

UNCLASSIFIED

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE
COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS
SEVENTH EDITION, SEPTEMBER 2018



BROUGHT TO YOU BY:



U.S. DEPARTMENT OF DEFENSE

UNCLASSIFIED

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT

Constant connectivity is a necessity in today's fast-paced, interconnected world. In 2018, a large portion of your daily activities takes place digitally on websites, mobile apps, smart devices, and social networks, all of which collect and distribute your personal information. Personally identifiable data doesn't just refer to traditional markers, such as name and date of birth, but also includes your behavioral patterns, purchasing histories, and connections. In your daily interaction with devices, sensors, and services, you are sharing traces of your identity in exchange for convenience, enjoyment, and consumer goods. This vast and ever-growing network of identity data and habits constructs your singular and unique online identity.

Without knowing how your identity data is collected, who is collecting it, and where it can end up, safeguarding your information becomes difficult. Fortunately, by using the recommendations presented in this guide, you can learn to better protect yourself, your friends, and your family online by becoming a more informed user.



The Anatomy of Your Online Identity: What Footprints Do You Leave?

TABLE OF CONTENTS

1. FACEBOOK.....	2
2. FACEBOOK MOBILE	4
3. TWITTER.....	6
4. INSTAGRAM.....	8
5. LINKEDIN.....	10
6. GOOGLE+.....	12
7. PHOTO SHARING SERVICES.....	14
8. ONLINE DATING SERVICES.....	16
9. MOBILE DATING APPS.....	18
10. SECURE CHAT APPS.....	20
11. SMARTPHONES.....	22
12. TRAVELING SAFELY WITH SMARTPHONES.....	24
13. EXIF DATA REMOVAL.....	26
14. MOBILE WALLETS.....	28
15. HEALTH APPS & FITNESS TRACKERS.....	30
16. SECURING YOUR HOME WIRELESS NETWORK.....	32
17. ONLINE REGISTRATION.....	34
18. OPTING OUT OF DATA AGGREGATORS.....	36
19. IDENTITY THEFT PREVENTION.....	38
20. KEEPING YOUR KIDS SAFE ONLINE.....	40
21. VOICE OVER INTERNET PROTOCOL (VOIP).....	42
22. VIRTUAL PRIVATE NETWORK (VPN).....	44
23. WINDOWS 10.....	46
INDEX.....	48

USEFUL LINKS AND RESOURCES

- | | |
|---------------------------------------|---|
| • IdentityTheft.gov (by the FTC) | https://www.identitytheft.gov/ |
| • A Parent's Guide to Internet Safety | http://www.fbi.gov/stats-services/publications/parent-guide |
| • The Balance: Identity Theft 101 | https://www.thebalance.com/identity-theft-basics-4073614 |
| • Protect My ID | http://www.protectmyid.com/identity-theft-protection-resources |
| • 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.



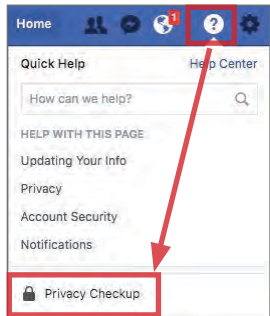
SOCIAL NETWORK - DO'S AND DON'TS

- 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 that your family takes 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.

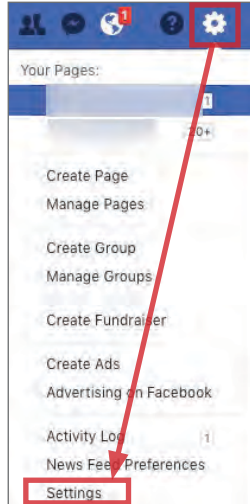
MAXIMIZING YOUR FACEBOOK PRIVACY

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.

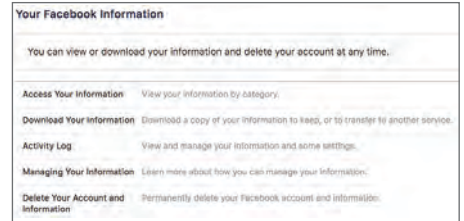


For more extensive and granular control, navigate to **Settings** from the top drop down menu. Click through each tab to control how your personal information is shared with others.



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

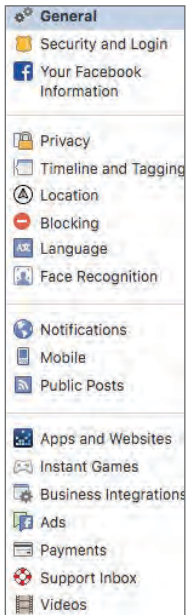
This tab contains shortcuts to your **Activity Log** and an informative **Managing Your Information** tab that guides you through common Facebook and Instagram data management questions and concerns.



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

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Close Friends	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
	Who sees tag suggestions when photos that look like you are uploaded?	No One	Edit
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review what other people see on your timeline	View As	
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

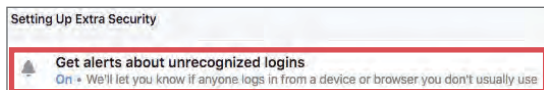
RECOMMENDED SETTINGS



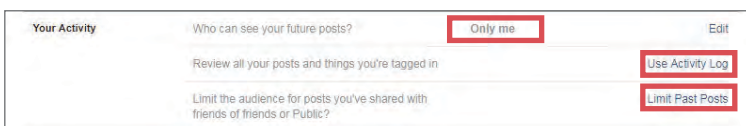
The (1) **Security and Login**, (2) **Privacy**, (3) **Your Facebook Information**, (4) **Timeline and Tagging**, (5) **Location**, (6) **Face Recognition**, (7) **Public Posts**, (8) **Ads** and (9) **Apps and Websites**, tabs contain settings for protecting personal information. Use the settings displayed 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.

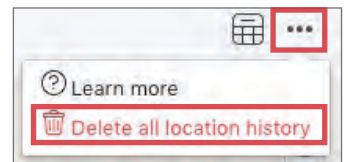
- 1 The **Security and Login** tab contains settings to protect your login credentials, monitor attempted and successful logins, and recover your account in the event of a lockout. Use **Where You're Logged in** to monitor login activity and end inactive sessions, and **turn ON** alerts for unauthorized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



- 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.



- 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.

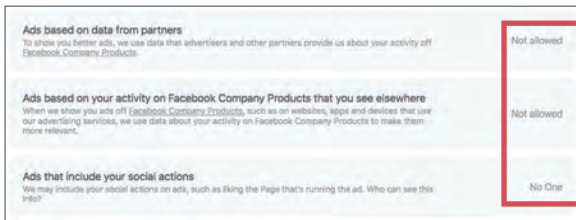


- 7 Followers are people outside your "Friends" network who interact with content you share publicly. Your **Public Posts** are streamed on their News Feeds. To prevent this, set **Who Can Follow Me** to **Friends**. Restrict **Public Post** and **Public Profile** settings as shown.

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.	Friends	
	Each time you post, you choose which audience you want to share with.		
	Learn more.		
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**.



- 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.



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.

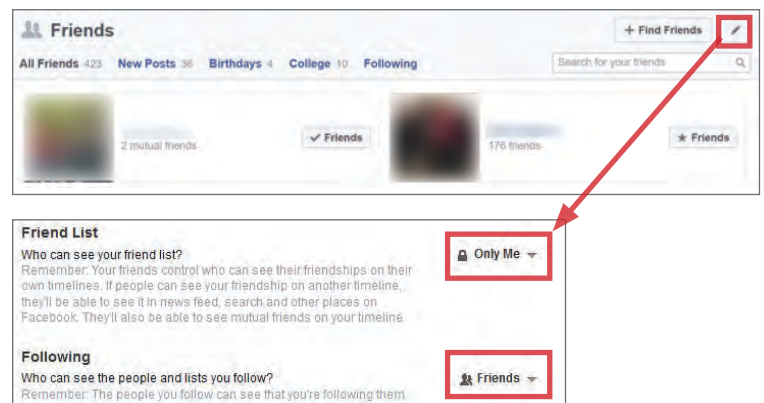
ABOUT

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**.



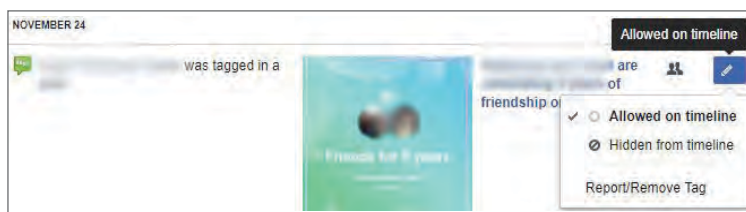
FRIENDS

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**.



ACTIVITY LOG

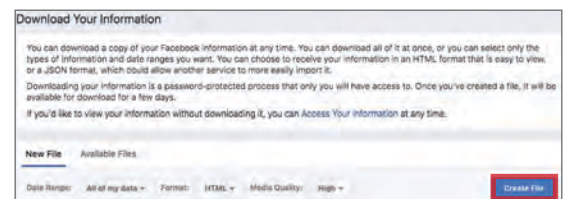
The **Activity Log** tool chronologically displays your **Posts**, **Posts You're Tagged in**, and **Others' Posts To Your Timeline**. Use the dropdown menu shown to delete or manage how individual posts appear on your Timeline.



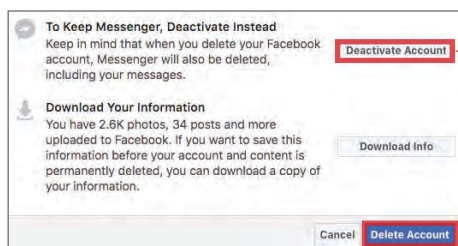
REVIEWING YOUR INFORMATION

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.



DEACTIVATING/DELETING YOUR FACEBOOK 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.



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 that your family takes 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 1.47 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 provides 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 at the bottom panel, select **Settings & Privacy > Settings**. Navigate tabs within the **Security**, **Privacy**, and **Ads** sections to implement settings shown below.

Security and Login

- Review your active sessions and devices frequently to spot unauthorized activity** (points to 'Where you're logged in')
- Turn ON "two-factor authentication"** (points to 'Use two-factor authentication')
- Turn ON** (points to 'Get alerts about unrecognized logins')

Privacy Settings

- 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
- 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

- Ad Preferences** (points to 'Ad Preferences')
- Privacy Settings** (points to 'Privacy Settings')
- Active Status** (points to 'Active Status')

About you

- Ad Preferences > Your Information** (points to 'Ad Preferences')
- Toggle all "OFF"** (points to 'Relationship status', 'Employer', 'Job title', 'Education')
- Toggle OFF in both Facebook mobile & Messenger (if using) apps to take full effect** (points to 'Show when you're active')

IPHONE SETTINGS

The iPhone's security settings can help to further protect your personal data while you use the Facebook Mobile App. From the iPhone's **Settings** icon, select **Privacy** and navigate through the **Location Services**, **Photos**, and **Facebook** tabs to disable all of the permissions, as seen below.

Settings > Privacy

- Location Services** (points to 'Location Services')
- Photos** (points to 'Photos')
- Facebook** (points to 'Facebook')

Privacy > Location Services

- Never** (points to 'Never')

Privacy > Photos

- Facebook** (points to 'Facebook')

Privacy > Facebook

- Photos** (points to 'Photos')
- Notifications** (points to 'Notifications')
- Background App Refresh** (points to 'Background App Refresh')
- Cellular Data** (points to 'Cellular Data')

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).

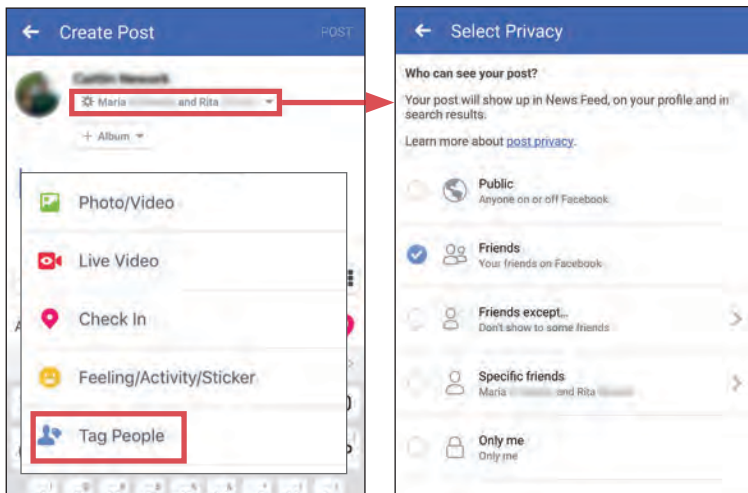
APPLICATION INFO

- Permissions** (points to 'Permissions')

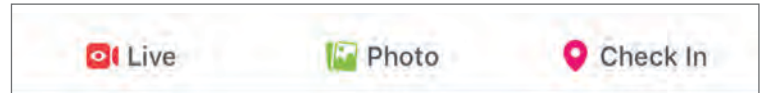
APP PERMISSIONS

- Facebook** (points to 'Facebook')
- Toggle all OFF** (points to 'Calendar', 'Camera', 'Contacts', 'Location', 'Microphone', 'Phone', 'SMS', 'Storage')

POSTING TO FACEBOOK



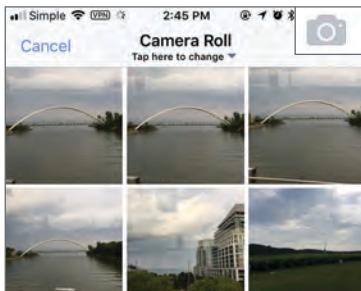
Facebook Mobile allows you to post a new status, upload photos, or check in to locations using the **What's on your mind?** prompt. The icons highlighted on the update prompt are shortcuts for adding further personal information to each post. Several shortcuts pose a significant risk to your privacy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



SELECTING YOUR PRIVACY

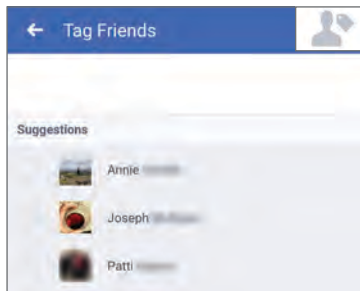
With every post, Facebook Mobile allows you to select the audience through the **Select Privacy** tab beneath your name. For maximum privacy, select **Specific friends** with whom you would like to share your post. Never make your posts available to the public.

ADD PHOTOS



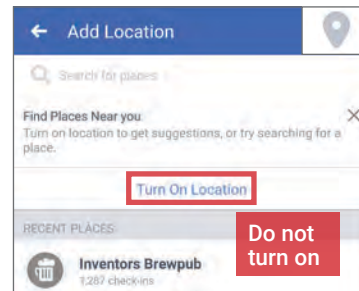
Avoid posting photos to your Timeline. These photos can often be viewed from your contacts' profile pages and can be saved without your knowledge or consent.

TAG FRIENDS



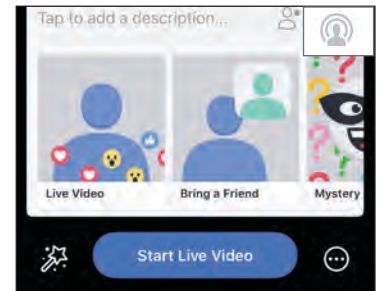
Tagging friends in individual posts extends the visibility of your post and profile to your friends' networks. Limit the number of tags you add to your Facebook posts.

ADD LOCATION



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.

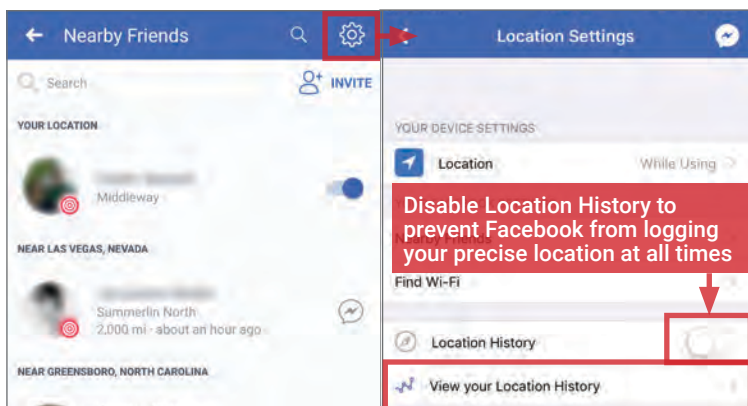
LIVE VIDEO BROADCAST



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

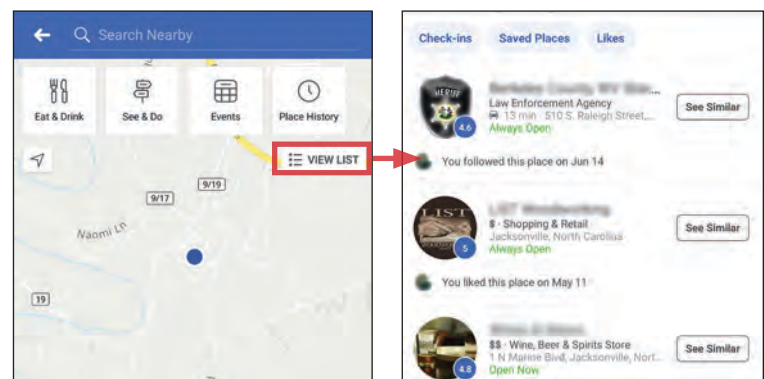
Nearby Friends allows you to share your location with friends. When activated, Facebook collects your location data, even while you are not using the app, and continually broadcasts your approximate locations to your friends. You also have the option to allow certain users to see your precise location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



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.



SOCIAL NETWORK - DO'S AND DON'TS

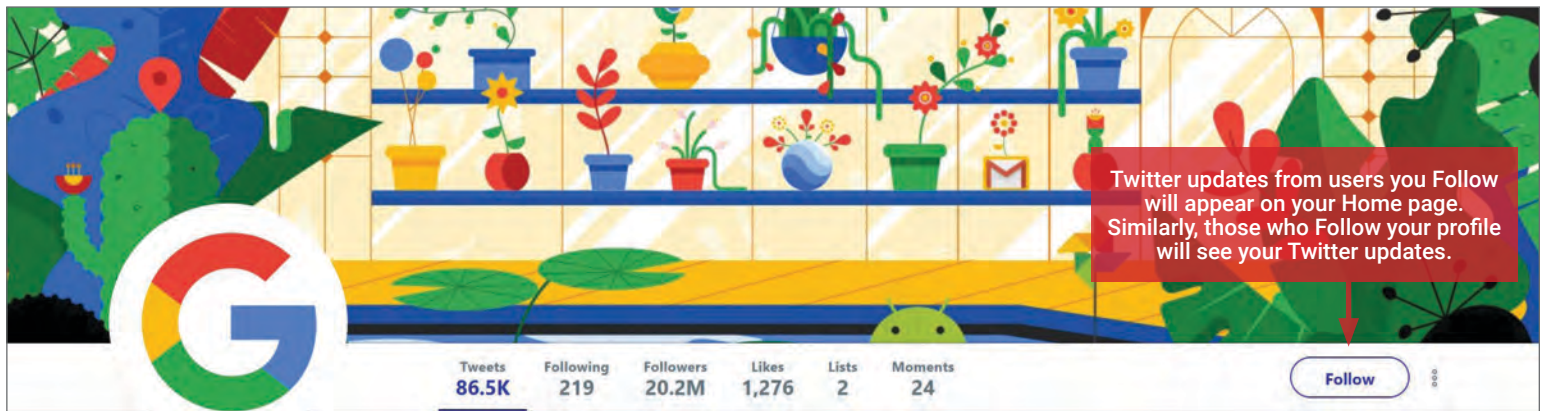
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
- Ensure that your family takes similar precautions with 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 327 million monthly active users, as of early 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.

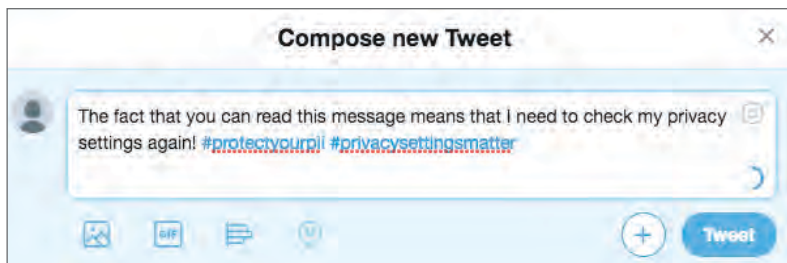
TWITTER PROFILES

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.



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.

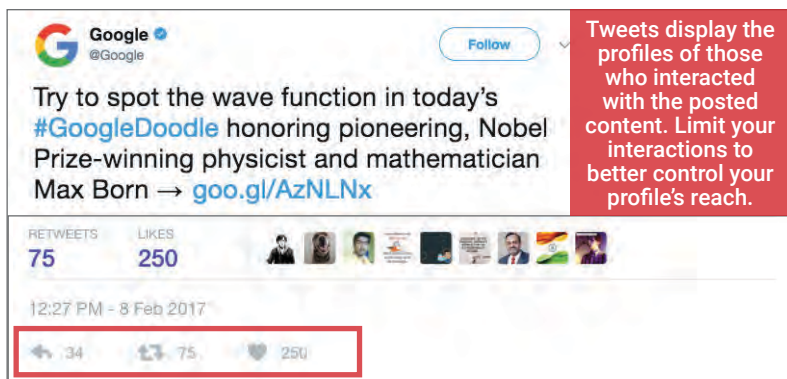


Mentions (@username) are used to tag other users or accounts in a Twitter update. Tags create a link to the mentioned individual's profile. When a public user mentions a private Twitter account, the link to the profile of the private account becomes visible to the public.

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 **Uncheck both**
☐ Let others find me by my phone number
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 ☐ **Personalize ads** **Uncheck both**
If selected, you will see interest-based ads. [Learn more](#)

☐ **Personalize based on your apps**
If selected, Twitter will view and store the apps on your devices to help show you more relevant content. Twitter won't see any data from within the apps. [Learn more](#)

☒ **Personalize across all your devices** **Check**
Twitter will always personalize across the devices you've used to log in. If you disable this setting, Twitter will forget that you've used other devices. [Learn more](#)

☐ **Personalize based on the places you've been** **Uncheck all**
Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. This setting lets Twitter personalize 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 data through select partnerships**

Go to "Personalization and Data" > "Edit"

EMAIL NOTIFICATIONS

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

Email is enabled. [Turn off](#)

Thanks, your notification settings have been saved.

Activity related to you and your Tweets

Email me when ☒ I have new notifications. [Learn more](#)
☒ I'm sent a direct message
☒ Someone emails a Tweet to me **Check all**

Activity from your network **Uncheck all**

Email me with ☐ Top Tweets and Stories
Sent periodically \updownarrow
☐ Updates about the performance of my Tweets

Updates from Twitter **Uncheck all**

Email me with ☐ News about Twitter product and feature updates
☐ Tips on getting more out of Twitter
☐ Things I missed since I last logged into Twitter
☐ News about Twitter on partner products and other third party

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

Email
Email will not be publicly displayed. [Learn more](#)

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.
[Save changes](#)

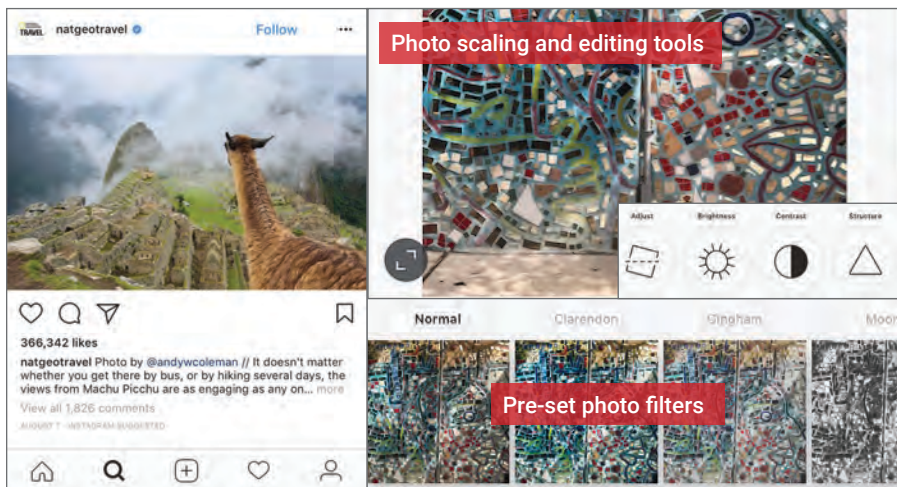
Deactivate your account



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 that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images 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.
- Don't embed your posts with hashtags (e.g., #foodie, #saturday), as hashtags increase your posts' visibility and make them searchable by others.
- Remember that even if you restrict your data from public view, Instagram still has access to your data and may share it with third-parties.

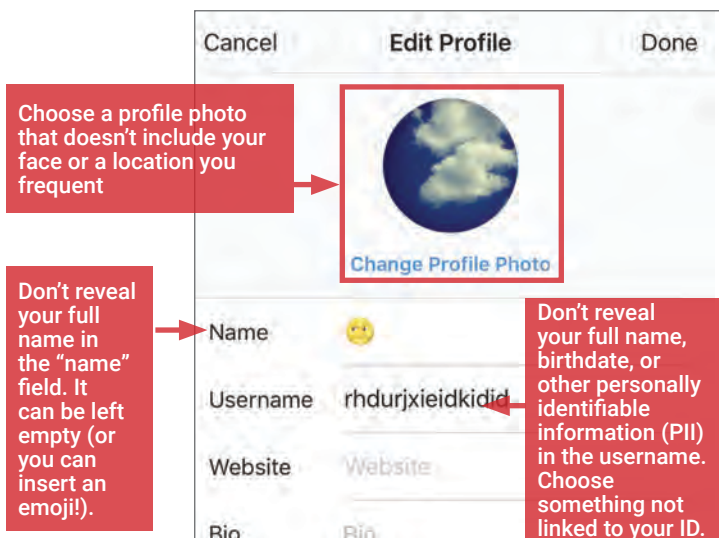
OVERVIEW



Instagram is a photo-sharing 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.**

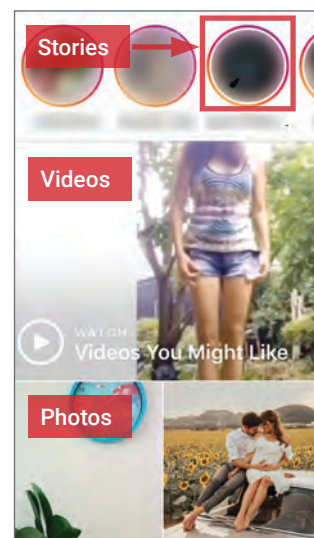
MANAGING YOUR INSTAGRAM PROFILE



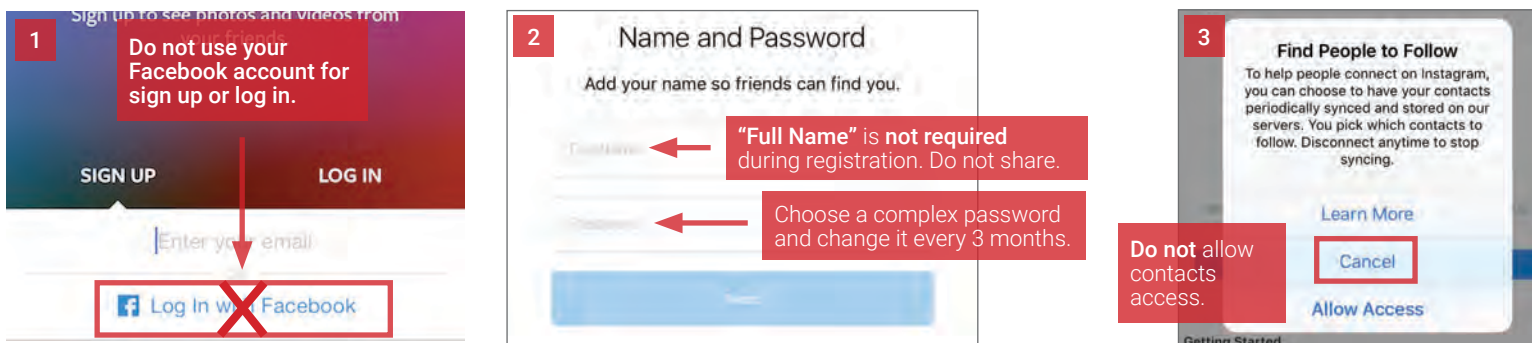
INSTAGRAM MEDIA FORMATS

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).

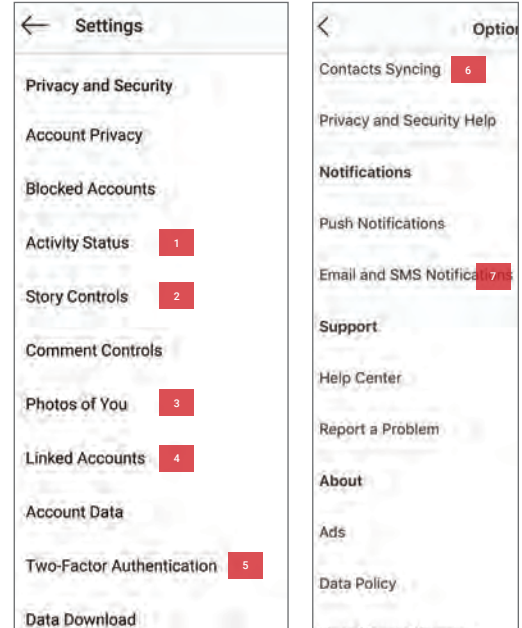
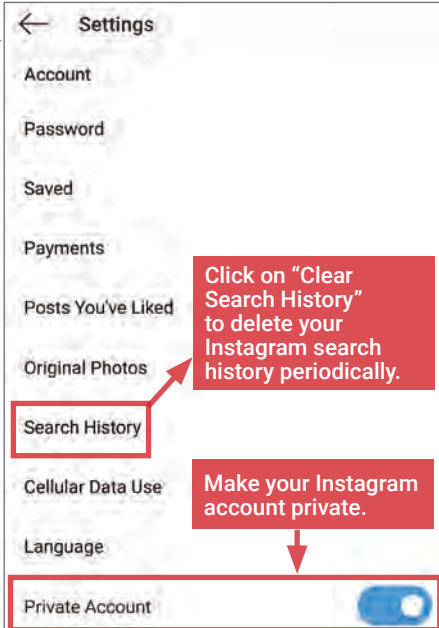


ACCOUNT REGISTRATION - PRIVACY TIPS



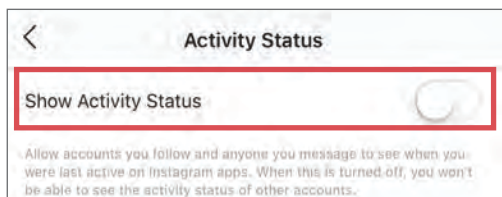
PRIVACY SETTINGS

To access your privacy settings, go to your **Profile** and tap  (iOS) or  (Android) 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.



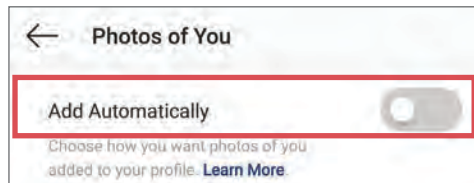
1 ACTIVITY STATUS

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

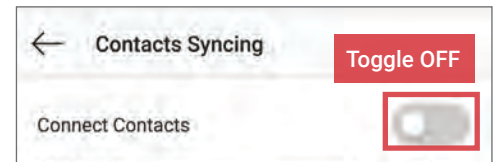


3 PHOTOS OF YOU

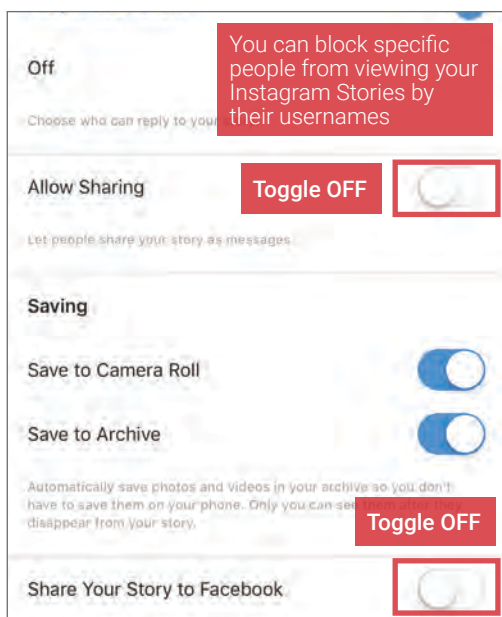
Toggle OFF "Add Automatically" to review when others tag you in photos before they are added automatically to your Instagram profile.



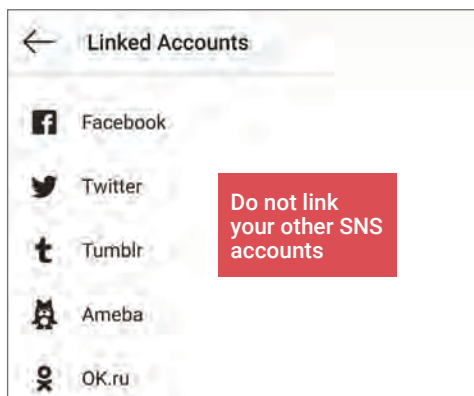
6 CONTACTS SYNCING



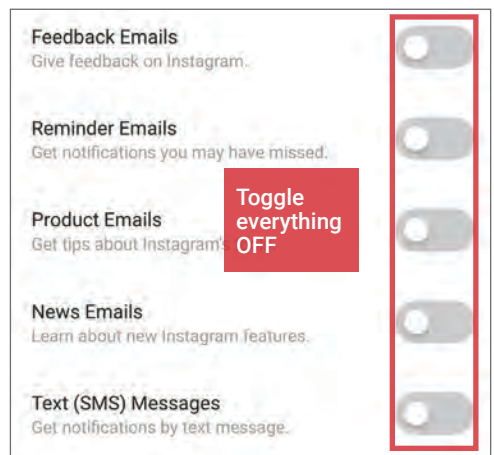
2 STORY CONTROLS



4 LINKED ACCOUNTS



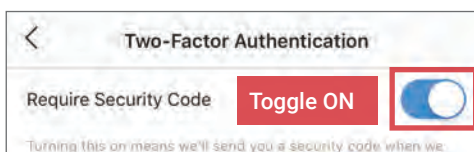
7 EMAIL AND SMS



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.

5 2-FACTOR AUTHENTICATION



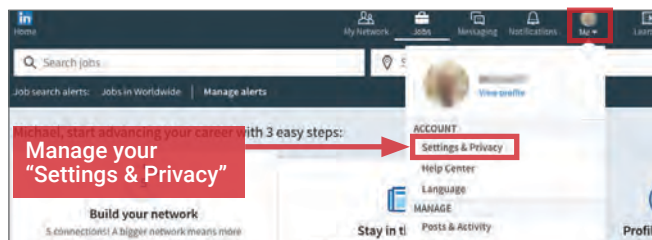


SOCIAL NETWORK - DO'S AND DON'TS

- 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 that your family takes 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.

MANAGING YOUR LINKEDIN PRESENCE

LinkedIn is a professional networking service that allows you to establish connections with coworkers, customers, business contacts, and potential employees or employers. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar backgrounds. You can also post and share your professional skills, personal interests, and hobbies. Follow the recommended settings to limit the exposure of your personally identifiable information (PII) without foregoing LinkedIn's many useful features.



PROFILE 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.

Profile privacy

Edit your public profile

Choose how your profile appears to non-logged in members via search engines or permitted services

1 Change

Manage active status

Choose who can see when you are on LinkedIn

Change

Who can see your connections

Choose who can see your list of connections

Set to "Only you" Only you

Viewers of this profile also viewed

Choose whether or not this feature appears when people view your profile

Set to "No" No

Sharing profile edits

Choose whether your network is notified about profile changes

Set to "No" No

Profile viewing options

Choose whether you're visible or viewing in private mode

2 Full profile

Notifying connections when you're in the news

Choose whether we notify people in your network that you've been mentioned in an article or blog post

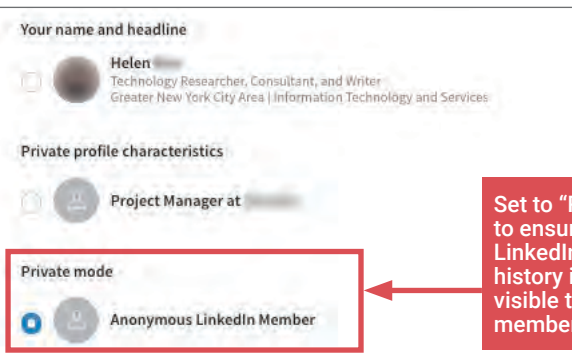
Set to "No" No

Who can see your last name

Choose how you want your name to appear

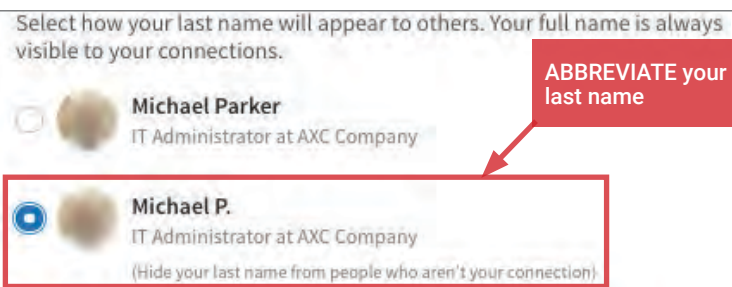
3 Full

2 PROFILE VIEWING OPTIONS



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

3 WHO CAN SEE YOUR LAST NAME



ABBREVIATE your last name

1 EDITING YOUR PUBLIC PROFILE

Your profile's public visibility

Off

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.

Uncheck all optional fields

LINKEDIN QUICK FACTS

- There are more than 500 million LinkedIn users around the world (as of Jan 2018). The service is widely adopted in the United States, India, Canada, and the United Kingdom.
- 40% of users visit LinkedIn daily. An average user spends about 17 minutes monthly on LinkedIn.
- Users tend to share information related to their careers or jobs as opposed to photos or text referencing social events, as is common in other SNS.
- Compared to free accounts, Premium LinkedIn accounts have access to more information about other users who viewed their profiles.

DATA PRIVACY AND ADVERTISING SETTINGS

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 > Data Privacy and Advertising**.

Data privacy and advertising

Manage who can discover your profile from your email address
Choose who can discover your profile if they have your email address. **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. **Set to "Nobody"**

Salary data on LinkedIn
See and delete your salary data. **Change**

Representing your organization
Choose if we can show your profile information on your employer's pages. **Set to "No"**

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

Microsoft Word
Choose whether work experience descriptions from your LinkedIn profile can be shown in Resume Assistant, a feature within Microsoft Word. **Change**

Advertising preferences
Choose whether LinkedIn can serve interest-based advertising through our platform for services.
LinkedIn may serve interest-based advertising through its platform for third parties.
Your change may take 24 hours to become effective, and afterwards, you may continue to see (1) ads that are personalized but are not interest-based advertising and (2) opt-out options in ads. **Do not let LinkedIn share your data with 3rd-party advertisers**

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 Third parties

Permitted Services
View services you've authorized and manage data sharing. **4 connected apps**

These are applications and other services to which you have granted access to your LinkedIn profile and network data. If you remove that access here, they will no longer be able to access your LinkedIn data. To re-enable them in the future, go to the application and grant access again.

Apps and other services you've added

Hootsuite	Remove
LinkedIn Help Center	Remove
LinkedIn Mobile	Remove
OS X Mavericks	Remove

Review this section monthly!

REQUEST DATA ARCHIVE

LinkedIn maintains an archive detailing each user's unique account activity. Navigate to **Settings & Privacy > Account > 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

COMMUNICATIONS SETTINGS

Navigate to **Settings & Privacy > Communications > Basic > Messages from members and partners** and apply these settings to prevent LinkedIn from sharing your data with its partners and to prevent LinkedIn sponsors from sending you targeted messages.

Messages from members and partners
Let us know what type of messages you'd prefer to receive

Allow others to send you InMail?
Yes ☒ No ☐ **Set to "No"**

Allow LinkedIn partners to show you Sponsored InMail?
LinkedIn **Sponsored InMails** are messages from our partners with informational or promotional content that is part of a marketing or hiring campaign. Unless you choose to, your name and e-mail address will not be disclosed to LinkedIn's marketing partners. **Set to "No"**

Navigate to **Settings & Privacy > Communications > LinkedIn messages > Participate in Research** and turn the setting to **No** to prevent LinkedIn from using your activities for internal research purposes.

LinkedIn messages

Participate in research
Choose whether you'd like to receive invitations to participate in research on LinkedIn

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?
Set to "No"

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.

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 that your family takes 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

Google+ is a social networking service (SNS) with approximately 395 million monthly active users. Like other SNS, Google+ provides a platform for users to connect with each other and share content. However, it is unique because your Google+ activities and profile extend into other popular Google products such as Youtube, Google Photos, Maps, and Search. The aggregated data and activities across all Google services create a highly individualized composite view of your online identity. Follow these recommendations to help limit the personal information you share through Google+ and with Google at large.

PROFILE INFORMATION

From your profile, select **About** and use the pencil icon to the right of your profile picture to edit your name (note changes are reflected across all Google products). Use the pencil icon under **Gender, birthday, and more** to edit and manage all profile fields. Mandatory fields, such as gender and birthday should be set to **Private**. Other optional fields can be left blank.

Add info **Optional fields**

Work contact info

Personal contact info

Education

Work history

Places

Sites

Gender, birthday, and more

Gender: Male

Birthday: August 16, 1990

Set to "Private"

Use the highlighted icons to adjust privacy settings, and select the plus sign to reveal additional personal data fields.

FOLLOWERS

Your social network consists of the people you follow and those who follow you. Your followers can see when you post content. Likewise, you are notified when the people you follow post. Your followers can be organized into subgroups, referred to as **Circles**, that help you control who can see your content. Select the **People** tab to manage your circles.

Your circles

Friends 9 people - in "Your circles"

Family empty - in "Your circles"

Acquaintances empty - in "Your circles"

Avoid identifying family members. Limit your followers to the "Friends" or "Following" circles.

POSTING TO GOOGLE+

Google+ allows you to share photos, links, locations, and text entries with others in your circles. Once posted, the entries appear in your personal profile and become visible to others in your default sharing audience. Your followers can interact with the posts as seen in the examples below.

USAJOBS.gov • Public

Have questions about your federal job search? Visit our Help Center!
<https://www.usajobs.gov/help>

USAJOBS Help

Explore Unique Hiring Paths known as a hiring authority you fall under one of the usajobs.gov

Post activities

Michael +1

Lith +1 and reshared

+1 14

Shared publicly

View activity

Viewers have the options to like, comment, or reshare individual posts. When a viewer uses one of these options, a clickable link to their profile appears directly within the post. Limit your use of these features and use the **View Activity** option to review the actions taken with your posts.

- **Likes** - Posted entries appear with a **+1** embedded in the window. Clicking this icon will mark your endorsement of the content (similar to Facebook "likes").
- **Comments** - Users may leave comments on individual posts. These comments are visible to anyone who has access to the post.
- **Reshares** - Users may repost your content to their own profiles. It is important to note that both public and private posts can be reshared by recipients and distributed to new audiences.

Select the **What's new with you?** prompt on the Home page to share a new post. Each post can include up to four different types of content: text, photos, links, and locations. Avoid sharing links to your other social media profiles, photos that clearly show your face, and any of your frequented locations, which may lead to unintended dissemination of your personally identifiable information.

Use the icons (highlighted in the image to the left) to disable reshares and set the appropriate audience settings. Available audience settings include **Public**, **Circles**, and **People**.

Lloyd **Friends**

What's new with you?

Disable comments

Disable reshares

AUDIENCE	WHO CAN SEE YOUR POST?	PRIVACY STRENGTH
Public	Anyone	Weak or None
Circles	All of the individuals within the specified circles	Intermediate
People	Designated individuals from your followers list	Strong

GOOGLE+ PROFILE SETTINGS

Google offers extensive settings to secure your Google accounts. To locate the settings unique to your Google+ profile, select **Settings** from the banner on the left side of your profile. Apply the following options to increase your profile's security and limit the reach of your personal data.

CIRCLES - HOW YOU SHARE ON GOOGLE+

A **Circle** is a customizable list of other users who can receive your shared content, and whose content can be streamed on your Google+ Home page. Circles are what you use to organize who sees which content you share on Google. Available sharing levels are: Public, Extended Circles, Circles, Custom, and Only You.

To adjust the default size of your audience, navigate to the top of the **Settings** page under **General**. The three settings under **General** control who can see your profile and interact with your posts by default. Set these options to **"Only You"** or for a more granular control, choose **"Custom"** to create a personalized default audience.

General

Who can send you notifications? **Only You**

[LEARN MORE](#)

Who can comment on your public posts? **Custom**

[LEARN MORE](#)

Who can see your "+1s on posts" activity? **Only You**

Limit audience size using different groups (or Circles) you've created

Circles

- Your Circles ☐
- Family ☒
- Friends ☒
- Work ☐
- Acquaintances ☐

Photos and Videos Shared on Google+

Show locations by default when you share Google+ albums **Turn "OFF"**

[LEARN MORE](#)

Allow viewers to download my photos and videos shared on Google+ **Turn "ON"**

Don't feature my publicly-shared Google+ photos as background images on Google products and services **Turn "ON"**

[LEARN MORE](#)

Profile

Show your Google+ Communities posts on your profile **Turn "OFF"**

[LEARN MORE](#)

Help others discover my profile in search results. **Only you**

[LEARN MORE](#)

Who can see the "people in your circles" section on your profile? **Turn "OFF"**

Show people who have added you to Circles **Turn "OFF"**

Stream

Restrict stream to single column layout on all screen sizes **Turn "OFF"**

Autoplay animated images in the stream (does not apply to Android apps): **On desktop only**

Amount of Trending & Recommended posts to show in stream **None**

Location Sharing

Share your real-time location with people you choose. [LEARN MORE](#)

MANAGE LOCATION SHARING **Never share your location.**

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

Privacy

Your search history helps to find what you're looking for faster through autocomplete.

CLEAR GOOGLE+ SEARCH HISTORY **Periodically delete your search history**

Your Google+ experience is customized to make the product more useful to you.

MANAGE WEB & APP ACTIVITY **Turn "OFF" web & app activity tracking by Google**

Manage Google+ Search history and activity across Google apps

MANAGE GOOGLE ACTIVITY

Web & App Activity (paused)

Use "Manage Google Activity" to review or delete your older entries.

Other

Shared Endorsements **Set to "OFF"**

Target Audience **Off Edit**

TARGET AUDIENCE

The **Target Audience** option under **Settings > Other** controls access to your public profile and content by setting country or age restrictions. Follow the guideline illustrated below to restrict your content from being viewed by specific age groups or countries of interest.

Control access to your content

[LEARN MORE](#) about setting access restrictions for my content

Target Audience: **Custom** **Set to "Custom" to set country restrictions**

Please select the countries and users who should be able to view your content. You are responsible for applying the correct restriction details for your content, in accordance with all relevant laws and policies, and for updating these settings when necessary.

Global settings

Who can view my content: **No one** **Set to "No one"**

Country-specific settings

These country-specific settings override the global settings

North Korea **No one** **ADD**

Type in specific countries to set restrictions here

DELETING YOUR GOOGLE+ PROFILE

Account

DELETE YOUR GOOGLE+ PROFILE

Scroll to the bottom of the Settings page > click on "Delete your Google+ Profile"



PHOTO SHARING SERVICES







UNCLASSIFIED

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 that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images 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

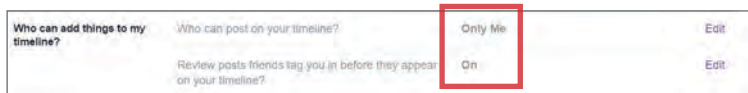
Photo sharing services (PSSs) are online photo albums that store, organize, and share your digital photos; many social networking services (SNSs) such as Facebook and Twitter also function as photo sharing services. PSS provide a convenient way to share photos, but can expose you to privacy risks if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

SERVICE	PRIMARY USE	PRIVACY OPTIONS?	EXIF?	LOCATION OPTIONS	ALLOW REPOSTING?	GOOGLE INDEXED?
	Share photos as posts or albums with SNS connections	Public, Friends of Friends, Friends, Only Me	No	Can tag location to photos; geolocation suggestions	Yes	If Public
	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
	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
	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)
	Share and comment on photos	Public, Private (images are only viewable with a direct URL); albums can be set to Public, or Hidden	No	None (can add location to photo description)	Yes	If Public
	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)

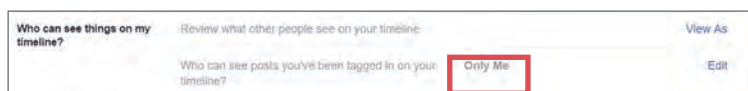
FACEBOOK

Facebook is an SNS with 2 billion active members who upload 700 million photos per day. To maximize your privacy on Facebook, navigate to **Settings > Privacy > Timeline and Tagging** and make the following changes:

- Who can post on your timeline? **Only Me**
- Review posts tag you in before they appear on your timeline? **On**



- Who can see posts you've been tagged in on your timeline? **Only Me**



- Review tags people add to your own posts before they appear? **On**
- When tagged in a post, who do you want to add to the audience that's not already in the audience? **Only Me**
- Who sees tag suggestions? **No One**



For more information, see the Facebook chapter.

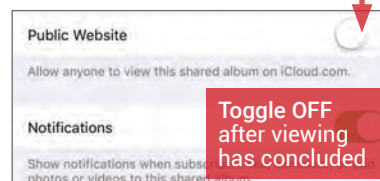
IOS PHOTOS

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 that allows users to create private albums from photos and share with their contacts. To share photos from your Apple device, navigate to **Settings > Photos**:

- iCloud Photo Sharing: **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.



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.28) before sharing them.

UNCLASSIFIED

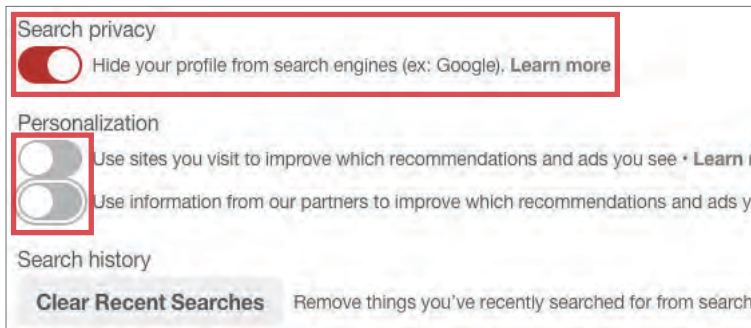
PINTEREST

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 175 million active users. 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:

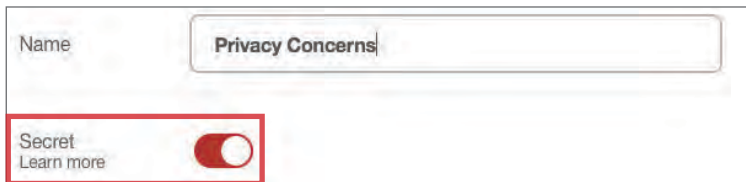
- Under Search privacy, **toggle ON** "Hide your profile from search engines"

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**



When you make a new Board in Pinterest, **toggle** the **Secret boards** option **ON** to keep your pins private.

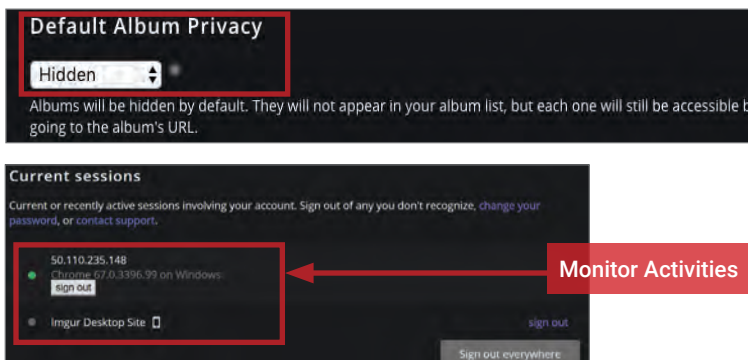


IMGUR

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 100 million users. 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:

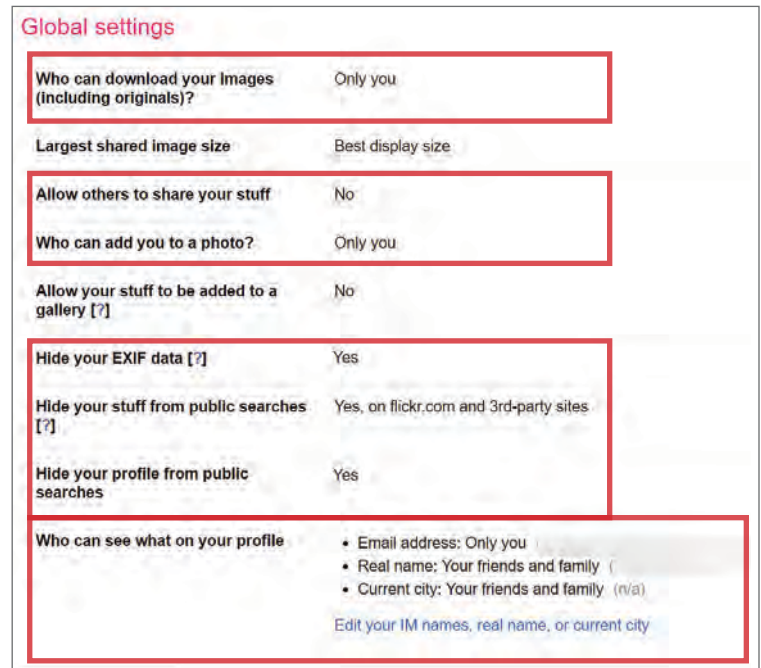
- Default Album Privacy:** Select **Hidden**
- Comment mentions:** check this box to receive notifications when you are mentioned in a comment.
- Use the **Security** tab to review account activity sessions.



FLICKR

Flickr, acquired by SmugMug in April 2018, is a site dedicated to sharing and editing photos. The site has more than 90 million monthly active users. 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**:



To receive a copy of the information Flickr stores about your account, navigate to **Account settings > Personal Information**. Click **Request my Flickr data**. Flickr will email you when your download is ready.

GOOGLE PHOTOS

Google Photos is a photo sharing and storage service with more than 500 million active users. It is the default photo app on Android devices. It is primarily used as a personal photo storage and organizational tool, but it seamlessly connects with Gmail and Google+ and allow photos to be easily shared online via shared 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 and then navigate to **Settings**:

- Go to **Group similar faces** and **turn OFF** face grouping
- Turn ON** **Remove geo location in items shared by link**
- Navigate to **Google Location** and **turn OFF** both **Google Location History** and **Google Location Sharing**





ONLINE DATING SERVICES

UNCLASSIFIED

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 which is used to match compatible individuals, and have only 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
	Name, gender, sexual orientation, email, ZIP code, birthdate, relationship status, biography, photo	Most registration information, optional lifestyle and dating preferences, photos	No questionnaires 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
	First name, gender, sexual orientation, email, ZIP code, country, birthdate, biography, lifestyle questionnaire, photo	First name, most registration information, optional questionnaire answers	Optional questionnaire Login with Facebook; upload photos from Facebook; connect Instagram feed and upload photos	Free to join and send messages; \$10-\$20/month for "A-List" membership, allowing users to see who likes them and who has read their messages
	Gender, sexual orientation, ZIP code, email, country, birthdate, ethnicity, physical description, personal questionnaires, biography, interests, face photo	Most registration information	Optional questionnaires Upload photos from Facebook	Free to join, send messages, and hide profile; \$6-\$13/month to see extended profiles
	Gender, sexual orientation, ZIP code, email, face photo, birthdate, physical description, lifestyle questionnaire, face photo	Most registration information, biography, optional lifestyle and dating preferences	Optional questionnaire Register with Facebook or Google; upload photos from Facebook.	Free to join; \$12-\$20/month to send messages and see profile visitors
	Name, gender, sexual preference, email, ZIP code, country, birthdate, relationship status, children, lifestyle questionnaire, occupation, face photo	All registration information, ethnicity, lifestyle information	Mandatory questionnaire Login with Facebook; upload photos from Facebook	Free to Join; \$12-\$30/month to activate SecureCalls and see profile viewers

UNCLASSIFIED

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.")

- 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

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.



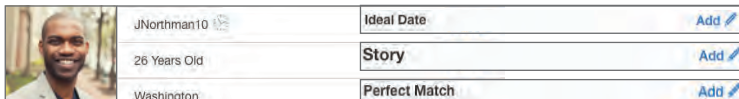
Navigate to **Settings > General** and activate **"Disable auto login links"** to help limit accidentally logging in through email. The questionnaire is optional: submitted answers may be kept private using the lock icon shown.



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

ZOOSK

Zoosk hosts ~3 million unique monthly visitors. 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 user-controlled security settings. Account verification options pose potential threats to privacy, as they require linking phone numbers, videos, or social networks.



When others visit the profile, 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).

MATCH.COM

Match.com hosts ~25 million unique monthly visitors. Free accounts display photos, information submitted during registration, interests, and the traits that users look for in significant others.



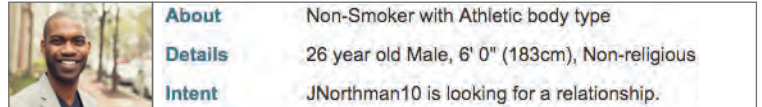
Select **Settings** to toggle profile visibility. Turn the member spotlight off to prevent the profile from appearing in ads. Hidden profiles prevent others from seeing the account but also disable Match.com's matching capability.



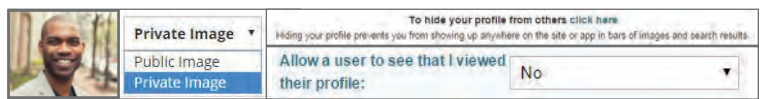
Private Mode is the optimal security setting—your profile is only visible to select people—and is available with a paid subscription. Private Mode permits matching and emailing, and enables a user to see who is interested in or has viewed the profile.

PLENTY OF FISH

Plenty of Fish hosts ~5 million unique monthly visitors. Profiles display the information submitted during registration and the traits that users look for in significant others.



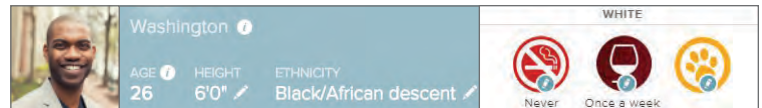
Select **Edit Profile** and elect to hide your profile from others. Hidden profiles do not appear in search results and, unlike other sites, do not lose matching or searching functionality as a result. Select **Upload Images** and set images to private so they can only be shared with individuals via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



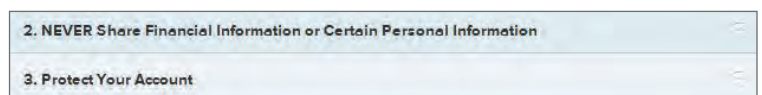
Paid subscriptions do not offer significant security upgrades compared to free accounts. Subscriptions are designed to increase the reach of a profile.

EHARMONY

eHarmony hosts ~2 million unique monthly visitors. Profiles display registration information, excluding photos and questionnaire responses. Other data includes free-text responses addressing the users' interests.



Free eHarmony accounts offer little to no user-controlled privacy settings. Instead, the site determines which data can be seen by others and warns users what types of data may potentially be harmful to share.



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



MOBILE DATING APPS UNCLASSIFIED

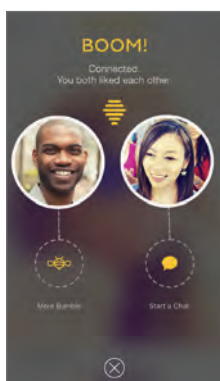
MOBILE DATING APPS - DO'S AND DON'TS

- 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

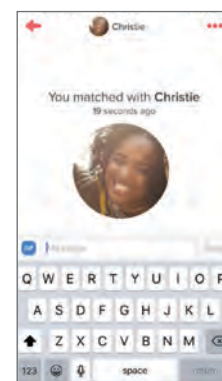
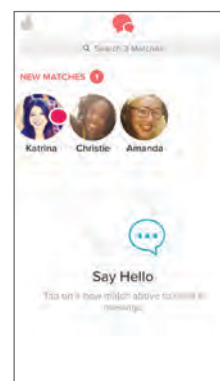
It is estimated that one out of every eight American adults actively uses mobile dating apps as the primary source for discovering romantic connections. As these apps continue to gain traction, users' identity data will be placed at a significantly higher privacy risk. Should you elect to participate 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

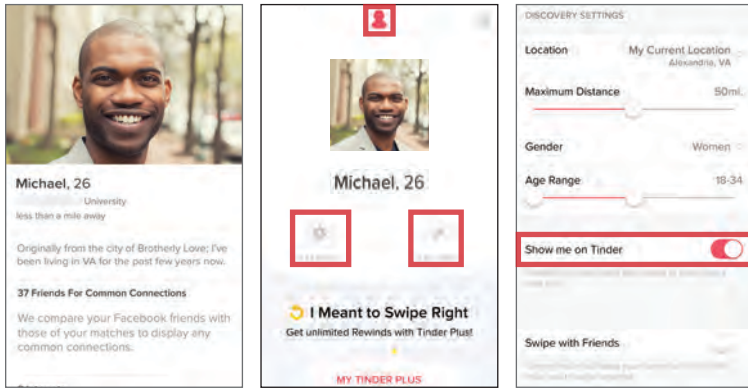
In general, mobile dating apps offer little to no user-controlled privacy settings. As a result, users must show discretion when registering an account and should avoid sharing potentially harmful data. Prior to registering an account, examine the types of data required by each mobile dating app, and 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	OPERATING SYSTEMS	REGISTRATION INFORMATION	VISIBLE PROFILE INFORMATION	APP PERMISSIONS	PRICING
Tinder 	iOS and Android	Phone number verification and Facebook account info: Likes, photos, general info, and relationship interests	Name, photos, age, approximate location, gender, biography, work information, education information, Instagram photos	Location, Cellular Data, & Push Notifications Access to personal Facebook Account	Free to join; up to \$10 / month for an upgraded account (change location, rewind features, disable ads)
Bumble 	iOS and Android	Phone number verification or Facebook account info: Likes, photos, general info, and relationship interests	Name, photos, age, location, biography, work information, education information	Location, Cellular Data, Push Notifications, & Photos Access to personal Facebook Account	Free to join; no paid accounts available
Hinge 	iOS and Android	Facebook account info: Likes, photos, general info, and relationship interests	Name, photos, age, location, biography, height, education information, work information, hometown, religion, interests, number of friends on Hinge, common Facebook friends, dating preferences	Location, Cellular Data & Push Notifications Access to personal Facebook Account	Free to join; no paid accounts available
Coffee Meets Bagel 	iOS and Android	Facebook account info: Likes, photos, general info, and relationship interests	Photos, age, location, height, ethnicity, religion, occupation, employer, education information, mutual friends, biography, lifestyle, and dating preferences	Location, Cellular Data, Push Notifications, Contacts, & Photos Access to personal Facebook Account	Free to join; up to \$25 can be spent on credits ("beans") at a time to view more profiles in a day

UNCLASSIFIED

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.



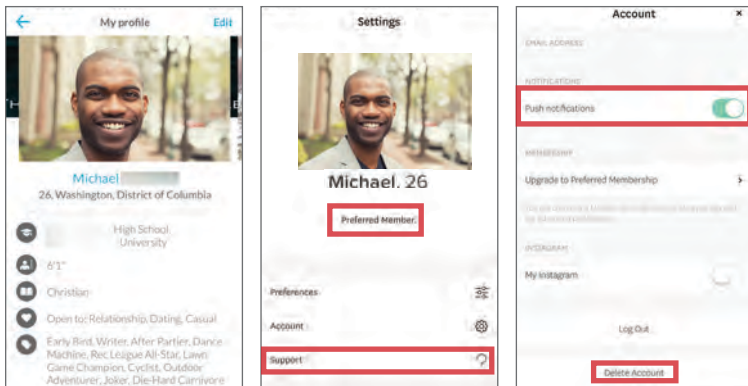
Use: Users may swipe through a limited number of profiles per day. There are no gender-based limitations on who is able to initiate a chat conversation once matched. Matches do not expire and are stored in the app unless they are manually removed by one of the users.

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.

HINGE

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



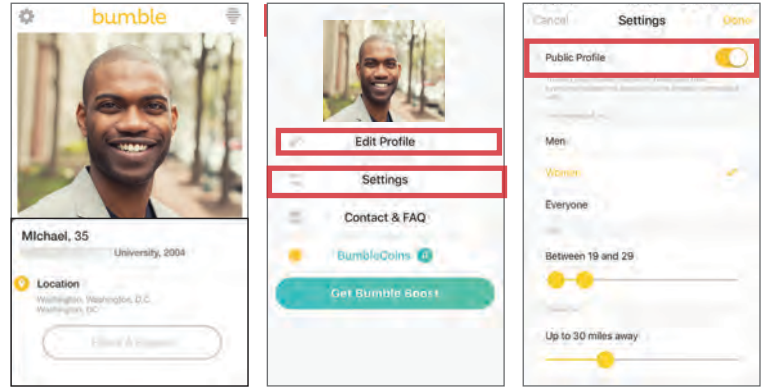
Use: Users may swipe through an unlimited number of profiles per day. There are no gender-based limitations on who is able to initiate chat conversations. Matches expire after 14 days; users can no longer view each others' profiles or communicate through the app without rematching.

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.

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.



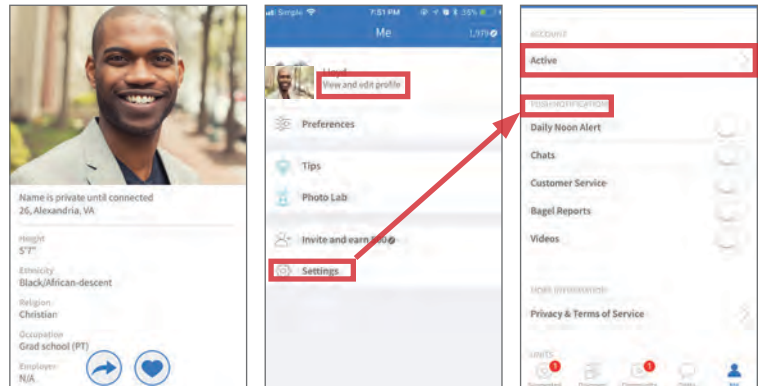
Use: Users may swipe through an unlimited number of profiles per day. Once matched, women are given 24 hours to initiate a conversation. For same-sex connections or friendship settings, either person has 24 hours to make the first move. The match expires if no communication is established.

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. Deactivating **Public Profile** hides your profile from view.

COFFEE MEETS BAGEL

Coffee Meets Bagel matches people who are in similar social circles on Facebook. It also takes into account geolocation, education, physical attributes, and past swiping tendencies to suggest compatible matches.



Use: The app shows users around six compatible matches ("Bagels") per day; these matches can be swiped anonymously. Twenty additional profiles appear under Give & Take; swiping on these profiles is not anonymous. Matches do not expire and there are no gender-based chat limitations.

Profiles: Select **Me > View and edit profile** to change or delete the information displayed in your profile.

Settings: Select **Me > Settings** to enable notifications and set your profile's visibility. Deselecting **Active** membership hides your profile.



SECURE CHAT APPS

UNCLASSIFIED

SECURE CHAT APPS - DO'S AND DON'TS

- Only establish and maintain contact with people you know and trust. Review your contacts often.
- 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 use the app.
- Ensure that your contacts take similar security precautions. Do not accept chat requests from unverified numbers or IDs.

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 when the app is in use: 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. Snapchat, but not the other three services, shares this information 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.

CHOOSING THE RIGHT SECURE CHAT APP

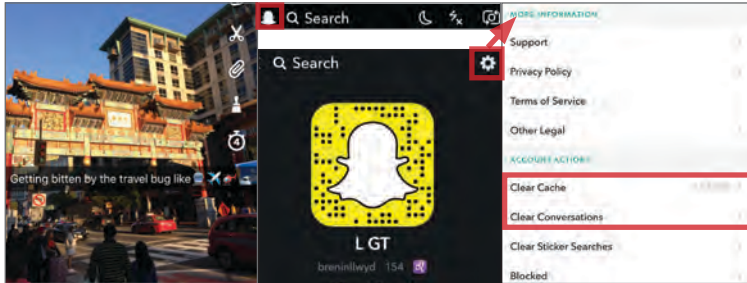
As a whole, secure chat apps afford users enhanced privacy. However, users may place themselves at unwanted risk if they do not take the time to research app capabilities and take proper precautions. Compare the capabilities of the four apps below to determine which may be best suited for your personal use.

SERVICE	COMPATIBILITY	DESCRIPTION	IDENTITY DATA	SECURITY	LINKAGES
Snapchat 	iPhone & Android	Temporary text/photo/video messages known as "Snaps"; money transfers (Square is the processor). US-based.	Sign up: Email address & birthday Optional: Phone number, debit card number, zip code	Potential for anonymity: Messages not encrypted end-to-end Encryption Type: AES/CBC with single synchronous key	Social Networks / Email: None Device / Internet: Address book, camera, microphone, location, cellular data, Wi-Fi
Telegram 	iPhone, iPad, Android, Windows Phone, Mac, Windows PC, Linux Computers	Cloud-based messenger syncs across devices; Secure Chat feature with temporary text messages. Based in Dubai as of April, 2018	Sign up: Phone number Optional: Name & picture	Potential for anonymity: Encrypted messages Encryption Type: MTProto with end-to-end encryption	Social Networks / Email: None Device / Internet: Address book, cellular data, Wi-Fi
WhatsApp 	iPhone, iPad, Android, Mac, Windows PC, Blackberry, Symbian, Web	Call/photo/video/text messages over the Internet and cell networks. US-based.	Sign up: Phone number Optional: Name & picture	Potential for anonymity: Encrypted messages & secure calls Encryption Type: Open Whisper System's Signal Protocol	Social Networks / Email: None Device / Internet: Address book, cellular data, Wi-Fi
Signal 	iPhone, Android, Windows PC & Mac	Encrypted texts/calls/video calls, photo sharing over the Internet and cell networks. US-based.	Sign up: Phone number Optional: Name & picture	Potential for anonymity: Encrypted messages Encryption Type: Open Whisper System's Signal Protocol	Social Networks / Email: None Device / Internet: Address book, cellular data, Wi-Fi

UNCLASSIFIED

SNAPCHAT

Snapchat is an app where users send temporary photo/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. Snapchat also offers a chat feature between users; chats are for one-time viewing only and permanently erased when the recipient exits the window. Snapchat can also securely process payment transfers by way of the Snapcash feature.

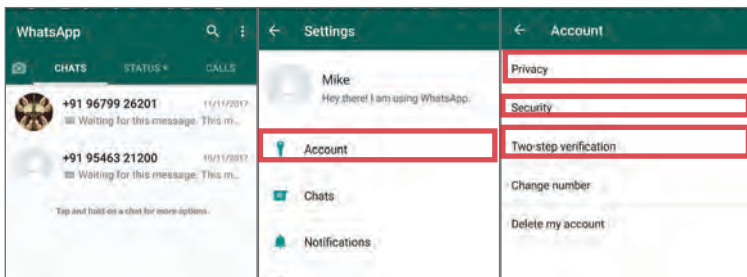


Tap the **ghost** at the far left of the camera page and then select the **gear** icon to adjust your privacy settings. Apply the following recommendations:

- Do not provide your real name in the **Name** or **Username** fields.
- Under the "who can..." section, set **Contact Me** and **View My Story** to **My Friends**.
- Clear Cache** and **Clear Conversations** after every use.
- Select **Manage** and disable both **Filters** and **Travel Mode**.
- If you elect to use Snapcash, turn on the security code (CVV) requirement and review transactions/receipts routinely.

WHATSAPP

WhatsApp, owned by Facebook, is currently the most popular social messaging app, with 1.3 billion monthly active users. WhatsApp provides end-to-end encryption for messages, calls, and video chats. Group messaging includes up to 10 participants while calls and video are person-to-person. The encryption offered by WhatsApp ensures that no one, not even WhatsApp engineers, can intercept the communication method except for the sender and recipient.



Tap the Settings icon to at the bottom right of your screen. Apply the following changes to best maximize your security. Go to **Settings>Account**:

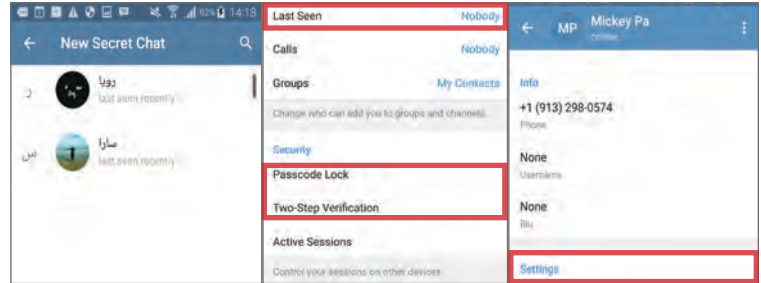
- Under **Privacy**, set **who can see my personal info** options to **Nobody**.
- Under **Security**, enable **Show security settings** to view changes in contacts' security codes.
- Enable **Two-Factor Authentication** to prevent outside access.

Follow these steps while using the app to ensure your protection:

- Manually delete your messages when your conversations conclude.
- To prevent third-party access, do not leave your device unattended.

TELEGRAM

Telegram is an app that primarily 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.

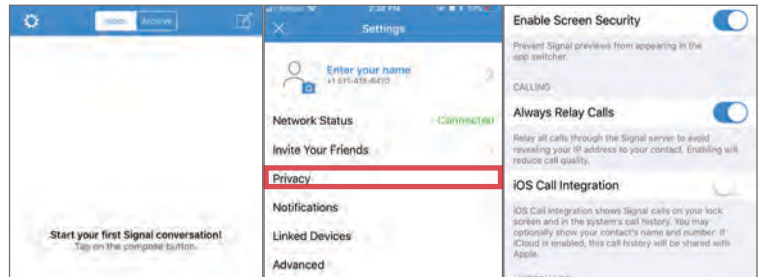


Tap the **Settings** icon and then select the **Privacy and Security** option. Apply the following recommendations to maximize security:

- Do not provide your real name or a profile photo.
- Set **Last Seen** to **Nobody**.
- Establish a secure **Passcode Lock** and **Two-Factor Authentication**.
- Review your active sessions routinely and close all unknown sessions.
- Set to **Delete My Account if away for 1 month**; accounts are free to make and there is no risk of losing contact information.

SIGNAL

Signal is used to establish end-to-end encrypted conversations between users. Signal 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.



Tap the **Settings** icon in the top left corner of the screen and select **Privacy**. Apply these options to best secure your conversations through the app:

- Enable **Screen Security**
- Enable **Always Relay Calls** to improve encryption for all phone calls.
- Disable **iOS Call Integration** to prevent Apple from tracking call history.
- Disable **Enable Debug Log** to limit what little information is collected.

Follow these basic instructions when using the app:

- Manually delete your messages when your conversations are over.
- Clear the app's history after each completed communication.



SMARTPHONES

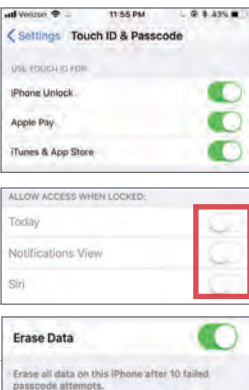
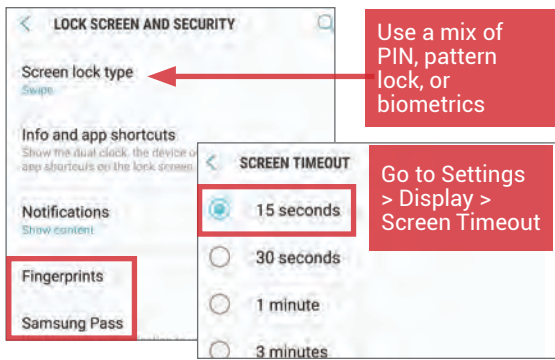

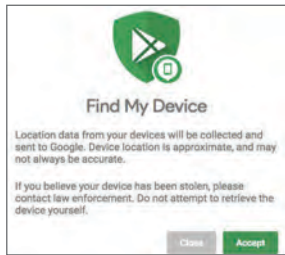

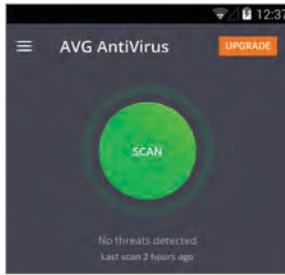
UNCLASSIFIED

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 	Navigate to Settings > Lock screen and security 
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  <p>Capabilities:</p> <ul style="list-style-type: none"> • Remote lock • Erase data • GPS locator • Sound alarm • Send text message to phone • Backup data through iCloud storage 	Install Find My Device  <p>Capabilities:</p> <ul style="list-style-type: none"> • 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  <p>While iOS is not readily susceptible to viruses, use this app to monitor the system for malicious activity.</p> <p>Capabilities:</p> <ul style="list-style-type: none"> • Monitor running apps for malicious activity • Check OS to ensure it is up-to-date 	Install AVG Antivirus 2018  <p>Capabilities:</p> <ul style="list-style-type: none"> • App scanner • File scanner • Website scanner • Text and call blocker • Remote lock • Erase data remotely • GPS locator • Kill slow tasks

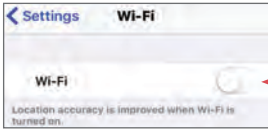


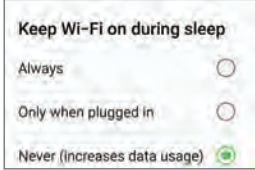





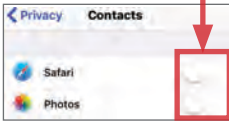
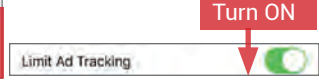
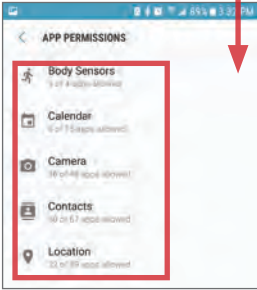
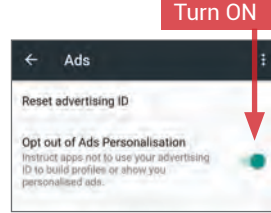
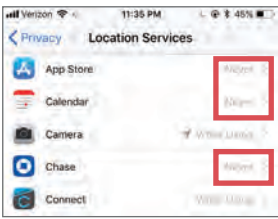


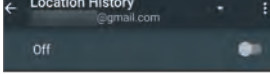
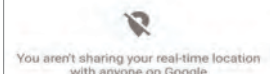
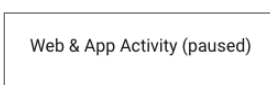
RECOMMENDATIONS TO MINIMIZE PHYSICAL ACCESS AND MALWARE RISKS

- 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.

UNCLASSIFIED

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  <p>Disable Wi-Fi when not in use</p>  <p>Enable network permissions</p> <p>Navigate to Settings > VPN to enable and establish a VPN connection</p>	Navigate to Settings > Connections > Wi-Fi  <p>Disable Wi-Fi when not in use</p> <p>Select the gear icon to configure Wi-Fi (feature varies by Android model) and select Never under "Keep Wi-Fi on during sleep"</p>  <p>Navigate to Settings > Connections > More connection settings to enable and establish a VPN connection</p>
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  <p>Disable Bluetooth when not in use</p> <p>Navigate to Settings > Personal Hotspot to disable broadcasting your private Internet connection</p>  <p>Never share your Internet connection</p>	Navigate to Settings > Connections > Bluetooth  <p>Disable Bluetooth when not in use</p> <p>Navigate to Settings > Connections > NFC and payment to manage Near Field Communications, which enables smartphones to transfer data by touching the devices together</p>  <p>Uncheck</p>
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  <p>Disable Siri</p> <p>Navigate to Settings > Privacy to manage which specific data each app accesses from your phone</p>  <p>Turn OFF</p> <p>Navigate to Settings > Privacy > Advertising</p>  <p>Turn ON</p>	Navigate to Settings > Apps > > App permissions  <p>Restrict excessive requests for personal data</p> <p>Navigate to Settings > Google > Ads</p>  <p>Turn ON</p>
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  <p>Only grant access to apps that require location</p> <p>Disable all location services when not in use</p> 	Navigate to Settings > Location  <p>Disable all location services when not in use</p>  <p>Turn OFF Google location history</p>  <p>Turn OFF Google location sharing</p>  <p>Turn OFF Google Web and App Activity</p>



TRAVELING WITH SMARTPHONES

UNCLASSIFIED

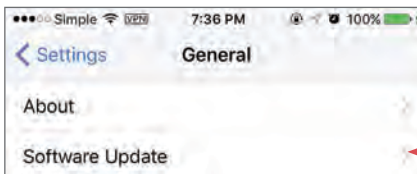
TRAVELING WITH SMARTPHONES - DO'S AND DON'TS

- 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.

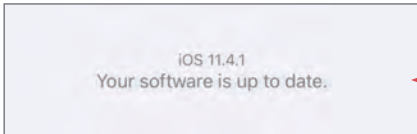
ENSURE THAT YOUR PHONE'S SOFTWARE IS UP-TO-DATE

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)



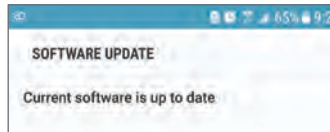
Go to Settings > General > Software Update. Check to see if your software is up-to-date.



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

ANDROID (V. 7.0)

Go to Settings > Software update > Check for updates

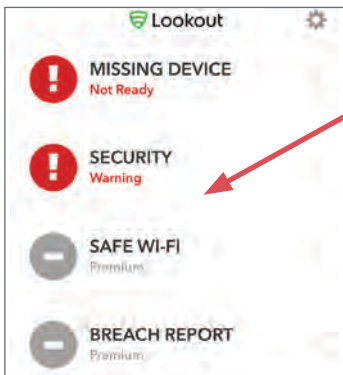


Confirm current software is up-to-date. If not, follow Android prompts to download and install the latest software.

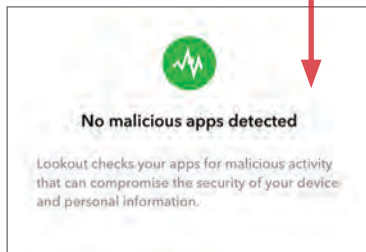
PROTECT YOUR PHONE AGAINST MALWARE

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)



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

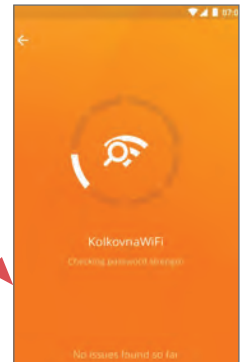


ANDROID (V. 7.0)



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

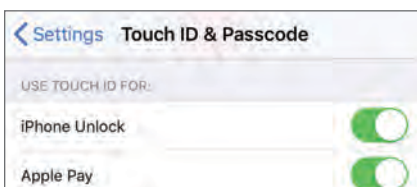
Avast also offers the option to scan Wi-Fi networks for threats.



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)



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



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

ANDROID (V. 7.0)



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



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

UNCLASSIFIED

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)



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



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

ANDROID (V. 7.0)



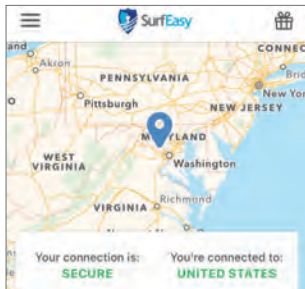
Go to **Settings > Connections > Wi-Fi**. Turn **Wi-Fi OFF**.

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

USE VPN ON WIRELESS NETWORKS

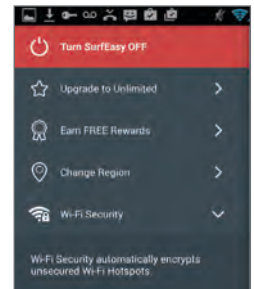
Virtual Private Networks—or **VPNs**—allow you to extend a private network across a public network such as public Wi-Fi. Using a VPN will make it more difficult for malicious individuals to eavesdrop on your Internet traffic. Use a VPN service such as SurfEasy VPN or Avast SecureLine to protect yourself.

IPHONE (V. 11.4.1)



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

ANDROID (V. 7.0)

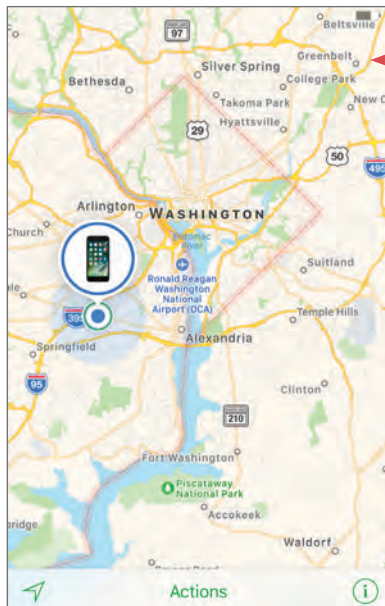


Use VPN services such as **SurfEasy** for Android to protect yourself on Wi-Fi.

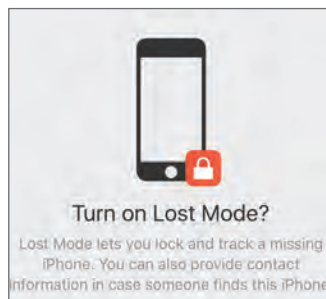
RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

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

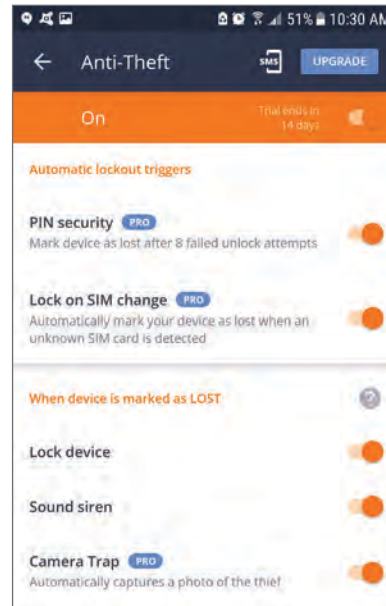
IPHONE (V. 11.4.1)



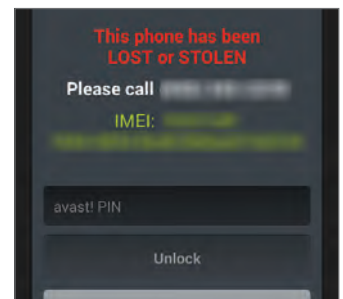
Use the **Find My iPhone** app to recover lost or stolen iPhone smartphones.



ANDROID (V. 7.0)



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





EXIF DATA REMOVAL

UNCLASSIFIED

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, 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.

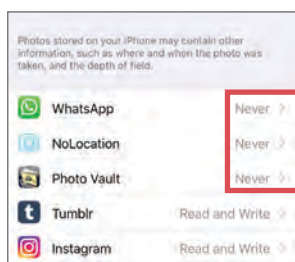
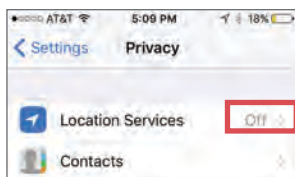
PREVENTING THE CAPTURE OF GEOLOCATION DATA

- 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; with a Nexus, press the lock and the volume-down buttons simultaneously.
- Photos taken in airplane mode still contain geolocation data. To prevent this data capture, turn off location services/storage for your smartphone's camera application, as shown below.
- When uploading or sharing photos, remember that EXIF data and image quality have no correlation. Lower quality images still contain EXIF data.

IOS (V. 11.2.1)

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

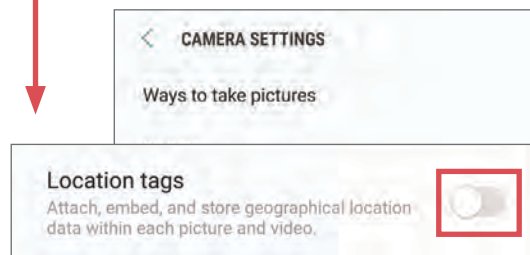
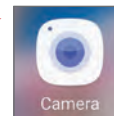
1. Select the **Settings** app and navigate to **Privacy > Location Services**.
2. Turn off location services altogether or for the iPhone's camera applications.
3. Return to the **Settings** app and navigate to **Privacy > Photos**.
4. Disable permissions for other apps to access photos already stored in your iPhone's Camera Roll.



ANDROID (V. 7.0)

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

1. Open the **Camera** app.
2. Tap the **white gear icon** in the top right corner to navigate to Camera Settings.
3. Scroll down to Location tags and turn the toggle into the **OFF** position.



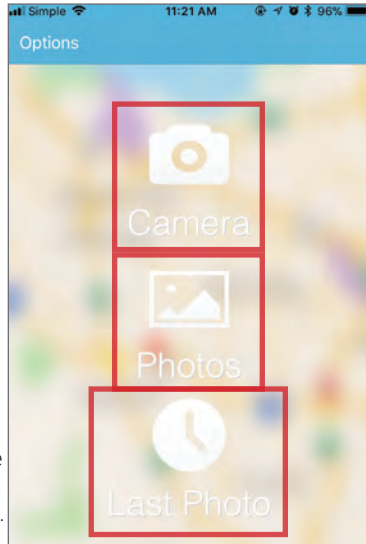
UNCLASSIFIED

EXIF REMOVAL RECOMMENDATIONS

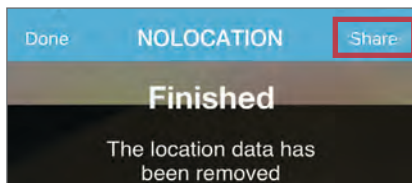
NOLOCATION FOR IOS

NoLocation is a free app that deletes EXIF information from image files stored on your iOS device, and that enables the captures of images without EXIF data.

1. Download the NoLocation app from the **App Store**.
2. Open the NoLocation app and select the appropriate actions:
 - Select **Camera** to take EXIF-free pictures. Select **Use Photo** when finished.
 - Select **Photos** to remove EXIF data from stored images on your device. Select **Choose** to finish.
 - Select **Last Photo** to remove the EXIF data from the most recent image on your device.



3. Click **Share** at the top right of the screen to download the image to your device or share it.



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**.

PHOTOINFO ERASER FOR ANDROID

PhotoInfo Eraser is a free app that deletes all EXIF data from image files stored on your Android device.

1. Download PhotoInfo Eraser from the **Play Store**.
2. Open the PhotoInfo Eraser app and select **Gallery**.
3. Navigate your device gallery and select an image.
4. Select the **eraser icon** and press OK to confirm deletion of EXIF tags.



5. A copy of your photo without EXIF data is now available. To share the photo, either:

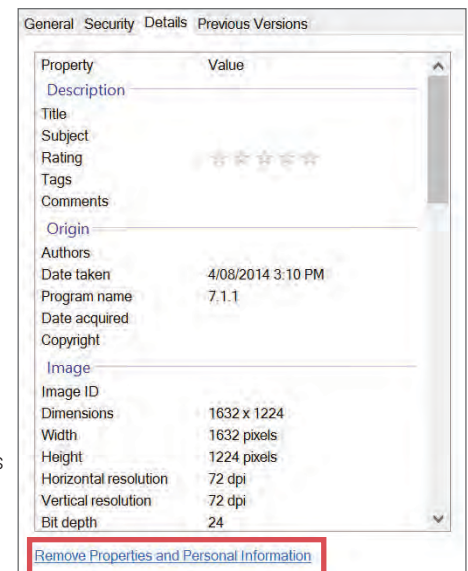
- Select the orange **Share** icon in the lower right, or
- Exit the PhotoInfo Eraser app and navigate to your camera **Gallery**. Navigate to the **PIEraser** image folder to access a copy of your photo without any EXIF data.



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.





MOBILE WALLETS

UNCLASSIFIED

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.

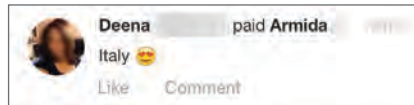


On most smartphones, fingerprints can be used as a purchase authentication method, enhancing your security over a physical credit or debit card.

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.



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?

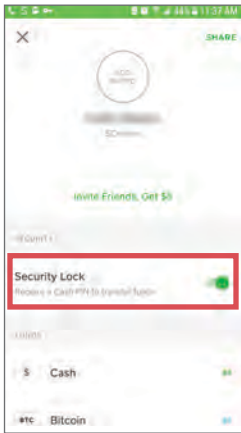
Six of the most popular mobile wallet services are outlined below.



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)
Apple 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
Google 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

UNCLASSIFIED

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**.

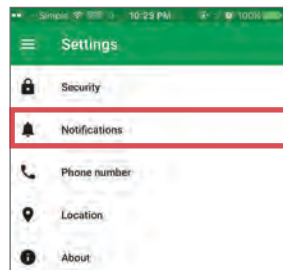
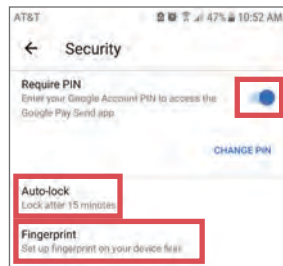
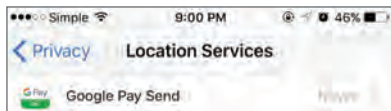
Users can link cash to a custom Visa debit card available through the app, or purchase/sell Bitcoin to use in transactions. An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

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.

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



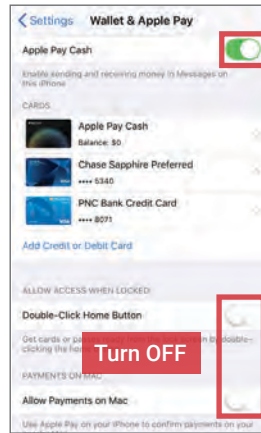
Android users: Navigate to **Google Pay Settings > Permissions** to disable location tracking for Google Pay

MOBILE WALLETS - BEST PRACTICES

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

- Avoid accessing mobile wallets on public Wi-Fi networks
- Use privacy settings to restrict the social features of mobile wallets, so only you can see account activity.
- **Turn ON** transaction alerts to receive email or text notifications of any transaction.
- 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.

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.

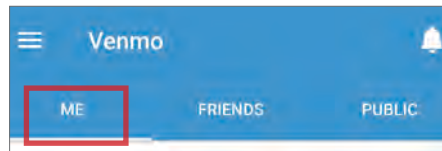
- **Toggle "Apple Pay Cash" ON** to enable direct money transfers with your contacts
- **Turn OFF "Double-Click Home Button"** to limit access to Apple Pay when your phone is locked
- **Turn OFF "Allow Payments on Mac"** to minimize risks of an unauthorized person making a purchase on your computer

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

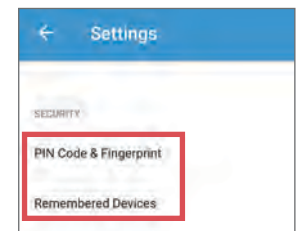
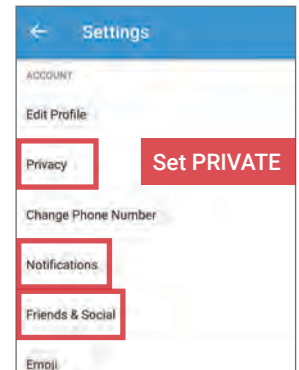
VENMO

Navigate the dropdown menu to **Settings**:

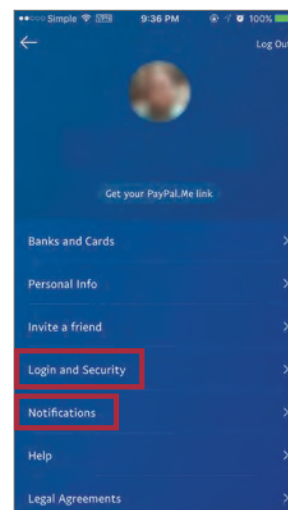
- Under **Privacy**, select **Private**
- Under **Notifications**, enable push notifications for all **Payments** and **Activity** options
- Under **Security**, enable **PIN Code & Fingerprint**.
- Review **Remembered Devices** to check for suspicious log-ons.
- Under **Friends & Social**, do not connect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



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



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

UNCLASSIFIED

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 throughout 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"

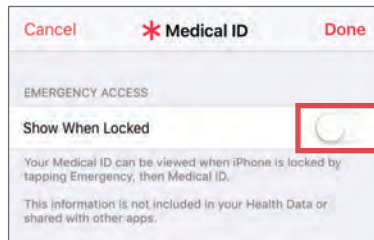
UNCLASSIFIED

APPLE HEALTH



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

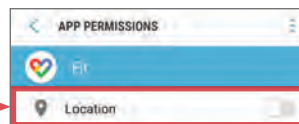
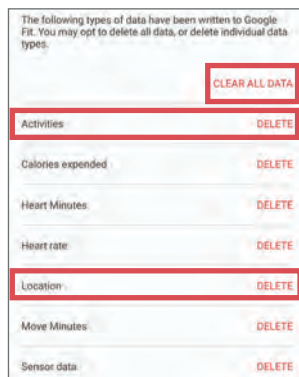
- Select **Delete Medical ID** at the bottom.
- If you wish to maintain Medical ID, **toggle OFF Show When Locked**.



GOOGLE FIT

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

- To delete existing 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.



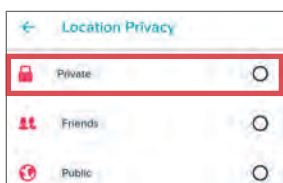
On your phone, navigate to **Settings > Apps > Fit > Permissions**, and toggle the **Location** permission **OFF**. Leaving location tracking enabled allows Google Fit to precisely map your daily activities, which may reveal sensitive information about your whereabouts.

Toggle OFF

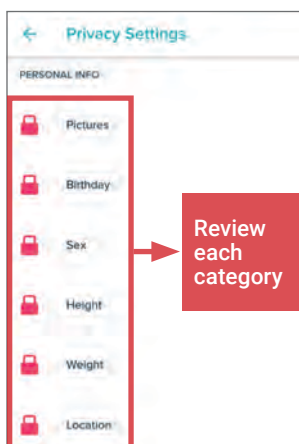
FITBIT

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.



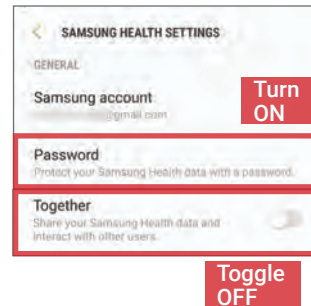
Select Private



SAMSUNG HEALTH

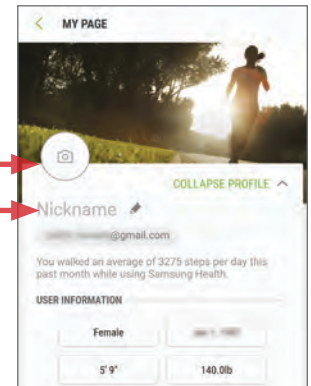
Navigate the upper-right drop-down menu to **Settings**.

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



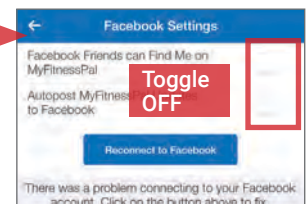
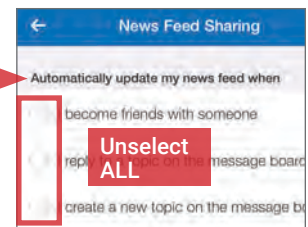
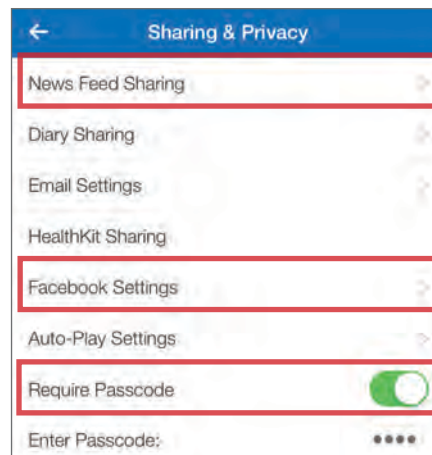
Leave blank

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



MYFITNESSPAL

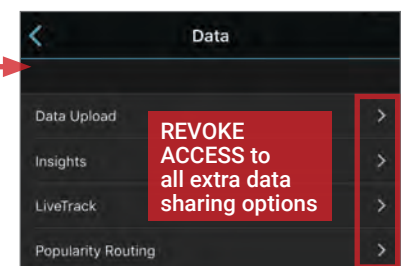
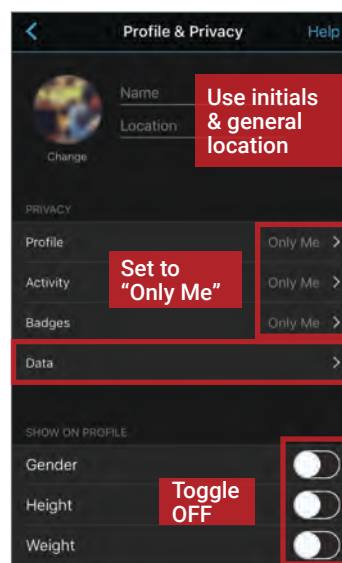
Navigate to the **More** tab > **Settings > Sharing & Privacy**. Implement data-protective settings suggested below. Do not link your Facebook account.



GARMIN CONNECT

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.





SECURING HOME WI-FI NETWORK

UNCLASSIFIED

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

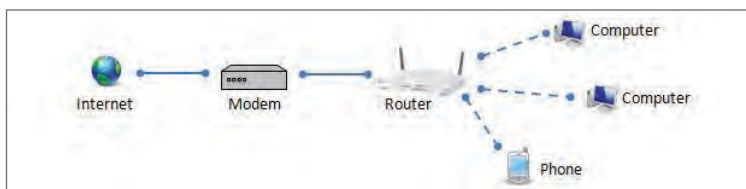
- Use an ethernet cable instead of a Wi-Fi connection when possible; disable the wireless network when it won't be used for an extended period of time.
- Use the most up-to-date hardware and operating systems to maximize your connecting device's security options.
- Turn on automatic updates for your 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, alphanumeric combinations with at least 12 characters.

UNCLASSIFIED

CREATING A NETWORK NAME AND PASSWORD

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

CHOOSING STRONG ENCRYPTION

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

ENCRYPTION PRIVACY STRENGTH

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

MAC ADDRESS FILTERING

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

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
iPhone-2	08:00:27:00:00:00	Wi-Fi 2.4G
iPad	08:00:27:00:00:00	Wi-Fi 5G
DESKTOP-1	08:00:27:00:00:00	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.

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.



ONLINE REGISTRATION UNCLASSIFIED

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.

Sign Up

First name	Last Name
------------	-----------

GENDER

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

Gender

Female
Male
Other

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.

Your Location	Country
	United States
	Zip Code

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.



Sign up with Facebook

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.



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)
+ Add another phone	

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.

Birthday

Month	Day	Year	Why do I need to provide my birthday?
-------	-----	------	---------------------------------------

EMAIL ADDRESS

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

Sign Up

First name	Last Name
Email	

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.

WORK	
Company	Where have you worked?
Position	
City/Town	
Description	










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
Friends	Save Changes Cancel

UNCLASSIFIED

IDENTITY FIELDS DURING REGISTRATION, BY SERVICE

									
Service Name	Outlook	Yahoo	Facebook	Twitter	Google Plus	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.
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.

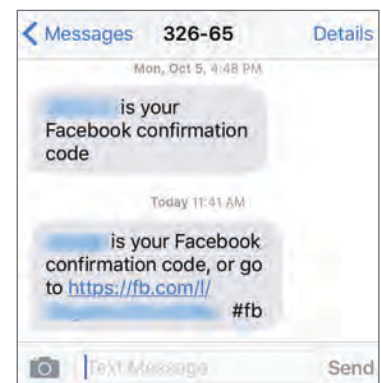
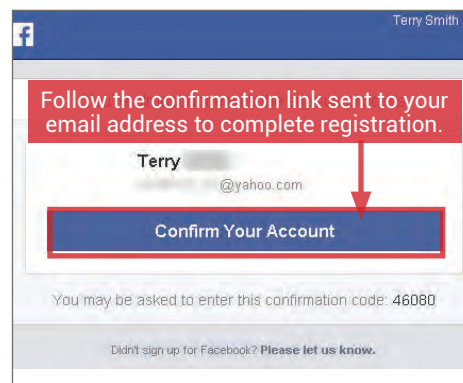
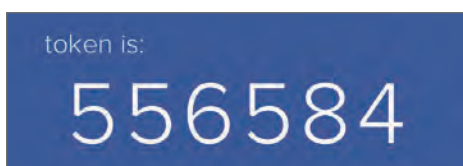


Sign Up
It's free and always will be.

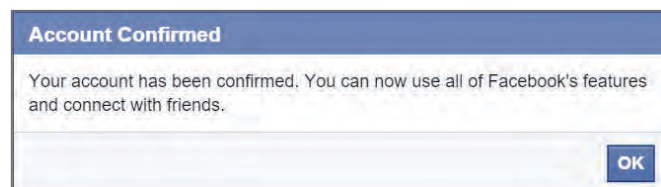
First name Last name

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.



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





OPTING OUT OF DATA AGGREGATORS

UNCLASSIFIED

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.

PrivateEye

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**.

PublicRecords**NOW**
Billions of Records at Your Fingertips

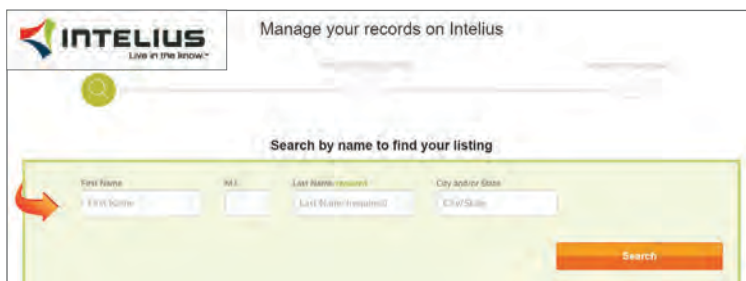
US SEARCH

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

USSEARCH
for PEOPLEDATA®

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.



ZABA®SEARCH



phonesbook

UNCLASSIFIED

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](http://www.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.peakyou.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 "UniquelD" 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

UNCLASSIFIED

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. Every year, more than 13 million incidents of identity theft are reported, equating to 25 individuals falling victim every minute. On average, each victim spends 30 to 60 hours and \$50 to \$500 trying to resolve the issue. While the common conception is that identity thieves are online scammers, new evidence indicates that up to 50% of all reported cases involve theft from a neighbor, co-worker, or family member. Most identity theft cases can be resolved if they are caught early.

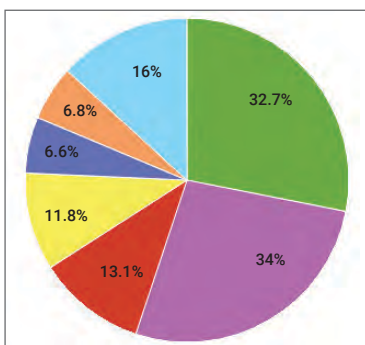
TYPES OF IDENTITY THEFT AND WHAT'S AT RISK

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 Numbers and Information

WHAT DOES IDENTITY THEFT LOOK LIKE?



- Employment/Tax Fraud
- Credit Card Fraud
- Phone or Utilities Fraud
- Bank Fraud
- Loan or Lease Fraud
- Government Documents/Benefits Fraud
- Other (Insurance, Medical, Criminal, etc.)

*Data Source: Consumer Sentinel Network for total reports by type in 2017. Some reports may display the data in different manners.

ID THEFT TYPES

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

POSSIBLY HARMFUL

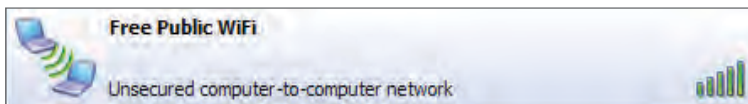
- Pets' RFID Numbers
- Utility Account Numbers
- Residential History
- Unsolicited Credit Offers

AGE OF VICTIMS

- 19 and Under (4%)
- 20 to 39 (36%)
- 40 to 59 (40%)
- 60 and Over (20%)

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.



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 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.

1 **From:** Payment Services <XXXXX@XXXX.XXX>
Reply-To: <XXXXXXXX@XXXX.XXX>
Date: Mon, 23 Nov 2014 12:34:13 -0700
2 **Subject:** Suspicious Account Activity!

3 Name:
Email:
Account Number:
Social Security Number:

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

5

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:

6

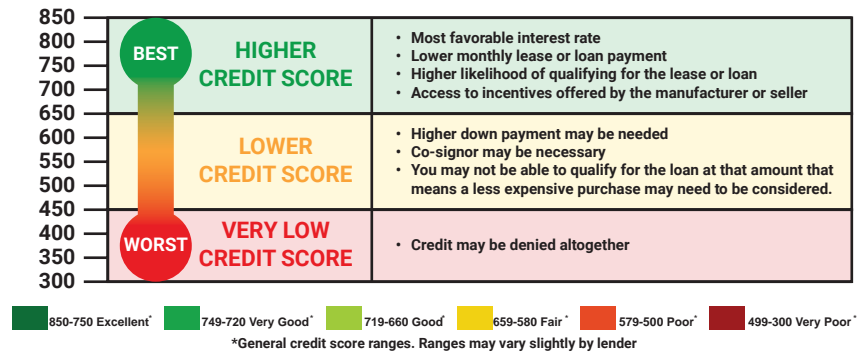
7

UNCLASSIFIED

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.



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 AND RECOVERY SERVICE OFFERINGS	SSN	BANK ACCOUNT	CREDIT CARD NUMBERS	MEDICAL FRAUD	PUBLIC & COURT RECORDS	COMPUTER SECURITY OFFERINGS	CREDIT REPORTS	FINANCIAL COVERAGE	PRICE PER MONTH
IDENTITY GUARD	✓	✓	✓		✓	✓	Monthly	Up to \$1 Million	\$19.99
IdentityForce. Protect What Matters Most	✓	✓	✓	✓	✓	✓	Quarterly	Up to \$1 Million	\$23.95
TrustedID® You're in control	✓	✓	✓	✓		✓	Available	Up to \$1 Million	\$19.95

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.

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.

1-888-202-4025	1-888-397-3742	1-800-680-7289



KEEPING YOUR KIDS SAFE ONLINE

UNCLASSIFIED

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

Enter email address: (###) ###-####

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.

Category	Allow	Block	Warning
Security Risk	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Warning"/>
Unethical	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Warning"/>
Adult/Mature Content	<input type="button" value="Allow"/>	<input checked="" type="button" value="Block"/>	<input type="button" value="Warning"/>
Bandwidth Consuming	<input checked="" type="button" value="Allow"/>	<input type="button" value="Block"/>	<input type="button" value="Warning"/>
Business	<input checked="" type="button" value="Allow"/>	<input type="button" value="Block"/>	<input type="button" value="Warning"/>
Personal	<input checked="" type="button" value="Allow"/>	<input type="button" value="Block"/>	<input type="button" value="Warning"/>
Unrated	<input checked="" type="button" value="Allow"/>	<input type="button" value="Block"/>	<input type="button" value="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 data.

[Learn more about Tracking Protection and your privacy](#)

Use Tracking Protection to block known trackers

☒ Always

☐ Only in private windows

[Exceptions...](#)

[Change Block List...](#)

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)

UNCLASSIFIED

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, mobile app, text, and video supervision; review activity history; lock devices; and receive email alerts, on up to 10 devices.

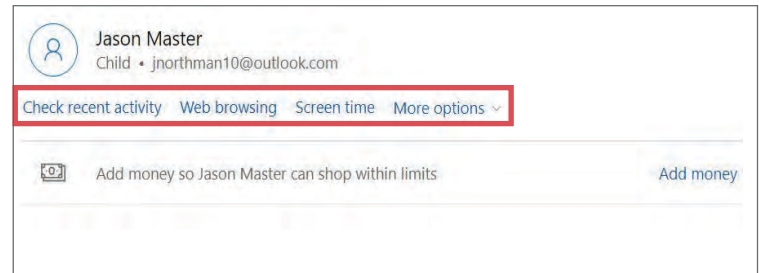
What	Which
Allowed Web site visited	onlinefamily.norton.com
Child warned for blacklisted site & did not proceed	facebook.com

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.



MICROSOFT FAMILY SAFETY

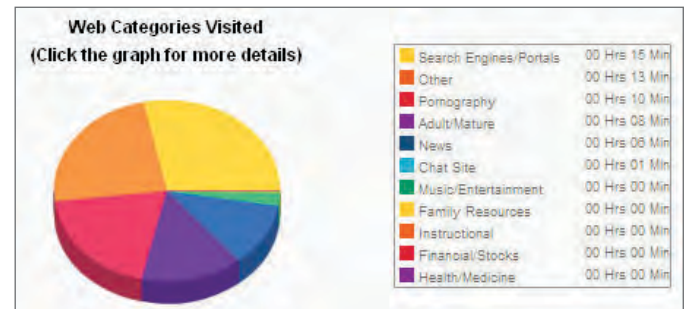
Activate this free service from your Microsoft/Outlook account. The service provides basic content filters and reports of programs/websites accessed by each account.



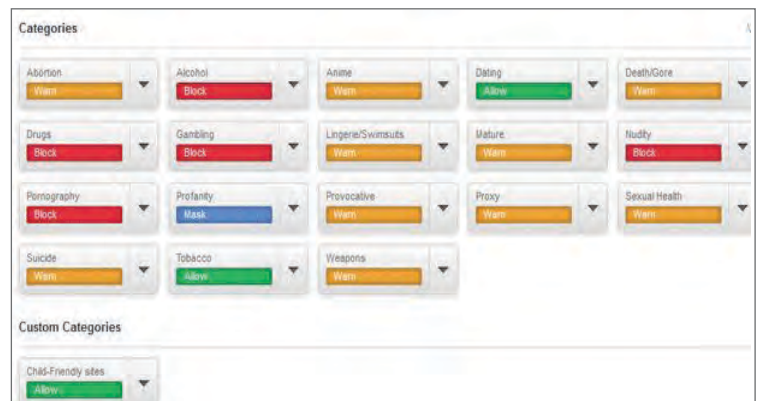
Adults can set individualized settings for each account and view their child's requests to access blocked content each time they log in.

NET NANNY

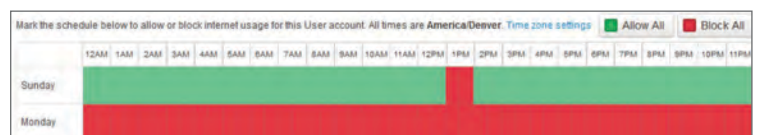
This service is available for download for \$39.99 and can both restrict and monitor content from computer programs, instant messengers, SNSes, and web browsing applications. It is installed onto the desktop and provides the most granular settings for filtering and reporting potentially harmful content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



Parents can respond to their child's permission requests remotely from a mobile app or computer in real time. Additional settings include blocking applications, Internet connections, proxy servers, blogs, and chat rooms. Net Nanny displays an extensive list of SNS and instant messengers as well as 35 categories of potentially harmful content to screen.



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





VOICE OVER INTERNET PROTOCOL (VOIP)

UNCLASSIFIED

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.

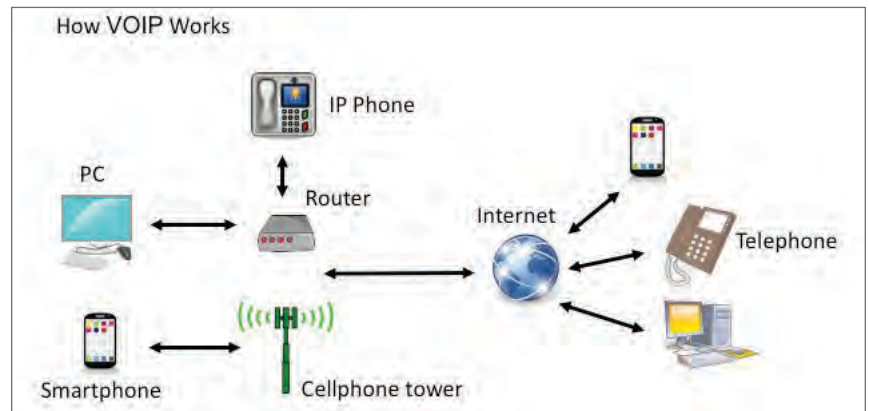
Some providers do not connect to 911 or emergency services, so a second phone line may be needed.

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




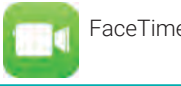


Password-protect your apps, and encrypt or erase sensitive information including texts, call history, and voicemail. Here are some tips and security-related questions to ask:

- 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?



UNCLASSIFIED

CHOOSING A VOIP PROVIDER

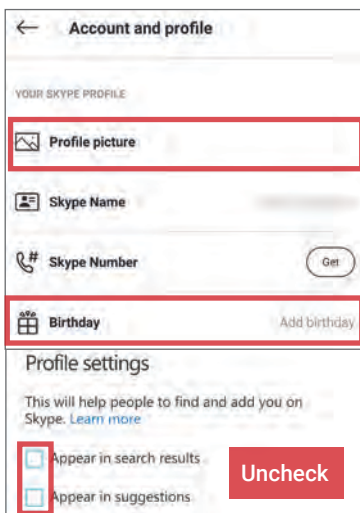
MOBILE SERVICE	OPERATING SYSTEM	COST	BEST USES
	Windows, Mac, iOS, web, Android	Free to \$13.99/month	File sharing, screen sharing, document collaboration, video calls
	iOS, Android, web	Free	Encrypted one-to-one or group audio/video calls, live streaming video, screen sharing (web)
	iOS, Android	\$9.95/month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



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**.

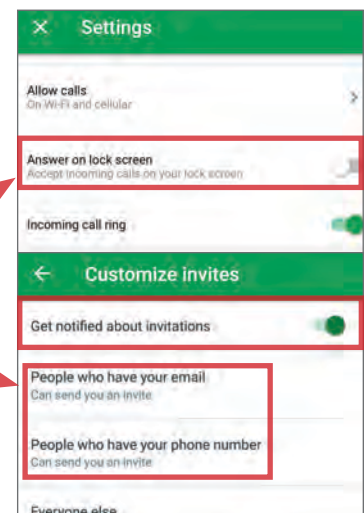
Under **Settings > Contacts**, toggle **"Sync your contacts"** to OFF.

GOOGLE HANGOUTS

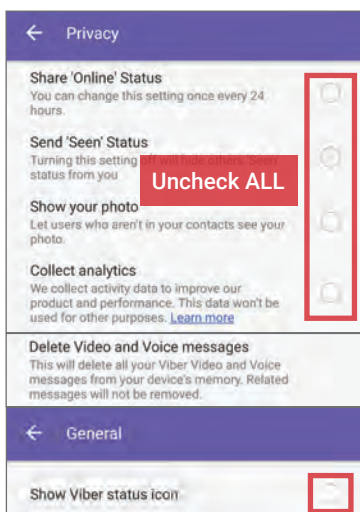
Sign up for a Google Voice (GV) account at google.com/voice for a free number or port your existing number.

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.



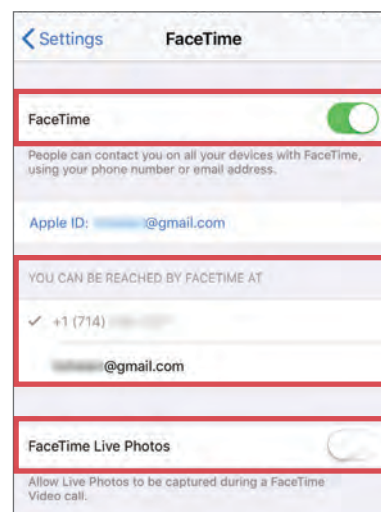
VIBER



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



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)

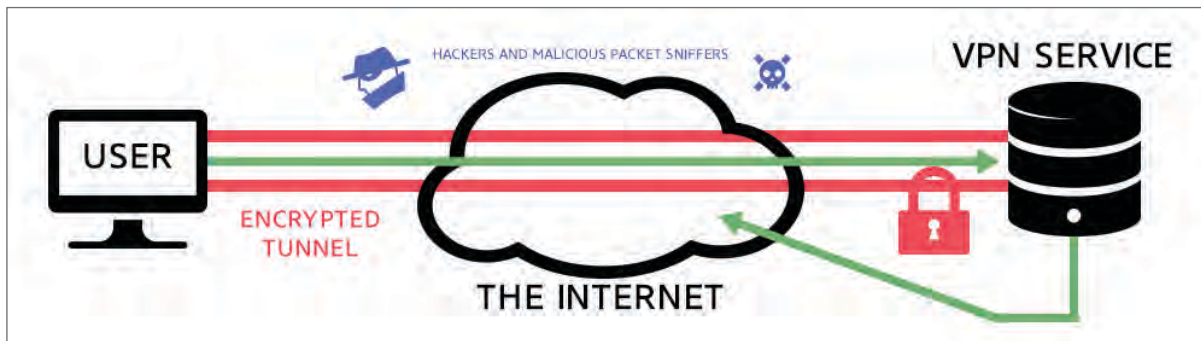
UNCLASSIFIED

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	<ul style="list-style-type: none"> • \$12.95 per month • 30-day money back guarantee 	<ul style="list-style-type: none"> • Can run 3 devices simultaneously (with premium service) • VPN killswitch offered for Windows • Provides content unblocking 	<ul style="list-style-type: none"> • Connection logs are retained • Limited simultaneous device connections
ZenMate	iOS, Windows, Android, Chrome, Firefox, Opera, routers	<ul style="list-style-type: none"> • Unlimited free browser add-on • \$8.99 per month • 14-day money back guarantee 	<ul style="list-style-type: none"> • Extremely streamlined and easy-to-use 	<ul style="list-style-type: none"> • Limited traffic settings • Uses one security protocol (L2TP)
IPVANISH VPN	iOS, Windows, Android	<ul style="list-style-type: none"> • \$10 per month • 7-day money back guarantee 	<ul style="list-style-type: none"> • 2 simultaneous connections • Unlimited bandwidth • No VPN traffic logs 	<ul style="list-style-type: none"> • No free trial • Limited device connections
CyberGhost	iOS, Windows, Android, Linux, Chrome OS, Raspberry Pi, routers	<ul style="list-style-type: none"> • Free limited service • \$10.99 per month for full service • 30-day money back guarantee 	<ul style="list-style-type: none"> • IP address shielding • Highly configurable • Unlimited bandwidth with premium subscription 	<ul style="list-style-type: none"> • Full service requires a paid subscription • Server availability varies by country

UNCLASSIFIED

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

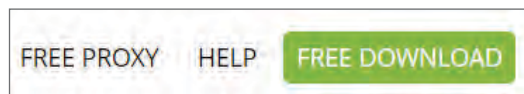
- VPNs can cause a reduction in Internet connection speed. The tunneling effect of most VPN services creates a lag in the connection.
- VPN service providers will have access to your username, password, session data, and some PII. Review your service's ToS frequently to ensure that the company is not 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

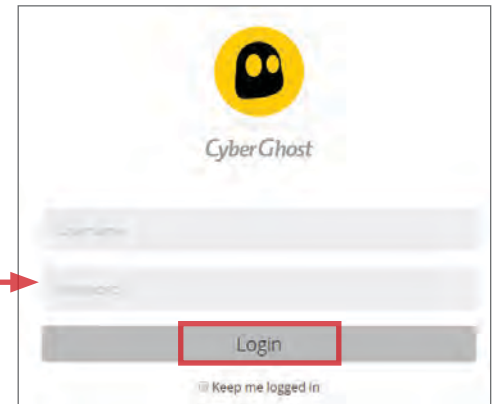
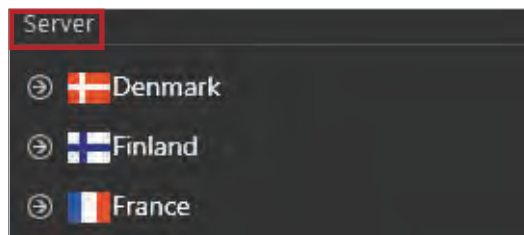
Following VPN provider selection, set up and begin your protected browsing session. Using VPN software will require you to login each time you wish to make a connection. Most services require a basic username/password combination for authentication. Additional security features, like use of an alphanumeric 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.

- 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.

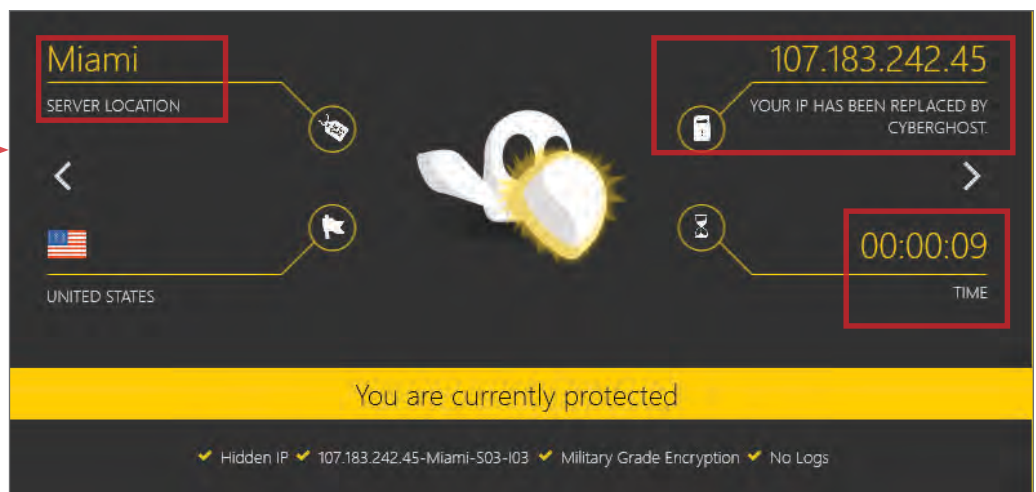


- 3** Open the program on your device and sign in. VPNs can be run indefinitely, however if you logout of the program or shutdown your device, you will need to login again.



- 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.



- 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 - 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

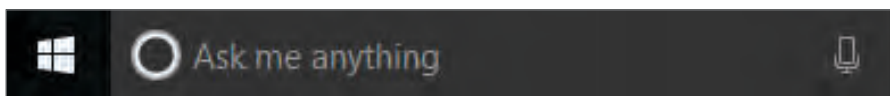
Windows 10 comes with many new additions: a new browser, a varied login protocol, a digital assistant, and a list of default settings that collect and send usage data to Microsoft. These new user-friendly features create additional risks for your personally identifiable information (PII). The programs 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:

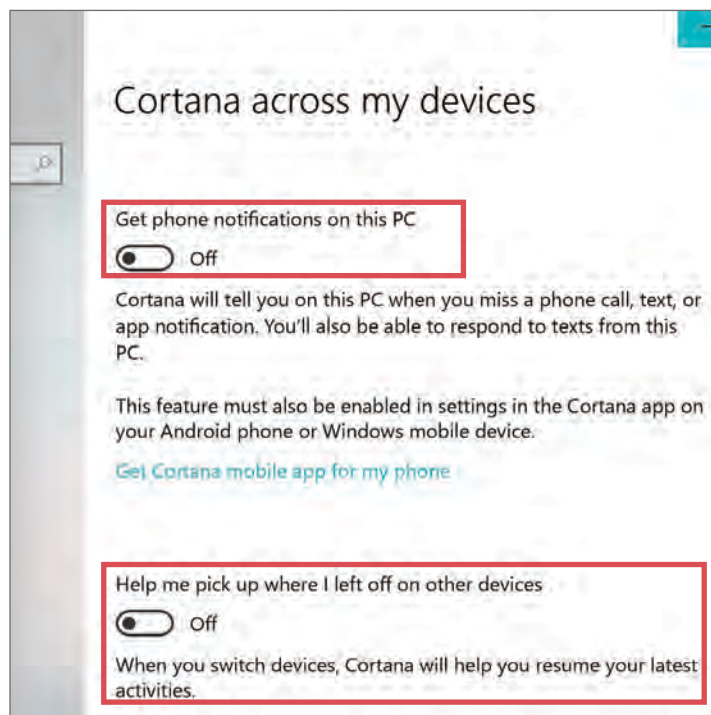
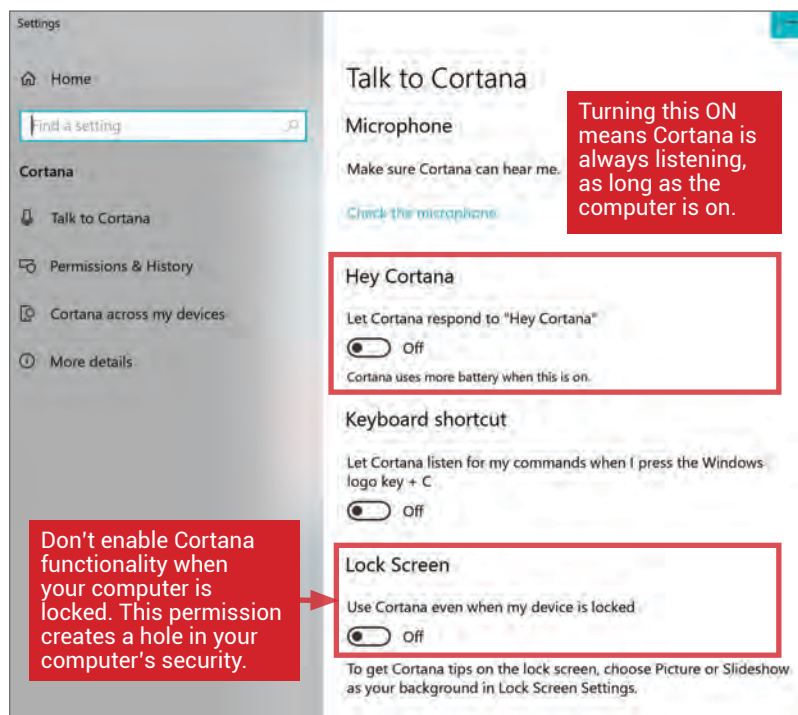
1 Access Cortana at the bottom left of your computer screen. It will appear as a search box or as the circle icon depending on your view settings.



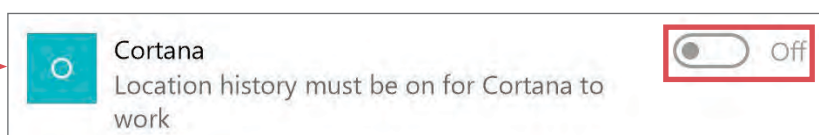
2 From the Options menu, click on **Start Menu > Settings > Cortana**. Click through each entry on the settings bar to review the settings pertaining to Cortana.

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**.



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.



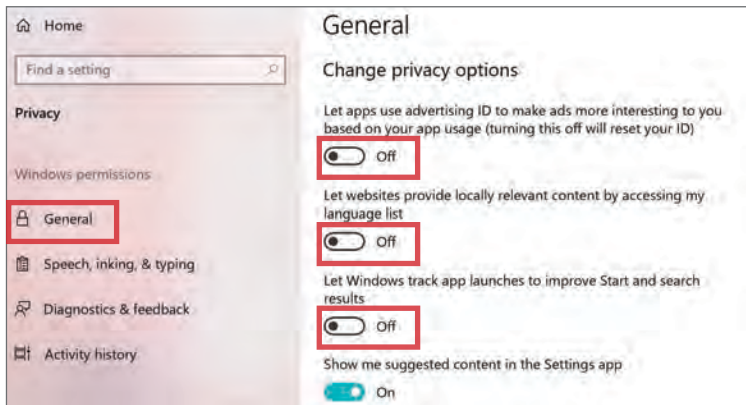
ADJUSTING WINDOWS 10 PRIVACY SETTING

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.

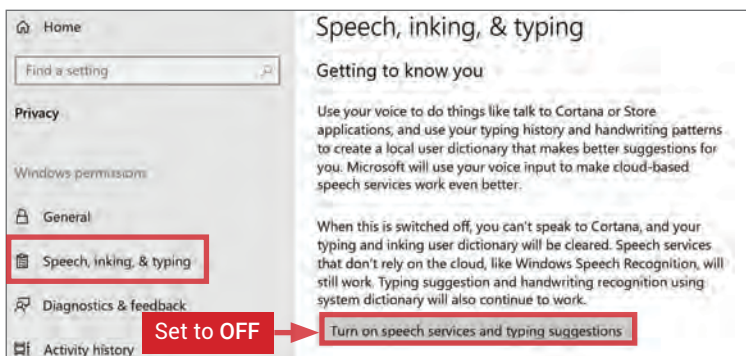
- 1 Navigate to Windows 10's privacy settings by **Start Menu > Settings > Privacy**.



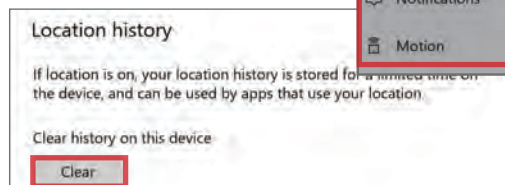
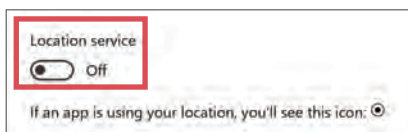
- 2 Under the **General** heading, modify the options as shown below in order to secure your computer and PII.



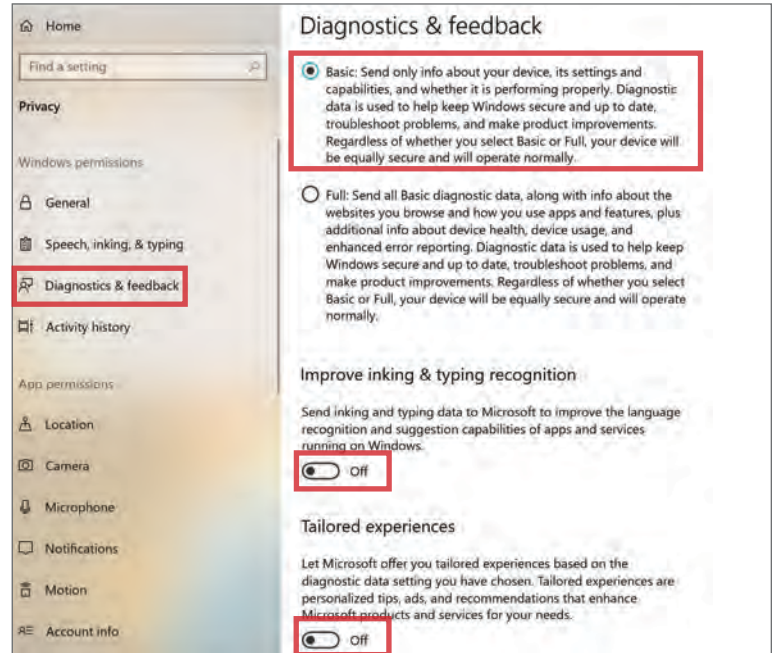
- 3 Under **Privacy > Speech, inking, & typing** ensure speech services and typing suggestions are turned **OFF** to prevent the collection of voice, typing, and touch interface patterns.



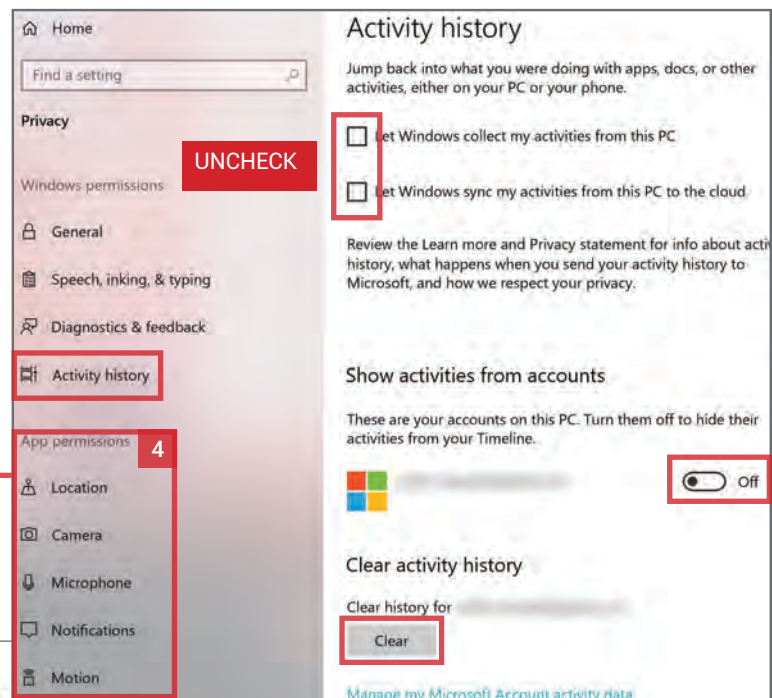
- 4 Microsoft automatically enables numerous categories of app permissions, including access to your device camera, microphone, location, and your account information. Examine each category listed under **Privacy > App permissions** in detail. When in doubt, toggle **OFF** all access permissions that 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)



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



- 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.



INDEX

A

ACCOUNT CLEAN-UP

EXIF Data Removal	
EXIF Removal - Do's and Don'ts	26
EXIF Removal Recommendations	27
Facebook	
About	3
Activity log	3
Deactivating/Deleting Your Facebook Account	3
Recommended Settings	2
Facebook Mobile	
Facebook Mobile Settings	4
Google+	
Circles - How You Share on Google+	13
Health Apps & Fitness Trackers	
Apple Health	31
Google Fit	31
Instagram	
Clearing Search History	9
Mobile Dating Apps	
Coffee Meets Bagel	19
Hinge	19
Mobile Wallets	
Apple Pay - iPhone Only	29
Mobile Wallets - Do's and Don'ts	28
Online Registration	34-35
Opting Out of Data Aggregators	36-37
Photo Sharing Services	
Flickr	17
Google Photos	15
Secure Chat Apps	
Signal	21
Snapchat	21
Telegram	21
Whatsapp	21
Voice Over IP (VOIP)	
Using VOIP Securely	42
Windows 10	
Adjusting Window 10's Privacy Setting	47

ACCOUNT DELETION/DEACTIVATION

Facebook	
Deactivating/Deleting Your Facebook account	3
Recommended Settings	2
Google+	
Deleting Your Google+ Profile	13
Instagram	
Deleting Instagram	9
Linkedin	
Closing Your LinkedIn Account	11
Mobile Dating Apps	
Hinge	19
Secure Chat Apps	
Telegram	21
Twitter	
Account Settings	7

ACTIVITY HISTORY

Facebook	
Activity Log	3
Recommended Settings	2
Facebook Mobile	
Facebook Mobile Settings	4
Google+	
Circles - How You Share on Google+	13
Posting to Google+	12
Health Apps & Fitness Trackers	
Google Fit	31
How People Track Health & Fitness	30
Overview	30
Identity Theft Prevention	
Possibly Harmful	38
Instagram	
Activity Status	9
Keeping Your Kids Safe Online	

Family Safety Services	41
Norton Security Premium	41
LinkedIn	
Request Data Archive	11
Mobile Wallets	
Google Pay	29
Mobile Wallets - Best Practices	29
PayPal	29
Risks of Using Mobile Wallets	28
Square Cash	29
Venmo	29
Photo Sharing Services	
Imgur	15
Virtual Private Network (VPN)	
What is a VPN?	44
Voice Over IP (VOIP)	
Using VOIP Securely	42
Windows 10	
Adjusting Windows 10's Privacy Settings	47

ADVERTISEMENTS

Facebook	
Recommended Settings	2
Facebook Mobile	
Facebook Mobile Settings	4
Overview	4
Mobile Dating Apps	
Selecting A Dating App	18
Online Dating Services	
Match.com	17
Photo Sharing Services	
Pinterest	15
Virtual Private Network (VPN)	
VPN Benefits	45

APPLE

EXIF Data Removal	
iOS (v. 11.2.1)	26
NoLocation for iOS	27
Preventing the Capture of Geolocation Data	26
Viewing and Removing EXIF Data on OS X	27
Facebook	
iPhone Settings	4
Health Apps & Fitness Trackers	
Apple Health	31
The table	30
Instagram	
Privacy Settings	9
Mobile Dating Apps	
Selecting A Dating App	18
Mobile Wallets	
Apple Pay - iPhone Only	29
Choosing the Right Mobile Wallet	28
Photo Sharing Services	
iOS Photos	14
Secure Chat Apps	
Choosing the Right Secure Chat App	20
Signal	21
What are Secure Chat Apps?	20
Smartphones	22-23
Traveling with Smartphones	24-25
Virtual Private Network (VPN)	
Choosing the Right VPN Service Provider	44
Voice Over IP (VOIP)	
Benefits of VOIP	42
Choosing a VOIP Provider	43
FaceTime	43

C

CHILD SAFETY

Identity Theft Prevention	
Age of Victims	38
ID Theft Types	38
Keeping Your Kids Safe Online	40-41

COMMUNICATING SECURELY

Identity Theft Prevention	
Fake Wi-Fi Networks	38
Identity Theft Prevention - Do's and Don'ts	38
Keeping Your Kids Safe Online	40-41
LinkedIn	
Communications Settings	11
Mobile Dating Apps	
Hinge	19
Mobile Dating Apps - Do's and Don'ts	18
Using Mobile Dating Apps: Communication	18
Secure Chat Apps	20-21
Voice Over IP (VOIP)	
Choosing a VOIP provider	43
Disadvantages	42
Using VOIP Securely	42

CONNECTIONS & FOLLOWERS

Facebook	
About	3
Facebook Profile Page	3
Friends	3
Recommended Settings	2
Social Network - Do's and Don'ts	2
Facebook Mobile	
Local	5
Nearby Friends - Location Settings	5
Selecting Your Privacy	5
Social Network - Do's and Don'ts	4
Tag Friends	5
Google+	
Followers	12
Overview	12
Social Network - Do's and Don'ts	12
Health Apps & Fitness Trackers	
Garmin Connect	31
MyFitnessPal	31
Samsung Health	31
The table	30
Instagram	
Instagram - Do's and Don'ts	8
Overview	8
Keeping Your Kids Safe Online	
Do's and Don'ts	40
LinkedIn	
Managing Your LinkedIn Presence	10
Social Network - Do's and Don'ts	10
Who Can See Your Last Name	10
Mobile Wallets	
Venmo	29
Twitter	
Overview	6
Posting to Twitter	6
Social Network - Do's and Don'ts	6
Twitter Profiles	6

D

DATING

Facebook	
About	3
Mobile Dating Apps	18-19
Online Dating Services	16-17
Online Registration	
Relationships/Orientation	34

DEVICE SETTINGS

Facebook Mobile	
Android Settings	4
iPhone Settings	4
Health Apps & Fitness Trackers	31
Keeping Your Kids Safe Online	40-41
Mobile Wallets	
Apple Pay - iPhone Only	29
Photo Sharing Services	
iOS Photos	14

Smartphones	22–23
Traveling with Smartphones	24–25
Voice Over IP (VOIP)	
FaceTime	43
Windows 10	46–47

E

EXCHANGEABLE IMAGE FILE FORMAT (EXIF)

EXIF Data Removal	26–27
Photo Sharing Services	
Flickr	15
Imgur	15
iOS Photos	14
Overview	14
Photo Sharing Services - Do's and Don'ts	14

F

FACEBOOK

EXIF Data Removal	
EXIF Data	26
Facebook	2–3
Facebook Mobile	4–5
Google+	
Posting to Google+	12
Health Apps & Fitness Trackers	
Built-in SNS Links	30
MyFitnessPal	31
Instagram	8–9
Mobile Dating Apps	
Selecting a Dating App - Registration Information	18
Mobile Wallets	
Choosing the Right Mobile Wallet	28
Mobile Wallets - Do's and Don'ts	28
Risks of Using Mobile Wallets	28
Venmo	29
Online Dating Services	
Selecting a Dating Site - Data Sharing Options	16
Online Registration	
Identity Fields During Registration, By Service	35
Social Login	34
Photo Sharing Services	
Facebook	14
Imgur	15
Overview	14
Secure Chat Apps	
Secure Chat Apps - Do's and Don'ts	20
Signal	21
WhatsApp	21
Voice Over IP (VOIP)	
Viber	43

FACE RECOGNITION

Facebook	
Recommended Settings	2
Online Dating Services	
Common Threats from Dating Sites	16
Photo Sharing Services	
Google Photos	15

FAMILY SAFETY

EXIF Data Removal	26–27
Facebook	2–3
Facebook Mobile	4–5
Google+	12–13
Identity Theft Prevention	38–29
Instagram	8–9
Keeping Your Kids Safe Online	40–41
LinkedIn	10–11
Opting Out of Data Aggregators	36–37
Photo Sharing Services	14–15
Secure Chat Apps	20–21
Smartphones	22–23

UNCLASSIFIED

Traveling with Smartphones	24–25
Twitter	6–7
Virtual Private Network (VPN)	44–45
Voice Over IP (VOIP)	42–43
Windows 10	46–47

FINANCIAL TRANSACTIONS

Identity Theft Prevention	38–39
Mobile Wallets	28–29
Secure Chat Apps	
Choosing the Right Secure Chat App	20
Snapchat	21

FINGERPRINT RECOGNITION

Mobile Wallets	
Apple Pay - iPhone Only	29
Benefits of Mobile Wallets	28
Choosing the Right Mobile Wallet	28
Google Pay	29
Venmo	29
Smartphones	
Protecting Your Smartphone from Physical Access and Malware Risks	22
Traveling with Smartphones	
Lock Screen (Android)	24

G

GOOGLE

EXIF Data Removal	
EXIF Data	26
EXIF Removal - Do's and Don'ts	26
PhotoInfo Eraser for Android	27
Preventing the Capture of Geolocation Data	26
Facebook Mobile	
Android Settings	4
Google+	12–13
Health Apps & Fitness Trackers	
Google Fit	31
How People Track Health & Fitness	30
The table	30
Instagram	
Overview	8
Privacy Settings	9
Keeping Your Kids Safe Online	
Google Chrome Settings	40
Mobile Dating Apps	
Selecting a Dating App - Operating Systems	18
Mobile Wallets	
Choosing the Right Mobile Wallet - OS	28
Google Pay	29
PayPal	29
What are Mobile Wallets?	28
Online Dating Services	
Selecting a Dating Site - Data Sharing Options	16
Online Registration	
Identity Fields During Registration, By Service	35
Social Login	34
Photo Sharing Services	
Google Photos	15
Overview	14
Secure Chat Apps	
Choosing the Right Secure Chat App - Compatibility	20
Signal	21
What are Secure Chat Apps?	20
Smartphones	22–23
Traveling with Smartphones	24–25
Virtual Private Network (VPN)	
Choosing the Right VPN Service Provider - Compatibility	44
How to Establish and Connect to a VPN	45
Voice Over IP (VOIP)	
Benefits	42
Google Hangouts	43
The Table - Operating System	43
What is VOIP?	42

H

UNCLASSIFIED

HOME SAFETY

EXIF Removal	
EXIF Removal - Do's and Don'ts	26
Identity Implications	26
Facebook	
About	3
Facebook Mobile	
Local	5
Nearby Friends - Location Settings	5
Identity Theft Prevention	
Social Media Mining	38
Opting Out of Data Aggregators	36–37
Securing Home Wi-Fi Network	32–33
Virtual Private Network (VPN)	
What is a VPN?	44
Voice Over IP (VOIP)	
Disadvantages	42
What Is VOIP?	42
Windows 10	
Adjusting Windows 10's Privacy Settings	47
Cortana - Windows' Intelligent Personal Assistant	46

L

LINKED ACCOUNTS

Health Apps & Fitness Trackers	
Fitbit	31
MyFitnessPal	31
The table	30
Instagram	
Linked Accounts	9
LinkedIn	
Data Privacy and Advertising Settings	11
Mobile Wallets	
Risks of Using Mobile Wallets	28
Online Registration	
Social Login	34
Photo Sharing Services	
iOS Photos	14
Secure Chat Apps	
Secure Chat Apps - Do's and Don'ts	20
The Table - Linkages	20

LIVE STREAMING

Facebook Mobile	
Live Video Broadcast	5
Instagram	
Instagram Media Formats	8
Secure Chat Apps	
Snapchat	21
Voice Over IP (VOIP)	
Choosing a VOIP Provider	43

LOCATION

EXIF Data Removal	26–27
Facebook	
About	3
Recommended Settings	2
Facebook Mobile	4–5
Google+	
Circles - How You Share on Google+	13
Posting to Google+	12
Health Apps & Fitness Trackers	
Garmin Connect	31
Google Fit	31
The table	30
Instagram	
Managing Your Instagram Profile	8
Mobile Dating Apps	18–19
Mobile Wallets	28–29
Online Dating Services	
Overview	16
Registration Data	17
Online Registration	
Employment Information	34
Location Information	34
Username	34
Opting Out of Data Aggregators	
Data Aggregators - Do's and Don'ts	36
Photo Sharing Services	

M

MATCHING

Mobile Dating Apps	18–19
Online Dating Services	
Common Threats from Dating Sites	16
Match.com	17
Plenty of Fish	17

MICROSOFT

EXIF Data Removal	
Viewing and Removing EXIF Data in Window 10	27
Keeping Your Kids Safe Online	
Family Safety Services	41
Microsoft Edge Settings	40
Microsoft Family Safety	41
Secure Chat Apps	
Choosing the Right Secure Chat App	20
Virtual Private Network (VPN)	
Choosing the Right VPN Service Provider	44
Voice Over IP (VOIP)	
Benefits of VOIP	42
Skype	43
Table - Operating System	43
Windows 10	46–47

P

PASSWORDS

Health Apps & Fitness Trackers	
Samsung Health	31
Identity Theft Prevention	
Identity Theft Prevention - Do's and Don'ts	38
Instagram	
Account Registration - Privacy Tips	8
Keeping Your Kids Safe Online	
Microsoft Edge Settings - Passwords	40
Mobile Wallets	
Apple Pay - iPhone Only	29
Choosing the Right Mobile Wallet	28
Mobile Wallets - Do's and Don'ts	28
Online Registration	
Identity Fields During Registration, By Service	35
Username	34
Secure Chat Apps	
Secure Chat Apps - Do's and Don'ts	20
Securing Home Wi-Fi Network	
Changing Device/Account Login Settings	32
Choosing Strong Encryption	33
Creating a Network Name and Password	33
What to do if You Suspect Your Network has been Compromised	32
Wireless Network Basics	32
Smartphones	
Protecting Your Smartphone from Physical Access and	

UNCLASSIFIED

Malware Risks	22
Recommendations to Minimize Physical access and	
Malware Risks	22
Smartphones - Do's and Don'ts	22
Traveling with Smartphones	
Set Your Phone to Lock Automatically and Set a Complex	
Screenlock Password	24
Traveling with Smartphones - Do's and Don'ts	24
Virtual Private Network (VPN)	
How to Establish and Connect to a VPN	45
VPN Vulnerabilities	45
Voice Over IP (VOIP)	
Using VOIP Securely	42

PAYMENTS

Mobile Wallets	28–29
Secure Chat Apps	
Snapchat	21

PERMISSIONS

EXIF Data Removal	
iOS (v. 11.2.1)	26
Facebook	
Recommended Settings, Continued	3
Facebook Mobile	
Android Settings	4
iPhone Settings	4
Local	5
Nearby Friends - Location Settings	5
Keeping Your Kids Safe Online	
Net Nanny	41
LinkedIn	
Data Privacy and Advertising Settings	11
Mobile Dating Apps	
Selecting a Dating App	18
Mobile Wallets	
Google Pay	29
Mobile Wallets - Best Practices	29
Photo Sharing Services	
Flickr	15
Smartphones	
Smartphones - Do's and Don'ts	22
Wireless Protection and App Security Settings	23

PHISHING

Identity Theft Prevention	
Phishing Scams	38

PIN

Mobile Wallets	28–29
Secure Chat Apps	
Secure Chat Apps - Do's and Don'ts	20
Smartphones	
Protecting Your Smartphone from Physical Access and	
Malware Risks	22
Traveling Safely with Smartphones	
Set Your Phone to Lock Automatically and Set a Complex	
Screenlock Password	24

R

RELOCATING

Identity Theft Prevention	
Social Media Mining	38
Online Registration	
Location Information	34
Opting Out of Data Aggregators	36–37
Securing Home Wi-Fi Network	32–33
Virtual Private Network (VPN)	
What is a VPN?	44
Windows 10	
Adjusting Windows 10's Privacy Settings	47

S

SHARING PHOTOS, VIDEOS, AND LIVE CONTENT

UNCLASSIFIED

EXIF Data Removal	26–27
Facebook	2–3
Facebook Mobile	4–5
Google+	12–13
Instagram	8–9
Keeping Your Kids Safe Online	40–41
LinkedIn	10–11
Mobile Dating Apps	18–19
Online Dating Services	16–17
Online Registration	34–35
Photo Sharing Services	14–15
Secure Chat Apps	20–21
Twitter	6–7

T

TAGS

EXIF Data Removal	
Android (v. 7.0)	26
EXIF Removal - Do's and Don'ts	26
Important Tags	26
PhotoInfo Eraser for Android	27
Facebook	
Activity Log	3
Recommended Settings - Timeline and Tagging	2
Social Network - Do's and Don'ts	2
Facebook Mobile	
Social Network - Do's and Don'ts	4
Tag People	5
Instagram	
Instagram - Do's and Don'ts	8
Photos of You	9
Keeping Your Kids Safe Online	
Keeping Your Kids Safe Online - Do's and Don'ts	40
Photo Sharing Services	
Facebook	14
Google Photos	15
Overview	15
Twitter	
Posting to Twitter	6

THIRD-PARTY ACCESS

Health Apps & Fitness Trackers	
Fitbit	31
Third-party Data Sharing	30
Instagram	
Instagram - Do's and Don'ts	8
Privacy Settings	9
LinkedIn	
Data Privacy and Advertising Settings	11
Online Registration	
Online Registration - Do's and Don'ts	34
Photo Sharing Services	
Photo Sharing Services - Do's and Don'ts	14
Secure Chat Apps	
Vulnerabilities	20
What are Secure Chat Apps?	20
WhatsApp	21
Securing Home Wi-Fi Network	
Preventing Third Party Access to Your Wireless Network	32
Smartphones	
Protecting Your Smartphone from Physical Access and	
Malware Risks	22
Wireless Protection and App Security Settings	23
Virtual Private Network (VPN)	
VPN Vulnerabilities	45
TRACKING	
Facebook	
Recommended Settings, Continued	3
Facebook Mobile	
Local	5
Nearby Friends - Location Settings	5
Google+	
Circles - How You Share on Google+	13
Health Apps & Fitness Trackers	30–31
Keeping Your Kids Safe Online	
Firefox Settings	40

Norton Security Premium	41
Mobile Wallets	
Google Pay	29
Photo Sharing Services	
The Table - Location Options	14
Secure Chat Apps	
Signal	21
Smartphones	
Wireless Protection and App Security Settings.....	23
Windows 10	
Adjusting Windows 10's Privacy Settings	47

TRAVELING

EXIF Data Removal	26-27
Facebook Mobile	
Add Location	5
Google+	
Circles - How You Share on Google+	13
Mobile Wallets	
Google Pay	29
Photo Sharing Services	
Google Photos	15
Secure Chat Apps	
Snapchat	21
Smartphones	22-23
Traveling with Smartphones	24-25
Twitter	
Privacy and Safety	7
Windows 10	
Adjusting Windows 10's Privacy Settings	47
Cortana - Window's Intelligent personal assistant	46

V

VERIFICATION

Mobile Wallets	
Mobile Wallets - Best Practices	29
Square Cash	29
Online Dating Services	
Common Threats from Dating Sites	16
Online Registration	
Birthday	34
Mobile Phone Numbers	34
Online Registration and Verification Process	35
Opting Out of Data Aggregators	
Been Verified	37
Whitepages	37
Secure Chat Apps	
Secure Chat Apps - Do's and Don'ts	20
Securing Your Home Wi-Fi Network	
MAC Address Filtering	33
Voice Over IP (VOIP)	
Choosing a VOIP Provider: Best Uses	43

VISIBILITY

Facebook	
Deactivating/Deleting Your Facebook Account.....	3
Recommended Settings	2
Facebook Mobile	
Facebook Mobile Settings	4
Tag People	5
Google+	
Circles - How You Share on Google+	13
Posting to Google+	12
Target Audience	13
Instagram	
Instagram - Do's and Don'ts	8
Privacy Settings	9
LinkedIn	
1. Editing Your Public Profile	10
2. Profile Viewing Options	10
Profile Settings	10
Mobile Dating Apps	
Bumble	19
Coffee Meets Bagel	19
Tinder	19
Mobile Wallets	
Default Visibility	28
Venmo	29
Online Dating Services	
Match.com	17

Opting Out of Data Aggregators	36-37
Photo Sharing Services	
Photo Sharing Services - Do's and Don'ts	14
Twitter	
Posting to Twitter	6
Voice Over IP (VOIP)	
Skype	43
Viber	43

W

WI-FI

Health Apps & Fitness Trackers	
Overview	30
Identity Theft Prevention	
Fake Wi-Fi Networks	38
Mobile Wallets	
Mobile Wallets - Best Practices	29
Secure Chat Apps	
Choosing the Right Secure Chat App	20
Securing Home Wi-Fi Network	32-33
Smartphones	
Wireless Protection and App Security Settings.....	23
Traveling with Smartphones	
Disable Wi-Fi and Bluetooth	25
Protecting Your Phone Against Malware - Android (v 7.0) ...	24
Traveling with Smartphones - Do's and Don'ts.....	24
Use VPN on Wireless Networks	25
Virtual Private Network (VPN)	44-45
Voice Over IP (VOIP)	
What is VOIP?	42

NOTES

UNCLASSIFIED



UNCLASSIFIED