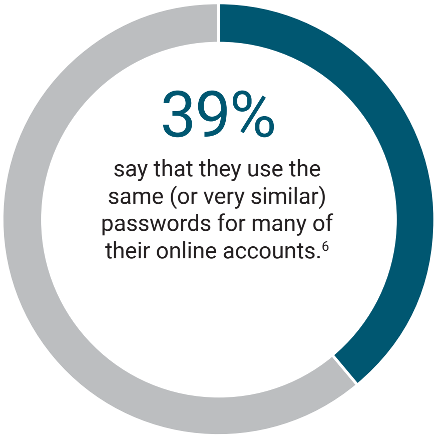
- Use caution before agreeing to share your information. Think before you click.
- Learn how to tell the legitimate from the illegitimate.
- When in doubt, opt out.
- Threats to your identity constantly change. Monitor your credit and online accounts, and keep your software and devices up-to-date.

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



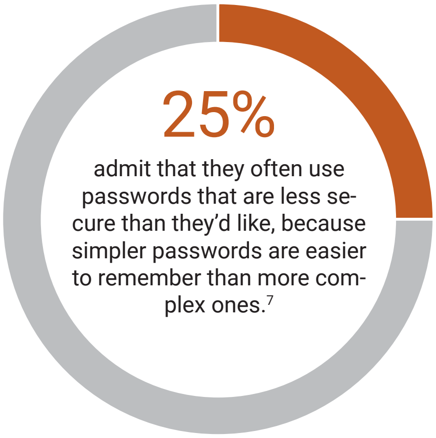
41%

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



39%

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



25%

admit that they often use passwords that are less secure than they'd like, because simpler passwords are easier to remember 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.

[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/*

FACEBOOK

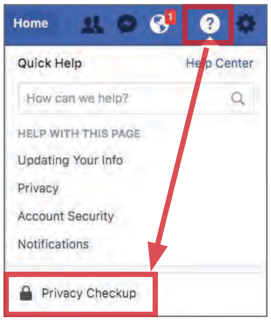
SOCIAL NETWORK - DO'S AND DON'TS

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information 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 access points.
- 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.

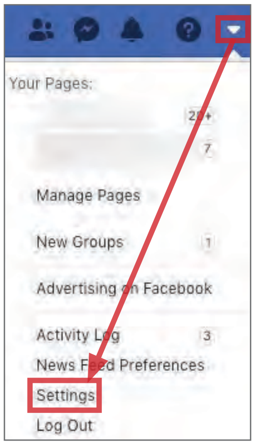
MAXIMIZING YOUR FACEBOOK PRIVACY

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

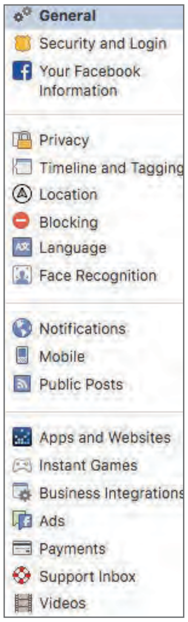
Click on **Privacy Checkup** to change your basic privacy settings.



For more extensive and granular control, navigate to **Settings** from the top drop down menu. Click through each tab to control how your personal information is shared with others.



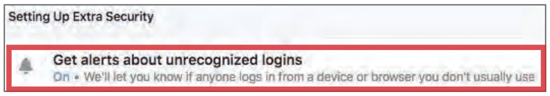
RECOMMENDED SETTINGS



The (1) Security and Login, (2) Privacy, (3) Your Facebook Information, (4) Timeline and tagging, (5) Location, (6) Face Recognition, (7) Public Posts, (8) Ads, and (9) 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.

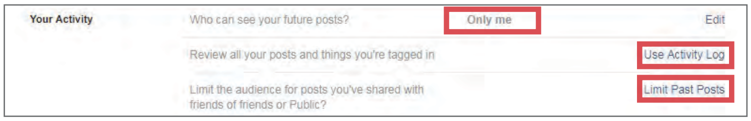
1 The **Security and Login** tab contains settings to protect your login credentials, monitor attempted and successful logins, and recover your account in the event of a lockout. Use **Where You're Logged In** to monitor login activity and end inactive sessions, and **turn ON** alerts for unauthorized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



Setting Up Extra Security

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

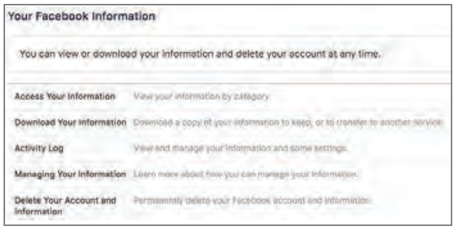
2 Use the **Privacy** tab to control which audiences can search for you, contact you, and see your posts. Under **Your Activity > Use Activity Log**, review past posts individually and limit the audiences for each entry. Use **Limit Past Posts** to retroactively change the settings of all "Public" posts to a "Friends" only audience.



Your Activity	Who can see your future posts?	Only me	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts

3 Use the **Your Facebook Information** tab to view or download your data or delete your account.

This tab contains shortcuts to your **Activity Log** and an informative **Managing Your Information** tab that guides you through common Facebook and Instagram data management questions and concerns.

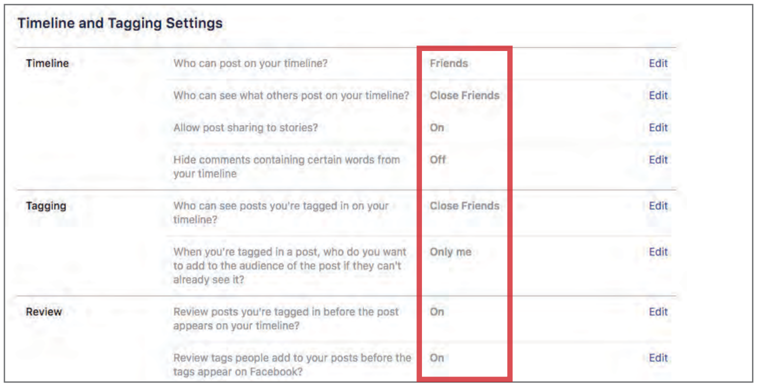


Your Facebook Information

You can view or download your information and delete your account at any time.

Access Your Information	View your information by category
Download Your Information	Download a copy of your information to keep, or to transfer to another service
Activity Log	View and manage your information and some settings.
Managing Your Information	Learn more about how you can manage your information.
Delete Your Account and Information	Permanently delete your Facebook account and information.

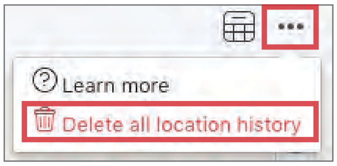
4 **Timeline and Tagging** controls how others interact with your Timeline. Select **View As** to preview what others can see on your profile.



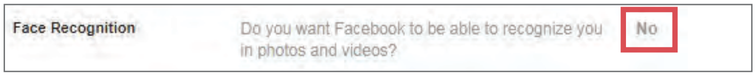
Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Close Friends	Edit
	Allow post sharing to stories?	On	Edit
	Hide comments containing certain words from your timeline	Off	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Close Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Only me	Edit
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

5 Facebook uses your device to obtain and store location data. The **Location** tab displays if your **Location History** is on. Use **View your location history > ••• > Delete all location history** to remove stored data.

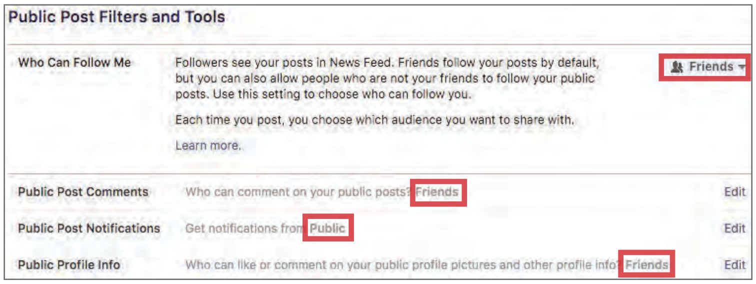


6 Use the **Face Recognition** tab and disable face recognition by setting to **No** as shown. This prevents Facebook from searching and matching your face against all photos and videos uploaded to its database.



Face Recognition	Do you want Facebook to be able to recognize you in photos and videos?	No

7 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** settings as shown.

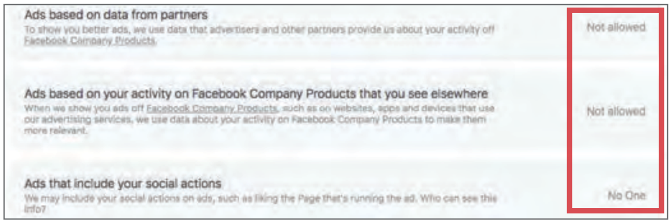


Public Post Filters and Tools

Who Can Follow Me	Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with. Learn more.	Friends
Public Post Comments	Who can comment on your public posts? Friends	Edit
Public Post Notifications	Get notifications from Public	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? Friends	Edit

RECOMMENDED SETTINGS CONTINUED

8 Use the **Ads** tab to prevent Facebook from tracking and using your data for advertising. Under **Ad settings**, adjust each entry to **Not allowed** or **No One.**

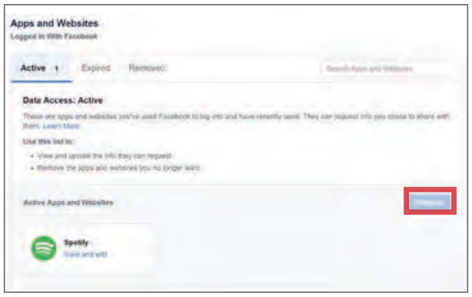


Ads based on data from partners — Not allowed
To show you better ads, we use data that advertisers and other partners provide us about your activity off Facebook Company Products.

Ads based on your activity on Facebook Company Products that you see elsewhere — Not allowed
When we show you ads off Facebook Company Products, such as on websites, apps and devices that use our advertising services, we use data about your activity on Facebook Company Products to make them more relevant.

Ads that include your social actions — No One
We may include your social actions on ads, such as liking the Page that's running the ad. Who can see this info?

9 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 to limit unnecessary access.



Apps and Websites
Logged in With Facebook

Active 1 | Expired | Removed | Search Apps and Websites

Data Access: Active
These are apps and websites you've used Facebook to log into and have recently used. They can request info you chose to share with them. Learn More

Use this list to:
- View and update the info they can request
- Remove the apps and websites you no longer want

Active Apps and Websites

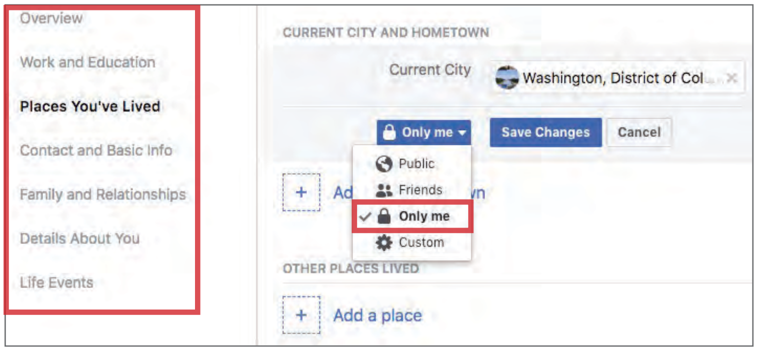
Spotify
View and edit

FACEBOOK PROFILE PAGE

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

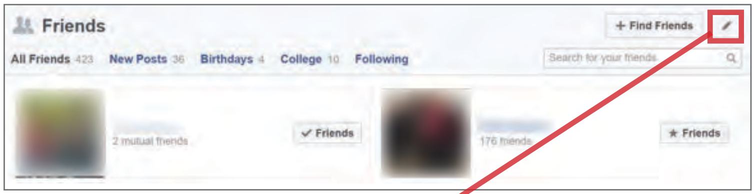
ABOUT

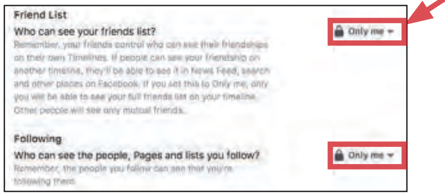
Avoid entering personal data in the **About** section unless required by Facebook. This information is mostly optional and contains data fields including **Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships, Details About You,** and **Life Events**. Use audience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



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**.



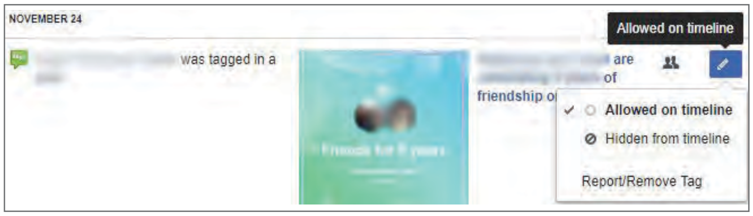


Friend List
Who can see your friends list? — Only me
Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.

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

ACTIVITY LOG

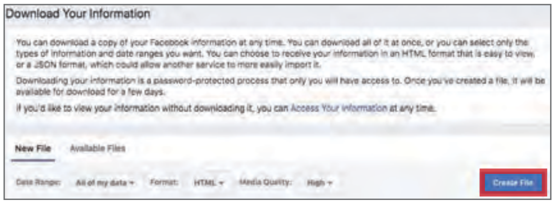
The **Activity Log** tool chronologically displays your **Posts, Posts You're Tagged in**, and **Others' Posts To Your Timeline**. Use the dropdown menu shown to delete or manage how individual posts appear on your Timeline.



REVIEWING YOUR INFORMATION

To review a comprehensive list of data collected by Facebook, navigate to **Settings > Your Facebook Information > Access Your Information**.

You can **Download Your Information** entirely or by type or date range; in HTML or JSON format; and in high, medium, or low media quality.



Download Your Information

You can download a copy of your Facebook information at any time. You can download all of it at once, or you can select only the types of information and date ranges you want. You can choose to receive your information in an HTML format that is easy to view, or a JSON format, which could allow another service to more easily import it.

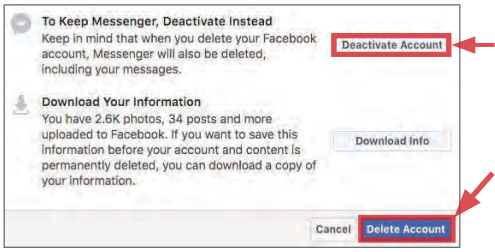
Downloading your information is a password-protected process that only you will have access to. Once you've created a file, it will be available for download for a few days.

If you'd like to view your information without downloading it, you can Access Your Information at any time.

New File | Available Files

Date Range: All of my data ▾ Format: HTML ▾ Media Quality: High ▾ | Create File

DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT



To Keep Messenger, Deactivate Instead
Keep in mind that when you delete your Facebook account, Messenger will also be deleted, including your messages. — Deactivate Account

Download Your Information
You have 2.6K photos, 34 posts and more uploaded to Facebook. If you want to save this information before your account and content is permanently deleted, you can download a copy of your information. — Download Info

Cancel | Delete Account

Deactivating an account removes your name and photos from posts that you have shared. To deactivate your Facebook account, navigate to **Settings > General > Manage Account** then click on **Deactivate your account**. Your account remains deactivated until the next login. Some information may still be visible, such as your name in someone else's friend list and messages you have exchanged.

To delete your account, navigate to **Settings > Your Facebook Information > Delete Your Account and Information**, then click **Delete Account**. The deletion process begins 14 days after request submission, and Facebook will permanently remove most of your data within 90 days.

FACEBOOK MOBILE

SOCIAL NETWORK - DO'S AND DON'TS

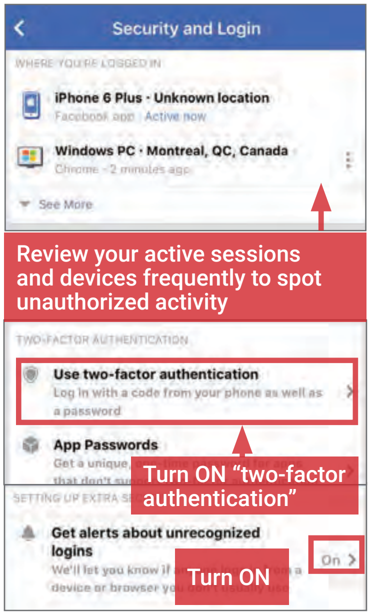
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of yourself or 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 access points.
- 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

Facebook reports 1.49 billion daily active global users in June 2018. Most users access the mobile app, as reflected by Facebook mobile's advertising revenue, which accounted for 91% of Facebook's overall advertising revenue for Q1 2018. Using Facebook's mobile app (vs. website) places your identity at greater risk because smartphones provide to access additional personal data (e.g., location). Use the following recommendations to best protect yourself.

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

iPhone 6 Plus · Unknown location
Facebook app · Active now

Windows PC · Montreal, QC, Canada
Chrome · 2 minutes ago

See More

Review your active sessions and devices frequently to spot unauthorized activity

TWO-FACTOR AUTHENTICATION

Use two-factor authentication
Log in with a code from your phone as well as a password

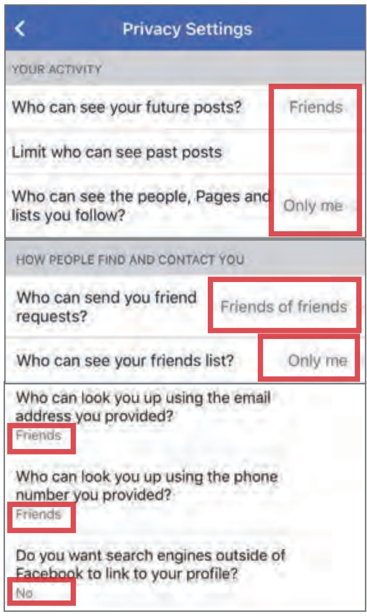
App Passwords
Get a unique,
that don't su

Turn ON "two-factor authentication"

SETTING UP EXTRA SE

Get alerts about unrecognized logins — On
We'll let you know if
device or browser yo

Turn ON



Privacy Settings

YOUR ACTIVITY

Who can see your future posts? — Friends

Limit who can see past posts

Who can see the people, Pages and lists you follow? — Only me

HOW PEOPLE FIND AND CONTACT YOU

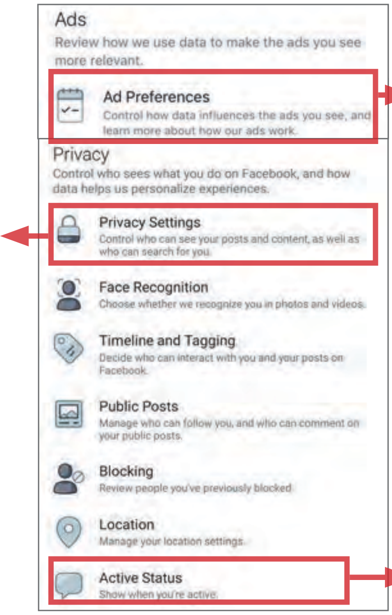
Who can send you friend requests? — Friends of friends

Who can see your friends list? — Only me

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.

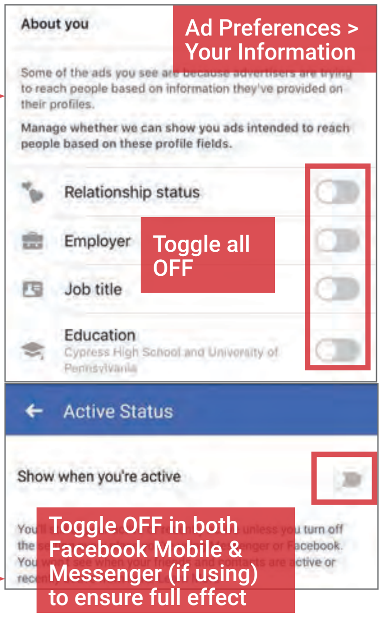
Timeline and Tagging
Decide who can interact with you and your posts on Facebook.

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.



About you

Ad Preferences > Your Information

Some of the ads you see are because advertisers are trying to reach people based on information they've provided on their profiles.

Manage whether we can show you ads intended to reach people based on these profile fields.

Relationship status — Off

Employer — Off

Job title — Off

Education — Off
Cypress High School and University of Pennsylvania

Toggle all OFF

Active Status

Show when you're active — Off

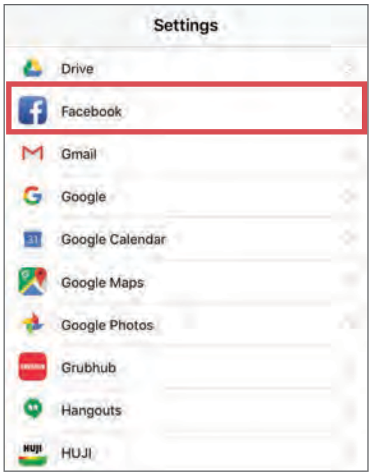
Toggle OFF in both Facebook Mobile & Messenger (if using) to ensure full effect

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.

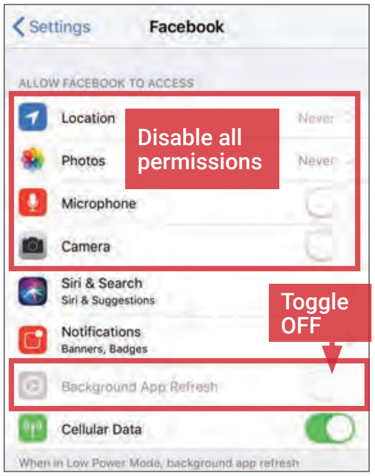
ANDROID SETTINGS

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



Settings

Drive
Facebook
Gmail
Google
Google Calendar
Google Maps
Google Photos
Grubhub
Hangouts
HUJI



Settings — Facebook

ALLOW FACEBOOK TO ACCESS

Location — Never
Photos — Never
Microphone — Off
Camera — Off

Disable all permissions

Siri & Search
Siri & Suggestions

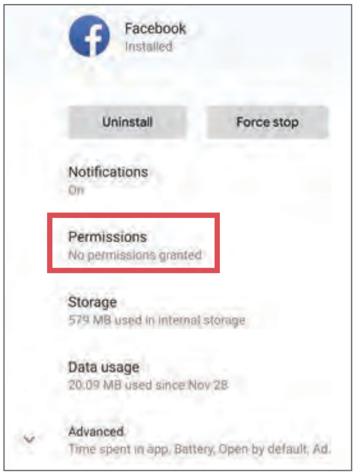
Notifications
Banners, Badges

Background App Refresh — Off

Toggle OFF

Cellular Data — On

When in Low Power Mode, background app refresh



Facebook
Installed

Uninstall — Force stop

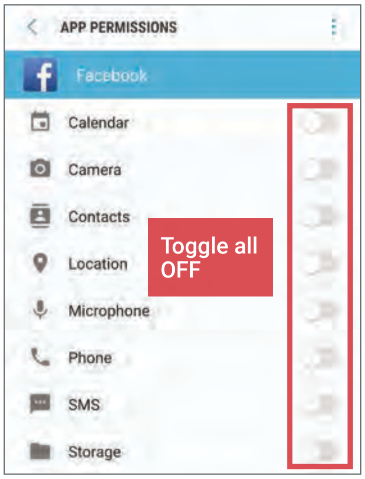
Notifications
On

Permissions
No permissions granted

Storage
579 MB used in internal storage

Data usage
20.09 MB used since Nov 28

Advanced
Time spent in app, Battery, Open by default, Ad



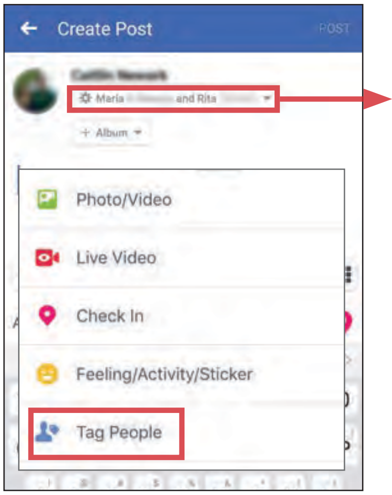
APP PERMISSIONS

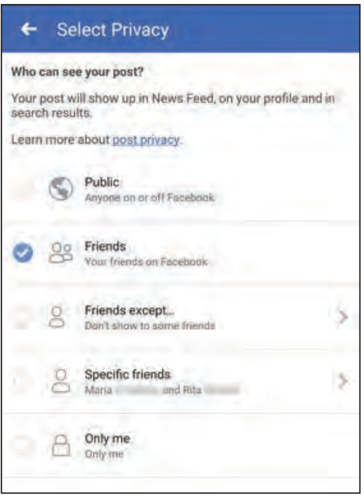
Facebook

Calendar — Off
Camera — Off
Contacts — Off
Location — Off
Microphone — Off
Phone — Off
SMS — Off
Storage — Off

Toggle all OFF

POSTING TO FACEBOOK




Select Privacy

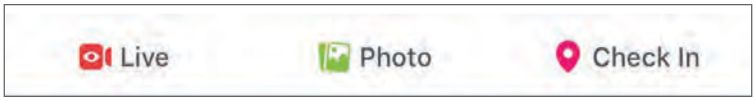
Who can see your post?

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

Learn more about post privacy.

Public
Anyone on or off Facebook
Friends
Your friends on Facebook
Friends except...
Don't show to some friends
Specific friends
Maria [redacted] and Rita [redacted]
Only me
Only me

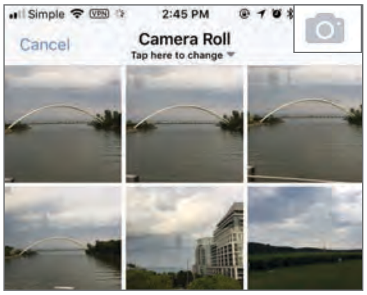
Facebook Mobile allows you to post a new status, upload photos, or check in to locations using the **What's on your mind?** prompt. The icons highlighted on the update prompt are shortcuts for adding further personal information to each post. Several shortcuts pose a significant risk to your privacy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



SELECTING YOUR PRIVACY

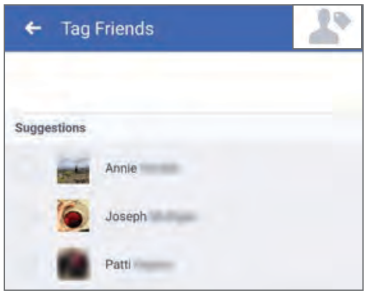
With every post, Facebook Mobile allows you to select the audience through the **Select Privacy** tab beneath your name. For maximum privacy, select **Specific friends** with whom you would like to share your post. Never make your posts available to the public.

ADD PHOTOS



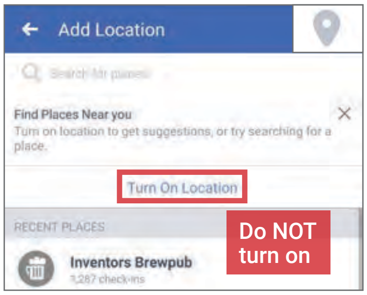
Avoid posting photos to your Timeline. These photos can often be viewed from your contacts' profile pages and can be saved without your knowledge or consent.

TAG FRIENDS



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

ADD LOCATION


Add Location

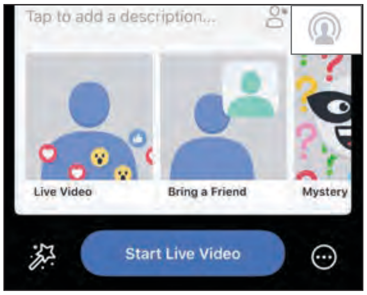
Find Places Near you

Turn on location to get suggestions, or try searching for a place.

Do NOT turn on

Never disclose your location within a Facebook post. Doing so allows Facebook to keep records on your whereabouts and allows others to see when you are away from home.

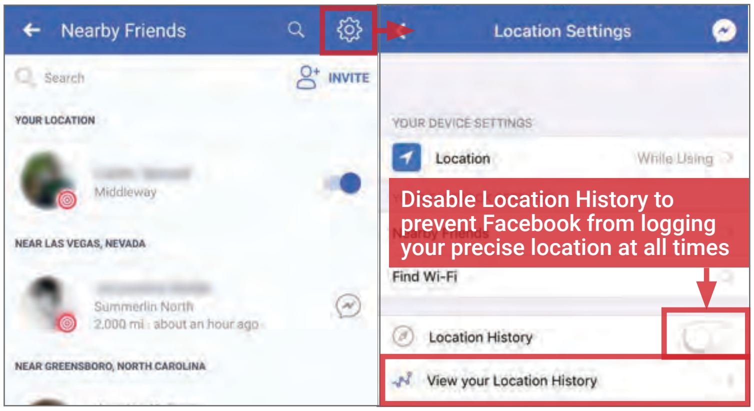
LIVE VIDEO BROADCAST



Avoid posting live video broadcasts. Videos are hard to vet for potentially harmful data and can lead to legal repercussions if others believe a video compromises their privacy.

NEARBY FRIENDS - LOCATION SETTINGS

Nearby Friends allows you to share your location with friends. When activated, Facebook collects your location data, even while you are not using the app, and continually broadcasts your approximate locations to your friends. You also have the option to allow certain users to see your precise location for set periods of time. Do not turn on **Nearby Friends**.

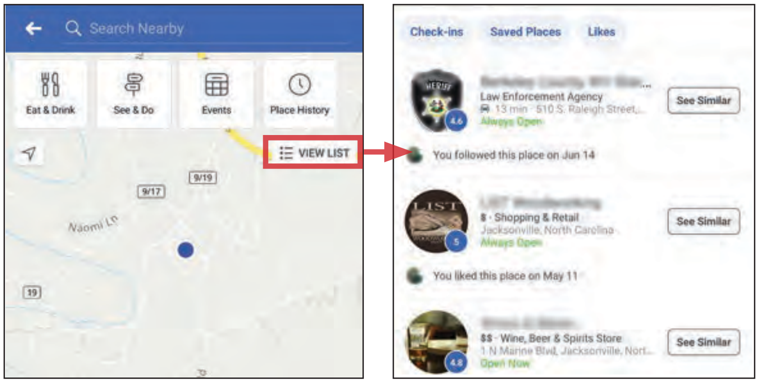


Disable Location History to prevent Facebook from logging your precise location at all times

When this feature is enabled, Facebook builds a history of your precise locations. You can view and manage this information from **Settings > Location > View your Location History**. In general, avoid giving Facebook permission to track your location.

LOCAL

Local uses your GPS location to display local venues. When activated, the feature permits check-ins, provides a map of your location, and suggests places to go based on where you and your friends have already been, or on situational needs such as dining. Avoid posting on these public threads.



To use this feature, you must have **Location History** enabled. This feature permits Facebook to track your precise location, even when the app is not in use. Avoid giving Facebook permission to track your location.

TWITTER

SOCIAL NETWORK - DO'S AND DON'TS

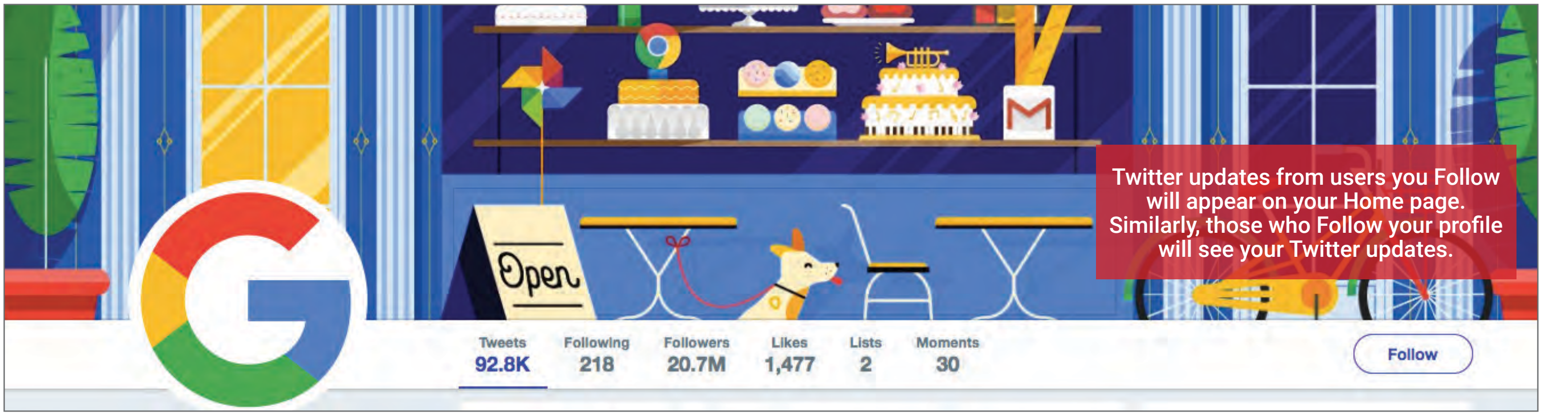
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions 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 access points.
- 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

Twitter is a social networking and micro-blogging site that hosts 326 million monthly active users, as of mid 2018. Twitter allows users to post text-based 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 its mobile app. For most, Twitter is used as a source to discover breaking news developments and stay up-to-date on current events or their friends' recent whereabouts. Should you choose to maintain a Twitter account, use the recommendations in this card to enhance your privacy.

TWITTER PROFILES

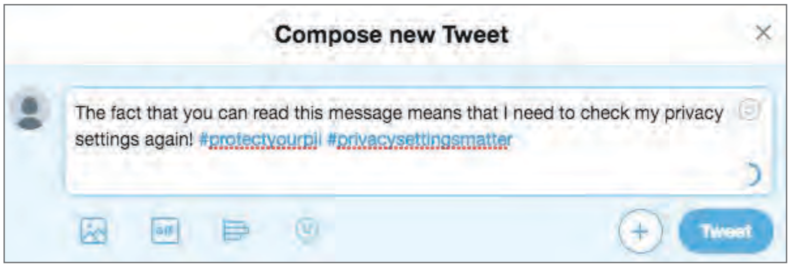
Profile pages can be operated by a single individual, a group of individuals, or even large organizations. Regardless of who maintains the account, each individual profile is labeled with a unique username known as a Twitter Handle (e.g., @google). Handles allow other users to locate profiles and mention them in posts. In general, profile pages tend to contain some of the account owner's personal data and display every Tweet posted by that user.



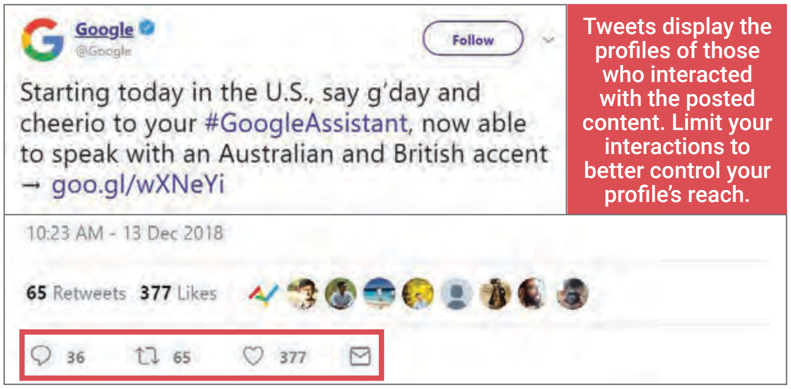
Twitter updates from users you Follow will appear on your Home page. Similarly, those who Follow your profile will see your Twitter updates.

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.



The fact that you can read this message means that I need to check my privacy settings again! #protectyourpii #privacysettingsmatter



Starting today in the U.S., say g'day and cheerio to your #GoogleAssistant, now able to speak with an Australian and British accent → goo.gl/wXNeYi

10:23 AM - 13 Dec 2018

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 the post through the icons highlighted to the left. These icons permit actions including **Replies, Retweets, Likes,** and **More**.

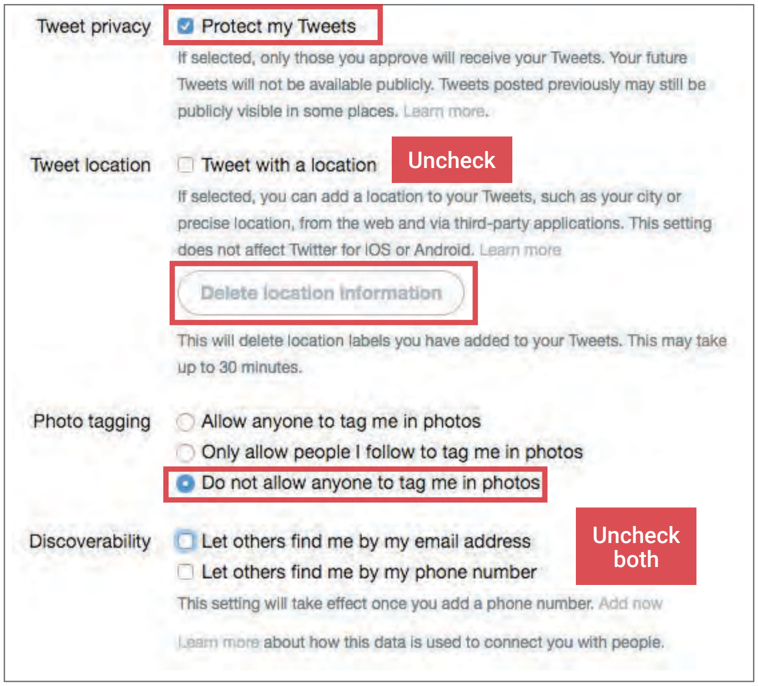
- **Replies** - Replies are text responses to another user's Tweet. The Reply prompt automatically mentions the author of the original Tweet within the text of the reply.
- **Retweets** - Retweets are used to forward other users' Tweets to your personal followers. Retweets always retain a link back to 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.

TWITTER SETTINGS

Access Twitter's settings by selecting the thumbnail image of your profile photo in the top banner. From the dropdown menu, select **Settings and privacy** and navigate to pages containing customizable security options: **Privacy and safety, Email notifications,** and **Account.** After configuring your privacy settings, access your Twitter data tab to review device and login histories to ensure that your account has not been accessed by unauthorized users.

PRIVACY AND SAFETY

Apply the settings shown below in the **Privacy and safety** tab to control how others can interact with your Twitter profile and your Tweets. Save changes.



Tweet privacy ☑ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location □ Tweet with a location **Uncheck**

If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more

Delete location information

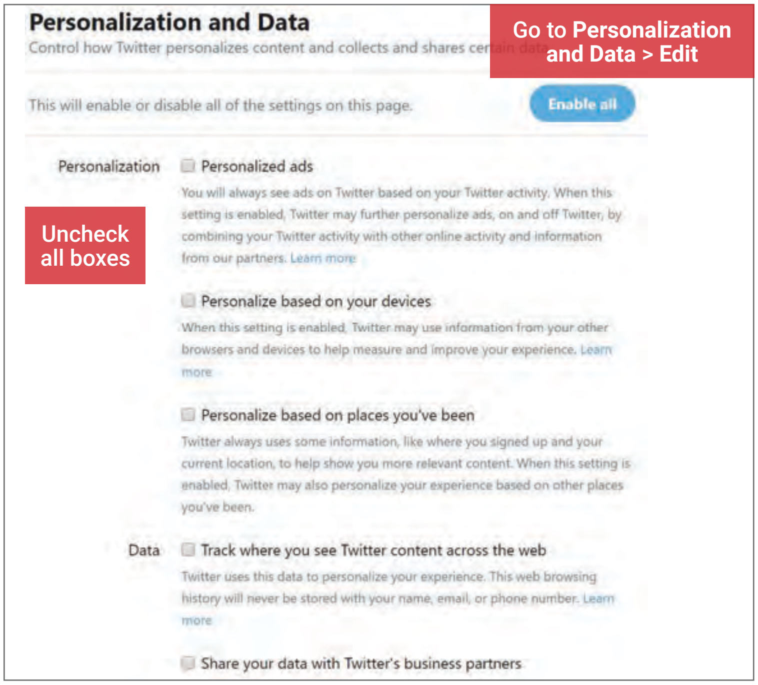
This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging
○ Allow anyone to tag me in photos
○ Only allow people I follow to tag me in photos
● Do not allow anyone to tag me in photos

Discoverability
□ Let others find me by my email address
□ Let others find me by my phone number
Uncheck both

This setting will take effect once you add a phone number. Add now

Learn more about how this data is used to connect you with people.



Personalization and Data

Control how Twitter personalizes content and collects and shares certain data

Go to Personalization and Data > Edit

This will enable or disable all of the settings on this page. Enable all

Uncheck all boxes

Personalization □ Personalized ads

You will always see ads on Twitter based on your Twitter activity. When this setting is enabled, Twitter may further personalize ads, on and off Twitter, by combining your Twitter activity with other online activity and information from our partners. Learn more

□ Personalize based on your devices

When this setting is enabled, Twitter may use information from your other browsers and devices to help measure and improve your experience. Learn more

□ 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.

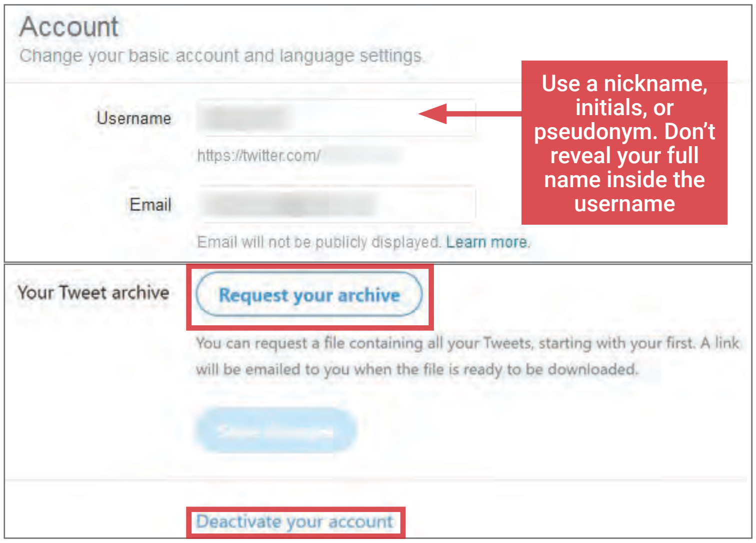
Data □ Track where you see Twitter content across the web

Twitter uses this data to personalize your experience. This web browsing history will never be stored with your name, email, or phone number. Learn more

□ Share your data with Twitter's business partners

ACCOUNT SETTINGS

Account settings allow you to customize your Twitter handle and contact email. You can also request your **Twitter archive** which contains a transcript of all of your past Tweets and replies, or elect to **Deactivate your account**.



Account

Change your basic account and language settings.

Username

https://twitter.com/

Email

Email will not be publicly displayed. Learn more.

Use a nickname, initials, or pseudonym. Don't reveal your full name inside the username

Your Tweet archive Request your archive

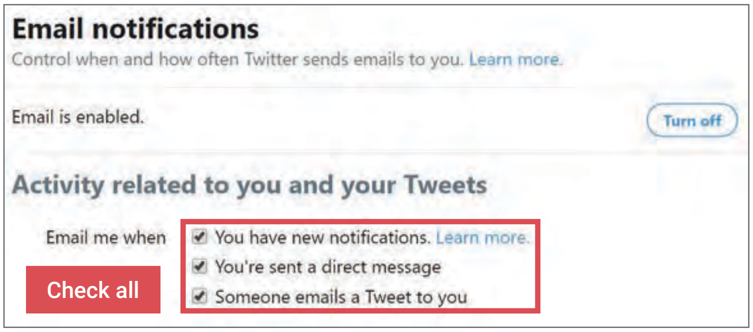
You can request a file containing all your Tweets, starting with your first. A link will be emailed to you when the file is ready to be downloaded.

Deactivate your account

In the **Security** section, use **Set up login verification** and check the box for **Password reset verification** to further secure your account.

EMAIL NOTIFICATIONS SETTINGS

Email notifications alert you when others interact with your profile or content. For maximum security, customize the notifications settings to receive all alerts related to you and your account activities. Save changes.



Email notifications

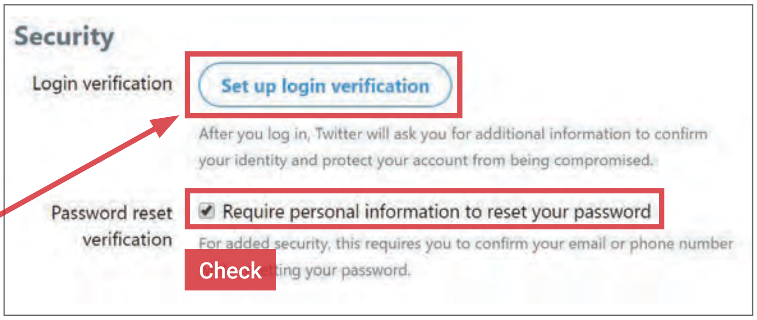
Control when and how often Twitter sends emails to you. Learn more.

Email is enabled. Turn off

Activity related to you and your Tweets

Email me when
☑ You have new notifications. Learn more.
☑ You're sent a direct message
☑ Someone emails a Tweet to you

Check all



Security

Login verification Set up login verification

After you log in, Twitter will ask you for additional information to confirm your identity and protect your account from being compromised.

Password reset verification ☑ Require personal information to reset your password

For added security, this requires you to confirm your email or phone number ~~when rese~~ting your password.

Check

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 and forward photos you post, and save or forward 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 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.

INSTAGRAM OVERVIEW

natgeoadventure

48,109 likes

natgeoadventure Photo @fred_pompermayer The magnificent power of Mother Nature

View all 222 comments

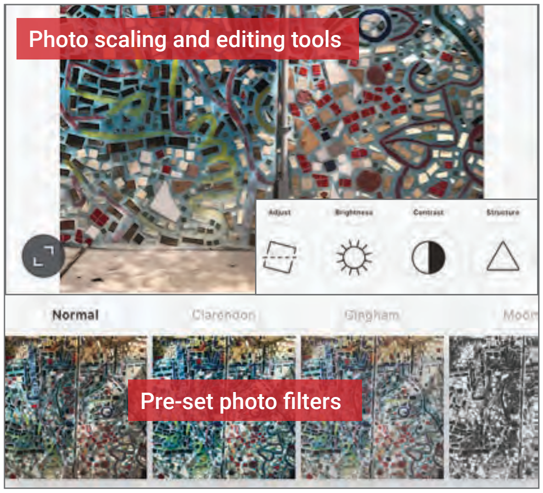


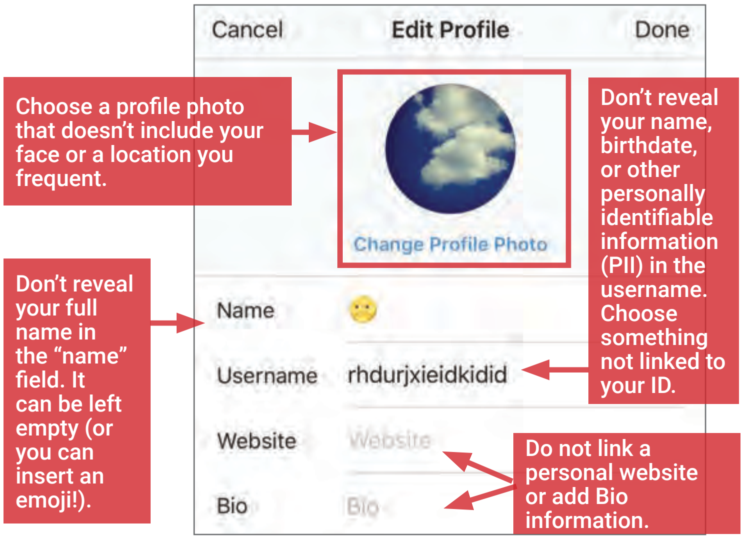
Photo scaling and editing tools

Pre-set photo filters

Instagram is a photo-sharing application that allows users to curate original content using pictures and videos. With 1 billion monthly active users as of June 2018, it is currently the second most popular social networking service (SNS) in the world, exceeded only by Facebook (which acquired Instagram in April 2012). Instagram functions primarily as a mobile platform. Its popularity stems from the ease with which users can take photos on the go and quickly upload, edit (using many pre-set digital filters), and post images.

In terms of privacy, Instagram accounts can be either **public** or **private**. Content posted on public Instagram accounts is indexed and can be searched and viewed by anyone, including non-Instagram members, via search engines such as Google. 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.**

MANAGING YOUR INSTAGRAM PROFILE


Cancel | Edit Profile | Done

Change Profile Photo

Name

Username rhdurjxieidkidid

Website: Website

Bio: Bio

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

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

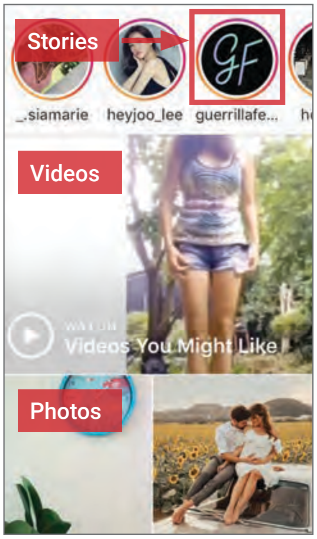
Don't reveal your name, birthdate, or other personally identifiable information (PII) in the username. Choose something not linked to your ID.

Do not link a personal website or add Bio information.

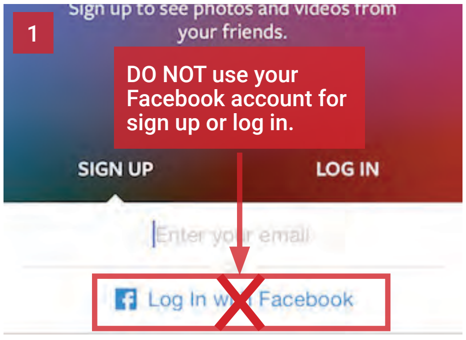
INSTAGRAM MEDIA FORMATS

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

- **Stories** are temporary video or photo posts that you share in real time but which are not 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).



ACCOUNT REGISTRATION - PRIVACY TIPS


1

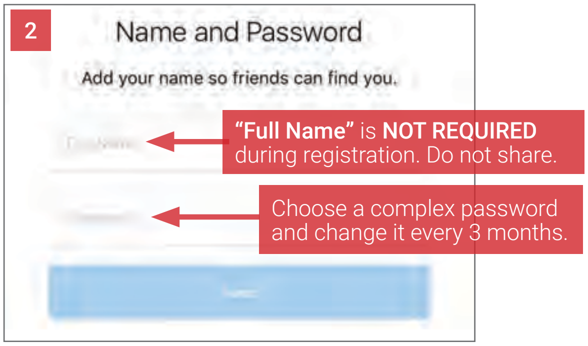
Sign up to see photos and videos from your friends.

SIGN UP | LOG IN

Enter your email

Log In with Facebook

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

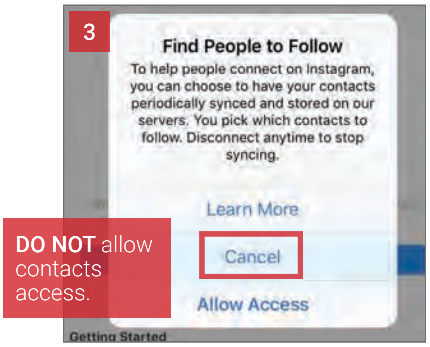

2

Name and Password

Add your name so friends can find you.

"Full Name" is NOT REQUIRED during registration. Do not share.

Choose a complex password and change it every 3 months.


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

Cancel

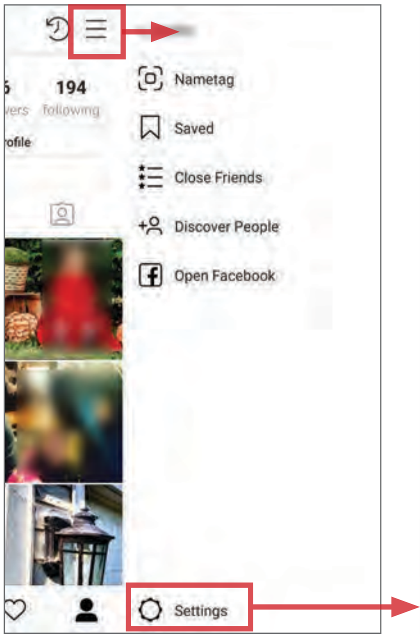
Allow Access

Getting Started

DO NOT allow contacts access.

PRIVACY SETTINGS

To access your privacy settings, go to your **Profile** and tap ☰ icon in the top-right corner of the screen. Apply the settings shown below to control how your photos and videos are shared, and to minimize the amount of personal information you share with Instagram and third parties.



194 following

Nametag

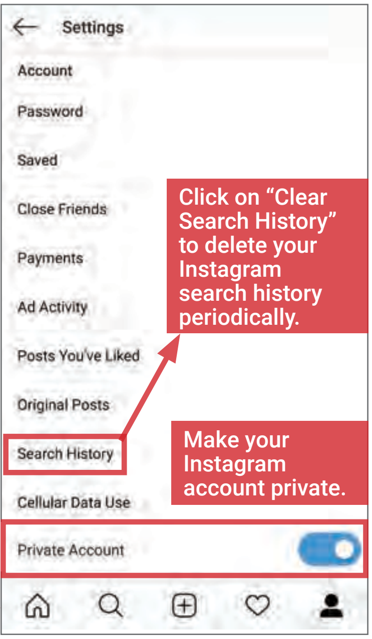
Saved

Close Friends

Discover People

Open Facebook

Settings



Settings

Account

Password

Saved

Close Friends

Payments

Ad Activity

Posts You've Liked

Original Posts

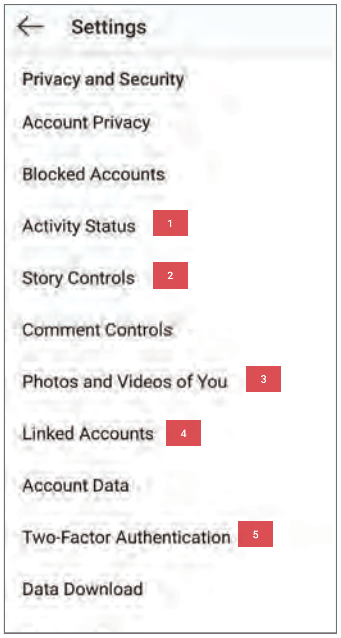
Search History

Cellular Data Use

Private Account

Click on "Clear Search History" to delete your Instagram search history periodically.

Make your Instagram account private.



Settings

Privacy and Security

Account Privacy

Blocked Accounts

Activity Status 1

Story Controls 2

Comment Controls

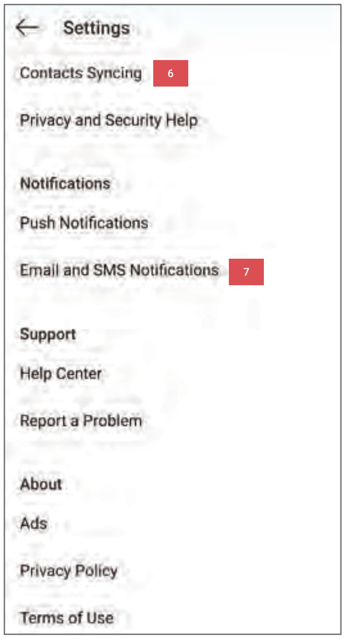
Photos and Videos of You 3

Linked Accounts 4

Account Data

Two-Factor Authentication 5

Data Download



Settings

Contacts Syncing 6

Privacy and Security Help

Notifications

Push Notifications

Email and SMS Notifications 7

Support

Help Center

Report a Problem

About

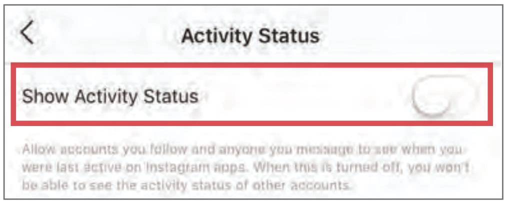
Ads

Privacy Policy

Terms of Use

1 ACTIVITY STATUS

Toggle OFF "Show Activity Status" to prevent other users from seeing when you were last active on Instagram apps.

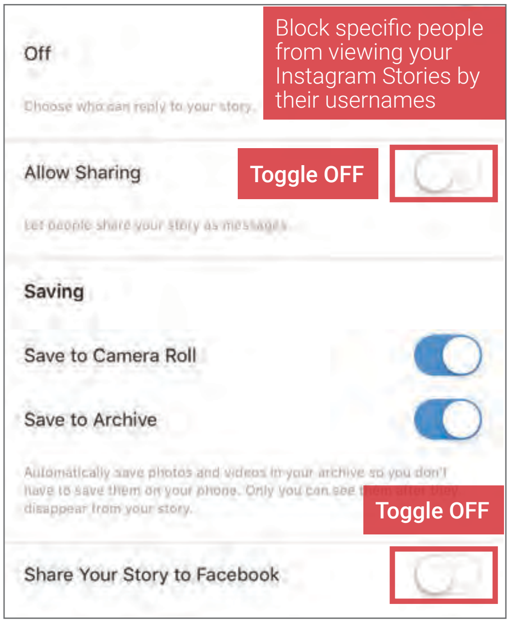


Activity Status

Show Activity Status

Allow accounts you follow and anyone you message to see when you were last active on Instagram apps. When this is turned off, you won't be able to see the activity status of other accounts.

2 STORY CONTROLS



Off

Choose who can reply to your story.

Block specific people from viewing your Instagram Stories by their usernames

Allow Sharing — Toggle OFF

Let people share your story as messages.

Saving

Save to Camera Roll

Save to Archive

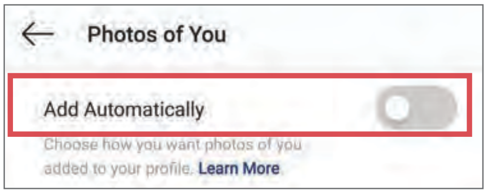
Automatically save photos and videos in your archive so you don't have to save them on your phone. Only you can see them after they disappear from your story.

Toggle OFF

Share Your Story to Facebook

3 PHOTOS & VIDEOS OF YOU

Toggle OFF "**Add Automatically**" to review when others tag you in photos before they are added automatically to your Instagram profile.

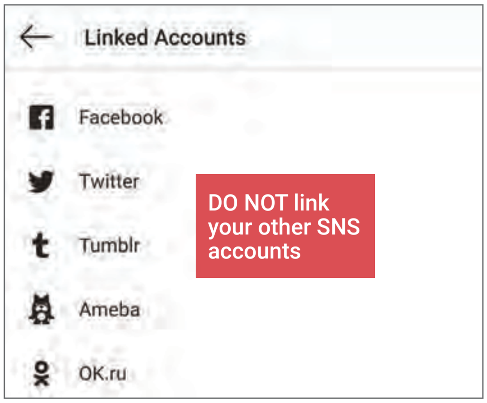


Photos of You

Add Automatically

Choose how you want photos of you added to your profile. Learn More

4 LINKED ACCOUNTS



Linked Accounts

Facebook

Twitter

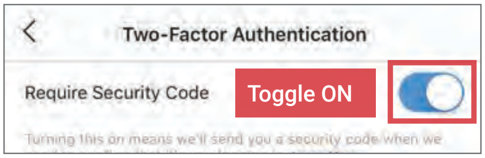
Tumblr

Ameba

OK.ru

DO NOT link your other SNS accounts

5 2-FACTOR AUTHENTICATION

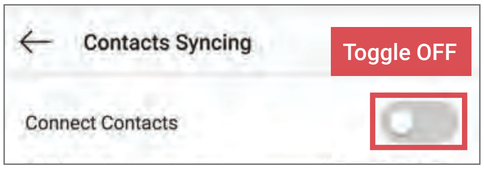


Two-Factor Authentication

Require Security Code — Toggle ON

Turning this on means we'll send you a security code when we

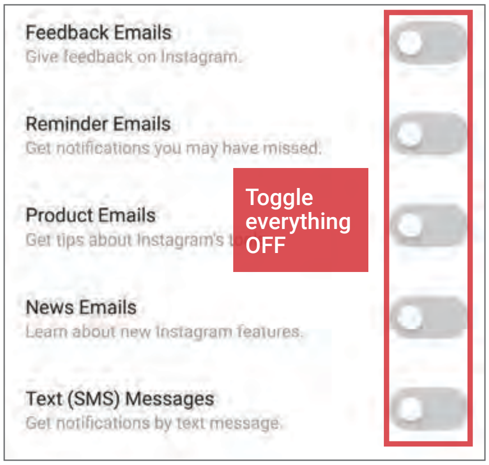
6 CONTACTS SYNCING



Contacts Syncing — Toggle OFF

Connect Contacts

7 EMAIL AND SMS



Feedback Emails

Give feedback on Instagram.

Reminder Emails

Get notifications you may have missed.

Product Emails

Get tips about Instagram's t

Toggle everything OFF

News Emails

Learn about new Instagram features.

Text (SMS) Messages

Get notifications by text message.

DELETING INSTAGRAM

From the **Settings** page, click on **Help Center**, then type in "**delete my account**" to pull up the Delete Your Account page. Follow the steps and confirm deletion by clicking "**Permanently delete my account.**" Once you delete your account, it can't be reactivated and you can't sign up again with the same username.

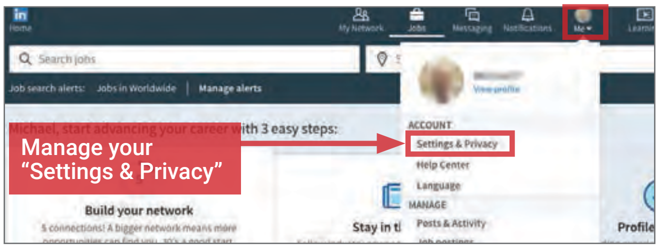
LINKEDIN

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 any information you post and share 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 access points.
- 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.

MANAGING YOUR LINKEDIN PRESENCE

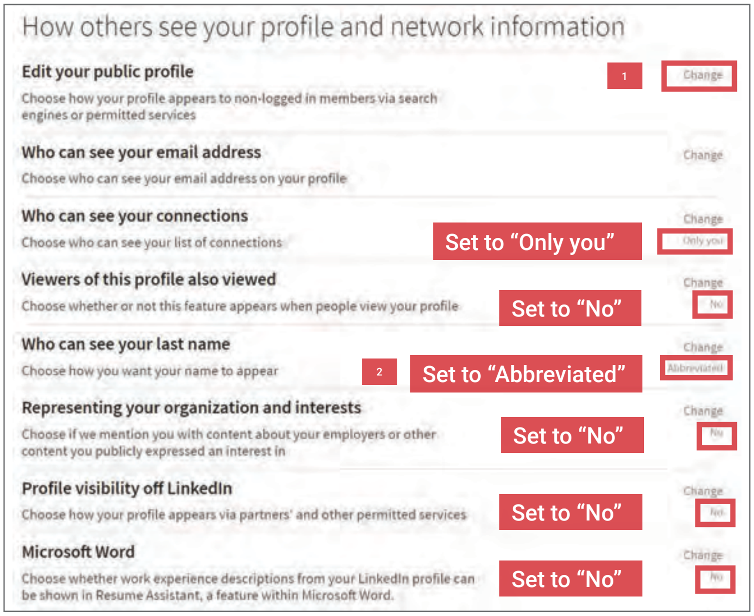
LinkedIn is a professional networking service with 590 million users worldwide. It is mainly used to connect employers who create job postings and job seekers who share their resumes and CVs. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar interests and backgrounds. They can also share their areas of expertise, skills, personal interests, and hobbies. Since 2016, LinkedIn has been a subsidiary of Microsoft. Follow the recommended settings to limit the exposure of your personally identifiable information (PII) without foregoing LinkedIn's many useful features.


Home
My Network
Jobs
Messaging
Notifications
Me
Learning
Search jobs
Job search alerts: Jobs in Worldwide | Manage alerts
[redacted]
View profile
ACCOUNT
Settings & Privacy
Help Center
Language
MANAGE
Posts & Activity
Job postings
Michael, start advancing your career with 3 easy steps:
Build your network
5 connections! A bigger network means more opportunities can find you. 30's a good start.
Stay in t
Profile

Manage your "Settings & Privacy"

PRIVACY SETTINGS

Click on the **Privacy** tab under **Settings & Privacy**. Apply the settings shown below to ensure that your profile is visible only to the people of your choosing.



How others see your profile and network information

Edit your public profile — 1 — Change
Choose how your profile appears to non-logged in members via search engines or permitted services

Who can see your email address — Change
Choose who can see your email address on your profile

Who can see your connections — Change — Only you — Set to "Only you"
Choose who can see your list of connections

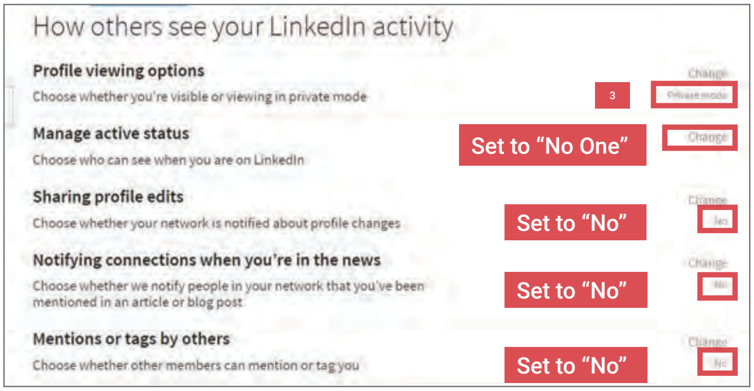
Viewers of this profile also viewed — Change — No — Set to "No"
Choose whether or not this feature appears when people view your profile

Who can see your last name — Change — Abbreviated — 2 — Set to "Abbreviated"
Choose how you want your name to appear

Representing your organization and interests — Change — No — Set to "No"
Choose if we mention you with content about your employers or other content you publicly expressed an interest in

Profile visibility off LinkedIn — Change — No — Set to "No"
Choose how your profile appears via partners' and other permitted services

Microsoft Word — Change — No — Set to "No"
Choose whether work experience descriptions from your LinkedIn profile can be shown in Resume Assistant, a feature within Microsoft Word.



How others see your LinkedIn activity

Profile viewing options — Change — Private mode — 3
Choose whether you're visible or viewing in private mode

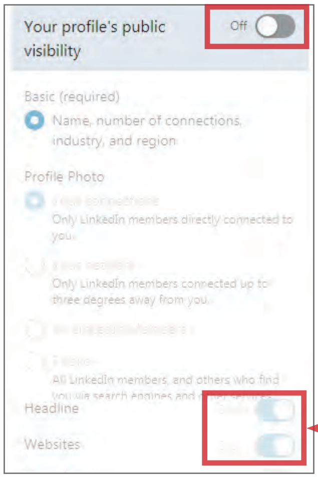
Manage active status — Change — Set to "No One"
Choose who can see when you are on LinkedIn

Sharing profile edits — Change — No — Set to "No"
Choose whether your network is notified about profile changes

Notifying connections when you're in the news — Change — No — Set to "No"
Choose whether we notify people in your network that you've been mentioned in an article or blog post

Mentions or tags by others — Change — No — Set to "No"
Choose whether other members can mention or tag you

1 EDITING YOUR PUBLIC PROFILE



Your profile's public visibility — Off

Basic (required)
● Name, number of connections, industry, and region

Profile Photo
○ Only LinkedIn members directly connected to you.
○ Only LinkedIn members connected up to three degrees away from you.
○
○ All LinkedIn members, and others who find you via search engines and other services

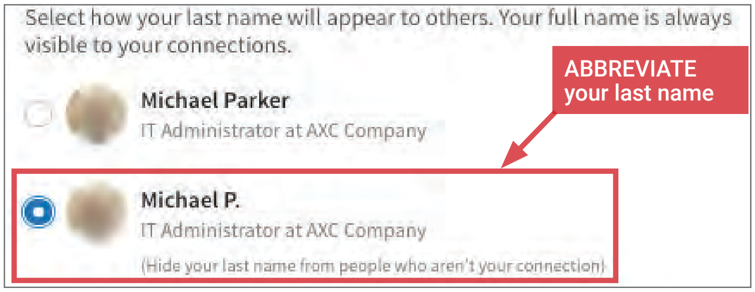
Headline
Websites

Uncheck all optional fields

Set your public profile visibility to "**Off**" unless you are actively seeking a job or are otherwise required to have a public professional web presence.

If your public profile is visible, make sure all the optional fields are checked **OFF** to prevent overexposure.

2 WHO CAN SEE YOUR LAST NAME



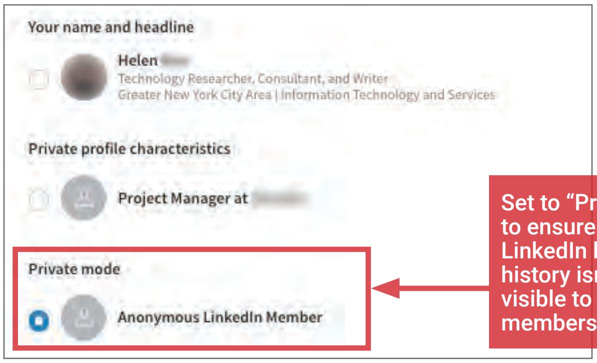
Select how your last name will appear to others. Your full name is always visible to your connections.

○ Michael Parker
IT Administrator at AXC Company

● Michael P.
IT Administrator at AXC Company
(Hide your last name from people who aren't your connection)

ABBREVIATE your last name

3 PROFILE VIEWING OPTIONS



Your name and headline
○ Helen [redacted]
Technology Researcher, Consultant, and Writer
Greater New York City Area | Information Technology and Services

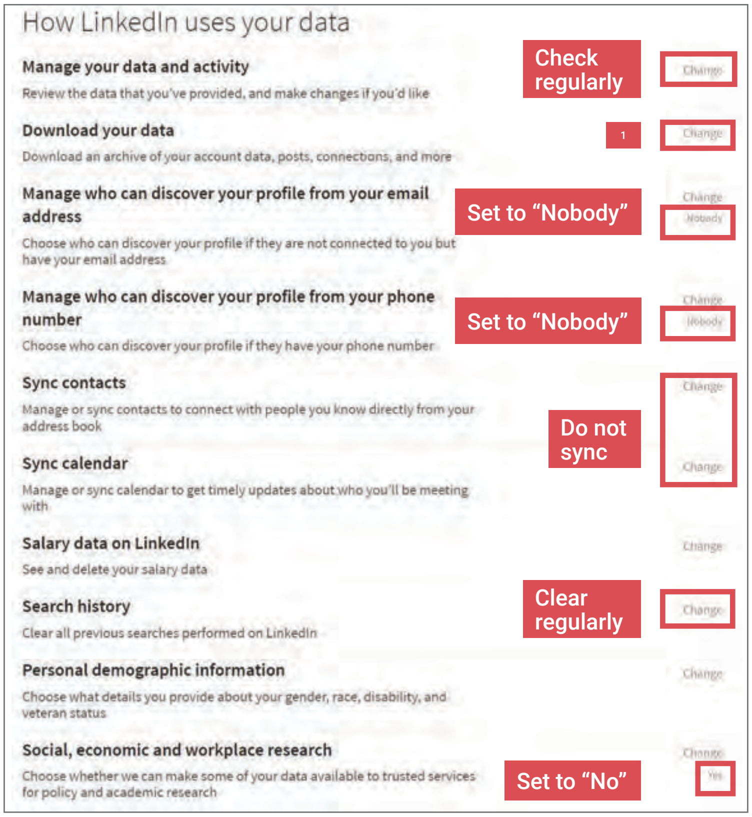
Private profile characteristics
○ Project Manager at [redacted]

Private mode
● Anonymous LinkedIn Member

Set to "Private Mode" to ensure that your LinkedIn browsing history isn't made visible to other members

DATA COLLECTION, DATA PRIVACY, & ADS

Apply the **Data Privacy and Advertising** settings shown below to minimize the amount of information you share with LinkedIn and third parties. You can find these settings under **Settings & Privacy > Privacy > How LinkedIn uses your data**. .



How LinkedIn uses your data

Manage your data and activity – Review the data that you've provided, and make changes if you'd like – Change – Check regularly

Download your data – Download an archive of your account data, posts, connections, and more – Change – 1

Manage who can discover your profile from your email address – Choose who can discover your profile if they are not connected to you but have your email address – Change – Nobody – Set to “Nobody”

Manage who can discover your profile from your phone number – Choose who can discover your profile if they have your phone number – Change – Nobody – Set to “Nobody”

Sync contacts – Manage or sync contacts to connect with people you know directly from your address book – Change – Do not sync

Sync calendar – Manage or sync calendar to get timely updates about who you'll be meeting with – Change – Do not sync

Salary data on LinkedIn – See and delete your salary data – Change

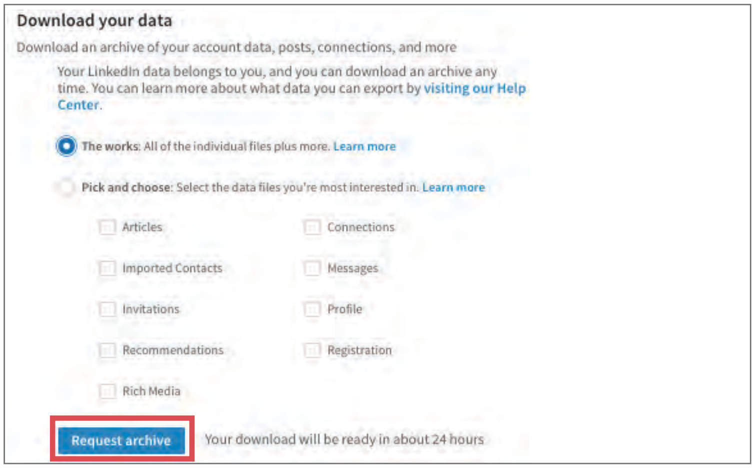
Search history – Clear all previous searches performed on LinkedIn – Change – Clear regularly

Personal demographic information – Choose what details you provide about your gender, race, disability, and veteran status – Change

Social, economic and workplace research – Choose whether we can make some of your data available to trusted services for policy and academic research – Change – Yes – Set to “No”

1 REQUEST DATA ARCHIVE

LinkedIn maintains an archive detailing each user's unique account activity. Navigate to **Settings & Privacy > Privacy > How LinkedIn uses your data > Download your data** to receive a comprehensive report of your past activity and network information. Review your data frequently to ensure that you are not over-sharing information. Visit the **Help Center** to see the types of information LinkedIn collects.



Download your data

Download an archive of your account data, posts, connections, and more

Your LinkedIn data belongs to you, and you can download an archive any time. You can learn more about what data you can export by visiting our Help Center.

● The works: All of the individual files plus more. Learn more

○ Pick and choose: Select the data files you're most interested in. Learn more

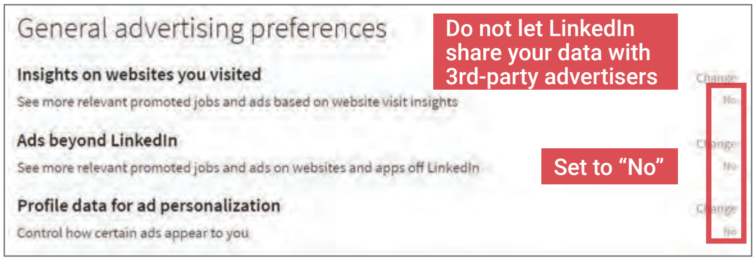
□ Articles □ Connections
□ Imported Contacts □ Messages
□ Invitations □ Profile
□ Recommendations □ Registration
□ Rich Media

Request archive – Your download will be ready in about 24 hours

CLOSING YOUR LINKEDIN ACCOUNT

If you no longer plan to use the LinkedIn service, click **Closing Your LinkedIn Account** under Account settings and confirm your decision.

Navigate to **Settings & Privacy > Ads > General advertising preferences** and implement the suggested settings below to minimize the amount of data LinkedIn collects about you. The section called **Data Collected on LinkedIn** on the Ads page should be reviewed frequently with most of the featured turned OFF unless you are actively job searching or building professional networks.



General advertising preferences

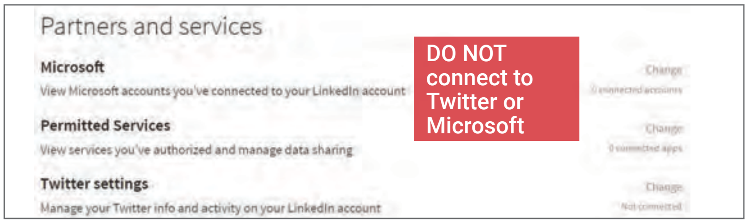
Do not let LinkedIn share your data with 3rd-party advertisers

Insights on websites you visited – See more relevant promoted jobs and ads based on website visit insights – Change – No

Ads beyond LinkedIn – See more relevant promoted jobs and ads on websites and apps off LinkedIn – Change – No – Set to “No”

Profile data for ad personalization – Control how certain ads appear to you – Change – No

Navigate to **Settings & Privacy > Account > Partners and Third Parties > Permitted Services** monthly and review which services and apps you've given access to your LinkedIn data. Remove permissions from services that you no longer use nor require.



Partners and services

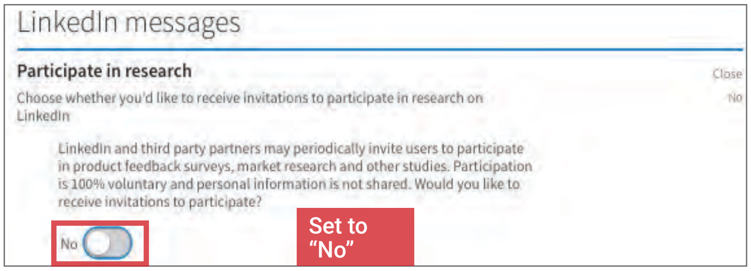
DO NOT connect to Twitter or Microsoft

Microsoft – View Microsoft accounts you've connected to your LinkedIn account – Change – 0 connected accounts

Permitted Services – View services you've authorized and manage data sharing – Change – 0 connected apps

Twitter settings – Manage your Twitter info and activity on your LinkedIn account – Change – Not connected

Navigate to **Settings > Communications > LinkedIn messages** and set **Participate in research** to **No** to prevent LinkedIn from using your activities for internal research purposes.



LinkedIn messages

Participate in research – Close

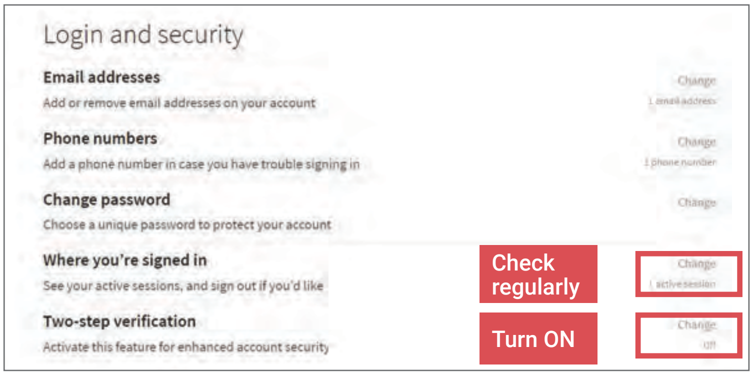
Choose whether you'd like to receive invitations to participate in research on LinkedIn – No

LinkedIn and third party partners may periodically invite users to participate in product feedback surveys, market research and other studies. Participation is 100% voluntary and personal information is not shared. Would you like to receive invitations to participate?

No – Set to “No”

LOGINS AND SECURITY SETTINGS

Navigate to **Settings & Privacy > Account > Login and security > Two-step verification** and select **Turn on**. Use **Where you're signed in** to regularly check for suspicious account access activity.



Login and security

Email addresses – Add or remove email addresses on your account – Change – 1 email address

Phone numbers – Add a phone number in case you have trouble signing in – Change – 1 phone number

Change password – Choose a unique password to protect your account – Change

Where you're signed in – See your active sessions, and sign out if you'd like – Change – 1 active session – Check regularly

Two-step verification – Activate this feature for enhanced account security – Change – Off – Turn ON

PHOTO SHARING SERVICES

PHOTO SHARING SERVICES - 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 and share 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?	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)

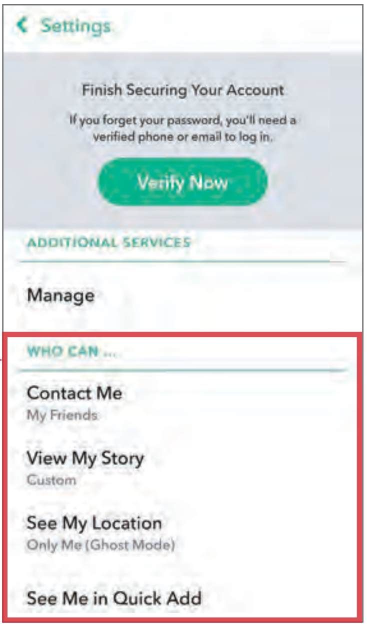
SNAPCHAT

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**



Finish Securing Your Account

If you forget your password, you'll need a verified phone or email to log in.

ADDITIONAL SERVICES

Manage

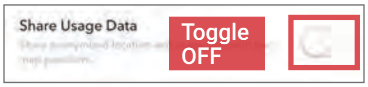
WHO CAN ...

Contact Me
My Friends

View My Story
Custom

See My Location
Only Me (Ghost Mode)

See Me in Quick Add


Share Usage Data

Toggle OFF

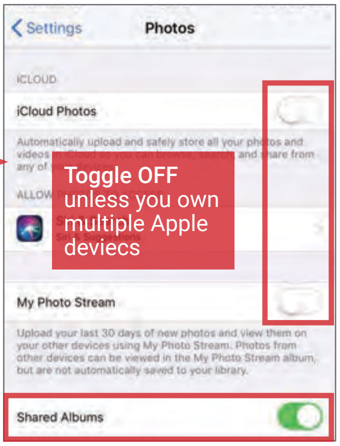
IOS PHOTOS

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 allows 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 does 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.



Photos

ICLOUD

iCloud Photos

Automatically upload and safely store all your photos and videos in iCloud so you can browse, search, and share from any of your devices.

ALLOW

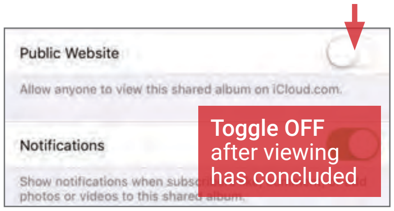
Siri & Suggestions

My Photo Stream

Upload your last 30 days of new photos and view them on your other devices using My Photo Stream. Photos from other devices can be viewed in the My Photo Stream album, but are not automatically saved to your library.

Shared Albums

Toggle OFF unless you own multiple Apple deviecs


Public Website

Allow anyone to view this shared album on iCloud.com.

Notifications

Show notifications when subscribers ... photos or videos to this shared album.

Toggle OFF after viewing has concluded

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.

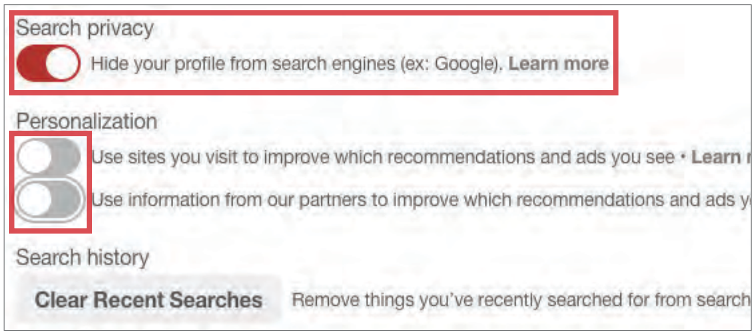
PINTEREST

Pinterest is a site where users can upload, categorize, and share images called Pins on dedicated pages called Pin Boards. The site has more than 250 million monthly active users (MAU). 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

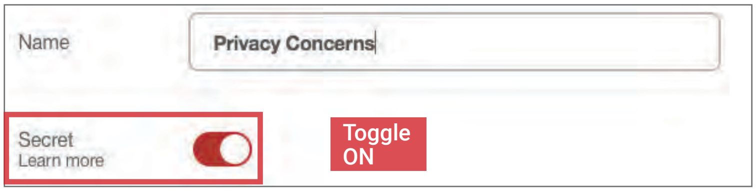
Use sites you visit to improve which recommendations and ads you see • Learn r

Use information from our partners to improve which recommendations and ads y

Search history

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

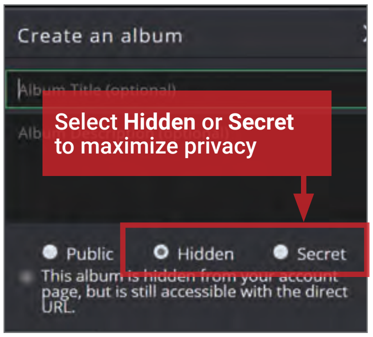
Toggle ON

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. Imgur has over 250 million MAU. 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

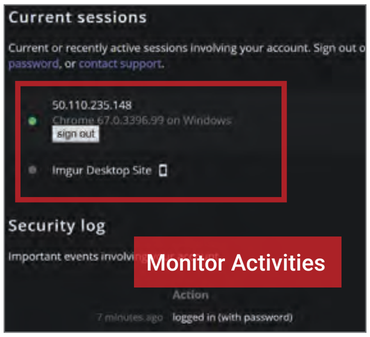
Alb

Alb

Select Hidden or Secret to maximize privacy

○ 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

Imgur Desktop Site

Security log

Important events involvi

Monitor Activities

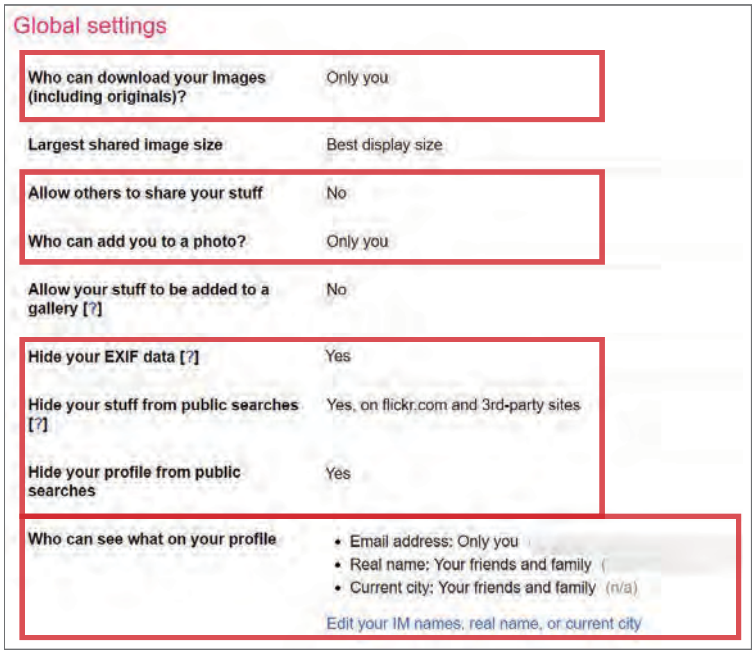
Action

7 minutes ago logged in (with password)

FLICKR

Flickr, acquired by SmugMug in April 2018 and supporting 90 million monthly active users, 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.

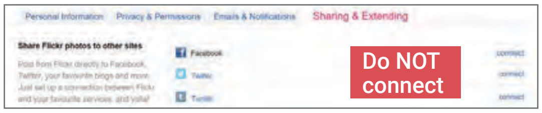
Make the following changes under the **Privacy & Permissions** tab for **Global settings** and **Defaults for new uploads**:



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.



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 voila!

Facebook connect
Twitter connect
Tumblr connect

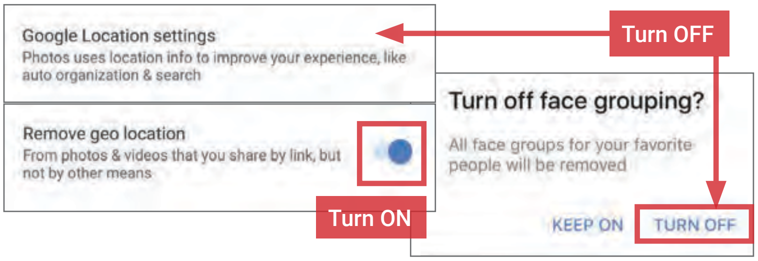
Do NOT connect

GOOGLE PHOTOS

Google Photos, the default photo app on Android devices, is a photo sharing, storage, and organizational tool with more than 500 million active users. 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

Turn OFF

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 sites.
- 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 are used by individuals looking to develop a personal or romantic relationship with other users. While each service is unique, sites typically ask users to maintain a public profile containing photos of themselves and personal information. These profiles are often searchable through the site and, at times, may be pushed to users who share common interests or locations. Should you elect to participate in online dating, use the recommendations in this card to protect your web-based online dating profiles and associated personal data. For additional information about mobile-based services such as Tinder, Bumble, Hinge, or Coffee Meets Bagel, please reference the Mobile Dating Apps chapter.

COMMON THREATS FROM DATING SITES

Online dating sites present a unique set of threats to users in comparison to other social networking sites. 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:

- Sites use questionnaires to pair like-minded individuals, allowing the services to collect targeted information about users' lifestyles.
- Most sites encourage users to connect a social network to their profiles 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). Use the dating site's chat feature as the only form of communication.
- Catfishing—a form of social engineering that uses a fake online persona to glean information from unsuspecting, real individuals—is common among online dating sites and can lead to identity theft, character defamation, and other general online scams.

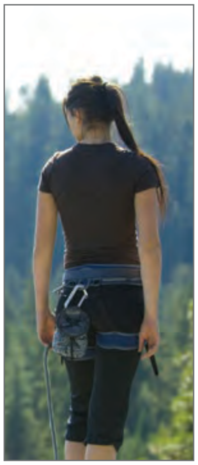
SELECTING A DATING SITE

Online dating sites are designed to pair individuals with one another based on common interests, values, lifetime achievements, and daily lifestyles. As a result, users of these sites often find themselves divulging additional information that they may not feel comfortable sharing on other social networking services (e.g., Facebook). Prior to registering an account, examine the types of data collected by each online dating site and select the service that best fits your privacy needs. Five of the top dating sites and their respective data requirements are outlined in the following table:

SITE	REGISTRATION INFORMATION	VISIBLE PROFILE INFORMATION	DATA SHARING OPTIONS	PRICING
match	Gender, partner gender preference, age preference, ZIP code, email address, password, birthday, seriousness of relationship, height, body type, relationship status, have/want kids, education, smoke, drink, ethnicities, religion, salary, interests	Most registration information, optional lifestyle and dating preferences, photos	Login with Facebook, upload photos from Facebook	Free to join; $21-$27/month to send messages and use the invisible browsing feature; other features available at cost
okcupid	First name, email address, birthday, location, gender, sexual orientation, biography, lifestyle questionnaire, photos	First name, most registration information, optional questionnaire answers	Login with Facebook, upload photos from Facebook, connect Instagram feed and upload photos	Free to join and send messages ("A-List Basic"). $25-35/month for A-List Premium, which offers enhanced profile priority and messaging features.
PlentyOfFish	Gender, sexual orientation, ZIP code, email address, country, birthdate, ethnicity, physical description, personal questionnaires, biography, interests, face photo	Most registration information	Upload photos from Facebook	Free to join, send messages, and hide profile; $6-$13/month to see extended profiles
zoosk	Gender, sexual orientation, ZIP code, email address, face photo, birthdate, physical description, lifestyle questionnaire, face photo	Most registration information, biography, optional lifestyle and dating preferences	Register with Facebook or Google, upload photos from Facebook	One-time activation fee of $24.95 for paid memberships. 1 month: $29.95, 3 months: $19.95/month, 6 months: $14.98/month
eharmony	Name, gender, sexual preference, ZIP code, email address, children, city of residence, DOB, ethnicity, height	Occupation, ethnicity, height, education, college, language, religion, smoke/drink preferences, children, passionate about, similarities, hobbies, positive characteristics, what user is most thankful for	Optional login with Facebook	Free to join. Membership required for active engagement ($15.95-$54.95/month depending on plan and subscription length)

REGISTRATION DATA

Protecting your identity data begins with registration. The example identity below displays the best ways to populate common dating site identity fields. Use the same principles in this example to register your account.



Name: Jennifer Vident (Use "Jen V." or "JV")
- Do not provide your full name

Date of Birth: 3/23/1981 (Use "1/1/1981")
- Supply a false date with your true birth year

Gender: Female
- True identification is required for proper site use

Sexual Preference: Male / Female / Other
- True identification is required for proper site use

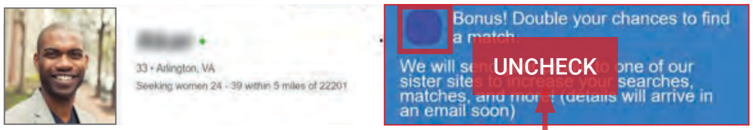
Current Location: Hackensack, NJ (Use New York, NY)
- Select a large metropolitan area / nearby zip code

Username: SightSeer889
- Usernames should not represent your true name

Photo: Use a photo that does not clearly show your face or distinguishable landmarks near your location

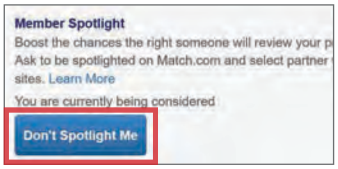
MATCH.COM

Match.com (parent company Match Group owns Tinder, OKCupid, Plenty of Fish, and Hinge) hosted 8.1 million paid subscribers in 2018. Free accounts display photos, interests, and desired traits in significant others.


33 • Arlington, VA
Seeking women 24 - 39 within 5 miles of 22201
Bonus! Double your chances to find a match.
We will send your profile to one of our sister sites to increase your searches, matches, and more! (details will arrive in an email soon)
UNCHECK

DO NOT opt to have your profile shared with a "**sister site**" during registration

Navigate to **Settings** to toggle profile visibility. Turn the member spotlight OFF to prevent the profile from appearing in ads. Hidden profiles prevent others from seeing the account but also disable its matching capability.



Member Spotlight
Boost the chances the right someone will review your p
Ask to be spotlighted on Match.com and select partner
sites. Learn More

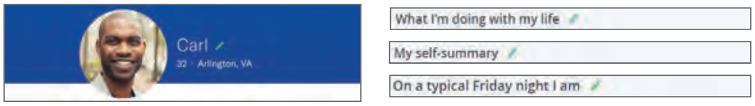
You are currently being considered

Don't Spotlight Me

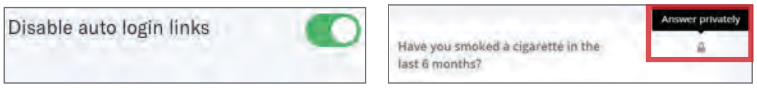
Private Mode is the optimal security setting—your profile is only visible to select people—and is available with a paid subscription. Private Mode permits matching and emailing, and enables a user to see who is interested in or has viewed the profile.

OKCUPID

OKCupid hosts ~8 million unique monthly visitors. Personal profiles display the user's first name, photos, registration information, and answers to free-text questions pertaining to the user's interests and daily activities.



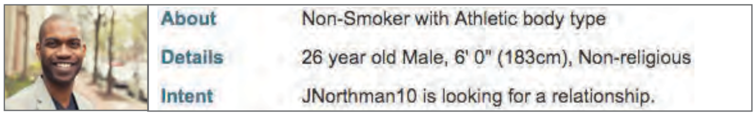
Navigate to **Settings > General** and activate "**Disable auto login links**" to help limit accidentally logging in through email. The questionnaire is optional: submitted answers may be kept private using the lock icon shown.



Paid subscriptions do not offer significant security upgrades compared to free accounts.

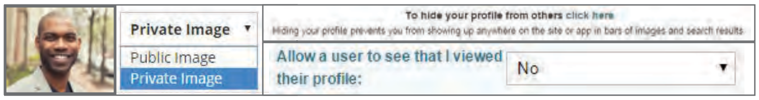
PLENTY OF FISH

Plenty of Fish hosts 80 million registered members. Profiles display the information submitted during registration and the traits that users look for in significant others.



About	Non-Smoker with Athletic body type
Details	26 year old Male, 6' 0" (183cm), Non-religious
Intent	JNorthman10 is looking for a relationship.

Select **Edit Profile** and elect to hide your profile from others. Hidden profiles do not appear in search results and, unlike other sites, do not lose matching or searching functionality as a result. Select **Upload Images** and set images to private so they can only be shared with individuals via private message.



Private Image ▾
Public Image
Private Image

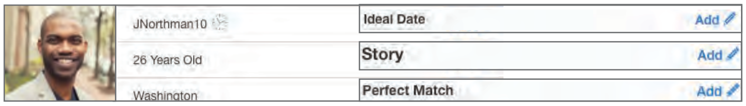
To hide your profile from others click here
Hiding your profile prevents you from showing up anywhere on the site or app in bars of images and search results

Allow a user to see that I viewed their profile: No ▾

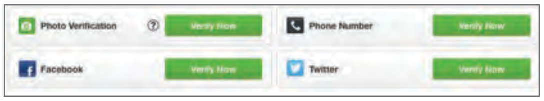
Paid subscriptions do not offer significant security upgrades compared to free accounts. Subscriptions are designed to increase the reach of a profile.

ZOOSK

Zoosk hosts 27 million registered members. Dating profiles consist of the data entered during registration and free-text entries describing the owners' dating preferences and personal background.



Free Zoosk accounts offer little to no privacy setting options. Zoosk provides multiple options to verify your account, including completing a photo verification and linking your number, Twitter, Facebook, or US military service records.

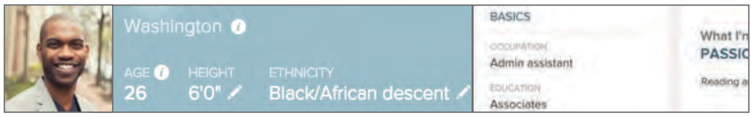


Avoid linking your accounts

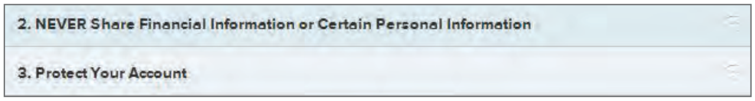
When others visit the proflie, Zoosk identifies the visitor to the profile owner. Users can activate private browsing for 30 minutes by paying 30 Zoosk coins (starting coin price: $5.95 for 60 coins, purchased within the profile).

EHARMONY

eHarmony hosts ~750k paid subscribers and 10 million active users. Profiles display registration information, photos, and Q&A responses. Other data includes free-text responses addressing the users' interests.



Free eHarmony accounts offer little to no privacy setting options; the site determines which data can be seen by others. The site provides detailed user safety tips and warns what types of data may be harmful to share.



2. NEVER Share Financial Information or Certain Personal Information

3. Protect Your Account

Photos can only be seen by users who maintain paid accounts. Paid accounts also permit users to see who has viewed their profiles and initiate SecureCalls (phone calls without sharing personal phone numbers).

MOBILE DATING APPS

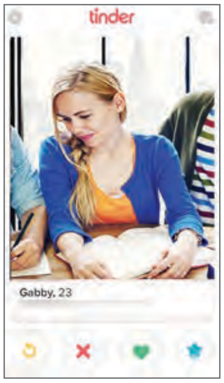
MOBILE DATING APPS - DO'S AND DON'TS

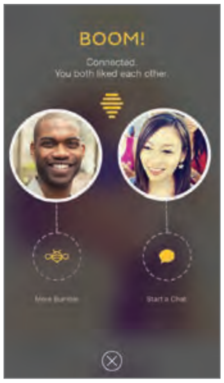
- Avoid using usernames and profile photos that also appear on other social networking services and profiles.
- Do not include information unique to you (e.g., last name or place of work) in your public profile data or messages.
- Install all app updates as soon as they become available. Check your app's privacy settings after each update to ensure maximum protection.
- Enable push notifications and alerts for your apps to help keep track of who is connecting with your profiles.
- Avoid posting images that may reveal your geographical location, such as a photo with a famous landmark in the background.
- Always read and take the time to understand the apps' Terms and Conditions before agreeing to register an account.

OVERVIEW

It is estimated that one out of every three American adults have used online dating services and mobile dating apps to actively discover romantic connections. As these apps continue to gain traction, users' identity data will be placed at a significantly higher privacy risk. Should you elect to participate in mobile dating, use the recommendations on this card to protect your personal and identity data. For additional information about the risks of online dating on web-based services such as Match, Plenty of Fish, Zoosk, OKCupid, or eHarmony, please reference the Online Dating Services chapter.

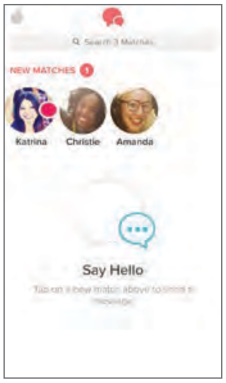
USING MOBILE DATING APPS

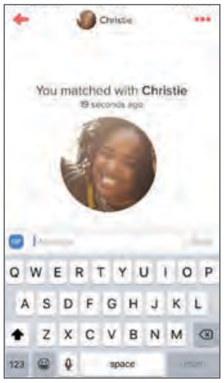




Matching: Mobile dating apps frequently employ a technique called "Swiping"—the motion of directing one's finger across a phone screen's surface—to help convey interest in other users' profiles. Traditionally, swiping a profile to the right indicates interest, while swiping it to the left indicates disinterest in the profile. Regardless of the swiping direction, selections are typically kept secret until both individuals show a mutual interest in one another.

Communication: Each app provides a matches page where users can revisit their matches' profiles or open a text dialogue with them through the app. Profiles and conversations remain accessible unless the app employs a time limit or a user manually unmatches the profiles.





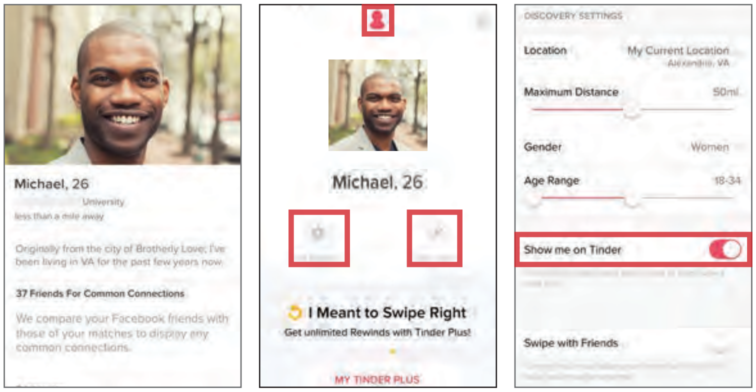
SELECTING A DATING APP

In general, mobile dating apps offer little to no user-controlled privacy settings. As a result, users must show discretion when registering an account and should avoid sharing potentially harmful data. Prior to registering an account, examine the types of data required by each mobile dating app, and select the service that best fits your privacy needs. Four of the top mobile dating apps and their respective data requirements are outlined in the following table:

DATING APP	REGISTRATION INFORMATION	VISIBLE PROFILE INFORMATION	APP PERMISSIONS	PRICING
Tinder	Facebook account or phone number verification (provided through Account Kit, which is powered by Facebook) Required: First name, birth date, gender, at least one profile photo, email address Optional: school.	Name, photos, age, approximate location, gender, biography, work information, education information, Instagram photos, Spotify account (top artists, favorite song)	Location, Cellular Data, Storage & Push Notifications Access to Facebook Account	Free to join; up to $10 / month for an upgraded account (change location, rewind features, disable ads)
Bumble	Phone number verification or Facebook account info Likes, photos, general info, and relationship interests	Name, photos, age, location, biography, work information, education information	Camera, Location, Phone, Cellular Data, and Storage Access to Facebook Account	Free to join; enhanced features available at-cost
Hinge	Facebook or Instagram account info Required: Name, profile picture, email address, First name, birthday, neighborhood, gender, sexual orientation, height, 6 photos, 3 questions	Name, photos, age, location, biography, height, education information, work information, hometown, religion, interests, dating preferences	Location, Cellular Data & Push Notifications Access to Facebook Account	Free to join; preferred membership with premium features available for $5-13/ month
Coffee Meets Bagel	Phone number verification or Facebook account info Relationship interests, gender, location	Passions, hobbies, height, ethnicity, religion, occupation, employer, education, photos	Location, Cellular Data, Push Notifications, Contacts, & Photos Access to Facebook Account	Free to join; up to $25 can be spent on credits ("beans") at a time to view more profiles in a day

TINDER

Tinder evaluates account users' geolocations, mutual Facebook friends, and common interests to match individuals. It also monitors users' viewing and swiping habits on the service to help predict more compatible matches.


Michael, 26
University
less than a mile away
Originally from the city of Brotherly Love; I've been living in VA for the past few years now.
37 Friends For Common Connections
We compare your Facebook friends with those of your matches to display any common connections.
Michael, 26
I Meant to Swipe Right
Get unlimited Rewinds with Tinder Plus!
MY TINDER PLUS
DISCOVERY SETTINGS
Location
My Current Location
Alexandria, VA
Maximum Distance
50mi.
Gender
Women
Age Range
18-34
Show me on Tinder
Swipe with Friends

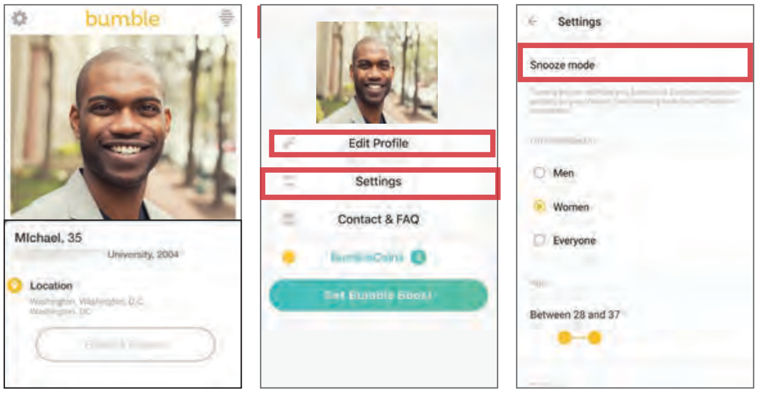
Use: Users may swipe through a limited number of profiles per day. There are no gender-based limitations on who is able to initiate a chat conversation once matched. Matches do not expire and are stored in the app unless they are manually removed by one of the users.

Profiles: Navigate to **Person Icon > Edit Info** to change or delete the information displayed in your profile.

Settings: Navigate to **Gear Icon > Discovery Settings** to change your profile's visibility. Deactivating **Show me on Tinder** hides your profile.

BUMBLE

Bumble uses geolocation and behavior metrics to pair individuals. The app measures the number of conversations started and the average length of conversations to match engaged users and incentivize others to participate.



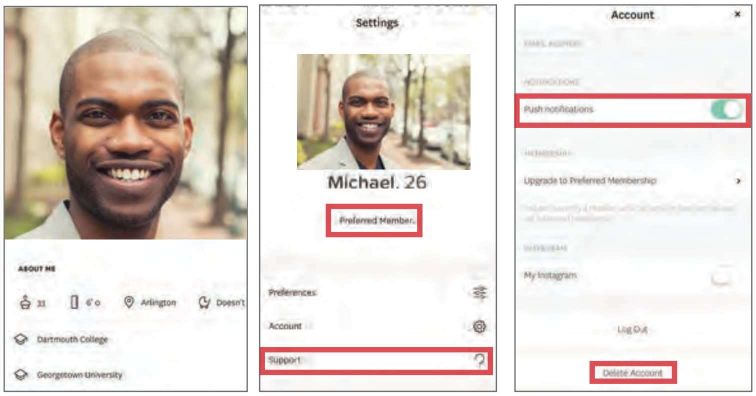
Use: Users may swipe through an unlimited number of profiles per day. Once matched, women are given 24 hours to initiate a conversation. For same-sex connections or friendship settings, either person has 24 hours to make the first move. The match expires if no communication is established.

Profiles: Navigate to **Edit Profile** to change the information displayed in your profile.

Settings: Select **Settings** to enable notifications and set your profile's visibility. Activate **Snooze Mode** when you are not actively searching or would like to hide your profile from public view.

HINGE

Hinge, acquired by Match Group in 2018, matches people who have mutual Facebook friends. The app factors in geolocation, common interests, and the types of profiles each user has liked in the past to suggest more attractive matches.



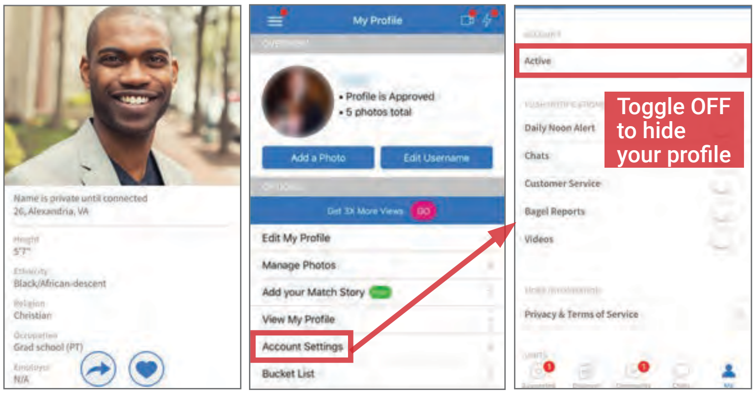
Use: Users may swipe through an unlimited number of profiles but are capped at sending 10 likes a day. There are no gender-based limitations on who is able to initiate chat conversations. Matches expire after 14 days; users can no longer view each others' profiles or communicate through the app without rematching.

Profiles: Select **Settings** and click on the pencil below your profile image to change or delete the information displayed in your profile.

Settings: Select **Settings > Account** to enable notifications, log out of, and delete your account. Profiles cannot be hidden, or de-linked from Facebook or Instagram.

COFFEE MEETS BAGEL

Coffee Meets Bagel matches people based on profile criteria and linked Facebook data. It also takes into account geolocation, education, physical attributes, and past swiping tendencies to suggest compatible matches.



Toggle OFF to hide your profile

Use: The app shows users a limited number of compatible matches ("Bagels") per day, which users swipe to match. Matches are directed to a chat room that is open for 7 days (time period can be extended with paid "beans"). Each day, users can record up to 8 seconds of video answering a "question of the day," using this feature provides additional opportunities for matching.

Profiles: Navigate to **My Profile** to **Edit Username**, **Edit My Profile**, **Manage Photos**, and adjust **Account Settings**.

Settings: Select **Account Settings** to enable push notifications. Toggle OFF the **Active** membership status to hide your profile and prevent location sharing.

SECURE CHAT APPS

SECURE CHAT 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 (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 SECURE CHAT APPS?

Secure chat apps are designed to protect users' electronic communications against surveillance from third parties. 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 previously downloaded the app. In general, secure chat apps afford users greater protection against eavesdropping by concealing the users' identities or making the contents of the messages indecipherable to anyone except the intended recipient(s). As a result, using secure chat apps may potentially offer users two layers of security: anonymity and data security.

- **Anonymity**: Secure chat 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**: Secure chat apps protect private messages and account information through specific message encryption methods, account settings, desktop support, or storing a limited collection of user data on the app provider's servers.

VULNERABILITIES

As with any communication over the Internet or a cellular network, 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 collect user content, 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. Screenshots of communications also allow data leakage.
- App providers may elect to log user data for an indefinite amount of time. Data logging can allow the recovery of older communications.
- Some apps require a phone number for account registration. Minimize identity linkages by using a secondary or VOIP number, rather than your primary.

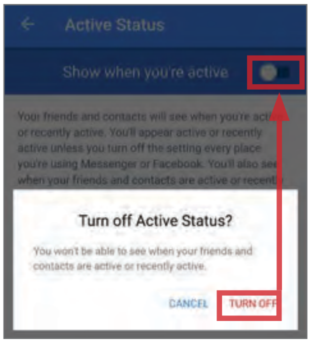
CHOOSING THE RIGHT SECURE CHAT APP

As a whole, secure chat 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. Compare the capabilities of the four apps below to determine which may be best suited for your personal use.

SERVICE	OS	DESCRIPTION	IDENTITY DATA	SECURITY	LINKAGES
Facebook Messenger	Android, iOS, Mac, Windows	Supports text/photo/video messages, voice/video calling, and sticker/audio/file exchange over the Internet or cellular networks. US-based. Optional encryption.	***Sign up***: Facebook Account OR Phone number/name/ contacts ***Optional***: Picture	***Potential for anonymity:*** Optional end-to-end encryption ***Encryption Type:*** Open Whisper System's Signal Protocol	***Social Network / Email:*** Facebook ***Device Permissions:*** Contacts, Phone, SMS
Telegram	Android, iOS, Linux, Mac, Windows	Cloud-based messenger supports text/photo/video messages, audio/file/sticker exchange. Syncs across devices; Secret Chat feature with temporary text messages. Based in Dubai (April 2018).	***Sign up***: Phone number, first name ***Optional***: Last name, contacts, picture	***Potential for anonymity:*** End-to-end encrypted messages (Secret chats) ***Encryption Type***: MTProto with end-to-end encryption	***Social Network / Email***: None ***Device Permissions:*** Contacts, Storage
WhatsApp	Android, iOS, Mac, Symbian, Windows	Supports encrypted test/ photo/audio/video message exchange, and voice/video calling over the Internet and cellular networks. US-based.	***Sign up***: Phone number ***Optional***: Name, picture	***Potential for anonymity:*** End-to-end encrypted messages, secure calls ***Encryption Type***: Open Whisper System's Signal Protocol	***Social Network / Email***: None ***Device Permissions:*** Contacts, Microphone, Storage
Signal	Android, iOS, Linux, Mac, Windows	Supports encrypted voice/video calls and texts/audio/photo/ video message exchange over the Internet and cell networks. US-based.	***Sign up***: Phone number ***Optional***: Name, picture	***Potential for anonymity:*** End-to-end encrypted messages ***Encryption Type:*** Open Whisper System's Signal Protocol	***Social Network / Email:*** None ***Device Permissions:*** Contacts, Phone, Storage

FACEBOOK MESSENGER

Facebook Messenger was originally developed as Facebook Chat in 2008 and become a standalone app in August 2011. It currently allows users to exchange messages, photos, videos, stickers, audio content, and files, as well as voice and video calls, using optional end-to-end encryption supported by Open Whisper System's Signal Protocol.


← Active Status

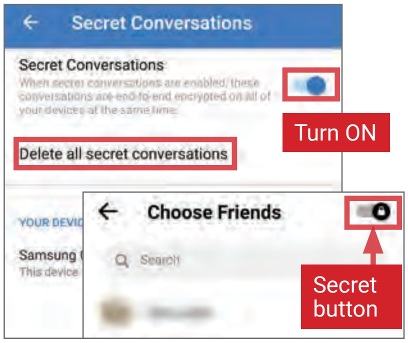
Show when you're active

Your friends and contacts will see when you're acti… or recently active. You'll appear active or recently active unless you turn off the setting every place you're using Messenger or Facebook. You'll also se… when your friends and contacts are active or recent…

Turn off Active Status?

You won't be able to see when your friends and contacts are active or recently active.

CANCEL TURN OFF


← Secret Conversations

Secret Conversations

When secret conversations are enabled, these conversations are end-to-end encrypted on all of your devices at the same time

Turn ON

Delete all secret conversations

YOUR DEVIC…

Samsung …
This device

← Choose Friends

Search

Secret button

Tap your profile photo to access settings. Under **Profile > Active Status**, **turn OFF Show when you're active.** To enable encrypted messaging, navigate to **Preferences > Secret Conversations** and **turn ON** Secret Conversations. When starting a new chat, **toggle ON** the Secret button [lock icon, upper right] prior to selecting the recipient. To use the expiring message feature, tap the clock icon in the text box and set the timer.

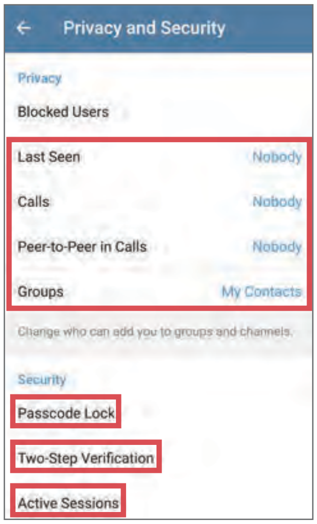
- Consider using a secondary phone number to create a Messenger account that is not linked to your Facebook account.
- Do not link Messenger with your SMS conversations or device contacts
- Use **Secret Conversations** for all conversations, and periodically delete all conversations.

TELEGRAM

Telegram uses the cloud to synchronize messages across multiple devices. The app also offers a Secure Chat feature designed to prevent eavesdropping by employing end-to-end encryption and destroying messages after a set period of time. Secure chats, unlike standard Telegram messages, are stored locally on the device and cannot be forwarded to other devices or users.

Consider using a secondary or VOIP phone number for registration. Do not provide your real name, a username, or a bio. Navigate to ☰ [upper left] **> Settings > Privacy and Security** and apply the following options:

- Under **Privacy,** set **Last Seen, Calls,** and **Peer-to-Peer Calls** to **Nobody.** Set **Groups** to **My Contacts.** Save each change by tapping ✓ [upper right].
- Under **Security,** establish a **Passcode Lock** and enable **Two-Step Verification.**
- Under **Advanced**, set **Delete my account if away for 6 months**; accounts are free to make and there is no risk of losing contact information.
- Under **Contacts,** disable **Sync Contacts** and **Suggest Frequent Contacts.**


← Privacy and Security

Privacy

Blocked Users	
Last Seen	Nobody
Calls	Nobody
Peer-to-Peer in Calls	Nobody
Groups	My Contacts

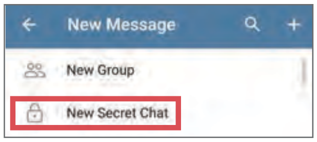
Change who can add you to groups and channels.

Security

Passcode Lock

Two-Step Verification

Active Sessions

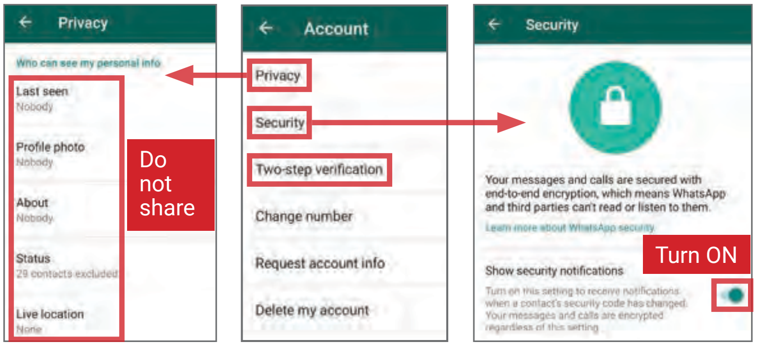

← New Message

New Group

New Secret Chat

WHATSAPP

WhatsApp, owned by Facebook, is currently the most popular social messaging app, with 1.5 billion monthly active users. WhatsApp provides end-to-end encryption for messages, calls, and video chats, which ensures that no one, not even WhatsApp engineers, can intercept the communication method except for the sender and recipient. 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.


← Privacy

Who can see my personal info

Last seen	Nobody
Profile photo	Nobody
About	Nobody
Status	29 contacts excluded
Live location	None

Do not share

← Account

Privacy

Security

Two-step verification

Change number

Request account info

Delete my account

← Security

Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

Learn more about WhatsApp security

Turn ON

Show security notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting

Tap the Settings icon [bottom right] to apply the following changes to best maximize your 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.

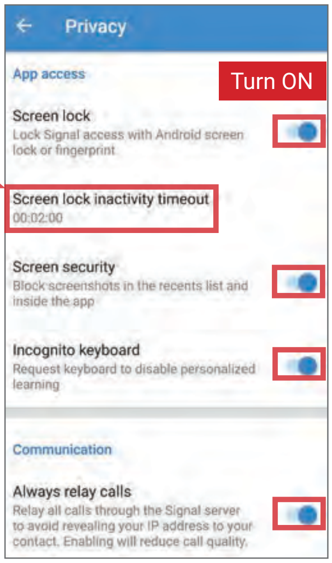
SIGNAL

Signal supports end-to-end encrypted communication between users. In 2018, Signal rolled out a unique "Sealed Sender" feature that also encrypts message sender/recipient information. The app does not collect user metadata, nor does it store messages when you backup your device. Signal's encryption code is open-source and also used by companies like Facebook and Google. iPhone users can only contact those who have the app as well; Android users can contact anyone, but messages with non-Signal users are unencrypted.

Consider using a secondary or VOIP number for account registration.

Tap the ⋮ icon and select **Settings > Privacy**. Apply the following options to best secure your conversations through the app:

- Enable **Screen Lock** and set the inactivity timeout to 2 minutes.
- Enable the **Screen Security** and **Incognito keyboard** features to limit opportunities for information collection.
- Under **Communication**, enable **Always relay calls** to ensure communications do not reveal your IP address.
- Manually delete your messages when your conversations are over.
- Clear the app's history after each completed communication.


← Privacy

App access

Turn ON

Screen lock
Lock Signal access with Android screen lock or fingerprint

Screen lock inactivity timeout
00:02:00

Screen security
Block screenshots in the recents list and inside the app

Incognito keyboard
Request keyboard to disable personalized learning

Communication

Always relay calls
Relay all calls through the Signal server to avoid revealing your IP address to your contact. Enabling will reduce call quality.

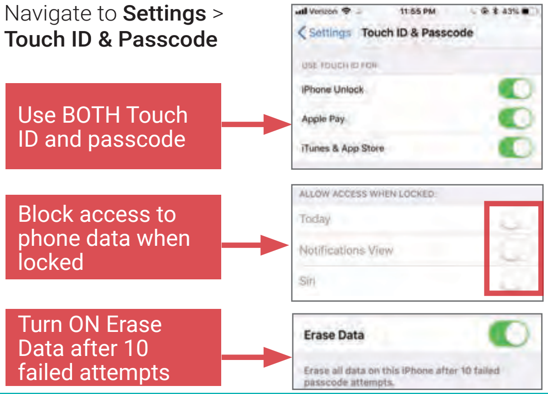
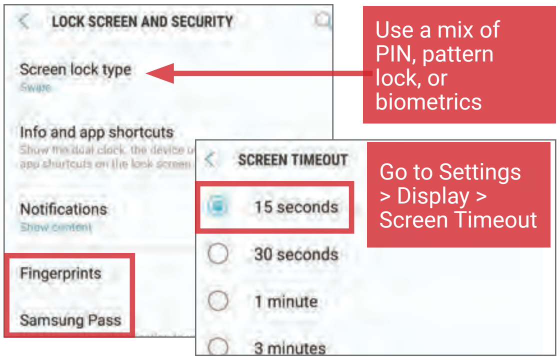
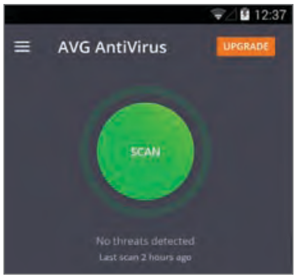
SMARTPHONES

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.

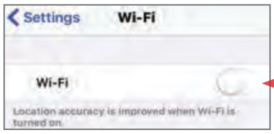
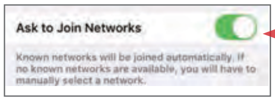
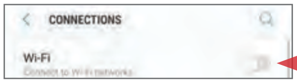
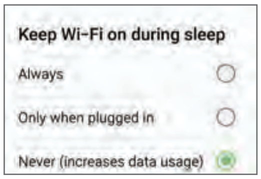
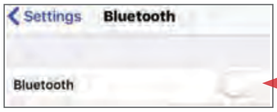
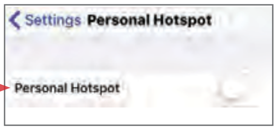
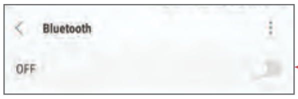
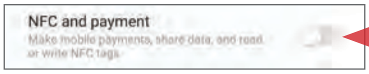
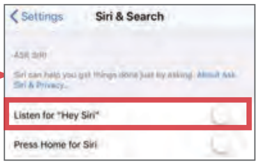
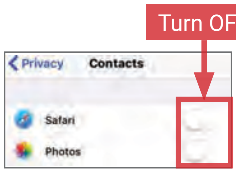
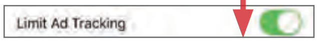
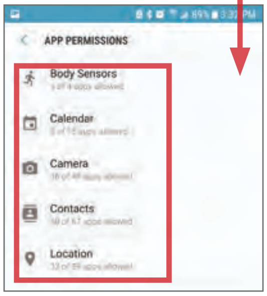
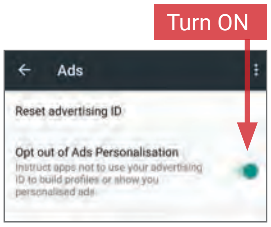
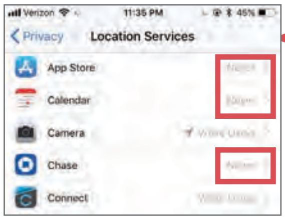
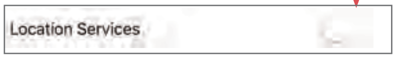
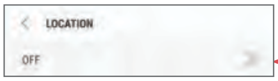
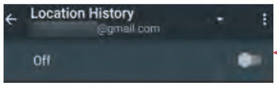
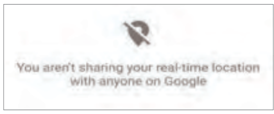
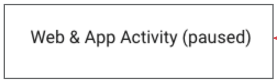
RISK SCENARIO	IPHONE (V. 11.4.1)	ANDROID (V. 7.0)
SMARTPHONE IS PHYSICALLY ACCESSED BY SOMEONE WITHOUT YOUR CONSENT - To prevent unauthorized access, set up a strong alphanumeric passcode or PIN at least eight digits long. Fingerprints, face recognition, and pattern locks may be strong, but they expose greater risks 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** > **Touch ID & Passcode**  Use BOTH Touch ID and passcode Block access to phone data when locked Turn ON Erase Data after 10 failed attempts Settings Touch ID & Passcode USE TOUCH ID FOR: iPhone Unlock Apple Pay iTunes & App Store ALLOW ACCESS WHEN LOCKED: Today Notifications View Siri Erase Data Erase all data on this iPhone after 10 failed passcode attempts.	Navigate to **Settings** > **Lock screen and security**  Use a mix of PIN, pattern lock, or biometrics Go to Settings > Display > Screen Timeout LOCK SCREEN AND SECURITY Screen lock type Swipe Info and app shortcuts Show the dual clock, the device u... app shortcuts on the lock screen Notifications Show content Fingerprints Samsung Pass SCREEN TIMEOUT 15 seconds 30 seconds 1 minute 3 minutes
SMARTPHONE IS LOST OR STOLEN - Download and install apps that allow you to locate, lock, and control your phone remotely from a web page or another device. Additionally, regularly backup data on your phone to a secure computer or cloud service. 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 Phone** Find My iPhone Apple ID Password Capabilities: • Remote lock • Erase data • GPS locator • Sound alarm • Send text message to phone • Backup data through iCloud storage	Install **Find My Device** Find My Device Location data from your devices will be collected and sent to Google. Device location is approximate, and may not always be accurate. If you believe your device has been stolen, please contact law enforcement. Do not attempt to retrieve the device yourself. Close Accept Capabilities: • Locate device by GPS • Remote lock • Erase data • Sound alarm • Change password remotely • Can use via Google search, app, website, or smartwatch
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 it to a compromised PC. Use browsers that enable ad- and script-blocking. Download third-party security apps to check for and prevent malware from stealing data.	Install **Lookout Mobile Security** While iOS is not readily susceptible to viruses, use this app to monitor the system for malicious activity. Capabilities: • Monitor running apps for malicious activity • Check OS to ensure it is up-to-date	Install **AVG Antivirus 2018**  12:37 AVG AntiVirus UPGRADE SCAN No threats detected Last scan 2 hours ago Capabilities: • App scanner • File scanner • Website scanner • Text and call blocker • Remote lock • Erase data remotely • GPS locator • Kill slow tasks

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. Availability of suggested settings may vary by OS version and type of phone.

USE CASE	IPHONE (V. 11.4.1)	ANDROID (V. 7.0)
CONNECTING TO WIRELESS NETWORKS - Information transmitted via public Wi-Fi networks can be intercepted by third parties. Avoid using public wireless networks when possible, 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**  Settings Wi-Fi Wi-Fi Location accuracy is improved when Wi-Fi is turned on. Disable Wi-Fi when not in use  Ask to Join Networks Known networks will be joined automatically. If no known networks are available, you will have to manually select a network. Enable network permissions Navigate to **Settings** > **VPN** to enable and establish a VPN connection	Navigate to **Settings > Connections > Wi-Fi**  CONNECTIONS Wi-Fi Connect to Wi-Fi networks Disable Wi-Fi when not in use Select the gear icon to configure Wi-Fi (feature varies by Android model) and select **Never** under "Keep Wi-Fi on during sleep"  Keep Wi-Fi on during sleep Always ○ Only when plugged in ○ Never (increases data usage) ● Navigate to **Settings > Connections > More connection settings** to enable and establish a VPN connection
CONNECTING VIA BLUETOOTH - Bluetooth involves the wireless communication of two devices within a 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 disable it when not in use.	Navigate to **Settings** > **Bluetooth** to disable services  Settings Bluetooth Bluetooth Disable Bluetooth when not in use Navigate to **Settings** > **Personal Hotspot** to disable broadcasting your private Internet connection Never share your Internet connection  Settings Personal Hotspot Personal Hotspot	Navigate to **Settings** > **Connections > Bluetooth**  Bluetooth OFF Disable Bluetooth when not in use Navigate to **Settings** > **Connections > NFC and payment** to manage Near Field Communications, which enables smartphones to transfer data by touching the devices together  NFC and payment Make mobile payments, share data, and read or write NFC tags Uncheck
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 Now may also collect data from users, which may include device information or audio from the device. However, 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  Settings Siri & Search ASK SIRI Siri can help you get things done just by asking. About Ask Siri & Privacy... Listen for "Hey Siri" Press Home for Siri Navigate to **Settings** > **Privacy** to manage which specific data each app accesses from your phone Turn OFF  Privacy Contacts Safari Photos Navigate to **Settings > Privacy > Advertising** Turn ON  Limit Ad Tracking	Navigate to **Settings > Apps >** ⋮ **> App permissions** Restrict excessive requests for personal data  APP PERMISSIONS Body Sensors Calendar Camera Contacts Location Navigate to **Settings** > **Google > Ads** Turn ON  Ads Reset advertising ID Opt out of Ads Personalisation Instruct apps not to use your advertising ID to build profiles or show you personalised ads
APPS USING REAL-TIME LOCATION - Many apps will ask permission to track your real-time location. Users should 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 iPhone"** or **"Find my device"**.	Navigate to **Settings** > **Privacy** > **Location Services**  Verizon 11:35 PM 45% Privacy Location Services App Store Never Calendar Never Camera While Using Chase Never Connect While Using Only grant access to apps that require location Disable all location services when not in use  Location Services	Navigate to **Settings** > **Location**  LOCATION OFF Disable all location services when not in use  Location History [redacted]@gmail.com Off Turn OFF Google location history  You aren't sharing your real-time location with anyone on Google Turn OFF Google location sharing  Web & App Activity (paused) Turn OFF Google Web and App Activity

TRAVELING WITH SMARTPHONES

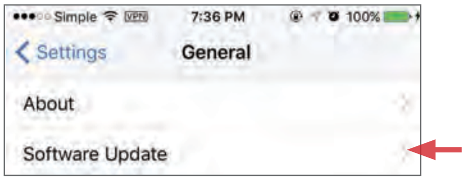
TRAVELING WITH SMARTPHONES - DO'S AND DON'TS

- Bring a dedicated loaner device when you travel overseas; do not bring your personal 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. 11.4.1)

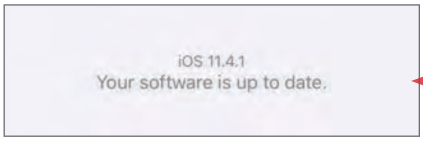

●●●○○ Simple 7:36 PM 100%

Settings General

About

Software Update

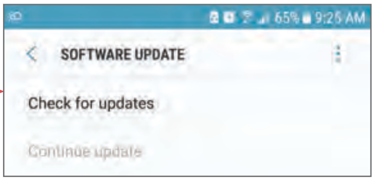
Go to **Settings > General > Software Update.** Check to see if your software is up-to-date.


iOS 11.4.1
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. 7.0)

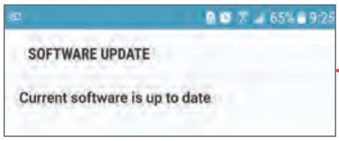
Go to **Settings > Software update > Check for updates**


65% 9:25 AM

SOFTWARE UPDATE

Check for updates

Continue update


65% 9:25

SOFTWARE UPDATE

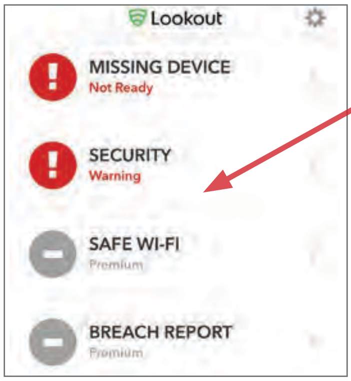
Current software is up to date

Confirm current software is up-to-date. If not, follow Android prompts to download and install the latest software.

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. 11.4.1)


Lookout

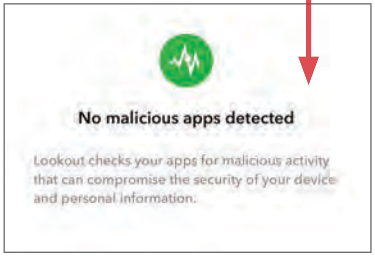
MISSING DEVICE
Not Ready

SECURITY
Warning

SAFE WI-FI
Premium

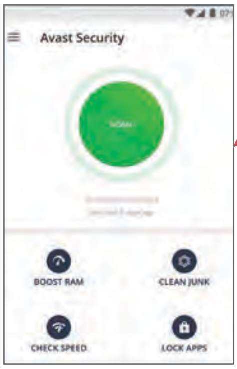
BREACH REPORT
Premium

Use the **Lookout** app for iPhone. Go to **Security** to see if your phone has any malicious apps.


No malicious apps detected

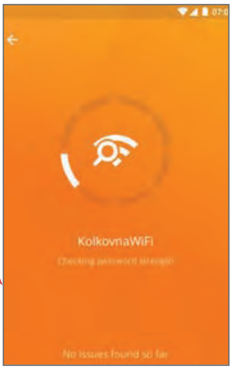
Lookout checks your apps for malicious activity that can compromise the security of your device and personal information.

ANDROID (V. 7.0)



Use the **Avast Antivirus Free** app for Android. Click **Scan Now** to monitor for viruses.

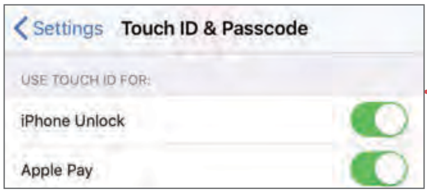
Avast also offers the option to scan Wi-Fi networks for threats.



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. 11.4.1)

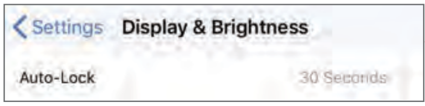

Settings Touch ID & Passcode

USE TOUCH ID FOR:

iPhone Unlock ●

Apple Pay ●

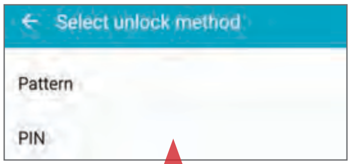
Go to **Settings > Touch ID & Passcode**. Turn on all Touch ID optons and set **Require Passcode** to **Immediately**.


Settings Display & Brightness

Auto-Lock 30 Seconds

Go to **Settings > Display & Brightness> Auto-Lock**. Set the **Auto-lock** to 30 seconds.

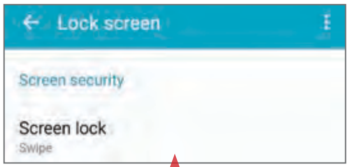
ANDROID (V. 7.0)


Select unlock method

Pattern

PIN

Go to **Settings > Lock screen and security > Screen lock type** to enable password protection. Choose between pattern, PIN, password, and fingerprint.


Lock screen

Screen security

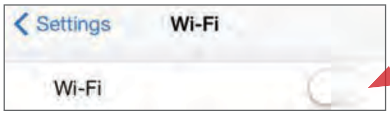
Screen lock
Swipe

Go to **Settings > Display > Screen timeout** and select the shortest timeout option available.

DISABLE WI-FI AND BLUETOOTH

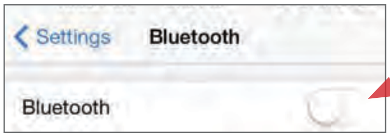
Disable **Wi-Fi** and **Bluetooth** on your smartphone when you are not using them; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware.

iPHONE (V. 11.4.1)


Settings Wi-Fi

Wi-Fi

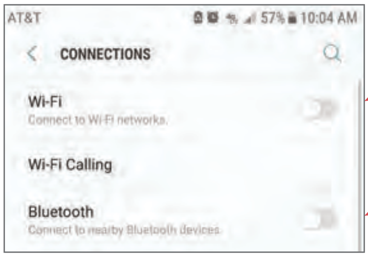
Go to **Settings > Wi-Fi**. Turn Wi-Fi **OFF**.


Settings Bluetooth

Bluetooth

Go to **Settings > Bluetooth**. Turn Bluetooth **OFF**.

ANDROID (V. 7.0)


AT&T 57% 10:04 AM

CONNECTIONS

Wi-Fi
Connect to Wi-Fi networks

Wi-Fi Calling

Bluetooth
Connect to nearby Bluetooth devices

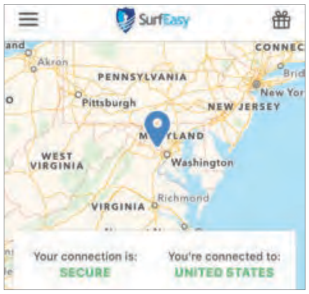
Go to **Settings > Connections > Wi-Fi.** Turn Wi-Fi **OFF**.

Go to **Settings > Connections > Bluetooth.** Turn Bluetooth **OFF**.

USE VPN ON WIRELESS NETWORKS

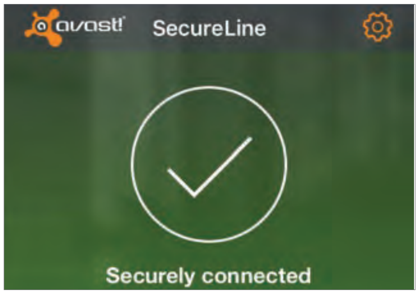
Virtual Private Networks—or **VPNs**—allow you to extend a private network across a public network such as public Wi-Fi. Using a VPN will make it more difficult for malicious individuals to eavesdrop on your Internet traffic. Use a VPN service such as SurfEasy VPN or Avast SecureLine to protect yourself.

iPHONE (V. 11.4.1)



Your connection is: SECURE

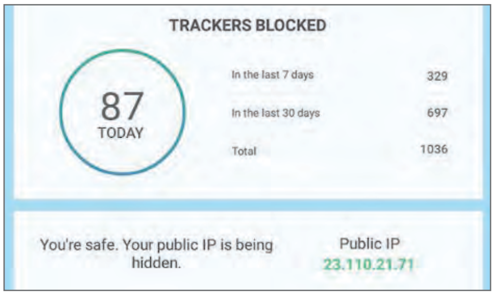
You're connected to: UNITED STATES


avast! SecureLine

Securely connected

Use VPN services such as **SurfEasy** and **Avast SecureLine** VPN for iOS to protect yourself on Wi-Fi.

ANDROID (V. 7.0)

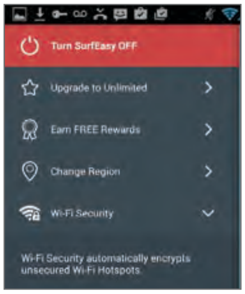

TRACKERS BLOCKED

87 TODAY

In the last 7 days	329
In the last 30 days	697
Total	1036

You're safe. Your public IP is being hidden.

Public IP 23.110.21.71


Turn SurfEasy OFF

Upgrade to Unlimited

Earn FREE Rewards

Change Region

Wi-Fi Security

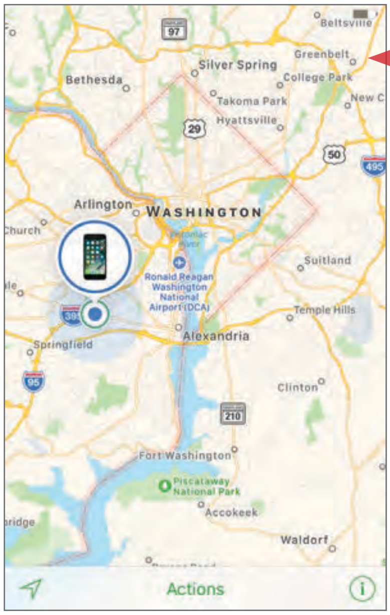
Wi-Fi Security automatically encrypts unsecured Wi-Fi Hotspots.

Use VPN services such as **SurfEasy for Android** to protect yourself on Wi-Fi.

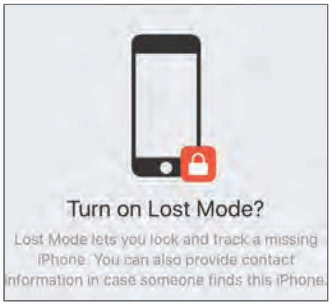
RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

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

iPHONE (V. 11.4.1)

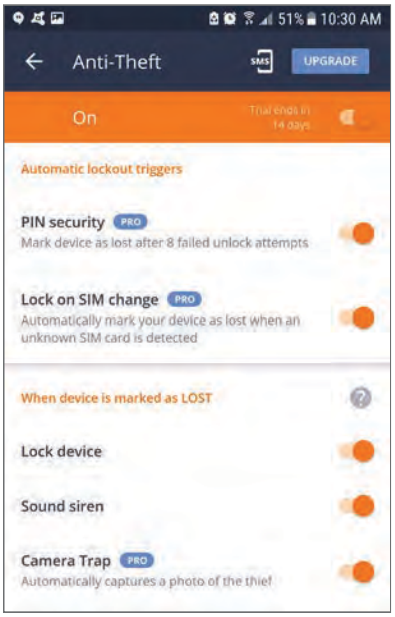


Use the **Find My iPhone** app to recover lost or stolen iPhone smartphones.


Turn on Lost Mode?

Lost Mode lets you lock and track a missing iPhone. You can also provide contact information in case someone finds this iPhone.

ANDROID (V. 7.0)


51% 10:30 AM

Anti-Theft SMS UPGRADE

On Trial ends in 14 days

Automatic lockout triggers

PIN security PRO
Mark device as lost after 8 failed unlock attempts

Lock on SIM change PRO
Automatically mark your device as lost when an unknown SIM card is detected

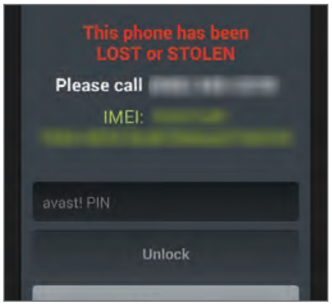
When device is marked as LOST

Lock device

Sound siren

Camera Trap PRO
Automatically captures a photo of the thief

Use the **Avast** app to recover lost or stolen Android smartphones and wipe data remotely from the device.


This phone has been LOST or STOLEN

Please call [redacted]

IMEI: [redacted]

avast! PIN

Unlock

EXIF DATA REMOVAL

EXIF REMOVAL - DO'S AND DON'TS

- Remove EXIF data before sharing images with people or posting them online, especially when images are captured in private homes or businesses.
- Use an EXIF viewer to verify that personal data has been removed from photos before sharing and prevent your phone from including location tags.
- Before uploading images, use available privacy settings to limit the audience to only you or close friends and family.
- Minimize the use of apps that automatically upload and share captured images (e.g., Google Photos, Flickr).
- Even without EXIF data, the image content may contain identifying information, such as associated persons or location histories. Screen content with the assumption that anyone can see, copy, or forward photos that you post online.

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.

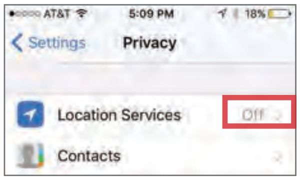
PREVENTING THE CAPTURE OF GEOLOCATION DATA

- 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 home 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. 12.1.3)

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 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.

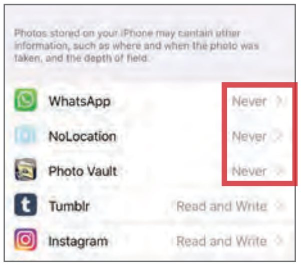


AT&T 5:09 PM 18%

Settings Privacy

Location Services Off

Contacts



Photos stored on your iPhone may contain other information, such as where and when the photo was taken, and the depth of field.

WhatsApp Never

NoLocation Never

Photo Vault Never

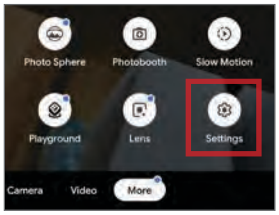
Tumblr Read and Write

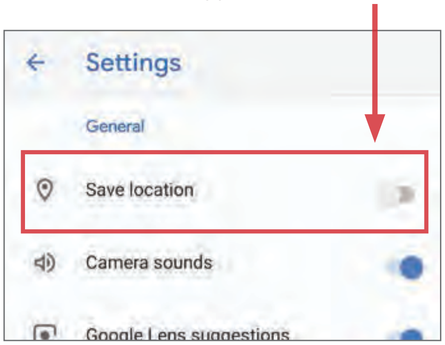
Instagram Read and Write

ANDROID (V. 9.0)

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

1. Open the **Camera** app and select **More**
2. Tap the **white gear icon** to access **Settings**
3. Under **General**, toggle OFF **Save location**





Settings

General

Save location

Camera sounds

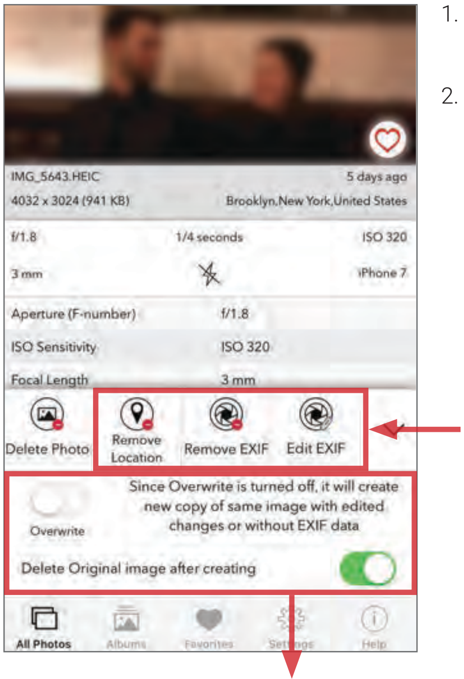
Google Lens suggestions

Last Updated: 03/01/2019

EXIF REMOVAL SOFTWARE

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 at $2.99.



IMG_5643.HEIC 5 days ago
4032 x 3024 (941 KB) Brooklyn,New York,United States

f/1.8	1/4 seconds	ISO 320
3 mm		iPhone 7
Aperture (F-number)	f/1.8	
ISO Sensitivity	ISO 320	
Focal Length	3 mm	

Since Overwrite is turned off, it will create new copy of same image with edited changes or without EXIF data

Overwrite

Delete Original image after creating

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.

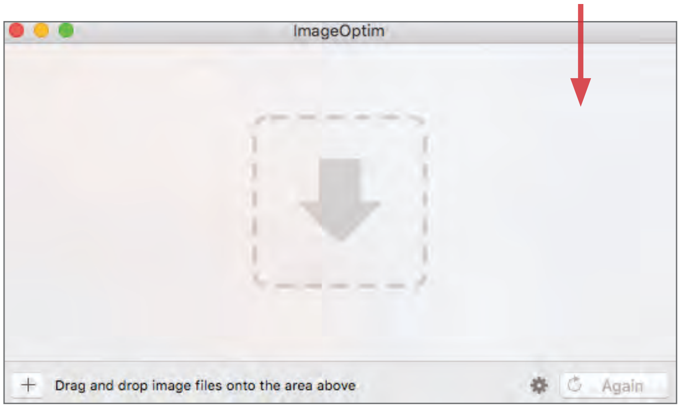
3. Finalize changes by approving the app to make changes to your photos.

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.

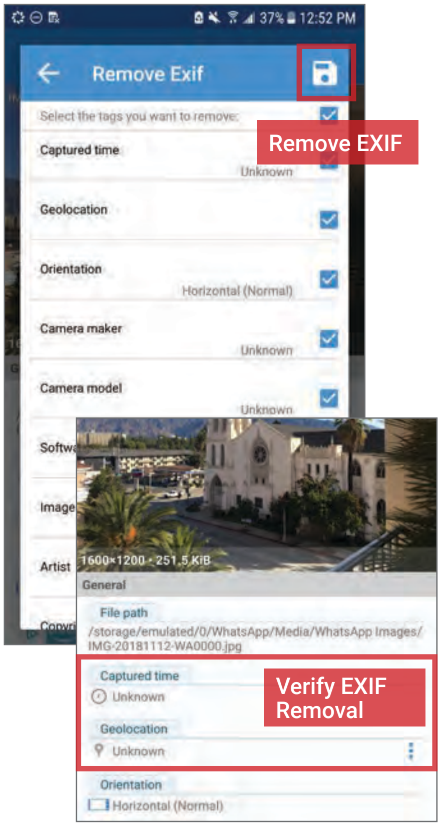
2. Drag the photos selected for EXIF removal into the application window and wait for a green check mark to appear next to the file name.



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**.

PHOTO EXIF EDITOR - METADATA EDITOR

Photo EXIF Editor - Metadata Editor is a free app that deletes all EXIF data from image files stored on your Android devices.



Select the tags you want to remove:

Captured time	Unknown
Geolocation	
Orientation	Horizontal (Normal)
Camera maker	Unknown
Camera model	Unknown
Softw	
Image	
Artist	
Copy	

1600×1200 · 251.5 KiB

General

File path
/storage/emulated/0/WhatsApp/Media/WhatsApp Images/IMG-20181112-WA0000.jpg

Captured time
Unknown

Geolocation
Unknown

Orientation
Horizontal (Normal)

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 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 IN WINDOWS

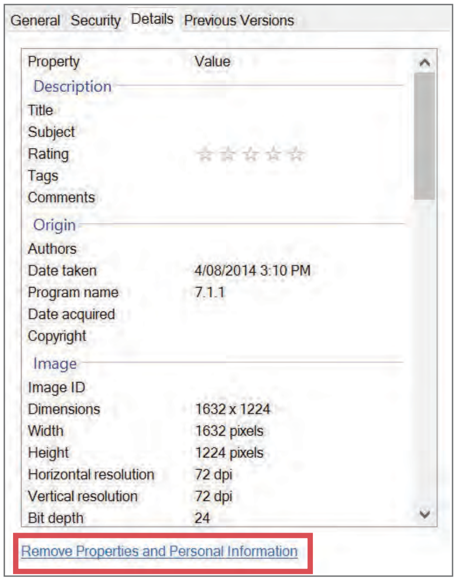
Use the Windows 10 operating system on your computer to verify EXIF data has been successfully removed.

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.



Property	Value
Description	
Title	
Subject	
Rating	☆☆☆☆☆
Tags	
Comments	
Origin	
Authors	
Date taken	4/08/2014 3:10 PM
Program name	7.1.1
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	1632 x 1224
Width	1632 pixels
Height	1224 pixels
Horizontal resolution	72 dpi
Vertical resolution	72 dpi
Bit depth	24

Remove Properties and Personal Information

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 monitor large purchases and transfers.
- Do not link your mobile wallet application to a social networking service (e.g., Facebook, Twitter).
- Link a bank account only to cash-out; delete bank account information once the cash-out process has 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 friends 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 NFC chip (near field communication). 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

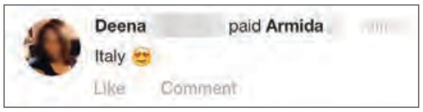
Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile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



Deena [redacted] paid Armida [redacted]

Italy 😍

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

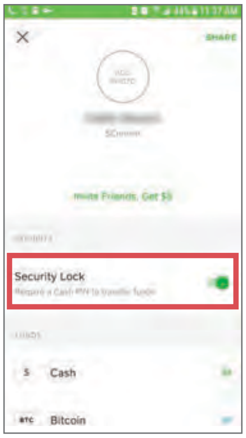
You should consider the following questions when choosing a mobile wallet:

- 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
$ Square Cash	iOS, Android	User to friend	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	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

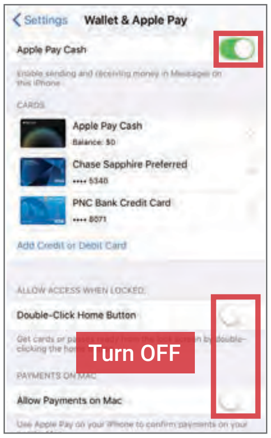


Navigate to **Settings** in the upper left portion of the home screen:

- 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.

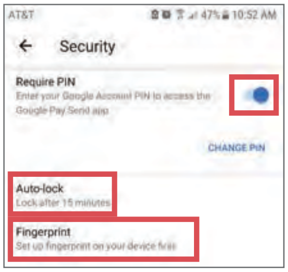
- **Toggle "Apple Pay Cash" ON** to enable direct money transfers with your contacts
- **Turn OFF "Double-Click Home Button"** to limit access to Apple Pay when your phone is locked
- **Turn OFF** "**Allow Payments on Mac"** to minimize risks of an unauthorized person making a purchase on your computer

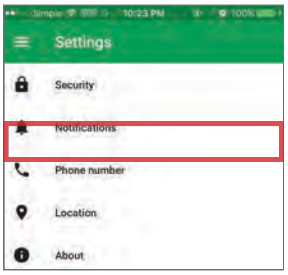
Enable PIN, password, or fingerprint protection for your iPhone's lock screen. Use more than one of these options to ensure extra security.

GOOGLE PAY

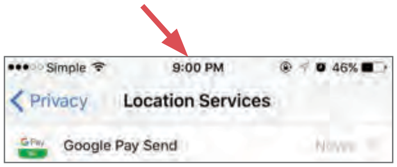
Navigate the dropdown menu to **Settings**:

- Under **Security**, **turn ON "Require PIN".**
- Set **Auto-lock** to **15 minutes**.
- Enable **Fingerprint/Touch ID**.
- Under **Notifications**, **turn ON** notifications for payments.
- Check monthly statements for unauthorized transactions.
- Monitor the **Transactions** section of the sidebar for unusual activity.


AT&T
10:52 AM
Security
Require PIN
Enter your Google Account PIN to access the Google Pay Send app
CHANGE PIN
Auto-lock
Lock after 15 minutes
Fingerprint
Set up fingerprint on your device first



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

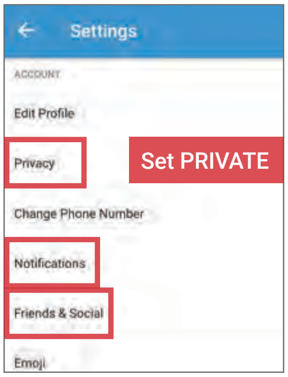


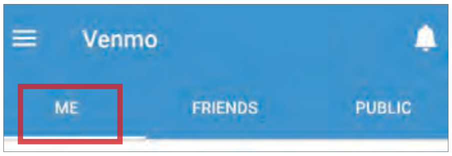
<u>Android users</u>: Navigate to **Google Pay Settings > Permissions** to disable location tracking for Google Pay

VENMO

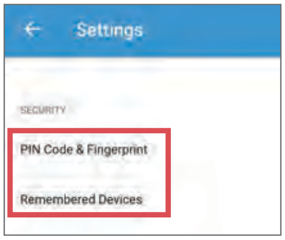
Navigate the dropdown menu to **Settings**:

- Under **Privacy**, select **Private**
- Under **Notifications**, enable push notifications for all **Payments** and **Activity** options
- Under **Security**, enable **PIN Code & Fingerprint.**
- Review **Remembered Devices** to check for suspicious log-ons.
- Under **Friends & Social**, do not connect Facebook or Phone Contacts





Monitor your transaction activity by selecting the **ME** tab at the top of the home screen

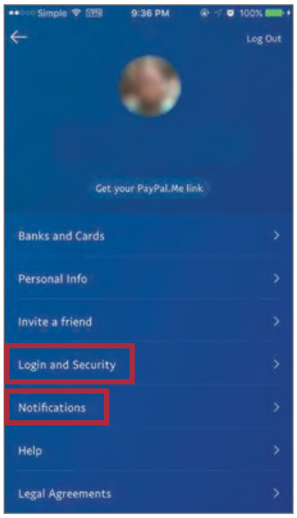


MOBILE WALLETS - BEST PRACTICES

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.
- Only provide personal or financial information that is required for mobile wallet use.
- Restrict permissions to your device contacts and settings.
- Never send or receive money from strangers or unverified accounts.

PAYPAL



Log in to PayPal using your browser and navigate to **Settings**.

- Use the **Security** tab to configure **Security questions**, **Mobile PIN**, and **Security key options**.
- Under the **Notifications** tab, configure email and/or text notifications for all account activities.
- Do not provide SSN or Passport numbers.
- Review account **Activity** routinely to monitor for suspicious activity.

Mobile: Under **Settings > Login and Security, toggle OFF** "**Remember Me"** to prevent account information from being accessed prior to login.

PayPal can now be linked with Google Pay.

HEALTH APPS & FITNESS TRACKERS

HEALTH APPS & FITNESS TRACKERS - DO'S AND DON'TS

- Do not connect your SNS accounts with your health and fitness profiles and apps. Ensure any social features are turned off.
- Provide minimal registration data during device setup; only complete required fields, and use your initials or an anonymous username when possible.
- Only enable connections during device data transmission; ensure they are disconnected when not in use.
- Frequently review permissions granted in your health and fitness apps under privacy settings. Sometimes permissions change without user notice.
- Research how to request archives and delete your health and fitness data with the wearable manufacturer before beginning to use the device.
- Limit the number of Internet of Things (IoT) and smart devices connected to the fitness-tracking device.

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 hitting 11.7% of the US population in 2018. The most common fitness tracker form factor is a wristband intended to be worn all day 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

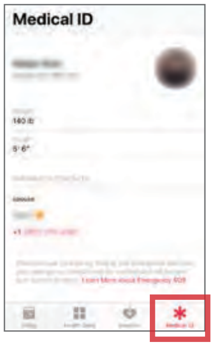
Most users track and analyze their health and fitness data in one of the three following ways:

- **Native apps**: Native fitness-tracking apps are native to 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 user's health and activities. These apps are device- and hardware-independent. They rely 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.

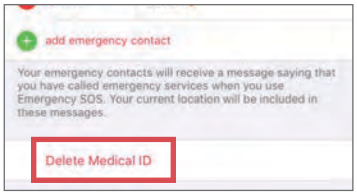
HEALTH & FITNESS APP	OS	COST	FITNESS DATA INPUT SOURCES	THIRD-PARTY DATA SHARING	BUILT-IN SNS LINKS	IDENTITY DATA	DEFAULT SHARING
APPLE HEALTH	iOS only	Free	iPhone, Apple Watch, third-party apps (e.g., FitBit)	Shares health and fitness data with other iOS apps	None	Name, birthdate, weight, height, emergency contacts	Private
SAMSUNG HEALTH	Android only	Free	Android devices; third-party fitness trackers, medical sensors, scales	Shares health and fitness data with partner apps	None	Email address, birthdate, gender, height, weight	Private
GOOGLE FIT/ WEAR OS	Android, iOS	Free	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	Free, Premium at $9.99 per month	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, birthdate	Private
FITBIT	Android, iOS, Windows	Free app, hardware $50-260	Fitbit fitness trackers	Shares data with compatible third-party apps	None	Name, display name, birthdate, gender, height, weight, place	Varies by data type
GARMIN	Android, iOS, Windows	Free app, hardware $50-560	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, birthdate	"My Groups and Connections"

APPLE HEALTH


Medical ID

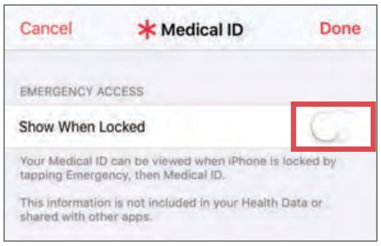
The Medical ID option shares personal data and is not required to access app features. Do not create one, or delete one if you already have one. If you already created Medical ID, navigate to the **Medical ID** tab at the bottom:

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


add emergency contact

Your emergency contacts will receive a message saying that you have called emergency services when you use Emergency SOS. Your current location will be included in these messages.

Delete Medical ID



EMERGENCY ACCESS

Show When Locked

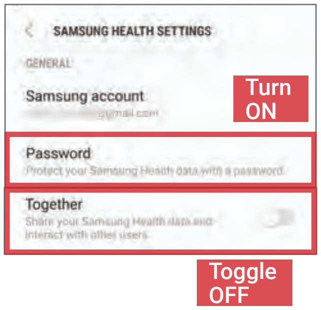
Your Medical ID can be viewed when iPhone is locked by tapping Emergency, then Medical ID.

This information is not included in your Health Data or shared with other apps.

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.


SAMSUNG HEALTH SETTINGS

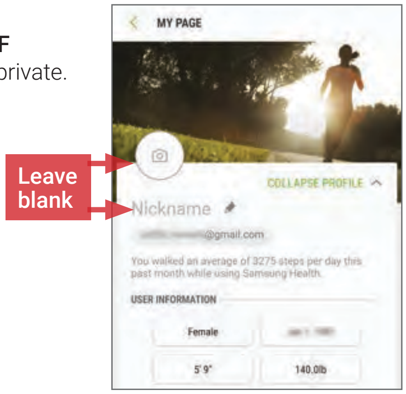
GENERAL

Samsung account

Password
Protect your Samsung Health data with a password.

Together
Share your Samsung Health data and interact with other users.

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


MY PAGE

Nickname

@gmail.com

You walked an average of 3275 steps per day this past month while using Samsung Health.

USER INFORMATION

Female

5'9"

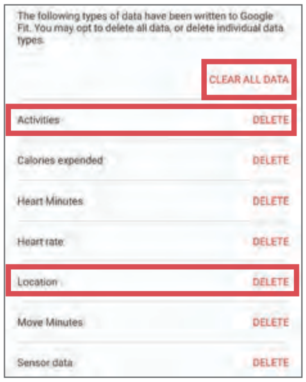
140.0lb

GOOGLE FIT

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

- To delete exisitng data: use **Manage your data > Manage data** to **Clear All Data** or delete **Activities** and **Location** data.
- Manage activity tracking (steps and distance) by setting **Track activity metrics** to **ON** or **OFF** as needed.

On your phone, navigate to **Settings > Apps > Fit > Permissions**, and toggle the **Location** permission **OFF**. Leaving location tracking enabled allows Google Fit to precisely map your daily activities, which may reveal sensitive information about your whereabouts.


The following types of data have been written to Google Fit. You may opt to delete all data, or delete individual data types.

CLEAR ALL DATA

Activities DELETE

Calories expended DELETE

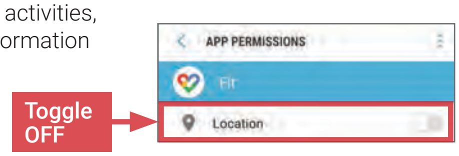
Heart Minutes DELETE

Heart rate DELETE

Location DELETE

Move Minutes DELETE

Sensor data DELETE

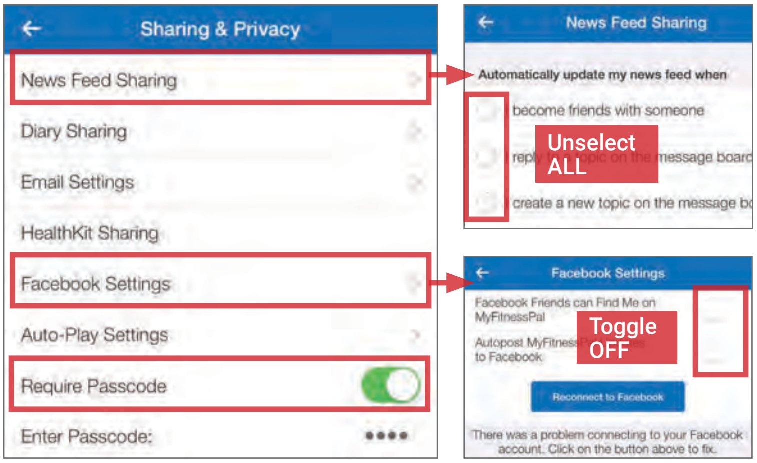

APP PERMISSIONS

Fit

Location

MYFITNESSPAL

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


Sharing & Privacy

News Feed Sharing

Diary Sharing

Email Settings

HealthKit Sharing

Facebook Settings

Auto-Play Settings

Require Passcode

Enter Passcode: ●●●●

News Feed Sharing

Automatically update my news feed when

○ I become friends with someone

○ I reply to a topic on the message board

○ I create a new topic on the message bo

Facebook Settings

Facebook Friends can Find Me on MyFitnessPal

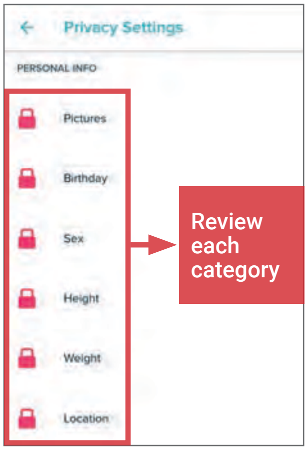
Autopost MyFitnessPal Updates to Facebook

There was a problem connecting to your Facebook account. Click on the button above to fix.

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 > Manage Account Access** to periodically review the devices accessing your account.
- Select **Manage Data > Manage Third Party Apps** to revoke access of connected apps.


Privacy Settings

PERSONAL INFO

Pictures

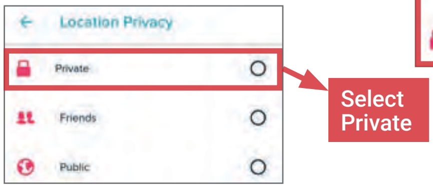
Birthday

Sex

Height

Weight

Location

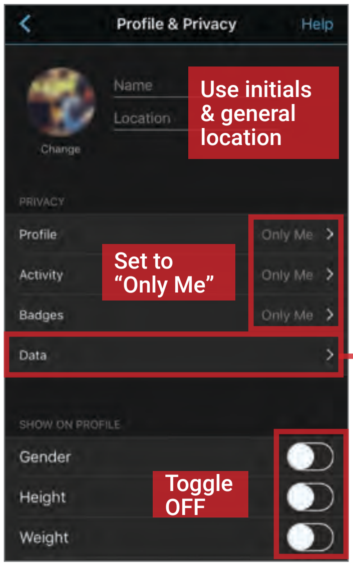

Location Privacy

Private ○

Friends ○

Public ○

GARMIN CONNECT



Name

Location

PRIVACY

Profile Only Me

Activity Only Me

Badges Only Me

Data

SHOW ON PROFILE

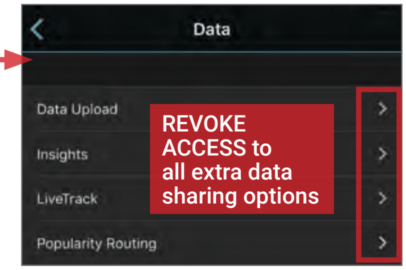
Gender

Height

Weight

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

- Set privacy settings of your Garmin profile and activities to **"Only Me."**
- **Toggle OFF** all personal data shown on your profile.
- Navigate to **Data**; **revoke access** to all additional data sharing.


Data

Data Upload

Insights

LiveTrack

Popularity Routing

SECURING HOME WI-FI NETWORK

SECURING HOME WIRELESS NETWORK - DO'S AND DON'TS

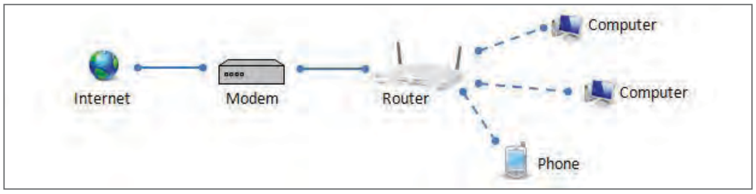
- Use an ethernet cable instead of a Wi-Fi connection when possible; disable the wireless network when it won't be used for an extended period of time.
- Use the most up-to-date hardware and operating systems to maximize your connecting device's security options.
- Turn on automatic updates for your 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 device's 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 card to secure your home wireless network and better protect your privacy.

WIRELESS 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. Launch any web browser and enter the default IP address of your wireless router into the 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 WIRELESS 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

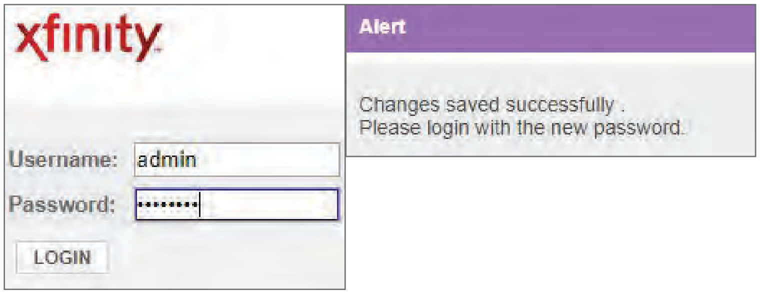
Following the recommendations outlined in this card will significantly reduce your home network's chances of becoming compromised. However, it is wise to periodically check if there has been any unauthorized activity on your network. Within the router's web interface, locate the section that identifies 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 unlawfully, **immediately change the usernames and passwords to the wireless network and administrative login pages**. Also remember to check and re-secure other online accounts including online banking, social media, and email accounts. If your network was compromised it is possible that the hacker may have been able to see your Internet traffic and gain access to your login credentials or other personal data.

WIRELESS 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 card 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.



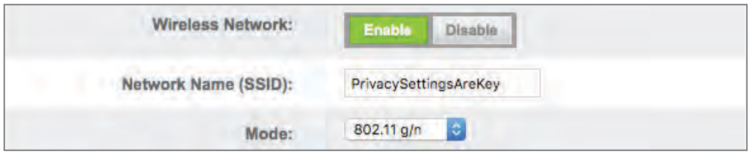
Username: admin

Password: ••••••••

Changes saved successfully .
Please login with the new password.

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.



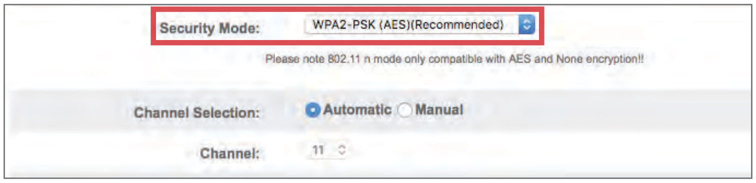
Wireless Network: Enable | Disable

Network Name (SSID): PrivacySettingsAreKey

Mode: 802.11 g/n

CHOOSING 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.



Security Mode: WPA2-PSK (AES)(Recommended)

Please note 802.11 n mode only compatible with AES and None encryption!!

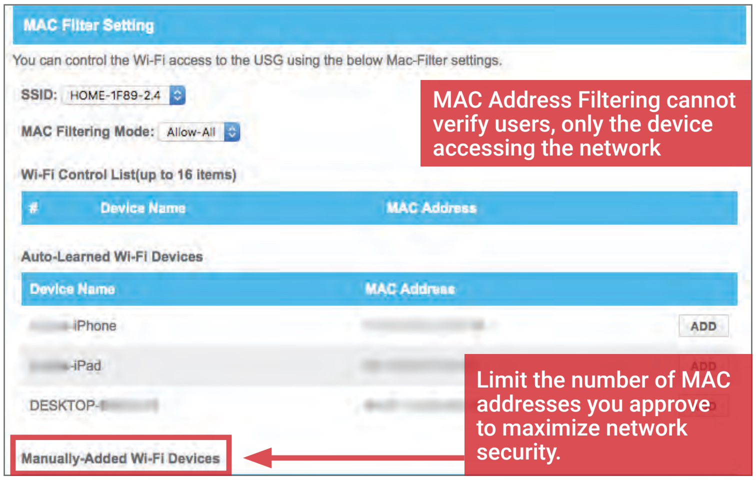
Channel Selection: ● Automatic ○ Manual

Channel: 11

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 Filter Setting

You can control the Wi-Fi access to the USG using the below Mac-Filter settings.

SSID: HOME-1F89-2.4

MAC Filtering Mode: Allow-All

Wi-Fi Control List(up to 16 items)

#	Device Name	MAC Address

Auto-Learned Wi-Fi Devices

Device Name	MAC Address	
[redacted]-iPhone	[redacted]	ADD
[redacted]-iPad	[redacted]	ADD
DESKTOP-[redacted]	[redacted]	ADD

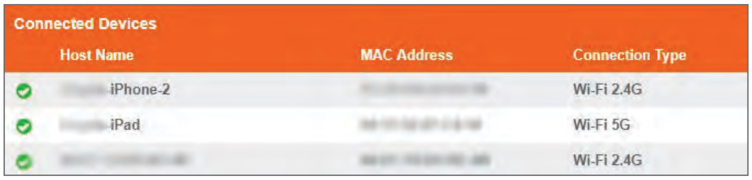
Manually-Added Wi-Fi Devices

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.

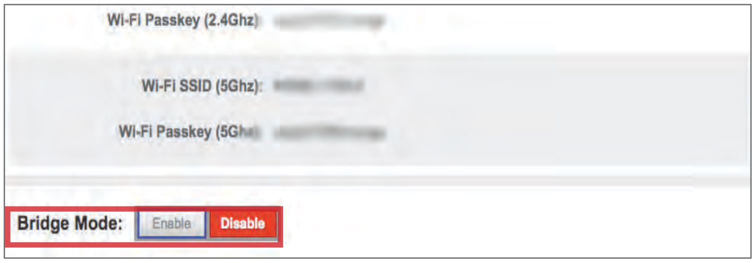


Connected Devices

	Host Name	MAC Address	Connection Type
✓	[redacted]-iPhone-2	[redacted]	Wi-Fi 2.4G
✓	[redacted]-iPad	[redacted]	Wi-Fi 5G
✓	[redacted]	[redacted]	Wi-Fi 2.4G

DISABLE HYBRID ROUTER SETTINGS

In the case of a hybrid router-modem, it is possible to 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.

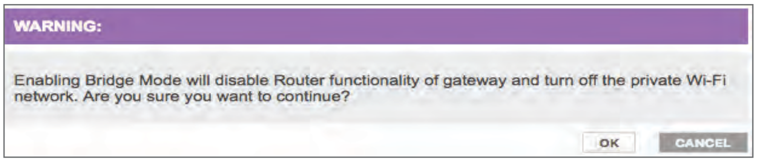


Wi-Fi Passkey (2.4Ghz): [redacted]

Wi-Fi SSID (5Ghz): [redacted]

Wi-Fi Passkey (5Ghz): [redacted]

Bridge Mode: Enable | Disable



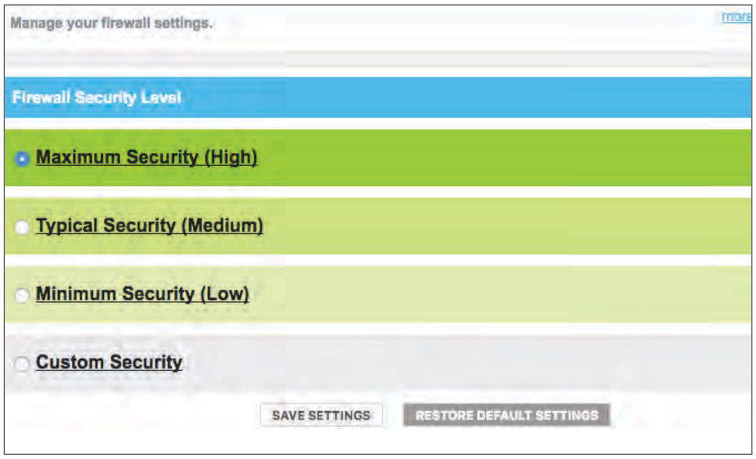
WARNING:

Enabling Bridge Mode will disable Router functionality of gateway and turn off the private Wi-Fi network. Are you sure you want to continue?

OK | CANCEL

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 techniques 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.



Manage your firewall settings. more

Firewall Security Level

● Maximum Security (High)

○ Typical Security (Medium)

○ Minimum Security (Low)

○ Custom Security

SAVE SETTINGS | RESTORE DEFAULT SETTINGS

ONLINE REGISTRATION

ONLINE REGISTRATION - DO'S AND DON'TS

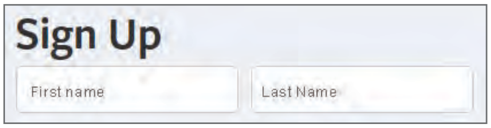
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your Social Security Number or physical address.
- Do not upload or share your existing contacts with a social networking service (SNS) during registration.
- Remove any identity data from your personal profile that was required during sign-up after completing the registration process.
- Change privacy settings to protect your identity information immediately after registering for an online profile.

IDENTITY DATA IN SOCIAL NETWORKING SERVICE (SNS) ACCOUNTS

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Common identity elements required by social networking services (SNS) in exchange for 1) creating accounts and 2) participating in their services and features are shown below.

FIRST AND LAST NAME

First and last names are mandatory for almost all SNS accounts. When possible, use your initial instead of your full last name, especially if it is uncommon.



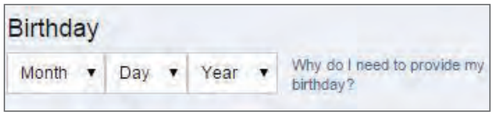
USERNAME

Usernames are unique to each user account, and are used to identify specific individuals within a network. When making your username, do not include personally identifiable information (PII), such as your name, location, or birthday.

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

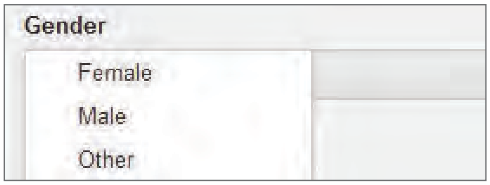
BIRTHDAY

Birthdays are used to verify the user's age and customize age-appropriate content on the site. This information is sometimes published on the SNS profile and has to be removed retroactively. Don't share your full birthdate unless it's required.



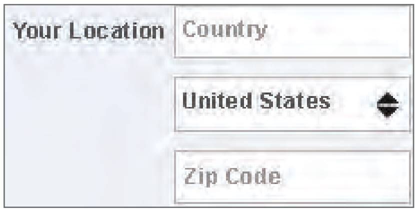
GENDER

Gender is a common field to fill out on the registration page. Whenever possible, avoid making a distinction when signing up.



LOCATION INFORMATION

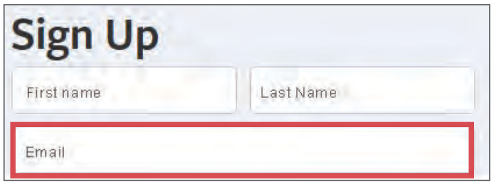
Location information is required at varied levels of granularity depending on the service. It may include address, city, ZIP code, and/or country. During sign up, only provide the most generic location level required by the service, or consider entering a nearby ZIP code or metropolitan area.



United States

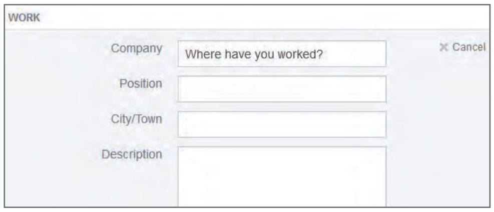
EMAIL ADDRESS

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



EMPLOYMENT INFORMATION

With the exception of professional-oriented SNS services, company and employment information are often optional data fields. When providing work information, try to be as generic as possible (i.e. only provide the industry you work in). Avoid posting your employer and your work location.

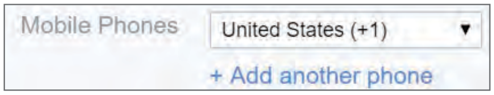


SOCIAL LOGIN

Services may allow users to sign up through preexisting SNS accounts (e.g., Google Plus, Twitter, or Facebook) by importing your existing data. Avoid using social login whenever possible.

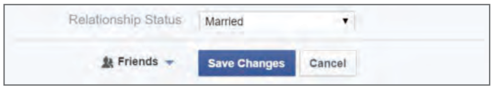
MOBILE PHONE NUMBERS

Increasingly, accounts may ask to verify your identity using a phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.


Mobile Phones: United States (+1)

RELATIONSHIPS/ORIENTATION

Relationship status and sexual orientation are almost always optional data fields, except for online dating sites. Refrain from sharing this data with the service unless it is required.


Relationship Status: Married

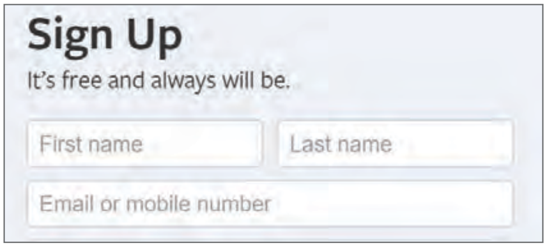
IDENTITY FIELDS DURING REGISTRATION, BY SERVICE

Service Name	Outlook	Yahoo	Facebook	Twitter	Google	LinkedIn	Pinterest	Instagram	Yelp
First and last name	✓	✓	✓	✓	✓	✓	✓	✓	✓
Username	✓			✓				✓	
Password	✓	✓	✓	✓	✓	✓	✓	✓	✓
Birthdate	✓	✓	✓		✓				Optional
Age							✓		
Gender		Optional	✓		✓		✓		Optional
Email address			Or Phone	Or Phone	✓	✓	✓	Or Phone	✓
Phone number	Optional	✓	Or Email	Or Email	Optional			Or Email	
Country	✓					✓			
Company						✓			
Job title						✓			
ZIP code						✓			✓
Social Login		Optional				Optional	Optional	Optional	Optional
Language	✓						✓		
Interests							✓		
CAPTCHA	✓								
Time Zone	✓								

ONLINE REGISTRATION AND VERIFICATION PROCESS

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

1. Enter required identity fields on the registration page. Avoid supplying more information than is required.



Sign Up

It's free and always will be.

First name

Last name

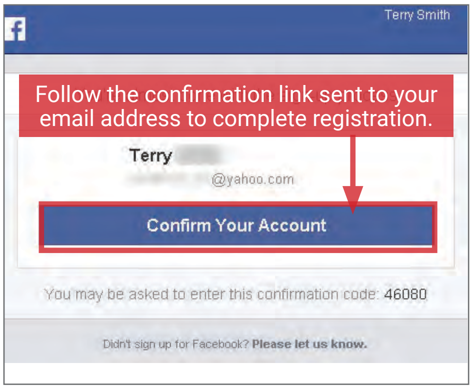
Email or mobile number

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. When possible, use an application such as Authy or Okta that automatically generates a login code, instead of providing your phone number for dual-factor authentication.

token is:

556584

3. 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.



Terry Smith

Follow the confirmation link sent to your email address to complete registration.

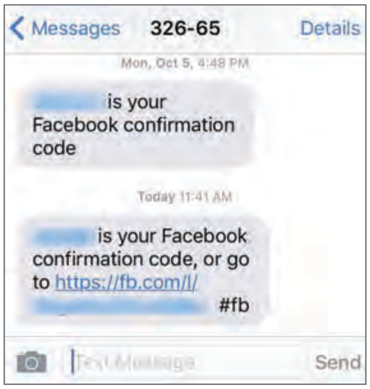
Terry [redacted]

[redacted]@yahoo.com

Confirm Your Account

You may be asked to enter this confirmation code: 46080

Didn't sign up for Facebook? **Please let us know.**



Messages 326-65 Details

Mon, Oct 5, 4:48 PM

[redacted] is your Facebook confirmation code

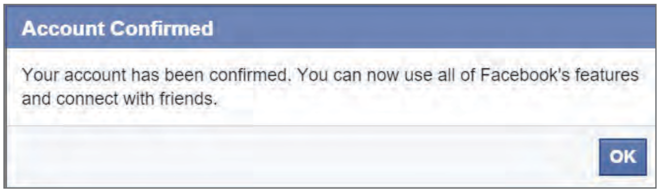
Today 11:41 AM

[redacted] is your Facebook confirmation code, or go to https://fb.com/l/ [redacted] #fb

Text Message

Send

4. Access your newly created account once it is confirmed. Review your populated personal identity data fields and remove any non-required personal information.



Account Confirmed

Your account has been confirmed. You can now use all of Facebook's features and connect with friends.

OK

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 media 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, regarding how to remove personal details from data aggregators, 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. Online methods often require your email address; monitor your inbox and spam folder to ensure you receive opt-out email instructions and confirmations. Note the timeframe required for data removal, and check the aggregator site after that time has passed to ensure your information has been removed. Given the quantity of data aggregators, it may be helpful to create and update a tracking sheet to guide your removal processes.

PRIVATEEYE - PEOPLEFINDERS - PUBLICRECORDSNOW - VEROMI

PrivateEye, PeopleFinders, PublicRecordsNow, and Veromi are all owned by the same parent company: **Confi-Chek.com**.

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 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 Veromi by visiting: veromi.net/Help.
Under **Privacy and Security** select **How do I remove myself from these records?** and follow the instructions.

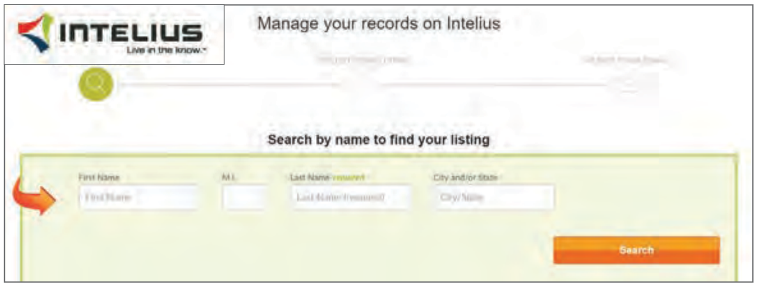
Opt out of PublicRecordsNOW by visiting:
https://www.publicrecordsnow.com/static/view/optout/
Enter your information and select **Opt out.**

US SEARCH

Opt out of US Search by visiting http://www.ussearch.com/privacylock. Search for your name and select the appropriate listing to block. Print the cover sheet and mail or fax to the address/number provided with a copy of a state issued ID or drivers license.
www.ussearch.com

INTELIUS - PUBLIC RECORDS - ZABASEARCH - SPOCK - ISEARCH - DATECHECK - LOOKUP - LOOKUPANYONE - PEOPLE LOOKUP - PHONESBOOK

Intelius owns, or is affiliated with, the following people search websites: Public Records, Zabasearch, Spock, iSearch, DateCheck, LookUp, LookupAnyone, People Lookup, and PhonesBook. Instructions for opting out of each site vary. Visit the help section of each website and search for instructions under Privacy and Opt Out topics. Opt out of Intelius online at http://intelius.com/optout. Requests are usually completed within 72 hours.


Manage your records on Intelius

Search by name to find your listing

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 reCAPTCHA, 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/opt_out/new.

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.

US IDENTITY

First, search for your information on US Identify and identify the profile(s) relevant to you. Be sure to include aliases, if applicable.

To opt out of US Identify, visit http://www.usidentify.com/company/contact.html. You may submit an opt-out email request to support@usidentify.com or contact customer service by phone at (855) 454-0394.

In an email request, write "*I would like all information for [Name] [Date of Birth] [Current City and State] removed from usidentify.com and all affiliated sites.*"

INSTANTCHECKMATE

To opt out of InstantCheckMate, follow the instructions at: www.instantcheckmate.com/optout

Select **Remove This Record**. Enter your email address, complete the reCAPTCHA 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 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. 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**.

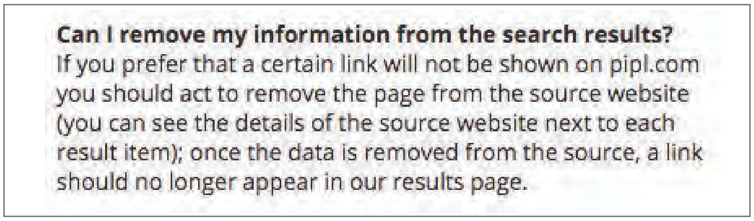
Verify your identity with a phone call; enter your phone number and you will immediately receive an automated call from Whitepages. Use your touchscreen to enter the 4 digit verification code provided via the opt out form. For further details, visit:

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.

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 the fastest growing crime in America. In 2017, more than 16.7 million incidents of identity fraud were reported by individuals in the US. On average, each victim spends 100 to 200 hours over a six-month period trying to resolve an identity fraud issue. 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. 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.

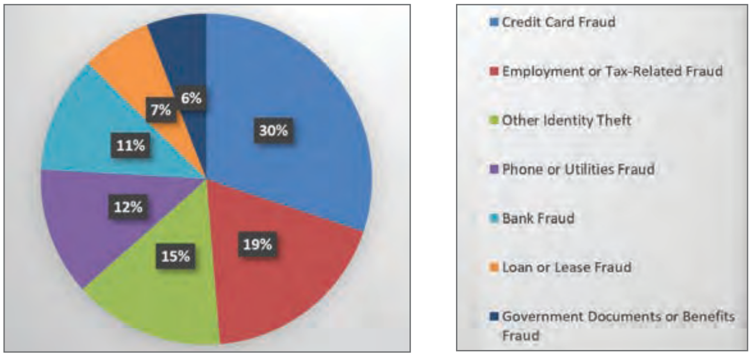
SENSITIVE DATA

- 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?



*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

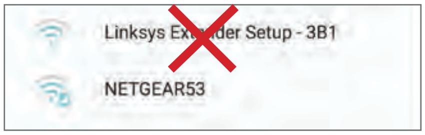
AGE OF VICTIMS

- < 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



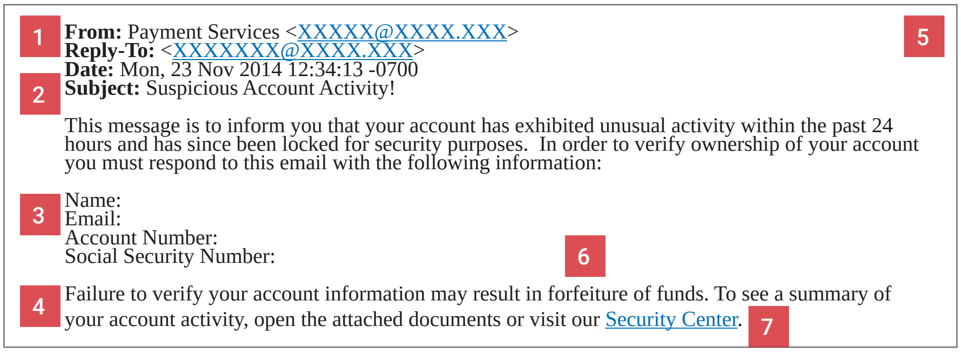
SOCIAL MEDIA MINING

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 profiles, and never disclose any of the sensitive information listed above.

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.



From: Payment Services <XXXXX@XXXX.XXX>
Reply-To: <XXXXXXX@XXXX.XXX>
Date: Mon, 23 Nov 2014 12:34:13 -0700
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:

Name:
Email:
Account Number:
Social Security Number:

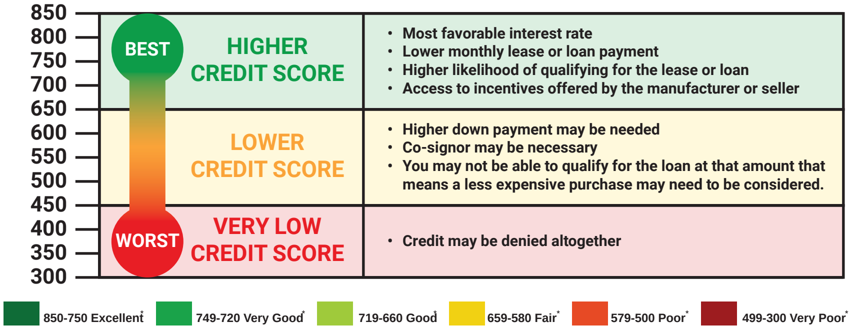
Failure to verify your account information may result in forfeiture of funds. To see a summary of your account activity, open the attached documents or visit our Security Center.

Last Updated: 03/01/2019

SIGNS OF IDENTITY THEFT

Credit scores are susceptible to damage through identity theft. However, damages from identity theft can be reduced significantly if caught early. Bank statements should be checked weekly, while each of the three credit reports 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.



*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.

DATA PROTECTION & RECOVERY VENDOR	PRODUCT	SSN	BANK ACCOUNT	CREDIT CARD	MEDICAL FRAUD	PUBLIC & COURT RECORDS	COMPUTER SECURITY OFFERINGS	CREDIT REPORTS	FINANCIAL COVERAGE	PRICE/ MONTH
IDENTITY GUARD	Premier	✓	✓	✓		✓	✓	Annually	Up to $1 Million	$24.99
IdentityForce Protect What Matters Most	UltraSecure + Credit	✓	✓	✓	✓	✓	✓	Quarterly	Up to $1 Million	$23.95
LifeLock	Ultimate Plus	✓	✓	✓		✓		Annually	Up to $1 Million	$29.99

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

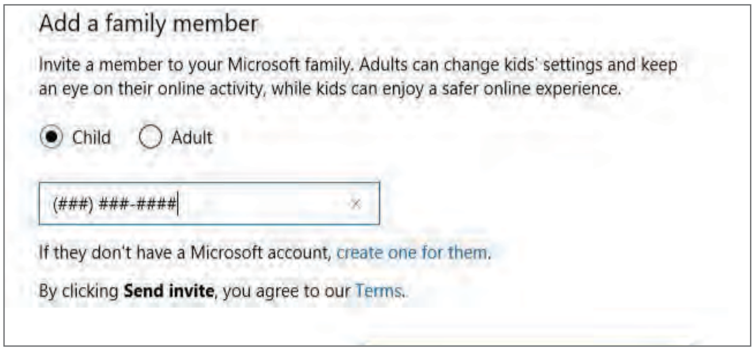
- One family member's unsecured privacy and sharing settings can expose personal data from the rest of the family.
- Ensure kids only establish and maintain connections with people you know and trust. Review their connections often.
- Assume that ANYONE can see any information kids post and share regarding 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

A 2016 study reported that 96% of children above the age of eight claimed to actively use the Internet, where kids are potentially exposed to cyber-bullying, influence operations, pornography, drugs/alcohol, 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.

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.



Add a family member

Invite a member to your Microsoft family. Adults can change kids' settings and keep an eye on their online activity, while kids can enjoy a safer online experience.

● Child ○ Adult

(###) ###-####

If they don't have a Microsoft account, create one for them.

By clicking **Send invite**, you agree to our Terms.

PARENTAL CONTROLS

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

PASSWORDS

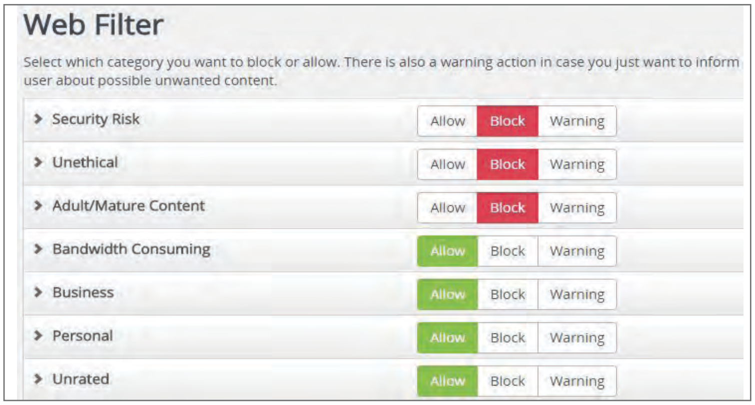
Create a username/password for your child's account that only you know.

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.



Web Filter

Select which category you want to block or allow. There is also a warning action in case you just want to inform user about possible unwanted content.

> Security Risk	Allow	[✓ Block]	Warning
> Unethical	Allow	[✓ Block]	Warning
> Adult/Mature Content	Allow	[✓ Block]	Warning
> Bandwidth Consuming	[✓ Allow]	Block	Warning
> Business	[✓ Allow]	Block	Warning
> Personal	[✓ Allow]	Block	Warning
> Unrated	[✓ Allow]	Block	Warning

ADVANCE SETUP

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

FILTERS

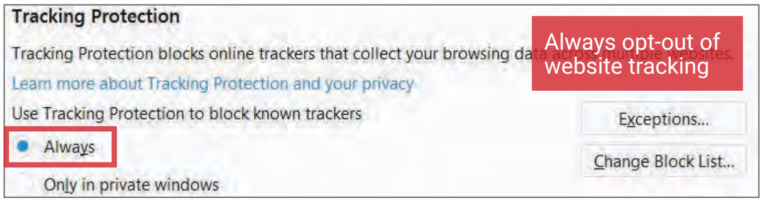
YouTube Filter - filters individual YouTube channels and videos for content.
Content Filtering - identifies specific words in webpages to prevent access.
Black/White List - allows users to add specific URLs to block or allow.

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**.



Tracking Protection

Tracking Protection blocks online trackers that collect your browsing da

Learn more about Tracking Protection and your privacy

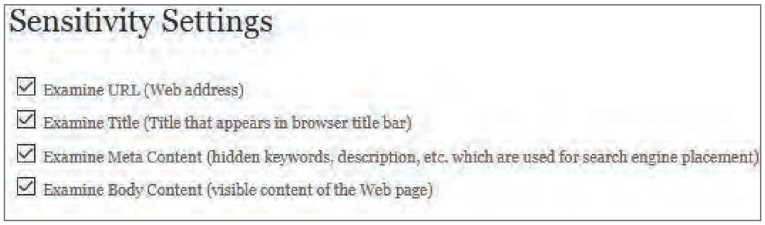
Use Tracking Protection to block known trackers

● Always

○ Only in private windows

Always opt-out of website tracking

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.



Sensitivity Settings

☑ Examine URL (Web address)

☑ Examine Title (Title that appears in browser title bar)

☑ Examine Meta Content (hidden keywords, description, etc. which are used for search engine placement)

☑ Examine Body Content (visible content of the Web page)

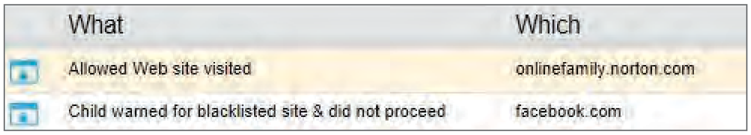
FAMILY SAFETY SERVICES

A variety of free and paid services are available for monitoring your children's online activities. The software options listed below are effective in either restricting or monitoring content that your child tries to access.

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

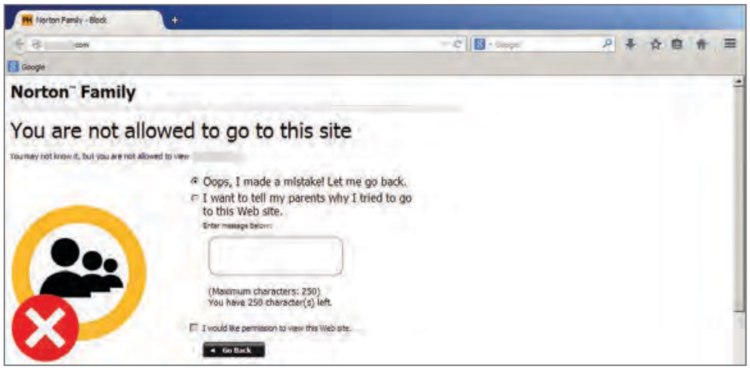
NORTON SECURITY PREMIUM

At a cost of $109.99/year, this comprehensive service offers online family monitoring features along with Norton Security protection. This service allows parents to track which websites children visit and prevent certain harmful content from being displayed on their monitors. Parents can use this tool to conduct web, time, search, social network, moible app, text, and video supervision; review activity history; lock devices; and receive email alerts, on up to 10 devices.



What	Which
Allowed Web site visited	onlinefamily.norton.com
Child warned for blacklisted site & did not proceed	facebook.com

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



Norton™ Family

You are not allowed to go to this site

You may not know it, but you are not allowed to view

● Oops, I made a mistake! Let me go back.
○ I want to tell my parents why I tried to go to this Web site.

Enter message below:

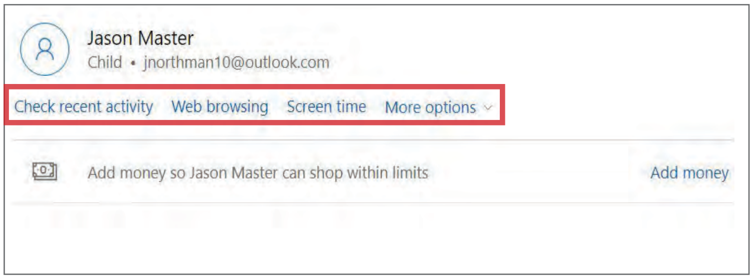
(Maximum characters: 250)
You have 250 character(s) left.

□ I would like permission to view this Web site.

◄ Go Back

MICROSOFT FAMILY SAFETY

Activate this free service from your Microsoft/Outlook account. The service provides basic content filters and reports of programs/websites accessed by each account.



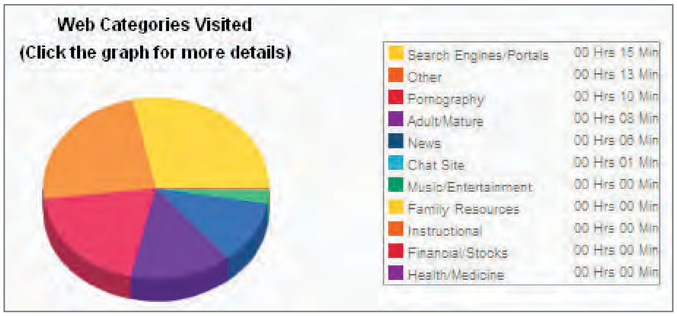
Jason Master
Child • jnorthman10@outlook.com

Add money so Jason Master can shop within limits

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

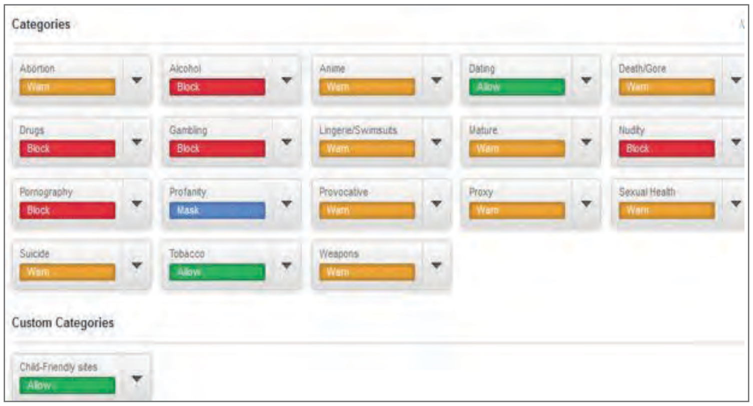
This service is available for download for $39.99 and can both restrict and monitor content from computer programs, instant messengers, SNSes, and web browsing applications. It is installed onto the desktop and provides the most granular settings for filtering and reporting potentially harmful content online.



Web Categories Visited
(Click the graph for more details)

Search Engines/Portals	00 Hrs 15 Min
Other	00 Hrs 13 Min
Pornography	00 Hrs 10 Min
Adult/Mature	00 Hrs 08 Min
News	00 Hrs 06 Min
Chat Site	00 Hrs 01 Min
Music/Entertainment	00 Hrs 00 Min
Family Resources	00 Hrs 00 Min
Instructional	00 Hrs 00 Min
Financial/Stocks	00 Hrs 00 Min
Health/Medicine	00 Hrs 00 Min

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.



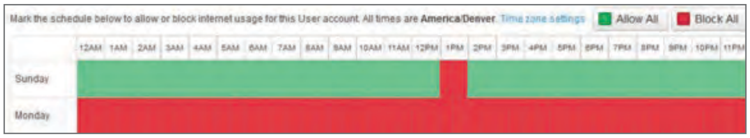
Categories

Abortion Warn	Alcohol Block	Anime Warn	Dating Allow	Death/Gore Warn
Drugs Block	Gambling Block	Lingerie/Swimsuits Warn	Mature Warn	Nudity Block
Pornography Block	Profanity Mask	Provocative Warn	Proxy Warn	Sexual Health Warn
Suicide Warn	Tobacco Allow	Weapons Warn		

Custom Categories

Child-Friendly sites
Allow

Net Nanny also provides time-based Internet usage restriction capabilities for each user profile.



Mark the schedule below to allow or block internet usage for this User account. All times are **America/Denver**. Time zone settings

VOICE OVER INTERNET PROTOCOL (VOIP)

VOICE OVER INTERNET PROTOCOL (VOIP) - DO'S AND DON'TS

- Determine the features you need. VOIP services range from free smartphone apps to full-featured subscription enterprise systems.
- Check your bandwidth. You may need to upgrade your Internet connection to optimally use bandwidth-heavy VOIP services.
- Keep a landline or cellphone active to use when Internet service is not available, during power outages, and for calls to emergency services.
- Prevent strangers from being able to discover your phone number or profile by implementing the most restrictive privacy settings after signing up.
- Watch your wallet. Keep an eye out for hidden charges for licensing and support, or free trials that become long-term contracts.
- Ask about your VOIP provider's disaster recovery plan in the event of a system failure.

WHAT IS VOIP?

Voice Over Internet Protocol (VOIP) is a group of technologies that allow voice and video calls and multimedia messages to be delivered over the Internet to other VOIP users, or to users on legacy telephone networks anywhere in the world. Communications travel over broadband Internet connections via computer, Internet Protocol (IP) telephones, tablets, smartphones, specially-equipped analog telephones, and television sets, making VOIP an attractive, low-cost alternative to traditional telephone services. Popular VOIP services include Skype, FaceTime, Silent Circle, Google Hangouts, Viber, Vonage, and WhatsApp, but there are several types:

- Business - Multi-line packages that require special equipment or cloud services and substantially more bandwidth than a typical home connection. Advanced features such as private branch exchanges, automated attendants, and faxing are available.
- Residential - VOIP services provided through a DSL or cable modem, or a special VOIP router that provides more bandwidth for calls. These packages often use a combination of installed equipment and mobile apps.
- Mobile - Free or low-cost VOIP services available through smartphone apps. Calls and messages travel over a cellular data connection or Wi-Fi.

BENEFITS

VOIP calls are affordable, particularly since most services do not have long-distance fees and offer low per-minute rates for international calls. Some companies, such as Google, Apple, and Microsoft, offer free VOIP services.

Popular features include group video chat, file-sharing, mobile apps, voicemail transcription, call screening, call recording, and transferring calls or messages between devices.

VOIP can be used anywhere you can connect to the Internet.

One number can ring multiple devices simultaneously. Users can also choose which calls go to which devices and at what times.

VOIP does not have geographic boundaries. Users can easily acquire local numbers in other states or countries.

Because of its extensibility and portability, it is easier for developers to create and implement new applications and technologies that can transmit data through VOIP.

EVALUATING PROVIDERS

- Which features are in the basic plan? Which require an additional fee?
- Is the service E911-compliant?
- Does the paid service provider itemize its fees? Does it breakdown its activation, licensing, equipment, support, per-minute rates, and any termination fees?
- Is special equipment required? Is it free?
- Can purchased equipment be used with other providers?
- Is live support available 24 hours a day, seven days a week?

DISADVANTAGES

As with any data online, VOIP is vulnerable to hacking. Also, service providers may be able to access encrypted messages and store them indefinitely. **VOIP is not considered secure for the purpose of transmitting sensitive data.**

A poor Internet connection can result in delayed messages, buffering, and low audio/image quality.

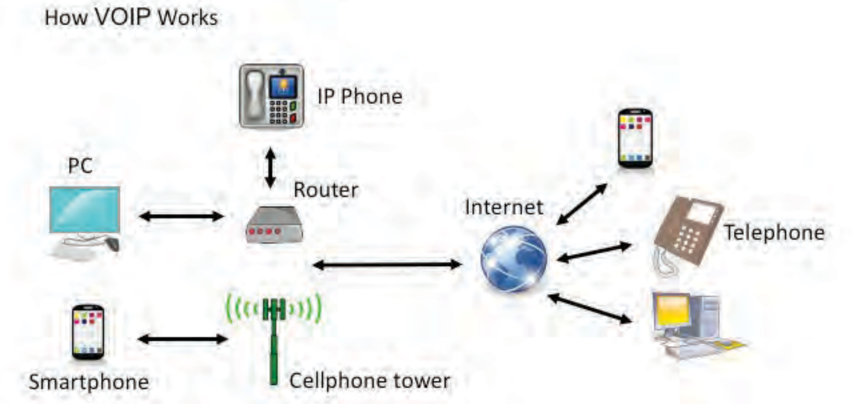
Some providers do not connect to 911 or emergency services, so a second phone line may be needed.

Not all devices are E911-compliant (Enhanced 911), meaning they do not automatically transmit a caller's location to emergency operators.

VOIP hardware cannot be used without power and an Internet connection.

Security systems and other devices in your home may not work with VOIP.

VOIP is vulnerable to routine computer disruptions, including crashes and malware.



USING VOIP SECURELY

Password-protect your apps, and encrypt or erase sensitive information including texts, call history, and voicemail. Here are some tips and security-related questions to ask:

- Are all calls on the provider network encrypted? For calls to landline phones, the portion of calls carried on the legacy network is not encrypted.
- Are messages encrypted in transit and at rest, so even the provider can not access them?
- Does the provider use firewalls, redundant servers, and 24/7 monitoring?
- How often does the provider test for system vulnerabilities? Are patches applied quickly?
- Can you use your own virtual private network (VPN) with the VOIP service?
- For residential service, can stolen equipment (routers, phones) be disabled remotely?

CHOOSING A VOIP PROVIDER

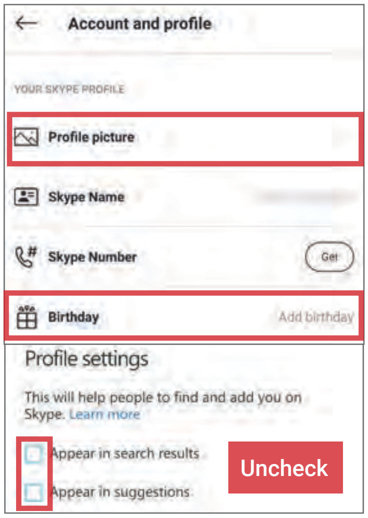
MOBILE SERVICE	OPERATING SYSTEM	COST	BEST USES
skype	Windows, Mac, iOS, web, Android	Free to $13.99/month	File sharing, screen sharing, document collaboration, video calls
Google+ Hangouts	iOS, Android, web	Free	Encrypted one-to-one or group audio/video calls, live streaming video, screen sharing (web)
silent circle	iOS, Android	$9.95/month	Anonymous, encrypted calls and messages, identity verification
FaceTime	iOS, Mac	Free	Encrypted audio calls, video calls, and messages; voice memos
Viber	iOS, Android, Windows, Linux	Free	Encrypted audio calls, video calls, and text messages; group chat up to 250 people.
Cryptocat	Windows, iOS, Mac, Linux, web	Free	Secure messaging, encrypted file sharing

Residential VOIP services have similar cost savings to mobile apps but require more hardware, including a broadband modem and a telephone adapter or VOIP-ready telephone. A service contract may also be required.

Popular residential VOIP services include:

- **Ooma**: $79.99 equipment purchase. Service is free (except taxes and fees) and calls to other Ooma users are encrypted.
- **Vonage**: $9.99 a month. Unlimited domestic calls and mobile app.
- **Via Talk**: $15.75 a month. Unlimited domestic calls.

SKYPE



← Account and profile

YOUR SKYPE PROFILE

Profile picture

Skype Name [redacted]

Skype Number Get

Birthday Add birthday

Profile settings

This will help people to find and add you on Skype. Learn more

□ Appear in search results

□ Appear in suggestions

Under **Settings**, go to **Account & Profile > Your Skype Profile**:

- Under **Profile picture**, set visibility to **Contacts only.**
- Do not add your **Birthday.**

Under **Account & Profile > Manage > Your profile**:

- Do not provide optional personal data such as gender, location, or contact information.
- Uncheck boxes for **Appear in search results** and **Appear in suggestions**.

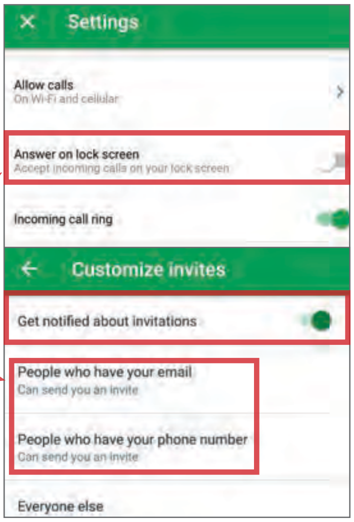
Under **Settings > Contacts, toggle "Sync your contacts"** to **OFF**.

GOOGLE HANGOUTS

Sign up for a Google Voice (GV) account at google.com/voice for a free number or port your existing number.

Install the Hangouts app and connect your GV number. In **Settings**:

- **Toggle "Answer on lock screen"** to **OFF**.
- Navigate to **Invitations > Customize invites** and select who can contact you directly and who needs an invite in order to establish a call.
- **Turn ON** invitation notifications.



× Settings

Allow calls
On Wi-Fi and cellular

Answer on lock screen
Accept incoming calls on your lock screen

Incoming call ring

← Customize invites

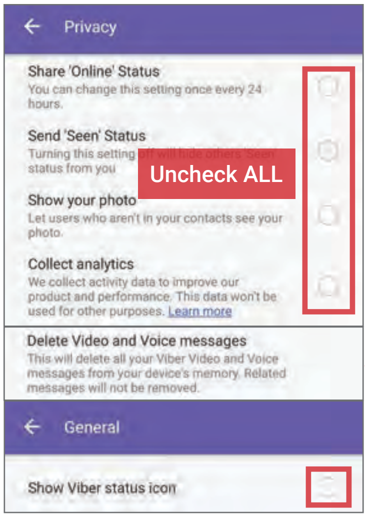
Get notified about invitations

People who have your email
Can send you an invite

People who have your phone number
Can send you an invite

Everyone else

VIBER



← Privacy

Share 'Online' Status
You can change this setting once every 24 hours.

Send 'Seen' Status
Turning this setting off will hide others 'Seen' status from you

Show your photo
Let users who aren't in your contacts see your photo.

Collect analytics
We collect activity data to improve our product and performance. This data won't be used for other purposes. Learn more

Delete Video and Voice messages
This will delete all your Viber Video and Voice messages from your device's memory. Related messages will not be removed.

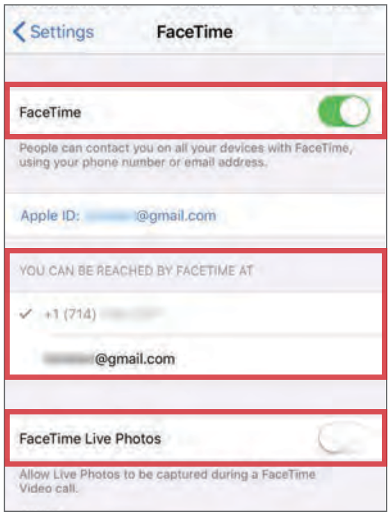
← General

Show Viber status icon

Download and install the Viber app.

- Under **Settings > Privacy**, uncheck all boxes. Do not connect Viber to your Facebook or Twitter account.
- Under **Calls and messages**, uncheck boxes for Viber-in Calls and Receive Service Messages.
- Under **Media**, select **Delete Video and Voice messages**. Deselect both **Auto download** options.
- Under **General**, deselect **Show Viber status icon** and **Open links internally.**

FACETIME



< Settings FaceTime

FaceTime

People can contact you on all your devices with FaceTime, using your phone number or email address.

Apple ID: [redacted]@gmail.com

YOU CAN BE REACHED BY FACETIME AT

✓ +1 (714) [redacted]

[redacted]@gmail.com

FaceTime Live Photos

Allow Live Photos to be captured during a FaceTime Video call.

FaceTime is a built-in VOIP option for Apple users. FaceTime simply requires being logged in with your Apple ID to Mac, iPhone, or iPad.

Navigate to **Settings > FaceTime**.

- **Turn** FaceTime **ON.**
- Select if others can reach you on FaceTime by your phone number, email, or both. We recommend only enabling one of the two options.
- **Toggle "FaceTime Live Photos"** to **OFF.**

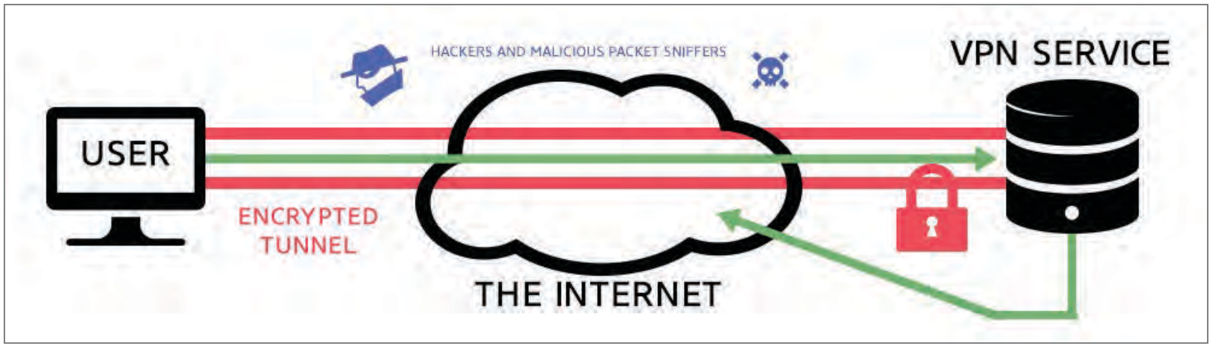
VIRTUAL PRIVATE NETWORK (VPN)

VIRTUAL PRIVATE NETWORKS - 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 on a VPN, 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 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.

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. These are some questions to consider before committing to one provider:

- 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 promise complete anonymity?
- What level of data encryption is offered? Does the service provider keep server logs?
- Where is the VPN provider located?

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. Compare the capabilities of four popular VPN service providers below to determine which product best suits your usage case and protection needs.

SERVICES	COMPATIBILITY	COST	PROS	CONS
ExpressVPN	iOS, Windows, Android, Linux, Blackberry, routers, browser extensions, media streaming devices	• $12.95 per month • 30-day money back guarantee	• Can run 3 devices simultaneously (with premium service) • VPN killswitch offered for Windows • Provides content unblocking	• Connection logs are retained • Limited simultaneous device connections
ZenMate	iOS, Windows, Android, Chrome, Firefox, Opera, routers	• Unlimited free browser add-on • $8.99 per month • 14-day money back guarantee	• Extremely streamlined and easy-to-use	• Limited traffic settings • Uses one security protocol (L2TP)
IPVANISH VPN	iOS, Windows, Android	• $10 per month • 7-day money back guarantee	• 2 simultaneous connections • Unlimited bandwidth • No VPN traffic logs	• No free trial • Limited device connections
CyberGhost	iOS, Windows, Android, Linux, Chrome OS, Raspberry Pi, routers	• Free limited service • $10.99 per month for full service • 30-day money back guarantee	• IP address shielding • Highly configurable • Unlimited bandwidth with premium subscription	• Full service requires a paid subscription • Server availability varies by country

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, decreasing the risk of identity exposure against data theft and malicious attacks.
- VPN users can route web traffic through servers in other countries, which offer unique benefits, such as allowing users to view country-specific content that is normally blocked in their physical location.

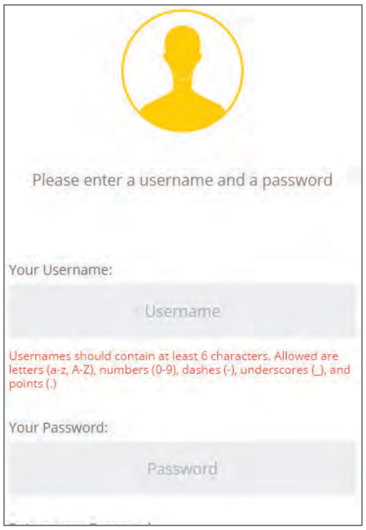
VPN VULNERABILITIES

- VPNs can cause a reduction in Internet connection speed. The tunneling effect of most VPN services creates a lag in the connection.
- 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.

HOW TO ESTABLISH AND CONNECT TO A VPN

Following VPN provider selection, set up 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.

1 Create an account with your chosen VPN service provider.



Please enter a username and a password

Your Username:

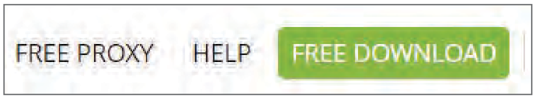
Username

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

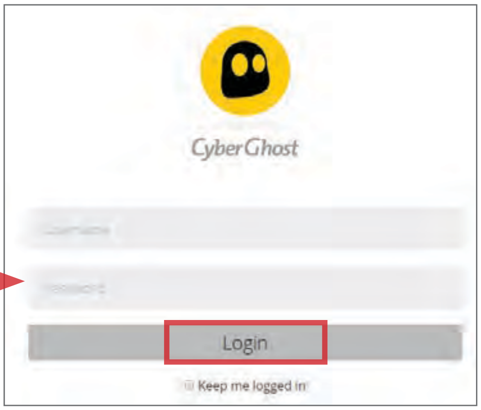
Your Password:

Password

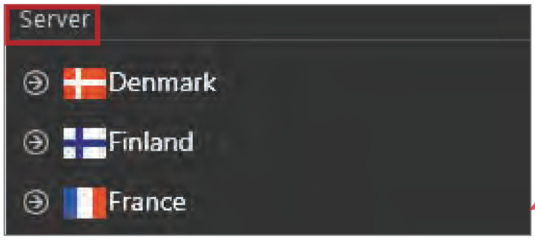
2 Download and install the selected VPN program. If you are using a mobile device, locate the app in the App Store or Google Play Store.



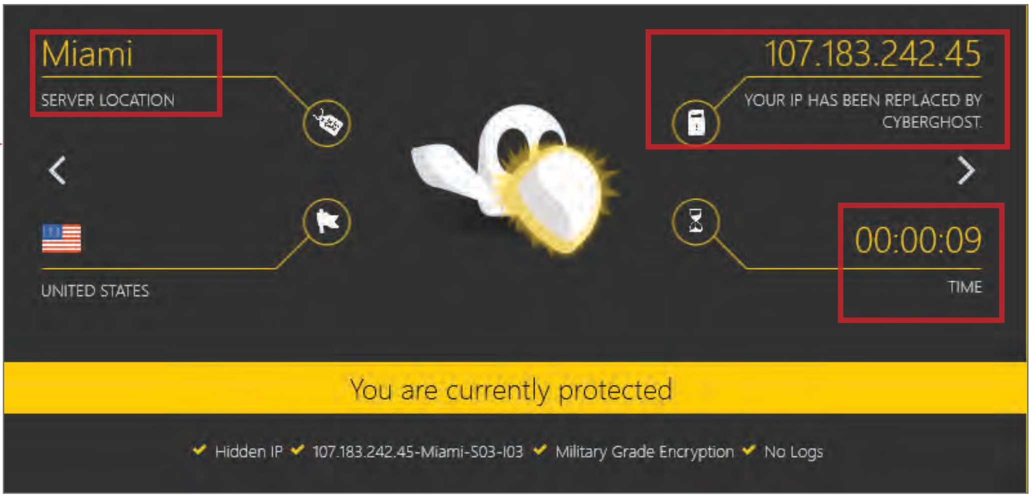
3 Open the program on your device and sign in. VPNs can be run indefinitely, however if you logout of the program or shutdown your device, you will need to login again.



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.



Miami
SERVER LOCATION

107.183.242.45
YOUR IP HAS BEEN REPLACED BY CYBERGHOST.

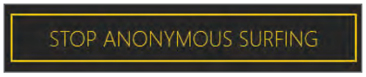
UNITED STATES

00:00:09
TIME

You are currently protected

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

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.



WINDOWS 10

WINDOWS 10 - DO'S AND DON'TS

- Don't use Windows 10 without adjusting the default factory settings; they are set to maximize data collection across all Microsoft apps and programs.
- Review and adjust Cortana's default privacy setting before the first use to prevent Microsoft from collecting any gratuitous personal data.
- Don't approve any suggested system updates or "Express Settings" without reviewing the Terms of Service (ToS).
- 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 apps, and web browsers to are up-to-date and functional.

OVERVIEW

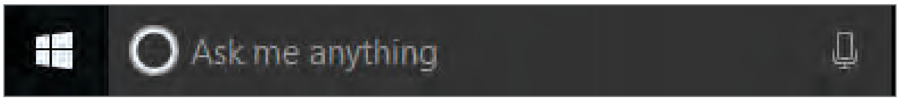
Windows 10 comes with many new additions: a new browser, a varied login protocol, a digital assistant, and a list of default settings that collect and send usage data to Microsoft. These new user-friendly features create additional risks for your personally identifiable information (PII). The programs in Windows 10 are more interconnected than before and require new sets of user data and input to function, such as additional account fields, access to the lock screen, and the user's contacts list. This means Windows 10 is collecting and using personal data in new ways compared to its previous iterations. Follow the recommended settings in this chapter to avoid sharing an unnecessary amount of personal information with Microsoft.

CORTANA - WINDOWS' INTELLIGENT PERSONAL ASSISTANT

Cortana is a voice-enabled intelligent personal assistant created by Microsoft. When used, Cortana is able to assist you in searching the web, creating alarms, managing your contacts, and writing emails and messages.

In order to function at full capacity, Cortana must access your Microsoft email address, geolocation data, microphone, calendar, and metadata, and connect with your computer settings. Using Cortana with the default factory settings will leave your PII exposed. If you choose to use Cortana, follow these recommended settings to maximize your privacy:

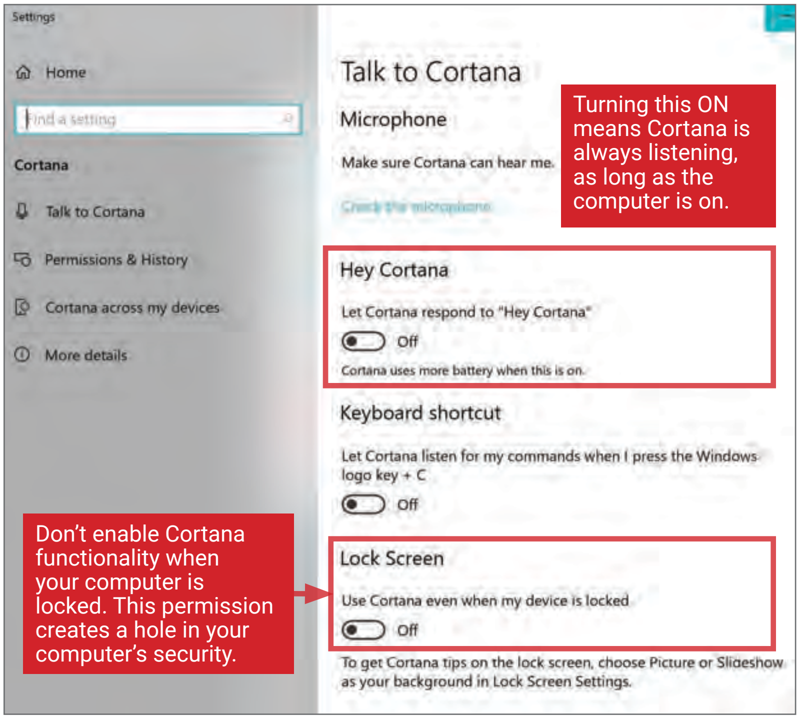
1 Access Cortana at the bottom left of your computer screen. It will appear as a search box or as the circle icon depending on your view settings.



2 From the Options menu, click on **Start Menu > Settings > Cortana**. Click through each entry on the settings bar to review the settings pertaining to Cortana.

3 We recommend that you **disable Cortana** during most normal usage scenarios. Enable Cortana only if you wish to access your microphone and use voice recognition as needed in special use cases.

4 Connecting your Windows-enabled devices allows you to share tasks, web browsers, and apps across multiple devices. It also syncs your data and exposes voice commands collected through Cortana. Set notifications to **OFF**.



Talk to Cortana

Microphone

Make sure Cortana can hear me.

Check the microphone

Turning this ON means Cortana is always listening, as long as 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

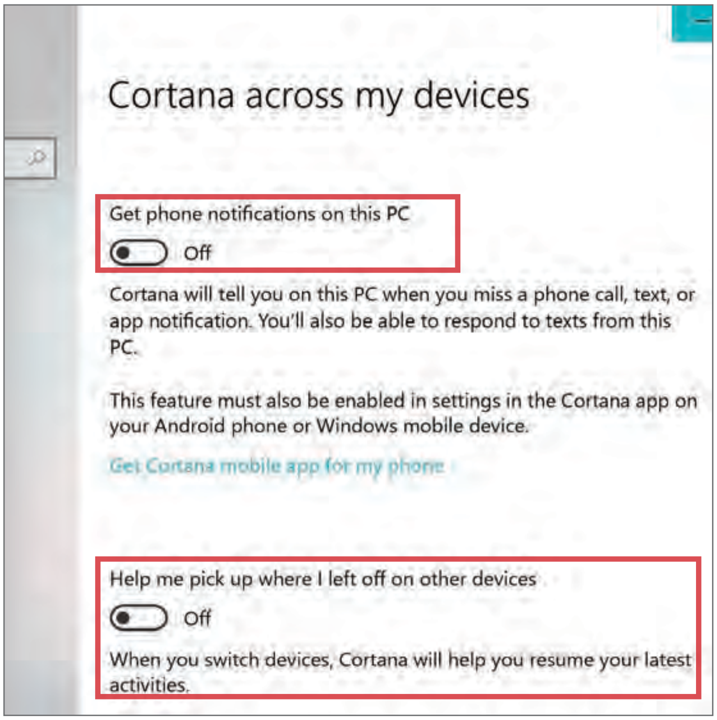
Lock Screen

Use Cortana even when my device is locked

Off

To get Cortana tips on the lock screen, choose Picture or Slideshow as your background in Lock Screen Settings.

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



Cortana across my devices

Get phone notifications on this PC

Off

Cortana will tell you on this PC when you miss a phone call, text, or app notification. You'll also be able to respond to texts from this PC.

This feature must also be enabled in settings in the Cortana app on your Android phone or Windows mobile device.

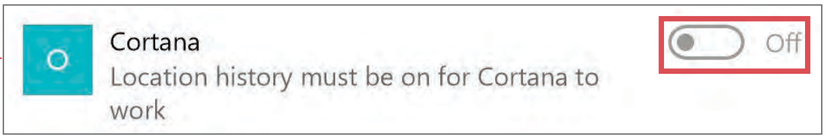
Get Cortana mobile app for my phone

Help me pick up where I left off on other devices

Off

When you switch devices, Cortana will help you resume your latest activities.

5 After adjusting Cortana settings, go to **Windows Settings > Privacy > App permissions** to ensure that Cortana's access to your data (including **Location**) is disabled.



Cortana

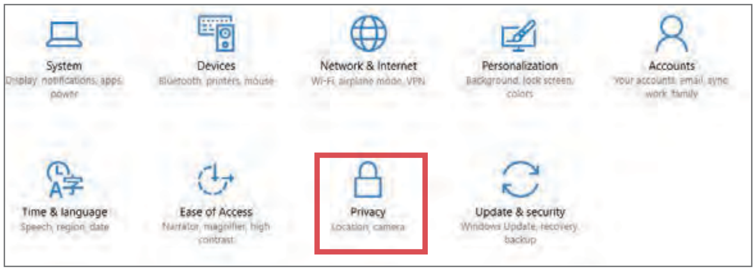
Location history must be on for Cortana to work

Off

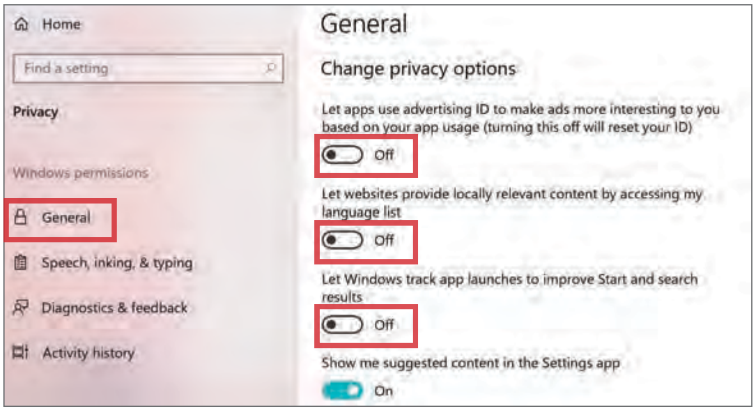
ADJUSTING WINDOWS 10 PRIVACY SETTING

Managing the privacy settings on Windows 10 is the only way to control what information is being 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 **Start Menu > Settings > Privacy**.


System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your accounts, email, sync, work, family
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

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



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

Off

Let websites provide locally relevant content by accessing my language list

Off

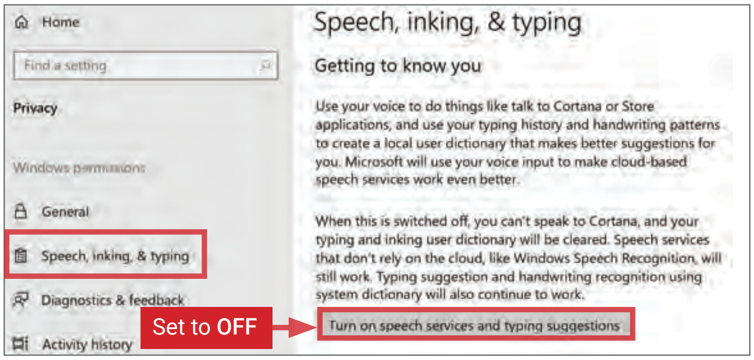
Let Windows track app launches to improve Start and search results

Off

Show me suggested content in the Settings app

On

3 Under **Privacy > Speech, inking, & typing** ensure speech services and typing suggestions are turned **OFF** to prevent the collection of voice, typing, and touch interface patterns.



Speech, inking, & typing

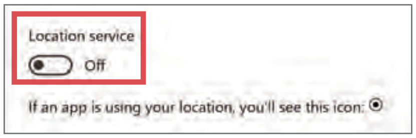
Getting to know you

Use your voice to do things like talk to Cortana or Store applications, and use your typing history and handwriting patterns to create a local user dictionary that makes better suggestions for you. Microsoft will use your voice input to make cloud-based speech services work even better.

When this is switched off, you can't speak to Cortana, and your typing and inking user dictionary will be cleared. Speech services that don't rely on the cloud, like Windows Speech Recognition, will still work. Typing suggestion and handwriting recognition using system dictionary will also continue to work.

Turn on speech services and typing suggestions

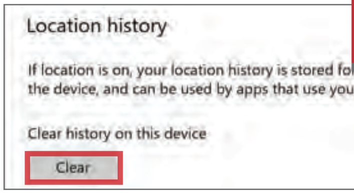
4 Microsoft automatically enables numerous categories of app permissions, including access to your device camera, microphone, location, and your account information. Examine each category listed under **Privacy > App permissions** in detail. When in doubt, toggle **OFF** all access permissions that are not essential to your device usage. For example, turn **OFF** all general settings under **Location** and limit the number of apps that have access to your location data to only essentials (e.g., Maps)



Location service

Off

If an app is using your location, you'll see this icon: ⦿



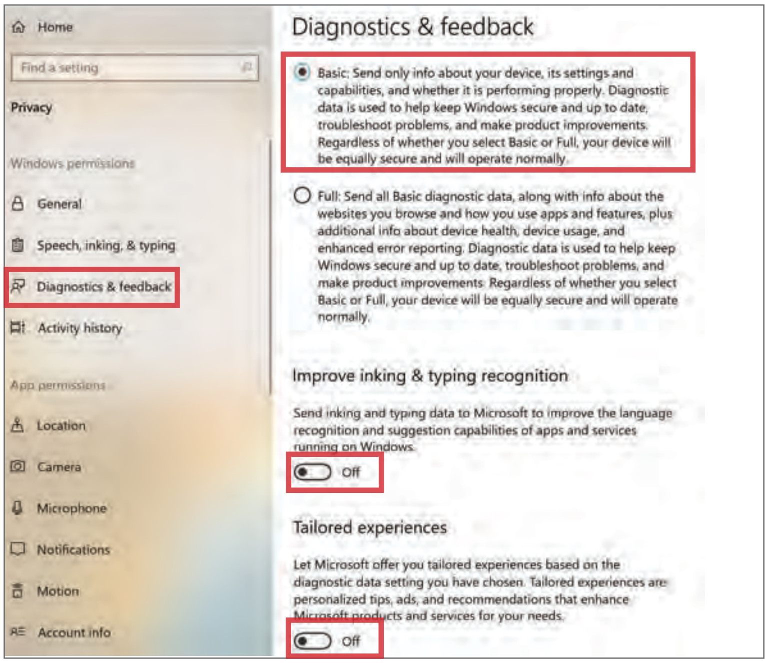
Location history

If location is on, your location history is stored for a limited time on the device, and can be used by apps that use your location

Clear history on this device

Clear

5 Under **Privacy > Diagnostics & feedback**, opt to send only **Basic** device information to Microsoft. Toggle **OFF** Improve inking & typing recognition and Tailored experiences.



Diagnostics & feedback

● Basic: Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

○ Full: Send all Basic diagnostic data, along with info about the websites you browse and how you use apps and features, plus additional info about device health, device usage, and enhanced error reporting. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of whether you select Basic or Full, your device will be equally secure and will operate normally.

Improve inking & typing recognition

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

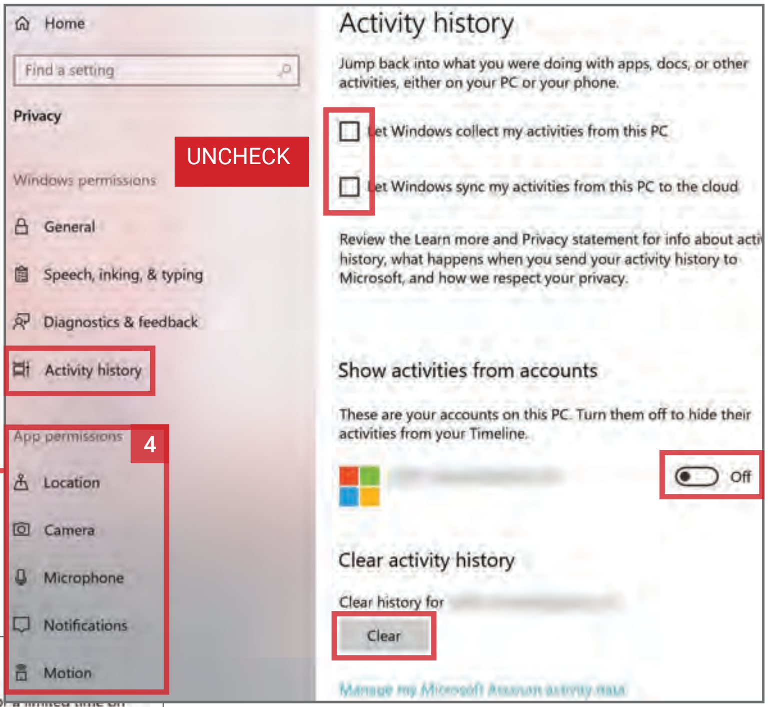
Off

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

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



Activity history

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

□ 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 acti 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.

[redacted] Off

Clear activity history

Clear history for [redacted]

Clear

Manage my Microsoft Account activity data

INDEX

NOTES

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA