IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

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

SECOND EDITION AUGUST 2015

BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

TABLE OF CONTENTS

Useful Links and Resources - For questions or more information email osd.ncr.osd.mbx.dodsmartcards@mail.mil

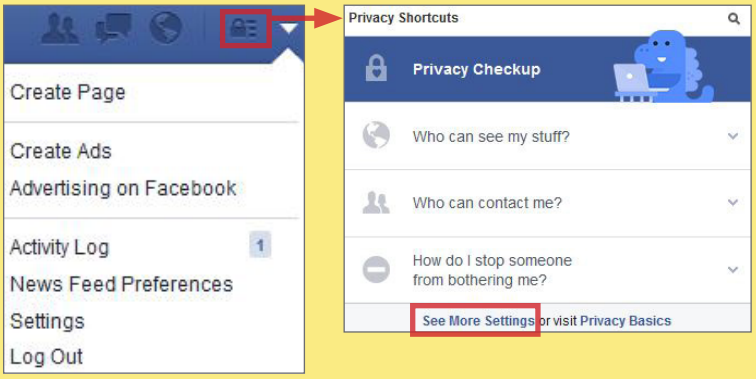
- IdentityTheft.gov (by the FTC) https://www.identitytheft.gov/
- A Parent's Guide to Internet Safety www.fbi.gov/stats-services/publications/parent-guide
- Microsoft Safety and Security www.microsoft.com/security/online-privacy/social-network
- Online Guardian www.onguardonline.gov/topics/social-networking-sites.aspx
- About Money http://idtheft.about.com/od/identitytheft101/
- Protect My ID www.protectmyid.com/identity-theft-protection-resources
- Privacy Right Clearinghouse 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

FACEBOOK

SOCIAL NETWORK - DO'S AND DON'TS

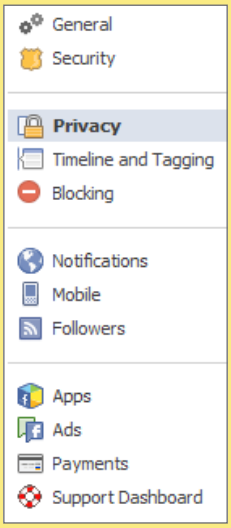
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts;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

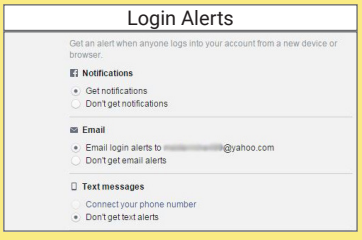
2 **Timeline and Tagging** controls how others interact with your timeline. Select **View As** to preview what others can see on your profile.

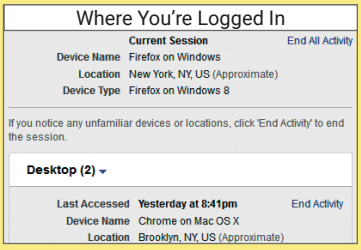
Who can add things to my timeline?	Who can post on your timeline?	**Friends**	Edit
	Review posts friends tag you in before they appear on your timeline?	**On**	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your 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.

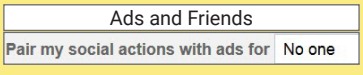
Who Can Follow Me	Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with.	Friends

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.

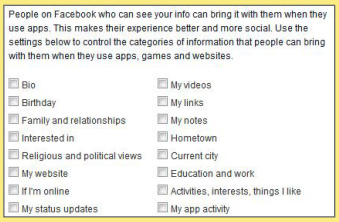




5 Use the **Ads** tab to prevent Facebook from using your data for advertising. Set **Third Party Sites** and **Ads & Friends** fields to 'No One'.



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.



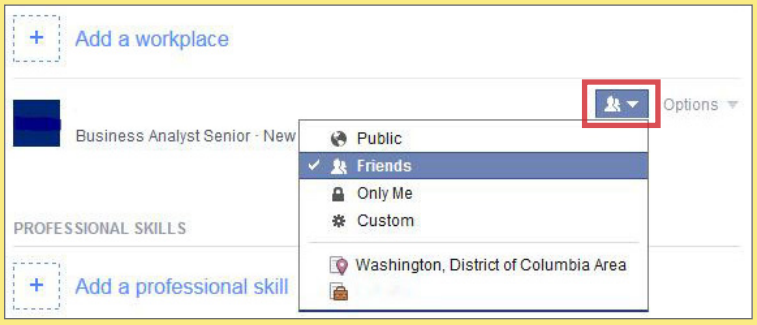
Avoid linking third-party apps (e.g. Twitter) with your Facebook account. Data shared with other apps becomes subject to their terms and conditions which may result in unwanted data aggregation and dissemination.

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

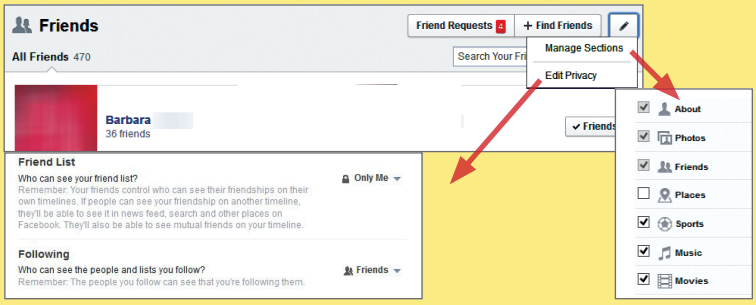
Avoid entering personal data within the **About** section. This information is mostly optional and contains data fields including **Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships,** and **Details About You**. Use the audience settings to change the mandatory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



FRIENDS

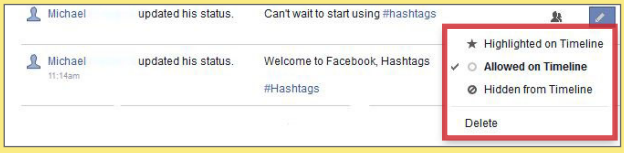
Under the **Friends** Tab:

- 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.



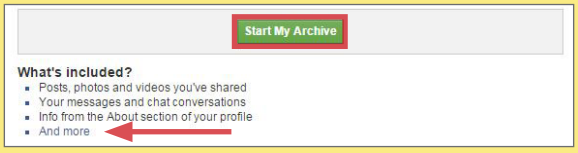
VIEW ACTIVITY LOG

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.

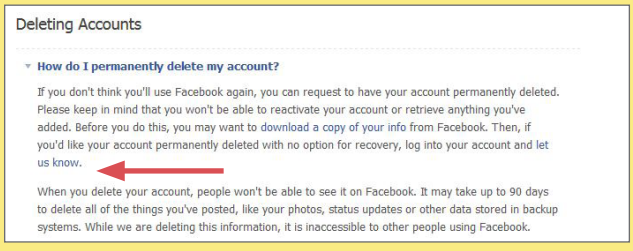


REVIEWING YOUR INFORMATION

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.



DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT



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

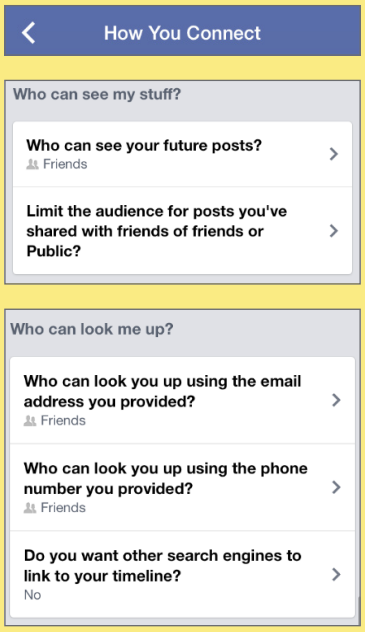
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that anyone can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their account;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

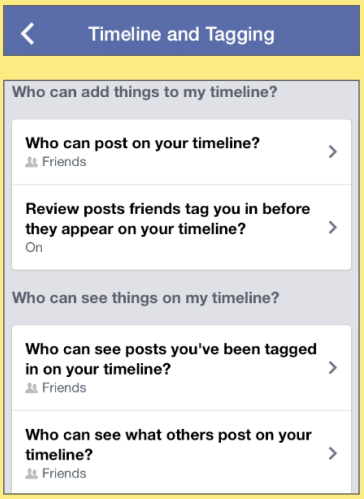
FACEBOOK MOBILE OVERVIEW

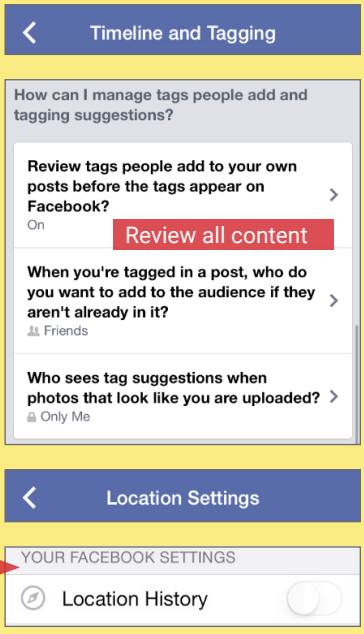
As of January 2015, Facebook Mobile hosted 745 million daily mobile active users who accounted for over 60% of all the mobile posts published to any online social networking service. Though privacy can still be achieved, these mobile users place their personal identity data at a greater risk when compared 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.

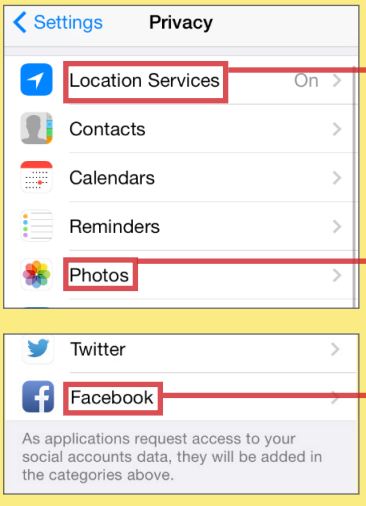


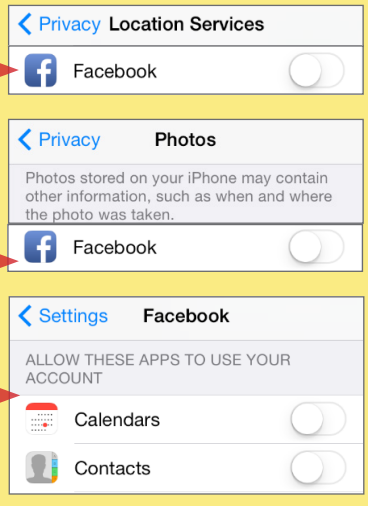




IPHONE SETTINGS

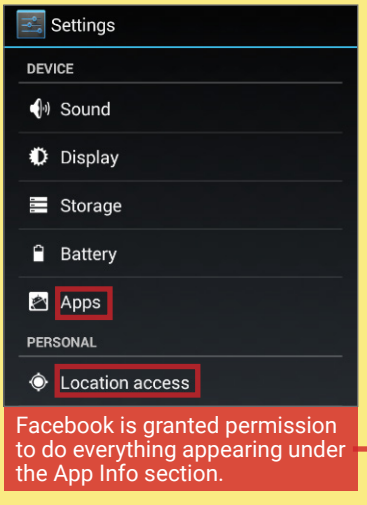
The iPhone's security settings can help to further protect your personal data while you use the Facebook Mobile App. From the iPhone's **Settings** icon, select **Privacy** and navigate through the **Location Services**, **Photos**, and **Facebook** tabs to disable all of the permissions, as seen below.

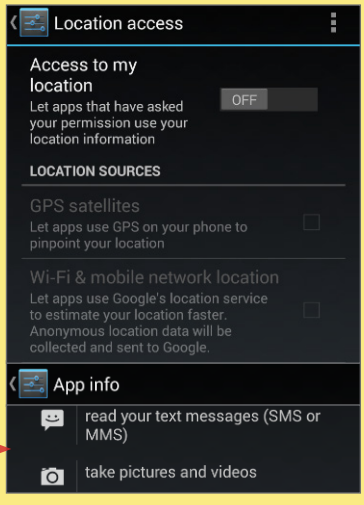




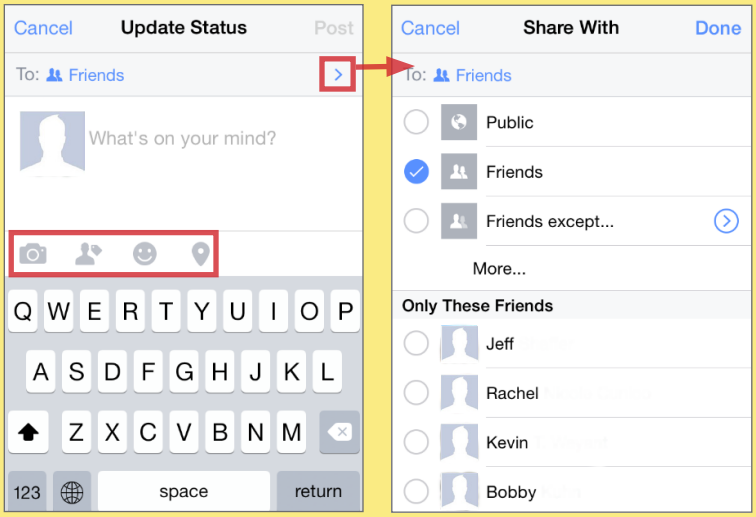
ANDROID SETTINGS

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 amount of data that Facebook can retrieve from your mobile device.

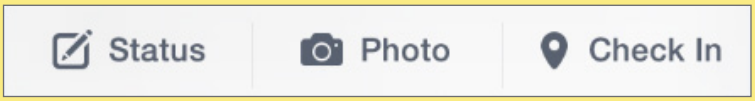




POSTING TO FACEBOOK



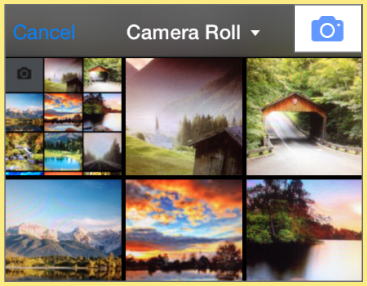
Facebook Mobile allows you to post new statuses, upload photos, or check-in to locations, using the **Update Status** prompt. The icons highlighted on the update prompt are shortcuts for adding further information about you to each post. Follow the guidelines outlined in this section to prevent over-sharing your information and to maximize your security. Remember, it is always best to limit the amount of personal information shared online.



SELECTING YOUR AUDIENCE

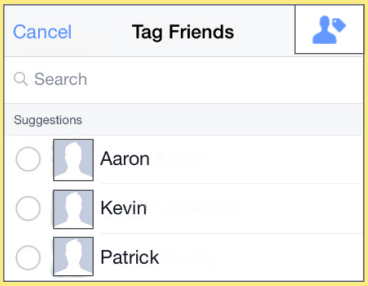
With every post, Facebook Mobile allows you to select the audience through the **Share With** prompt. For maximum privacy, select individual friends with whom you would like to share your post. Never make your posts available to the public.

ADD PHOTOS



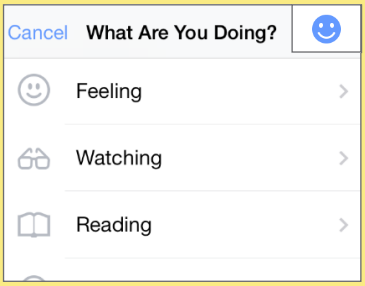
Avoid posting photos to timelines. These photos can often be viewed from your contacts' profile pages and can be saved without your knowledge or consent.

TAG FRIENDS



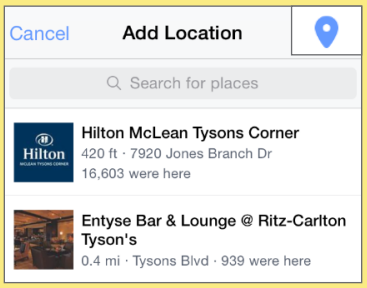
Tagging friends in individual posts extends the reach of your profile and your contacts' profiles. Limit the number of tags you post to your Facebook entries.

WHAT ARE YOU DOING?



This feature does not pose an immediate threat to your privacy. However, Facebook likely uses this information to push targeted ads to you based on your activities.

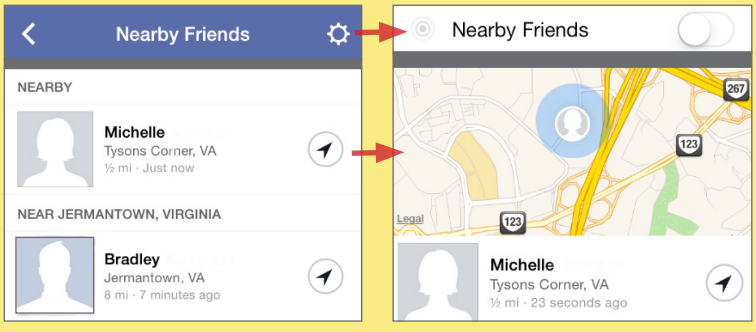
ADD LOCATION



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

NEARBY FRIENDS

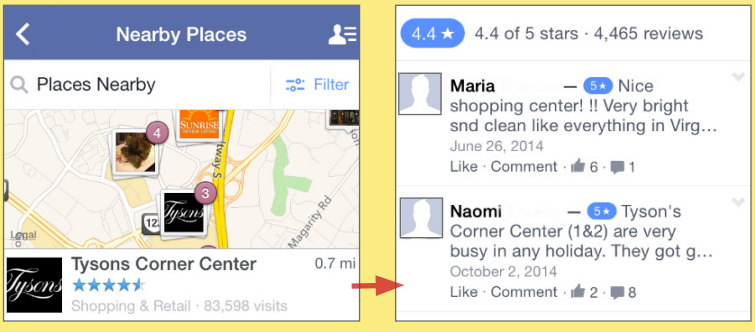
Nearby Friends allows you to share your location with friends. When activated, it routinely broadcasts your approximate locations to your friends. You also have the option to allow certain users to see your precise location for set periods of time.



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 displays the distance to and ratings from other users about the destination. When a venue is selected, individual reviews appear with links to the posters' profiles. Don't post on these public threads.



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

TWITTER

SOCIAL NETWORK - DO'S AND DON'TS

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

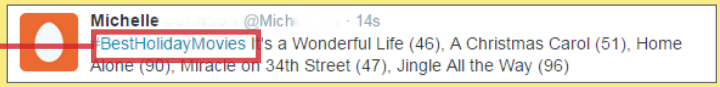
MANAGING YOUR TWITTER ACCOUNT

Twitter is a social networking and micro-blogging site whose users send and read text-based posts online. As of July 2014, the site hosted approximately 284 million daily active users, generating 58 million Tweets, and 2.1 billion search engine queries daily.

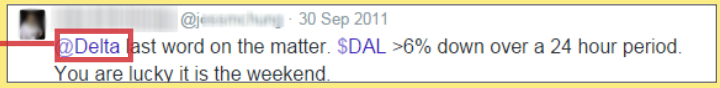
TWEETS

"Tweets" are short text-based messages - up to 140 characters - that users post to Twitter. A "Tweet" can refer to a post or to the act of posting to Twitter. Tweets are public, indexed, and searchable unless protected by the user. Many users never Tweet, choosing only to follow persons or topics of interest.

Hashtags (#[topic]) are used to highlight a keyword or topic in a post. Tweets with hashtags are searchable within the Twitter search engine. Hashtagged words that appear most often turn into trending topics (ex. #Grammys2015).

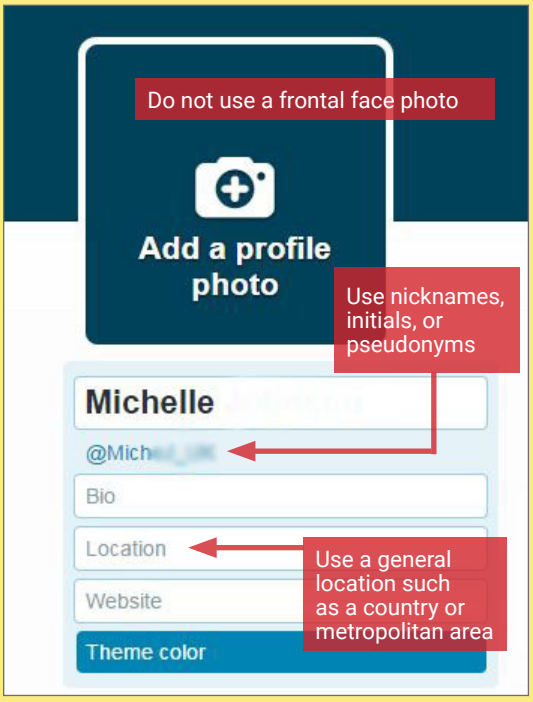


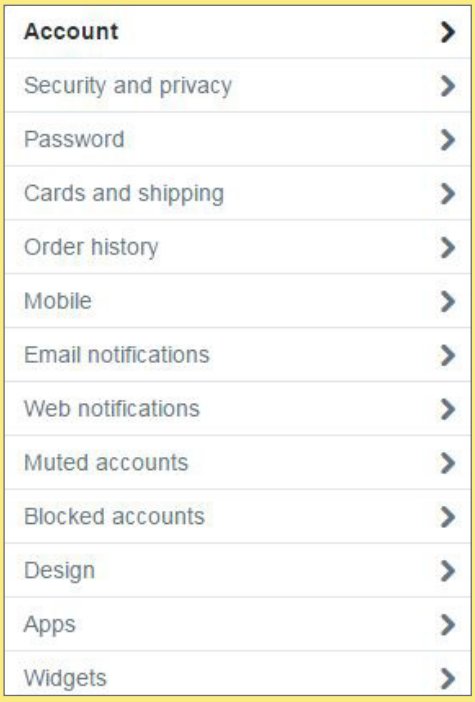
Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the profile of the private account becomes visible to the public.



PROFILE SETTINGS

Apply the profile and other settings shown to ensure that your information is visible only to the people of your choosing.



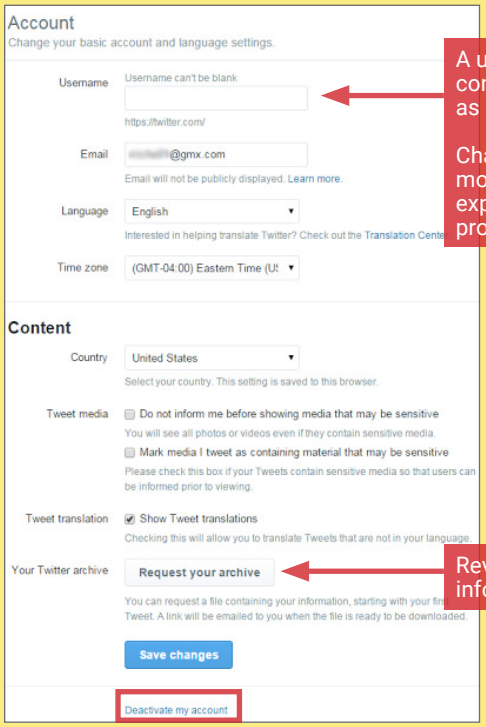


TWITTER BEST PRACTICES

- Avoid using hashtags (#) in updates to prevent Twitter from indexing and extending the reach of your posts
- Tweet responsibly. Do not share personal details regarding your whereabouts or activities within your posts.
- Do NOT share links to personal photos or other online profiles through Twitter.
- Do NOT allow Twitter to use your location on mobile devices.
- Switch your Twitter username quarterly to limit your account's exposure.

ACCOUNT SETTINGS

Apply the **Account** settings shown below to ensure that your information is shared in a limited fashion.



A username is also commonly referred to as a Twitter Handle.

Change it every 6 months to limit the exposure of your profile

Review your posted information regularly

DEACTIVATE & DELETE YOUR TWITTER ACCOUNT

To deactivate your account, got to **Settings** and select **Account**. At the bottom of the page, click **Deactivate my account**. You can only reactivate the account within 30 days after deactivation.

SECURITY AND PRIVACY SETTINGS

Apply the **Security** and **Privacy** settings recommended below to protect and reduce the visibility of your personal information.

Require information to reset passwords

Do NOT allow others to tag you in photos

Protecting your Tweets makes all your posts private. Only those who you approve can access your Tweets

Do NOT add locations to your Tweets

Do NOT allow others to find your account by email

Do NOT allow Twitter to use third-party data for promotion or personaliztion.

NOTIFICATIONS & APPS SETTINGS

Set up notifications to help you track the progression of your posted content. Revoke access to all unnecessary third-party applications.

Twitter updates may highlight new security tools or possible risks

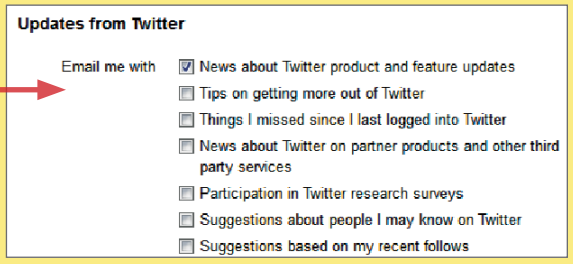
For maximum security:

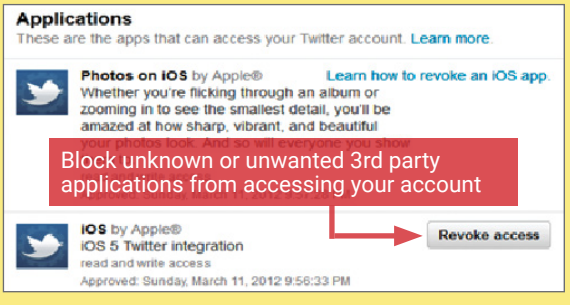
Check All and Set to **By Anyone**

Notes:

Private Tweets cannot be re-Tweeted

Direct messages are never visible to the public





Block unknown or unwanted 3rd party applications from accessing your account

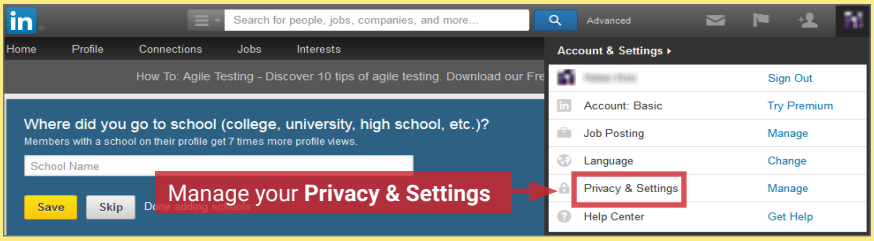
LINKEDIN

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.
- 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.

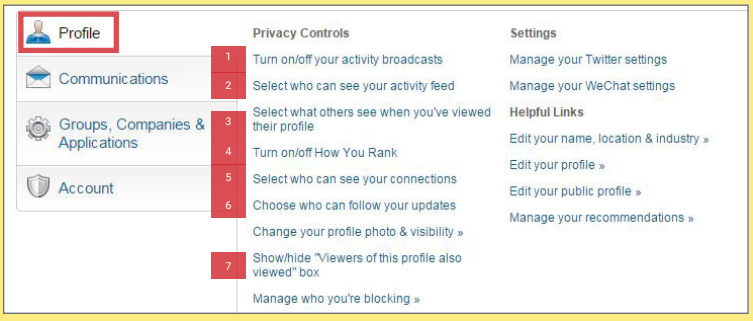
MANAGING YOUR LINKEDIN PROFILE

LinkedIn is a professional networking service that allows you to establish connections with co-workers, customers, business contacts, and potential employees or employers. You can post and share information about current and previous employment, education, military activities, specialties, and interests. To limit exposure of your personal information, you can manage who can view your profile and activities.



PROFILE SETTINGS

Apply the **Profile** settings shown below to ensure that your information is visible only to the people of your choosing.



1 ACTIVITY BROADCASTS

By selecting this option, your activity updates will be shared in your activity feed.

☐ Let people know when you change your profile, make recommendations, or follow companies

Note: You may want to turn this option off if you're looking for a job and don't want your present employer to see that you're updating your profile.

Uncheck

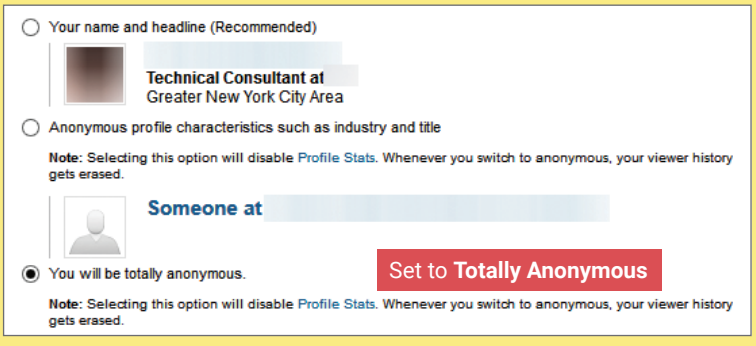
2 WHO CAN SEE YOUR ACTIVITY FEED

Your activity feed displays actions you've performed on LinkedIn. Select who can see your activity feed.

Only you ▾

Set to **Only You**

3 WHAT OTHERS SEE WHEN YOU VIEW PROFILES



4 TURN ON/OFF HOW YOU RANK

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.

☐ Let others see how you rank

Uncheck

5 WHO CAN SEE YOUR CONNECTIONS

Select who can see your list of connections. Note: 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.)

Only you ▾

Set to **Only You**

6 WHO CAN FOLLOW YOUR UPDATES

Choosing Everyone lets people outside your network follow your public updates. If you switch from Everyone to Your connections, you'll lose any out-of-network followers you have now. Any changes you make will take about 24 hours to take effect.

Your connections ▾

Set to **Your Connections**

7 VIEWERS OF THIS PROFILE ALSO VIEWED...

☐ Display "Viewers of this profile also viewed" box on my Profile page

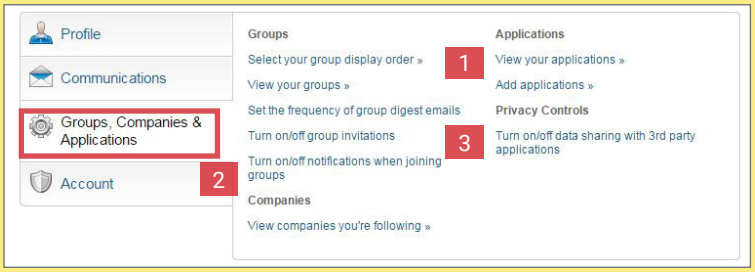
Uncheck

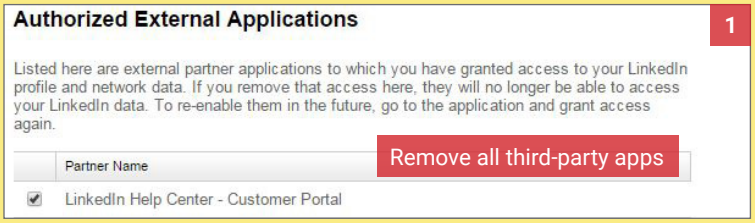
LINKEDIN QUICK FACTS

- There are over 330 million LinkedIn users around the world. The service is widely adopted in the US, India, Canada, and the UK.
- 43% of users invest 0-2 hours per week on LinkedIn; 30% spend more than 4 hours per week.
- Users tend to share information related to their careers or jobs opposed to photos or text referencing social events.
- Compared to free accounts, paid LinkedIn accounts have access to more information about other users who viewed their profiles.

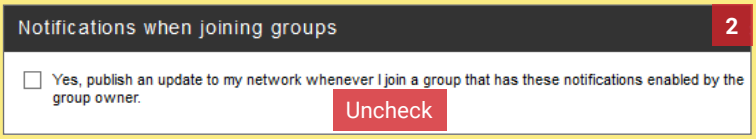
APPLICATION SETTINGS

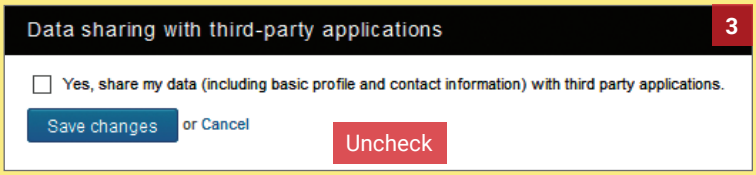
Apply the **Groups, Companies, & Applications** settings shown below to minimize the amount of information you share with third-parties.





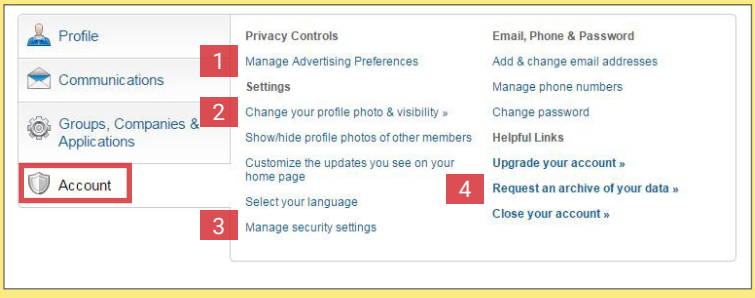
Granting third-party applications access to your LinkedIn account places your data at risk of unwanted collection and distribution. It is best not to tether applications to the LinkedIn service and to avoid using the LinkedIn smartphone app in order to prevent further data aggregation. Remember, LinkedIn actively records your online activity and reports comprehensive summaries about you through the Bing search engine.

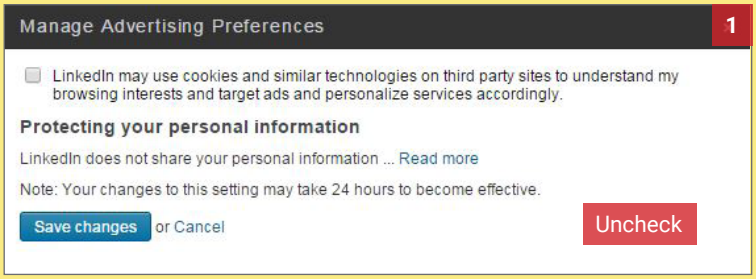


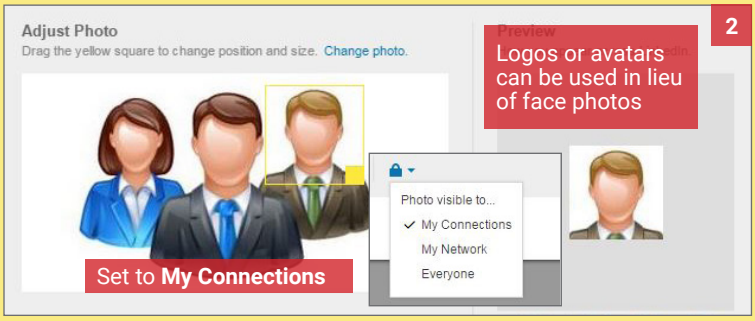


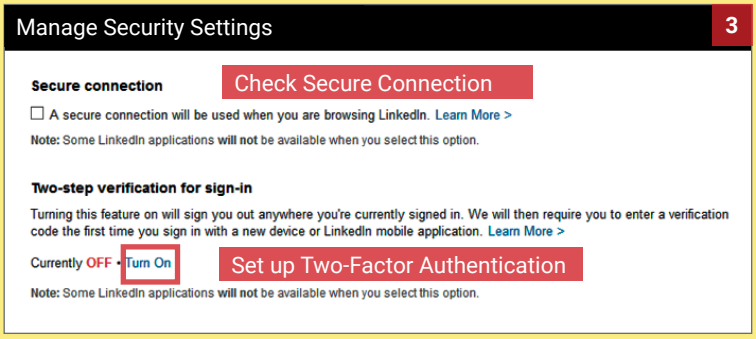
ACCOUNT SETTINGS

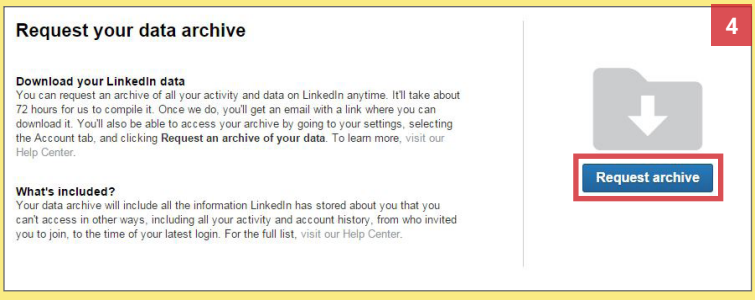
Apply the **Account** settings shown below to ensure that your information is visible only to the people of your choosing.











REQUEST DATA ARCHIVE

LinkedIn maintains an archive detailing each user's unique account activity. Select **Request Archive** to receive a comprehensive report of your past activity and network information. Review your data frequently to ensure that you are not over-sharing information. Visit the **Help Center** to see the types of information LinkedIn collects.

CLOSING YOUR LINKEDIN ACCOUNT

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

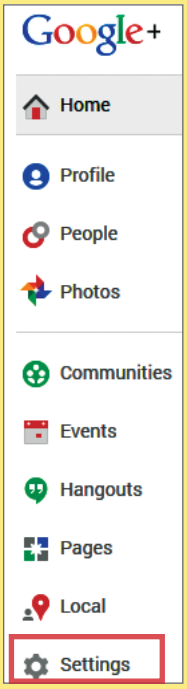
GOOGLE+

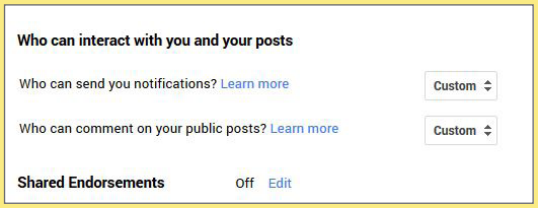
SOCIAL NETWORK - DO'S AND DON'TS

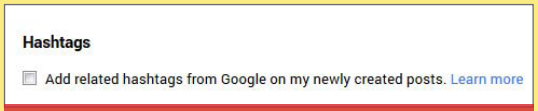
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts;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

GENERAL SETTINGS

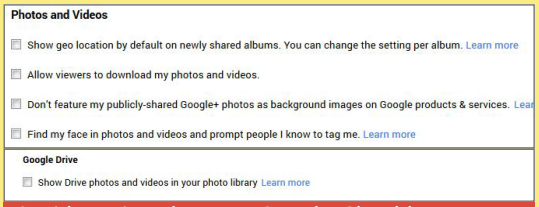
The general settings for Google+ allow you to select how your data appears and how others can interact with your profile. Using the dropdown menu from the profile page, navigate to **Settings**, and apply the following options in order to increase your profile's security.



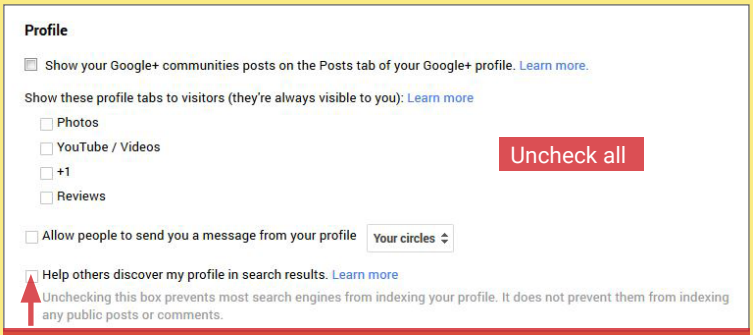




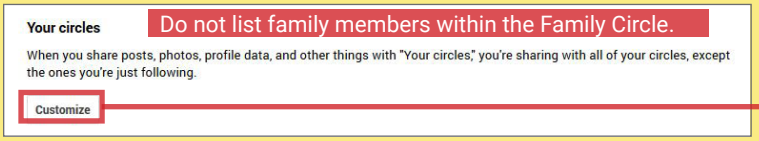
Google sometimes adds hashtags to posts to make them more discoverable. Uncheck.



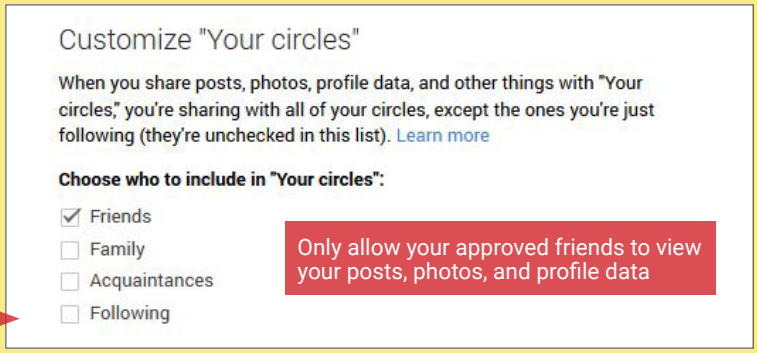
Avoid posting photos to Google. Should you choose to post photos, ensure that the **Photos and Videos** options are unchecked, as seen above.



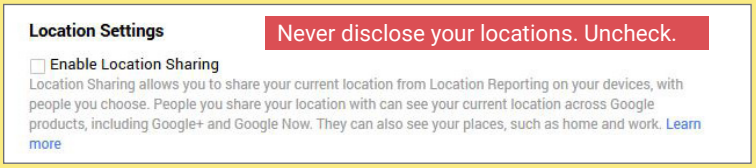
Unchecking this box prevents most search engines from indexing your profile. However, it does not prevent them from indexing any public posts or comments posted to the network.



Do not list family members within the Family Circle.

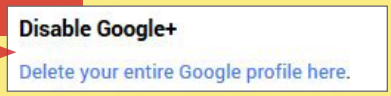


Only allow your approved friends to view your posts, photos, and profile data



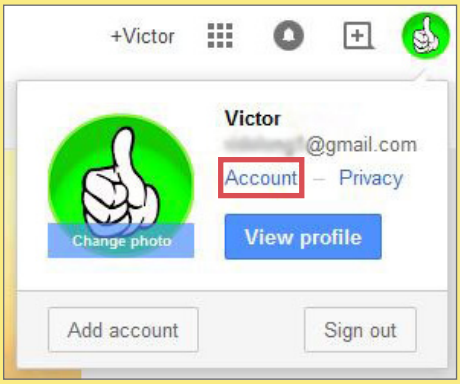
Never disclose your locations. Uncheck.

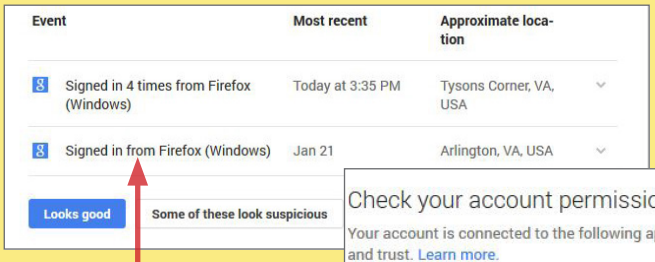
Google allows you to opt out of Google+. This does not delete your Gmail or other Google services' functionalities.



ACCOUNT SETTINGS

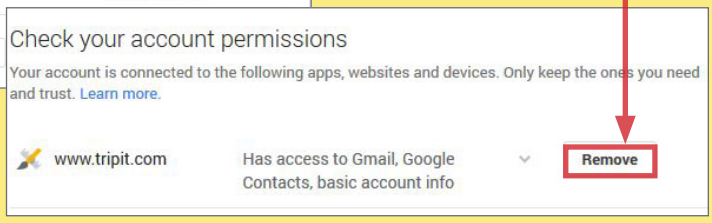
Select **Account** from the dropdown menu shown, and perform the **Security Checkup** to review your logins and account permissions.





Review your past logins to identify suspicious or unauthorized activity

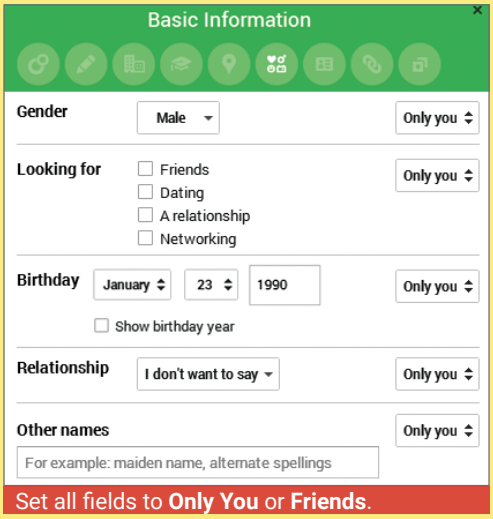
Avoid linking your account to third-party services. Remove any apps or websites that currently have access to your data.



PROFILE SETTINGS

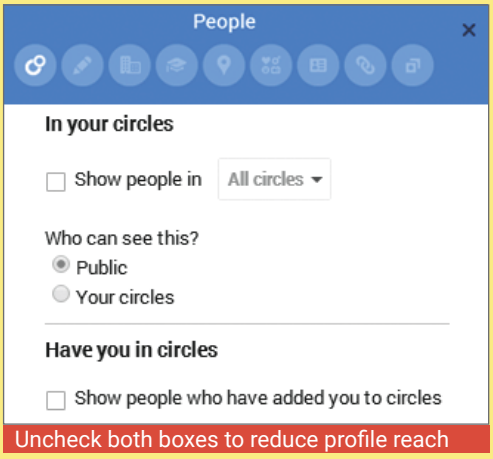
Click the **About** tab to display the 9 personal data fields for your account. Select **Edit** within each card to display the options shown below. These windows allow you to alter your personal information and the audiences who can see your information. Remember, these data fields are mostly optional, and it is always best to limit the amount of personal information you share online. Use the table below to select the audience settings best suited for your profile.

AUDIENCE SETTING	WHO CAN SEE YOUR PROFILE?	PRIVACY STRENGTH	RECOMMENDATIONS
Public	Anyone	None	Not Recommended
Extended Circles	People in your circles plus individuals from their circles	Minimal	Not Recommended
Your Circles	People within your circles	Intermediate	Minimum Setting
Custom	Designated individuals or circles from your profile	Strong	Recommended
Only You	No one	Maximum	Recommended

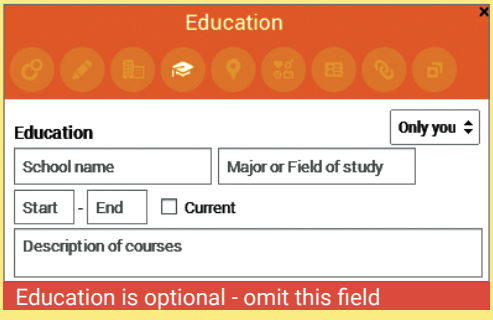


Set all fields to **Only You** or **Friends**.

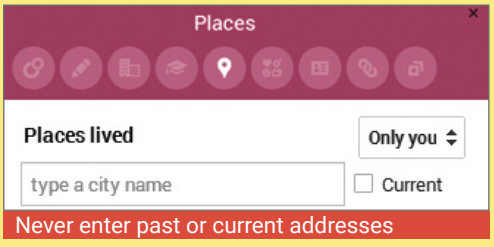
Taglines are always **Public** - leave field blank



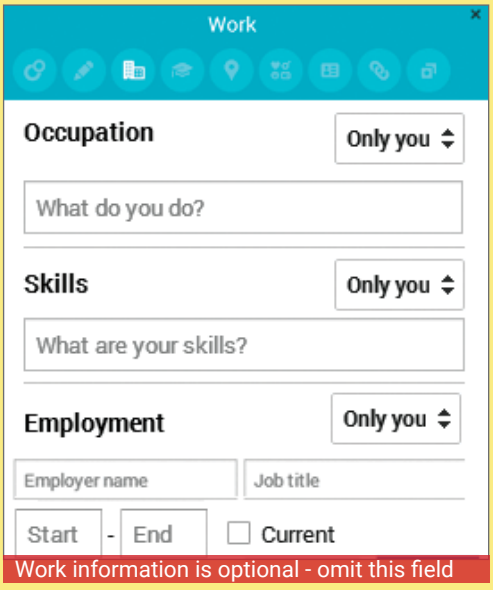
Uncheck both boxes to reduce profile reach



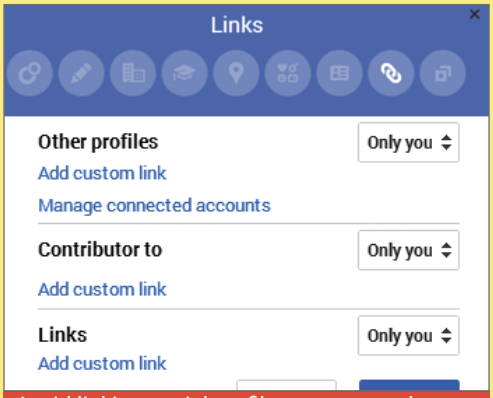
Education is optional - omit this field



Never enter past or current addresses

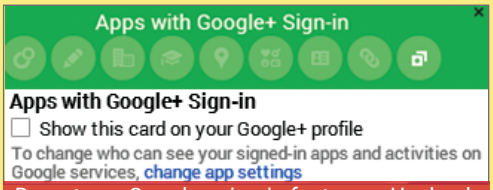


Work information is optional - omit this field



Avoid linking social profiles to one another

Never enter or display phone numbers



Do not use Google+ sign-in features - Uncheck

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 taken at a distance, at an angle, or otherwise concealed (e.g. sunglasses).
- Do not use your face as a profile photo, and do NOT enable location services for your smartphone camera or photo sharing apps.

CHOOSING THE RIGHT PHOTO SHARING SERVICES

Choosing the right photo sharing service for your needs depends both on your 1) intent for sharing and 2) audience. Key questions to consider are:

- Are you sharing photos primarily for yourself, your friends and family, or for public distribution
- Are your contacts or viewers already using a specific service?
- How much control do you need to maintain over your images? Would it be problematic if the service retained your photo's EXIF data?

Choosing the right photo sharing service dictates the amount of control you have in how your images are shared and distributed online. All services allow you to remove images you've previously posted, but not all services allow members to delete their accounts. However, it is important to remember deleting your content or your account does not ensure that photos you've once shared are removed from the Internet.

Eight popular photo sharing services are described below. Default privacy settings are noted in **bold**.

SERVICE	PRIMARY USE	PRIVACY OPTIONS?	EXIF?	LOCATION OPTIONS	ALLOW REPOSTING?	GOOGLE INDEXED?
flickr	Share photos within gruoped user environments	**Public**, Private, Contacts, Family, Friends	**Yes**, No	Manual locations, map-based	**Yes**, No	If Public (can opt-out)
	Social Networking Site (SNS)	**Public**, Friends of Friends, Only Me, Friends	No	Link to Facebook page, map-based, GPS-enabled device location	Yes	If Public
Instagram	Share photos directly from mobile phones	**Public**, Private (requests to follow must be approved)	No	GPS-based device location, customizable location, text search	No	If third-party apps enabled
photobucket	Share photos publicly or privately	**Public**, Private (optional password protection)	**Yes**, No	None	Yes	If Public
	Social Networking Site (SNS)	Public, **Circles**, Only You	Yes	Manual locations, map-based	Yes	If Public
	Microblogging, Social Networking Site (SNS)	**Public**, Private (requests to follow must be approved)	No	GPS-based device location, manual location for user profiles	Yes	If Public
Pinterest	Share concepts and ideas using images	**Public**	Yes	None	Yes	Yes

FLICKR

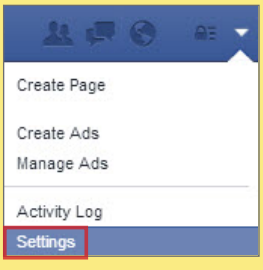
Flickr gives users a detailed set of controls over how their photos are shared across the web. In upper right, go to **Camera** > **Settings** > **Privacy & Permissions**. Set as follows to ensure your privacy:

- Who can access your original image files? **Your friends and family** or **Only You**
- Allow others to share your stuff? **No**
- Who can add you to a photo? Set to **Only You** and select **Remove me from all photos**
- 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 pubic searches? Check all three options
- Who can see what's on your profile? **Friends and family**
- Who will be able to see, comment on...? **Friends and family**
- Who will be able to see your stuff on a map? **Only You**
- Import EXIF location data? **No**

FACEBOOK

Facebook automatically compresses any uploaded images to a pre-selected size and deletes their EXIF data. These steps ensure added privacy in how your images are shared across the site. For privacy-maximizing settings, go to **Triangle** > **Settings** > **Privacy**:

- Who can see your future posts? **Friends**
- Limit the audience for old posts? **Limit Old Posts**

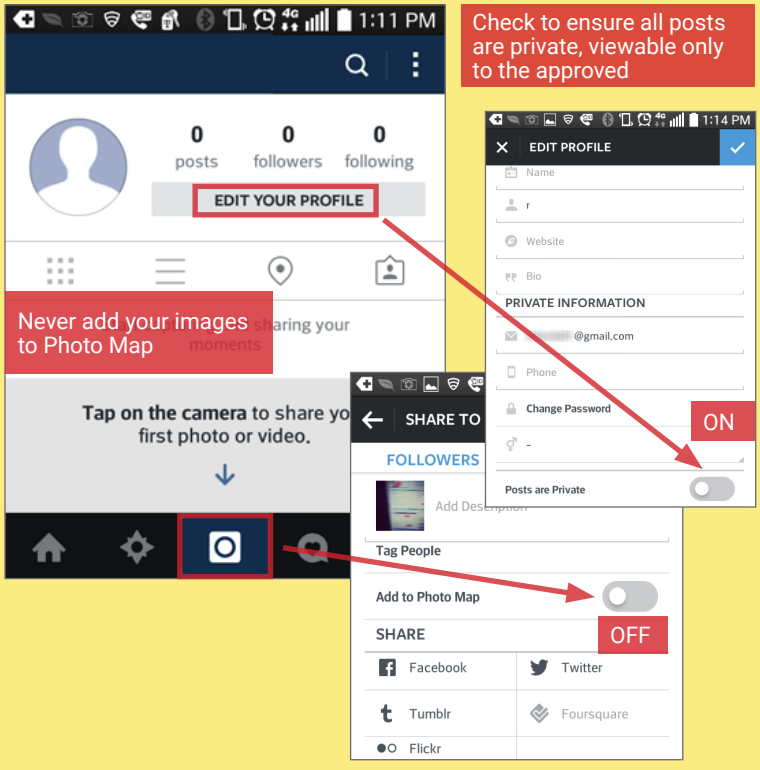


Then click **Timeline and Tagging**. Set as follows:

- Who can post on your timeline? **Friends**
- Review posts friends tag you in before they appear on your timeline? **Enabled**
- Who can see posts you've been tagged in on your timeline? **Friends**
- Who can see what others post on your timeline? **Friends**
- Review tags people add to your own posts on Facebook? **On**
- When you are 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 when photos that look like you are uploaded? **No One**

INSTAGRAM

Photos are made public by default on Instagram, but they can be made private by following these photographic instructions:



GOOGLE+

Google+ retains all EXIF data on photos by default but allows users multiple privacy settings to better control how their photos are shared. For maximum privacy-protective settings:

Navigate to Google+'s **DropDown Menu** > **Settings**.

Under Photos and Videos, set as follows:

- Show geolocation information. **Uncheck**
- Allows viewers to download my photos and videos. **Uncheck**
- Find my face in photos and videos. **Uncheck**
- People whose tags of you are automatically approved. **Groups and Persons**

Under **Profile**, set as follows:

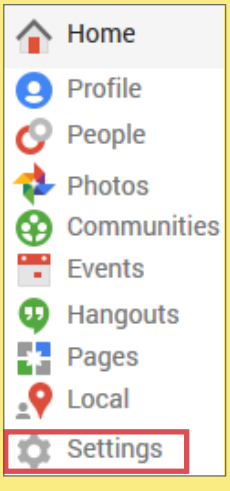
- Show these profile tabs to visitors. **Uncheck all**

Under **Hashtags**, set as follows:

- Add related hashtags from Google. **Uncheck**

Under **Location settings**, set as follows:

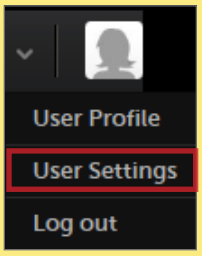
- Enable location sharing. **Uncheck**



PHOTOBUCKET

Photobucket is unique in its ability to allow users to share password-protected photos. For maximum privacy-protective settings:

In the upper right, go to **User Settings**.



On the Albums tab, uncheck all options listed under Links except Link back to albums.

Under **Privacy** set as follows:

- Allow others to follow me. **Uncheck**
- Allow comments in my albums. **Check**
- Show where my photos were taken. **Uncheck**
- Allow others to copy my photos & videos. **Uncheck**
- When I upload, permanently remove information about where my photos were taken. **Check**

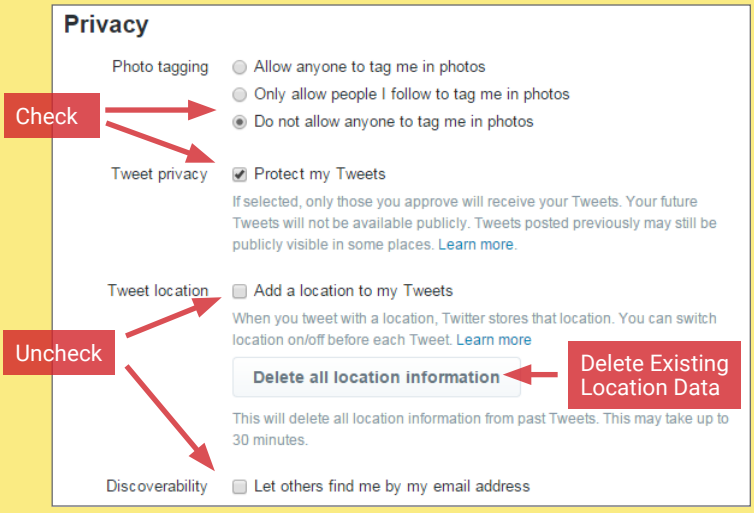
Under **Album Privacy**, for each album choose to either:

- Make Private – Only you can view, or
- Password Protect – Anyone with the URL link and the password can view
  - Remember, choose unique passwords for each album

TWITTER

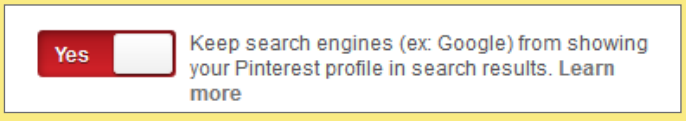
Upon uploading, Twitter removes all EXIF data associated with the photos but it provides minimal options for limiting photo's visibility across the site. For maximum privacy-protective settings:

In the upper right, go to **Settings** > **Security and Privacy**. Match your settings to those shown below under **Privacy** tab.



PINTEREST

Pinterest retains all EXIF data on photos and provides very limited privacy settings to control how the photos are shared. To enable protection, go to **Settings** under the dropdown menu on the upper right. Under **Basic Information**, set **Search Privacy** to **Yes**.



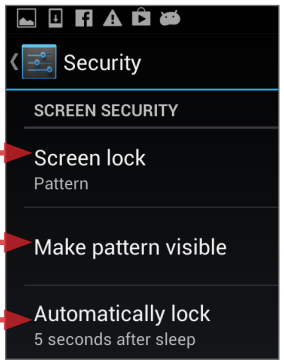
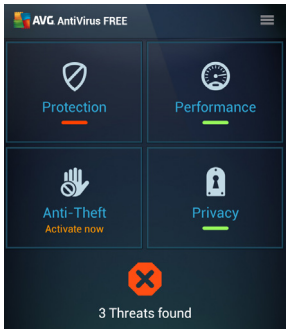
SMARTPHONES

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.

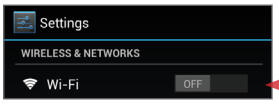
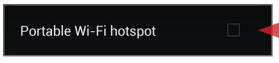
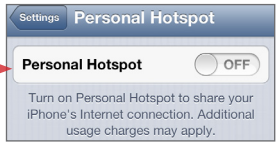
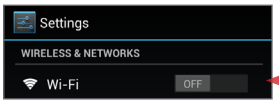
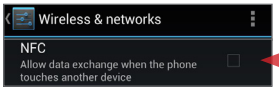
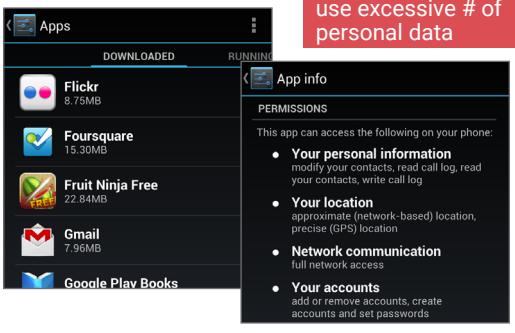
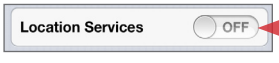
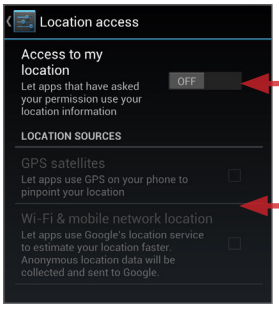
RISK SCENARIO	IPHONE	ANDROID
SMARTPHONE IS PHYSICALLY ACCESSED BY SOMEONE WITHOUT YOUR CONSENT - To prevent others from accessing data on your smartphone, set up a passcode to protect your information. Use all passcode styles made available by your phone (e.g. pattern lock, PIN, password, and fingerprints)	Navigate to **Settings** > **General** > **Passcode Lock** Use a complex password mixing letters + numbers Block access Optional setting 	Navigate to **Settings** > **Security** > **Screen Lock** 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**  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**  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**  Disable WiFi when not in use  Enable network permissions Navigate to **Settings** > **General** > **VPN** to enable and establish a VPN connection	Navigate to **Settings** > **WiFi** to manage connections  Disable WiFi when not in use Navigate to **Settings** > **More** > **Tethering & Portable Hotspot** and disable **Portable WiFi 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  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 	Navigate to **Settings** > **Bluetooth**  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  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**  Disable Siri Navigate to **Settings** > **Privacy** to manage which specific data each app accesses from your phone 	Navigate to **Settings** > **Apps** Delete apps that use excessive # of personal data 
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**  Only grant access to apps that require a location function  Disable all location services when not in use	Navigate to **Settings** > **Location Access**  Disable all location services when not in use Uncheck both boxes when location services are not in use

TRAVELING SAFELY WITH SMARTPHONES

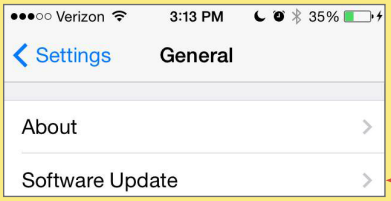
TRAVELING WITH SMARTPHONES - DO'S AND DON'TS

- Bring a dedicated loaner device; do not bring your personal smartphones.
- Use smartphones with removable batteries when possible.
- Assume that all information on your device could be compromised while traveling in a foreign country.
- Avoid social media, banking, and other sensitive sites while traveling. Never store passwords or sensitive information on your smartphones.
- Do not click on links in text messages or emails - especially from people you do not know.
- Do not jailbreak or root your smartphones. Upon your return, examine all mobile devices for evidence of tampering.

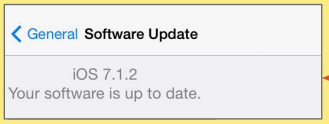
ENSURE THAT YOUR PHONE'S SOFTWARE IS UP TO DATE

Use applications on your phone to ensure that the software on your smartphone is up to date.

IPHONE

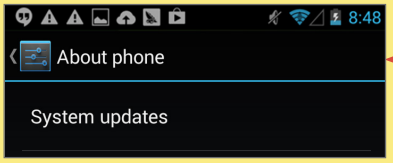


Go to Settings > General > Software Update.



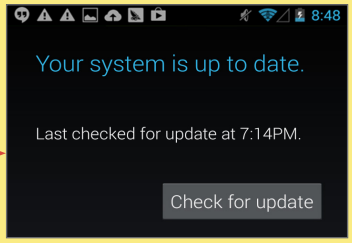
Check to see if your software is up to date; if not, your iPhone will prompt you to download the latest software.

ANDROID



Go to Settings > About Phone > System Updates.

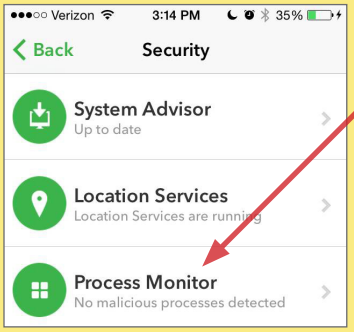
Check to see if your software is up to date; if not, your phone will prompt you to download the latest software



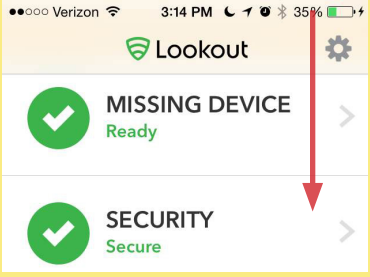
PROTECT YOUR PHONE AGAINST MALWARE

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

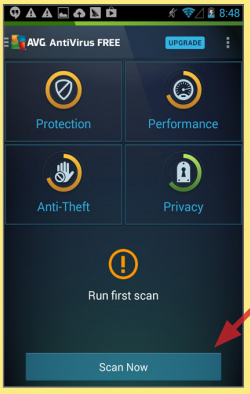
IPHONE



Use the **Lookout** app for iPhone. Go to Security > Process Monitoring to see if malicious processes are running.



ANDROID



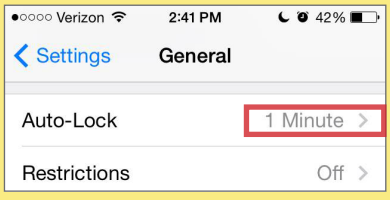
Use the **AVG Antivirus Free** app for Android. Click Scan Now to monitor for viruses.

SET YOUR PHONE TO LOCK AUTOMATICALLY

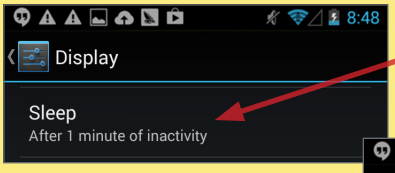
In case you lose your device, you want your smartphone to lock automatically to prevent physical access.

IPHONE

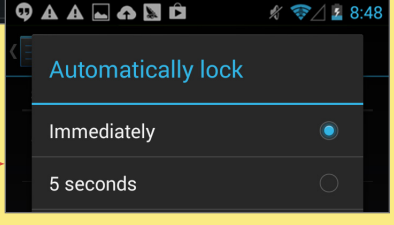
Go to Settings > General > Auto-Lock. Set the Auto-lock to 1 minute.



ANDROID



Go to Settings > Display > Sleep. Set the phone to sleep after 1 minute



Go to Settings > Security > Automatically lock > Immediately

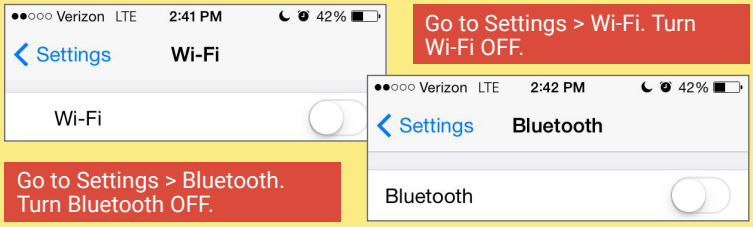
TRAVELING WITH SMARTPHONES - ADDITIONAL BEST PRACTICES

- Assume that your phone may be scanned forensically when you enter a foreign country.
- If possible, encrypt the data on your phone.
- Consider installing a VPN on your device as more secure alternative to saving information locally.

DISABLE WIFI AND BLUETOOTH

Disable WiFi and bluetooth on your smartphone; WiFi and bluetooth can render your smartphone vulnerable to malware and hacking.

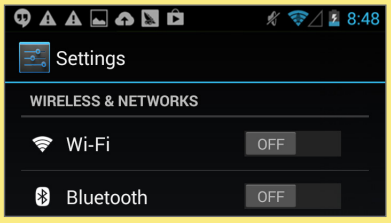
IPHONE



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

Go to Settings > Bluetooth. Turn Bluetooth OFF.

ANDROID

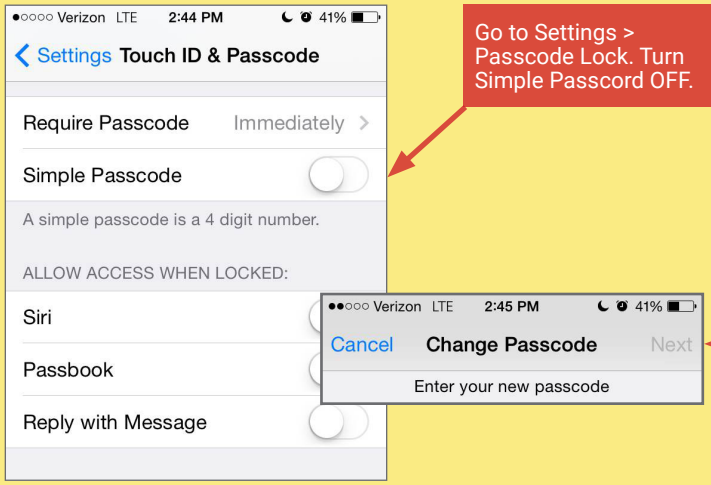


Go to Settings > Wireless & Networks. Turn both Wi-Fi and Bluetooth OFF.

USE A 10+ CHARACTER PASSWORD OR SCREEN LOCK PATTERN

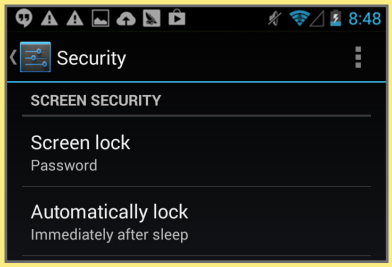
Short passwords are vulnerable to brute force attacks. Choose a password with a combination of letters, numbers, and symbols. If using a Screen Lock Pattern, choose a complicated pattern.

IPHONE

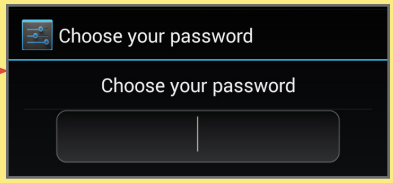


Go to Settings > Passcode Lock. Turn Simple Passcord OFF.

ANDROID



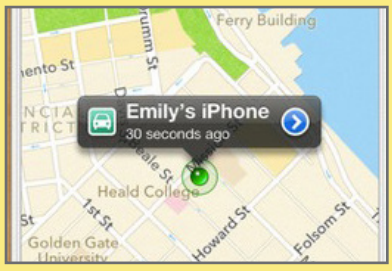
Enter a new passcode with 10+ characters, symbols, and numbers



RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

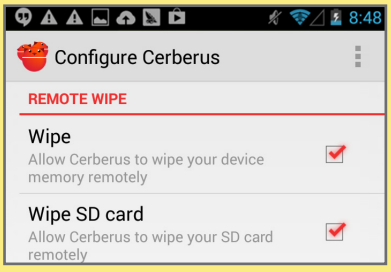
Find my iPhone and **Cerebus** can locate lost devices and wipe data remotely from lost or stolen smartphones.

IPHONE



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

ANDROID



Use the Cerebus app to recover lost or stolen Android smartphones and wipe data remotely from the device memory and SD card

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)

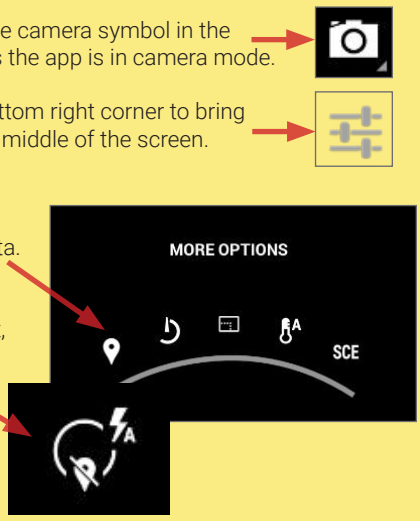
Turn off iOS location services to ensure images captured with the native iPhone camera app will not contain any gelocation EXIF data.

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.

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.

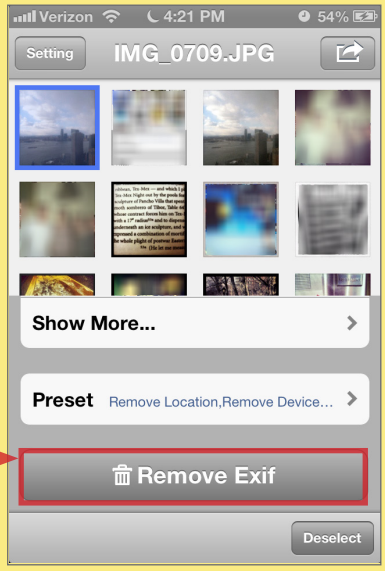


EXIF REMOVAL SMARTPHONE APPS

TRASHEXIF FOR IOS

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

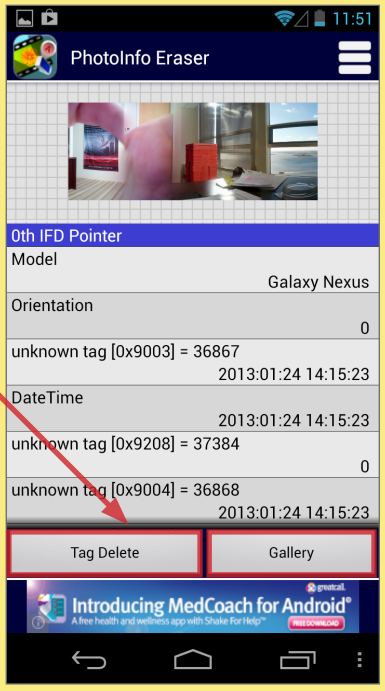
1. Download the TrashEXIF app from the **App Store.**
2. Open the TrashEXIF app and select photo(s) which you want EXIF data removed.
3. Select **Presets**, then in the **Removal Presets** window, select **Remove Location** and **Remove Device Information**.
4. Return to the pervious screen by clicking 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.

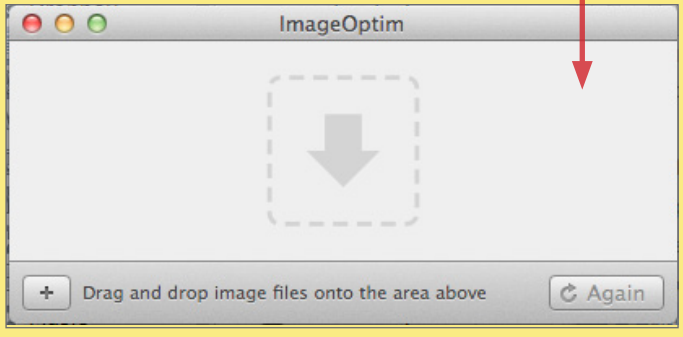
1. Download PhotoInfo Erase from the **Play Store**.
2. Open the PhotoInfo Eraser app and select **Gallery**.
3. Navigate your phone and select an image.
4. Select **Tag Delete** and press OK.
5. Click **Gallery**. A copy of your photo without EXIF data is now available in the **PIEraser** folder.



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.

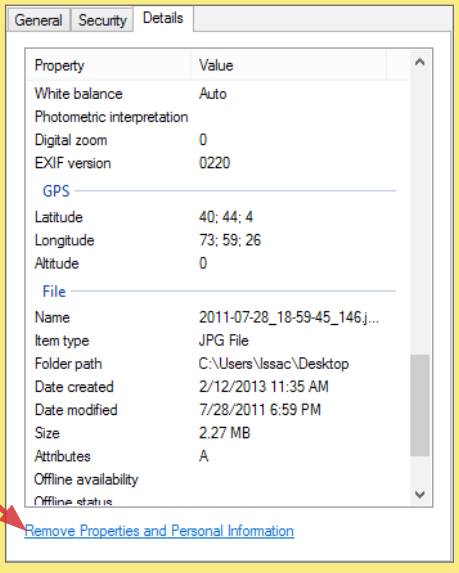


3. Check that the EXIF data has been removed by right-clicking the image and select **Get Info**. EXIF data is listed under **More Info**.

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.



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

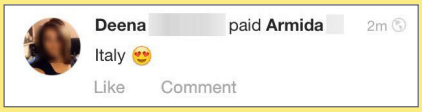
Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile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



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

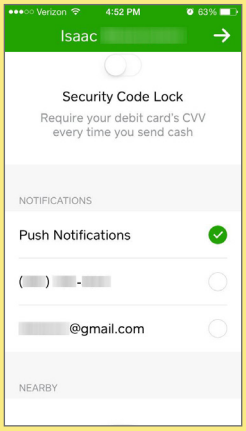
You should consider the following questions when choosing a mobile wallet:

- 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



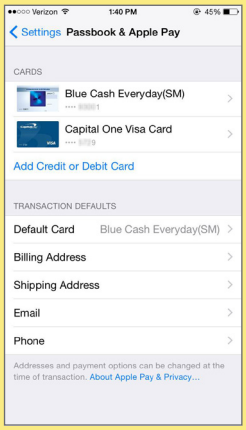
Navigate to **Settings** in the upper left portion of the home screen:

- 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.

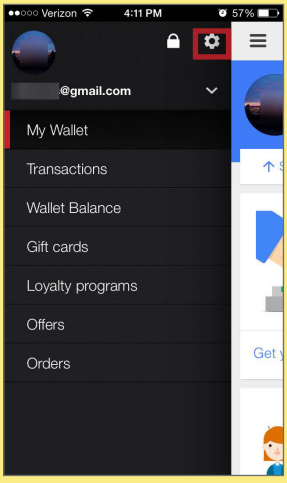
Note that an unauthorized user of your iPhone can view the last 4 digits of your cards, your billing address, shipping address, email address, and phone number.

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.

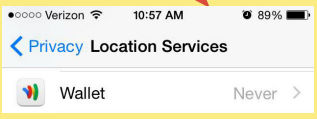
GOOGLE WALLETS

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**.

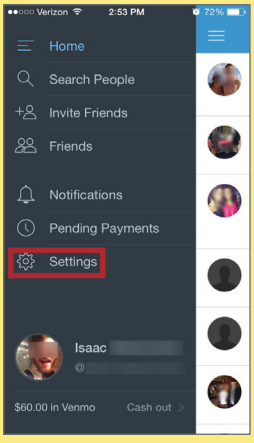


Note to Android users: It is recommended you disable all location services by navigating to **Settings** > **Personal / Location Access**

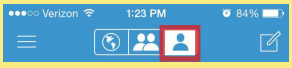
VENMO

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.

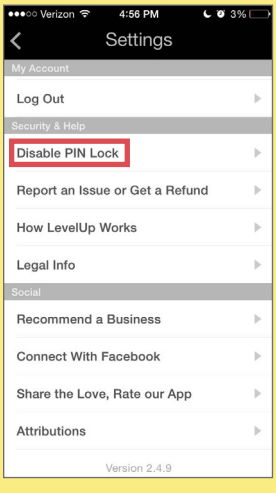


Monitor your transaction activity by clicking on the logo of a single person at the top of the home screen.



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

LEVELUP

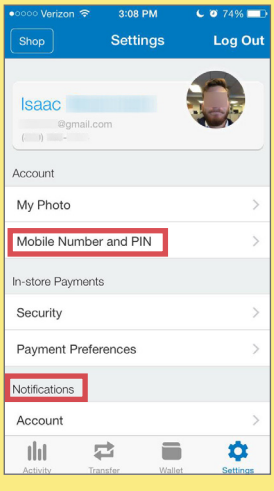


Navigate to the **Settings** menu, found in the top left corner of the home screen:

- 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

- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest access set up, ensure that it is password protected.
- When possible, turn on automatic updates for your network device's firmware. If automatic updates are not offered, periodically check for firmware updates on the network devices' websites and manually download and install them.
- Position the router away from windows and further into the interior of your house to decrease the exterior reach of the signal.
- Use a cable to directly access the Internet for any computers that remain stationary.

GLOSSARY OF COMMONLY USED TERMS

- **Wireless Router** - Physical hardware that allows users to connect their devices to a shared Internet network.
- **Service Set Identifier (SSID)** - The public name of a wireless network.
- **Wired Equivalent Privacy (WEP)** - Older security algorithm for wireless networks that has numerous security flaws.
- **Wi-Fi Protected Access (WPA)** - More recent security algorithm for wireless networks. Also has many security flaws.
- **Wi-Fi Protected Access II (WPAZ)** - The most secure algorithm for wireless networks. Improved upon and replaced WPA.
- **Pre-shared key (PSK)** - An authentication mechanism that mandates a password. Adds additional security to wireless networks.
- **Hypetext Transfer Protocol (HTTP**) - Protocol for communication over a computer network.
- **Hypertext Transfer Protocol Secure (HTTPS)** - Uses various encryption protocols to add additional security to HTTP.
- **Media Access Control (MAC) Address** - A unique, individual identifier assigned to computers and devices.

ACCESSING YOUR ROUTER

To access your router, you must enter the appropriate IP address, username, and password. Most routers share similar log-in information.

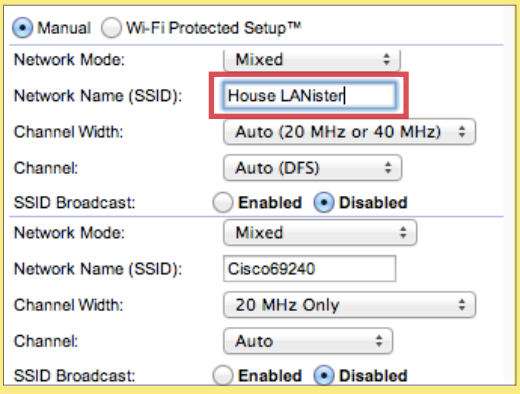
ROUTER	IP ADDRESS	USERNAME	PASSWORD
3Com	192.168.1.1	n/a	admin
Apple	192.168.1.1	admin	admin
Asus	192.168.1.1	admin	admin
Belkin	192.168.2.1	admin	n/a
Dell	192.168.1.1	n/a	admin
Linksys	192.168.0.1	admin	admin
Medialink	192.168.0.1	n/a	admin
Motorola	192.168.100.1	admin	motorola
Netgear	192.18.0.1	admin	password
TP-LINK	192.168.1.1	admin	admin
US Robotics	192.168.1.1	admin	admin

CHANGING THE USERNAME AND PASSWORD

Choose an username that does not include you or your family's names and a password that is long and complex.

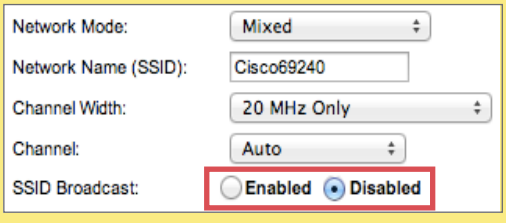
CREATING A UNIQUE SSID

Choose a SSID that does not include you or your family's names or physical address.



DISABLING THE SSID BROADCAST

This prevents the SSID from being listed under available Wi-Fi networks, thereby requiring users to know and enter the SSID before connecting to the network.

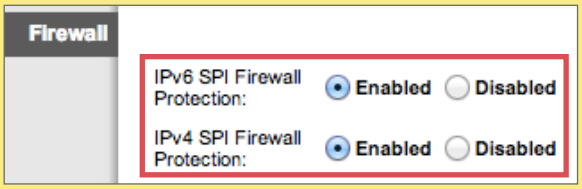


SETTING UP YOUR WIRELESS NETWORK - BEST PRACTICES

- When creating passwords for your network's devices, ensure that they are sufficiently long and complex by using uppercase letters, lowercase letters, numbers, and symbols. Consider a multi-word phrase that does not consist of dictionary-based words. An example of a satisfactorily long and complex password would be ILuvF00tb@77 from the phrase "I love football."
- If your router is compromised, or if you cannot remember the password, you can restore it to its factory settings by pressing the reset button located on the back of the router.

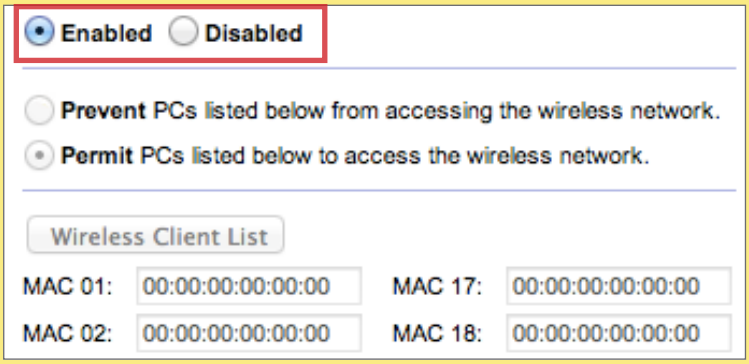
ROUTER FIREWALL

Enable the router's firewall protection to limit its vulnerability to viruses and cyber attacks.



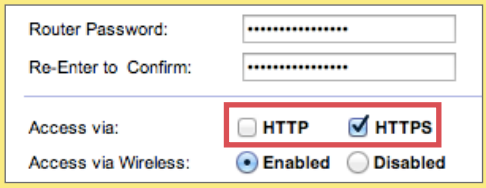
WIRELESS MAC FILTERING

Enable MAC address filtering to ensure that only approved computers and devices can connect to your router.



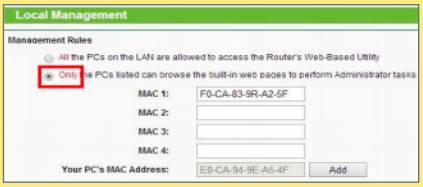
ENABLING HTTPS

Enable access via HTTPS to add additional layer of security.



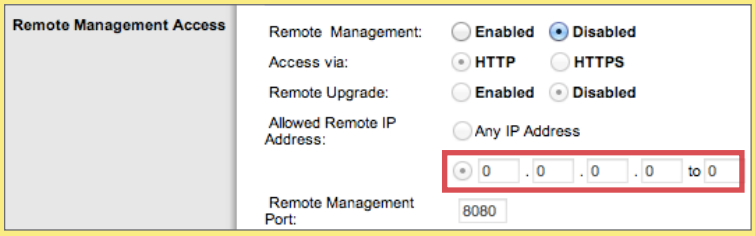
LIMITING ADMINISTRATIVE ACCESS

Restrict administrative access through the web to specific devices. Add the MAC addresses for each computer and device you wish to have administrative access.



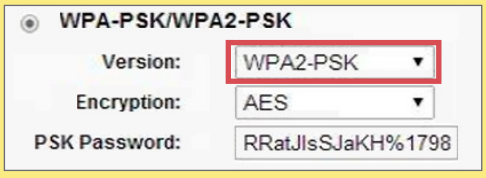
REMOTE ACCESS

Check that the Remote Management IP Address is set to **0.0.0.0** to ensure that remote access is disabled.



ENCRYPTION

Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select **WPA2-PSK** and also **AES** for encryption. The PSK password should be long and complex, but different than the administrative router access password.



ONLINE REGISTRATION

ONLINE REGISTRATION - DO'S AND DON'TS

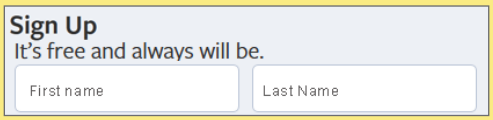
- Online services include any sites that require users to register for personal profiles prior to using their functionality.
- Review the service's terms of service to determine their data sharing policies with third party entities.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your social security number or physical address.
- Turn down options to upload and share your existing contacts with the new social networking service during registration.
- Change privacy settings to protect your identity information immediately after registering for an online profile.

IDENTIFY ELEMENTS OF SNS ACCOUNTS

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

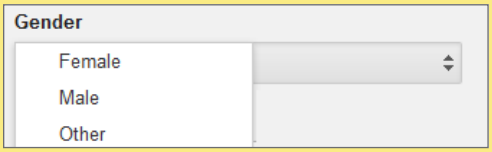
FIRST AND LAST NAME

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.



GENDER

Gender is a common field to fill out on the registration page, used mostly for future content customization. Whenever possible, avoid making a distinction when signing up for your account.



LOCATION: ADDRESS, ZIP, COUNTRY

Location information is required at varied levels of granularity depending on the service. It may include address, zip code, and/or country. Sign up by filling out the most generic location level required by the service (i.e. Country only, or City, State only, etc).

FACEBOOK ACCOUNT

Many services allow users to sign up for their service using Facebook Connect, enabling users to quickly create new accounts by importing existing data from Facebook. Avoid opting for this step unless the service requires it.

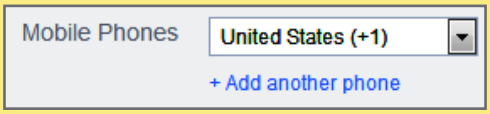
USERNAME

Username is unique to each user account, unlike first and last name which can be shared across multiple users. **DO NOT** include personally identifiable information, such as last name or birthday, when making your username.

DO NOT use the same password or username across your SNS Accounts. Use unique passwords for each of your accounts.

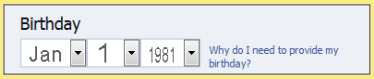
MOBILE PHONE NUMBER

Registering for email accounts frequently requires a verifiable phone #. Refrain from using services that require phone #s or opt to use an alternative method to verify accounts.



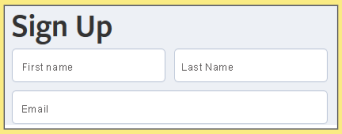
BIRTHDAY

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. Most services only require users to be 18+, and you should use a false birthday or birth year.



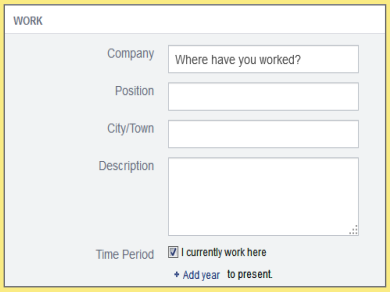
EMAIL ADDRESS

Email is the 2nd most common requirement for creating a SNS account. It is used to **verify your account** during registration and often used as a credential during future log-ins. Avoid using your business email address.



COMPANY/EMPLOYMENT INFO

Company and employment information are required for professionally-oriented SNS services, such as LinkedIn, where the main purpose is to meet and build your network with other people in your field. Limit the amount of this data that you provide and keep location information generic.



RELATIONSHIP + ORIENTATION

These fields are most often required in **online dating sites**, where the main purpose is to meet people. Always provide only the required minimum amount of data.

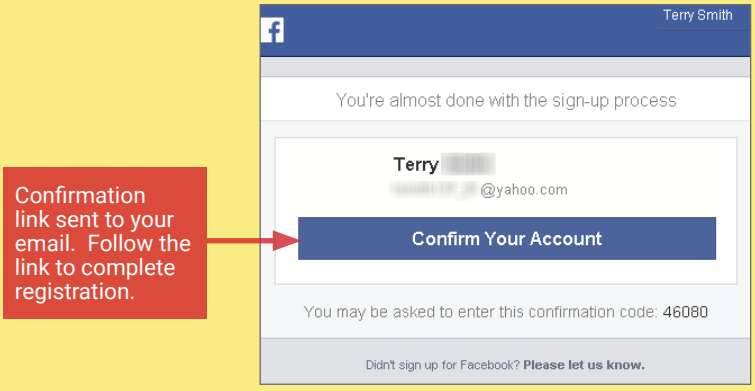
IDENTIFY INFORMATION REQUIRED DURING REGISTRATION BY SERVICES

	in	f		g+	YAHOO!	msn	FOURSQUARE		okc
First and last name	X	X	X	X	X	X	X	X	
Username			X	X	X	X		X	X
Password	X	X	X	X	X	X	X	X	X
Birthday		X		X	X	X	X		X
Gender		X		X	X	X	X	X	X
Email address	X	X	X			X	X	X	X
Phone number				Optional	X	Optional			
Country	X			X		X			X
Company / employment	X								
Job title	X								
Zip code	X					X			X
Facebook account	Optional				Optional		Optional	Optional	Optional
Sexual orientation									X
Relationship status									X

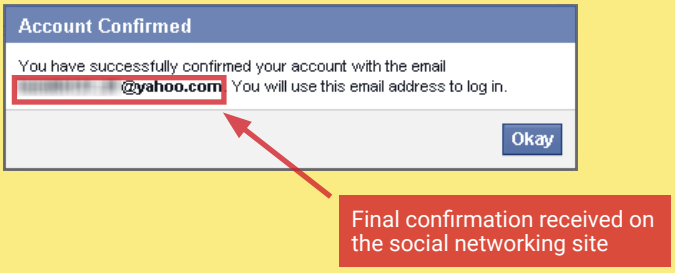
ONLINE REGISTRATION AND VERIFICATION PROCESS

1. Enter required identity fields on the registration page.

2. Confirm your account via email. Avoid using mobile phone verification when possible to prevent sharing additional personal contact information.



3. Finish the confirmation process on the service website.



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 / 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 - VEROMI

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

Opt out of PrivateEye by completing the form at:
https://secure.privateeye.com/optout-form.pdf

Opt out of PeopleFinders and PublicRecordsNow by visiting:
peoplefinders.com/manage/

Opt out of Veromi by visiting:
veromi.net/Help#27

www.privateeye.com
www.peoplefinders.com
www.publicrecordsnow.com
www.veromi.com

WINK - MYLIFE

Wink is owned and operated by MyLife, so the same opt out instructions apply for both.

Call MyLife at (888) 704-1900 and press 2 to speak to an operator. Have the following information ready: name, age, date of birth, email, current address, and one previous address. Tell the representative that you want your listing removed and provide the information you want deleted. Be sure to specifically request your information is removed from Wink.com as well as MyLife.com. Once they confirm the removal, the listing will be off the site in 7-10 days.

www.wink.com
www.mylife.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 drivers license to the listed address or fax number.
www.ussearch.com

INTELIUS - PUBLIC RECORDS - ZABASEARCH - SPOCK - ISEARCH - DATECHECK - LOOKUP - PEOPLEFINDER - LOOKUPANYONE - PEOPLE LOOKUP - 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 at 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."

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.

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. To do this, click the listing containing your information, then click the **Claim and Edit** and login buttons. Once an account is created, privatized the desired information using the **Edit** buttons . Additionally, check the box under **Hide** and hit the update button to finalize changes. Delete all information whenever possible.

www.whitepages.com

INSTANTCHECKMATE

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

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 operating system and anti-virus software protection.
- Never share 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.

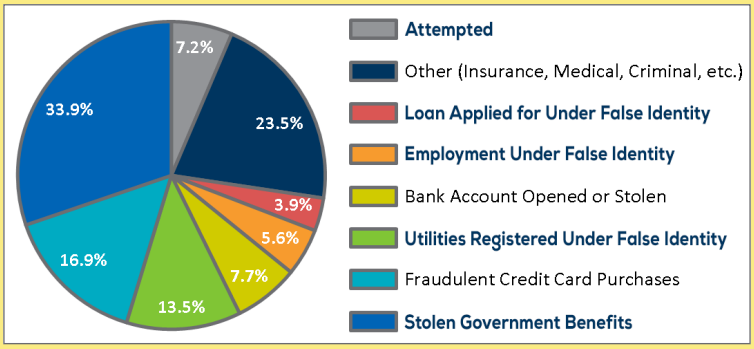
SENSITIVE DATA

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

POTENTIALLY HARMFUL

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

WHAT IS AT RISK?



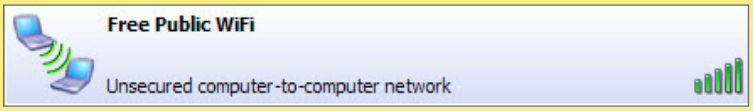
*Percentages are according to the Consumer Sentinel Network for total theft reports in 2013. Some reports contained multiple theft types.

ID THEFT TYPES

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

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.



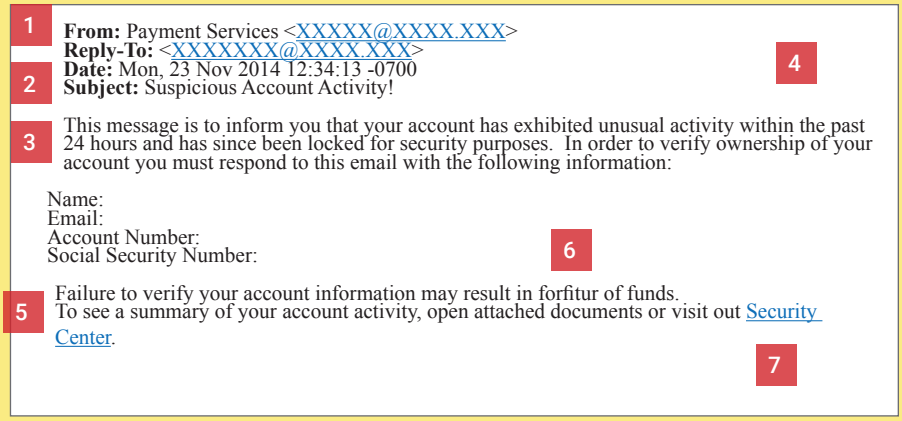
SOCIAL MEDIA MINING

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. This information can then be used to open fraudulent accounts or assume control of existing accounts. The model below outlines the common identifiers of a phishing email.

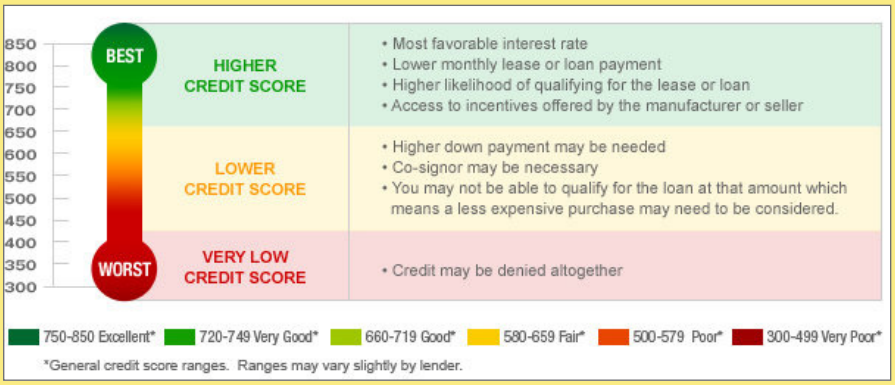
1. Non-descriptive sender or mismatched email addresses (e.g. "From" and "Reply-To" addresses do not match)
2. Unprofessional subject titles.
3. Phrases demanding the user to share personal information.
4. Absence of a company logo within the email header.
5. Threats to close accounts without compliance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



SIGNS OF IDENTITY THEFT

Credit scores can be damaged through identity theft. The damages from identity theft can be reduced significantly if caught early. Bank statements should be checked weekly while each of your 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 call to inform about delinquent debts.
- Problems filing insurance claims.
- Fraud alerts activated on credit cards.



IDENTITY THEFT PROTECTION SERVICES

Select companies offer services to monitor customers' credit scores and protect their personal information online. Each company will work 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 SERVICES OFFERED	SSN	BANK ACCOUNT	CREDIT CARD NUMBERS	MEDICAL INSURANCE	CRIMINAL	DRIVER'S LICENSE	COMPUTER SECURITY	FINANCIAL COVERAGE	PRICE PER MONTH
IDENTITY GUARD www.IdentityGuard.com	X	X	X	X	X		X	Up to $1 Million	$14.95
IdentityForce. Protect What Matters Most	X	X	X	X	X	X	X	Available	$14.99

IDENTITY THEFT PROTECTION SERVICES

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.

Request Your Credit Scores:
Look for inconsistencies in your credit reports and send letters explaining the misuse to each of the three credit reporting companies. Contact the fraud department of each business that reported a fraudulent transaction on an account in your name.

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 IdentityTheft.gov. Together these documents make up an identity theft report and can be used to remove fraudulent activity from your credit report and obtain information about accounts the identity thief opened or misused.identity data during online activity.

EQUIFAX®	Experian	TransUnion®
1-800-525-6285	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.

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.

ADVANCE SETUP

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

FILTERS

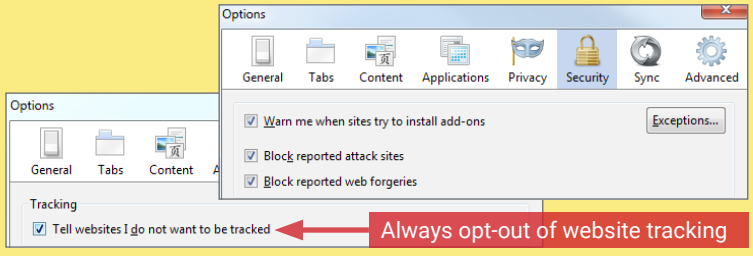
YouTube Filter - filters individual YouTube channels and videos for content.
Content Filtering - identifies specific words in webpages to prevent access.
Black/White List - allows users to add specific URL's to block or allow.

TIME CONTROL

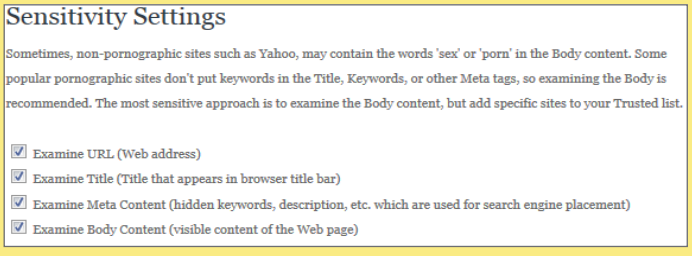
Set a time frame of acceptable computer use for your child that permits an adult supervisor to be present.

FIREFOX SETTINGS

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



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.



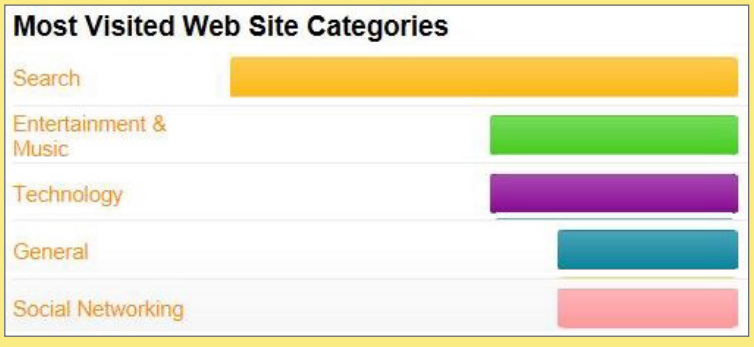
OVERVIEW

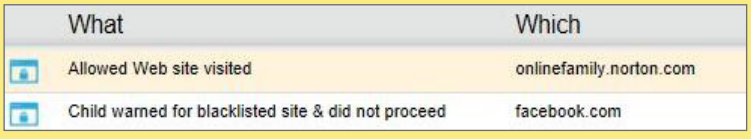
A variety of free and paid software are available for monitoring your child's online activities. The software listed below are effective in either preventing or monitoring content that your child tries to access.

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.

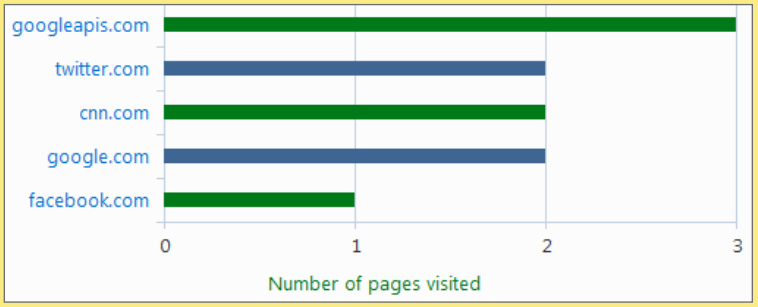




Norton Family identifies SNS profiles that children maintain and allows supervisors to see what they are sharing with the public (name, age, profile picture, etc.). It also prevents children from sharing personal information including phone numbers, Social Security numbers, and email addresses.

MICROSOFT FAMILY SAFETY

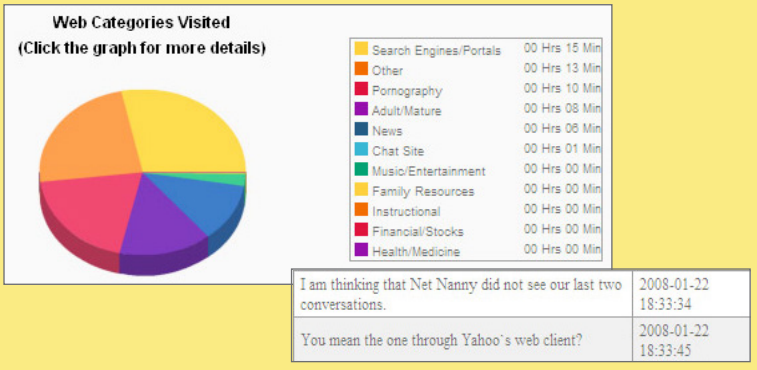
Download this free service from the Microsoft Windows website. The service provides basic content filters and reports of programs/websites accessed by each account.



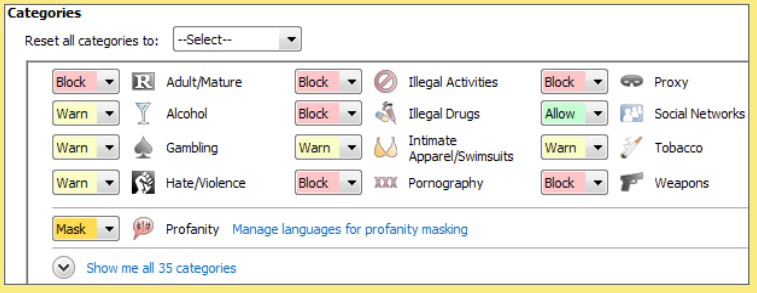
Parents can set individualized settings for each account and view their child's requests to access blocked content each time they log in.

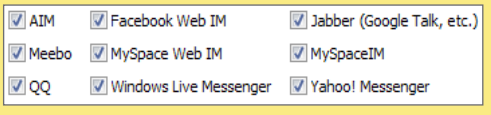
NET NANNY

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.



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.





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.

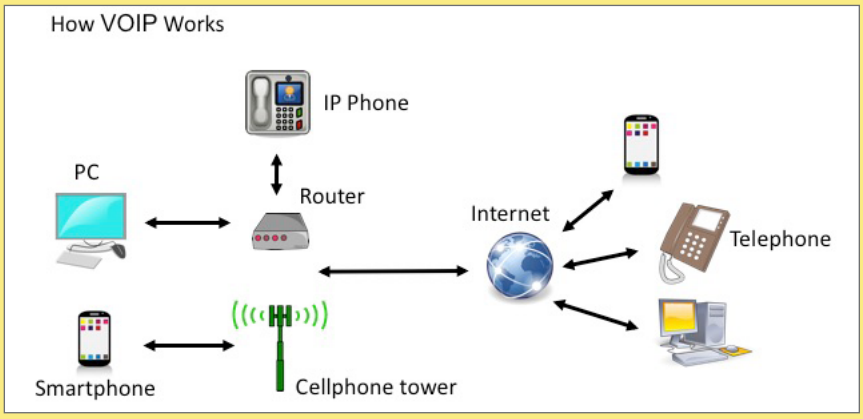
Some providers do not connect to 911 or information services, so a second phone line may be needed.

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:

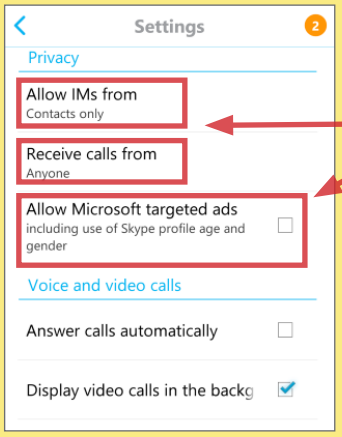
- Are all calls on the provider network encrypted? For calls to landline phones, the portion of calls carried on the legacy network is not encrypted.
- Are messages encrypted in transit and at rest so even the provider can not access them?
- Does the provider use firewalls, redundant servers, and 24/7 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



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.

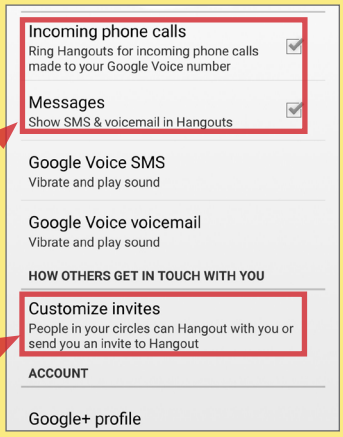
HANGOUTS

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**:

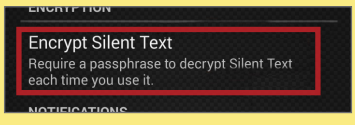
- Check **"Incoming phone calls"** and **"Messages"** for Hangouts to manage all calls, texts, and voicemail.
- Customize who can contact you directly and who needs an invite.



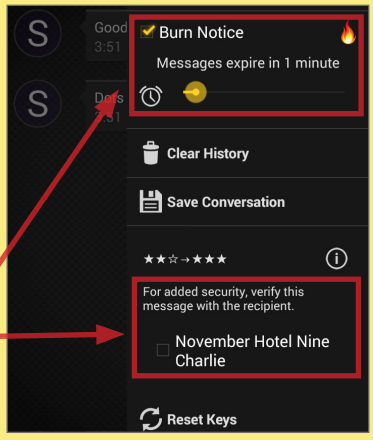
SILENT CIRCLE

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

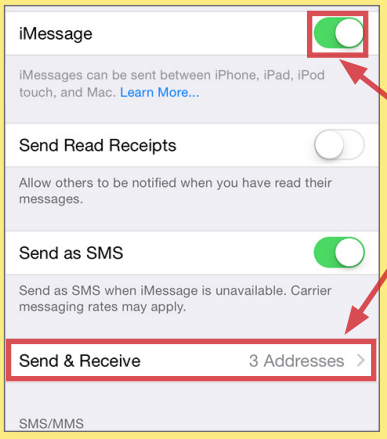
In **Settings**, select **"Encrypt Silent Text"** and select a passphrase (14 characters is recommended).



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



FACETIME



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.

NOTES


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA