IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

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

THIRD EDITION, MAY 2016

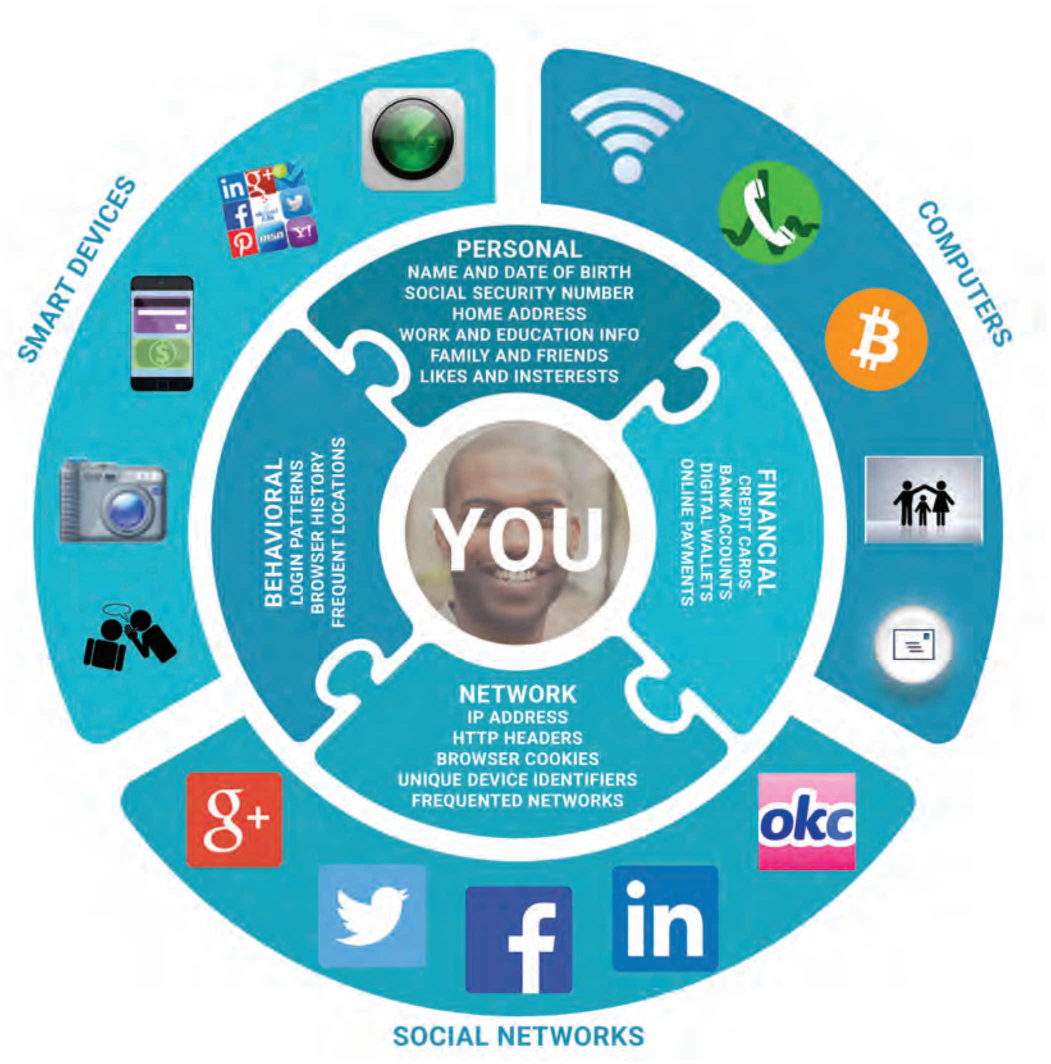
BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT

Constant Internet connectivity is increasingly becoming a necessity in today's fast-paced, interconnected world. Online services, devices, and networks increasingly share personal identity information—moving beyond the traditional name and date of birth to include behavioral patterns, purchasing history, and network of associates—to create the complex network that is your online identity.

Without knowing the common ways our data is collected, who is collecting it, and where it can end up, safeguarding our information becomes difficult. Fortunately, by following the recommendations presented in this guide, you can learn to better protect yourself, your friends, and your family online.



Your Total Online Identity: What Footprints Do You Leave?

TABLE OF CONTENTS

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
•	**Microsoft Safety and Security**	http://www.microsoft.com/security/online-privacy/social-network
•	**Online Guardian**	http://www.onguardonline.gov/topics/social-networking-sites.aspx
•	**About Money**	http://idtheft.about.com/od/identitytheft101/
•	**Protect My ID**	http://www.protectmyid.com/identity-theft-protection-resources
•	**Privacy Right Clearinghouse**	http://www.privacyrights.org/privacy-basics
•	**How to Disable Flash**	http://goo.gl/DQa6HJ
•	**How to Disable Java**	http://java.com/en/download/help/disable_browser.xml
•	**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.

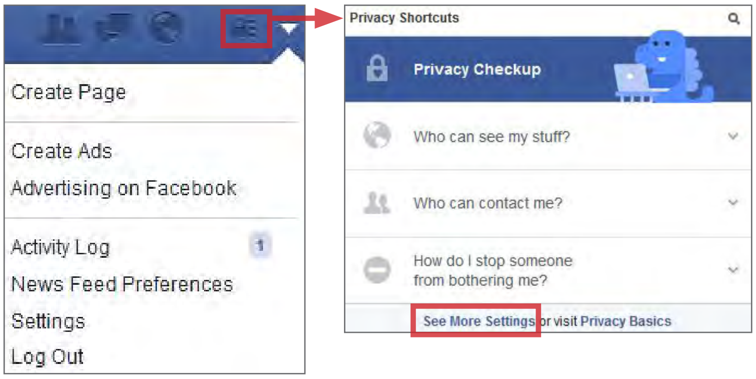
DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use 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.

FACEBOOK

SOCIAL NETWORK - DO'S AND DON'TS

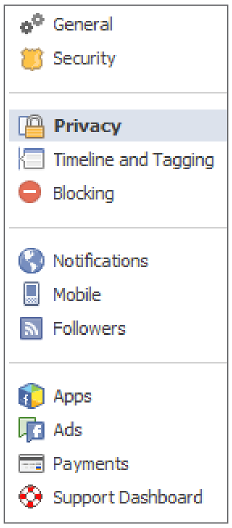
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; 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.
- Never post Smartphone photos and do not use your face as a profile photo; instead, use cartoons or avatars.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.

MINIMIZING YOUR FACEBOOK PROFILE



Facebook provides shortcuts to their privacy settings that help to limit what others can see in your profile. Select **Privacy Checkup** to change your basic privacy setting. For more extensive settings, click **See More Settings**. From there, navigate through the pages of the settings toolbar to control how your personal information is shared with others.

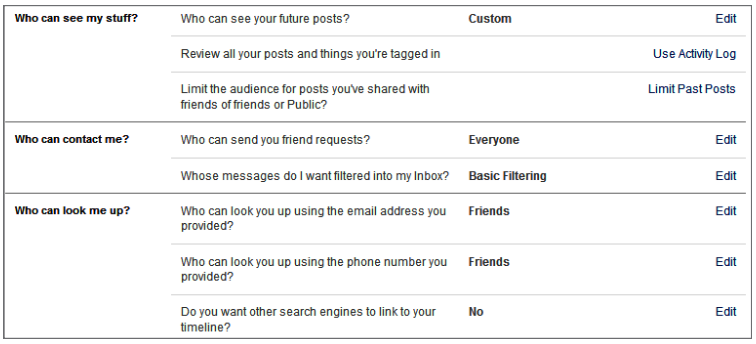
SETTINGS TOOLBAR



The (1) Privacy, (2) Timeline and Tagging, (3) Followers, (4) Security, (5) Ads, and (6) Apps tabs all contain settings for concealing personal information. Use the settings displayed below to maximize your online security.

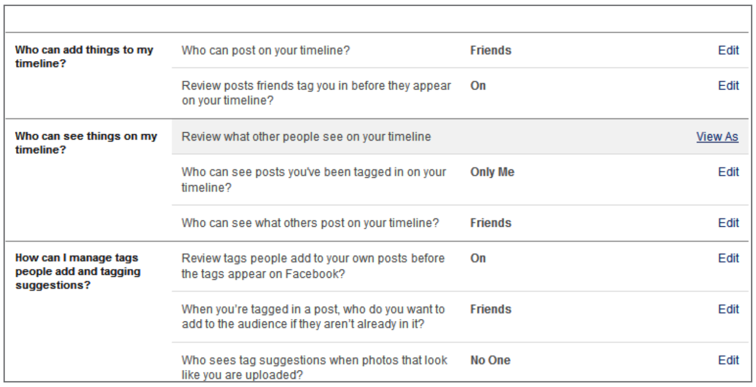
Remember, Facebook interactions such as likes and wall posts have been effectively used to profile individuals based on their behaviors. Try to minimize the amount of personal information that you post on your social networking services and limit your interactions.

1 Use the **Privacy** tab to declare which audiences can search for you, contact you, and see your posts. In general, it is best to limit the audiences to 'Friends' or 'Only Me'. The **Use Activity Log** selection can be used to review past posts individually and edit the audiences for each entry. The **Limit Past Posts** selection can be used to retroactively change the settings of all 'Public' posts to a 'Friends' only audience.



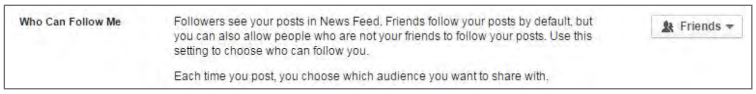
Who can see my stuff?	Who can see your future posts?	**Custom**	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	**Everyone**	Edit
	Whose messages do I want filtered into my Inbox?	**Basic Filtering**	Edit
Who can look me up?	Who can look you up using the email address you provided?	**Friends**	Edit
	Who can look you up using the phone number you provided?	**Friends**	Edit
	Do you want other search engines to link to your timeline?	**No**	Edit

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



Who can add things to my timeline?	Who can post on your timeline?	**Friends**	Edit
	Review posts friends tag you in before they appear on your timeline?	**On**	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	**Only Me**	Edit
	Who can see what others post on your timeline?	**Friends**	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	**On**	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	**Friends**	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	**No One**	Edit

3 **Followers** can view your post from their personal News Feeds. It is even possible for followers to view the content you post without being an accepted Facebook friend. Set **Who Can Follow Me** to 'Friends' only.



Who Can Follow Me

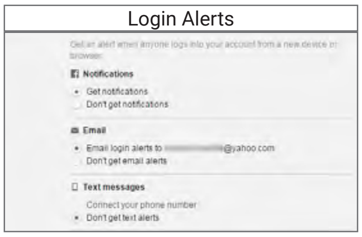
Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your posts. Use this setting to choose who can follow you.

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

Friends ▾

4 The **Security** tab provides ways to protect your credentials and become aware of suspicious login attempts. Use **Login Alerts** and **Where You're Logged In** to monitor login activity and end inactive sessions.

Login Alerts



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

Notifications

● Get notifications
○ Don't get notifications

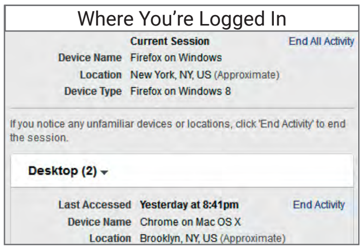
Email

● Email login alerts to [redacted]@yahoo.com
○ Don't get email alerts

Text messages

Connect your phone number
● Don't get text alerts

Where You're Logged In



	Current Session	End All Activity
Device Name	Firefox on Windows	
Location	New York, NY, US (Approximate)	
Device Type	Firefox on Windows 8	

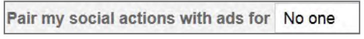
If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Desktop (2) ▾

Last Accessed	**Yesterday at 8:41pm**	End Activity
Device Name	Chrome on Mac OS X	
Location	Brooklyn, NY, US (Approximate)	

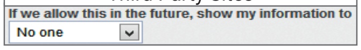
5 Use the **Ads** tab to prevent Facebook from using your data for advertising. Set **Third Party Sites** and **Ads & Friends** fields to 'No One'.

Ads and Friends



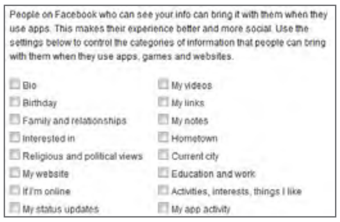
Pair my social actions with ads for No one

Third Party Sites



If we allow this in the future, show my information to No one ▾

6 Your Facebook contacts may be sharing your information with third party apps without your knowledge. Navigate **Apps > Apps Others Use** and uncheck all data fields to prevent others from sharing your data.



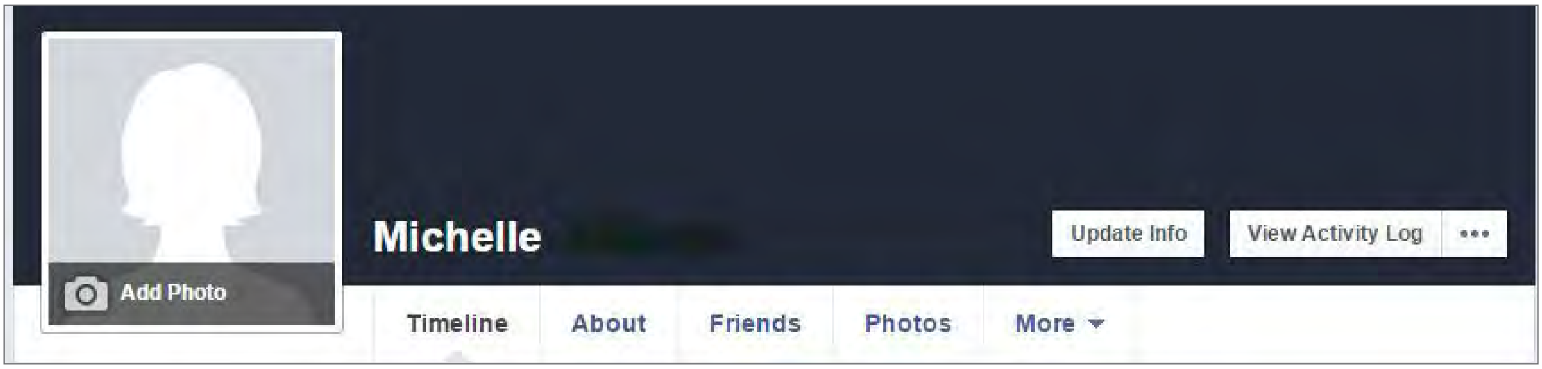
People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

□ Bio	□ My videos
□ Birthday	□ My links
□ Family and relationships	□ My notes
□ Interested in	□ Hometown
□ Religious and political views	□ Current city
□ My website	□ Education and work
□ If I'm online	□ Activities, interests, things I like
□ My status updates	□ My app activity

Avoid linking third-party apps (e.g. Twitter) with your Facebook account. Data shared with other apps becomes subject to their terms and conditions which may result in unwanted data aggregation and dissemination.

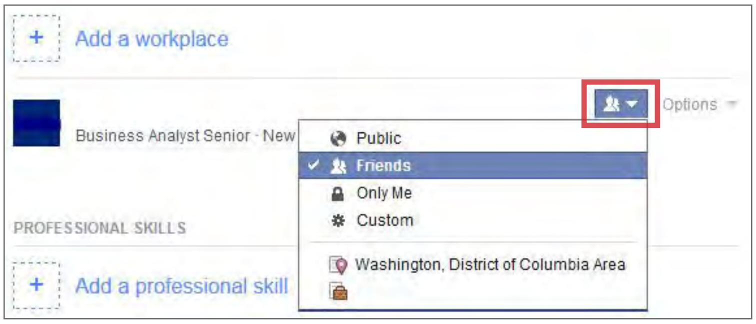
FACEBOOK PROFILE PAGE

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. Within these tabs reside general audience settings. Use the guidelines below to maximize your security while interacting with these features.



ABOUT

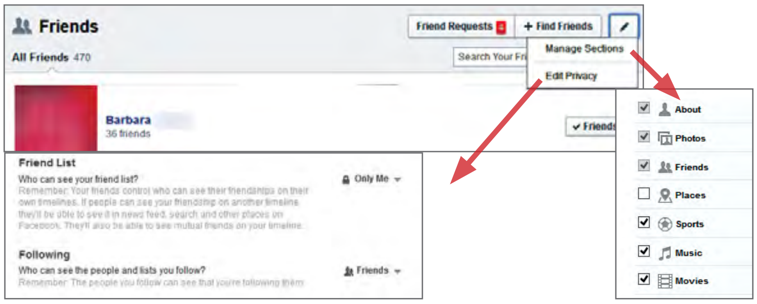
Avoid entering personal data within the **About** section. This information is mostly optional and contains data fields including **Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships,** and **Details About You**. Use the audience settings to change the mandatory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


+ Add a workplace
Business Analyst Senior · New
Options
Public
✓ Friends
Only Me
Custom
Washington, District of Columbia Area
PROFESSIONAL SKILLS
+ Add a professional skill

FRIENDS

Under the **Friends** Tab:

- Navigate **Manage > Edit Privacy** to change who can view your contacts. Limit your Friend List to 'Only Me'.
- Navigate **Manage > Manage Sections** to control which data fields will appear on your timeline. Avoid sharing places on your timeline and use discretion when posting information regarding your personal interests.



Friend List

Who can see your friend list? Only Me

Remember: Your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline they'll be able to see it in news feed, search and other places on Facebook. They'll also be able to see mutual friends on your timeline.

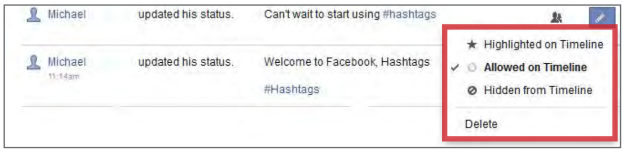
Following

Who can see the people and lists you follow? Friends

Remember: The people you follow can see that you're following them.

VIEW ACTIVITY LOG

The **View Activity Log** tool displays the information that is posted to your timeline in a chronological order. Use the dropdown menu shown to delete or manage how individual posts appear on your timeline.

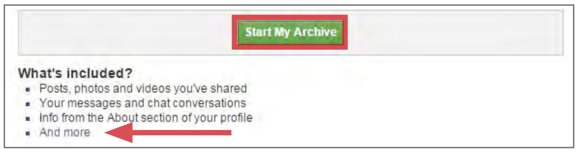


Michelle updated his status. Can't wait to start using #hashtags

Michelle 11:14am updated his status. Welcome to Facebook, Hashtags #Hashtags

REVIEWING YOUR INFORMATION

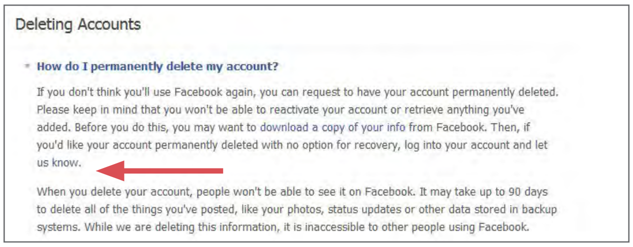
To review a comprehensive list of data collected by Facebook, navigate **Settings > Download a Copy of your Facebook Data > And More**. Select **Start My Archive** to view a personalized report of the data collected on you.



What's included?

- Posts, photos and videos you've shared
- Your messages and chat conversations
- Info from the About section of your profile
- And more

DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT



Deleting Accounts

How do I permanently delete my account?

If you don't think you'll use Facebook again, you can request to have your account permanently deleted. Please keep in mind that you won't be able to reactivate your account or retrieve anything you've added. Before you do this, you may want to download a copy of your info from Facebook. Then, if you'd like your account permanently deleted with no option for recovery, log into your account and let us know.

When you delete your account, people won't be able to see it on Facebook. It may take up to 90 days to delete all of the things you've posted, like your photos, status updates or other data stored in backup systems. While we are deleting this information, it is inaccessible to other people using Facebook.

Deactivating an account removes your name and photos from things that you have shared. To deactivate your Facebook account, navigate to **Settings > Security > Deactivate Your Account**. Your account remains deactivated until your next login.

To delete your Facebook account, select **Help** from the triangle icon's dropdown menu and select **Visit the Help Center**. Navigate **Manage Your Account > Deactivating, Deleting & Memorializing Accounts > How Do I Permanently Delete My Account > Let Us Know**. Verify that you wish to delete your account by clicking **Delete My Account**. Facebook will permanently remove most of your data within 90 days of submission.

FACEBOOK MOBILE

SOCIAL NETWORK - DO'S AND DON'TS

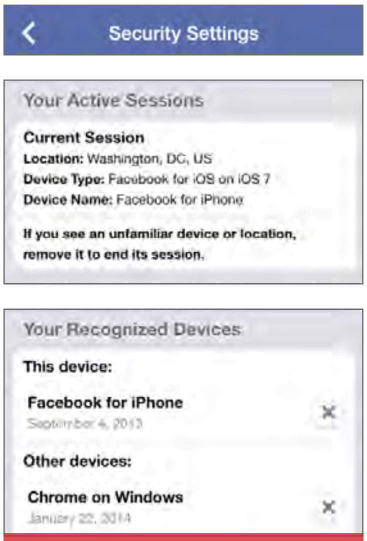
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that anyone can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their account; 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 other parties.

FACEBOOK MOBILE OVERVIEW

As of January 2015, Facebook Mobile hosted 745 million daily mobile active users who accounted for over 60% of all the mobile posts published to any online social networking service. Though privacy is still achievable, these mobile users place their personal identity data at a greater risk when compared to users logging in via desktop computer. This is in large part due to the fact that mobile devices provide Facebook with a means to access additional location information, contact lists, photos, and other personal data. Use the following recommendations to best protect yourself against over-sharing.

FACEBOOK MOBILE SETTINGS

Facebook Mobile's general security settings closely resemble those of Facebook's desktop application. Click **More** on the Facebook banner and select **Settings**. From there, navigate through the **Security**, **Privacy**, **Timeline and Tagging**, and **Locations** tabs to apply the settings shown below.



Security Settings

Your Active Sessions

Current Session
Location: Washington, DC, US
Device Type: Facebook for iOS on iOS 7
Device Name: Facebook for iPhone

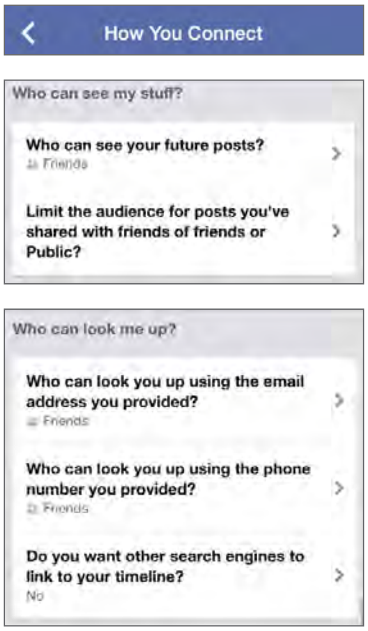
If you see an unfamiliar device or location, remove it to end its session.

Your Recognized Devices

This device:
Facebook for iPhone ×
September 4, 2013

Other devices:
Chrome on Windows ×
January 22, 2014

Review your active sessions and devices frequently to spot unauthorized activity



How You Connect

Who can see my stuff?

Who can see your future posts? ›
Friends

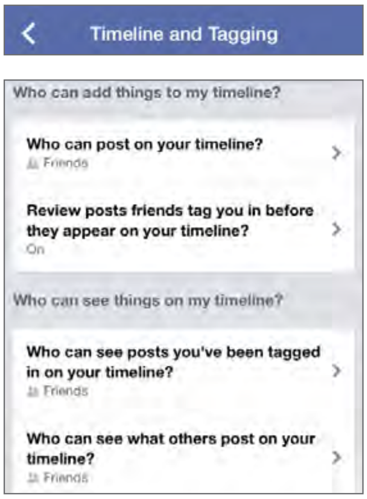
Limit the audience for posts you've shared with friends of friends or Public? ›

Who can look me up?

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 other search engines to link to your timeline? ›
No



Timeline and Tagging

Who can add things to my timeline?

Who can post on your timeline? ›
Friends

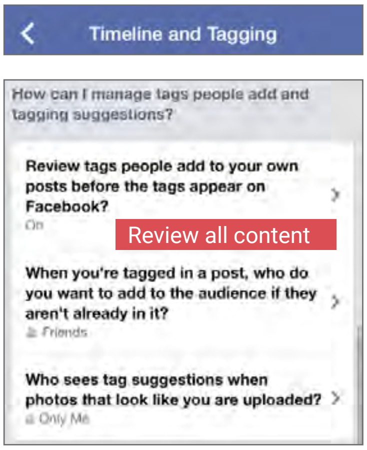
Review posts friends tag you in before they appear on your timeline? ›
On

Who can see things on my timeline?

Who can see posts you've been tagged in on your timeline? ›
Friends

Who can see what others post on your timeline? ›
Friends

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



Timeline and Tagging

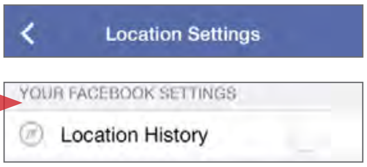
How can I manage tags people add and tagging suggestions?

Review tags people add to your own posts before the tags appear on Facebook? ›
On

Review all content

When you're tagged in a post, who do you want to add to the audience if they aren't already in it? ›
Friends

Who sees tag suggestions when photos that look like you are uploaded? ›
Only Me



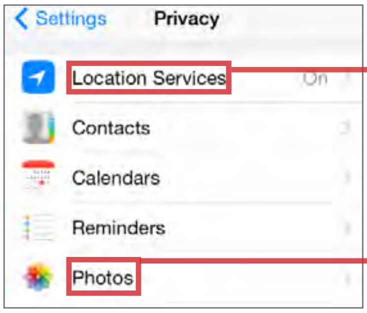
Location Settings

YOUR FACEBOOK SETTINGS

Location History

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

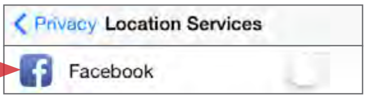
Location Services On

Contacts

Calendars

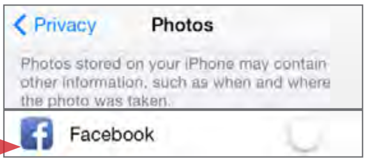
Reminders

Photos



Privacy Location Services

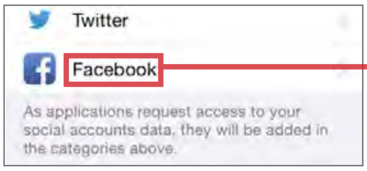
Facebook



Privacy Photos

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

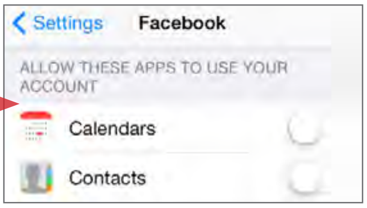
Facebook



Twitter

Facebook

As applications request access to your social accounts data, they will be added in the categories above.



Settings Facebook

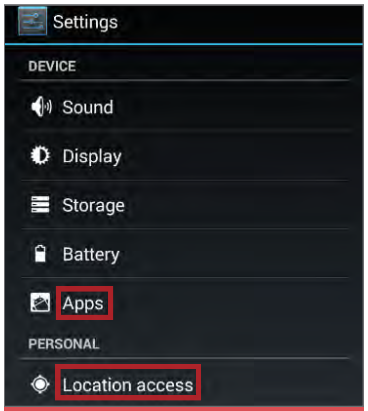
ALLOW THESE APPS TO USE YOUR ACCOUNT

Calendars

Contacts

ANDROID SETTINGS

Android phones can be configured to protect your personal data while you access the Facebook Mobile App. Access the phone's general **Settings** feature and navigate through the **Location Access** and **Apps** tabs to limit the types of data that Facebook can retrieve from your mobile device.



Settings

DEVICE

Sound

Display

Storage

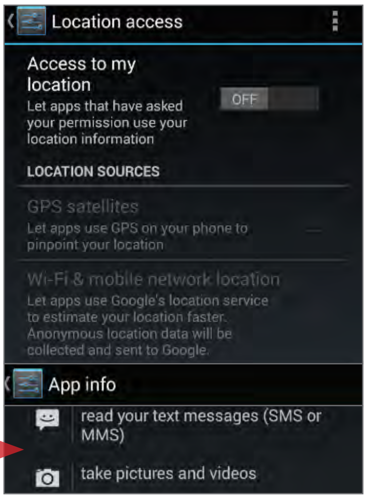
Battery

Apps

PERSONAL

Location access

Facebook is granted permission to do everything appearing under the App Info section.



Location access

Access to my location
Let apps that have asked your permission use your location information
OFF

LOCATION SOURCES

GPS satellites
Let apps use GPS on your phone to pinpoint your location

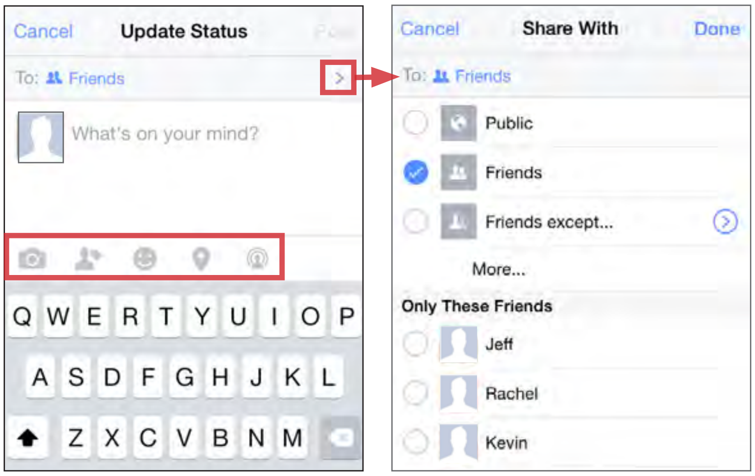
Wi-Fi & mobile network location
Let apps use Google's location service to estimate your location faster. Anonymous location data will be collected and sent to Google.

App info

read your text messages (SMS or MMS)

take pictures and videos

POSTING TO FACEBOOK



Facebook Mobile allows you to post new statuses, upload photos, or check-in to locations, using the **Update Status** prompt. The icons highlighted on the update prompt are shortcuts for adding further information about you to each post. Four of these five 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 when posting to Facebook.

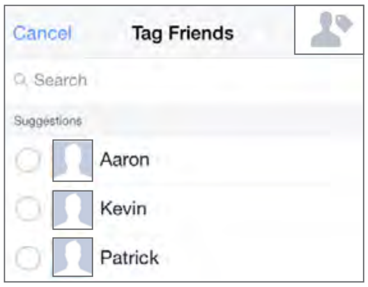
SELECTING YOUR AUDIENCE

With every post, Facebook Mobile allows you to select the audience through the **Share With** prompt. For maximum privacy, select individual friends with whom you would like to share your post. Never make your posts available to the public.

ADD PHOTOS

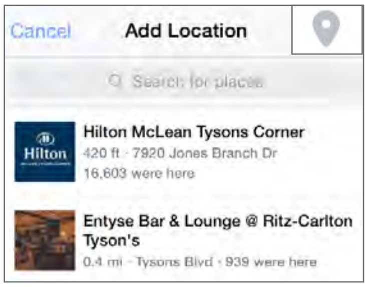
Avoid posting photos to timelines. These photos can often be viewed from your contacts' profile pages and can be saved without your knowledge or consent.

TAG FRIENDS



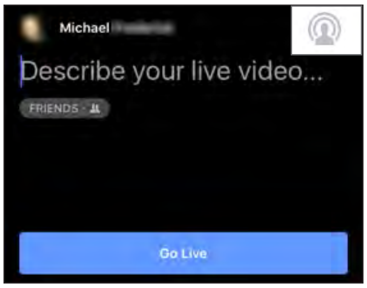
Tagging friends in individual posts extends the reach of your profile and your contacts' profiles. Limit the number of tags you post to your Facebook entries.

ADD LOCATION


Cancel
Add Location
Search for places
Hilton McLean Tysons Corner
420 ft · 7920 Jones Branch Dr
16,603 were here
Entyse Bar & Lounge @ Ritz-Carlton Tyson's
0.4 mi · Tysons Blvd · 939 were here

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.

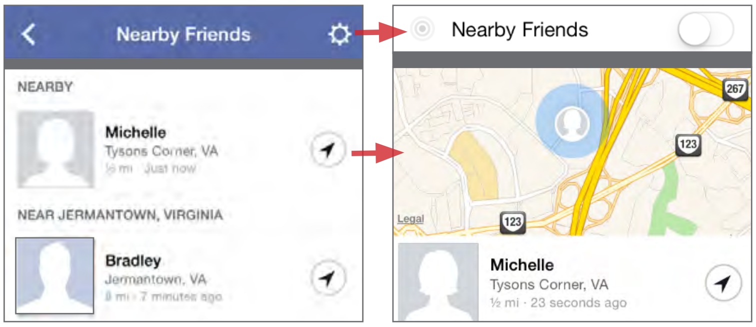
LIVE VIDEO BROADCAST



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

NEARBY FRIENDS

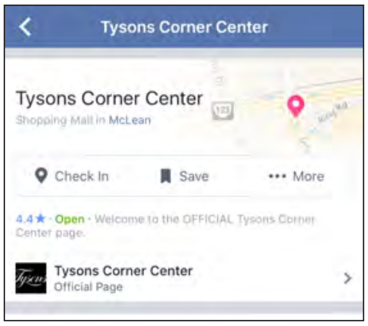
Nearby Friends allows you to share your location with friends. When activated, it continually broadcasts your approximate locations to your friends. You also have the option to allow certain users to see your precise location for set periods of time.

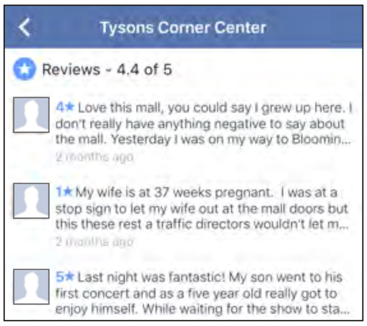


When this feature is enabled, Facebook builds a history of your precise location. You can view and manage this information from the **Activity Log**. In general, avoid giving Facebook permission to track your location.

NEARBY PLACES

Nearby Places uses your GPS location to display local venues. When activated, the feature permits check ins, provides a map to select locations, and shows other users' reviews about the venue. Individual reviews link back to the poster's Facebook profile. Avoid posting on these public threads.





4★ Love this mall, you could say I grew up here. I don't really have anything negative to say about the mall. Yesterday I was on my way to Bloomin...
2 months ago

1★ My wife is at 37 weeks pregnant. I was at a stop sign to let my wife out at the mall doors but this these rest a traffic directors wouldn't let m...
2 months ago

5★ Last night was fantastic! My son went to his first concert and as a five year old really got to enjoy himself. While waiting for the show to sta...

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

TWITTER

SOCIAL NETWORK - DO'S AND DON'TS

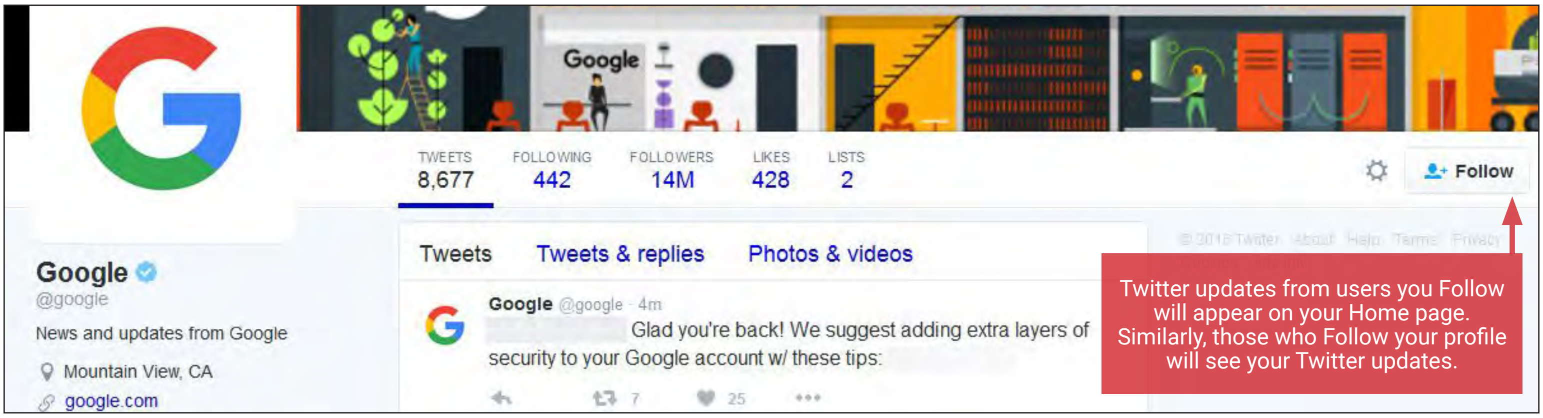
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that anyone can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting 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 other parties.

OVERVIEW

Twitter is a social networking and micro-blogging site that hosts more than 305 million monthly active users. The platform allows users to post text-based entries to their profiles and follow updates from other accounts. On average, Twitter users issue approximately 500 million entries per day from the web-based and mobile platforms combined. For most, Twitter is used as a source to discover breaking news coverages and staying 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 labelled 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 the account owner's personal identity data and display every Tweet posted by that user.



TWEETS 8,677 | FOLLOWING 442 | FOLLOWERS 14M | LIKES 428 | LISTS 2

Follow

Google
@google
News and updates from Google
Mountain View, CA
google.com

Tweets | Tweets & replies | Photos & videos

Google @google · 4m
Glad you're back! We suggest adding extra layers of security to your Google account w/ these tips:

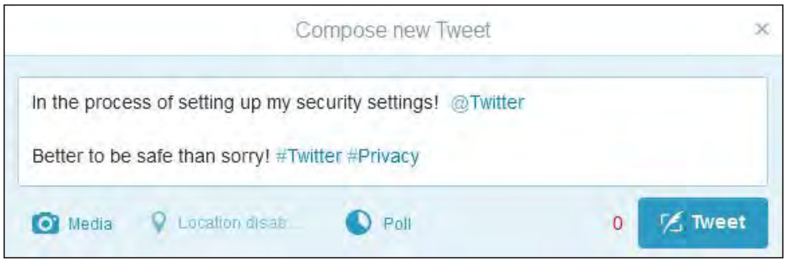
7 25

© 2016 Twitter About Help Terms Privacy

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

POSTING TO TWITTER

A Twitter entry is referred to as a "Tweet". Tweets can be composed of photos, videos, links, polls, or short text entries, limited to 140 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.

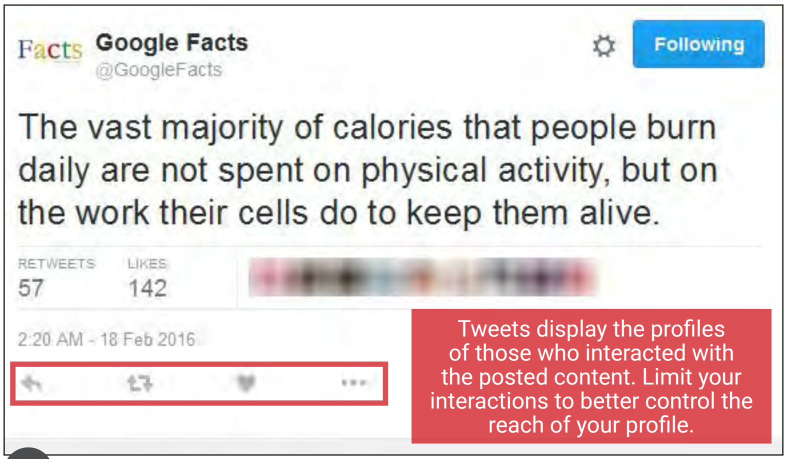


Compose new Tweet

In the process of setting up my security settings! @Twitter

Better to be safe than sorry! #Twitter #Privacy

Media | Location disab... | Poll | 0 | Tweet



Google Facts
@GoogleFacts
Following

The vast majority of calories that people burn daily are not spent on physical activity, but on the work their cells do to keep them alive.

RETWEETS 57 | LIKES 142

2:20 AM - 18 Feb 2016

Tweets display the profiles of those who interacted with the posted content. Limit your interactions to better control the reach of your profile.

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 used by multiple 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.
- **More** - Additional actions include Share via Direct Message, Copy Link to Tweet, Embed Tweet, Embed Video, Mute, Block, and Report.

TWITTER SETTINGS

Access Twitter's settings by selecting the thumbnail image of your profile photo in the top banner of the webpage. From the dropdown menu, select **Settings** and locate the pages containing customizable security options: **Security and Privacy, Account, Web Notifications.** After configuring your settings, access **Your Twitter Data** to review the device and login histories to ensure that your account has not been accessed by unauthorized users.

SECURITY AND PRIVACY

Apply the settings shown below within the Security and Privacy tab to control how others can interact with your Twitter profile and your Tweets.

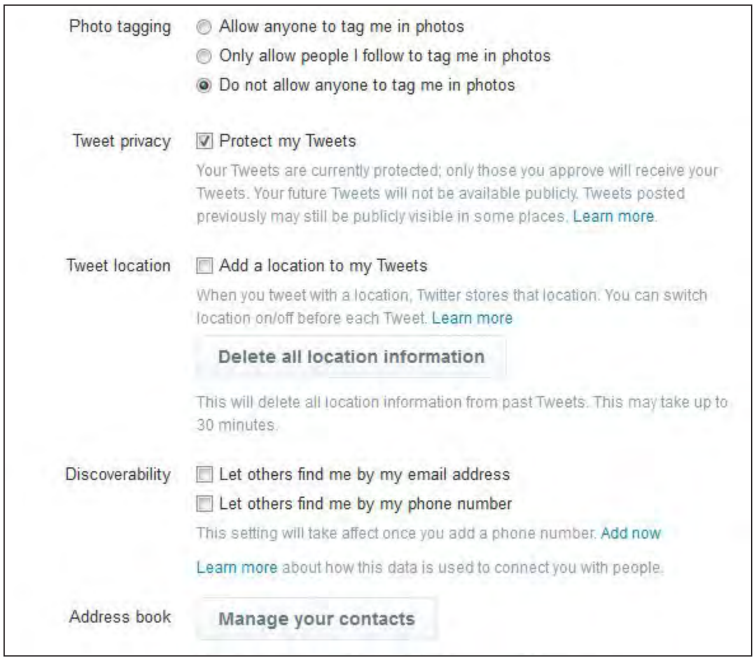


Photo tagging
○ Allow anyone to tag me in photos
○ Only allow people I follow to tag me in photos
● Do not allow anyone to tag me in photos

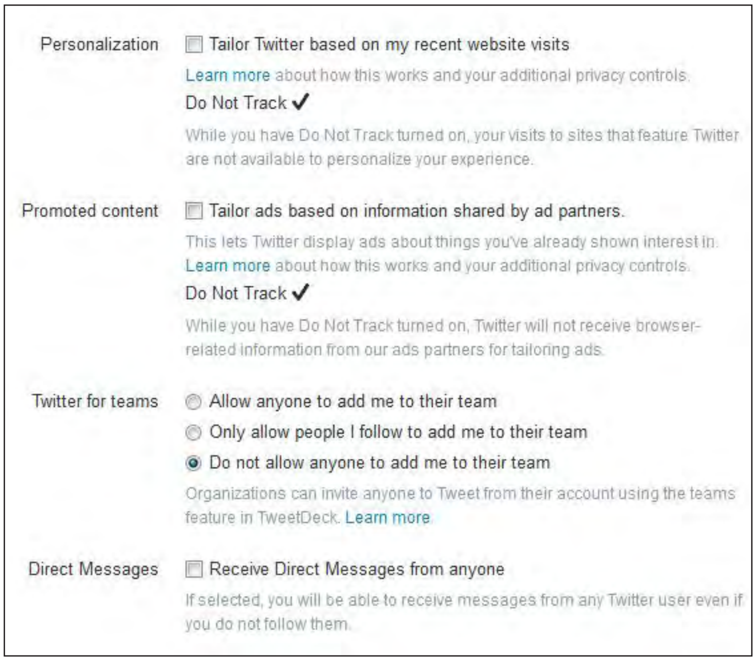
Tweet privacy
☑ Protect my Tweets
Your Tweets are currently protected; only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location
□ Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

This will delete all location information from past Tweets. This may take up to 30 minutes.

Discoverability
□ Let others find me by my email address
□ Let others find me by my phone number
This setting will take affect once you add a phone number. Add now
Learn more about how this data is used to connect you with people.

Address book



Personalization
□ Tailor Twitter based on my recent website visits
Learn more about how this works and your additional privacy controls.
Do Not Track ✓
While you have Do Not Track turned on, your visits to sites that feature Twitter are not available to personalize your experience.

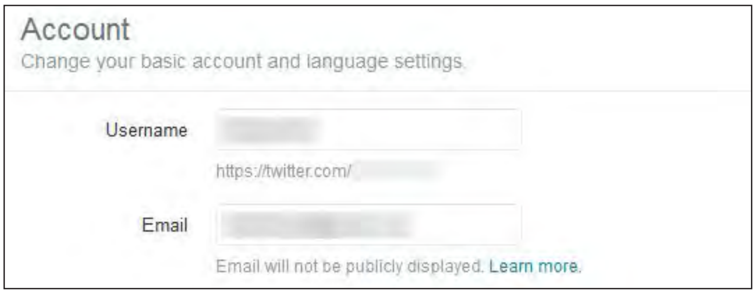
Promoted content
□ Tailor ads based on information shared by ad partners.
This lets Twitter display ads about things you've already shown interest in.
Learn more about how this works and your additional privacy controls.
Do Not Track ✓
While you have Do Not Track turned on, Twitter will not receive browser-related information from our ads partners for tailoring ads.

Twitter for teams
○ Allow anyone to add me to their team
○ Only allow people I follow to add me to their team
● Do not allow anyone to add me to their team
Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. Learn more

Direct Messages
□ Receive Direct Messages from anyone
If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

ACCOUNT SETTINGS

Account settings allow users to customize their Twitter handles and contact emails. Users can also request their Twitter archives which contain a transcript of all of their past Tweets or elect to deactivate theirs accounts.

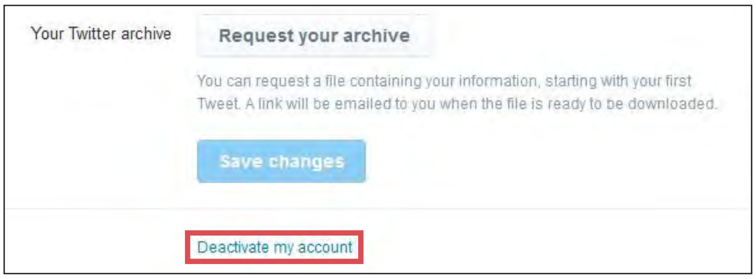


Account

Change your basic account and language settings.

Username [redacted]
https://twitter.com/[redacted]

Email [redacted]
Email will not be publicly displayed. Learn more.

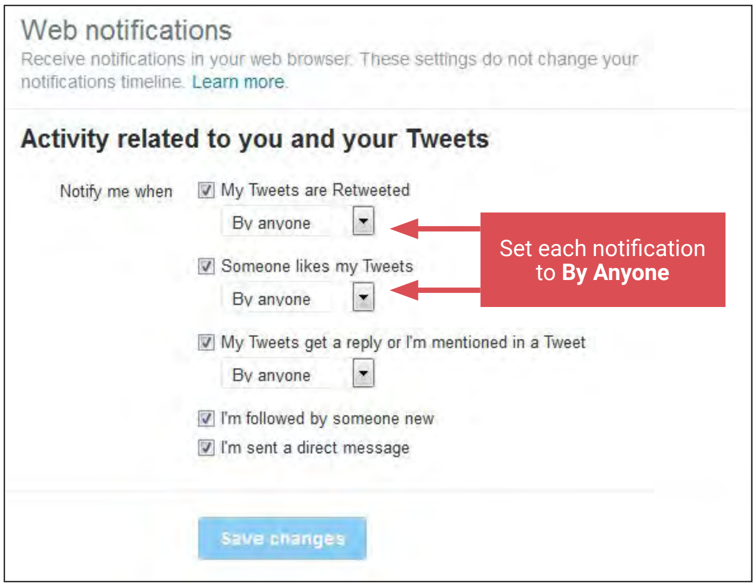


Your Twitter archive

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

NOTIFICATIONS

Email and web notifications alert users when others interact with their profiles or content. For maximum security, customize the notifications settings to receive as many alerts as possible.



Web notifications

Receive notifications in your web browser. These settings do not change your notifications timeline. Learn more.

Activity related to you and your Tweets

Notify me when
☑ My Tweets are Retweeted
By anyone
☑ Someone likes my Tweets
By anyone
☑ My Tweets get a reply or I'm mentioned in a Tweet
By anyone
☑ I'm followed by someone new
☑ I'm sent a direct message

Set each notification to **By Anyone**

LINKEDIN

SOCIAL NETWORK - DO'S AND DON'TS

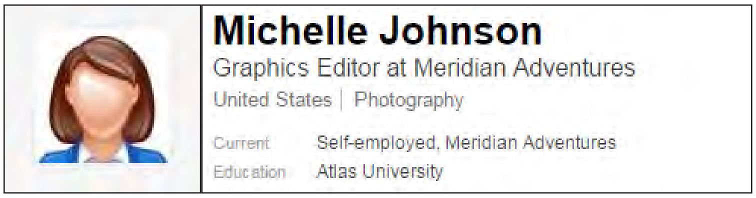
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting 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 other parties.

LINKEDIN OVERVIEW

LinkedIn is a professional networking service currently hosting more than 400 million users around the world. The site is primarily used by individuals looking to establish mutually beneficial professional relationships with companies, hiring managers, and other working professionals on the site. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar backgrounds. Though the site offers valuable services, LinkedIn profiles tend to have high visibility, even to people who are not within the network. For this reason, it is essential to limit the exposure of your information. Follow the recommendations on this card to better protect your data while using LinkedIn.

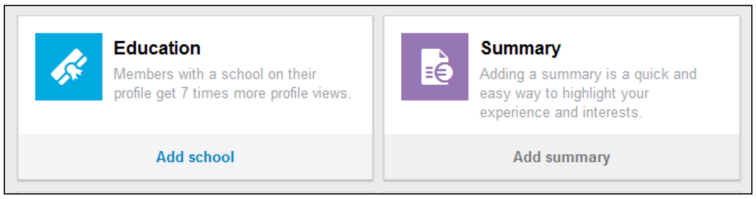
LINKEDIN PROFILE

A standard LinkedIn profile contains a user's profile picture and current position or education level. The information supplied beyond these fields is largely optional and should be limited to maximize privacy. The colored tiles on the user's profile page provide a means to include unique information.



Michelle Johnson
Graphics Editor at Meridian Adventures
United States | Photography

Current	Self-employed, Meridian Adventures
Education	Atlas University

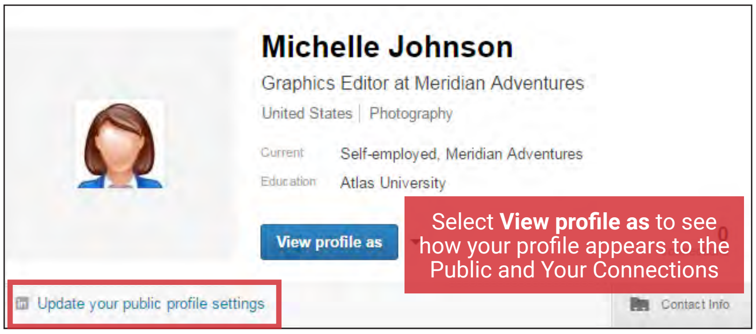


Education
Members with a school on their profile get 7 times more profile views.
Add school

Summary
Adding a summary is a quick and easy way to highlight your experience and interests.
Add summary

MINIMIZING PUBLIC PROFILES

By default, LinkedIn profiles can be discovered through public search engines. Due to the service's high visibility, it is imperative to change your public profile privacy settings to adjust how your data is presented. The images below show how your data may appear to the public on your LinkedIn profile page.

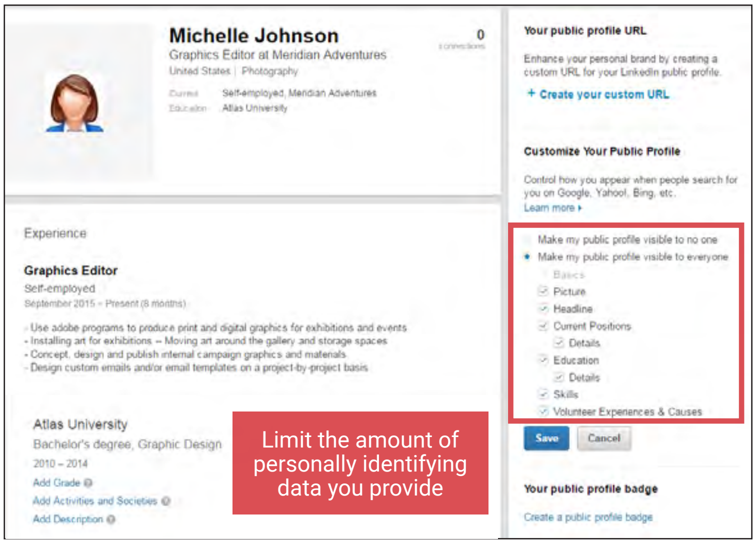


Michelle Johnson
Graphics Editor at Meridian Adventures
United States | Photography

Current	Self-employed, Meridian Adventures
Education	Atlas University

Select **View profile as** to see how your profile appears to the Public and Your Connections

Select **Update your public profile settings** to reveal the prompt shown to the right. This prompt controls how your LinkedIn data appears on public search engines such as Google, Yahoo!, or most notably, Bing. It is recommended that you make your public profile visible to no one in order to limit the reach of your data. If you wish to still remain visible to everyone, use the basic filters to uncheck sensitive data fields such as your picture and the details of your current position or educational programs.



Michelle Johnson 0 connections
Graphics Editor at Meridian Adventures
United States | Photography

Current	Self-employed, Meridian Adventures
Education	Atlas University

Experience

Graphics Editor
Self-employed
September 2015 – Present (8 months)

- Use adobe programs to produce print and digital graphics for exhibitions and events
- Installing art for exhibitions – Moving art around the gallery and storage spaces
- Concept, design and publish internal campaign graphics and materials
- Design custom emails and/or email templates on a project-by-project basis

Atlas University
Bachelor's degree, Graphic Design
2010 – 2014
Add Grade
Add Activities and Societies
Add Description

Your public profile URL
Enhance your personal brand by creating a custom URL for your LinkedIn public profile.
+ Create your custom URL

Customize Your Public Profile
Control how you appear when people search for you on Google, Yahoo!, Bing, etc.
Learn more ▸

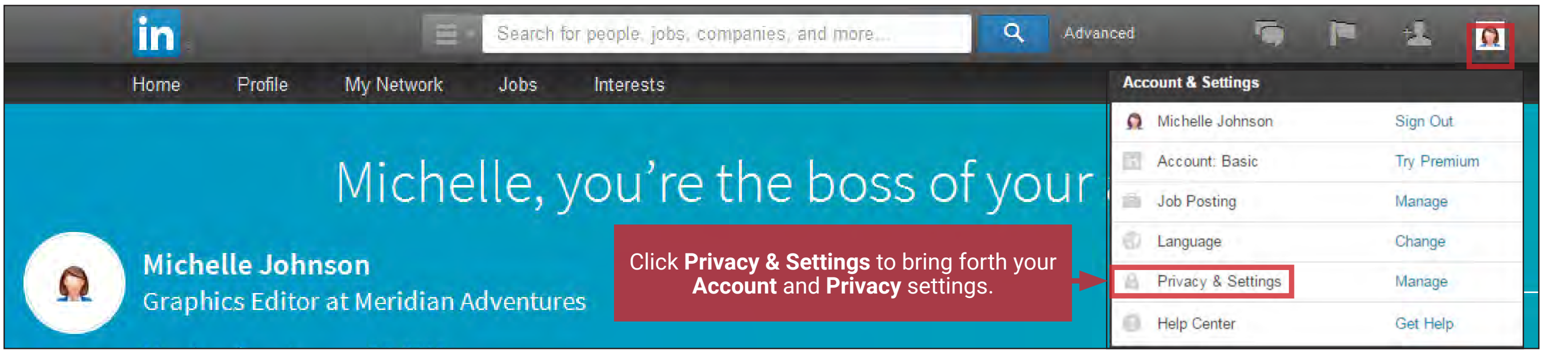
○ Make my public profile visible to no one
● Make my public profile visible to everyone
- Basics
- ☑ Picture
- ☑ Headline
- ☑ Current Positions
  - ☑ Details
- ☑ Education
  - ☑ Details
- ☑ Skills
- ☑ Volunteer Experiences & Causes

Save Cancel

Your public profile badge
Create a public profile badge

Limit the amount of personally identifying data you provide

Click the **Privacy & Settings** tab, shown in the image below, to reveal additional **Account**, **Privacy**, and **Communication** settings for your LinkedIn profile.



Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Michelle, you're the boss of your
Michelle Johnson
Graphics Editor at Meridian Adventures

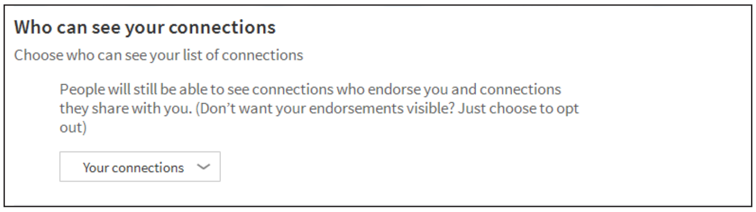
Account & Settings

Michelle Johnson	Sign Out
Account: Basic	Try Premium
Job Posting	Manage
Language	Change
Privacy & Settings	Manage
Help Center	Get Help

Click **Privacy & Settings** to bring forth your **Account** and **Privacy** settings.

PRIVACY SETTINGS

Apply the **Privacy** settings shown below to control how your data is displayed and to ensure that your information is visible only to the people you authorize.

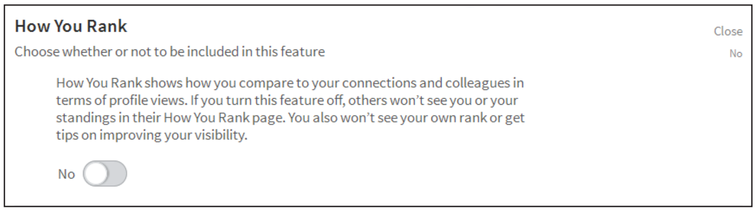


Who can see your connections

Choose who can see your list of connections

People will still be able to see connections who endorse you and connections they share with you. (Don't want your endorsements visible? Just choose to opt out)

Your connections ˅

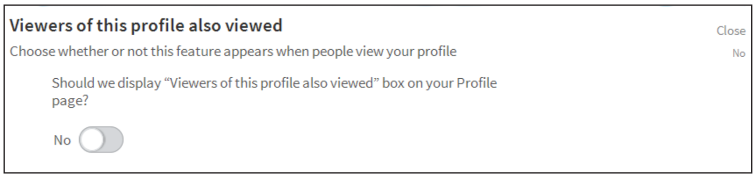


How You Rank Close

Choose whether or not to be included in this feature No

How You Rank shows how you compare to your connections and colleagues in terms of profile views. If you turn this feature off, others won't see you or your standings in their How You Rank page. You also won't see your own rank or get tips on improving your visibility.

No

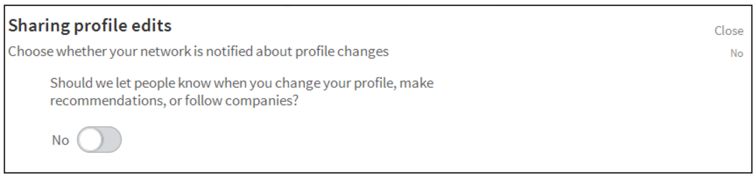


Viewers of this profile also viewed Close

Choose whether or not this feature appears when people view your profile No

Should we display "Viewers of this profile also viewed" box on your Profile page?

No

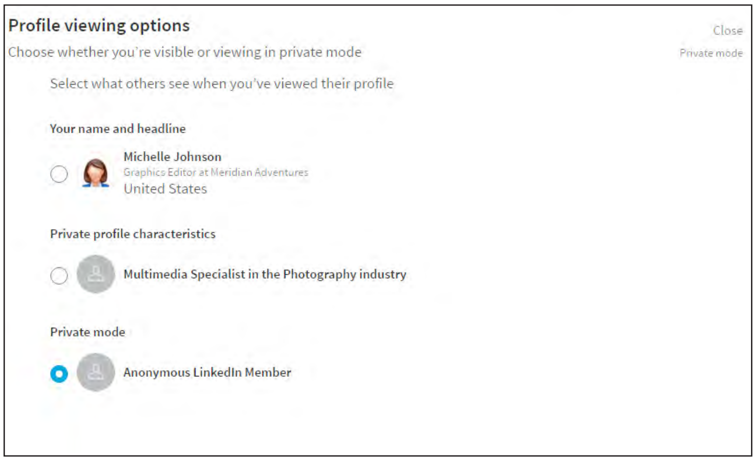


Sharing profile edits Close

Choose whether your network is notified about profile changes No

Should we let people know when you change your profile, make recommendations, or follow companies?

No



Profile viewing options Close

Choose whether you're visible or viewing in private mode Private mode

Select what others see when you've viewed their profile

Your name and headline

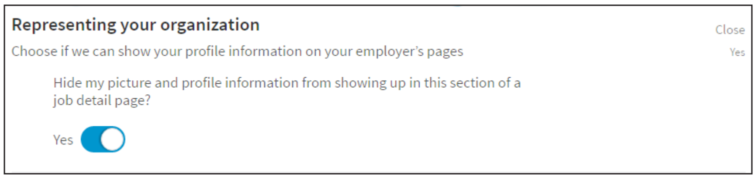
○ Michelle Johnson
Graphics Editor at Meridian Adventures
United States

Private profile characteristics

○ Multimedia Specialist in the Photography industry

Private mode

● Anonymous LinkedIn Member

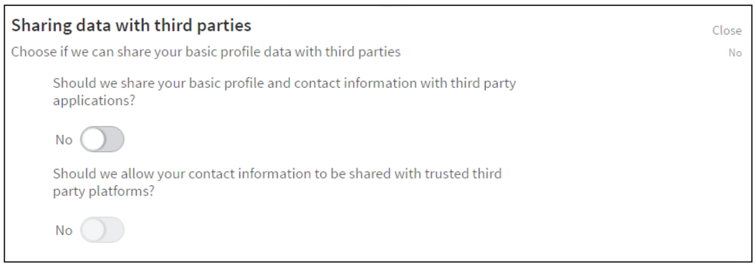


Representing your organization Close

Choose if we can show your profile information on your employer's pages Yes

Hide my picture and profile information from showing up in this section of a job detail page?

Yes



Sharing data with third parties Close

Choose if we can share your basic profile data with third parties No

Should we share your basic profile and contact information with third party applications?

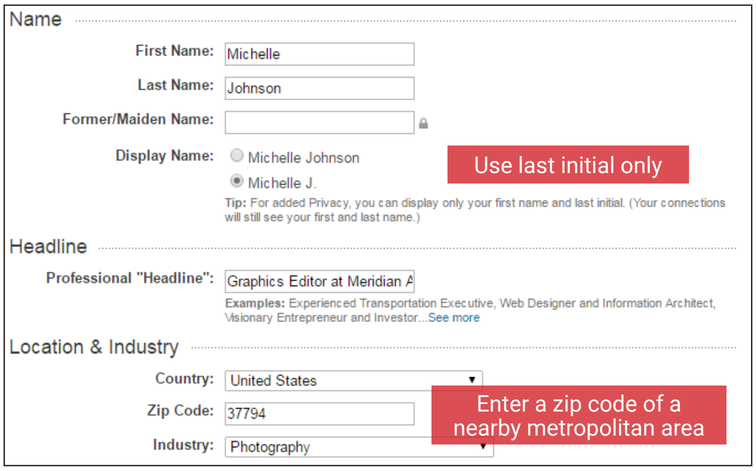
No

Should we allow your contact information to be shared with trusted third party platforms?

No

ACCOUNT SETTINGS

Apply the **Account** settings shown below to limit the amount of data you display and control who has access to your data.



Name

First Name:	Michelle
Last Name:	Johnson
Former/Maiden Name:	
Display Name:	○ Michelle Johnson ● Michelle J.

Tip: For added Privacy, you can display only your first name and last initial. (Your connections will still see your first and last name.)

Use last initial only

Headline

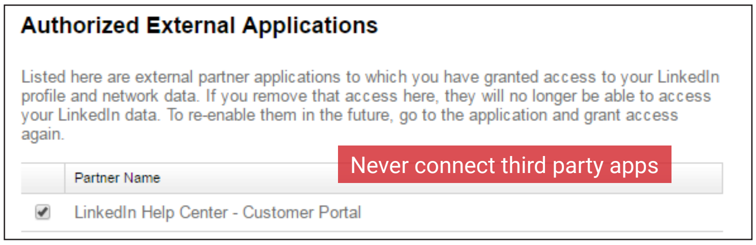
Professional "Headline": Graphics Editor at Meridian A

Examples: Experienced Transportation Executive, Web Designer and Information Architect, Visionary Entrepreneur and Investor...See more

Location & Industry

Country:	United States
Zip Code:	37794
Industry:	Photography

Enter a zip code of a nearby metropolitan area

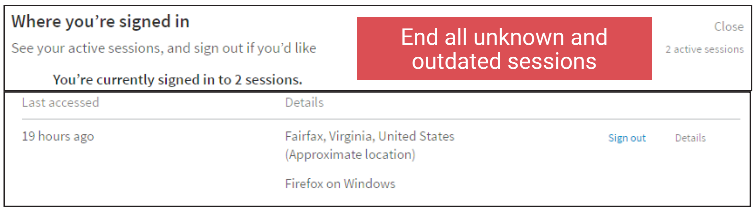


Authorized External Applications

Listed here are external partner applications 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.

	Partner Name
☑	LinkedIn Help Center - Customer Portal

Never connect third party apps



Where you're signed in Close

See your active sessions, and sign out if you'd like 2 active sessions

You're currently signed in to 2 sessions.

Last accessed	Details		
19 hours ago	Fairfax, Virginia, United States (Approximate location) Firefox on Windows	Sign out	Details

End all unknown and outdated sessions

LinkedIn maintains an archive of each individual's unique account activity. To request a copy of your archived data, select **Account > Getting an archive of your data**. In time, LinkedIn will provide you with a comprehensive report of your activities including account data, past posts, connections, and other network interactions. Review your data frequently to ensure that you are not over-sharing information. If you no longer plan to use the LinkedIn service, click **Account > Closing your account** and follow the subsequent prompts to unsubscribe from LinkedIn and officially close your account.

GOOGLE PLUS

SOCIAL NETWORK - DO'S AND DON'TS

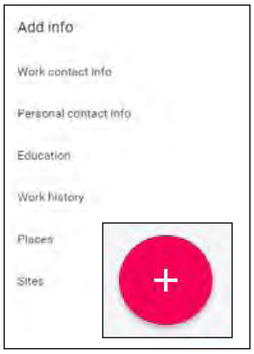
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post or share about your activities, personal life, or professional life.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you, or your family, that clearly show faces. Pictures of individuals should be taken at a distance or a severe angle.
- 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 other parties.

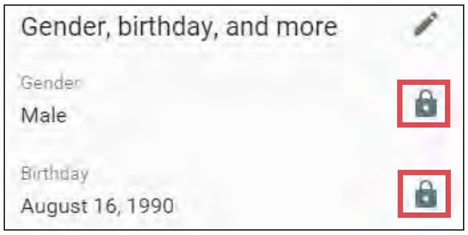
OVERVIEW

Google Plus is a social networking site visited by approximately 300 million monthly active users. Like other social networking sites, Google Plus provides a platform for its users to connect and share media. However, Google also uses these profiles to identify individuals interacting with other Google properties including YouTube, Gmail, Android services, and Google Search. These connections place users' identity data at greater risks because a unique identity can be linked to other online activity. Follow the recommendations on this card to help limit the information you share through your Google Plus profile.

PROFILE INFORMATION

Google Plus profiles can be used to share personally identifiable information. Most data fields such as work history, education, and contact information are optional and should not be entered. Mandatory data fields, including gender and birthday, should be set to private. From your profile, select **Edit Profile** followed by the **About Me** icon to manage these fields.





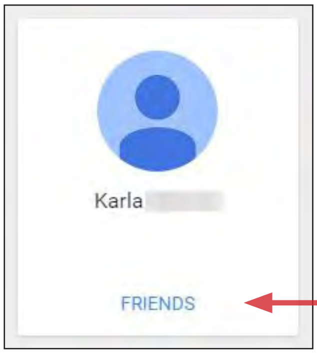
Gender
Male

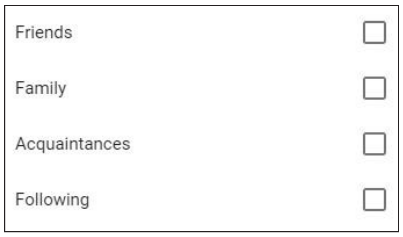
Birthday
August 16, 1990

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

FOLLOWERS

Your 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 posts appear from the people you follow. 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.

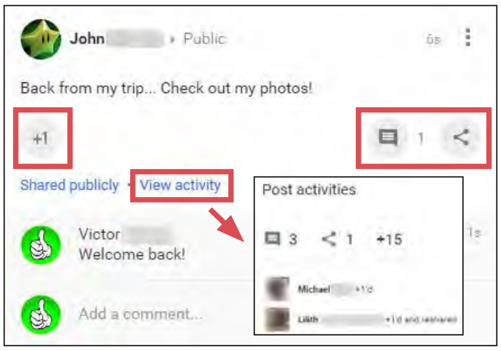




Avoid identifying family members. Limit your followers to the Friends or Following circles.

POSTING TO GOOGLE PLUS

Google Plus allows you to share photos, links, locations, and text entries with others in your circles. Once posted, the entries appear within your personal profile and become visible to others with whom you have given permission. Your followers can interact with the posts as seen in the examples below.



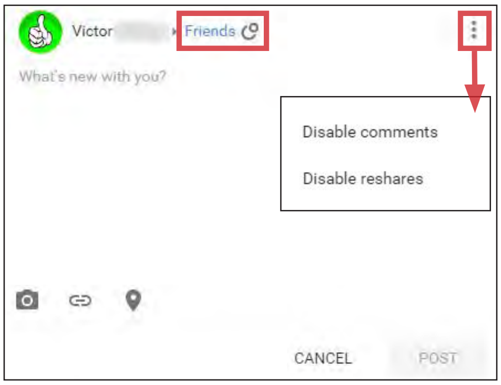
Back from my trip... Check out my photos!

Victor [redacted]
Welcome back!

Michael [redacted] +1'd
Lilith [redacted] +1'd and reshared

Viewers have the options to like, comment, or reshare individual posts. When they use one of these options, a clickable link to their profiles 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's "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 their recipients and distributed to new audiences.



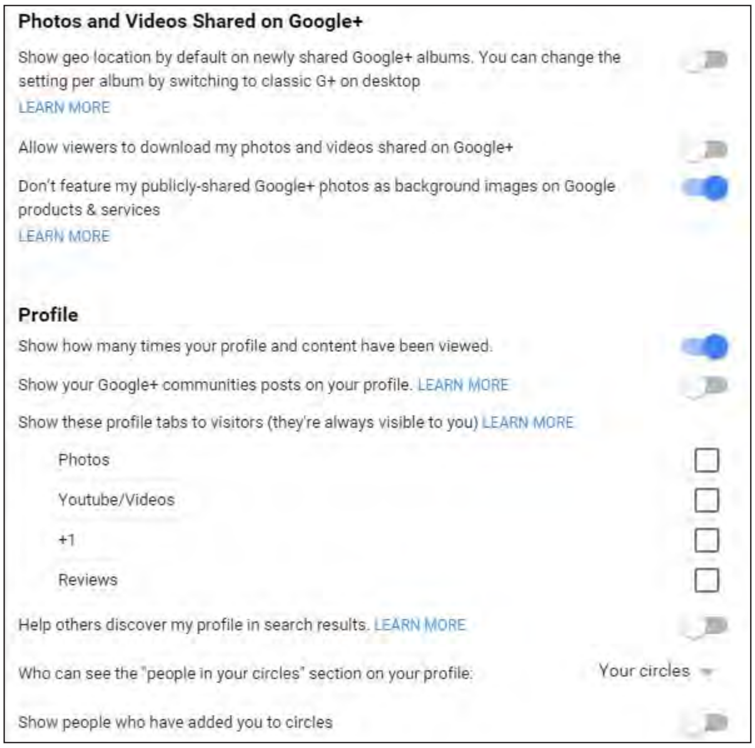
Select the **What's new with you?** prompt on your Home page to post a new entry to your profile. Each post can include up to four different types of content: text, photos, links, and locations. Avoid sharing links to other social profiles, photos that clearly show your face, or any of your frequented locations, as these may lead to unintended dissemination of your personal identity data.

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

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

PROFILE SETTINGS

Google offers extensive settings to secure your Google accounts. To locate the settings unique to your Google Plus 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.



Photos and Videos Shared on Google+

Show geo location by default on newly shared Google+ albums. You can change the setting per album by switching to classic G+ on desktop
LEARN MORE

Allow viewers to download my photos and videos shared on Google+

Don't feature my publicly-shared Google+ photos as background images on Google products & services
LEARN MORE

Profile

Show how many times your profile and content have been viewed.

Show your Google+ communities posts on your profile. LEARN MORE

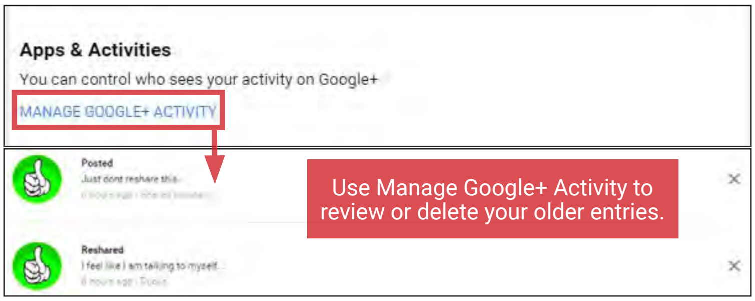
Show these profile tabs to visitors (they're always visible to you) LEARN MORE

- Photos □
- Youtube/Videos □
- +1 □
- Reviews □

Help others discover my profile in search results. LEARN MORE

Who can see the "people in your circles" section on your profile: Your circles

Show people who have added you to circles



Apps & Activities

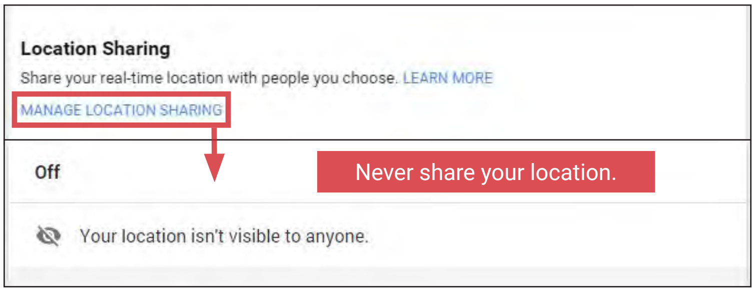
You can control who sees your activity on Google+

MANAGE GOOGLE+ ACTIVITY

Posted
Just dont reshare this.
6 hours ago · Shared privately

Reshared
I feel like I am talking to myself...
6 hours ago · Public

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



Location Sharing

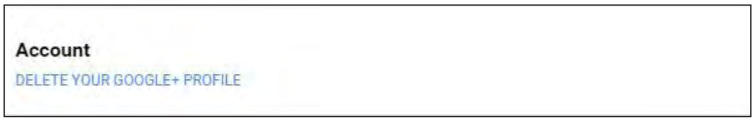
Share your real-time location with people you choose. LEARN MORE

MANAGE LOCATION SHARING

Off

Your location isn't visible to anyone.

Never share your location.

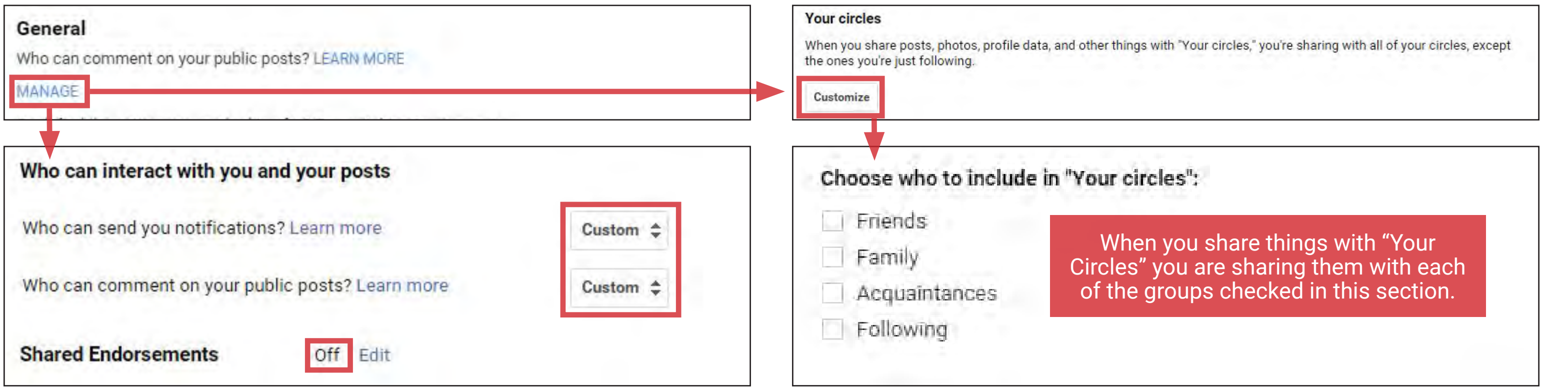


Account

DELETE YOUR GOOGLE+ PROFILE

GENERAL SETTINGS

Navigate to the top of the **Settings** page to manage your **General Settings**. General settings allow you to control who can see the content you share. Use the settings shown below, and reference the table at the bottom of this section, to help determine how you will share your data.



General

Who can comment on your public posts? LEARN MORE

MANAGE

Who can interact with you and your posts

Who can send you notifications? Learn more — Custom

Who can comment on your public posts? Learn more — Custom

Shared Endorsements Off Edit

Your circles

When you share posts, photos, profile data, and other things with "Your circles," you're sharing with all of your circles, except the ones you're just following.

Customize

Choose who to include in "Your circles":

- □ Friends
- □ Family
- □ Acquaintances
- □ Following

When you share things with "Your Circles" you are sharing them with each of the groups checked in this section.

AUDIENCE	WHO CAN SEE YOUR PROFILE DATA?	PRIVACY STRENGTH	RECOMMENDATIONS
Public	Anyone	None	Not Recommended
Extended Circles	People in your circles plus individuals from their circles	Minimal	Not Recommended
Your Circles	All of the individuals within the approved circles	Intermediate	Minimum Setting
Custom	Designated individuals or circles from your followers list	Strong	Recommended
Only You	No one except for you	Maximum	Recommended

PHOTO SHARING SERVICES

PHOTO SHARING SERVICES - DO'S AND DON'TS

- Only share photos with people you know and trust. Assume that ANYONE can see, 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 other 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.

PHOTO SHARING SERVICES OVERVIEW

Photo Sharing Services are online virtual photo albums that store, organize, and share your photos; many Social Networking Services (SNS) such as Facebook are also Photo Sharing Services. These services provide a convenient way to share photos, but can expose you to privacy risks if you do not take proper precautions. This Smart Card explains how you can change the security settings of six popular Photo Sharing Services to protect your privacy.

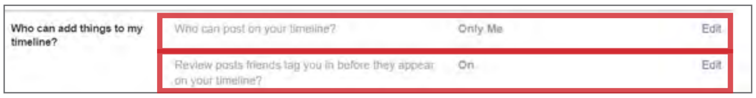
SERVICE	PRIMARY USE	PRIVACY OPTIONS?	EXIF?	LOCATION OPTIONS	ALLOW REPOSTING?	GOOGLE INDEXED?
facebook	Social Networking Site (SNS)	Public, Friends of Friends, Friends, Only Me	No	Can tag location to photos; geolocation suggestions	Yes	If Public
twitter	Social Networking Service (SNS)	Public, Private (requests to follow must be approved by the user)	No	Can tag location to photos; geolocation suggestions	Yes	If Public
Instagram	Share photos directly from mobile phones	Public, Private (requests to follow must be approved by the user)	No	Can tag location to photos; geolocation suggestions	No	If third-party apps enabled
flickr	Share photos within grouped user environments	Public, Private, Contacts, Family, Friends	Yes	Can tag location to photos, can embed location in EXIF data	Yes	If Public (can opt out)
imgur	Site dedicated to sharing and commenting on photos	Public, Private (images are only viewable with a direct URL); Albums can be set to Public, Hidden, or Secret	No	None (can add location to photo description)	Yes	If Public
Pinterest	Share concepts and ideas using images	Public, Private (with Secret Boards)	No	None (can add location to photo description)	Yes	If Public (can opt out)

FACEBOOK

Facebook is an SNS with 1.59 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**

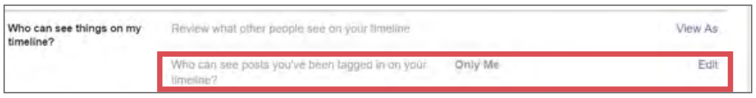


Who can add things to my timeline?

Who can post on your timeline? Only Me Edit

Review posts friends tag you in before they appear on your timeline? On Edit

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



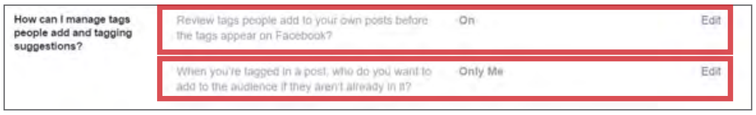
Who can see things on my timeline?

Review what other people see on your timeline View As

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

- Review tags people add to your own posts before the tags appear on Facebook?: **On**
- When you're tagged in a post, who do you want to add to the audience if they aren't already in it?: **Only Me**
- Who sees tag suggestions?: **No One**

For more information, see the Facebook Smart Card.



How can I manage tags people add and tagging suggestions?

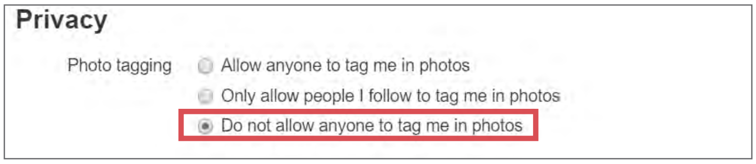
Review tags people add to your own posts before the tags appear on Facebook? On Edit

When you're tagged in a post, who do you want to add to the audience if they aren't already in it? Only Me Edit

TWITTER

Twitter is an SNS with 320 million active members. Users commonly Tweet photos of themselves and others. To maximize your privacy on Twitter, navigate to **Settings > Security and privacy > Privacy** and make the following change:

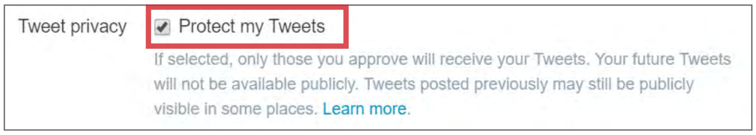
- Photo tagging: select **Do not allow anyone to tag me in photos**



Privacy

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

- Tweet privacy: select **Protect my Tweets**

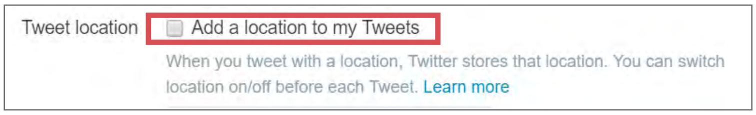


Tweet privacy ☑ Protect my Tweets

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: deselect **Add a location to my Tweets**
- Click **Delete all location information.**

This change will prevent others from viewing your location. For more information, see the Twitter Smart Card.



Tweet location □ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

PINTEREST

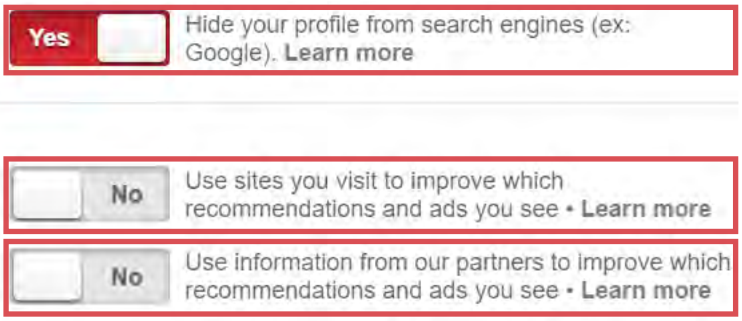
Pinterest is a site where users can upload, categorize, and share images called Pins on dedicated pages called Pin Boards. The site has more than 100 million active users.

To maximize your privacy on Pinterest, make the following modifications to your account settings. Go to **Settings > Account Basics** and make the following changes:

- Search Privacy: select **Yes - Hide your profile from search engines (ex: Google).**

In the **Personalization** section of the **Account Basics** Menu, make the following selections:

- **Use sites you visit to improve which recommendations and ads you see**: select **No**
- **Use information from our partners to improve which recommendations and ads you see:** select **No**

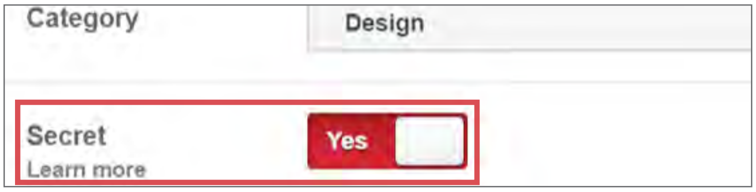


Yes — Hide your profile from search engines (ex: Google). **Learn more**

No — Use sites you visit to improve which recommendations and ads you see • **Learn more**

No — Use information from our partners to improve which recommendations and ads you see • **Learn more**

When you make a new Board in Pinterest, select the **Secret Boards** option to keep your Pins private.



Category — **Design**

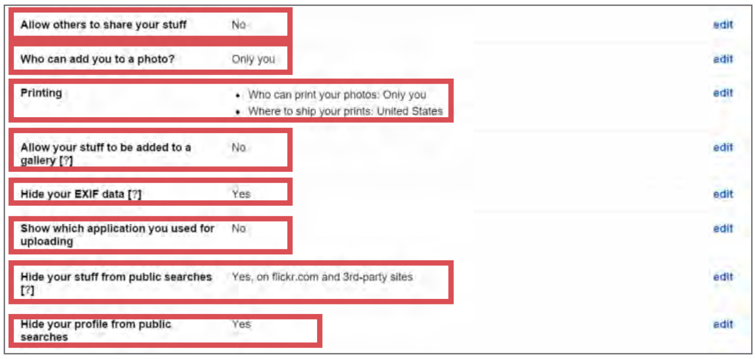
Secret — **Yes**

Learn more

FLICKR

Flickr is a site dedicated to sharing and editing photos. The site has more than 100 million active users. To maximize your privacy, go to **Settings > Privacy & Permissions** and make the following changes:

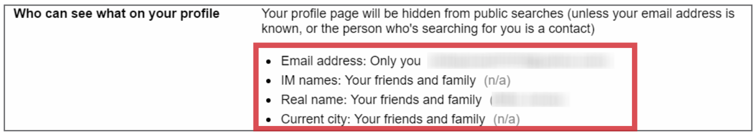
- Who can download your images? - **Only You**
- Allow others to share your stuff - **No**
- Who can add you to a photo? - **Only You**
- Who can print your photos - **Only You**
- Allow your stuff to be added to a gallery? - **No**
- Hide your EXIF data - **Yes**
- Show which application you used for uploading - **No**
- Hide your stuff from public searches - **Yes, on flickr and 3rd-party sites**



Allow others to share your stuff	No	edit
Who can add you to a photo?	Only you	edit
Printing	• Who can print your photos: Only you • Where to ship your prints: United States	edit
Allow your stuff to be added to a gallery [?]	No	edit
Hide your EXIF data [?]	Yes	edit
Show which application you used for uploading	No	edit
Hide your stuff from public searches [?]	Yes, on flickr.com and 3rd-party sites	edit
Hide your profile from public searches	Yes	edit

In the subsection of the Privacy Settings, **Who can see what on your profile**, make the following additional changes:

- Email address: **Only You**
- IM names: **Your friends and family**
- Real name: **Your friends and family**
- Current city: **Your friends and family**



Who can see what on your profile

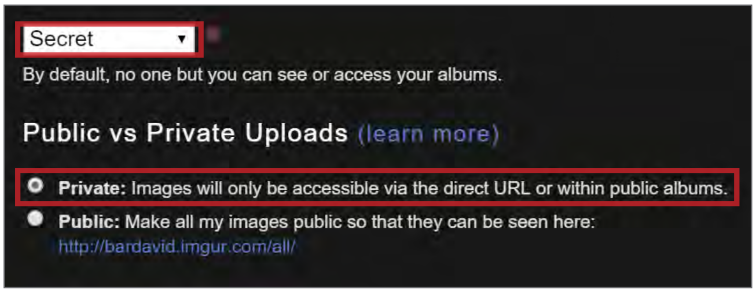
Your profile page will be hidden from public searches (unless your email address is known, or the person who's searching for you is a contact)

- Email address: Only you [redacted]
- IM names: Your friends and family (n/a)
- Real name: Your friends and family ([redacted]
- Current city: Your friends and family (n/a)

IMGUR

Imgur allows users to share photos and photo albums and to automatically post photos to other sites such as Reddit and Facebook. The site has more than 150 million active users. By default, Imgur strips all EXIF data from the photos you upload. However, to maximize your privacy on Imgur, you need to make a few additional simple modifications to your account settings. Navigate to **Account > Settings** and make the following changes:

- Default Album Privacy: select **Secret**
- Public vs Private Uploads: select **Private**



Secret ▾

By default, no one but you can see or access your albums.

Public vs Private Uploads (learn more)

● **Private:** Images will only be accessible via the direct URL or within public albums.

○ **Public:** Make all my images public so that they can be seen here: http://bardavid.imgur.com/all/

INSTAGRAM

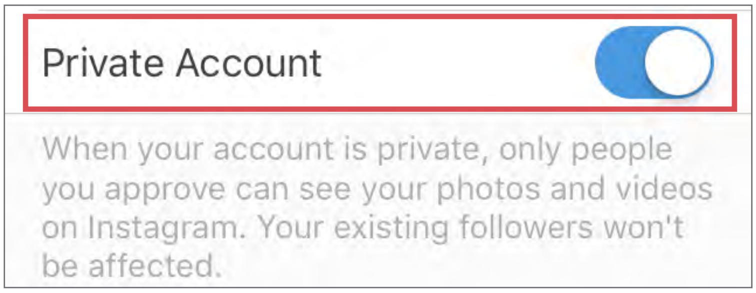
Instagram is a site dedicated to sharing and commenting on photos. The site has more than 400 million active users.

To maximize your privacy, make the following changes to your account settings:

Open the Instagram Mobile App on your Smartphone and then navigate to **Settings > Options > Account**

- Select **Private Account**

Now you can approve which followers can see your photos on Instagram.



Private Account

When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

ONLINE DATING SITES

ONLINE DATING SITES - DO'S AND DON'TS

- Do not link online dating profiles to your social networking or photo sharing services (e.g. Facebook and Instagram).
- Avoid using usernames and profile photos that appear on other social networking services.
- 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.
- 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 other parties.

OVERVIEW

Online dating services are used by individuals looking to develop a personal or romantic interest with others on the site. While each service is unique, sites typically ask users to maintain a public profile containing photos and personal information about themselves. These profiles are often searchable through the site and at times may be pushed to other users who share common interests or locations. Should you elect to participate in online dating, use the recommendations on this card to protect your website-based online dating services. For additional information about mobile, app-based services such as Tinder, Bumble, Hinge, or Coffee Meets Bagel, please reference the Mobile Dating section on page 18.

COMMON THREATS FROM DATING SITES

Online dating sites present a unique set of threats to users when compared to other social networking sites. Dating sites encourage interactions between unacquainted indviduals, require an increased amount of personal information used to match compatible individuals, and have minimal ways of verifying the accuracy of users' claims. Before participating in online dating, consider the following threats to your personal identity data:

- Sites use questionnaires to pair like-minded individuals, allowing the services to collect targetted 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 accounts' legitimacies.
- Matches may request personal contact information (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 THE PROPER DATING SITE

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 required by each online dating site, and select the service that best fits your privacy needs. Five of the top dating sites and their respective data requirements are outlined in the following table:

SITE	REGISTRATION INFORMATION	VISIBLE PROFILE INFORMATION	DATA SHARING OPTIONS	PRICING
Match	Name, gender, sexual orientation, email, ZIP code, birthdate, relationship status, biography	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 have invisible browsing; other features extra
OKCupid	Gender, sexual orientation, email, ZIP code, country, birthdate, biography, lifestyle questionnaire, photo	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; "A-List" membership (invisible browsing) ~ $10-$20/month
Plenty of Fish	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
Zoosk	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
eHarmony	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

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 required for proper site use

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

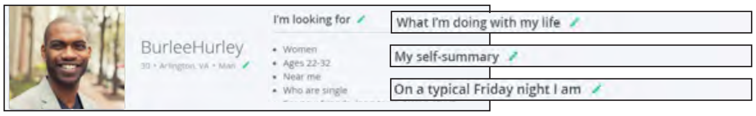
Current Location: Hackensack, NJ (Use New York, NY)
- Select a large metropolitan area / nearby zip code

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 ~2.9 million unique monthly visitors. Personal profiles display photos, registration information, and answers to free-text questions pertaining to the owners' interests and daily activities.



BurleeHurley
30 • Arlington, VA • Man

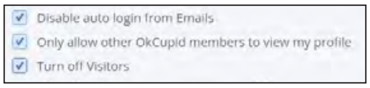
I'm looking for
- Women
- Ages 22-32
- Near me
- Who are single

What I'm doing with my life

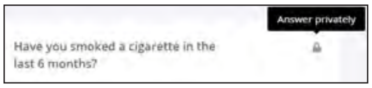
My self-summary

On a typical Friday night I am

Navigate **Settings**>**General** and activate the three **Privacy** options to help control who has access to your profile. The questionnaire is optional — submitted answers may be kept private using the lock icon shown below.



☑ Disable auto login from Emails
☑ Only allow other OkCupid members to view my profile
☑ Turn off Visitors



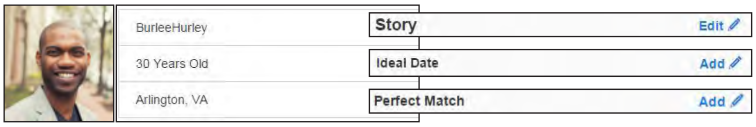
Answer privately

Have you smoked a cigarette in the last 6 months?

A paid subscription known as the "A-List" is the most secure option. It allows you to browse profiles anonymously and hides your profile from everyone except those who you choose to like or message first.

ZOOSK

Zoosk hosts ~1.8 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.



BurleeHurley	Story Edit
30 Years Old	Ideal Date Add
Arlington, VA	Perfect Match Add

Free Zoosk accounts offer little to no user-controlled security settings. Options including account verification pose potential threats to privacy — verification requires linking phone numbers, videos, or social networks.

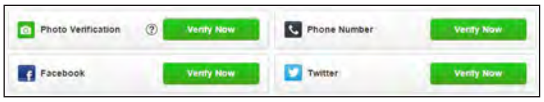


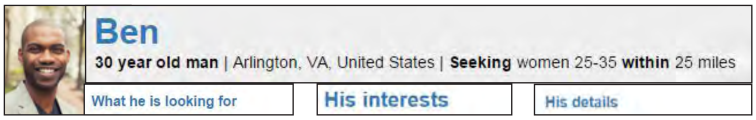
Photo Verification	Verify Now	Phone Number	Verify Now
Facebook	Verify Now	Twitter	Verify Now

Avoid linking your accounts

When profiles are visited, 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

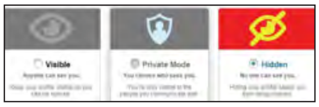
Match.com hosts ~4.3 million unique monthly visitors. Free accounts display photos, information submitted during registration, interests, and the traits that users look for in their significant others.



Ben
30 year old man | Arlington, VA, United States | **Seeking** women 25-35 **within** 25 miles

What he is looking for | His interests | His details

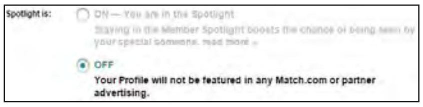
Select **Settings** to toggle profile visibility. Turn the member spotlight off to prevent the profile from appearing in ads. Hidden profiles prevent others from seeing the account but also disable Match.com's matching capability.



○ Visible
Anyone can see you.

○ Private Mode
You choose who sees you.

● Hidden
No one can see you.

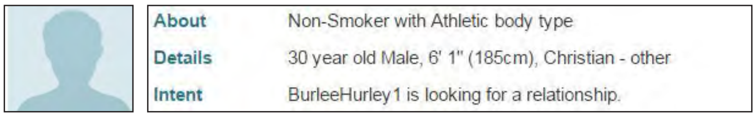


Spotlight is:
○ ON — You are in the Spotlight
Staying in the Member Spotlight boosts the chance of being seen by your special someone. read more »
● OFF
Your Profile will not be featured in any Match.com or partner advertising.

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

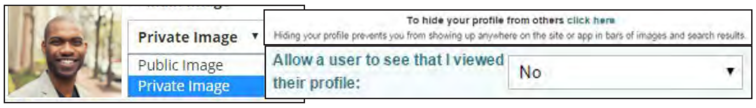
PLENTY OF FISH

Plenty of Fish hosts ~2.5 million unique monthly visitors. Profiles display the information submitted during registration and the traits that users look for in their significant others.



About	Non-Smoker with Athletic body type
Details	30 year old Male, 6' 1" (185cm), Christian - other
Intent	BurleeHurley1 is looking for a relationship.

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



Private Image ▾
Public Image
Private Image

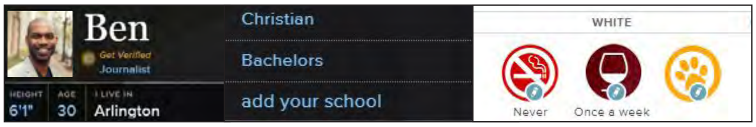
To hide your profile from others click here
Hiding your profile prevents you from showing up anywhere on the site or app in bars of images and search results.

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

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

EHARMONY

EHarmony hosts ~1.2 million unique monthly visitors. Profiles display registration information excluding photos and questionnaire responses. Other data includes free-text responses addressing the users' interests.

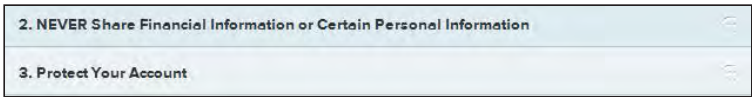


Ben
Get Verified
Journalist
HEIGHT 6'1" | AGE 30 | I LIVE IN Arlington

Christian
Bachelors
add your school

WHITE
Never
Once a week

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.



2. NEVER Share Financial Information or Certain Personal Information

3. Protect Your Account

Photos can only be seen by those 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

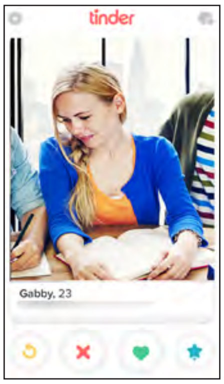
MOBILE DATING SITES - DO'S AND DON'TS

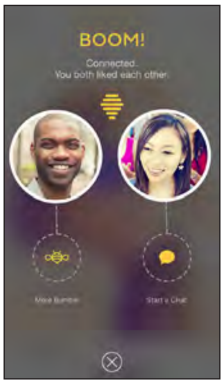
- Avoid using usernames and profile photos that appear on other social networking services.
- Do not include information unique to you (e.g. last name or place of work) in your public profile data or messages.
- Install all app updates as soon as they become available. Check your app's privacy settings 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 potentially reveal your geographical location, such as a photo with a famous landmark in the background.
- Always read and take the time to understand the app's Terms and Conditions before agreeing to register an account.

OVERVIEW

It is estimated that one out of every ten American adults actively uses mobile dating apps as their 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 app-based online dating services. For additional information about the risks of Internet dating and more information on web-based services such as Match, Plenty of Fish, Zoosk, OKCupid, or EHarmony, please reference the Online Dating Smart Card.

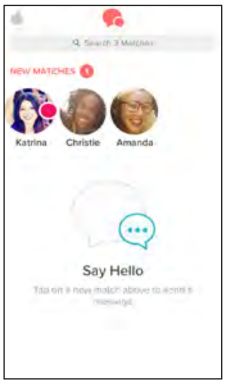
USING MOBILE DATING APPS

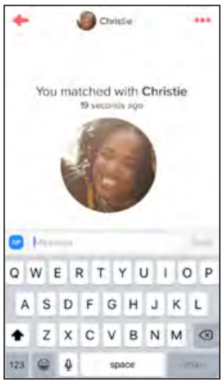




Matching: Mobile dating apps frequently employ a technique called "Swiping" — the motion of directing one's finger across a phone screen's surface — to help convey interest in other users' profiles. Traditionally, swiping a profile to the right indicates interest while swiping it to the left passes on the profile. Regardless of the swiping direction, users' 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.





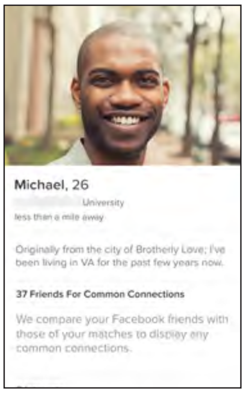
SELECTING A DATING APP

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	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	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

TINDER

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

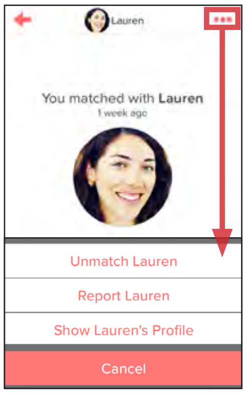


Michael, 26
[redacted] University
less than a mile away

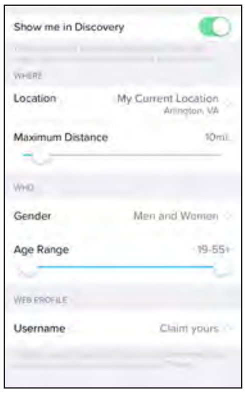
Originally from the city of Brotherly Love; I've been living in VA for the past few years now.

37 Friends For Common Connections

We compare your Facebook friends with those of your matches to display any common connections.



You matched with Lauren
1 week ago



Show me in Discovery

WHERE

Location: My Current Location, Arlington, VA

Maximum Distance: 10mi.

WHO

Gender: Men and Women

Age Range: 19-55+

WEB PROFILE

Username: Claim yours

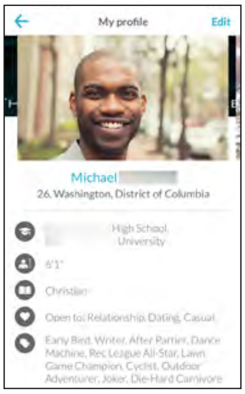
Use: Users may swipe through an unlimited number of profiles per day. There are no gender-based limitations on who is able to initiate a chat conversation once matched. Matches do not expire and are stored in the app unless they are manually removed by one of the users.

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

Settings: Navigate to **Gear Icon > Discovery Settings** to change your profiles' visibility. Deactivating **Show me in Discovery** 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.



Michael [redacted]
26, Washington, District of Columbia

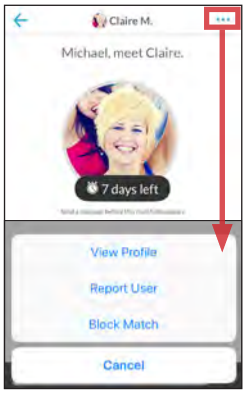
[redacted] High School, University

6'1"

Christian

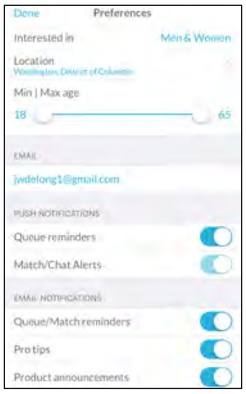
Open to: Relationship, Dating, Casual

Early Bird, Writer, After Partier, Dance Machine, Rec League All-Star, Lawn Game Champion, Cyclist, Outdoor Adventurer, Joker, Die-Hard Carnivore



Michael, meet Claire.

7 days left



Preferences

Interested in: Men & Women

Location: Washington, District of Columbia

Min | Max age: 18 – 65

EMAIL

jwdelong1@gmail.com

PUSH NOTIFICATIONS

Queue reminders

Match/Chat Alerts

EMAIL NOTIFICATIONS

Queue/Match reminders

Pro tips

Product announcements

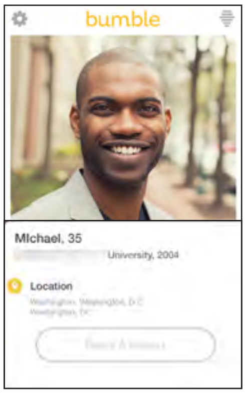
Use: Users may swipe through an unlimited number of profiles per day. There are no gender-based limitations on who is able to initiate chat conversations. Matches expire after 14 days; users can no longer view each others' profiles or communicate through the app, without rematching.

Profiles: Select **More > My Profile > Edit** to change or delete the information displayed in your profile.

Settings: Select **More > Preferences** to enable notifications and change your location to the nearest metropolitan area. Profiles cannot be hidden.

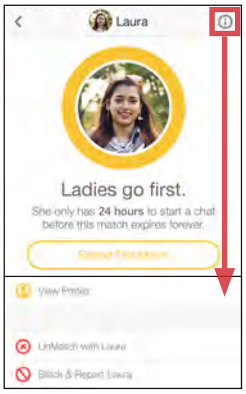
BUMBLE

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.



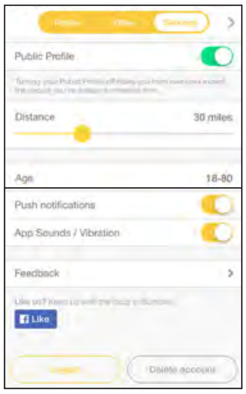
Michael, 35
[redacted] University, 2004

Location



Ladies go first.

She only has **24 hours** to start a chat before this match expires forever.



Public Profile

Distance: 30 miles

Age: 18-80

Push notifications

App Sounds / Vibration

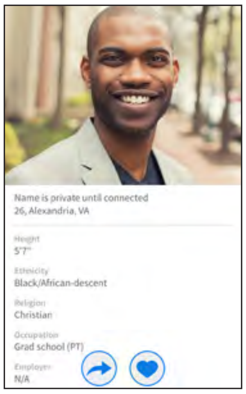
Use: Users may swipe through an unlimited number of profiles per day. Once matched, women are given 24 hours to open a conversation through the app. The match expires if a communication is not opened within the allotted time. Gender-based limitations do not apply for same-sex matches.

Profiles: Navigate to **Gear Icon > Pencil Icon** to change the information displayed in your profile.

Settings: Navigate to **Gear Icon > Settings** to enable notifications and set your profile's visibility. Deactivating **Public Profile** hides your profile.

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.



Name is private until connected
26, Alexandria, VA

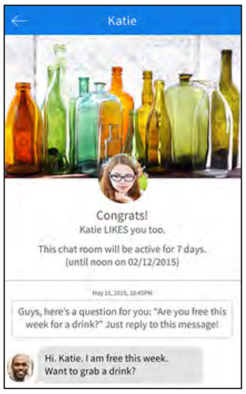
Height: 5'7"

Ethnicity: Black/African-descent

Religion: Christian

Occupation: Grad school (PT)

Employer: N/A

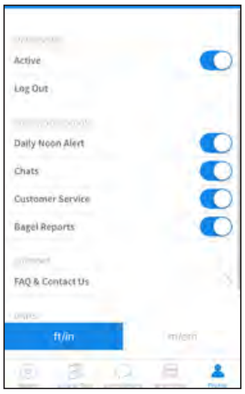


Congrats!
Katie LIKES you too.
This chat room will be active for 7 days.
(until noon on 02/12/2015)

May 11, 2015, 10:45PM

Guys, here's a question for you: "Are you free this week for a drink?" Just reply to this message!

Hi. Katie. I am free this week.
Want to grab a drink?



Active

Log Out

Daily Noon Alert

Chats

Customer Service

Bagel Reports

FAQ & Contact Us

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 **Profile > Edit Profile** to change or delete the information displayed in your profile.

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

SECURE CHAT APPS

SECURE CHAT APPS - DO'S AND DON'TS

- Only establish and maintain contact with people you know and trust. Review your contacts often.
- Ensure that your contacts take similar security precautions as you. Do not accept chat requests from unverified numbers or IDs.
- Do not send messages you do not want copied, screenshot, or re-posted by another member.
- Use all available PIN, password, and privacy protection options available. Change passwords every six months for enhanced 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.

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 security against eavesdropping by concealing the users' identities or making the contents of the messages indecipherable to anyone except the intended receivers. 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**: Mobile applications do not connect personally identifying information to messages and often require zero or limited identity data to create an account. These apps often offer private or public messaging to pseudonymous profiles and messages that expire after an allotted time.
- **Data Security**: Mobile applications promote the protection of 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 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.

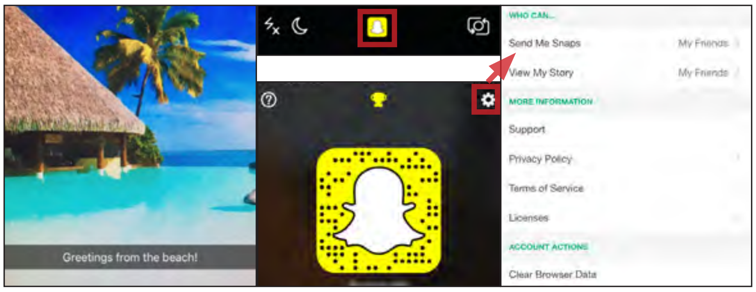
CHOOSING THE RIGHT SECURE CHAT APP

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. Germany-based.	***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
VSee	iPhone, iPad, Android, Mac, Windows PC	Text messages or video conferences; application file sharing on PC. US-based.	***Sign up***: Email address, first name, last name	Potential for anonymity; Encrypted messages & secure calls ***Encryption Type***: End-to-end encryption with FIPS 140-2 certified 256 AES encryption	***Social Networks / Email***: Gmail, Yahoo, MSN, AOL email contacts ***Device / Internet***: Microphone, camera, address book, cellular data, Wi-Fi, LAN
KeyTone	iPhone & Android	Call/text/video messages over an Internet network. US-based.	***Sign up***: Phone number & email address	Encrypted messages & secure calls ***Encryption Type***: TLS with AES-GCM 256 encryption	***Social Networks / Email:*** None ***Device / Internet:*** Address book, cellular data, Wi-Fi

SNAPCHAT

Snapchat is used to send temporary photo/video messages ('Snaps') to other users. Snaps can only be viewed once by the intended recipients and are set to expire between 1 and 10 seconds. Snapchat also offers a chat feature where text mesages can be sent to others. Chats are permanently erased when the recipient closes the chat window. Snapchat can also securely process payment transfers by way of the Snapcash feature.

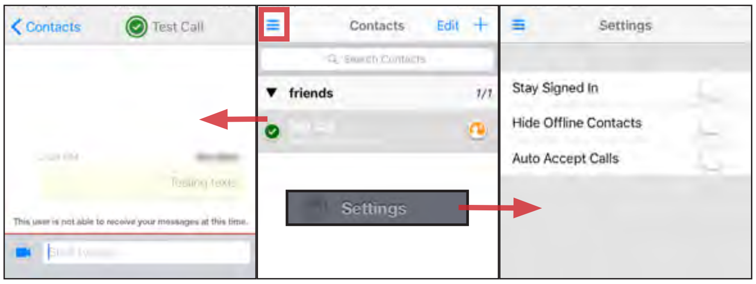


Tap the **ghost** in the center of the camera page and then select the **gear** icon to adjust your privacy settings. Apply the following recommendations:

- Do not provide your real name in the **Name** or **Username** fields.
- Set who can **Send me Snaps** and **View My Story** to **My Friends**.
- **Clear Browser Data** 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.

VSEE

VSee is a social messaging app used to establish secure conversations with other app users. VSee users can initiate video conferences with up to four people at a time and can send text messages protected with end-to-end encryption. Instant text messages are deleted when users choose to log out of their active sessions. Phone calls made within the app are also encrypted with end-to-end protection to prevent eavesdropping.



Tap the **blue icon (three lines)** in the top left corner of the screen. Proceed to **Settings** and apply the following selections to maximize your security:

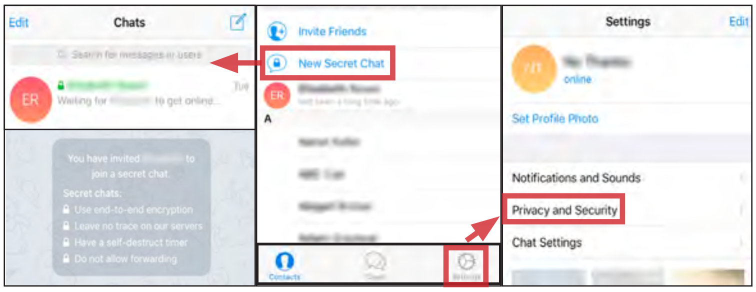
- Disable **Stay Signed In**
- Disable **Auto Accept Calls**

Follow these basic instructions when using the app:

- VSee accounts are linked to email accounts; avoid using an email address linked to your true identity data.
- Delete the app's history after each completed communication.
- Manually log out of your sessions when your conversations conclude.

TELEGRAM MESSENGER

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.

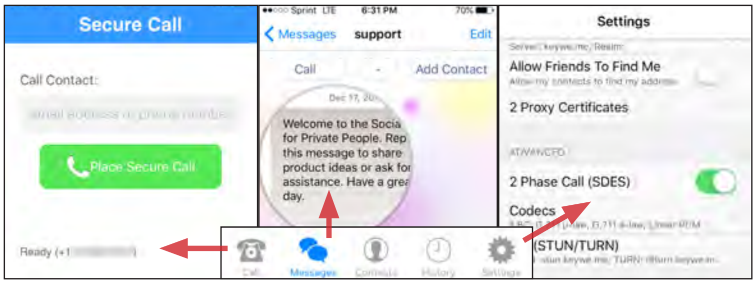


Tap the **Settings** icon and then select the **Privacy and Security** option. Apply the following recommendations to maximize security:

- 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.

KEYTONE

KeyTone is a social app designed to securely promote multiple forms of communication through the application. KeyTone users can share short video and audio messages, send text messages, and make secure VoIP phone calls to other app users. It employs standards-based protocols and cryptography for protecting data in transit, and offers in-app features such as 'Ghost Mode' to prevent over-the-shoulder eavesdropping.



Tap the **Settings** icon in the bottom right corner of the screen. Apply the following options to best secure your conversations through the app:

- Enable **Ghost Mode**
- Enable **2 Phase Call (SDES)** to improve encryption for phone calls.
- Enable **ICE** to prevent temporary storage of secure phone calls.

Follow these basic instructions when using the app:

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

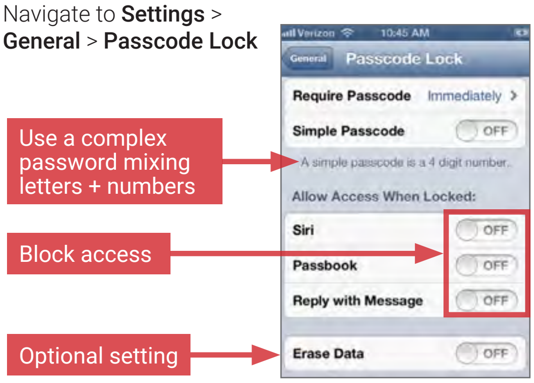
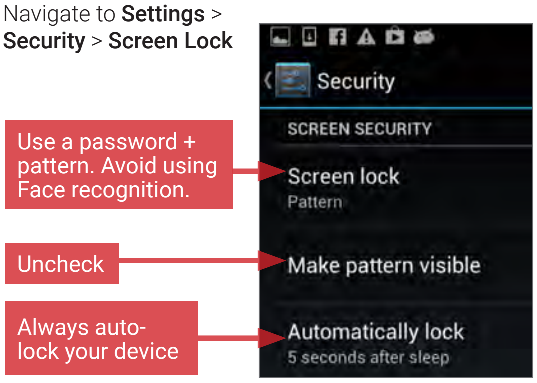
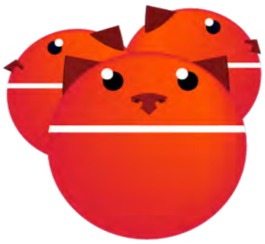
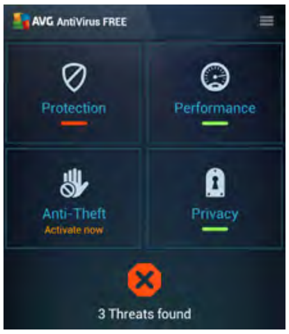
SMARTPHONES

SMARTPHONES - DO'S AND DON'TS

- Always protect your device with a password, and run apps such as Android Lost and Find My iPhone to help you recover lost or stolen smartphones.
- Malicious emails and text messages can infect your smartphone with malware; run anti-virus software periodically on your device.
- The camera and microphone can be remotely activated; do not take a smartphone in situations where personal or legal matters are being discussed.
- As an extra precaution, remove the battery before discussing any sensitive information.
- When possible use VPN when accessing wireless networks, and turn off Bluetooth unless needed to prevent unwanted access to your device.
- Apps may gain real-time access to the data stored on your smartphone; review what data (e.g. location) the app collects before downloading.

PROTECTING YOUR SMARTPHONE FROM PHYSICAL ACCESS AND MALWARE RISKS

Use the following settings and recommendations to minimize inherent security risks posted by your smartphone and protect your personal data.

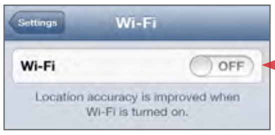
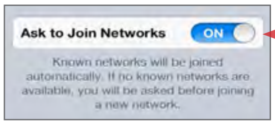
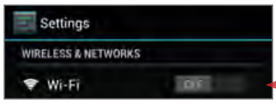
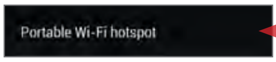
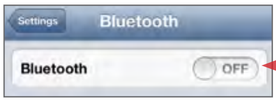
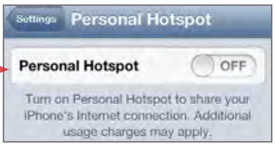
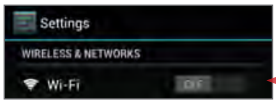
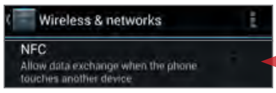
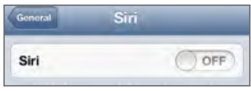
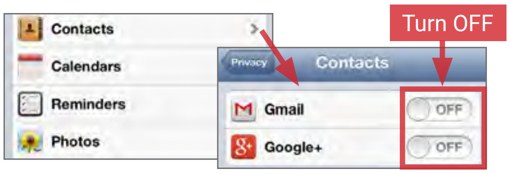
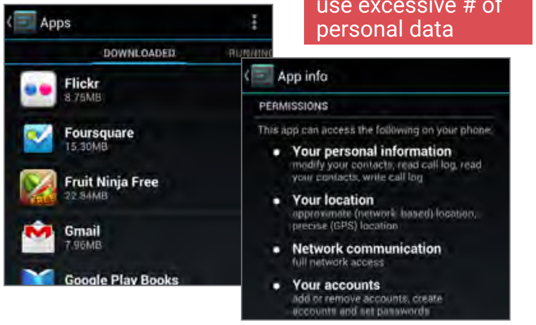
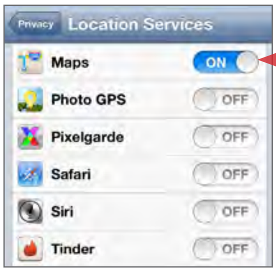
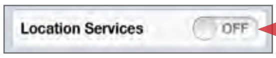
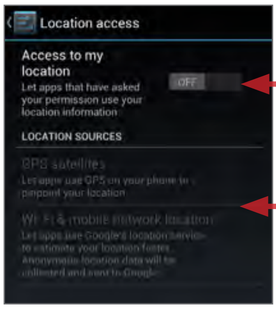
RISK SCENARIO	IPHONE		ANDROID	
SMARTPHONE IS PHYSICALLY ACCESSED BY SOMEONE WITHOUT YOUR CONSENT - To prevent others from accessing data on your smartphone, set up a passcode to protect your information. Use all passcode styles made available by your phone (e.g. pattern lock, PIN, password, and fingerprints)	Navigate to **Settings** > **General** > **Passcode Lock**  Verizon 10:45 AM General Passcode Lock Require Passcode Immediately > Simple Passcode OFF A simple passcode is a 4 digit number. Allow Access When Locked: Siri OFF Passbook OFF Reply with Message OFF Erase Data OFF Use a complex password mixing letters + numbers Block access Optional setting		Navigate to **Settings** > **Security** > **Screen Lock**  Security SCREEN SECURITY Screen lock Pattern Make pattern visible Automatically lock 5 seconds after sleep Use a password + pattern. Avoid using Face recognition. Uncheck Always auto-lock your device	
SMARTPHONE IS LOST OR STOLEN - It is reported that on average 113 cellphones will be stolen every minute in the US. Download and install apps that allow you to locate, lock, and control your data remotely from a web page.	Install **Find My Phone** Find My iPhone Apple ID name@example.com Password Required	Capabilities: • Remote lock • Erase data • GPS locator • Sound alarm • Send text message to phone • Backup data through iCloud storage	Install **Cerberus Anti Theft** 	Capabilities: • Remote lock • Erase data • Sound alarm • Send text message to phone • Activate camera • Read texts sent • View call list
SMARTPHONE IS INFECTED WITH MALWARE - Your smartphone can catch a malware from emails, websites, or downloading apps. Between 2011 and 2012 alone, smartphones had an increase in malware attacks by 1200% with Android being the most susceptible. Download third-party security apps to prevent malware from stealing your information.	Install **Lookout Mobile Security** 	Phones are not readily susceptible to viruses. Use this app to prevent passing malware to contacts. Capabilities: • Scan for spyware, adware, and trojans • Scan emails and PDF files before sending	Install **Antivirus Security by AVG**  AVG AntiVirus FREE Protection Performance Anti-Theft Activate now Privacy 3 Threats found	Capabilities: • App scanner • File scanner • Website scanner • Text and call blocker • Remote lock • Erase data remotely • GPS locator • Kill slow tasks

RECOMMENDATIONS TO MINIMIZE PHYSICAL ACCESS AND MALWARE RISKS

- Updates for smartphones' operating systems are sent out frequently. Install the updates immediately to maximize your protection.
- Jailbroken phones allow malicious apps to bypass vetting processes taken by the app stores. Never jailbreak your smartphones.
- Write down the serial number of your phone when it is purchased to help identify devices if lost or stolen.
- Avoid linking social networking services like Facebook and Twitter to your smartphones to prevent personal information aggregation.
- Change passwords on your phone frequently (approximately every 6 months) to maximize security.

WIRELESS PROTECTION AND APP SECURITY SETTINGS

Smartphones communicate personal data across a variety of networks and apps in order to bring its complex functionalities to the user. Follow these steps to best protect your identity data in one of the following four common smartphone use case scenarios.

USE CASE	IPHONE	ANDROID
CONNECTING TO WIRELESS NETWORKS - Information transmitted via public WiFi 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** > **WiFi**  Settings Wi-Fi Wi-Fi OFF Location accuracy is improved when Wi-Fi is turned on. Disable WiFi when not in use  Ask to Join Networks ON Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network. Enable network permissions Navigate to **Settings** > **General** > **VPN** to enable and establish a VPN connection	Navigate to **Settings** > **WiFi** to manage connections  Settings WIRELESS & NETWORKS Wi-Fi OFF Disable WiFi when not in use Navigate to **Settings** > **More** > **Tethering & Portable Hotspot** and disable **Portable WiFi Hotspot**  Portable Wi-Fi hotspot Uncheck Navigate to **Settings** > **More** > **VPN** to enable and establish a VPN connection
CONNECTING VIA BLUETOOTH - Bluetooth involves the wireless communication of two devices within a close geographical proximity. When Bluetooth is enabled, hackers may be able to access the connection to your calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and disable it when it is not being used.	Navigate to **Settings** > **Bluetooth** to disable services  Settings Bluetooth Bluetooth OFF Disable Bluetooth when not in use Navigate to **Settings** > **Personal Hotspot** to disable broadcasting your private Internet connection with others Never share your Internet connection  Settings Personal Hotspot Personal Hotspot OFF Turn on Personal Hotspot to share your iPhone's Internet connection. Additional usage charges may apply.	Navigate to **Settings** > **Bluetooth**  Settings WIRELESS & NETWORKS Wi-Fi OFF Disable Bluetooth when not in use Navigate to **Settings** > **More** > **NFC** to manage Near Field Communications settings, which enable smartphones to transfer data by touching the devices together  Wireless & networks NFC Allow data exchange when the phone touches another device Uncheck
DATA RETAINING APPS - Downloaded apps frequently collect user's personal information to sell to third party data aggregators. Native applications such as Siri and Google Now will also collect data from users which may include name, email address, credit card numbers, contacts, and device information. These services also record and catalogue the audio during sessions. Avoid using these voice recording services.	Navigate to **Settings** > **General** > **Siri**  General Siri Siri OFF Disable Siri Navigate to **Settings** > **Privacy** to manage which specific data each app accesses from your phone  Contacts Calendars Reminders Photos Privacy Contacts Gmail OFF Google+ OFF Turn OFF	Navigate to **Settings** > **Apps** Delete apps that use excessive # of personal data  Apps DOWNLOADED RUNNING Flickr 8.75MB Foursquare 15.30MB Fruit Ninja Free 22.84MB Gmail 7.96MB Google Play Books App info PERMISSIONS This app can access the following on your phone: • Your personal information: modify your contacts, read call log, read your contacts, write call log • Your location: approximate (network-based) location, precise (GPS) location • Network communication: full network access • Your accounts: add or remove accounts, create accounts and set passwords
APPS USING REAL-TIME LOCATION - The majority of apps in the market 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 retain their location information inside their EXIF data. Be aware that your location is being shared when photos are uploaded from your smartphone to a SNS.	Navigate to **Settings** > **Privacy** > **Location Services**  Privacy Location Services Maps ON Photo GPS OFF Pixelgarde OFF Safari OFF Siri OFF Tinder OFF Only grant access to apps that require a location function  Location Services OFF Disable all location services when not in use	Navigate to **Settings** > **Location Access**  Location access Access to my location OFF Let apps that have asked your permission use your location information LOCATION SOURCES GPS satellites Let apps use GPS on your phone to pinpoint your location Wi-Fi & mobile network location Let apps use Google's location service to estimate your location faster. Anonymous location data will be collected and sent to Google. Disable all location services when not in use Uncheck both boxes when location services are not in use

TRAVELING SAFELY WITH SMARTPHONES

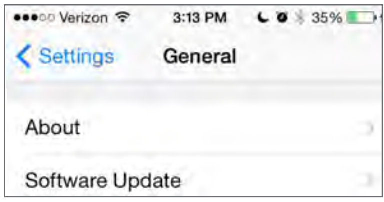
TRAVELING WITH SMARTPHONES - DO'S AND DON'TS

- Bring a dedicated loaner device when you travel overseas; do not bring your personal smartphone
- Make sure your device is running the latest software; this will help to protect you against the newest technical vulnerabilities
- Assume that all information on your device could be compromised while traveling in a foreign country; leave sensitive information off of your phone
- Use VPN to protect your phone when accessing WiFi 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

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

iPHONE



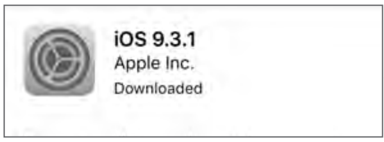
●●●○○ Verizon 3:13 PM 35%

Settings General

About

Software Update

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

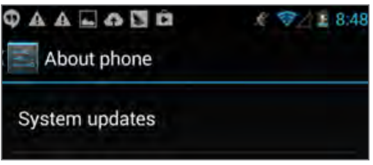


iOS 9.3.1
Apple Inc.
Downloaded

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

ANDROID

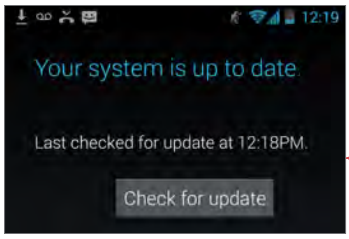
Go to **Settings > About Phone > System Updates.**



8:48

About phone

System updates



12:19

Your system is up to date

Last checked for update at 12:18PM.

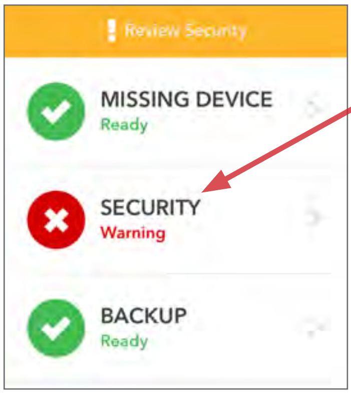
Check for update

Check to see if your software is up-to-date; if not, your phone will prompt you to download 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



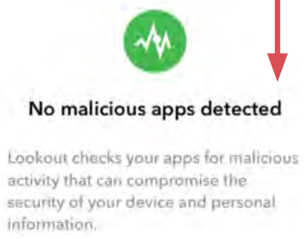
Review Security

MISSING DEVICE
Ready

SECURITY
Warning

BACKUP
Ready

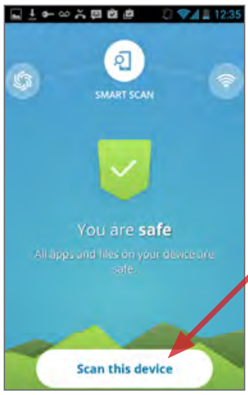
Use the **Lookout** app for iPhone. Go to Security to see if your phone has any malicious apps.



No malicious apps detected

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

ANDROID



12:35

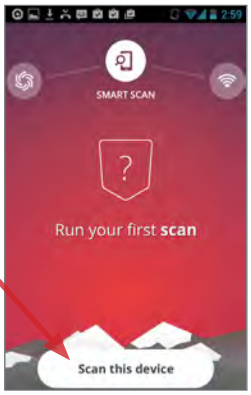
SMART SCAN

You are safe

All apps and files on your device are safe.

Scan this device

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



2:59

SMART SCAN

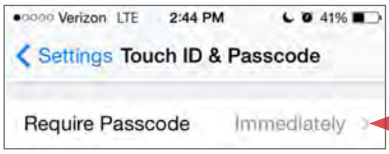
Run your first scan

Scan this device

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

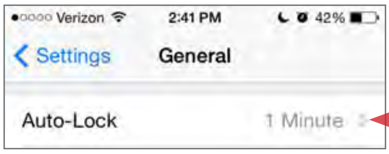


●○○○○ Verizon LTE 2:44 PM 41%

Settings Touch ID & Passcode

Require Passcode Immediately

Go to **Settings > Touch ID & Passcode.** Set Require Passcode to **Immediately**



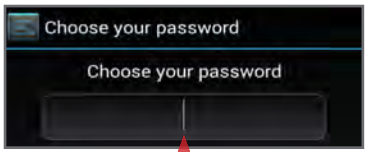
●○○○○ Verizon 2:41 PM 42%

Settings General

Auto-Lock 1 Minute

Go to **Settings > General > Auto-Lock.** Set the **Auto-lock** to **1 Minute.**

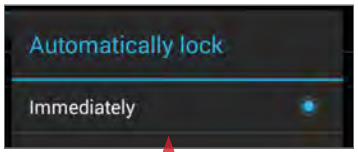
ANDROID



Choose your password

Choose your password

Go to **Settings > Choose your password** to enable password protection.



Automatically lock

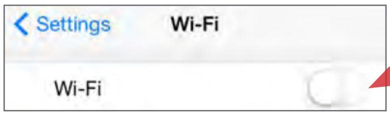
Immediately ●

Go to **Settings > Security > Automatically lock > Immediately**

DISABLE WIFI AND BLUETOOTH

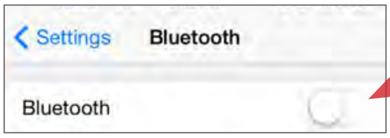
Disable **WiFi** and **Bluetooth** on your smartphone when you are not using them; WiFi and bluetooth can render your smartphone vulnerable to malware.

iPHONE


< Settings Wi-Fi

Wi-Fi

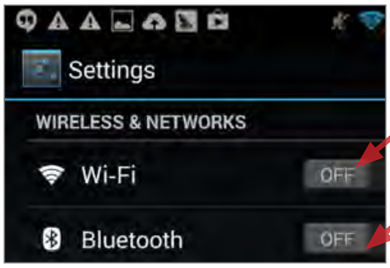
Go to **Settings > WiFi**. Turn Wi-Fi OFF


< Settings Bluetooth

Bluetooth

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

ANDROID


Settings

WIRELESS & NETWORKS

Wi-Fi OFF

Bluetooth OFF

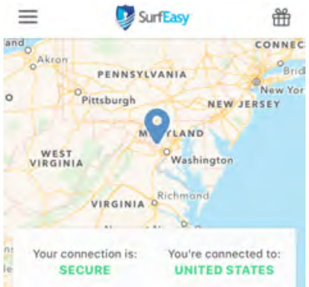
Go to **Settings > WiFi**. Turn Wi-Fi OFF

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

USE VPN ON WIRELESS NETWORKS

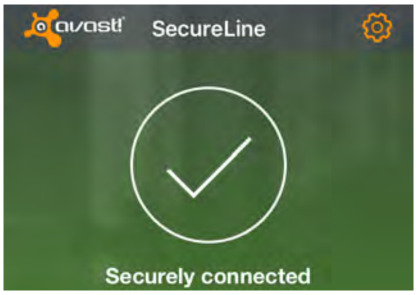
Virtual Private Networks — or **VPN** — allow you to extend a private network across a public network such as public WiFi. Using VPN will make it more difficult for malicious individuals to easedrop on your Internet traffic. Use VPN services such as SurfEasy VPN and Avast SecureLine to protect yourself.

iPHONE



Your connection is: SECURE

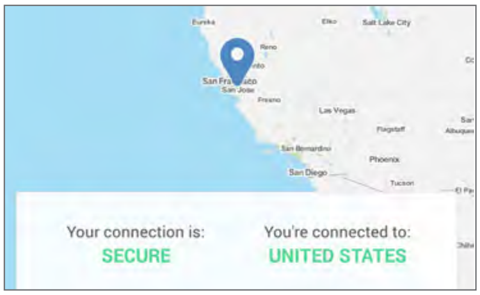
You're connected to: UNITED STATES



Securely connected

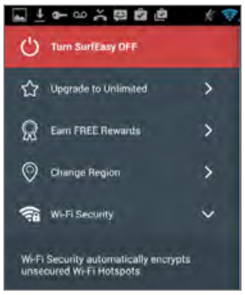
Use VPN services such as **SurfEasy** and **Avast SecureLine** VPN for iOS to protect yourself on WiFi.

ANDROID



Your connection is: SECURE

You're connected to: UNITED STATES



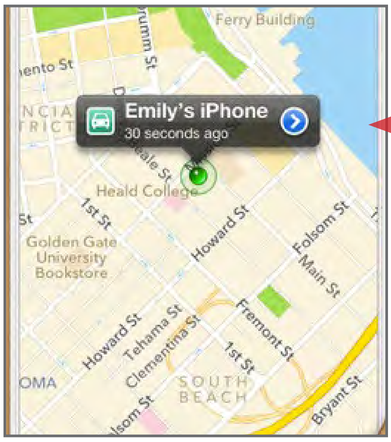
Wi-Fi Security automatically encrypts unsecured Wi-Fi Hotspots

Use VPN services such as **SurfEasy** for Android to protect yourself on WiFi.

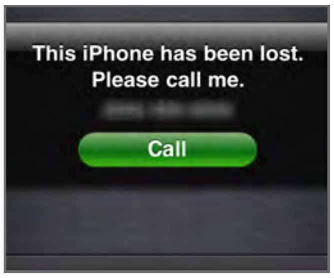
RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

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



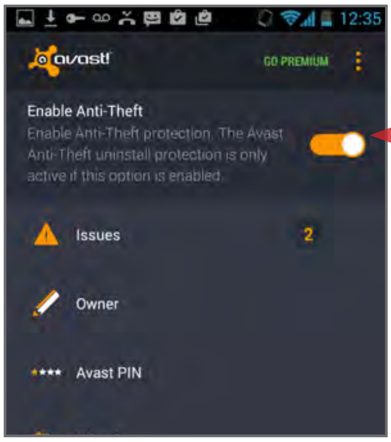
Use the **Find My iPhone** app to recover lost or stolen iPhone smartphones.


This iPhone has been lost. Please call me.

[redacted]

Call

ANDROID



Enable Anti-Theft

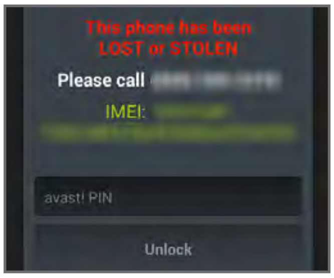
Enable Anti-Theft protection. The Avast Anti-Theft uninstall protection is only active if this option is enabled.

Issues 2

Owner

Avast PIN

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


This phone has been LOST or STOLEN

Please call [redacted]

IMEI: [redacted]

[redacted]

avast! PIN

Unlock

SMARTPHONE EXIF REMOVAL

EXIF REMOVAL - DO'S AND DON'TS

- Remove EXIF data before sharing or posting images, especially when images are captured in private homes or businesses.
- Whenever possible, use an EXIF viewer to verify that personal data is removed from photos, and prevent your phone from including geolocation data.
- Before uploading images, use 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 with no EXIF data, the content of images may contain identifying information, including associated persons and locations. Screen content with the assumption that anyone can see, copy, or forward photos that you post online.

EXIF DATA

EXIF (Exchangeable image File Format) 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+, and Instagram, have features that share EXIF data alongside images. Others, including Facebook and Twitter, do not share EXIF data but my utilize the information internally. EXIF data is stored as tags, some of which reveal unique identifying information.

CATEGORY	IMPORTANT TAGS	IDENTITY IMPLICATIONS
Geolocation	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photosharing sites, including Google+ 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 particular device for 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 + locations.

Limiting EXIF data, especially geolocation information, before distributing image files can help protect your online 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.

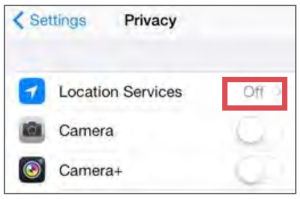
PREVENTING THE CAPTURE OF GEOLOCATION DATA

- Taking a screenshot of a photo on a device running iOS 7 or Android Jelly Bean will create a new image containing no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons; with a Galaxy S3 or Note, press the power and home buttons simultaneously; with a Nexus 4, 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.
- Remember that uploading or sharing a lower quality image will still contain EXIF data. EXIF data and image quality have no correlation.

IOS (V. 6.0.1)

Turn off iOS location services to ensure images captured with the native iPhone camera app will not contain any gelocation 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 the permissions for other apps to access photos already stored in your device's Camera Roll.

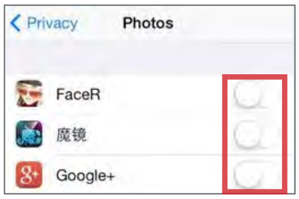


< Settings Privacy

Location Services Off

Camera

Camera+



< Privacy Photos

FaceR

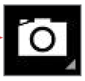
魔镜

Google+

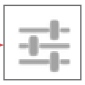
ANDROID (V. 4.3)

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

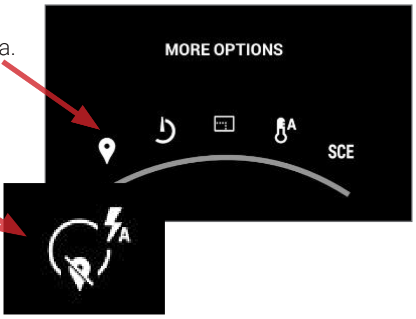
1. Open the camera app. A white camera symbol in the bottom right corner indicates the app is in camera mode.



2. Tap the white circle in the bottom right corner to bring up a cluster of options in the middle of the screen. Click settings symbol.



3. Click the location icon on the far left to disable location data.
4. When the location symbol appears with a line through it, then location data has been successfully disabled.

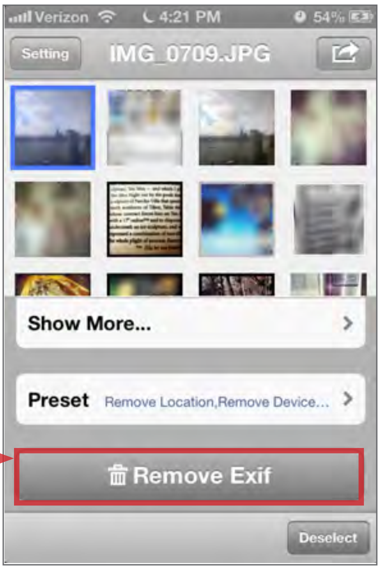


EXIF REMOVAL SMARTPHONE APPS

TRASHEXIF FOR IOS

TrashEXIF is a free app that deletes EXIF information from image files stored on your iOS device.

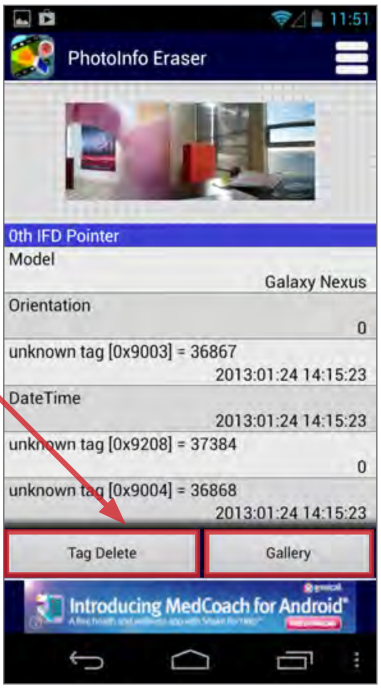
1. Download the TrashEXIF app from the **App Store.**
2. Open the TrashEXIF app and select photo(s) which you want EXIF data removed.
3. Select **Presets**, then in the **Removal Presets** window, select **Remove Location** and **Remove Device Information**.
4. Return to the pervious screen by clicking the name of the image in the upper-left.
5. Scroll down and click **Remove Exif**. This creates a copy of the image file(s) without EXIF and does not alter the original image file. The copy without EXIF data is displayed as most recent in your iPhone Photo app.



PHOTOINFO ERASER FOR ANDROID

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

1. Download PhotoInfo Erase from the **Play Store**.
2. Open the PhotoInfo Eraser app and select **Gallery**.
3. Navigate your phone and select an image.
4. Select **Tag Delete** and press OK.
5. Click **Gallery**. A copy of your photo without EXIF data is now available in the **PIEraser** folder.



0th IFD Pointer

Model
Galaxy Nexus

Orientation
0

unknown tag [0x9003] = 36867
2013:01:24 14:15:23

DateTime
2013:01:24 14:15:23

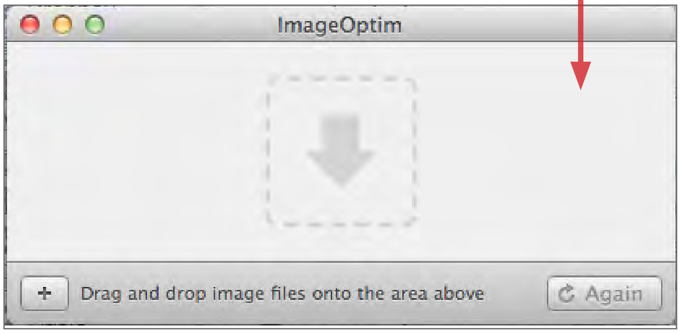
unknown tag [0x9208] = 37384
0

unknown tag [0x9004] = 36868
2013:01:24 14:15:23

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

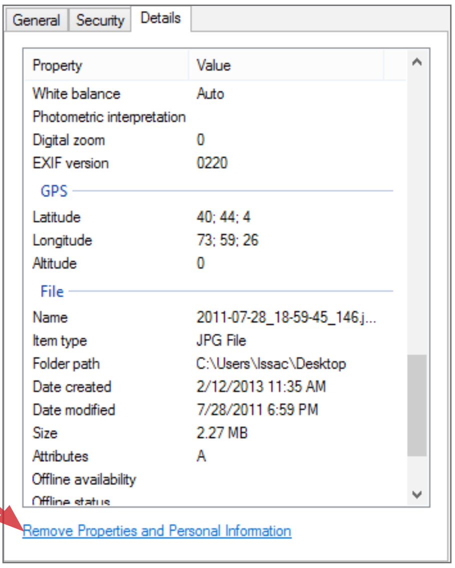


3. Check that the EXIF data has been removed by right-clicking the image and select **Get Info**. EXIF data is listed under **More Info**.

VIEWING AND REMOVING EXIF DATA IN WINDOW 8

Use the Windows 8 OS 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 8 also allows system administrators to remove all EXIF data from the selected image by clicking the **Remove Properties and Personal Information** link.



Property	Value
White balance	Auto
Photometric interpretation	
Digital zoom	0
EXIF version	0220
GPS	
Latitude	40; 44; 4
Longitude	73; 59; 26
Altitude	0
File	
Name	2011-07-28_18-59-45_146.j...
Item type	JPG File
Folder path	C:\Users\Issac\Desktop
Date created	2/12/2013 11:35 AM
Date modified	7/28/2011 6:59 PM
Size	2.27 MB
Attributes	A
Offline availability	
Offline status	

Remove Properties and Personal Information

MOBILE WALLETS

MOBILE WALLETS - DO'S AND DON'TS

- Utilize all available PIN, password, and fingerprint protection options.
- Turn on notifications, and regularly monitor transaction history for unauthorized payments.
- Only transfer money to people or merchants you know and trust.
- 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.

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 at the point-of-sale using a QR code or NFC chip (near field communication). You can pay selecting a specific card, account, or existing balance, if available.

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 maintain multiple wallets.

BENEFITS OF MOBILE WALLETS

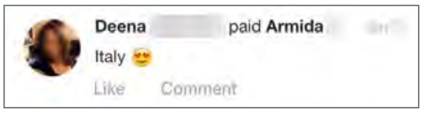
Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile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

On iPhones, 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 exposes you to an increased risk. 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 habits, activity, and finances.

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



Deena [redacted] paid **Armida** [redacted]

Italy 😍

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

CHOOSING THE RIGHT MOBILE WALLET

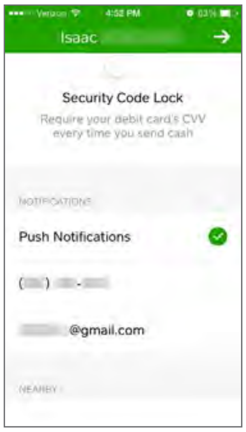
You should consider the following questions when choosing a mobile wallet:

- 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	IDENTITY DATA	SECURITY OPTIONS	SNS LINKS	DEFAULT VISIBILITY
$ Square Cash	iOS, Android	User to friend	Photo, phone number, email, debit card number	CVV requirement before transfer	None	None
Pay	iOS	User to merchant	Full name, billing address, shipping address, email, phone number	Fingerprint required for transactions	None	None
Google wallet	iOS, Android, browser	User to friend, User to merchant	Photo, full name, email, bank account, card numbers	PIN	None	None
venmo	iOS, Android, browser	User to friend	Photo, full name, email, about (optional), phone number, bank account, card numbers	PIN or fingerprint	Facebook (optional), internal social features	In-app contacts
LevelUp	iOS, Android, browser (limited)	User to merchant	Full name, email, birthday, gender, card numbers	PIN or fingerprint	Facebook (optional)	Private
PayPal	iOS, Android, browser	User to friend, User to merchant	Photo, full name, email, phone number, bank account, card numbers	Password	None	Private

SQUARE CASH



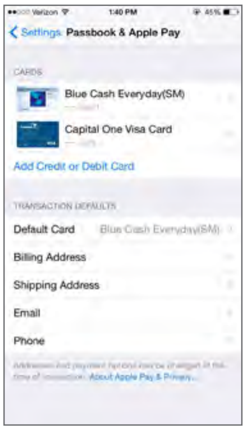
Navigate to **Settings** in the upper left portion of the home screen:

- Add your **Email Address** to verify your account.
- Require **CVV Security Code Lock**.
- Enable **Push Notifications**.

Utilizing Cash's bluetooth-based Nearby option allows you to be seen by nearby users. This feature is not recommended.

An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

APPLE PAY - IPHONE ONLY



In the iPhone **Settings** > **Passbook & Apple Pay** menu, add credit or debit cards you wish to use with the service.

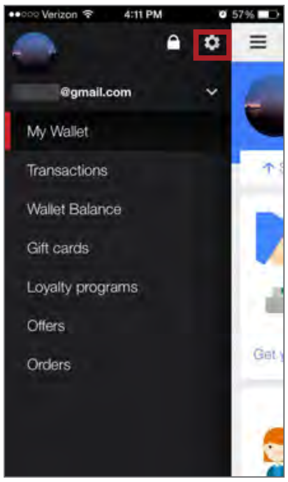
Note that an unauthorized user of your iPhone can view the last 4 digits of your cards, your billing address, shipping address, email address, and phone number.

To mitigate the risk of exposing personal information, enable PIN, password, or fingerprint protection for your iPhone's lock screen. Use more than one of these options to ensure extra security and protection.

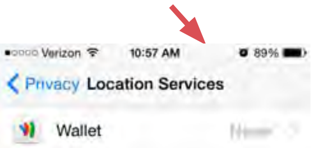
GOOGLE WALLETS

In the Settings menu:

- Turn on Notifications for Wallet Card purchases.
- Set PIN Timeout to '15 minutes.'
- 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**.

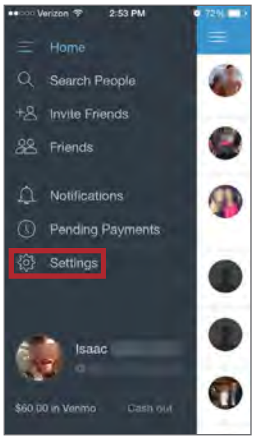


Note to Android users: It is recommended you disable all location services by navigating to Settings > Personal / Location Access

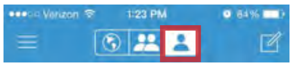
VENMO

Navigate the dropdown menu to **Settings**:

- Under **Notifications**, enable push notifications for payment sent, trust charge received, and bank transfers to Venmo completed.
- Enable **Touch ID & Passcode** and turn on **Use Touch ID**.
- To limit social visibility, under **Privacy**, set audience for future transactions to **Private**. Set **Who can share transactions involving you?** to **Only Me**. Make all past transactions 'Private.'
- Venmo provides an option to 'trust' friends and automatically pay their requests. Utilizing this feature is not recommended.

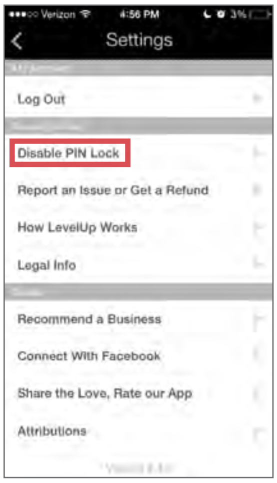


Monitor your transaction activity by clicking on the logo of a single person at the top of the home screen.



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

LEVELUP

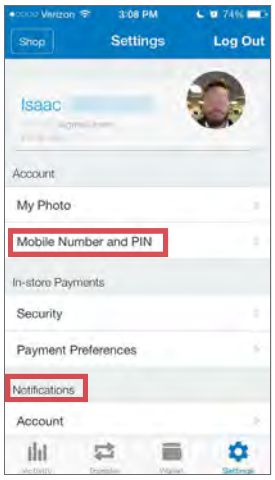


Navigate to the **Settings** menu, found in the top left corner of the home screen:

- Monitor your transaction history under **Transaction History**.
- Enable PIN lock.
- iPhone users should utilize the Touch ID lock option
- Do not connect your Facebook account to LevelUp.

iPhone users: navigate to your iPhone's **Settings** > **Privacy** > **Location Services** and set LevelUp location access to **Never**.

PAYPAL



Navigate to **Settings**:

- Upload an up-to-date **My Photo** to protect against fraud.
- Set a PIN under **Mobile Number and PIN**.
- Verify your phone number **Mobile Number and PIN**.
- Turn on all options under **Notifications**. Your account activity can also be monitored on the **Activity** home screen.
- Only enable bluetooth when engaging in an in-store transaction.

iPhone users: navigate to your iPhone's **Settings** > **Privacy** > **Location Services** and set PayPal location access to **Never**.

SECURING HOME WIRELESS NETWORK

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

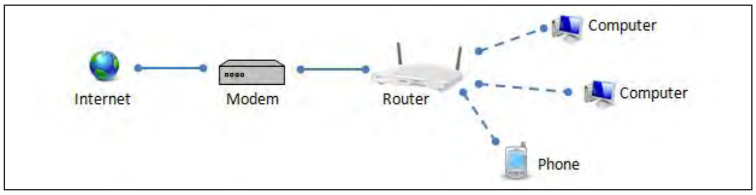
- Use the most up-to-date hardware and operating systems to maximize your connecting device's security options.
- Turn on automatic updates for your network device's firmware or periodically check for updates on the device's website.
- Limit the reach of your router's signal; position the router further towards the interior of your house and decrease the signal strength.
- Use an ethernet cable instead of a WiFi connection when possible; disable the wireless network when it will not be used for an extended time.
- Enable your router's firewall and strong encryption to block a number of 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.

WIRELESS NETWORKS OVERVIEW

Home wireless networks allow users to connect multiple devices to a single, remote Internet network. While wireless technology makes it easier for individuals 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

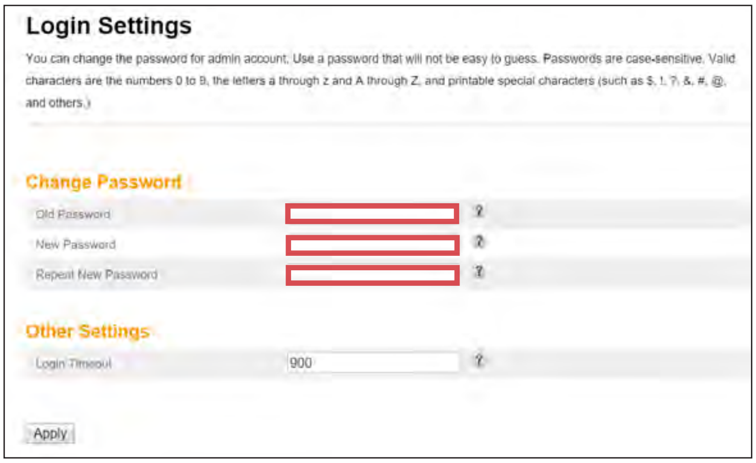
A home wireless network consists of a modem, a router, and a selection of personal electronic devices. Unlike Local Area Networks (LAN) — networks requiring all devices to be linked together via network cables — a home wireless network broadcasts radio waves from a router to allow wireless devices to 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.



To begin configuring your wireless network's security settings, you must first gain access to your router. Begin by launching any web browser and entering 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.

CHANGING ROUTER LOGIN SETTINGS

Routers often come preconfigured with a default username and password (e.g. Username = "Admin" and Password = "Password"). The first step toward securing your network should be to change these fields to more secure entries. Usernames should not represent your name, home address, or any other personal identity data. Passwords should be complex and different from the password used to access your network.



Login Settings

You can change the password for admin account. Use a password that will not be easy to guess. Passwords are case-sensitive. Valid characters are the numbers 0 to 9, the letters a through z and A through Z, and printable special characters (such as $, !, ?, &, #, @, and others.)

Change Password

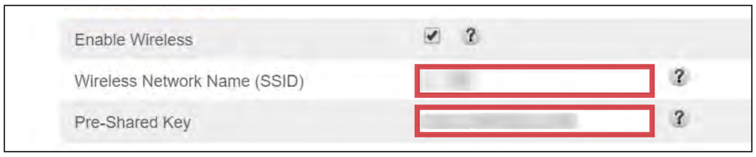
Old Password ?
New Password ?
Repeat New Password ?

Other Settings

Login Timeout: 900 ?

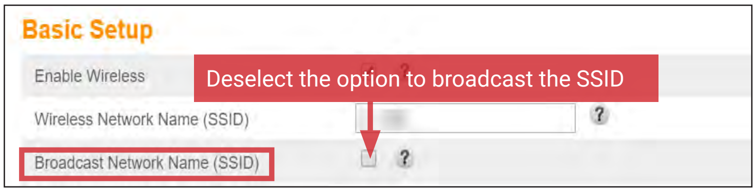
CREATING A NETWORK NAME AND PASSWORD

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.



Enable Wireless ☑ ?
Wireless Network Name (SSID) [redacted] ?
Pre-Shared Key [redacted] ?

Broadcasting an SSID is a quick way for devices to discover and connect to target networks. However, broadcasts can be seen by other individuals close to your proximity and may draw unwanted attention to your network.



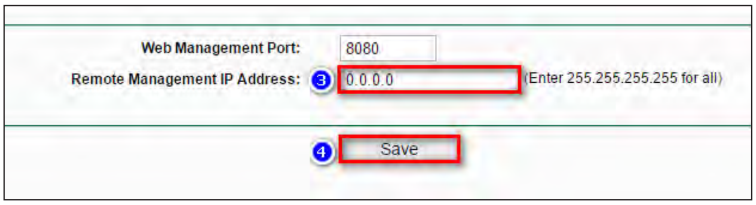
Basic Setup

Enable Wireless
Wireless Network Name (SSID) [redacted] ?
Broadcast Network Name (SSID) ☐ ?

Deselect the option to broadcast the SSID

DISABLING REMOTE ADMINISTRATION

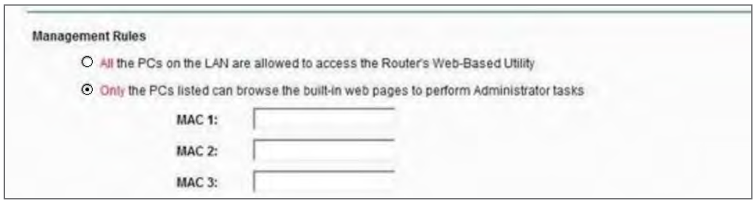
Disable the remote administration of your wireless router to ensure that individuals cannot make changes to your router remotely. You can accomplish this by setting the remote management IP address to "0.0.0.0".



Web Management Port: 8080
3 Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)
4 Save

LIMITING ADMINISTRATIVE ACCESS

Add the Media Access Control (MAC) Addresses — unique individual identifiers assigned to computers and devices — for each computer and device you wish to have administrative access to your network.



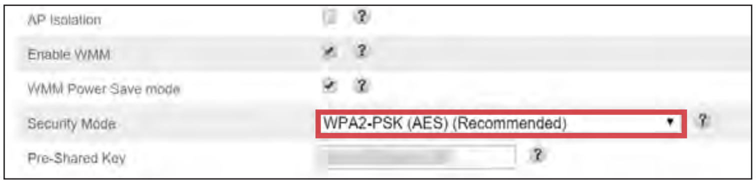
Management Rules

○ All the PCs on the LAN are allowed to access the Router's Web-Based Utility
● Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:
MAC 2:
MAC 3:

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 eavesedrop on your Internet activities.



AP Isolation □ ?

Enable WMM ☑ ?

WMM Power Save mode ☑ ?

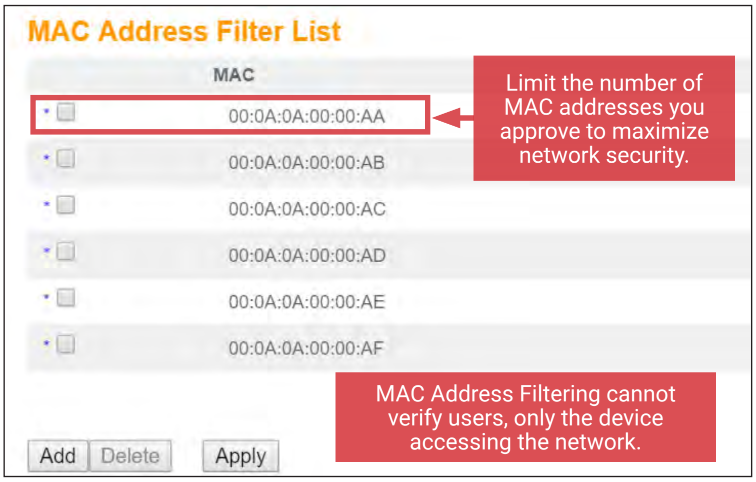
Security Mode: WPA2-PSK (AES) (Recommended) ?

Pre-Shared Key ?

ENCRYPTION	PRIVACY STRENGTH
WPA2-PSK (AES)	Maximum
WPA2-PSK (TKIP)	Minimal (older devices only)
WPA-PSK	None
WEP	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 router's settings; search online for ways to retrieve your personal devices' MAC addresses based on their operating systems.



MAC Address Filter List

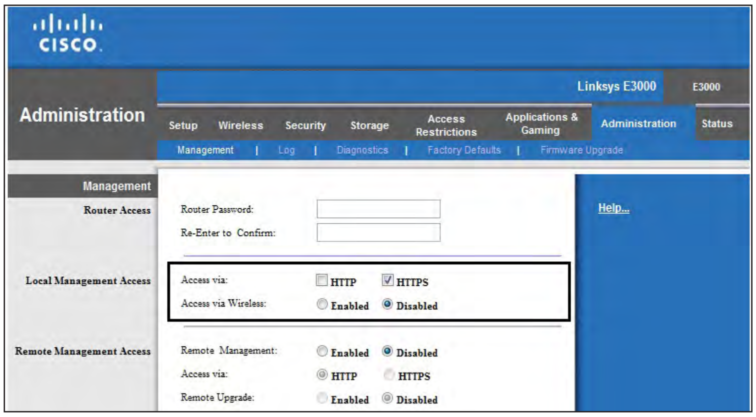
MAC
00:0A:0A:00:00:AA
00:0A:0A:00:00:AB
00:0A:0A:00:00:AC
00:0A:0A:00:00:AD
00:0A:0A:00:00:AE
00:0A:0A:00:00:AF

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

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

ENABLING HTTPS

Enable Hyptertext Transfer Protocol Secure (HTTPS) encryption to make it more difficult for unauthorized individuals to access your network traffic. HTTPS is the secure version of HTTP, the protocol used to send data between a website and your Internet browser. By enabling HTTPS on your router, you will ensure that the information that you send between your personal electronic devices and your router is encrypted. This is especially useful for protecting your most sensitive information, such as the passwords you use to administer your network.



Management

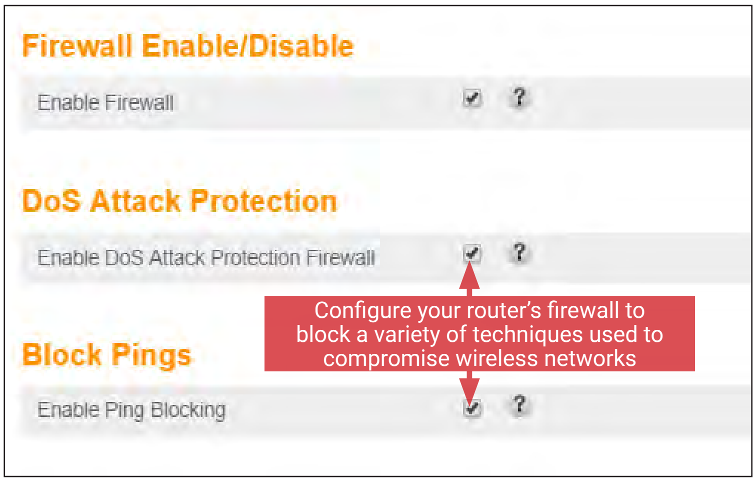
Router Access — Router Password: ; Re-Enter to Confirm:

Local Management Access — Access via: □ HTTP ☑ HTTPS; Access via Wireless: ○ Enabled ● Disabled

Remote Management Access — Remote Management: ○ Enabled ● Disabled; Access via: ● HTTP ○ HTTPS; Remote Upgrade: ○ Enabled ● Disabled

SETTING UP A FIREWALL

Enable the firewall on your router for additional protection. 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.



Firewall Enable/Disable

Enable Firewall ☑ ?

DoS Attack Protection

Enable DoS Attack Protection Firewall ☑ ?

Block Pings

Enable Ping Blocking ☑ ?

Configure your router's firewall to block a variety of techniques used to compromise wireless networks

WHAT TO DO IF YOU SUSPECT YOUR NETWORK HAS BEEN COMPROMISED

Following the recommendations outlined in this card will significantly reduce your network's chances of becoming compromised. However, it is wise to periodically check to see 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 it is determined 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 resecure 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 was able to gain access to your login credentials or other personal data.

ONLINE REGISTRATION

ONLINE REGISTRATION - DO'S AND DON'TS

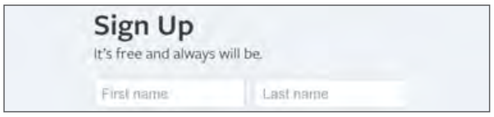
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with other parties.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access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

IDENTITY ELEMENTS OF SNS ACCOUNTS

Your online identity is the aggregate of your online accounts and their associated personal identity data fields. Therefore, protecting your identity must begin as early as registering your online accounts. The identity data shown below is often required when registering social network accounts.

FIRST AND LAST NAME

First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, use an alias or use the initial of your last name instead of its full version, especially if you have an uncommon last name.



Sign Up
It's free and always will be.
First name | Last name

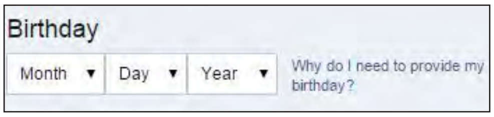
USERNAME

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, including 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.

BIRTHDAY

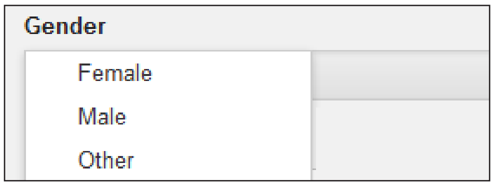
Birthdays are used to verify the user's age and customize age-appropriate content on the site. This information is sometimes published on the SNS profile and has to be removed retroactively. Only provide your true birth year.



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

GENDER

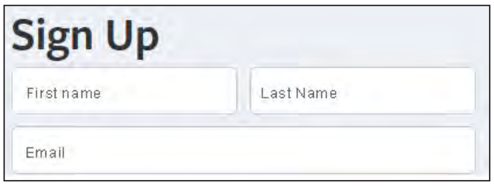
Gender is a common field to fill out on the registration page. Whenever possible, avoid making a distinction when signing up.



Gender
Female
Male
Other

EMAIL ADDRESS

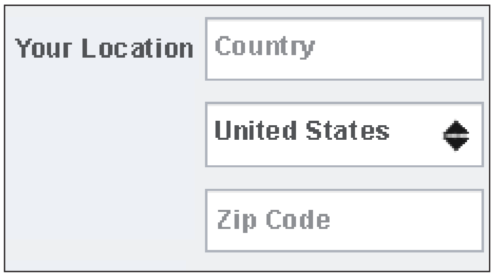
Email accounts are ubiquitous in online registration. Consider creating a unique email address for each SNS account you register.



Sign Up
First name | Last Name
Email

LOCATION INFORMATION

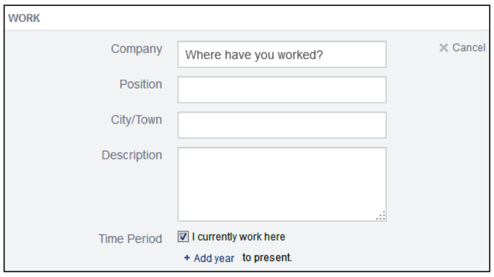
Location information is required at varied levels of granularity depending on the service. It may include address, city, ZIP code, and/or country. During sign up, only provide the most generic location level required by the service or consider entering a nearby ZIP code or metropolitan area.



Your Location | Country
United States
Zip Code

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 generic as possible (i.e. only provide the industry you work in). Avoid posting your employer and your work location.



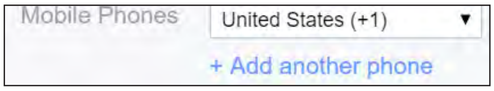
WORK
Company: Where have you worked? ✕ Cancel
Position:
City/Town:
Description:
Time Period: ☑ I currently work here
+ Add year to present.

SOCIAL LOGIN

Services may allow users to sign up through a preexisting social network (e.g. Google Plus, Twitter, or Facebook). Avoid opting for this step unless the service requires it.

MOBILE PHONE NUMBERS

Select accounts may ask to verify your identity via a personal 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

RELATIONSHIPS/ ORIENTATION

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

Relationship Status: Married ▼

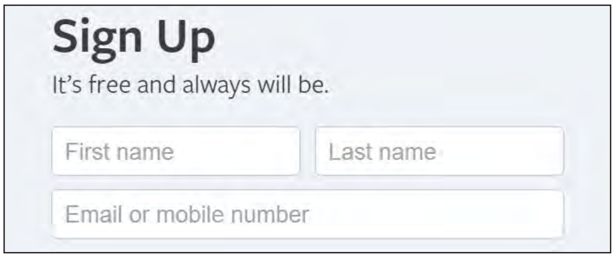
IDENTITY INFORMATION REQUIRED DURING REGISTRATION BY SERVICES

Service Name	Outlook	Yahoo	Facebook	Twitter	Google Plus	LinkedIn	Pinterest	Instagram	Yelp
First and last name	X	X	X	X	X	X	X	X	X
Username	X	X		X			X	X	
Password	X	X	X	X	X	X	X	X	X
Birthdate	X	X	X		X				Optional
Age							X		
Gender	X	X	X		X		X		Optional
Email address	X		X	Or Phone	X	X	X	X	X
Phone number	X	X		Or Email	Optional				
Country	X					X			
Company / Employment						X			
Job title						X			
ZIP code						X			X
Social Login		Optional				Optional	Optional	Optional	Optional

ONLINE REGISTRATION AND VERIFICATION PROCESS

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

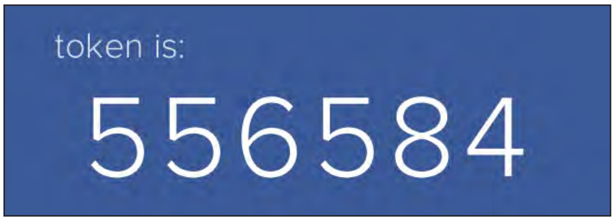
1. Enter required identity fields on the registration page. Avoid supplying more information than is required.



Sign Up

It's free and always will be.

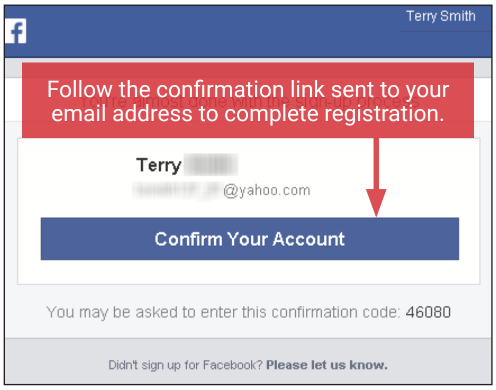
2. Consider using dual-factor authentication to add an additional layer of security to your account. Dual-factor authentication requires the user to verify an attempted login via email, text message, or an automatically generated code. When possible, use an application such as Authy or Okta that automatically generates a login code instead of providing your phone number for dual-factor authentication.



token is:

556584

3. Confirm your account via email, if possible. Avoid using mobile phones or other identity verification procedures in order to prevent further dissemination of your data.



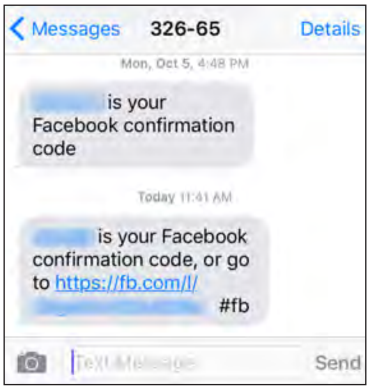
Follow the confirmation link sent to your email address to complete registration.

Terry [redacted]

[redacted]@yahoo.com

You may be asked to enter this confirmation code: 46080

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



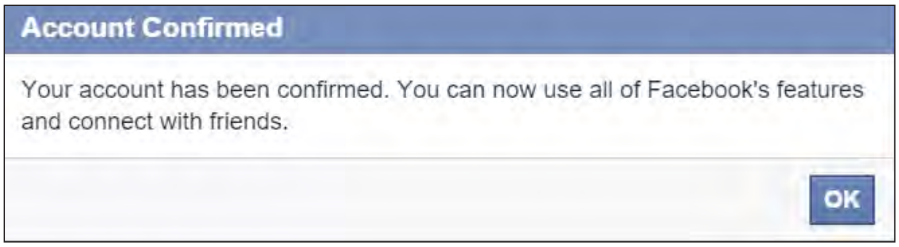
Mon, Oct 5, 4:48 PM

[redacted] is your Facebook confirmation code

Today 11:41 AM

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

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



Account Confirmed

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

OPTING OUT OF DATA AGGREGATORS

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

- Conduct research to see what records each data aggregator has collected about you and your loved ones.
- 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 collecting public records information and extensive web indexing + 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

PRIVATEEYE, PEOPLEFINDERS, PUBLICRECORDSNOW, AND VEROMI

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

Opt out of PrivateEye by visiting:
https://secure.privateeye.com/optout-form.pdf
Complete the form, and mail it to the listed address.

PrivateEye

Opt out of PeopleFinders and PublicRecordsNow by visiting:
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**. Select **No thanks, skip this step**.

peoplefinders find anyone, anywhere

PublicRecordsNOW Billions of Records at Your Fingertips

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.

Veromi

www.privateeye.com
www.peoplefinders.com

www.publicrecordsnow.com
www.veromi.com

INSTANTCHECKMATE

INSTANT checkmate

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

You can opt out by mail or online. You must include your full name, current address, email, and date of birth in order to opt out.

www.instantcheckmate.com

US SEARCH

Opt out of US Search by visiting http://www.ussearch.com/privacylock. Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax with a copy of a state-issued ID or driver's license to the listed address or fax number.
www.ussearch.com

US SEARCH BE INFORMED

INTELIUS, PUBLIC RECORDS, ZABASEARCH, SPOCK, ISEARCH, DATECHECK, LOOKUP, PEOPLEFINDER, LOOKUPANYONE, PEOPLE LOOKUP, AND PHONESBOOK

Intelius owns, or is affiliated with, the following people search websites: Public Records, Zabasearch, Spock, iSearch, DateCheck, LookUp, PeopleFinder, LookupAnyone, People Lookup, and PhonesBook. When you request removal of your records, also request removal from this network of sites. Opt out of Intelius online at http://intelius.com/optout.php. You can also fax your ID and a letter containing the information you want removed to 425-974-6194, using the following coversheet:

"As per your privacy policy, please remove my listing from Intelius, Spock, iSearch, ZabaSearch, Public Records, People Lookup, PhonesBook, DateCheck, LookupAnyone, and all other affiliated people search sites. Thank you for your help with this personal security issue."

INTELIUS Live in the know.

PublicRecords.com If it's out there, it's in here

ZABA® SEARCH

peoplesmart

People Lookup Your source for locating anyone!

phonesbook

www.intelius.com
www.zabasearch.com
www.peoplelookup.com
www.isearch.com

www.publicrecords.com
www.peoplesmart.com
www.phonesbook.com
www.lookupanyone.com

OPTING OUT INSTRUCTIONS CONTINUED...

BEEN VERIFIED

BeenVerified allows you to opt out at: beenverified.com/optout. Search for your listing, and claim it with the **That's Me!** button. Enter your email address. You must click the opt out link within the email sent to your account by the service.

www.beenverified.com/

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 and your email address. Go to your email, and click on the removal confirmation link.

www.spokeo.com

US IDENTITY

To opt out of US Identify, send a request to:

9450 SW Gemini Dr. Suite #29296
Beaverton, OR 97008-7105

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

Be sure to include aliases, if applicable.

www.usidentify.com

PEEKYOU

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

Under **Actions,** select **Remove my entire listing**. Paste the numbers at the end of your profile's URL in the 'UniqueID' field, fill in the CAPTCHA, and you're all set. You'll get an immediate 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.

www.peekyou.com

WHITEPAGES

Search for your information on Whitepages using your first name, last name, city, and state. Before deleting these records you must first register with the service. Click on your name in bold in the **Filter by Age** block. Copy the URL address at the top of your screen. Scroll down to the bottom of the screen and under **Your Whitepages** select **Remove From Directory**. On the Log In screen, select **Sign up**, and fill in your name, email address, and a new password. Select **Create an account.** You will be sent an email at the address you listed. Click the "Verify my email" link provided. Once you verify your email, you will then be taken to the **Opt-out of Whitepages** screen, paste the URL and click on **Opt-out.** If the information shown is correct, cLick on **Remove this info from Whitepages**. Select a reason from the drop down box and click on **Next step**. Verify the phone number, check the box, and click on **Call now to verify**. Answer the call and press 1.

www.whitepages.com

PIPL

Search for your information on pipl using your first name, last name, city, and state. Go to www.pipl.com/directory/remove. Ignore the instruction to copy the page address, and enter the page address in the format shown. Add your email address and click **SUBMIT.** The next page will show any listings with your name or a name close to it. Click **Remove** for each item you want deleted. You will be sent one or more emails at the address you listed. You must click on the confirmation link provided in each email.

www.pipl.com

IDENTITY THEFT PREVENTION

IDENTIFY THEFT PREVENTION - DO'S AND DON'TS

- Create unique passwords for each of your accounts to limit the chances of having multiple accounts compromised.
- Keep your computer up-to-date with the latest versions of your operating system and anti-virus software protection.
- Avoid sharing sensitive information such as credit card or Social Security numbers through text, email, 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, approximately 9.9 million incidents of identity theft are reported, equating to 19 individuals falling victim every minute. On average, each victim spends 30 to 60 hours and 50 to 500 dollars 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 assets at risk.

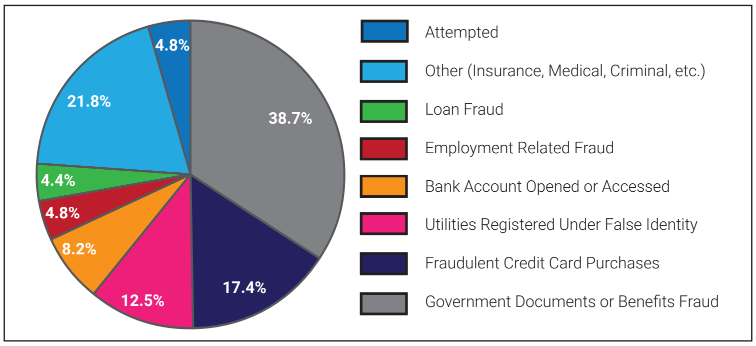
SENSITIVE DATA

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

POSSIBLY HARMFUL

- Pets' RFID Numbers
- Utility Account Numbers
- History of Residence
- Unsolicited Credit Offers

WHAT IS AT RISK?



*Data Source: Consumer Sentinel Network for total theft reports in 2014. Some reports contained multiple theft types.

ID THEFT TYPES

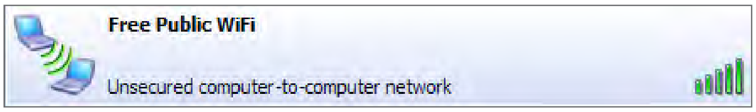
- Financial
- Insurance
- Medical
- Criminal
- Driver's License
- Social Security
- Synthetic
- Child

AGE OF VICTIMS

- 19 and Under (6%)
- 20 to 39 (36%)
- 40 to 59 (38%)
- 60 and Over (20%)

FAKE WIFI NETWORKS

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



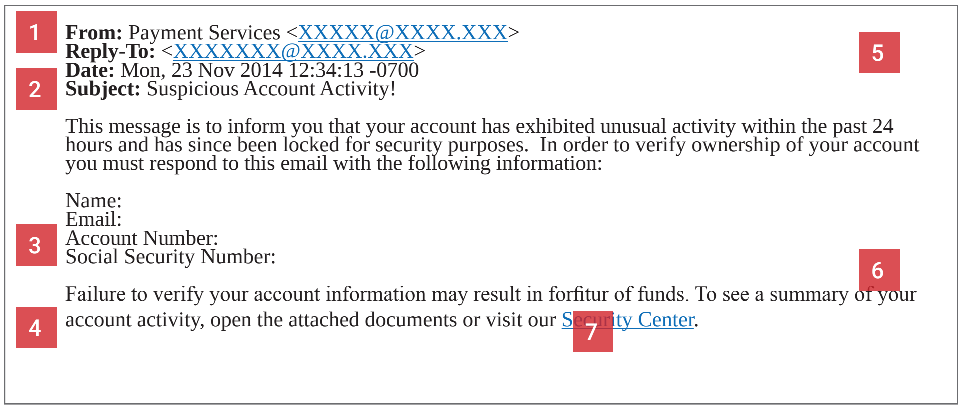
SOCIAL MEDIA MINING

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 a company logo within the email header.
6. Presence of grammatical or spelling errors.
7. Emails containing links to other pages or attachments may contain malicious scripts to install malware.



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

This message is to inform you that your account has exhibited unusual activity within the past 24 hours and has since been locked for security purposes. In order to verify ownership of your account you must respond to this email with the following information:

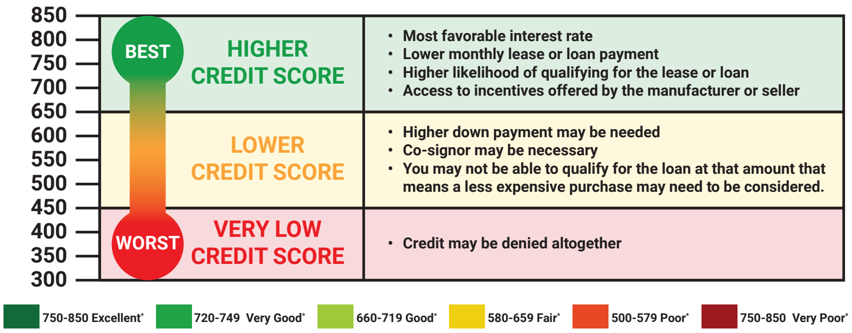
Name:
Email:
Account Number:
Social Security Number:

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

SIGNS OF IDENTITY THEFT

Credit scores are susceptible to damage through identity theft. However, damages from identity theft can be reduced significantly if caught early. Bank statements should be checked weekly, while each of the three credit reports should be checked once per year. The following occurrences may indicate a stolen identity:

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



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

IDENTITY THEFT PROTECTION SERVICES

Select companies offer services to monitor customers' credit scores and to protect their personal information online. Each company works with creditors to identify fraudulent activity and restore a customer's reputation. Most packages also offer financial reimbursements for significant personal losses. Individuals should still follow best practice guides to prevent the leak 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 www.IdentityGuard.com	X	X	X		X	X	Monthly	Up to $1 Million	$19.99
IdentityForce. Protect What Matters Most™	X	X	X	X	X	X	Quarterly	Up to $1 Million	$18.95
TrustedID® You're in control	X	X	X	X		X	Available	Up to $1 Million	$16.99

RESOLVING IDENTITY THEFT

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

Request Your Credit Scores:
Use www.annualcreditreport.com to request free copies of your credit scores. Look for inconsistencies amongst 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.

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

KEEPING YOUR KIDS SAFE ONLINE

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

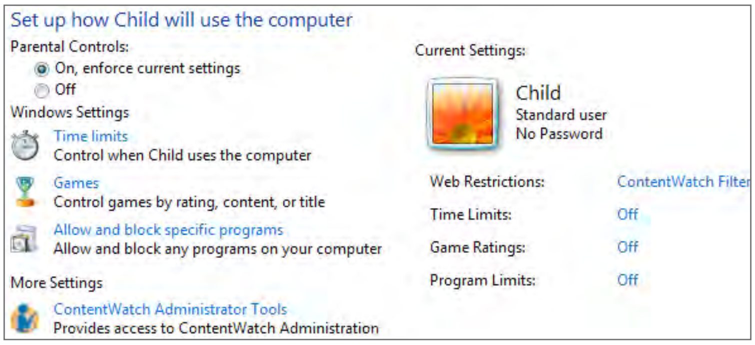
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you 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 don't use your face as a profile photo - use cartoons or avatars instead.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.

CHILD SAFETY ONLINE

A 2013 study reported that 96% of children above the age of 8 claimed to actively use the Internet, where kids are at risk of being exposed to cyber-bullying, coercion, pornography, drugs/alcohol, and violence. Dangers were not limited to the content that a child was subjected to, but also included the information that the child made available to the public through social networking services (SNS). The following web browser settings, add-ons, and software downloads are available to prevent and/or monitor a child's activities online.

INTERNET EXPLORER SETTINGS

To view child safety options, navigate to **Tools** > **Internet Options** > **Content**. Click **Parental Controls** (Internet Explorer 9) or **Family Safety** (Internet Explorer 10) to customize settings for the different accounts registered on the computer.



Set up how Child will use the computer

Parental Controls:

● On, enforce current settings

○ Off

Windows Settings

Time limits
Control when Child uses the computer

Games
Control games by rating, content, or title

Allow and block specific programs
Allow and block any programs on your computer

More Settings

ContentWatch Administrator Tools
Provides access to ContentWatch Administration

Current Settings:

Child
Standard user
No Password

Web Restrictions:	ContentWatch Filter
Time Limits:	Off
Game Ratings:	Off
Program Limits:	Off

PARENTAL CONTROLS

Adjust how your children can use the computer. Allow or block specific programs, and set personalized restrictions based on game ratings.

PASSWORDS

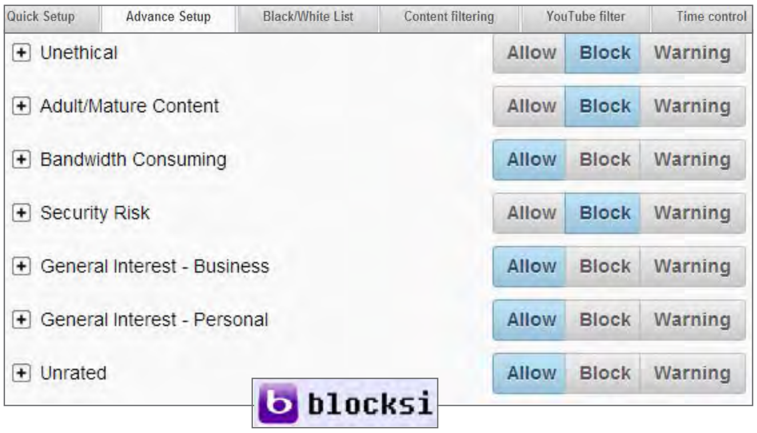
Create a password for your child's account that only you know.

TIME RESTRICTIONS

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

GOOGLE CHROME SETTINGS

Download the Blocksi extension from the Google Chrome Web Store to employ child safety settings for the Google Chrome browser.



+ Unethical	Allow [✓ Block] Warning
+ Adult/Mature Content	Allow [✓ Block] Warning
+ Bandwidth Consuming	[✓ Allow] Block Warning
+ Security Risk	Allow [✓ Block] Warning
+ General Interest - Business	[✓ Allow] Block Warning
+ General Interest - Personal	[✓ Allow] Block Warning
+ Unrated	[✓ Allow] Block Warning

ADVANCE SETUP

Allow, block, or warn users of certain content types. Select the "+" next to each type to set more granular restrictions.

FILTERS

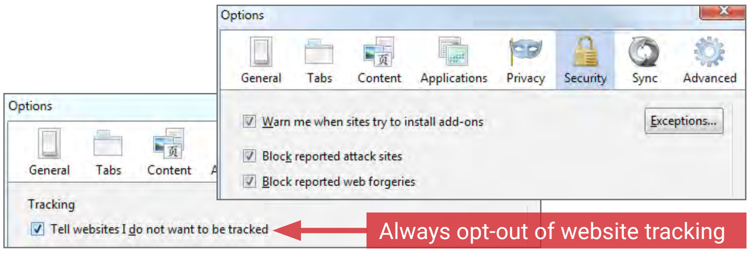
YouTube Filter - filters individual YouTube channels and videos for content.
Content Filtering - identifies specific words in webpages to prevent access.
Black/White List - allows users to add specific URL's to block or allow.

TIME CONTROL

Set a time frame of acceptable computer use for your child that permits an adult supervisor to be present.

FIREFOX SETTINGS

STANDARD FIREFOX: Navigate to **Firefox** > **Options** > **Privacy** to prevent web tracking and **Firefox** > **Options** > **Security** to block sites with malicious content.



☑ Warn me when sites try to install add-ons

☑ Block reported attack sites

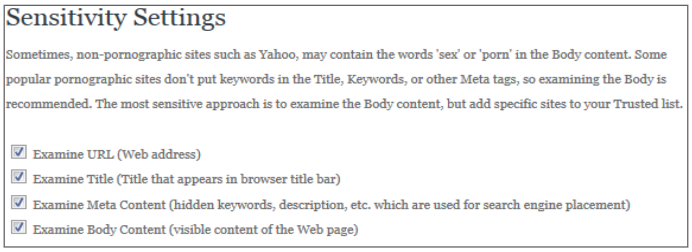
☑ Block reported web forgeries

Tracking

☑ Tell websites I do not want to be tracked

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 sites, and set sensitivity settings.



Sensitivity Settings

Sometimes, non-pornographic sites such as Yahoo, may contain the words 'sex' or 'porn' in the Body content. Some popular pornographic sites don't put keywords in the Title, Keywords, or other Meta tags, so examining the Body is recommended. The most sensitive approach is to examine the Body content, but add specific sites to your Trusted list.

☑ 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)

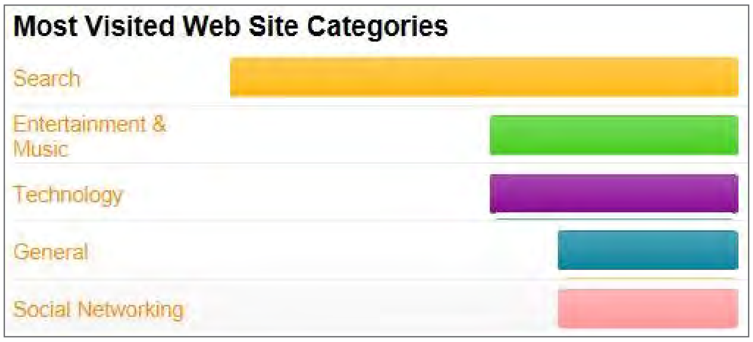
OVERVIEW

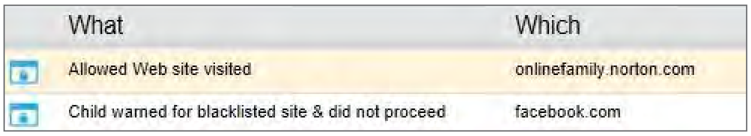
A variety of free and paid software are available for monitoring your child's online activities. The software listed below are effective in either preventing or monitoring content that your child tries to access.

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

NORTON FAMILY

Register online with this service to monitor your child's online activity. This service allows parents to track which websites children visit and prevent certain harmful content from being displayed on their monitors. Information reported to the parent includes websites visited, timestamps, searches conducted, and actions taken by the Norton Family security suite.


Most Visited Web Site Categories

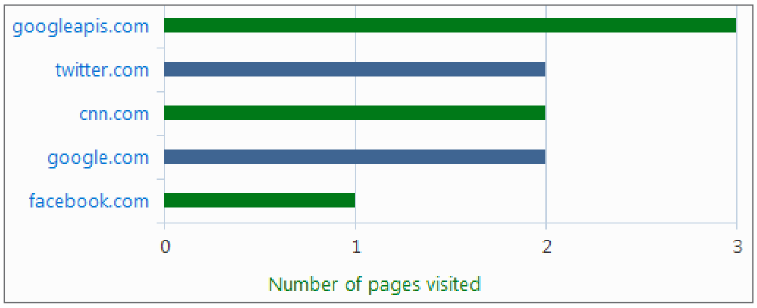


	What	Which
	Allowed Web site visited	onlinefamily.norton.com
	Child warned for blacklisted site & did not proceed	facebook.com

Norton Family 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

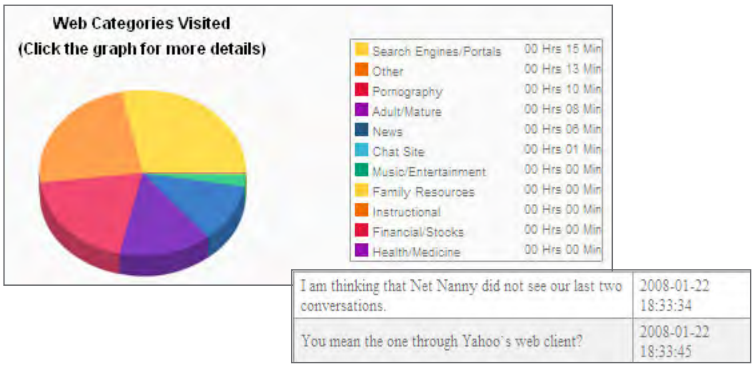
Download this free service from the Microsoft Windows website. The service provides basic content filters and reports of programs/websites accessed by each account.



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

NET NANNY

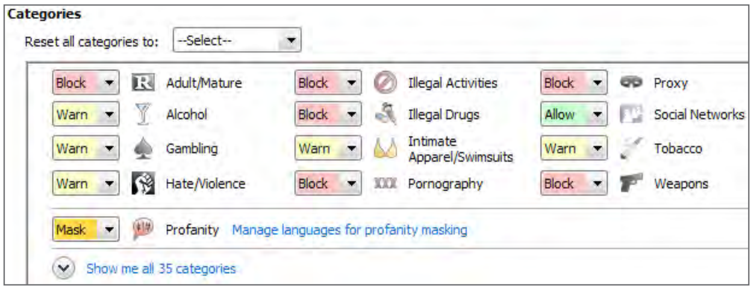
This service is available for download for $39.99 and can both prevent and monitor content from computer programs, instant messengers, SNS, and web browsing applications. It is installed onto the desktop and provides the most granular settings for filtering and reporting potentially harmful content.


Web Categories Visited
(Click the graph for more details)

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

I am thinking that Net Nanny did not see our last two conversations.	2008-01-22 18:33:34
You mean the one through Yahoo`s web client?	2008-01-22 18:33:45

Parents can respond to their child's permission requests remotely from a mobile app or computer in real time. Additional settings include blocking 64 Bit applications, HTTPS connections, proxy servers, blogs, and chat rooms. Net Nanny displays an extensive list of SNS and instant messengers as well as 35 categories of potentially harmful content to screen.

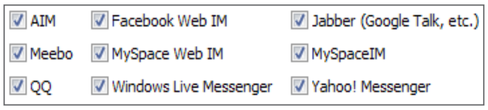

Categories

Reset all categories to: --Select--

Block	Adult/Mature	Block	Illegal Activities	Block	Proxy
Warn	Alcohol	Block	Illegal Drugs	Allow	Social Networks
Warn	Gambling	Warn	Intimate Apparel/Swimsuits	Warn	Tobacco
Warn	Hate/Violence	Block	Pornography	Block	Weapons

Mask Profanity Manage languages for profanity masking

Show me all 35 categories


☑ AIM ☑ Facebook Web IM ☑ Jabber (Google Talk, etc.)
☑ Meebo ☑ MySpace Web IM ☑ MySpaceIM
☑ QQ ☑ Windows Live Messenger ☑ Yahoo! Messenger

VOIP

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

- Determine the features you need. VOIP services range from free smartphone apps to full-featured subscription enterprise systems.
- Check your bandwidth. You may need to upgrade your Internet connection to get the best use of bandwidth-heavy VOIP services.
- Keep a landline or cellphone active for times when Internet service is not available, power is out, or for calls to emergency services.
- Watch your wallet. Keep an eye out for hidden charges for licensing and support or free trials that may 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, or 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, 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 WiFi.

BENEFITS OF VOIP

VOIP calls are much less expensive, 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.

CHOOSING THE RIGHT PROVIDER

- 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 companies?
- Is live support available 24 hours a day, seven days a week?

VOIP DISADVANTAGES

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

A poor Internet connection can result in low call quality, delayed messages, or buffering during video chats.

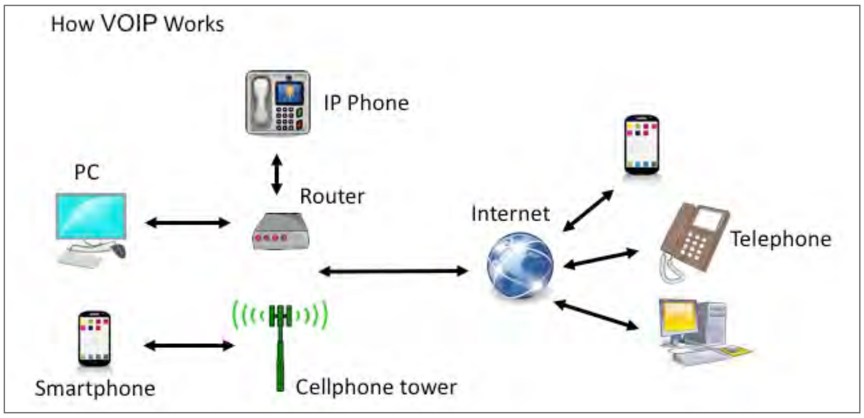
Some providers do not connect to 911 or information services, so a second phone line may be needed.

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.

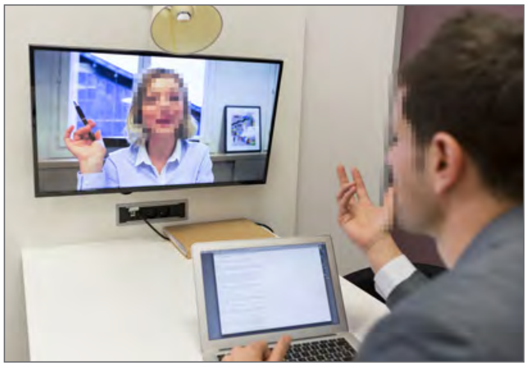
VOIP is vulnerable to routine computer disruptions, including crashes and malware.



USING VOIP SECURELY

Password-protect your apps, and encrypt or erase sensitive information, including texts, call history and voicemail. **But keep in mind even if a service offers encryption, some providers may include a "back door" to allow for lawful government surveillance of communications, i.e. during a criminal investigation.** 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?
- Be sure your WiFi network is password-protected and uses strong encryption (WPA2).
- Change default passwords on equipment and the remote-management interface.

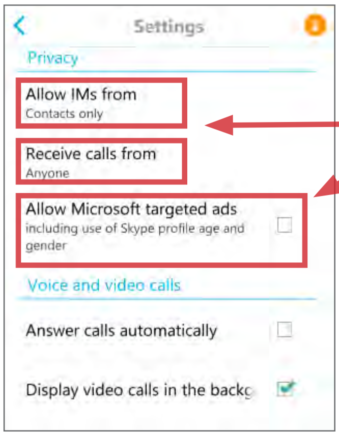


SERVICE	OPERATING SYSTEM	COST	BEST USES	SECURITY RATING*
skype	Windows, Mac, iOS, web, Android	Free to $13.99/ month	Filesharing, screen sharing, document collaboration, video calls	★☆☆☆☆
Google+ Hangouts	iOS, Android, web	Free	Encrypted one-to-one or group audio/video calls, livestreaming video	★★☆☆☆
SILENT CIRCLE	iOS, Android, Windows	$12.95 to $39.95/month	Anonymous, encrypted calls and messages, identity verification	★★★★★
FaceTime/ iMessage	iOS, Mac	Free	Encrypted audio and video calls and messages, voice memos	★★★★☆
BlackBerry	Blackberry, iOS, Android	$29.99/yr for BBM Protected	Secure messaging	★★☆☆☆
Crypto-cat	iOS, Mac, web	Free	Secure messaging, encrypted filesharing	★★★★★

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.
Among the most popular services:
Ooma: $129 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.

** The rating is based on encryption protocols, code reviews, audits, and documentation as compiled by the Electronic Frontier Foundation in March 2015.*

SKYPE


Settings

Privacy

Allow IMs from
Contacts only

Receive calls from
Anyone

Allow Microsoft targeted ads
including use of Skype profile age and gender ☐

Voice and video calls

Answer calls automatically ☐

Display video calls in the backg ☑

Navigate to **Settings** in the pull-out menu:

- Indicate who you want to be able to call or instant message you.
- Be sure **"Allow Microsoft targeted ads"** is not checked to keep your profile information (age, gender, or location) or app usage from being used to serve ads.

On the **"My Profile"** page, do not upload a picture or enter personal information, such as your name, birthday, city, gender, or bio.

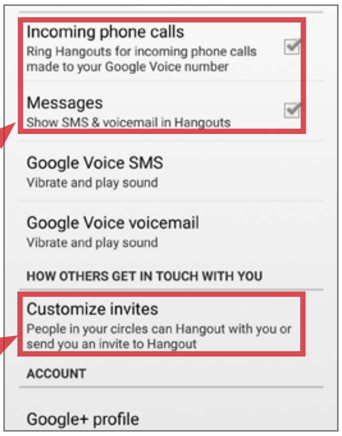
HANGOUTS

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

Install Hangouts app. In main screen menu, choose **"turn history off."**

In **Settings**:

- Check **"Incoming phone calls"** and **"Messages"** for Hangouts to manage all calls, texts, and voicemail.
- Customize who can contact you directly and who needs an invite.


Incoming phone calls
Ring Hangouts for incoming phone calls made to your Google Voice number ☑

Messages
Show SMS & voicemail in Hangouts ☑

Google Voice SMS
Vibrate and play sound

Google Voice voicemail
Vibrate and play sound

HOW OTHERS GET IN TOUCH WITH YOU

Customize invites
People in your circles can Hangout with you or send you an invite to Hangout

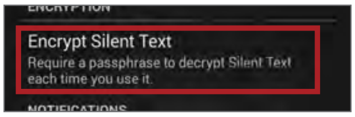
ACCOUNT

Google+ profile

SILENT CIRCLE

On launch, swipe right and check **"Start silent phone on boot."**

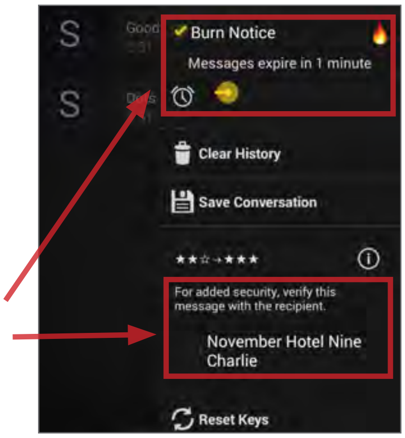
In **Settings**, select **"Encrypt Silent Text"** and select a passphrase (14 characters is recommended).


ENCRYPTION

Encrypt Silent Text
Require a passphrase to decrypt Silent Text each time you use it

NOTIFICATIONS

Activate **"Burn Notice"** in a conversation to auto-delete messages. To verify users, confirm passphrase by phone and tick box.


✓ Burn Notice
Messages expire in 1 minute

Clear History

Save Conversation

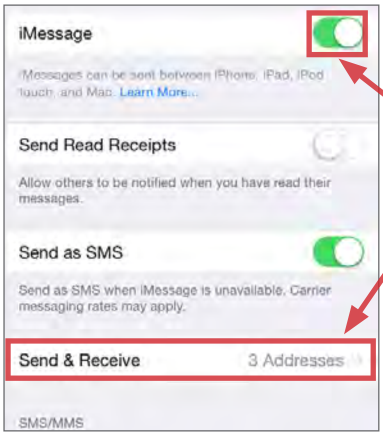
★★☆→★★★

For added security, verify this message with the recipient.

November Hotel Nine Charlie

Reset Keys

FACETIME


iMessage

Messages can be sent between iPhone, iPad, iPod touch, and Mac. Learn More...

Send Read Receipts

Allow others to be notified when you have read their messages.

Send as SMS

Send as SMS when iMessage is unavailable. Carrier messaging rates may apply.

Send & Receive 3 Addresses

SMS/MMS

For security, be sure to enable two-factor authentication for FaceTime.

- Go to **Settings > Messages** and turn on iMessage. Then tap **"Send & Receive"** and sign in with your Apple ID and password.
- Go to **Settings > FaceTime** and turn on FaceTime. Follow the steps to sign in and link your phone number to your Apple Id.

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA